



FritzOS 7.20: Mehr Schutz für die Privatsphäre aktivieren

# Fritzbox absichern

Sicher surfen, vertraulich telefonieren,  
WLAN besser verschlüsseln



- Kompaktkamera gegen Fotohandy
- Hybrid-Notebook mit Tiger-Lake-CPU
- Samsungs große Stift-Tablets
- Shopsysteme für Online-Händler

TVs und HDR-Monitore bis 65 Zoll und 144 Hz

## Große Gaming-Displays

Tutorial zur Open-Source-Software

## Kreativ malen mit Krita

Flugsimulator-Controller mit Arduino

PC-Ersatz: Smartphone am Monitor

Medientrend Newsletter

Windows 10 kaufen: Die FAQ



Formate und Strategien zur Datenkonservierung

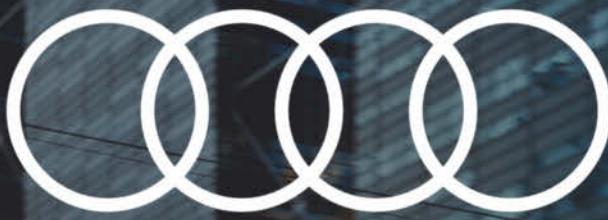
## Ihre Daten für immer speichern

Langzeitarchivierung mit Festplatte, M-Disc und Cloud



€ 5,20

AT € 5,70 | LUX, BEL € 6,00  
NL € 6,30 | IT, ES € 6,50  
CHF 7.60 | DKK 57,00



# Elektrisierende Gelegenheit.

Jetzt exklusiv für Businesskunden<sup>1</sup>: rein elektrisch Audi e-tron fahren für nur € 399,– pro Monat zzgl. MwSt.



Jetzt digital erleben.  
Kosten laut Mobilfunkvertrag.

Sichern Sie sich den Umweltbonus inklusive Innovationsprämie<sup>2</sup>.

**€ 399,–**

pro Monat zzgl. MwSt.

Leasingbeispiel für Businesskunden<sup>1</sup>: Audi e-tron S line 50 quattro<sup>3</sup>

<sup>3</sup> Stromverbrauch (kombiniert) in kWh/100 km: 23,6–21,4 (NEFZ); 25,8–21,7 (WLTP); CO<sub>2</sub>-Emissionen (kombiniert) in g/km: 0; Effizienzklasse: A+. Angaben zu den Kraftstoff-/Stromverbrächen und CO<sub>2</sub>-Emissionen bei Spannbreiten in Abhängigkeit von der gewählten Ausstattung des Fahrzeugs.

Leistung:	71 kWh/230 kW
Vertragsdauer:	36 Monate
Jährliche Fahrleistung:	10.000 km
Monatliche Leasingrate:	€ 399,– zzgl. MwSt.
Sonderzahlung (entspricht Bundesanteil am Umweltbonus <sup>2</sup> ):	€ 5.000,–

Ein Angebot der Audi Leasing, Zweigniederlassung der Volkswagen Leasing GmbH, Gifhorner Straße 57, 38112 Braunschweig. Zzgl. Überführungskosten und MwSt. Bonität vorausgesetzt. Nur beim teilnehmenden Audi Partner erhältlich.

<sup>1</sup> Das Angebot gilt nur für Kunden, die zum Zeitpunkt der Bestellung bereits sechs Monate als Gewerbetreibender (ohne gültigen Konzern-Großkundenvertrag bzw. in keinem gültigen Großkundenvertrag bestellberechtigt), selbstständiger Freiberufler, selbstständiger Land- und Forstwirt oder Genossenschaft aktiv sind.

<sup>2</sup> Etwasige Rabatte bzw. Prämien sowie der Herstelleranteil am Umweltbonus sind im Angebot bereits berücksichtigt. Der Erwerb (Kauf oder Leasing) eines neuen Audi e-tron 50 quattro<sup>4</sup> durch Privatpersonen, Unternehmen, Stiftungen, Körperschaften und Vereine nach dem 18.05.2016 wird mit dem Umweltbonus inklusive Innovationsprämie gefördert, sofern das Fahrzeug nach dem 03.06.2020 und bis zum 31.12.2021 zugelassen und der Erwerb nicht zugleich mit anderen öffentlichen Mitteln gefördert wird. Das Fahrzeug muss im Inland auf den/die Antragsteller/-in zugelassen werden (Erstzulassung) und mindestens sechs Monate zugelassen bleiben. Sofern das Fahrzeug nach dem 04.11.2019 erstmalig zum Straßenverkehr zugelassen wird, beträgt die Höhe des Umweltbonus inklusive Innovationsprämie insgesamt € 7.500,–. Ein Drittel des Umweltbonus wird seitens der AUDI AG direkt auf den Nettokaufpreis gewährt, zwei Drittel des Umweltbonus (Bundesanteil am Umweltbonus inklusive Innovationsprämie) werden nach positivem Zuwendungsbescheid auf Antrag beim Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) unter [www.bafa.de](http://www.bafa.de) ausbezahlt. Der Antrag auf Gewährung des Bundesanteils am Umweltbonus muss spätestens ein Jahr nach Zulassung über das elektronische Antragsformular unter [www.bafa.de](http://www.bafa.de) eingereicht werden. Auf die Gewährung des Umweltbonus besteht kein Rechtsanspruch und die Förderung endet mit Erschöpfung der bereitgestellten Fördermittel, spätestens jedoch zum 31.12.2025. Nähere Informationen zum Umweltbonus sind auf den Internetseiten des BAFA unter [https://www.bafa.de/DE/Energie/Energieeffizienz/Elektromobilitaet/Neuen\\_Antrag\\_stellen/neuen\\_antrag\\_stellen.html](https://www.bafa.de/DE/Energie/Energieeffizienz/Elektromobilitaet/Neuen_Antrag_stellen/neuen_antrag_stellen.html) abrufbar.

Das abgebildete Fahrzeug ist teilweise mit Sonderausstattungen gegen Mehrpreis ausgerüstet.



## Archivierung: Einfach mal machen

Mehr als hunderttausend Fotos liegen auf der Festplatte, gigabyteweise Filme; teils sind die Kinder drauf, teils haben sie die Filme selbst gedreht und geschnitten. Dazu Hunderte von c't-Artikeln, Briefe, die Steuererklärungen der vergangenen Jahre und die Diplomarbeit von 1984. Von Lizenzschlüsseln oder eher unwichtigen Dingen wie Downloads oder gekaufter Software für längst nicht mehr erhältliche Betriebssysteme mal ganz abgesehen. Ein über viele Festplatten gewachsenes Durcheinander, das durch die Dateien von Frau und Kindern immer komplexer wurde.

Klar, es gibt ein Backup auf einem NAS. Und auf einer USB-Festplatte. Und vor einigen Jahren habe ich noch Fotos auf DVDs gebrannt, die liegen bei den Schwiegereltern im Tresor. Ob die noch lesbar sind? Keine Ahnung. Bislang hatte ich keinen Grund, das auszuprobieren; noch hatte ich keinen Datenverlust.

Daher war der Druck, mich um ein ordentliches Archiv zu kümmern, bislang eher gering. Das mag anderen anders gehen: Wer erst einmal eine Reihe von unwiederbringbaren Erinnerungen im digitalen Nirvana verloren hat, der wird vorsichtig.

Doch jetzt, wo die Abende länger werden und man Freundschaften eher virtuell pflegt, bleibt einem ja etwas Zeit. Zeit, mal kräftig aufzuräumen, auszumisten und wirklich Aufhebenswertes dauerhaft zu sichern. Das Auswählen ist zwar oft

schwierig, lässt einen die alten Erinnerungen aber auch neu entdecken. Genau solche Sachen gehören dann auch in das eigene persönliche Archiv. Doch auf welchem Medium speichert man das?

Festplatten sind naheliegend, doch wir haben uns auch alte Sachen (Silberscheiben) und moderne Aufbewahrungsmöglichkeiten (Cloud) angeschaut. Was davon am besten für die Aufbewahrung über Jahrzehnte geeignet ist, lesen Sie ab Seite 64. Außerdem geben wir Tipps zu Konzepten und Strategien der Langzeitarchivierung (Seite 60).

Von der Wunschvorstellung, sich nach dem Speichern der Daten im Archiv nie wieder darum kümmern zu müssen, verabschieden Sie sich jedoch am besten gleich. Unternehmen kopieren ihre Archive alle paar Jahre auf neue Medien; diese Arbeit droht auch Privatleuten. Immerhin aber sind die Daten dann schon einmal sortiert und Sie wissen, was zu tun ist. Sie müssen es nur einfach mal machen.



*Lutz Labs*

Lutz Labs

# Inhalt c't 22/2020

## Titelthemen

### Fritzbox absichern

- 14 **FritzOS 7.20** schützt Ihre Privatsphäre
- 18 **Telefonate verschlüsseln** Aktiviert mit fünf Klicks
- 22 **DNS-over-TLS** bietet Schutz beim Surfen
- 26 **WPA3** für mehr Sicherheit im WLAN

### Ihre Daten für immer speichern

- 60 **Langzeitarchivierung** Ihrer digitalen Daten
- 64 **Festplatten** als Langzeitarchiv
- 68 **M-Disc** Speichermedium für 1000 Jahre
- 72 **Cloudspeicher** als „Cold Storage“

### Große Gaming-Displays

- 100 **TVs und HDR-Monitore** bis 65 Zoll und 144 Hz

## Aktuell

- 12 **Europa-Cloud** Gaia-X tritt an
- 30 **Online-Werbung** Keine Cookies? Kein Problem!
- 32 **Internet** Firefox 81 bunter und funktionsreicher
- 34 **Registrierkassenverordnung** Rechtsunsicherheit
- 35 **KI** Ergebnisse der Enquete-Kommission
- 36 **c't testet VW ID.3**
- 38 **Sprachassistentin** Alexa behält Nutzer im Blick
- 40 **Forschung** KI liest Gedanken, Panoramalinse
- 41 **Sensoren** Roboterhand mit Tastsinn
- 42 **Bit-Rauschen** Probleme mit RTX 3080, IBM A2O
- 43 **Embedded Systems** Intel Atom x6000E
- 44 **Hardware** GeForce RTX 3090, Business-PC
- 45 **Security** Trojaner kostenlos entschlüsseln
- 46 **Netze** AVM kontra Fritzblock, Netzwerktester
- 48 **Server & Storage** NAS-Festplatten, AMD Neoverse
- 49 **Cloud-Gaming-Dienst** Amazon Luna
- 50 **Apple** Unmut wegen App-Store-Provision
- 52 **Linux** Lenovo-PCs mit Ubuntu, Live-Linux Puppy
- 53 **Windows** Sysinternals-Tools für ARM
- 54 **Foto-Software** Photoshop CC, PicApport 9
- 55 **Microsoft 365** Erweiterungen für Teams
- 56 **Web-Tipps** Terror, bropages, TheirTube

## Test & Beratung

- 76 **Mini-PC für Ryzen 4000G** Asrock Deskmini X300
- 78 **Hybrid-Notebook mit Tiger-Lake-CPU**
- 80 **16-Zoll-Notebook** Honor MagicBook Pro
- 82 **Flaches 15,6-Zoll-Notebook** Lenovo Legion Y740Si
- 84 **CPU mit GPU** AMD Ryzen 5 Pro 4650G
- 84 **18-Byte-NAS-Festplatte** Seagate Ironwolf NAS
- 85 **Aktivboxen mit Bluetooth** Klipsch The Fives
- 86 **Spiegellose Systemkamera** Canon EOS R5
- 88 **Samsungs große Stift-Tablets**
- 90 **Bluetooth-Headset** Sony WH-1000MX4
- 91 **Offener Kopfhörer** Sennheiser HD 560S
- 91 **Uhrenmodul für Echo Flex** Third Reality Smart Clock
- 92 **Spielzeugroboter** zum Programmierenlernen
- 93 **Videokonferenzkamera** Logitech MeetUp
- 94 **Linux-Desktop** Gnome 3.38
- 110 **Kompaktkamera gegen Fotohandy**
- 114 **Shopsysteme für Online-Händler**
- 120 **Medientrend Newsletter**
- 166 **Action-Rollenspiel** Marvel's Avengers
- 180 **Bücher** Ende der Zukunft, Programmieren lernen

### 14 Fritzbox absichern



FritzOS 7.20 verbessert die Privatsphäre gleich an drei Stellen: DNS-over-TLS beugt Ausspähungen vor, VoIP-Verschlüsselung gewährleistet vertrauliche Telefonate, WPA3 schottet das WLAN ab. Das alles ist ratzfatz konfiguriert.

## Wissen

- 96 **Netzteilstandard ATX12VO** Umweltfreundlich
- 134 **Zahlen, Daten, Fakten** Telefonie
- 136 **Warn- und Notfall-Apps** Desaster am Warntag
- 138 **Lithium-Gewinnung** in Deutschland
- 142 **E-Government** Software allein reicht nicht
- 146 **Active Directory** Sicherheitsempfehlungen
- 168 **Datenschutz** Schmerzensgeld bei Verstößen

## Praxis

- 106 **PC-Ersatz: Smartphone am Monitor**
- 124 **Kreativ malen mit Krita**
- 128 **Porträts zeichnen** mit Krita
- 152 **Flugsimulator-Controller mit Arduino**
- 156 **Autorisierung** Flexibel mit Open Policy Agent
- 160 **Chemische Formeln** mit LaTeX

## 60 Ihre Daten für immer speichern



Wer seine wertvollen Urlaubserinnerungen, die Fotos der Kinder und wichtige Dokumente aufbewahren möchte, braucht nicht nur die richtigen Medien, sondern auch eine Strategie für die Langzeitarchivierung.

## Immer in ct

- 3 **Standpunkt** Archivierung: Einfach mal machen
- 6 **Leserforum**
- 11 **Schlagseite**
- 58 **Vorsicht, Kunde** Klarmobil jubelt Extras unter
- 170 **Tipps & Tricks**
- 174 **Windows 10 kaufen: Die FAQ**
- 182 **Story** Eine Aufgabe fürs Leben
- 190 **Stellenmarkt**
- 192 **Inserentenverzeichnis**
- 193 **Impressum**
- 194 **Vorschau 23/2020**

## 100 Große Gaming-Displays



HDR-taugliche 4K-Monitore ab 55 Zoll schicken sich an, den Fernseher als großformatiges Spiele-Display abzulösen. Doch auch aktuelle Smart-TVs sind inzwischen spieletauglich. Vier Displays ab 1300 Euro im Test.



ct Hardcore kennzeichnet im Heft besonders anspruchsvolle Artikel.

# Leserforum



Der Standpunkt aus c't 21/2020 zu Linux sprach vielen Lesern aus dem Herzen – der Umstieg auf Linux fällt aber nicht allen leicht.

## Hardware und Linux

Standpunkt: Linux, c't 21/2020, S. 3

Ihr Editorial und die Artikel zu Linux sprechen mir aus dem Herzen. So richtig cool wäre allerdings, wenn andere Redakteure im Haus das auch so sehen würden und bei Vorstellungen neuer Hardware direkt ein paar Worte zur Linux-Unterstützung verlieren würden. Im gleichen Heft ein Mini-PC und zwei Notebooks, aber kein Wort zu Linux. Genau das ist für uns Linux-Willige aber der erste und wichtigste Punkt. Ohne Unterstützung der Hardware macht Linux keinen Spaß.

Daniel Quathamer

## Jungbrunnen Linux

Produktiv unter Linux mit den richtigen Programmen und Anpassungen, c't 21/2020, S. 16

Was ich nach zehn Monaten mit Linux sagen kann: Privat auf meinem Heimrechner nutze ich nur noch Mint. Um Updates muss ich mich nicht mehr kümmern. Systemsicherung macht Timeshift im Hintergrund. Einmal musste ich davon Gebrauch machen, weil mit Version 19 ein Update reinkam und es das Arbeiten fast unmöglich machte, weil der Grafikkartentreiber ein Bug hatte. Der wurde aber sehr schnell gefixt und ich konnte wieder auf Auto-Update stellen.

Freue mich beim Start von Eclipse, das deutlich schneller startet als unter Windows. Auch sonst fühlt sich mein

Rechner an, als wäre er in einen Jungbrunnen gefallen.

Sven Pastorik

## Nicht so einfach

Dreimal Ja: Ja, eine Linux-Installation ist inzwischen einfacher und klarer als eine Windows-Installation. Ja, man kommt mit Linux ganz gut zurecht, wenn man von Windows kommt. Ja, Linux ist eine gute Sache!

Aber: Wenn man kein Techniker, kein Ingenieur ist (ich habe Geschichte studiert), kommt man, komme ich immer wieder an Grenzen. Vor einem Jahr ist es mir dank Ihrer Anleitung tatsächlich gelungen, Linux Mint parallel neben Windows zu installieren - aber drucken konnte ich ums Verrecken nicht.

Ich habe inzwischen auf dem betreffenden Desktop-Rechner (neun Jahre alt) Ubuntu 20.04 installiert und bin mit dem Ergebnis ganz zufrieden, denn Ubuntu hat im Hintergrund auch gleich den Drucker erkannt und eingerichtet. Aber Thunderbird bockte.

Natürlich hat jeder ein anderes Problem, und natürlich sind das keine dringenden Linux-Probleme. Aber bis einem Linux so selbstverständlich wird wie bisher Windows, vergeht viel Zeit – es ist nicht immer so einfach, den richtigen oder einen guten Weg zu finden.

Karl Streiter

## Plank-Dock

Linux-Mint-Desktop anpassen, c't 21/2020, S. 18

Im Artikel stand, dass Plank-Dock keinen grafischen Konfigurationsdialog hat. Der ist zwar schon ein wenig versteckt, aber mit Strg+Rechtsklick geht das sehr wohl, und es gibt da auch Docklets – Clippy und Trash sind sehr nützlich.

Frank B.

## Umweltschäden?

Eingabetastatur auf Papier oder Pappe, c't 21/2020, S. 58

Als Chemiker mit langjähriger Erfahrung in Toxikologie, Pharmakologie und Biochemie hat mich beim Lesen fast der Schlag getroffen. Der Artikel beschreibt ein nettes, vielleicht sehr profitables Produkt für den massenhaften Einsatz. Aber was ist mit den Umweltfolgen der perfluorierten Papier-Billig-Elektronik?

Es gibt bereits heute genug Probleme mit Perfluorooctanoat (wunderbares Imprägnierungsmittel – krebserregend, beständig bis zum Ende des Planeten oder zum Abtauchen auf einer Kontinentscholle in den Erdmantel). Über die üblichen Kartonagerecyclingverfahren würde so ein Label beziehungsweise seine Komponenten unkontrollierbar in der Umwelt verteilt.

Klaus Belsner

## Sinn der Datensammelei

Datenschutz-Negativpreis für Tesla, c't 21/2020, S. 56

Tesla-Autos senden manchmal gigabyteweise Daten nach Hause. Das ruft Datenschützer auf den Plan, denn es sind auch

## Fragen zu Artikeln

✉ Mail-Adresse des Redakteurs am Ende des Artikels

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

# Home-Office? Aber sicher! Desktop-Virtualisierung mit VDI

## Effizientes Arbeiten durch Desktop-Virtualisierung

Mit unseren VDI-Lösungen profitieren Sie mehrfach von der Virtualisierung Ihrer Desktop-Arbeitsplätze und Workstations: Sie sparen mit Thin Clients Hardware- sowie Energiekosten und reduzieren den Verwaltungsaufwand für Ihre IT. Damit schaffen Sie eine hoch performante Infrastruktur für CAD-Anwendungen oder ortsunabhängige Arbeit via Home-Office.



Jetzt informieren:

[thomas-krenn.com/home](http://thomas-krenn.com/home)

+49 (0) 8551.9150-300

**THOMAS  
KRENN®**

Bewegungsdaten und Daten aus den Kameras dieser Autos. Der Artikel erklärte aber nicht, warum Tesla so viele Daten sammelt und hinterließ den Eindruck, das Unternehmen sei einfach nur ein böser Datensammel-Krake.

Tesla benutzt diese Daten, um das Kartenmaterial und den Autopilot weiterzuentwickeln, was für Tesla-Fahrer ein großer Vorteil ist. Durch die ständigen Verbesserungen wird das Auto von Monat zu Monat besser benutzbar und sicherer. Dies ist ein wichtiger Teil des Tesla-Geschäftsmodells und trägt zum erstaunlich hohen Wiederverkaufswert dieser Autos bei. Das Produkt reift beim Kunden.

Hans-Georg Michna 

## Interrupt-Handler

*Lüftersteuerung mit PWM, Poti und WLAN,*  
c't 21/2020, S. 160

In dem Interrupt-Handler auf Seite 161 versteckt sich etwas, das ich gern als looming desaster [drohendes Unheil, Anm. d. Red.] bezeichne. Der Interrupt-Handler – aufgerufen pro Lüfterumdrehung – allokiert Speicher, der dann von `Serial.printf()` verwendet wird, und gibt den Speicher dann wieder frei. Dies kann im schlimmsten Fall dazu führen, dass der Interrupt-Handler den Speicher wieder freigibt, während die Serial-Klasse noch damit beschäftigt ist, Zeichen auszugeben.

Die Implementierung der Serial-Klasse ist in der Regel asynchron, das heißt, es ist bei 1000 Interrupts pro Sekunde und ungefähr 5700 Zeichen pro Sekunde bei 57600 Baud recht wahrscheinlich, dass das `free()` ausgeführt wird, bevor die Ausgabe beendet ist (je nach Lüfterdrehzahl und Baudrate).

Ich empfehle in Interrupt-Handlern Dinge wie `malloc()` oder die Ausgabe von Werten zu vermeiden und stattdessen diese so einfach wie möglich zu gestalten. Im Beispiel würde es genügen, die Lüfterdrehzahl in einer global definierten Variable zu speichern und den Wert ab und zu in `loop()` auszulesen und auszugeben. Das Auslesen muss bei nicht atomar zu speichernden Variablen gesichert werden, damit nicht die `loop()` die Variable halb gelesen hat, und der Interrupt-Handler dies unterbricht und den Wert verändert (Interrupts sperren). Wenn man diese Dinge nicht beachtet, hat man es mit schwer zu findenden Fehlern zu tun, die

## Wir freuen uns über Post

 [redaktion@ct.de](mailto: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>

Software-Updates und praktisch allen Banking-Anwendungen um solche „minderwertigen und leicht zu fälschenden Signaturen“. Alleine an dieser Sichtweise sieht man, wie praxisfern die Fokussierung auf QES ist. Wenn Updates der Werkzeuge für die Prüfung meiner Signaturen schlechter gesichert sind als meine Signaturen, ist das ganze absurd.

Michael Schlenker 

## Ergänzungen & Berichtigungen

### Outbank auf Apple Watch

*Multibanking-Apps mit Licht und Schatten,*  
c't 21/2020, S. 68

Um die Zwei-Faktor-Authentifikation mit Farbcodes beim photoTAN-Verfahren (Deutsche Bank, Comdirect und andere) zu erleichtern, bietet anders als angegeben auch Outbank die Möglichkeit, diese Codes auf einer Apple Watch anzeigen zu lassen.

Alexander Haarer 

gegebenenfalls abhängig von Betriebszuständen erst dann auftreten, wenn man den verursachenden Code als „funktionierte doch stabil seit Monaten“ wahrnimmt.

*Vielen Dank für diesen und weitere Hinweise, die wir von unseren Lesern zu dem Artikel bekommen haben. Wir arbeiten schon am nächsten Projekt, das die Lüftersteuerung nutzt und werden die Verbesserungsvorschläge für eine Version 2 der Firmware berücksichtigen.*

## Digitale Signaturen

*Elektronische Signatur: eine Bestandsaufnahme,*  
c't 21/2020, S. 128

Die Qualifizierte elektronische Signatur (QES) ist zweifelsfrei die rechtlich und technisch sicherste Lösung. Allerdings ist sie wegen der hohen Zugangshürden zugleich auch eine absolute Nischenlösung, was sich auch durch die immer noch umständliche Fernsignatur nur in geringem Ausmaß ändern wird.

Insbesondere folgendes Zitat des Autors ist mir negativ aufgestoßen: „Die Anforderungen an fortgeschrittene elektronische Signaturen sind strenger, aber auch hier sind Fälschungen relativ einfach möglich.“ Sachlich betrachtet handelt es sich also bei der kompletten TLS-Zertifikatsinfrastruktur, allen Code-Signing-Zertifikaten für die Absicherung von Firmware und

### GBit, nicht GByte

*NAS-Festplatte mit 18 TByte und konventioneller Technik,* c't 20/2020, S. 50

Im ursprünglichen Text war von 1146 GByte pro Quadratzoll die Rede. Es sind 1146 GBit.

### Daten in die USA

*FAQ: Das Ende des Privacy Shields,* c't 21/2020, S. 178

Die Aussage im Text: „Nach derzeitigem Stand ist man nicht dafür verantwortlich zu machen, dass ein Dienstleister seinerseits die Daten in die USA transferiert“ stimmt nach aktueller Lage so nicht.

Der Europäische Datenschutzausschuss hat betont, dass die Aufsichtsbehörden von einer Mitverantwortung des Auftraggebers einer Datenverarbeitung ausgehen. In einem Vertrag zur Auftragsverarbeitung müsste demnach angegeben werden, ob ein Datenexport insbesondere in die USA erfolgt, inklusive Nennung der Rechtsgrundlage. Das gilt auch, wenn der Dienstleister die EU-Tochter eines US-Konzerns ist und seine Server in der EU betreibt (wie beim in der FAQ genannten Beispiel Microsoft).

1blu

# Ein starkes Angebot: Homepage XXL



**10 .de-Domains inklusive  
Kostenlose SSL-Zertifikate**

- > SSL-Zertifikate von Let's Encrypt für alle Domains per Mausklick
- > 100 GB Webspace
- > 4 externe Domains
- > 1000 E-Mail-Adressen
- > 100 GB E-Mail-Speicher
- > 100 aktuelle 1-Klick-Applikationen
- > 100 SSD MySQL-5-Datenbanken

**2,29  
€/Monat\***

**Dauerpreis!**

**Nur im Oktober 2020!**  
Nach dem 31.10.2020 keine  
Bestellung mehr möglich.  
!

**1-Klick-Apps inklusive**



Komfortable Online-  
Lernplattform  
Datenaustausch &  
Videokonferenzen



\* Preis/Monat inkl. 16% MwSt. Es fällt keine Einrichtungsgebühr an. Vertragslaufzeit jeweils 6 Monate, jederzeit kündbar mit einem Monat Frist zum Vertragsende.

030 - 20 18 10 00 | nur unter **www.1blu.de/xxl**

# c't Windows –



NEU

## Das Praxishandbuch 2020

### c't WINDOWS Das Praxishandbuch 2020

#### Effizienter nutzen

Neue Funktionen entdecken  
Windows im Homeoffice  
Dateien schneller finden  
Tipps zum Startmenü

#### Schlauer einrichten

Microsoft-Konto vermeiden  
Maßgeschneidert installieren  
Gratis umsteigen auf Windows 10  
So finden Sie die richtige Lizenz

#### Tiefer einsteigen

Windows-Rechte verstehen  
Registry-Änderungen nachvollziehen  
Windows virtualisieren wie die Profis



Auch als  
Heft + PDF  
erhältlich mit  
29 % Rabatt



#### Windows absichern

Trojanersicheres Backup · Privacy-Checkliste  
SSDs, Festplatten und USB-Sticks verschlüsseln  
Passwörter sicher und trotzdem bequem verwahren

#### c't Windows 2020

Das Praxishandbuch 2020 der c't-Experten gibt Ihnen einen perfekten Rundumblick über Ihr Windows-System. Auf über 200 Seiten gibt es Tipps darüber wie Sie eine ganze Reihe kaum bekannter, praktischer Funktionen für sich nutzen können. Aber auch zahlreiche Infos, die im Homeoffice hilfreich sind, oder wie Sie Ihr System besser schützen können und vieles mehr.

[shop.heise.de/ct-windows20](http://shop.heise.de/ct-windows20)

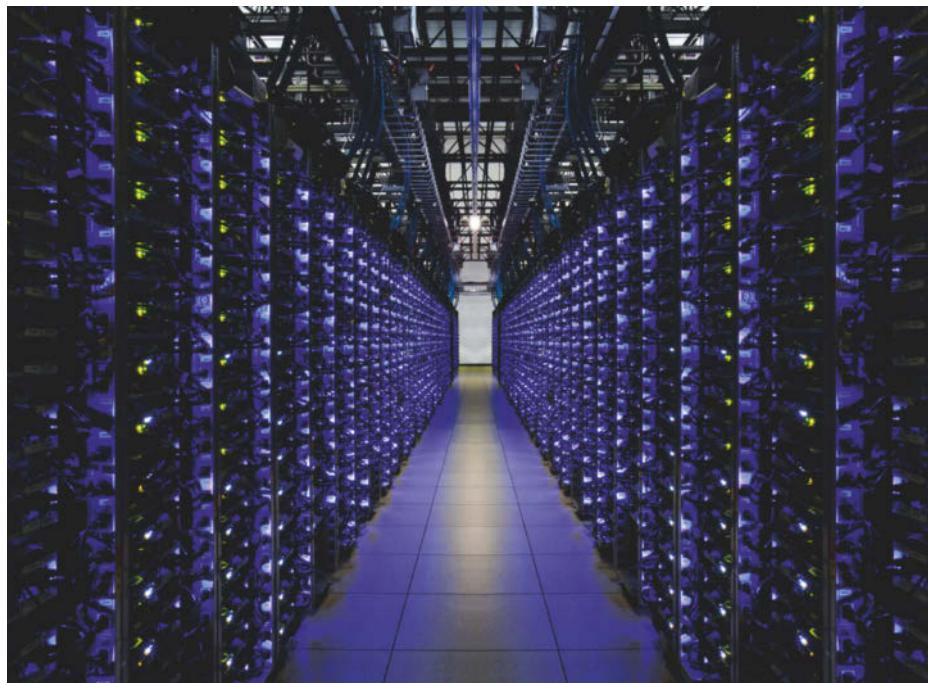
Einzelheft  
für nur

14,90 €





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



können und dadurch Abhängigkeiten vermeiden. Ein maschinenlesbarer Katalog soll die Auswahl geeigneter Dienste vereinfachen. Außerdem legt die Initiative nach eigenem Bekunden besonders viel Wert auf „Datenhoheit“: Anwender sollen entscheiden, wo Daten gespeichert werden und „von wem sowie zu welchem Zweck sie verarbeitet werden dürfen“.

### US-Clouds beliebt trotz Risiken

Mit dem Fokus auf Unabhängigkeit und Datenschutz trifft Gaia-X einen Nerv. Laut Umfragen des IT-Verbands Bitkom stiegen die Bedenken deutscher Unternehmen gegen Clouddienste von 2017 bis 2019 spürbar an. Vor allem die Sorge vor unberechtigtem Zugriff auf Daten treibt die Entscheider demnach um.

Das Ende des Privacy-Shield-Abkommens spielt der Initiative zusätzlich in die Hände. Das im Juli verkündete Urteil des Europäischen Gerichtshofs erhöht die Rechtsunsicherheit bei der Nutzung ausländischer Clouddienste für personenbezogene Daten noch einmal. Selbst wenn Kunden sich für die europäischen Rechenzentren von Google, Amazon oder Microsoft entscheiden, sind sie nach Auffassung der Datenschutzbehörden nicht auf der sicheren Seite. Denn laut amerikanischem Recht dürfen US-Behörden auch dann auf die Daten von EU-Bürgern zugreifen. Hinzu kommt das Horrorszenario eines Handelskrieges, in dem Donald Trump europäischen Konkurrenten einfach den Stecker zieht.

Allerdings muss man auch festhalten: Datenschutzkonforme Clouddienste von europäischen Anbietern gibt es schon lange, auch ohne Gaia-X. Trotzdem haben viele Unternehmen ihre Daten und Anwendungen lieber den amerikanischen „Hyperscalern“ anvertraut.

Die drei führen nicht nur weltweit und in Europa den Cloud-Markt an, sondern auch in Deutschland. Die Telekom liegt laut der Marktforschungsfirma Synergy selbst in ihrem Heimatmarkt nur auf Rang 4.

### Deutsche Bank will zu Google

Prominente Beispiele für Kooperationen mit den Hyperscalern gibt es genug. Im Juli kündigte die Deutsche Bank an, ihre IT-Architektur zusammen mit Google neu auszurichten und künftig auf die „erstklassigen Clouddienstleistungen“ der Kalifornier zu setzen. Auch die damit verbundene Risiken thematisiert die Bank in ihrer

# Wolkenschloss

## Europa-Cloud Gaia-X tritt gegen übermächtige Konkurrenz an

**Die europäische Cloud-Initiative Gaia-X steht in den Startlöchern. Mit dem Fokus auf digitale Souveränität trifft sie den Nerv der Zeit. Trotzdem sehen manche Experten die Marktchancen skeptisch.**

Von Christian Wölbert

ränen digitalen Infrastruktur für Europa“ koordinieren soll.

Gleichzeitig kündigten einige der Partner erste konkrete, Gaia-X-kompatible Produkte an. So wollen zum Beispiel die Telekom und der französische Hoster OVHcloud Anfang 2021 ein „vertrauenswürdiges Public-Cloud-Angebot für alle Branchen schaffen, in denen Datensouveränität und DSGVO-Konformität eine bedeutende Rolle spielen“. Auch Plusserver und weitere Anbieter planen Gaia-X-kompatible Cloud-Dienste.

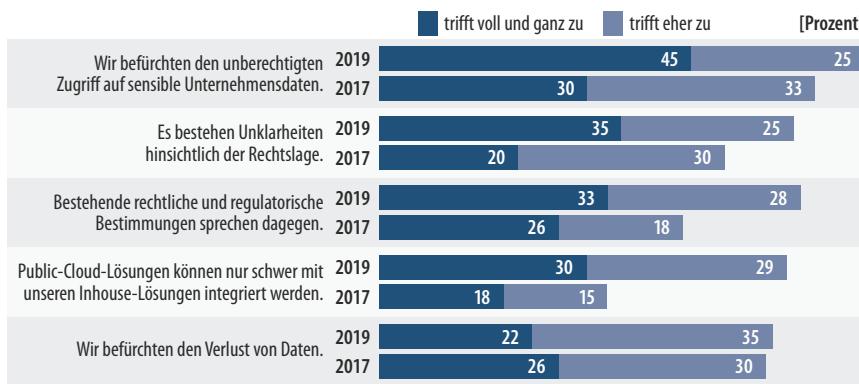
Schon bald wird sich also zeigen, ob es für das von der Politik mit vorangetriebene und mit Steuergeldern geförderte Konzept auch einen Markt gibt.

Offizielles Ziel der Initiative ist ein „Verbundsystem von bestehenden Cloudanbietern“. Kunden sollen dank einheitlicher Open-Source-Schnittstellen schnell und günstig zwischen Cloudanbietern wechseln oder mehrere parallel nutzen

Für die von der deutschen und der französischen Regierung angeschobene Cloud-Initiative Gaia-X wird es bald ernst. Mitte September haben 22 Organisationen und Konzerne aus Deutschland und Frankreich – darunter Atos, BMW, Bosch, SAP und Telekom – in Brüssel eine gemeinnützige Organisation gegründet, die den Aufbau der „vertrauenswürdigen, souve-

## Cloud-Risiken

Die Bedenken deutscher Unternehmen gegen Cloud-Lösungen haben in den vergangenen Jahren zugenommen, wie Umfragen von Bitkom und KPMG zeigen.



spezifisch gestaltet, der Wechsel für Kunden deshalb relativ kompliziert und teuer.

Als aktuelles Beispiel nennt Bienert die vom kalifornischen Unternehmen OpenAI entwickelte Anwendung GPT-3. Diese kann automatisiert Texte erstellen, die von menschengeschriebenen praktisch nicht zu unterscheiden sind. Ende September erwarb Microsoft eine exklusive Lizenz für die Integration der Textmaschine in seine Azure-Cloud – andere Nutzer müssen sich mit eingeschränkten Zugängen zufriedengeben. „GPT-3 könnte bald so uneinholbar sein wie Google“, warnt Bienert. Aus seiner Sicht sollte die EU versuchen, eine Alternative aufzubauen.

Auch der Deutschland-Chef der Unternehmensberatung Accenture, Frank Riemensperger, betont die Bedeutung der Zusatzdienste. Die großen amerikanischen Anbieter investierten massiv in den Ausbau von Big Data und KI, aber auch Quantencomputing aus der Cloud. „Jedes Unternehmen, das diese Milliardeninvestitionen nicht zum eigenen Vorteil hebt, schneidet sich von den rapiden Innovationszyklen der Digitalisierungsindustrie ab“, mahnt er.

Riemensperger vermutet, dass schon in sechs Jahren „nahezu 50 Prozent der deutschen Unternehmens-IT“ in den Clouds der amerikanischen Hyperscaler laufen könnte. Der Spagat zwischen Wettbewerbsfähigkeit und Souveränität dürfte also weitergehen. (cwo@ct.de) ct

Pressemitteilung: Beide Partner würden sicherstellen, „dass die Kundendaten und Informationen der Deutschen Bank vertraulich und integer behandelt werden sowie jederzeit verfügbar sind“.

Was beruhigend klingen soll, kann man auch als Offenbarungseid lesen: Das größte deutsche Geldhaus würde seine Daten künftig nicht mehr allein kontrollieren, sondern darauf angewiesen sein, dass der Partner sich an die Regeln hält. Doch der Wettbewerb lässt den Bankern offensichtlich keine andere Wahl.

Sogar bei der „Industrie 4.0“, der Vernetzung von Fabriken, spielen die US-Anbieter inzwischen vorne mit. Volkswagen setzt seine „Industrial Cloud“ in Amazons Serverfarmen auf. Zunächst sollen die 122 Werke des Konzerns angeschlossen werden, langfristig auch 30.000 Standorte von Zulieferern und Partnern. Parallel baut der Autobauer seine „Automotive Cloud“ für vernetzte Fahrzeuge zusammen mit Microsoft auf. Laut Volkswagen hat Datenschutz bei den Kooperationen „höchste Priorität“. Man entwickelt die Sicherheitssysteme kontinuierlich weiter und lasse sie extern zertifizieren.

Die Beispiele zeigen: Die Wirtschaft tickt beim Thema digitale Souveränität anders als der Staat. Sie muss sich Unabhängigkeit auch leisten können. Zwar betont das Bundeswirtschaftsministerium mittlerweile, dass Gaia-X keinen europäischen Hyperscaler bauen soll, der Microsoft, Amazon und Google weltweit die Stirn biete, was angesichts des Vorsprungs der Amerikaner ohnehin utopisch wäre. Wettbewerbsfähig müssen die Gaia-Dienste aber trotzdem sein.

Lehrreich ist die Geschichte der „Microsoft Cloud Deutschland“: Von 2016 an beherbergte die Telekom als „Datentreuhänder“ einen Ableger der Microsoft-Cloud in eigenen Rechenzentren. Doch das Angebot war teurer und bot weniger Funktionen als das Original. Zu wenige Kunden waren bereit, diese Kröten zu schlucken, das Angebot floppte.

Manche Experten äußern sich deshalb skeptisch über die Marktchancen der Gaia-X-Dienste. Die Initiative gehe zwar in die richtige Richtung, meint Jörg Bienert, Vorsitzender des KI-Bundesverbands und Partner bei der IT-Beratungsfirma Alexander Thamm. Es müssten dabei aber auch Angebote von großen Playern zu attraktiven Preisen entstehen. „Wir brauchen ein Leuchtturm-Rechenzentrum“ betonte er im Gespräch mit c't. „Mit PowerPoint-Folien und Open-Source-Repositories allein gewinnt man nichts.“

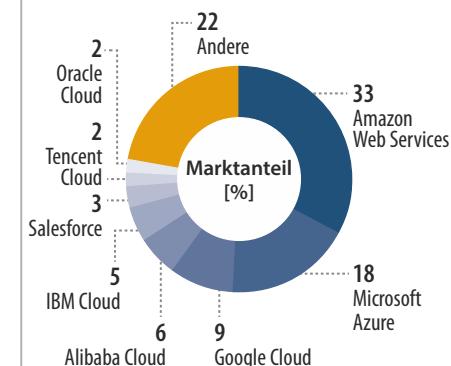
### KI aus der Cloud

Außerdem dürfe Gaia-X sich nicht allein auf Infrastruktur konzentrieren, fordert Bienert. Höherwertige Dienste wie KI-Anwendungen seien „mindestens genauso wichtig“. Aus seiner Sicht sind die US-Player auch deshalb so dominant, weil sie Gesamtpakete anbieten. Kunden können nicht nur Speicherplatz und Rechenleistung mieten (Infrastructure as a Service), sondern auch Entwicklungs-umgebungen und Anwendungen, etwa für Datenanalysen oder Sprach- und Bilderkennung (Platform und Software as a Service). Bei solchen Tools sei die Gefahr eines „Lock-ins“ viel höher als bei reiner Infrastruktur. Sie seien häufig plattform-

## Cloud-Markt weltweit

Chinesische und US-amerikanische Anbieter dominieren den Cloud-Markt\*.

\* Platform as a Service und Infrastructure as a Service



# Mehr Privatsphäre mit Fritzboxen

FritzOS 7.20 schützt VoIP-Telefonie, WLAN und Surf-Daten



<b>Mehr Privatsphäre mit Fritzboxen</b> .....	<b>Seite 14</b>
<b>Telefonate verschlüsseln</b> .....	<b>Seite 18</b>
<b>Beim Surfen die Privatsphäre schützen</b> .....	<b>Seite 22</b>
<b>WLAN mit WPA3 absichern</b> .....	<b>Seite 26</b>

# Lange Zeit war lediglich bekannt, wie vielfältig die Privatsphäre von Nutzern ausgespäht werden kann. Nun mehren sich aber die Gegenmittel. In aktuellen Fritzboxen lassen sich drei wichtige besonders einfach aktivieren.

Von Dušan Živadinović

**S**eine Privatsphäre muss man selbst verteidigen, Konzerne und der Staat haben daran naturgemäß kein Interesse. Das ist soweit nichts Neues. Wie Sie Ihre PCs, Smartphones und andere Geräte ohne viel Aufwand konfigurieren, damit sie einen minimalen Fußabdruck im Internet hinterlassen, haben wir beispielsweise in c't 13/2020 zusammengefasst.

Doch für manche Lücken materialisieren sich die Gegenmittel nur verzögert. Beispielsweise ist die Telefonie per Voice over IP seit jeher ungeschützt. Obwohl erste Verschlüsselungen schon Anfang der 2000er-Jahre spezifiziert worden sind, ließen Provider, Telefon-, Tk-Anlagen- und Routerhersteller sie fast zwei Jahrzehnte lang links liegen. Derweil haben Messenger mit VoIP-Funktion davon profitiert. Signal, Wire, WhatsApp, iMessage und andere verschlüsseln Ende-zu-Ende und der Nutzer muss nicht einen Finger dafür rühren.

## VoIP-Telefonie schützen

Höchste Zeit also, dass mit der Telekom ein großer Player im Markt wenigstens eine der vielen Methoden aufgreift und Routerhersteller wie AVM, Lancom oder Bintec-elmeg mitzieht. Denn Messenger sind nicht interoperabel und heute noch weniger verbreitet als Festnetztelefone.

Doch übliche VoIP-Gespräche, die auch grenzüberschreitend laufen können, lassen sich leicht massenhaft abhören, auch von fremden Nachrichtendiensten. Nicht zu vergessen die blank in den Hausverteilern zusammenlaufenden Telefonkabel: An Hausverteilern, die oft unbeachtet in Kellern stehen oder gar außen an Gebäuden, können Angreifer mit Notebook und DSL-Analysator oft unbehelligt alles mit-schneiden, was über die DSL-Leitungen ins

Internet geht. Und es soll ja Firmen geben, in denen man sich Passwörter oder auch Kreditkartendaten telefonisch durchgibt.

Die Geräteentwickler haben es allerdings nicht immer leicht, die Spezifikationen zur VoIP-Verschlüsselung umzusetzen. An manchen Stellen sind die Schriften zu knapp oder sie überlassen die genaue Implementierung dem Gespür der Programmierer. Das geht nicht immer gut und so haben wir auch für die Fritzbox Verbesserungsvorschläge. Unterm Strich muss man aber sagen: Der Einstieg in die VoIP-Verschlüsselung ist gelungen, auch wenn der hiesige Branchenprimus AVM zu wünschen übrig gelassen hat. Einzelheiten dazu finden Sie im Beitrag ab Seite 18.

## WLAN absichern

Manche Sicherheitstechnik bekommt im Laufe der Zeit Risse. Bei der WLAN-Verschlüsselung kennt man das schon zur Genüge: Mit WEP und WPA sind schon zwei Methoden gekommen und (hoffentlich rückstandslos) gegangen. Nun sollte man für die dritte Methode, das aktuelle WPA2, den Abschied einläuten.

Zwar ist WPA2 nicht so grundlegend lächerlich wie die WLAN-Steinzeittechnik WEP: WPA2-geschützte Funknetze lassen sich bisher nur über hartnäckiges Ausprobieren knacken (Brute Force). Aber Hochrechnungen, laut denen ein erwürfeltes 16-stelliges Passwort dem stumpfen Ausprobieren rund 19 Billionen Jahre lang standhalten soll, sind nun mal Hochrechnungen. Zudem gehen sie von aktuellen Methoden und aktueller Hardware aus. Doch WPA2 fehlt der Vertraulichkeitschutz Perfect Forward Secrecy (PFS). Deshalb muss eine Attacke nicht zur Laufzeit des angegriffenen WLANs abgeschlossen sein, sondern kann auch aufgezeichnete Daten aufdecken. Falls man in einigen Jahren Quanten-Computer darauf ansetzen kann, sind Angreifer vermutlich weit schneller am Ziel als heute prognostiziert.

Je eher Sie auf das bereits verfügbare WPA3 umsteigen desto besser. Die neue WLAN-Verschlüsselung ist zwar beileibe nicht perfekt. Aber zum Beispiel ist anders als bei WPA2 für jede Passworteingabe ein neuer Verbindungsversuch erforderlich, sodass sich automatisierte Brute-Force-Angriffe auf eine WLAN-Basis derart in die Länge ziehen, dass sie aussichtslos sind. Zudem werten die Basisstationen zu viele misslungene Einbuchungsversuche als Angriffe und zögern ihre Antworten dann hinaus. Was WPA3 im Detail bringt, wie Sie es in Fritzboxen aktivieren und wie aktuelle Geräte im Test abschneiden, lesen Sie ab Seite 26.

## DNS-Leckage stopfen

Für manche Privatsphären-Lecks müssen Gegenmittel komplett neu entwickelt und implementiert werden. Dazu zählt die

Bekannte WLAN-Geräte					
Signal	Name	Band	Datenrate (Mbit/s)	Eigenschaften	
Heimnetz ctest-reshw-vdsl					
WiFi	dz	5 GHz	1300 +1300	ac/Wi-Fi 5, 80 MHz, WPA3, ...	 
WiFi	resdz-v13	5 GHz	1866 +780	ac/Wi-Fi 5, 80 MHz, WPA2, ...	 
WiFi	vivo-ea	5 GHz	1866 +1866	ac/Wi-Fi 5, 80 MHz, WPA3, ...	 
Gastzugang					
WiFi	vivo-amo	5 GHz	1866 +780	ac/Wi-Fi 5, 80 MHz, OWE, ...	 
Nicht verbundene Geräte					
WiFi	AppleWatch5	10	10	nicht verbunden	  

Stellt man aktuelle Fritzboxen auf das moderne WPA3 um, erhöht das die Sicherheit erheblich. WLAN-Clients, die sich nicht aufrüsten lassen, können weiterhin WPA2 verwenden.

Verschlüsselung der Kommunikation mit DNS-Resolvern, den „Telefonbüchern des Internet“. Denn alle Geräte sprechen Server im Internet anhand ihrer IP-Adresse an, die sie von Resolvern hauptsächlich im Klartext abfragen. Als die Technik Mitte der 1980er-Jahre entstand, hatte kein Entwickler auf dem Zettel, dass man anhand von DNS-Anfragen Nutzerprofile erstellen könnte. Auch kam später manche DNS-Erweiterung hinzu, die anderen Zwecken dienen sollte, aber nebenbei User-Tracking ermöglicht.

Dazu zählt insbesondere die Methode, mit der Provider die Betreiber von Content Delivery Networks (CDNs) informieren, wo auf der Welt sich der anfragende Client befindet (Geolocation). Damit können sie den Client zum nächstgelegenen Rechenzentrum leiten, was die Paketlaufzeit verkürzt (EDNS0-Option: edns-client-subnet, ECS). Große Content-Anbieter wie Apple, Microsoft oder Netflix nutzen CDNs, um Weitverkehrsstrecken zu entlasten. Daher ist ECS grundsätzlich von Vorteil.

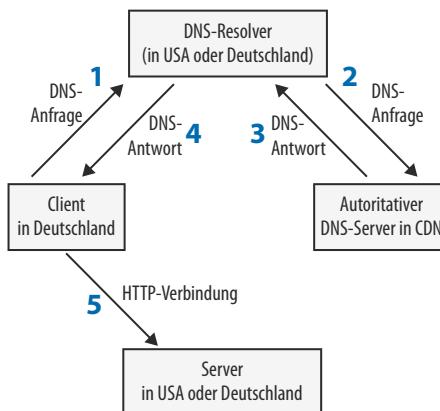
Aber um Kinderschutzfilter zu implementieren, markieren Provider DNS-Anfragen vor der Weiterleitung – und auf den Strecken zu den Root-Server und zum autoritativen Server können die Anfragen Dritte lesen (zum Beispiel am weltgrößten Internet-Drehkreuz DE-CIX in Frankfurt). Auch dagegen ist erst mal nichts einzubinden. Man kann zum Markieren Hashtags nutzen oder andere Merkmale, die keinem User direkt zugeordnet werden können.

## User-Tracking geschenkt

Doch manche Provider nutzen die MAC-Adresse, den Usernamen oder andere Daten, die eine Identifizierung (Fingerprinting) hinter einem Router leicht machen. Wenn Lauscher diese Daten mit dem HTTP(S)-Verkehr korrelieren, sehen sie, welche Seiten Sie sich in der Freizeit ansehen und welche, wenn Sie beruflich aktiv sind.

Anhand solcher tageszeit- und wochentagabhängigen Profile lässt sich ein User sowohl auf Desktop- als auch auf Mobilgeräten identifizieren. So lässt sich grob ableiten, wo sich ein User gerade befindet (zu Hause oder unterwegs). Einzelheiten dazu finden Sie über ct.de/yxkt im RFC 7626 sowie in einem Vortrag der Sicherheitsspezialistin Sara Dickinson.

Die Internet Engineering Task Force kommentiert die Situation so: Die weitaus meisten Webseiten sind zwar öffentlich (anonyme Alkoholiker, BitTorrent-Tracker,



**Vom konfigurierten DNS-Resolver hängt wesentlich ab, welches Rechenzentrum etwa einen angefragten Netflix-Stream liefert und damit auch die Länge der Übertragungsstrecke. Leider plappern manche Resolver private Daten aus.**

Suchmaschinen, Beratungsseiten etc.), aber die Daten darüber, wer welche Webseiten besucht, sollten weder öffentlich sein noch gesammelt werden können. Daher entwickelte die Organisation Verschlüsselungsmethoden für DNS-Abfragen: DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT). Beide schützen die Privatsphäre nur bis zum Resolver und verhindern den Datenabfluss über die ECS-Technik nicht. Aber wer einen nicht-protokollierenden Resolver nutzt, kann einer Resolver-Petze entgehen. AVM baut in seine Fritzboxen DoT ein. Wie man die Technik aktiviert und wie gut sie im Test funktionierte, lesen Sie ab Seite 22.

Jedoch ist AVM nicht der erste Hersteller, der DoT in Routern integriert. Beispielsweise bringt das Router-Betriebssystem pfSense DoT seit 2018 mit. Auch die Turris-Router der tschechischen Registry CZ.NIC, das freie Routerbetriebssystem OpenWrt und die Firewall-Distribution IP-Fire können DNS-Anfragen verschlüsseln.

## Was DoT nicht macht

DoT ist ein wichtiger Baustein beim Schutz der Privatsphäre, aber nur einer von vielen. Die Technik verschlüsselt nur die Strecke vom Client zum Resolver. Der Resolver löst den Namen der angefragten Domain weiterhin im Klartext auf (er kommuniziert unverschlüsselt mit DNS-Root-Servern und autoritativen Servern).

Wer also den Verkehr eines Resolvers langfristig erfasst, kann im Datenstrom der vielen Nutzer, die diesen Resolver verwenden, vermutlich unterschiedliche

Profile erkennen. Fachleute meinen, es sei nicht Privacy-relevant, ob zum Beispiel irgendein Telekom-Kunde die Webseite der Deutschen Aids-Hilfe besuchen wollte. Trotzdem gibt es Pläne, die restliche DNS-Kommunikation abzusichern.

## DNS-Ratschläge

Über die DNS-Verschlüsselung hinaus hilft eine Handvoll einfacher Faustregeln, die Privatsphäre zu verbessern.

Meiden Sie kommerzielle VPN-Dienste. VPN-Anbieter betreiben eigene DNS-Server, um Kunden den Zugang zu Diensten zu ermöglichen, die ihnen das Geo-Blocking normalerweise vorenthält. Jedoch verrät man dabei seine Internet-Ziele dem VPN-Betreiber. Prinzipiell kann er diese Kenntnisse zu Geld machen, etwa durch Verkauf von Profilen an Werbetreibende.

Welchen DNS-Server Ihr aktuelles Gerät gerade benutzt (Smartphone, PC, Tablet, Smart-TV), verrät beispielsweise die Testseite Browserleaks (siehe ct.de/yxkt). Dort stehen im Bereich „DNS Leak Test“ die IP-Adressen der genutzten DNS-Resolver. Vor allem VPN-Anbieter unterhalten Webdienste zur DNS-Analyse, darunter „DNS leak test“ oder „Perfect Privacy“. Damit lässt sich prüfen, welche DNS-Informationen Streaming-Anbietern wie Netflix vorliegen, um etwa länderspezifische Zugänge zu ihren Videoangeboten durchzusetzen.

Prüfen Sie ab und zu, welchen Resolver Ihre Geräte befragen, denn es gab schon etliche Attacken auf Router, um darin den DNS-Server umzubiegen. Angreifer können so mitlesen, wer was tut oder DNS-Anfragen auf Werbeseiten umlenken, die für sie lukrativ sind – oder gleich Malware wie Erpressungstrojaner in den Browser schleusen.

Um Attacken auf Router möglichst kleine Angriffsflächen zu bieten, halten Sie deren Firmware aktuell. Sichern Sie das Webinterface mit einem individuellen, möglichst langen Passwort aus Groß-, Kleinbuchstaben und Sonderzeichen, schalten Sie Zugriffe aus dem Internet auf das Webinterface ab, nutzen Sie für die Fernwartung ein VPN. Verwenden Sie für das WLAN ein anderes, ebenfalls langes Passwort. Verweisen Sie Geräte von Besuchern ins Gastnetz. Bleibt uns noch eins für Ihre Internet-Surf-Unternehmungen zu wünschen: Mast- und Schotbruch!

(dz@ct.de)

Weitere Infos: [ct.de/yxkt](http://ct.de/yxkt)

DAS GLAUBT UNS  
KEINER. AUSSER  
UNSERE KUNDEN.  
99% ZUFRIEDENHEIT  
IM SCHADENFALL.

Umfrage zur Zufriedenheit der Schadenbearbeitung unter allen Hiscox Kunden in Deutschland, die in 2019 einen Schaden gemeldet haben.

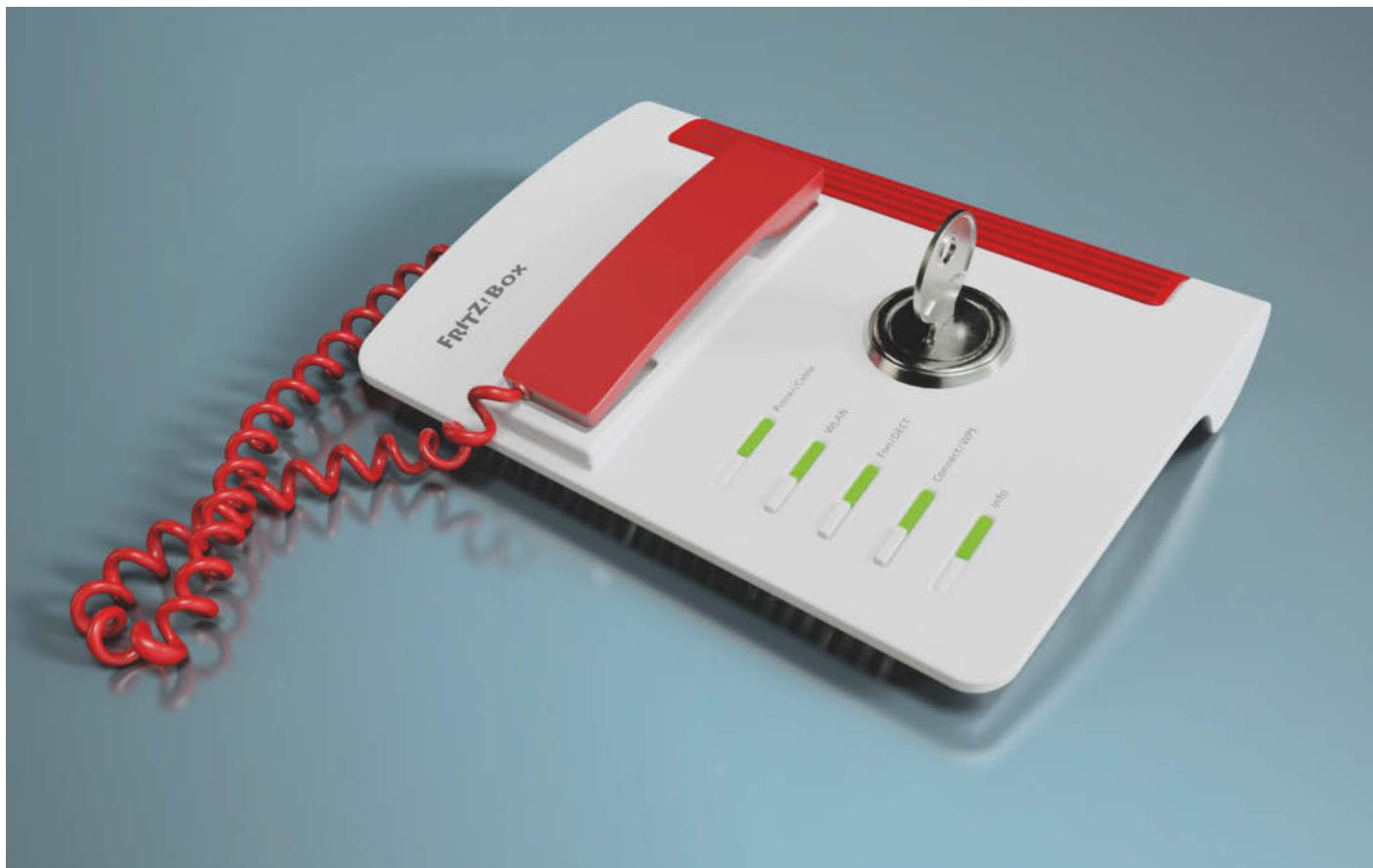
DIE BUSINESS-  
VERSICHERUNG  
VON HISCOX.

Versicherung neu gedacht. Seit 1901.

Mehr erfahren: [hiscox.de/business](http://hiscox.de/business)



**HISCOX**  
WISSEN VERSICHERT.



# Chiffriert fernsprechen

## FritzOS 7.20: Verschlüsselt telefonieren, Grenzen der Methode kennen

**Zum Schutz der Privatsphäre schaltet man in Fritzboxen die Telefonieverschlüsselung mit nur fünf Mausklicks ein – das klingt komfortabel und tatsächlich schnitt die Box in unseren Praxistests ordentlich ab. Eingehende Laboranalysen deckten aber auch unerwartete Schwächen auf.**

Von Alexander Traud

**M**it der im Juli erschienenen FritzOS-Version 7.20 brachte AVM die Verschlüsselung für die VoIP-Telefonie auf aktuelle Fritzboxen. Ursprünglich für die Deutsche Telekom und ihren Dienst „DeutschlandLAN SIP-Trunk“ ausgelegt, funktioniert die Methode auch mit VoIP-Konten anderer Anbieter, etwa dus.net und easybell.

Das ist ein wichtiger Schritt, denn Voice-over-IP-Telefonate laufen größtenteils unverschlüsselt ab. Selbst Hacker-Praktikanten kennen Tricks, solche Datenströme unerkannt aufzuzeichnen und dann etwa im Protokollanalysator Wireshark abzuhören. Erste Gegenmaßnahmen in Form von Verschlüsselungen gibt

es seit fast 20 Jahren. Dazu gehört die Methode SDES-sRTP (siehe Glossar), die Anfang der 2000er-Jahre in erste Geräte implementiert wurde. Auf Tischtelefone, Soft-Clients, Clouds und Router und so auch auf Fritzboxen zog sie erst in jüngster Zeit ein.

Oft verhindert fehlende Benutzerfreundlichkeit die Nutzung von Verschlüsselungstechniken. Nicht so bei SDES-sRTP: Es bringt gute Voraussetzungen für stillschweigende, also nutzerfreundliche Verschlüsselung mit, weil es alle Parameter automatisch aushandeln kann. Schon 2006 führte Nokia vor, wie das geht: Nokia-Handys forderten Aufmerksamkeit vom Nutzer, nur wenn die Verschlüsselung

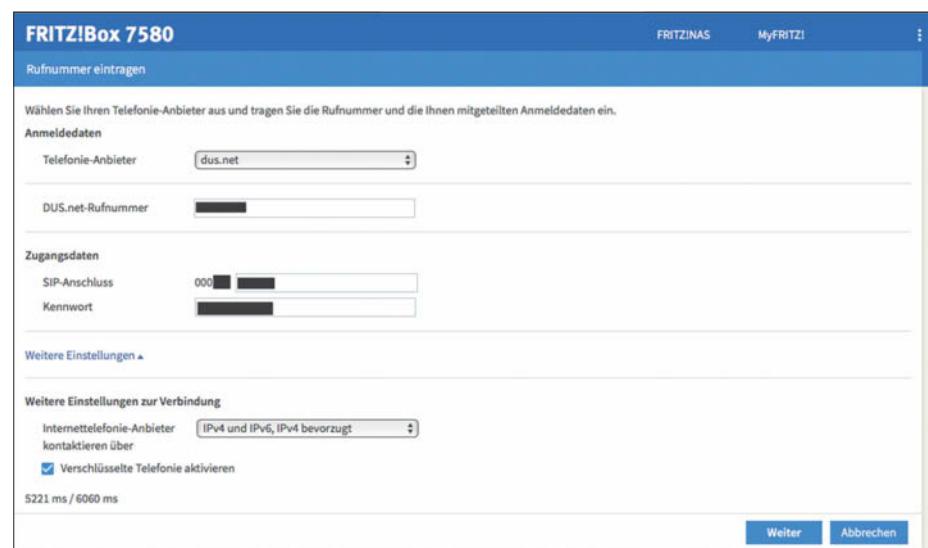
scheiterte und zeigten dann zur Warnung ein offenes Vorhängeschloss.

SDES-sRTP ist eine Transportverschlüsselung für die Strecke vom Teilnehmer bis zum Server des Providers. Das klingt nach weniger, als es ist: Denn Kunden desselben Providers sind damit ebenso abgesichert wie Außendienstler bei hausinternen Telefonaten oder entfernte Niederlassungen von Firmen – zumal „hausinterne“ Gespräche auch Landesgrenzen überspannen können. Nützlich ist die Technik auch, weil in Mehrparteienhäusern die Telefonleitungen blank am gemeinsamem Hausverteiler zusammenlaufen, wo der Verkehr aufgezeichnet werden kann. Und gelegentlich versorgt ein einziger Hausverteiler sogar die Telefonanschlüsse mehrerer Reihenhäuser. Aktiviert man SDES-sRTP, kann also niemand mehr mithören, bloß weil er Know-how und Zugang zum Hausverteiler hat. Schließlich kann man damit seinen SIP-Account prinzipiell auch nomadisch in ungesicherten WLAN-Hotspots nutzen, ohne ein VPN aufzusetzen.

In Fritzboxen muss man die Funktion eigens aktivieren. Dafür ist ein VoIP-Konto bei der Telekom, bei dus.net oder easybell erforderlich: Wenn Sie eines eingerichtet haben, öffnen Sie im Menü „Telefonie/Eigene Rufnummern“ eine geeignete Rufnummernkonfiguration und darin den Bereich „Weitere Einstellungen“. Setzen Sie bei der Option „verschlüsselte Telefonie“ das Häkchen – fertig. Jedes Telefon, das zur betreffenden Rufnummer konfiguriert ist, kann nun verschlüsselte Verbindungen nutzen. So haben wir problemlos diverse Telefonate mit unterschiedlichen Geräten netzintern und auch überkreuz zwischen allen drei Anbietern geführt. So weit, so schön.

Doch SDES-sRTP ist komplex und die Hersteller implementieren die Technik unterschiedlich. Daher können Verbindungen scheitern oder unverschlüsselt laufen und deshalb möchte man für jeden Anruf wissen, ob er verschlüsselt ist. Doch die Fritzbox zeigt das nicht direkt, auch nicht das hauseigene FritzFon C5 (Firmware 4.57). Ein bisschen verrät die Fritzbox im Menü „Telefonie/Eigene Rufnummern/Sprachübertragung“. Dort blendet sie „verschlüsselt“ ein, wenn sie eine SDES-sRTP-Übertragung ausgehandelt hat.

Jedoch verbirgt sie einen Teil der Optionen. Diese zu verstehen ist nicht weiter schwer, aber die Zusammenhänge sind



Mit nur fünf Klicks aktiviert man in Fritzboxen mit aktuellem FritzOS 7.20 die Telefonieverschlüsselung.

teils vertrackt, sodass wir einige Grundlagen voranstellen.

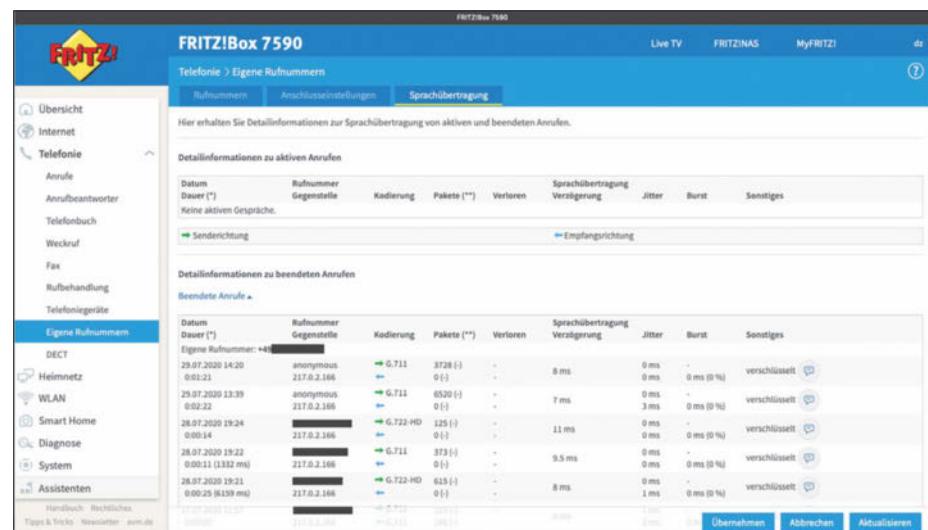
### Ohne TLS am Start

Wer im Internet surft oder Mails abruft, nutzt dabei häufig die Verschlüsselung TLS (siehe Glossar). Dabei tauschen der lokale Client und die Gegenstelle Schlüssel aus, bevor Nutzdaten fließen. Die Gegenstelle weist sich mittels eines Zertifikats gegenüber dem Client aus. Diese Merkmale sind auch für die VoIP-Verschlüsselung nützlich. Dennoch wurde VoIP zunächst ohne TLS spezifiziert.

Das liegt daran, dass TLS auf dem Transmission Control Protocol (TCP) aufsetzt und bei TCP der Empfänger eingehen-

de TCP-Pakete quittiert, damit der Sender Übertragungsfehler erkennt und per Sendewiederholung ausbügelt. Für VoIP sind Wiederholungen aber nutzlos, denn sie kämen beim Empfänger erst an, wenn ihr Wiedergabezeitpunkt schon verstrichen ist.

So setzt VoIP auf das schlanke User Datagram Protocol auf (UDP), das ohne Wiederholung arbeitet. Da die Sprachpakete nur 20 Millisekunden kurz sind, nimmt der Gesprächspartner einzelne Paketverluste nicht wahr. Unterm Strich blieb: ohne TCP keine TLS-Verschlüsselung. Zu Beginn der VoIP-Ära konnte man nur auf VPN-Vernetzung zurückgreifen, um so zumindest zwischen Niederlassungen geschützt zu telefonieren.



Ab FritzOS 7.20 erfassen Fritzboxen im Journal, ob sie mit Gegenstellen die Verschlüsselung ausgehandelt haben – auch für laufende Gespräche.

Web	E-mail	VoIP: Signalisierung	Medien
HTTP	IMAP	SIP	RTP
TLS	TLS	TLS	sRTP
TCP	TCP	TCP	UDP
IP	IP	IP	IP

**Anders als etwa beim Surfen sind bei der VoIP-Telefonie pro Sitzung zwei Verbindungen aufgebaut: eine für die Signalisierung und eine für die Nutzdatenübertragung.**

Die übliche, also unverschlüsselte VoIP-Telefonie verzahnt drei Protokolle miteinander: Die Gegenstellen melden sich über das Session Initiation Protocol (SIP) beim Anbieter an, bauen Verbindungen auf und ab et cetera. Über das Session Description Protocol (SDP) handeln sie die genutzten Medien aus (Audio, Video, Text). Und sie einigen sich auf eine UDP-Verbindung für das Real-Time Transport Protocol (RTP) zur Sprachübertragung. Daher existieren während eines Telefonats mindestens zwei Verbindungen: eine für die Signalisierung, eine für Sprachpakete.

## Verschlüsselung als Nachschlag

Per SDP lassen sich auch verschlüsselte Übertragungen aushandeln. Damit tauschen die Geräte symmetrische Schlüssel untereinander aus. So wird RTP zum „secure RTP“ (sRTP). Damit die Schlüssel vertraulich bleiben, kommuniziert SDP selbst verschlüsselt. Zumindest dafür und für SIP konnten die Protokolldesigner auf TLS zurückgreifen: Somit war SIP-over-TLS mit SDES-sRTP geboren.

In diesem Zusammenhang ist mit „Gegenstelle“ nicht nur das Telefon des Gesprächspartners gemeint, es kann auch der Server eines Anbieters wie der Telekom sein. So sind netzübergreifende Gespräche möglich, auch ins analoge Festnetz. Damit der Anbieter den Datenstrom zur angerufenen Seite weiterleiten kann, entschlüsselt er ihn. Auch das belegt: SDES-sRTP ist keine Ende-zu-Ende-Verschlüsselung, sondern eine Transportverschlüsselung.

Nun zurück zu FritzOS 7.20 und dem zweiten Konfigurationsweg für die Verschlüsselung: Öffnen Sie das Webinterface, klicken Sie auf „Telefonie/Eigene Rufnummern“ und dann auf einen der Einträge – dabei muss es sich um Telekom-, dus.net oder easybell-Nummern

handeln. Stellen Sie das Menü „Telefonie-Anbieter“ auf „Anderer Anbieter“ um.

Jetzt erscheinen die Einstellungen im Detail und sind änderbar – sichern Sie zuvor die aktuelle Konfiguration, damit Sie sie im Fehlerfall wieder einspielen können. Änderungen bieten sich zum Beispiel an, wenn Sie dus.net etwa an einem Kabelanschluss mit DS-Lite-Konfiguration nicht über IPv4, sondern IPv6 erreichen möchten. Dazu tragen Sie im Feld Registrar securev6.dus.net ein.

## Menü zum Ansehen

Die verschlüsselte Telefonie wird mittels drei Optionen eingeschaltet. Im Menü Transportprotokoll muss TLS aktiviert sein und die Option „Anbieter unterstützt verschlüsselte Telefonie“ muss angehakt sein. Die dritte Option folgt im Menü „Media Protocol“.

Hier sind drei Einträge zu finden: RTP/AVP, „RTP/SAVP und RTP/AVP“ sowie RTP/SAVP (siehe RFC 8643). Was genau gewählt ist, hängt vom Anbieter ab und sollte nur nach Absprache mit ihm geändert werden. Wir beschreiben dieses Menü dennoch, weil manches Fritzbox-Verhalten besser verständlich wird.

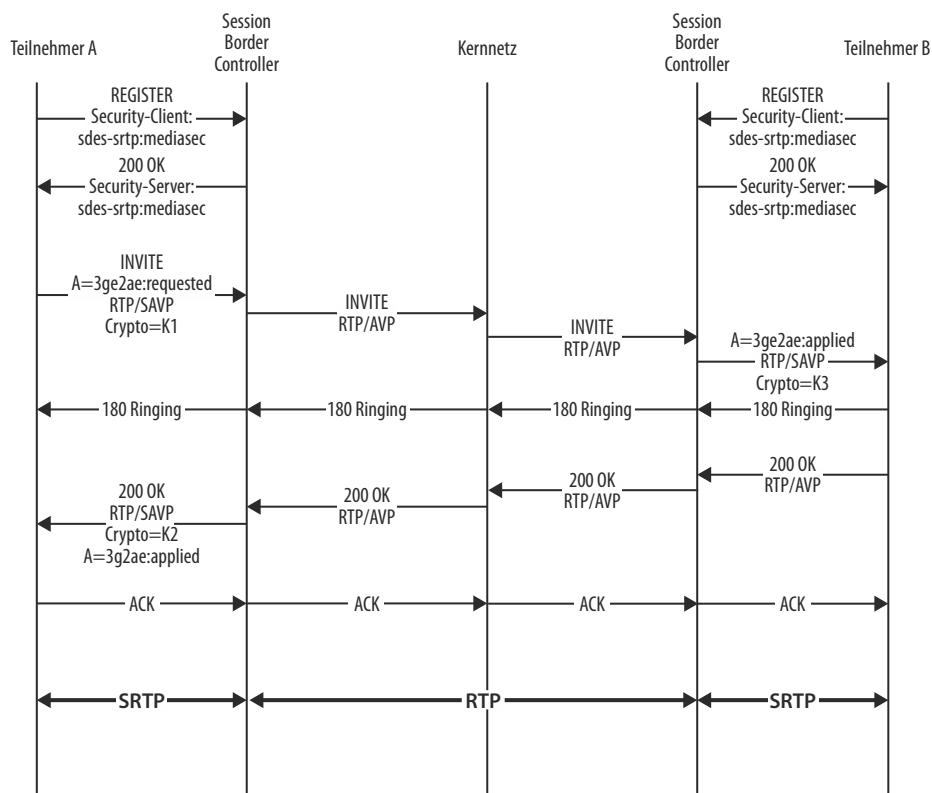
Mit der Einstellung RTP/AVP wird ein Gespräch wie üblich aufgebaut, nur wird

via SDP zusätzlich ein Schlüssel übertragen. Wenn die Gegenstelle SDES-sRTP beherrscht, greift sie sich diesen, sendet ihren eigenen zurück und fortan wird chiffriert telefoniert. Wenn sie sich nicht für SDES-sRTP eignet, soll sie den Schlüssel ignorieren. So wird SDES-sRTP also optional verwendet.

Aber dabei lauern Stolperfallen: Nimmt die Gegenstelle den Schlüssel an, kann sie statt mit RTP/AVP alternativ mit RTP/sAVP antworten. Die Spezifikation toleriert diesen Fall stillschweigend. Der Entwickler muss also selbst darauf kommen, diesen Ablauf korrekt zu behandeln. Fritzboxen tun das nicht, sondern legen einfach auf. Das passiert reproduzierbar mit Gegenstellen wie Digium Asterisk und Sangoma FreePBX mit dem Channel-Driver chan\_sip.

Die Einstellung „RTP/SAVP und RTP/AVP“ soll dieses Problem lösen. Dabei wird ein Gespräch mit einem verschlüsselten und einem unverschlüsselten Medienstrom angeboten, damit die Gegenstelle den bevorzugten selbst wählt. Auch damit wird SDES-sRTP also nur optional ausgehandelt. Diese Variante setzt AVM beim dus.net-Profil ein.

Erst mit der Einstellung RTP/sAVP erzwingt man SDES-sRTP. Das nutzt die



**Mit der Methode SDES-sRTP lässt sich die Transportschicht vom Teilnehmergerät zum Server des VoIP-Anbieters verschlüsseln.**

Fritzbox für easybell- und Telekom-Profile. Wenn die Gegenstelle die Option ablehnt und den SIP-Fehler 488 sendet, scheitert der Verbindungsauftakt. Ein FritzFon meldet dann „Ziel nicht kompatibel“ und die Fritzbox notiert im Journal „Internettelefonie war nicht erfolgreich. Ursache: 488“.

Zwischenfazit: Positiv fällt auf, dass FritzOS 7.20 drei Optionen offeriert. Die Digitalisierungsboxen von Bintec-elmeg (Standard, Smart, Premium) sowie Zyxel (Basic) bieten nur RTP/sAVP.

Der RFC 8643 führt als Gedankenspiel noch eine weitere Option auf, verwirft sie aber, weil diese Variante zur Folge haben kann, dass der Status 488 nicht bei der anrufenden Seite ankommt (Option „RTP/sAVP, SIP-Status 488, RTP/AVP“). Bei Fritzboxen und anderen Routern ist sie konsequenterweise nicht eingebaut, nur Lancom hat sie dennoch implementiert.

Die Telekom fordert für chiffrierte Telefonie zusätzlich das Erfüllen der MediaSec-Spezifikation. Die Telekom weiß so, dass das Endgerät mit Verschlüsselung umgehen kann, auch bei ankommenden Telefonaten. AVM hat das eingebaut, ebenso die Routerhersteller Bintec-Elmeg, Lancom und Zyxel sowie die Tischtelefon-Hersteller Cisco Sipura (ab Multiplatform-Firmware 11.3) und Snom (ab Firmware 10.1).

Weitere Stolpersteine lauern bei der Aushandlung der Chiffre, denn AES-128 ist verpflichtend und AES-256 optional. Doch an der korrekten Behandlung nicht berücksichtiger Chiffren hapert es bei manchen Gegenstellen. Falls eine Gegenstelle damit nicht klarkommt, ist es also wünschenswert, AES-256 abschalten zu können. Bei Cisco Sipura ist diese Chiffre standardmäßig ausgeschaltet, bei Lancom abschaltbar, bei AVM jedoch nicht.

## Was Fritz schon kann

Für die obigen Ergebnisse haben wir die Fritzbox in einem Testaufbau genauer unter die Lupe genommen: Um die Signialisierung mitlesen zu können, haben wir als VoIP-Server Asterisk 13 LTS mit dem Channel-Driver chan\_sip aufgesetzt und diesen in der Fritzbox über das Menü „Anderer Anbieter“ konfiguriert. Asterisk war dabei auf TLS 1.2 mit der Chiffre AES-GCM fixiert und der Verschlüsselungsschutz Perfect Forward Secrecy deaktiviert. So lassen sich sowohl an der Fritzbox als auch am Asterisk-Server

Daten mitschneiden und in Wireshark analysieren.

Dabei kam unter anderem heraus: AVM nutzt intern die Bibliothek OpenSSL 1.1.1 und damit auch das moderne TLS 1.3. Auch NIST-freie Kryptografie mittels Curve25519 und sogar Curve448 sind eingebaut. Das ist vorbildlich. Zwar nutzt Lancom ebenfalls OpenSSL 1.1.1. Aber das aktuelle LCOS 10.42.116 bietet weder TLS 1.3 noch Curve448.

Zusätzlich haben wir die Fritzbox mit VoIP-Clients wie Linphone getestet. Damit kann man Peer-to-Peer-Telefonate mit Internet-Gegenstellen führen (z. B. von Linphone zu iptel.org). Verbindungen zu traditionellen Telefonnetzen bekommt man allenfalls mit kostenpflichtigen Tarifen. Mit FritzOS 7.20 klappte im Test die unverschlüsselte Kommunikation mit linphone.org/freesip, iptel.org, voip.opensips.org und sip2sip.info reibungslos. Gespräche mit SIP-over-TLS kamen nur mit antisip.com/service zustande.

## Was Fritz noch lernen sollte

Telefonie-Router bieten nicht nur Adapter für analoge und ISDN-basierte Telefone. An manchen lassen sich auch SIP-Telefone anmelden. AVM bietet seinen Registrar nur über UDP und TCP an, bisher aber nicht über TLS (Bintec-Elmeg und Lancom tun das). Wer sich aus der Ferne mit einem SIP-Soft-Client in seine Fritzbox einbucht, braucht also weiterhin VPN als Transportmedium, um unerwünschte Mithörer fernzuhalten.

Noch aus den VoIP-Anfangszeiten bringt eine Fritzbox die Funktion zum direkten Anruf einer SIP-Gegenstelle mit, also am üblichen Anbieter vorbei. Für diese „Anwahl von Internettelnummern“ (SIP-URI-Dialing) legt man im Fritz-Telefonbuch Einträge im E-Mail-Adressformat an (z. B. 500@hd-telefonie.avm.de). Doch weil die automatische Transporterkennung für TLS fehlt (DNS-NAPTR), kann die Fritzbox beim SIP-URI-Dialing nicht verschlüsseln.

## Glossar

AVP: Audio Video Profile

RTP: Real-time Transport Protocol

sRTP: Secure RTP

sAVP: Secure Audio Video Profile

SDP: Session Description Protocol

SDES: Session Description Protocol

Security Descriptions

SIP: Session Initiation Protocol

TCP: Transmission Control Protocol

TLS: Transport Layer Security

Ab OpenSSL 1.1 könnten User je nach Sicherheitseigenschaften ihres Geräts prinzipiell eine durchgehende Mindestverschlüsselung in Stufen von 1 bis 5 festlegen. Bisher hat das noch kein Hersteller implementiert, auch AVM nicht. Dabei eignet sich FritzOS 7.20 sogar für die Stufe 4. Stattdessen schließt AVM lediglich TLS 1.0 aus und fordert mindestens TLS 1.1. Für die Authentifizierung setzt TLS Zertifikate voraus. Aber in FritzOS 7.20 fehlt eine Zertifikatsverwaltung, um kompromittierte Zertifikate stillzulegen oder eigene Zertifikate hinzuzufügen. AVM erwägt, den einen oder anderen Verbesserungsvorschlag in FritzOS aufzunehmen.

## Fazit

AVM macht es den Nutzern leicht, die Verschlüsselung zu verwenden. An den Komfort führender Implementierungen kommen Fritzboxen aber noch nicht heran, schon weil die Verschlüsselung aktiv eingeschaltet werden muss. Und den Status kann man nur umständlich überwachen. Aber ein Anfang ist gemacht – besser eine Verschlüsselung, die etwas Mitarbeit erfordert als gar keine. Und nicht zuletzt ist die Verschlüsselung in Fritzboxen in manchen Punkten umfangreicher als bei anderen Routern. (dz@ct.de) ct

**Infos zu SDES-sRTP: [ct.de/yntg](http://ct.de/yntg)**



Fritzboxen können zur Aushandlung der Verschlüsselung eines von drei Verfahren verwenden. Manche andere Router nutzen nur eines.



Bild: Andreas Martini

# Vertrauliche Auskunft

## Mit Fritzboxen beim Surfen die Privatsphäre schützen

An jedem Internetanschluss, egal ob privat, geschäftlich, WLAN-Hotspot oder Hotel können identifizierende Metadaten von Nutzern unerkannt abfließen. Dagegen hilft eine moderne DNS-Verschlüsselung, die sich für viele Betriebssysteme nachrüsten lässt. Mit einer aktuellen Fritzbox erspart man sich den Aufwand und schützt mit einem Schlag das komplette Netz.

Von Dušan Živadinović

**M**it FritzOS 7.20 hat auf aktuellen Fritzboxen eine wenig beachtete Funktion Einzug gehalten: die verschlüsselte Abfrage von Domainnamen, DNS-over-TLS (kurz DoT). Das klingt nach einer der vielen Spezialfunktionen für Netzwerk-Freaks, doch DoT ist für jeden Nutzer von Belang: Richtig angewendet, schützt sie vor einer Methode der Massenüberwachung, die zum Beispiel Geheimdienste und manche Provider einsetzen. Die Grundlage bilden Metadaten, die bei jedem Internetzugriff nebenbei anfallen; wer diese in die Hände bekommt, kann das Surf-Verhalten der Nutzer wie offene Tagebücher lesen. Manche Provider verkaufen das als Surf-Profile an Werbetreibende.

Der Zusammenhang in aller Kürze: Fast alle Internetprogramme, zum Beispiel Webbrowser, Mail-Clients, Spiele

oder Messenger, sprechen ihre Server anhand von maschinenlesbaren IP-Adressen an. Menschen ziehen aber leichter zu merkende Domainnamen wie ct.de vor. Die Wandlung vom Namen zu IP-Adressen erledigen DNS-Server (Resolver). Die Kommunikation mit den Resolvern läuft weitgehend im Klartext ab und lässt sich daher leicht protokollieren. Ein Man-in-the-Middle kann die DNS-Antworten der Resolver sogar manipulieren und sein Opfer über gefälschte DNS-Einträge auf mit Malware präparierte Server locken.

### Internet-Tagebuch verschlüsseln

Abhilfe schaffen neue Protokolle, die die Kommunikation mit den Resolvern verschlüsseln. Die wichtigsten sind DNS-over-TLS (DoT) und DNS-over-HTTPS

(DoH), die beide die Internet Engineering Task Force spezifiziert hat. Daneben hat auch das proprietäre DNSCrypt eine gewisse Verbreitung erreicht. Alle drei haben wir in diversen Beiträgen beschrieben, siehe [ct.de/ymb4](http://ct.de/ymb4). DoT soll drei Probleme lösen: die Privatsphäre der Anwender gegen Lauscher schützen, das Einschleusen manipulierter DNS-Informationen verhindern und den Attacken, die gezielt die Resolver mancher Firmen überlasten sollen, ein Ende setzen (Distributed Denial of Service, DDoS).

DoT und DoH sind noch junge Spezifikationen, verbreiten sich aber schneller als beispielsweise IPv6. In Smartphones ab Android 9 kann man DoT im Bereich „Private DNS Mode“ einschalten. Der DNS-Resolver in Linux-Systemd (Systemd-Resolved) eignet sich ebenfalls für DoT. Microsoft arbeitet daran, DoH in Windows zu implementieren und Apple hat für macOS 11 und iOS 14 sowohl DoT als auch DoH angekündigt (siehe [ct.de/ymb4](http://ct.de/ymb4)). Apple hat auch APIs eingebaut, über die beliebige Apps die verschlüsselte DNS-Kommunikation nutzen können und ermuntert Entwickler, die Funktionen zu nutzen. Diverse ältere Betriebssysteme kann man mit DoT-Clients nachrüsten.

Weil es unpraktisch ist, mehrere Computer und Smartphones einzeln aufzurüsten und aktuell zu halten, richtet man verschlüsselnde DNS-Clients zum Beispiel auf dem DNS-Filter Pi-hole für sein komplettes Netz ein (siehe [ct.de/ymb4](http://ct.de/ymb4)); dann sind auch IoT-Geräte, Medienreceiver, Webcams und sonstige Netzwerkgeräte geschützt, die sich nicht aufrüsten lassen. Einen Pi-hole zu betreiben erfordert allerdings etwas Know-how und Pflegeaufwand. Beides hat AVM in Fritzboxen mit FritzOS 7.20 auf ein Minimum reduziert. Jedoch fehlt der Fritzbox ein Werbeblocker vom Schlag eines Pi-hole.

Auf Fritzboxen lässt sich DoT mit nur wenig Know-how einrichten. Grundsätzlich kann man die Technik mit einem von zwei Profilen betreiben. Im „Strict Privacy Profile“ kommuniziert ein DoT-Client nur mit Resolvern, die sich mit gültigem TLS-Zertifikat authentifizieren und verschlüsselt kommunizieren. Wenn die Authentifizierung oder die Verschlüsselung scheitert, gibt der Client auf und kann keine DNS-Anfragen auflösen – aus Sicht des Nutzers ist dann „das Internet kaputt“ und er muss einen anderen Resolver einstellen, bei dem beides klappt.

## Zwei DoT-Profile

Das zweite Profil „Opportunistic Privacy Profile“ ist weniger streng: Es gewichtet funktionierende DNS-Auflösung höher als den Privatsphärenschutz. Falls eine authentifizierte und verschlüsselte Verbindung scheitert, nimmt der Client auch mit einem Resolver vorlieb, den er nicht kennt oder der nicht verschlüsselt. Das zweite Profil bietet also begrenzten Schutz vor Spähern und manipulierten DNS-Informationen. AVM hat in FritzOS 7.20 beide DoT-Profile eingebaut.

Vor der Aktivierung der Funktion benötigen Sie mindestens einen, besser mehrere Domainnamen von DoT-Resolvern (zum Beispiel [dns.quad9.net](http://dns.quad9.net)). Eine Handvoll großer Resolver-Betreiber, darunter Cloudflare und Quad9 bieten öffentliche Namensauflösung via DoT an und validieren die DNS-Informationen auch. Validieren bedeutet: per DNSSEC sicherstellen, dass der Inhalt von DNS-Antworten nicht manipuliert ist und dass die Information ein vertrauenswürdiger Server gesendet hat. Ob Ihr aktueller Resolver DNS-Daten validiert, können Sie etwa mit dem „Connection Test“ auf [internet.nl](http://internet.nl) prüfen. Kandidatenlisten für DoT-Resolver finden Sie über [ct.de/ymb4](http://ct.de/ymb4).

Die bei seinen Resolvern eingehenden DNS-Anfragen von Nutzern verwendet Cloudflare, um sein Content Distribution Network zu optimieren und Inhalte seiner Großkunden möglichst dort zu platzieren, wo sie oft nachgefragt werden. Wer sein Surf-Protokoll einem amerikanischen Konzern lieber nicht schenken möchte, findet über den Link am Ende des Artikels Listen kleinerer, offener DoT-Server mit „no logging“-Policy, darunter den

Bielefelder Anbieter Digitalcourage ([dns.digitalcourage.de](http://dns.digitalcourage.de)).

## Mal eben einschalten

Wenn Sie Ihre Resolver ausgewählt haben, öffnen Sie im Webinterface der Fritzbox das Menü Internet/Zugangsdaten/DNS-Server. Die Standardeinträge für unverschlüsselte DNS-Anfragen lassen Sie unverändert, damit Sie bei etwaigen DoT-Problemen Ihre ursprüngliche DNS-Konfiguration schnell reaktivieren können.

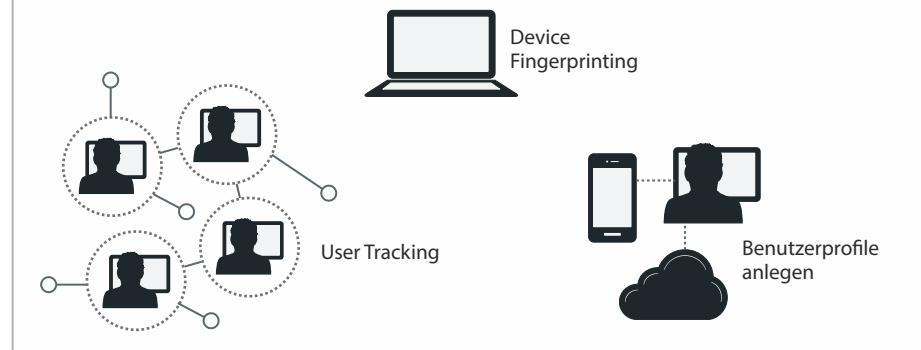
Setzen Sie im Abschnitt „DNS over TLS“ mindestens die ersten beiden Häckchen („Verschlüsselte Namensauflösung im Internet“ und „Zertifikatsprüfung für verschlüsselte Namensauflösung im Internet erzwingen“). Mit dem ersten aktivieren Sie DoT und mit dem zweiten stellen Sie sicher, dass der weiter unten eingetragene DoT-Resolver anhand seines TLS-Zertifikats authentifiziert wird. Dann können Sie sicher sein, dass tatsächlich der Resolver befragt wird, den Sie eingetragen haben (Strict Privacy Profile).

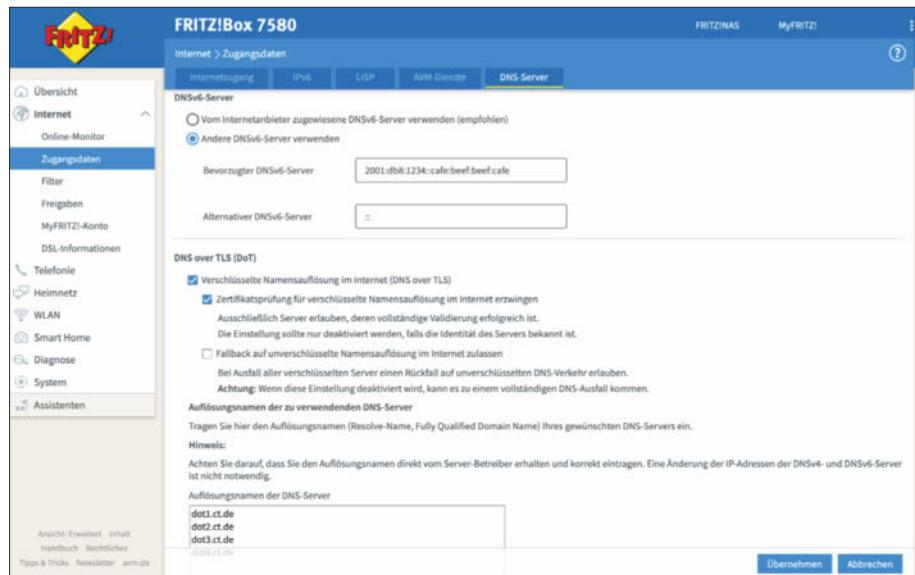
AVM merkt unter den zweiten Punkt an: „Die Einstellung sollte nur deaktiviert werden, falls die Identität des Servers bekannt ist.“ Das ist ein wenig zu knapp beschrieben. Gemeint ist wohl: Wenn Sie einen DoT-Resolver nutzen, der nur ein selbstsigniertes Zertifikat liefert, dann lässt er sich nicht authentifizieren. Damit die Fritzbox diesen Resolver akzeptiert, muss der Haken weg.

Es ist empfehlenswert, mehrere Resolvern zu verwenden, falls mal einer ausfällt. Auf Anfrage erklärte AVM, dass die Fritzbox die Wahl des „besten“ Servers anhand des Validierungsstatus und der

## Wie die DNS-Namensauflösung missbraucht werden kann

In unverschlüsselten DNS-Anfragen stecken vertrauliche Informationen, die sich vielfältig nutzen lassen, um Nutzerverhalten auszuleuchten.





Einige Mausklicks genügen, um in Fritzboxen verschlüsselte DNS-Anfragen einzuschalten. Längst gibt es nicht nur experimentelle DoT-Resolver wie im obigen Screenshot abgebildet, sondern auch öffentlich zugängliche.

Latenz trifft. Bei der Validierung prüft die Box die Zertifikatskette und die im Serverzertifikat eingetragenen Werte wie die IP-Adresse oder den DNS-Namen (Subject-Alternative-Name). Anschließend sortiert sie die Resolver nach absteigendem Validierungsstatus. Haben zwei oder mehr denselben Status, zieht die Box den Resolver mit der kürzesten Latenz vor.

Eigentlich möchte man Anfragen an mehrere Resolver streuen, um die Profilerstellung zu erschweren. Das sei aktuell aber nicht geplant, antwortete AVM auf Anfrage.

Nachteilig ist, dass die Box in der Resolverliste ausschließlich Domainnamen akzeptiert. So ist schon für die Verbindungsaufnahme eine erfolgreiche herkömmliche DNS-Auflösung nötig. Besser wäre eine Tabelle mit IP-Adressen und Domainnamen.

Mit der Option „Fallback auf unverschlüsselte Namensauflösung im Internet zulassen“ hat AVM das zweite DoT-Profil implementiert, das Opportunistic Privacy Profile. Schaltet man es ein, sendet die Box Klartext-DNS-Anfragen an einen der weiter oben eingetragenen Resolver, falls die Kommunikation mit dem DoT-Resolver scheitert. In sicherheitskritischen Bereichen sollte man diese Option nicht nutzen.

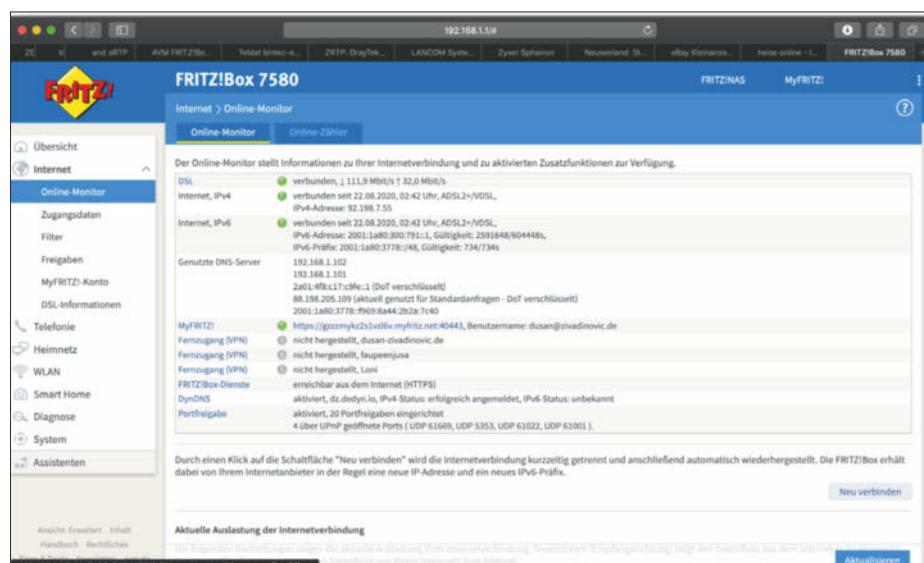
Wenn Sie Ihre Auswahl getroffen haben, speichern Sie die Änderungen mit „Übernehmen“ und legen Sie anschließend ein Backup der Fritzbox-Konfiguration

auf Ihrem PC an (System/Sicherung/Sichern).

## Dinge bedenken

Im Menü Internet/Online-Monitor sollten alle konfigurierten Resolver zu sehen sein (Genutzte DNS-Server). Zum neu eingerichteten DoT-Resolver sollte dort stehen: „aktuell genutzt für Standardanfragen - DoT verschlüsselt“.

Nun können Sie wie üblich surfen. Die netzinterne DNS-Auflösung, etwa für Ihre Drucker oder Dateiserver, funktioniert



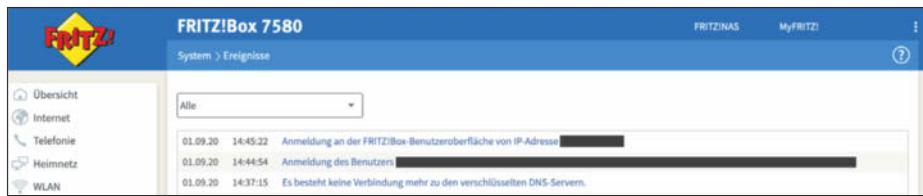
In Fritzboxen lassen sich mehrere DNS-Resolver (DNS-Server) konfigurieren. Im Monitorbereich kann man nachschlagen, welche gerade in Verwendung sind.

wie zuvor. Es gibt jedoch einige Dinge zu bedenken: Der DoT-Client kommuniziert standardmäßig über den TCP-Port 853. Somit können etwa Provider den DoT-Verkehr leicht per Firewall-Regel unterbinden. Aktuell kennen wir für Deutschland zwar keinen solchen Fall, aber manche Staaten sperren Internetzugriffe anhand von DNS-Verkehrsanalysen, sodass sie DoT blockieren, um Klartext-DNS zu erzwingen. Russland plant ein Gesetz, das unter anderem DoT und TLS 1.3 verbietet.

Prinzipiell kann man DoT-Clients und -Resolver auch auf anderen Ports betreiben, beispielsweise auf Port 443, der normalerweise HTTPS-Verkehr vorbehalten ist. DoT und HTTPS lassen sich nur mit erheblichem Aufwand und damit teuer unterscheiden (Deep Packet Inspection), sodass DoT auf Port 443 nicht blockiert wird.

Leider kann man in der Fritzbox den Zielport nicht einstellen und es gibt kaum DoT-Resolver, die über Port 443 ansprechbar sind. Ein Beispiel ist dns.cmrg.net, den Daniel Kahn Gillmor betreibt, der Entwickler des zugehörigen Multiplexers hddmux für HTTPS und DoT. Unterm Strich bedeutet das: Sollte der DoT-Verkehr einer Fritzbox providerseitig gesperrt sein, muss man sie auf Klartext-DNS zurückstellen. Wer weiterhin eine DNS-Verschlüsselung benötigt, kann ersatzweise einen eigenen DoH-Server auf einer Linux-Maschine einrichten.

Auch DoT-Server können ausfallen. Es gibt aber Webseiten, die darüber informieren, ob einer der dort erfassten Server



Wenn „das Internet kaputt“ ist, schaut man im Log der Fritzbox nach (System/Ereignisse). In seltenen Fällen kann das Symptom nämlich auch ein ausgefallener DNS-Server (Resolver) bewirken.

läuft oder nicht (siehe [ct.de/ymb4](http://ct.de/ymb4)). Ist dort ein Eintrag grün markiert und er für Sie dennoch nicht erreichbar, blockiert vermutlich eine Firewall die Kommunikation – wenn Sie dieses Verhalten auch mit anderen Servern beobachten, ist das ein Beleg für einen DoT-Filter.

## Geheimnisse und Schwächen

DoT-Clients verschlüsseln den Verkehr per TLS und müssen dafür das Transmission Control Protocol nutzen (TCP). Beide zusammen, TCP und TLS, erfordern etwas mehr Zeit für den Verbindungsaufbau als unverschlüsselter DNS-Verkehr, der über das schlanke User Datagram Protocol abläuft (UDP). Als Faustregel gilt aber: Je schneller die DNS-Auflösung, desto schneller der Aufbau von komplexen Webseiten, weil dafür besonders viele DNS-Anfragen erforderlich sind.

Deshalb versuchen DoT-Clients über eine einmal geöffnete TLS-Verbindung mehrere DNS-Abfragen abzuwickeln. Mit TLS-Version 1.2 verbleiben dennoch messbare Einbußen. Erst TLS 1.3 bringt Optimierungen mit, die DoT nahe an die Geschwindigkeit des klassischen DNS heranbringen (0-RTT, asynchrone Kanäle, TCP Fast Open, TCP Connection Re-Use, Pipelining).

Ob auch die Fritzbox davon Gebrauch macht, lässt sich noch nicht sagen. Zwar zeigen unsere Protokollanalysen, dass sie schon TLS 1.3 und den Verschlüsselungsschutz Perfect Forward Secrecy (PFS) nutzt; beides ist vorbildlich. Doch wenn PFS aktiviert ist, kann man den TLS-Verkehr selbst dann nicht entschlüsseln, wenn man den Server-Key besitzt; man braucht zusätzlich die Session-Keys des Clients. Diese lässt sich die Fritzbox bisher nicht entlocken.

## Kurzer Servertest

Die Fritzbox notiert im Menü unter System/Ereignisse, falls es bei der DoT-Kommunikation mal knirscht. In unserem zweimonatigen Testzeitraum mit eigenem

DoT-Server ist das nur zwei Mal vorgekommen. Aus dem Eintrag im Fritzbox-Journal geht aber nicht hervor, was genau der Fehler ist (Client-Fehler, Port-Blockade oder Server-Fehler). Um Licht ins Dunkel zu bringen, kann man die konfigurierten DoT-Server auf einem PC mit dem Tool `kdig` befragen. Auf gängigen Linux-Distributionen gehört `kdig` zu den Paketen „Knot-Resolver“ und „Knot-Server“; beide gibt es auch für Macs. Den Knot-Resolver kann man über den macOS-Paketmanager Homebrew beziehen und den Knot-Server über den Paket-Manager MacPorts. Ein Beispielbefehl sieht so aus:

```
kdig @dns.digitalcourage.de ct.de +tls
```

Damit befragt `kdig` den Resolver von Digitalcourage nach der IP-Adresse der Domain ct.de. Mit der Option `+tls` lässt man sich Einzelheiten über die Verschlüsselung anzeigen. In der Ausgabe steht dann beispielsweise „TLS 1.3“, wenn `kdig` eine solche Verbindung aufgebaut hat. Darunter folgt die IP-Adresse der angefragten Domain (193.99.144.80).

## Verkehrsanalyse

Um zu prüfen, ob die Fritzbox DNS-Anfragen tatsächlich verschlüsselt, ist mehr Aufwand erforderlich. Trennen Sie zunächst alle Geräte bis auf einen PC von der Fritzbox, damit Sie nur den DNS-Verkehr der Fritzbox aufzeichnen. Andernfalls können zum Beispiel Smart-TVs oder IoT-Geräte Verwirrung stiften, wenn sie direkt mit Resolvern kommunizieren.

Schalten Sie die Verkehrsaufzeichnung in der Fritzbox ein (über `fritz.box/support.lua` im Abschnitt „Paketmitschmitte“), surfen Sie mit dem PC einige Webseiten an und stoppen Sie die Aufzeichnung. Nun können Sie die übrigen Netzwerkgeräte wieder anschließen. Öffnen Sie das von der Fritzbox an den PC geschickte PCAP-File im Protokollanalysator Wireshark und dort im Menü „Statistics“ die

Option „DNS“. Dann öffnet Wireshark ein Fenster mit diversen Einzelheiten. In der ersten Spalte sind Rubriken wie „Total packets“, „Service Stats“ und „Query Stats“ aufgeführt. In der Spalte „Count“ steht die Anzahl der Pakete zur jeweiligen Rubrik. Wenn in der gesamten Count-Spalte nur Nullen stehen, hat die Fritzbox keine Klartext-DNS-Anfragen verschickt – also ausschließlich DoT genutzt.

Um zu prüfen, wie die Fritzbox auf Resolver-Ausfälle reagiert, haben wir das mit einem eigenen DoT-Resolver simuliert. Clients, die auf die DNS-Auflösung der Fritzbox angewiesen waren, konnten dann keine Webseiten öffnen. Leider lieferte die Box in dieser Testreihe auch nach zehn Minuten keine DoT-Fehlermeldung (FritzOS 7.20 auf Fritzbox 7590 und FritzOS 07.19-80420 BETA auf Fritzbox 6890 LTE). Im realen Einsatz würde das die Fehlersuche erschweren. Nach Reaktivieren des DoT-Resolvers klappte die Auflösung über die Fritzbox nicht umgehend wieder; im Ereignisprotokoll tauchten keinerlei Versuche oder Fehlermeldungen auf. Erst nachdem wir DoT kurz aus- und wieder einschalteten, funktionierte die sichere Namensauflösung.

Einige Tage nach den induzierten Serverfehlern klappte die Auflösung ohne ersichtlichen Grund nicht mehr. Im Log notierte die Box: „Es besteht keine Verbindung mehr zu den verschlüsselten DNS-Servern.“ Aber mit `kdig` ließ sich der betreffende Server durchaus ansprechen und er lieferte auch korrekte Antworten auf DNS-Anfragen. Nach Aus- und Einschalten der DoT-Funktion klappte auch die Auflösung mit der Fritzbox wieder. AVM antwortete auf Nachfrage: „Mit dem nächsten Release werden wir die Robustheit der DNS-over-TLS-Kommunikation insbesondere bei bestimmten Anbietern verbessern.“

## Fazit

An Kleinigkeiten feilt AVM noch, doch unterm Strich konnte die DoT-Implementierung der Berliner im Dauertest weitgehend überzeugen, zumal nach dem sehr einfachen Einschalten das gesamte (W) LAN mit einem Schlag von den verschlüsselten DNS-Anfragen profitiert. Diese Technik in Fritzboxen zu haben, ist ein Gewinn. Weitere kommerzielle Routerhersteller sollten das als Ansporn nehmen und nachziehen.

(dz@ct.de) ct

Weitere Infos: [ct.de/ymb4](http://ct.de/ymb4)



Bild: Andreas Martini

# Extrasicher funkeln

## WPA3 schützt das WLAN, nicht nur an Fritzboxen

**Einer der großen Fortschritte in FritzOS 7.20 ist die verbesserte WLAN-Verschlüsselung WPA3. Sie stopft nicht nur die in WPA2 in den letzten Jahren entdeckten Lücken, sondern bringt auch nützliche neue Funktionen mit. WPA3 klappt auch schon mit vielen Geräten.**

Von Dr. Alfred Arnold und Ernst Ahlers

**M**it WPA3 in FritzOS 7.20 liefert AVM eine Runderneuerung der WLAN-Verschlüsselung: Für den Anwender sieht alles mehr oder weniger wie gewohnt aus, aber er wird besser gegen Angriffe und Ausspähen geschützt.

Im Folgenden schildern wir, wie WPA3 das schafft. Beim Verständnis hilft ein kurzer Rückblick, der nicht nur Fritzbox-Besitzern nutzt, sondern auch denen anderer Router und WLAN-Basen (Access-Points). Er schildert die WPA2-Ausgangslage und gibt Einrichtungstipps, unter anderem zu sicheren Passwortlängen und Optionen, mit denen man Geräte bequem koppeln kann. Wer das schon im Hinterkopf hat, kann zum Abschnitt „WPA3 endlich da“ vorspringen.

Bereits 2004 erschien das heute übliche WPA2. Es verwendet den immer noch als sicher geltenden AES-Algorithmus (Advanced Encryption Standard) für das Chiffrieren der Daten. Sein Schutz hielt fast fünfzehn Jahre, eine in IT-Maßstäben sehr lange Zeit, in der sich die WLAN-Datenrate von 54 auf 1733 MBit/s brutto mehr als verdreifacht. Aber auch die besten Schlosser rosten.

Vor einigen Jahren stellte sich heraus, dass WPA2-Personal anfällig gegen Offline-Dictionary-Attacken ist: Ein Angreifer kann die notwendigerweise noch unverschlüsselte Anmeldung eines Clients, den sogenannten Key Handshake, mitschneiden und mithilfe eines Wörterbuches durchprobieren, welches Passwort zu den dabei ausgetauschten kryptografischen Prüfsummen passt.

Die Hardware für solche Brute-Force-Angriffe wurde wie die fürs WLAN über die Jahre immer billiger und leistungsfähiger. 2016 stellte ein Forscherteam der Uni Wien auf einer internationalen Konferenz eine auf die Aufgabe spezialisierte Hardware vor: Die knapp 100.000 US-Dollar teure FPGA-Implementierung kann über 10 Millionen Passwörter pro Sekunde testen (siehe Link unter [ct.de/yt8p](http://ct.de/yt8p)) – so was gönnen sich Dienste mit dreibuchstabigen Ab-

kürzungen für staatlich gedeckte Spionage.

### Bitte würfeln!

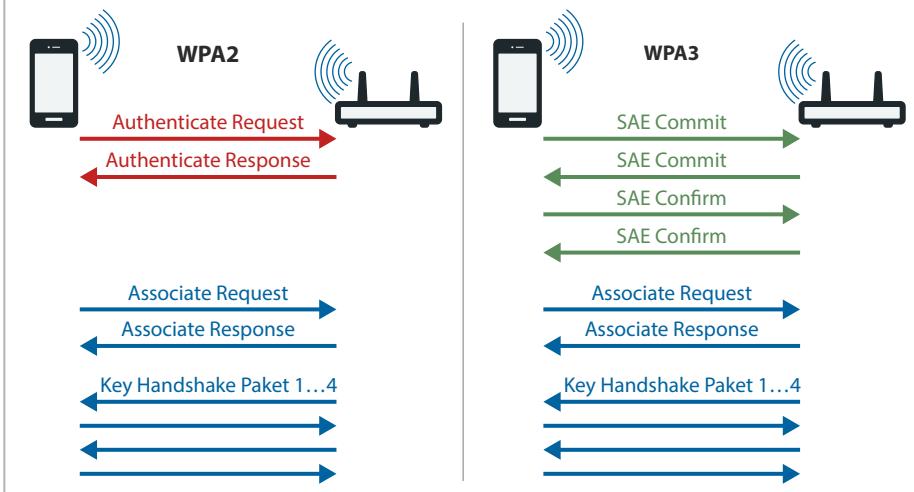
Falls Sie einen Router haben, der sich nicht für WPA3 eignet (etwa ältere Fritzboxen), prüfen Sie Ihren WPA2-Schlüssel: Dabei gilt der dringende Rat, möglichst lange und – besonders wichtig – erwürfelte Passwörter zu verwenden. Mit jedem weiteren Zeichen, das zufällig aus Buchstaben (groß und klein) sowie Ziffern gewählt wird, vergrößert sich der Suchraum um den Faktor 62.

Setzt man seit 2016 eine Vervierfachung der Hardware-Leistung an, dann würde ein solches 16-stelliges Passwort dem 100.000-Dollar-Knacker heute im Mittel immer noch rund 19 Billionen Jahre standhalten. Selbst wenn einem Aggressor die tausendfache Leistung zur Verfügung steht und noch eine kryptologische Abkürzung entdeckt wird, die den Aufwand auf ein Tausendstel reduziert, genügt WPA2-PSK mit einem so langen Passwort noch weiiiiit über Ihre Rente hinaus.

Um die zunehmende Sperrigkeit beim Eintippen zu umgehen, kann man WLAN-Clients per Knopfdruck (WPS-Taste) oder bei Smartphones und Tablets auch per Abfotografieren eines QR-Codes koppeln. Es gibt also keinen Grund, sichere Passwörter zu meiden.

## WLAN-Anmeldung bei WPA2 und WPA3

Der Hauptunterschied zwischen den WPA-Varianten liegt am Anfang des Verbindungsaufbaus: Bei WPA3 machen die Stationen einen an Diffie-Hellman angelehnten Schlüsseltausch. Mit dem darüber vereinbarten temporären Schlüssel schützen sie den eigentlichen Key Handshake, was Angreifern die Grundlage für Wörterbuchattacken und das nachträgliche Dechiffrieren von Nutzerdaten entzieht (Perfect Forward Secrecy, PFS).



Weiterhin fehlt WPA2-PSK der Vertraulichkeitsschutz Perfect Forward Secrecy (PFS): Hat ein Angreifer die WPA2-Passphrase in die Finger bekommen, kann er aufgezeichnete Daten nachträglich entschlüsseln. WPA2-Enterprise mit Zertifikaten ist da besser aufgestellt.

2017 kam der Paukenschlag. Ein Team von Sicherheitsforschern um Mathy Vanhoef veröffentlichte die von ihnen gefundene, auf den Namen KRACK getaufte Lücke: Die meisten WPA2-Implementierungen stellten sich als anfällig gegen eine Replay-Attacke heraus (c't 23/2017, S. 16). Mit der konnte ein Angreifer Clients dazu bewegen, verschiedene Pakete mit demselben Schlüssel zu chiffrieren – eine kryptografische Todsünde.

Zwar konnten die Hardwarehersteller die KRACK-Lücke mit Software-Updates schließen. Aber die Wi-Fi Alliance sah sich angesichts des öffentlichen Interesses unter Zugzwang und stellte kurzfristig die bereits in Arbeit befindliche WPA-Version 3 fertig – so schnell, dass eine ganze Weile kein Hersteller WPA3-fähige Geräte vorweisen konnte.

### WPA3 endlich da

Mittlerweile hat sich die Situation gewandelt und WPA3 ist nicht nur in die Firmware teurer Enterprise-Basen eingezogen, sondern auch in der aktuellen Version 7.20 von AVMs FritzOS angekommen. Damit können nun viele Fritzbox-Besitzer von WPA3 profitieren.

Erfreulicherweise ändert sich auf den ersten Blick beim Einrichten der WLAN-Verschlüsselung nichts. Wie früher gewährt bei WPA3-Personal eine Passphrase den Zugang. So wird auch der mittelfristig

WLAN > Sicherheit

Verschlüsselung      WPS-Schnellverbindung

Hier legen Sie fest, wie das WLAN-Funknetz gesichert wird.

WPA-Verschlüsselung (größte Sicherheit)

unverschlüsselt (nicht empfohlen, ungeschützt)

**WPA-Verschlüsselung**

Legen Sie einen WLAN-Netzwerkschlüssel fest. Der Netzwerkseinstellung.

WPA-Modus

WPA2 + WPA3

WLAN-Netzwerkschlüssel

Ganz23total42geheimes08Pass15wort

sehr stark

Weitere Sicherheitseinstellungen

AVM Stick & Surf aktivieren

Unterstützung für geschützte Anmeldungen von WLAN

Zugang zum Internet für Ihre Gäste

Gastzugang aktiv

Bieten Sie Ihren Besuchern mit dem Gastzugang einen Zugang zum Internet an.

privater WLAN-Gastzugang

Dieser kennwortgeschützte Gastzugang eignet sich um Freunden und Namen für das WLAN-Funknetz und einen WLAN-Netzwerkschlüssel zu verwenden.

öffentlicher WLAN-Hotspot

Mit dieser Option bieten Sie WLAN an, das allen Besuchern offen steht. Arztpraxis sinnvoll sein, wo Sie den Nutzern den WLAN-Netzwerkschlüssel öffentlichen Hotspot, grundsätzlich unverschlüsselt übertragen werden (OWE).

WLAN-Zugang für Gastzugang/Hotspot

Vergeben Sie hier den Funknetznamen für Ihren WLAN-Hotspot. Ihre Besuchernetzwerkschlüssel wird nicht verwendet. Beachten Sie, dass der WLAN-Name nicht verändert werden darf.

Name des WLAN-Hotspots (SSID)

cttest-reshw-hotspot

Offenes WLAN. Zugang ist ohne WLAN-Netzwerkschlüssel möglich.

**FritzOS 7.20 bringt die WPA3-Mixed-Mode-Verschlüsselung fürs Haupt- und fürs Gast-WLAN. Letzteres kann alternativ im Hotspot-Modus betrieben, um Besuchern und Kunden einen verschlüsselten Internetzugang ohne Passworteingabe anzubieten.**

unverzichtbare Mixed-Mode möglich: Die Funkzelle bietet WPA2 und WPA3 parallel an, damit ältere Clients weiterhin über WPA2 Verbindung bekommen. Denn bis die nicht WPA3-fähigen Smartphones, Tablets, Notebooks und PC-Adapter aus dem Markt verschwunden sind, wird es noch einige Jahre dauern.

Stellen Sie in der Router-Konfiguration unter „WLAN/Sicherheit“ den Ausklapper WPA-Modus von „WPA2(CCMP)“ auf „WPA2 + WPA3“ um. Wenn sich nun ein WPA3-fähiger Client anmeldet, ist bei ihm der Sitzungsschlüssel gegen Abhören und einen folgenden Brute-Force-Angriff geschützt, der Client lässt sich nicht mehr per Deauth-Paketen vom Fritz-WLAN abmelden, um ihn auf einen Fake-Hotspot umzulenken, und sein Datenverkehr ist nicht mehr nachträglich entschlüsselbar.

## Auch für Hotspots

Als Bonus hat AVM auch das optionale Gastnetz mit WPA3 im Mixed-Mode versehen, sodass Ihre Besucher ebenfalls besser geschützt sind. Alternativ können Gastwirte und andere Selbstständige das Fritzbox-Gastnetz für ihre Kunden auf den WPA3-Hotspot-Modus Enhanced Open umstellen: Die dort mit dem alten Namen OWE (Opportunistic Wireless Encryption) bezeichnete automatische Verschlüsselung ist zwar auch nicht perfekt, weil sie Man-in-the-Middle-Attacken zulässt. Trotzdem schützt Enhanced Open die Kunden in Restaurants, Praxen oder Kanzleien weit besser gegen simples Abhören als unverschlüsselte Hotspots. Damit alte Clients nicht hinten runterfallen, läuft Enhanced Open im Transitional-Modus. Geräte, die sich nicht darauf verstehen, bekommen so wenigstens eine unverschlüsselte Verbindung und sind nicht komplett ausgeschlossen.

Auch bei WPA3-PSK gilt es, ein sicheres Passwort zu verwenden, das weder in einem Wörterbuch steht noch einfach zu erraten ist. Nun geht bei Ihnen gewiss die Frage im Kopf auf, wo denn überhaupt die Vorteile von WPA3 liegen. Sie liegen im Detail und haben es in sich.

Zum einen verwendet WPA3 die Passphrase während der Anmeldung so, dass ein Angreifer allein durch passives Mithören nicht mehr in der Lage ist, eine Offline-Wörterbuch-Attacke auf das WLAN-Passwort zu führen.

WPA3 verknüpft dazu die Passphrase mit einem Diffie-Hellman-artigen Schlüsselaustausch, über den sich die Stationen auf einen temporären Schlüssel einigen. Damit schützen sie den folgenden Key Handshake, mit dem sie den für die WLAN-Übertragungen genutzten Pairwise Key ermitteln. Das entzieht dem Angreifer einen wesentlichen Baustein, den er braucht, um ein Passwort zu erraten.

Wer Passwörter durchprobieren will, muss bei WPA3 folglich aktiv eine Verbindung zum AP aufbauen. Dabei lässt sich aber jedes Mal nur ein Passwort testen. Brute-Force-Attacken dauern so unrealistisch lange und fallen schnell auf. Die WLAN-Basen wehren sich dann mit verzögerten Antworten, was blindes Raten völlig aussichtslos macht.

## Entspannt zurücklehnen?

Die neue Schlüsselaushandlung erfüllt auch den PFS-Wunsch: Ist WPA3 auf den Stationen korrekt umgesetzt, dann verworfen sie die Aushandlungsschlüssel nach der Verwendung. Spätestens beim Verbindungsende ist kein Material mehr vorhanden, anhand dessen sich mitgeschnittene Daten nachträglich dechiffrieren ließen, was Seitenkanal-Attacken vorbeugt.

Dieses Verfahren ist weder neu noch eine Erfindung der Wi-Fi Alliance, sondern unter dem Namen Simultaneous Authentication of Equals (SAE) schon seit Langem Teil der WLAN-Norm IEEE 802.11: Es wurde einst für sichere Verbindungen zwischen den Nodes in Mesh-WLANs entwickelt (IEEE 802.11s).

Als Nutzer merkt man von all dem nichts: Der zusätzliche Rechenaufwand kostet nur Sekundenbruchteile. Außerdem ist er nur einmal beim Verbindungsauftbau fällig. Die Stationen können ihre paarweisen Schlüssel zwischenspeichern und bei späterer Wiederaufnahme der Verbindung einen Teil der Aushandlung überspringen. Das nützt besonders in verteilten WLANs für größere Gebäude, wo die Mobilgeräte häufig zwischen mehreren Basen hin und her springen, etwa einem Mesh-WLAN aus Fritzbox und Fritz-Repeatern. Mit dem kommenden SAE-FT (Fast Transition, IEEE 802.11r) klappt das zukünftig auch mit einer Anmeldung an einer Basis, die dann fürs ganze Netz gilt.

## Leider nicht ganz ...

Auch wenn SAE schon viele Jahre existiert, weckte es erst das Interesse von Sicherheitsforschern, als WPA3-fähige Geräte auf den Markt kamen. Wieder war es Mathy Vanhoef, der die ersten Ergebnisse präsentierte (c't 18/2019, S. 44). Die fielen nicht unbedingt schmeichelhaft aus:

- Die Passphrase lässt sich zwar dank des Diffie-Hellman-artigen Schlüsselaustauschs nicht mehr ermitteln, aber ein Angreifer kann eine WLAN-Basis schon mit wenigen WPA3-Anmeldeversuchen pro Sekunde nahezu auslasten (Denial of Service, DoS). Der dagegen vorgesehene Anti-Clogging-Mechanismus hat sich als untauglich erwiesen.
- Ein Angreifer kann sich als Man-in-the-Middle in den Verbindungsauftbau einschleichen und den Client dazu bringen, eine WPA2-Verbindung aufzubauen, obwohl die Basis WPA3 unterstützen würde. Zwar bemerken die Stationen das und unterlassen die Verbindung, aber es sind genug Pakete in WPA2-Manier gelaufen, dass der Angreifer eine Offline-Wörterbuchattacke darauf starten kann.
- Der Schlüsselaustausch findet auf Basis einer elliptischen Kurve statt. Dabei kann ein Angreifer Client und AP auf eine schwächere Kurve herunterzwingen, was den Schutz mindert.

Diese drei Macken stellen WPA3 nicht insgesamt infrage, aber man darf sich schon

## WLAN verteidigen mit PMF

Protected Management Frames (PMF) verhindern, dass Angreifer Ihren WLAN-Client mit einem gefälschten Steuerungspaket von der Basis lösen können. Im besten Fall resultiert solch eine Attacke nur im Verbindungsabriss (Denial of Service, DoS). Für solchen WLAN-Vandalismus genügt schon ein billiges, als Smartwatch getarntes Spielzeug (Deauther Wristband V2, c't 8/2019, S. 17).

Schlimmstenfalls gelingt es dem Angreifer aber, den WLAN-Client auf seinen Fake-Hotspot umzuleiten, sodass er sich als Man-in-the-Middle in Ihren Datenverkehr einklinken kann. Weil Basen und Clients bei einer WPA3-Verbindung PMF nutzen müssen, sind sie dagegen gefeit. Falls Ihre WLAN-Basis nur WPA2 spricht, aber die PMF-Option bietet, aktivieren Sie sie.

wundern, wieso sie erst im Nachhinein aufgefallen sind. Anders als die KRACK-Lücke lassen sie sich nicht durch Workarounds in der Geräte-Firmware umgehen. Deshalb arbeitet die Wi-Fi Alliance an Erweiterungen und Korrekturen, die voraussichtlich in die Version 3 der WPA3-Spezifikation münden.

## WPA3 aktivieren!

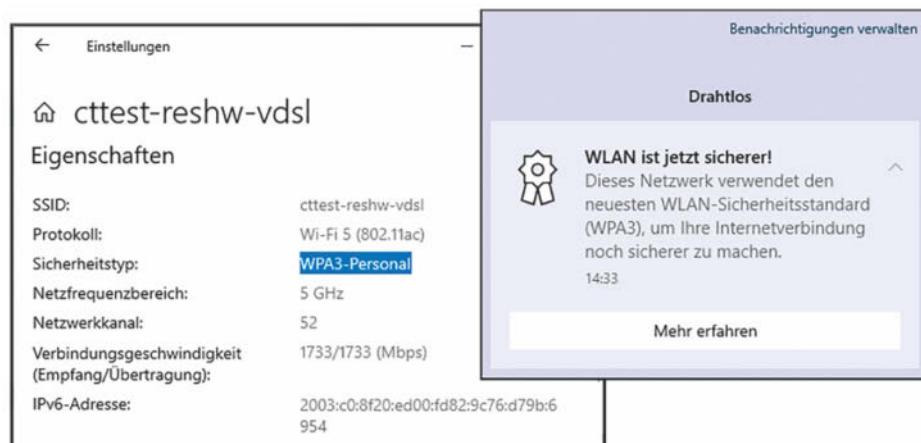
Wer nun zweifelt, ob er WPA3 schon nutzen sollte: Bitte unbedingt! Selbst Mathy Vanhoef hat zugestanden, dass es auch in seiner jetzigen imperfekten Form einen Fortschritt gegenüber WPA2 darstellt.

So setzt Apple WPA3 ab macOS 10.15 beziehungsweise iOS 13 ein und Google ab Android 10. Microsoft Windows 10 beherrscht WPA3 seit Build 1903, setzt aber Unterstützung im Treiber der WLAN-Hardware voraus.

Der auf Linux-Systemen üblicherweise verwendete WPA-Supplicant kann seit Version 2.7 mit WPA3 umgehen. Das Tool ist aber nur der Unterbau auf Betriebssystemebene. Je nach Distribution und verwendetem Desktop (Gnome, KDE et cetera) bietet das nutzerseitige Werkzeug zum Verwalten und Anlegen vom WLAN-Profilen – etwa der GUI-Teil des Network-Managers – WPA3 eventuell noch nicht an. Manchmal zeigt es ein WPA3-fähiges Netz mit „Unbekannter Sicherheitstyp“ an. Probieren Sie die Verbindung trotzdem, unter Kubuntu 20.04 klappte sie.

Nach welchem Verfahren ein Gerät die WLAN-Verschlüsselung ausgehandelt hat, zeigt die Fritzbox in der Liste aktiver Clients an (im Menü unter WLAN/Funknetz). Dort steht unter den Eigenschaften dann „WPA3“ oder „OWE“.

Es gibt auch Clients, die kein WPA3-Update bekommen, beispielsweise AVMs Fritz!WLAN-Sticks. Manche dieser Kandidaten werden sich, anstatt in einem



Beim ersten Verbinden meldet Windows 10, dass das neue WLAN WPA3 spricht und bietet Informationen dazu an. Wer sich später vergewissern will, klickt auf das WLAN-Tray-Symbol, öffnet die Verbindungseigenschaften und blättert herunter zum Sicherheitstyp.

Mixed-Mode-Netz (WPA2+3) auf WPA2 zurückzufallen, gar nicht mehr verbinden. Der Grund sind – wie meistens – Implementierungsfehler, die im WPA2-Netz nicht auffielen. Wenn die Basis es unterstützt, kann man für solche Clients per Multi-SSID eine separate WPA2-only-Funkzelle aufspannen und mit einer eigenen Passphrase versehen. Das beherrschten Fritzboxen leider noch nicht. Sollte es in Ihrem Gerätepark Clients geben, die den Mixed-Mode nicht mögen, müssen Sie vorerst bei WPA2 bleiben.

Als Momentaufnahme haben wir eine Handvoll Geräte an zwei WLAN-Basen geprüft und durchwachsene Ergebnisse verzeichnet (siehe Tabelle). Neuere WLAN-Adapter (Wi-Fi 6: Intel AX200) werden offensichtlich besser gepflegt als ältere (Wi-Fi 5: Qualcomm QCA6174) und deren Windows-Treiber ebenso besser als die Linux-Varianten.

Beim riesigen Android-Hard- und Software-Zoo muss man mit Überraschungen rechnen: So verhielt sich unser

vergleichsweise altes Android-8-Muster (Sony Xperia X Compact) kompatibler als ein Android-9-Beispiel (Nokia 5), das WPA3-Funkzellen aller Spielarten komplett verschmähte. Der verschlüsselte Hotspot-Betrieb (Enhanced Open) klappete an der Fritzbox nur mit einem Client (Intel AX200 unter Windows 10).

## Fazit

Trotz seiner anfänglichen Hakeleien ist WPA3 ein großer und wichtiger Schritt zu mehr WLAN-Sicherheit. Auch wenn es noch etwas Zeit braucht, bis WPA3 in den meisten Netzen mit den meisten Clients reibungslos läuft, sollten es Fritzbox-Nutzer jetzt aktivieren. Bei der erfahrungsgemäß langfristigen Firmware-Pflege von AVM stehen die Chancen gut, dass sich das weiter verbesserte WPA3 Release 3 ab 2021 nachrüsten lässt und man WLAN-sicherheitstechnisch eine Weile Ruhe hat. (ea@ct.de) **ct**

**WPA3-Hinweise von AVM und Microsoft: [ct.de/yt8p](http://ct.de/yt8p)**

## WPA3-Kompatibilität

	Fritzbox-WLAN Mixed-Mode	Fritzbox-Gastnetz Mixed-Mode	Fritzbox-Hotspot (Enh. Open Trans.)	L822 Mixed-Mode	L822 WPA3 only	L822 Hotspot (Enhanced Open)	L822 Hotspot (Enh. Open Trans.)
Windows 10 (Wi-Fi-5: QCA6174)	WPA2	WPA2	unverschlüsselt	WPA2	keine Verbindung	keine Verbindung	unverschlüsselt
Windows 10 (Wi-Fi-6: AX200)	WPA3	WPA3	WPA3	WPA3	WPA3	WPA3	keine Verbindung
Linux (Kubuntu 20.04, QCA6174)	WPA3	keine Verbindung	unverschlüsselt	WPA3	WPA3 <sup>1</sup>	keine Verbindung	unverschlüsselt
Linux (Kubuntu 20.04, AX200)	WPA3	keine Verbindung	unverschlüsselt	WPA3 <sup>1</sup>	WPA3 <sup>1</sup>	keine Verbindung	unverschlüsselt
macOS 10.15.6 (MBP 2015, A1502)	WPA3	WPA3	unverschlüsselt	WPA3	WPA3	keine Verbindung	unverschlüsselt
macOS 10.15.6 (MBP 2020, A2251)	WPA3	WPA3	unverschlüsselt	WPA3	WPA3	keine Verbindung	unverschlüsselt
Android 8 (Sony Xperia X Compact)	WPA2	WPA2	keine Verbindung	WPA2	keine Verbindung	keine Verbindung	unverschlüsselt
Android 9 (Nokia 5)	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung
Android 10 (Samsung S7+)	WPA3	keine Verbindung	unverschlüsselt	WPA3	WPA3	WPA2	unverschlüsselt
iOS 14 (iPhone X)	WPA3	WPA3	unverschlüsselt	WPA3	WPA3	keine Verbindung	unverschlüsselt

<sup>1</sup> nach manuellem Einrichten der Verbindung Fritzbox: AVM Fritzbox 7590 mit FritzOS 7.20, L822: Access-Point Lancom L822 mit Firmware 10.40.0291RU1

# Keine Cookies – auch kein Problem

## Onlinewerbung floriert in der Krise

**Dank des Siegeszugs der programmatischen Werbung trotz die Online-Werbebranche der Corona-Krise. Dem Wegfall der Cookies sehen die Werber optimistisch entgegen.**

Von Torsten Kleinz

Pünktlich zur Branchenmesse Dmexco konnte der Online-Vermarkterkreis (OVK) im Bundesverband Digitale Wirtschaft (BVDW) erstaunlich positive Zahlen vermelden (siehe ct.de/yw5m). Während der Werbemarkt für Reisen im Verlauf der Coronakrise fast komplett weggebrochen war, fingen andere Branchen wie der Handel die ausgefallenen Umsätze weitgehend auf. Für das gesamte Jahr 2020 erwartet die Werbebranche einen Umsatz von 3,93 Milliarden Euro, ein Wachstum von 8,6 Prozent im Vergleich zum Vorjahr.

Eigentlich hatte die Werbebranche einen größeren Umsatzverlust durch die nachgezogenen Effekte der Datenschutz-Grundverordnung erwartet. Denn bisher konnten deutsche Websites nach einer Regelung des Telemediengesetzes auch dann Cookies setzen, wenn die Nutzer nicht explizit der Speicherung zugestimmt hatten. Doch der BGH hatte dem ein Ende bereitet (siehe ct 14/2020, S. 48). Dadurch drohte der Werbewirtschaft eines der zentralen Elemente für die Personalisierung wegzufallen.

### Unverminderter Datenhunger

Doch diese Befürchtungen haben sich bisher nicht bestätigt. Im Gegenteil: Das programmatische Advertising, bei dem über Echtzeitbörsen personalisierte Werbung versteigert und auftausenden verschiede-

nen Websites und Apps ausgespielt wird, konnte seinen Anteil am Werbemarkt sogar noch steigern – von 62 Prozent im Jahr 2019 auf 67 Prozent im laufenden Jahr. Dieses Wachstum geht zu Lasten der klassischen Werbebuchungen, die in Jahresfrist von 1,367 auf 1,287 Milliarden Euro zurückgingen.

Ein Teil des Erfolgs ist auf neue Cookie-Banner zurückzuführen, die die Ablehnung der Datenverarbeitung zu einer schwer durchschaubaren Klickorgie machen. So hat Werbevermarkter Ströer in Feldversuchen zum Beispiel den Schließen-Button entfernt, der das einfache Ablehnen von Cookies möglich macht. Nach Angaben von Christopher Kaiser, stellvertretender Vorsitzender des OVK und CEO von Ströer Digital, bewirkten solche Banner enorme Zustimmungsraten von 80 bis 90 Prozent.

Kritik an der irreführenden Gestaltung wollte er auf der Dmexco-Pressekonferenz nicht gelten lassen. So seien die Consent-Banner vor Einführung ausgiebig von Anwälten geprüft worden. „Die Form, in der das jetzt im Markt sehr einheitlich umgesetzt wird, ist in meinen Augen der beste Weg, wie man das machen kann“, sagte Kaiser.

Dennoch bereiten sich viele Anbieter auf eine Cookie-lose Zeit vor, weil Browser immer mehr Cookies mit den Voreinstellungen blockieren (siehe ct 21/2019, S. 38). Sogar Google, selbst großer Werbe-

vermarkter, hatte bereits angekündigt, dass sein Browser Chrome binnen zwei Jahren auf Third Party Cookies verzichten werde. Allerdings machte Google im Rahmen der Dmexco klar: Der Zeitplan ist nicht in Stein gemeißelt. Man werde die Unterstützung der Third Party Cookies nicht einstellen, ohne für Ersatzlösungen zu sorgen, die nicht nur das Targeting weiter ermöglichen, sondern auch andere Aspekte des Marketings wie die Erfolgskontrolle abdecken.

Viele Anbieter fragen mit ihren Cookie-Bannern ohnehin nicht nur den derzeitigen Status quo ab, sondern bereiten sich bereits auf die Cookie-lose Zeit vor und holen beim Surfer ein Einverständnis zum Beispiel für Browser-Fingerprinting ein. Das Cookie ganz aufzugeben wollen die meisten Adtech-Unternehmen nicht. So arbeitet der Werbeverband IAB am Projekt „Rearc“, das einen universellen Identifier schaffen will, der die Kopplung von Kundenprofilen weiterhin ermöglichen soll.

In Deutschland ist der Anbieter Net-ID dabei, eine Login-Allianz zu schmieden, bei der sich Nutzer mit den gleichen Zugangsdaten bei einer Reihe unterschiedlicher Anbieter einloggen können. Gewinnt das Konzept mehr Anhänger, könnten sich die Cookie-Banner in Login-Walls verwandeln, die den Zugang zu freien Inhalten nur noch nach Anmeldung erlauben.

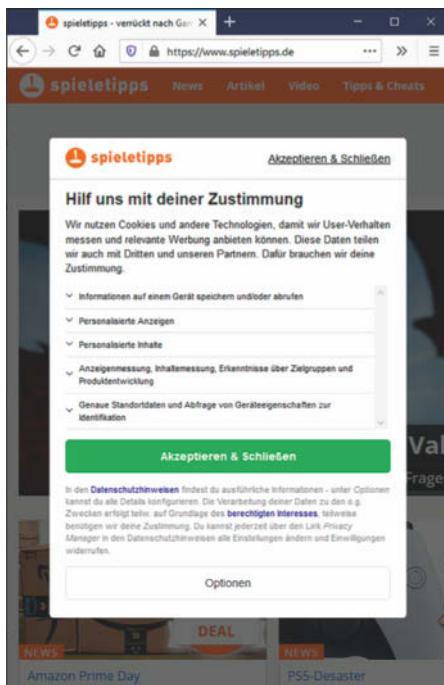
### First Party Tracking

Das Tracking wird dazu in Richtung der Website-Betreiber verlagert – First Party Data ist das neue Modewort der Branche. Statt Third Party Cookies in Websites und Apps einzubetten, die von Werbenetzwerken erfasst werden, sollen Handel und Medien die Daten erfassen oder Werbenetzwerke und Adtech-Firmen Zugriff auf ihre First-Party-Cookies geben.

Wie Targeting direkt beim Website-Betreiber konkret funktioniert, de-

**Das programmatische Advertising konnte seinen Anteil am Werbemarkt sogar noch steigen.**





**Einfaches Ablehnen von Cookies?  
Das ist bei diesem Consent Banner  
nicht vorgesehen.**

monstrierte der Anbieter 1plusX mit seiner Predictive Marketing Platform für Verleger. Das Werbeprofil speist sich aus dem Artikel, den ein Nutzer im Augenblick betrachtet sowie aus seinen historischen Nutzungsdaten auf der Site. Mittels der gewonnenen Erkenntnisse sollen auch Redakteure wertvolle Daten bekommen, welche Inhalte beim Publikum besonders beliebt sind und wie sie optimal ausgespielt werden können.

Einen ähnlichen Ansatz verfolgt BurdaForward mit seinem System „Sugarless“, das der Münchener Verlag kurz vor der Dmexco vorgestellt hatte. Statt nach dem persönlichen Interessenprofil des Nutzers richtet sich die ausgespielte Werbung danach, welche Inhalte sein Browser anzeigt. Dazu nutzt Burda ein neues System der Inhalteerkennung, das über die üblichen Taxonomien mit einigen hundert Schlagwörtern hinausgeht.

Als Alternative zum Tracking setzen immer mehr Medien auf ein tracking-freies Abonnement, bei dem Leser zur

Kasse gebeten werden. Für das Hamburger Magazin Spiegel ist dies derzeit ein Erfolgskonzept, wie Projektmanager Hannes Engler in Köln erläuterte. So zahlt mittlerweile eine fünfstellige Anzahl von Lesern für die Werbefreiheit – für Abonnenten des Print-Magazins kostet dies 2 Euro, für Nicht-Abonnenten 5 Euro pro Monat. Wer dieses Angebot jedoch ablehnt, erklärt sich automatisch mit der vollen Datenweitergabe zu Werbezwecken einverstanden.

Dass sich mit technischen Tricks und Überredung immer noch nicht alle Kunden adressieren lassen, haben mittlerweile auch die Werbenetzwerke eingesehen. So wirbt etwa das Anbieter Xandr dafür, dass Werbetreibende zusätzliche Kampagnen buchen, bei denen sie alle Personalisierungsoptionen deaktivieren und so die attraktive Zielgruppe der Cookie-Verweigerer erreichen. Das Schlagwort: „Simple Ads“.

(jo@ct.de) **ct**

**Zahlen BVDW/OKV:** [ct.de/yw5m](http://ct.de/yw5m)

**V** Genossenschaftliche FinanzGruppe  
Volksbanken Raiffeisenbanken

## IT-Job, der über 0 und 1 hinausgeht |

**DZ BANK Gruppe**  
Zweitgrößte FinanzGruppe Deutschlands  
Digitale Trendsetter im Bankwesen  
Moderne Projektmanagement-Methoden  
Vielseitige Entwicklungsmöglichkeiten  
Ganzheitlicher Problemlöser

Wenn auch Sie im Job mehr bewirken wollen: Willkommen im Team.  
Bewerben Sie sich jetzt: [www.karriere.dzbankgruppe.de](http://www.karriere.dzbankgruppe.de)



MEHR BE WIR KEN

**Jetzt bewerben!**

**DZ BANK Gruppe**

# Firefox mit mehr Farbe und Funktionen

**In der Desktop-Version von Firefox 81 kann man Audio- und Videoinhalte mit der Tastatur steuern. Unter iOS 14 und iPadOS 14 lässt er sich als Standardbrowser einrichten.**

Mozillas Firefox-Browser hat ein Update und neue Funktionen bekommen. In der Desktopversion können Sie Audio- und Videoinhalte nun auch über die Tastatur oder ein Headset steuern. Das geht selbst dann, wenn Sie gerade in einem anderen Tab oder Programm arbeiten. Außerdem hat Mozilla der Anzeige ein „Alpenglow“ (Alpenglühen) als Effekt spendiert. Das farbenfrohe Theme ergänzt die bisherigen drei bordeigenen Looks „Standard“, „Hell“ und „Dunkel“.

Firefox unterstützt ab Version 81 außerdem „AcroForm“ für PDFs. Diese können Sie damit ausfüllen, ausdrucken und abspeichern. Zusätzlich hat Mozilla der PDF-Anzeige ein Facelift spendiert. Den Bild-in-Bild-Modus erreichen Sie über ein neues, besser auffindbares Icon. Neu ist auch die Unterstützung der Dateitypen XML, SVG und WEBP. Die belgische, die österreichische und die schweizeri-

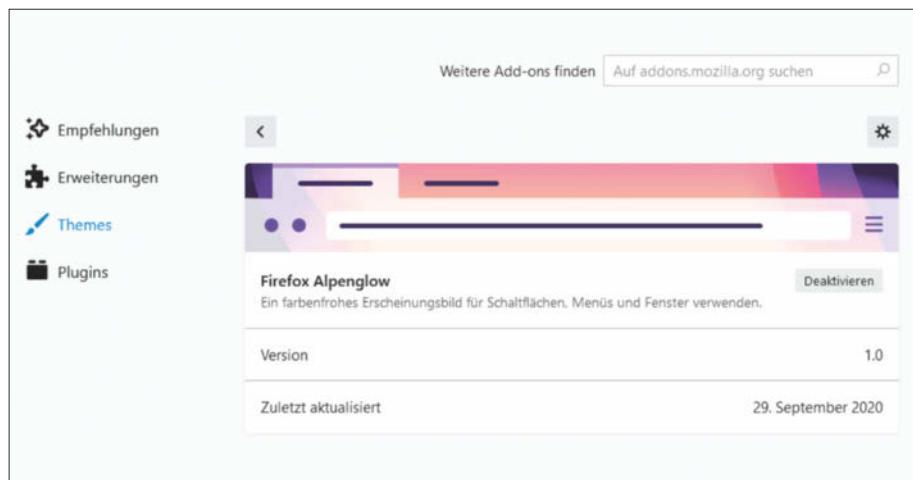
sche Variante erhalten zudem die deutsche Ausgabe des Nachrichtenvorschlagsystems Pocket.

Als Nutzer von iOS 14 und iPadOS 14 können Sie Firefox fortan zum Standardbrowser auf ihren iPhones und iPads machen. Dabei kommt Mozilla zugute, dass Apple seine mobilen Betriebssysteme mit dem letzten Upgrade im September auch

für andere Browser als den hauseigenen Safari geöffnet hat.

Mit dem Update hat Mozilla außerdem einige Sicherheitslücken gestopft und Bugs gefixt. Die Standardspracheinstellung soll nach Updates nicht mehr auf Englisch zurückspringen; bei Audio- und Videoinhalten hat das Team die Barrierefreiheit erhöht.

(mon@ct.de)



**Firefox wird bunter: Das neue bordeigene „Alpenglow“-Theme soll an den Sonnenuntergang im gleichnamigen Hochgebirge erinnern.**

## DSGVO: Rekordbuße gegen H&M

Der schwedische Bekleidungshändler Hennes & Mauritz (H&M) soll eine Strafe in Höhe von 35.258.707,95 Euro zahlen, nachdem er in einem Servicecenter in Nürnberg Mitarbeiter massiv ausgespäht hatte. Einen entsprechenden Bußgeldbescheid hat der Hamburgische Datenschutzbeauftragte Johannes Caspar jetzt an das Unternehmen geschickt, das seinen deutschen Sitz in der Hansestadt hat. Es handelt sich um **das höchste Bußgeld**, das Aufsichtsbehörden hierzulande verhängten, seit die Datenschutz-Grundverordnung (DSGVO) anwendbar ist.

Im Nürnberger Call-Center sei es mindestens seit 2014 bei einem Teil der Mitarbeiter „zu umfangreichen Erfassungen privater Lebensumstände“ gekommen, wirft Caspar der Firma vor. Selbst nach kurzen Urlaubs- oder Krankheitsabwesenheiten hätten die vorgesetzten Teamleiter einen sogenannten „Welcome

Back“-Talk durchgeführt. Danach seien in etlichen Fällen nicht nur konkrete Urlaubserlebnisse der Beschäftigten festgehalten, sondern auch Krankheitssymptome und Diagnosen.

Zusätzlich eigneten sich einige Vorgesetzte über Einzel- und Flurgespräche ein breites Wissen über das Privatleben ihrer Mitarbeitenden an, heißt es bei der Behörde weiter, „das von eher harmlosen Details bis zu familiären Problemen sowie religiösen Bekenntnissen reichte“. Die Erkenntnisse seien teils digital gespeichert worden und mitunter für bis zu 50 weitere Führungskräfte im ganzen Haus lesbar gewesen.

Die Sache flog auf, weil die Datei infolge eines Konfigurationsfehlers unzureichend gesichert und im Oktober 2019 für einige Stunden unternehmensweit einsehbar war. Insgesamt kam dabei ein Datensatz von rund 60 Gigabyte zusammen.

(Stefan Krempel/jo@ct.de)

## c't <webdev> 2021 wird virtuell

Save the date: Die **Frontend-Entwickler-Konferenz** der c't wird im Frühjahr 2021 ausschließlich als Online-Veranstaltung stattfinden. Am 9. Februar dreht sich in einem Track alles um das Thema Web-Performance. Am 10. Februar werden wir mehrere Workshops anbieten. Eine detaillierte Agenda veröffentlichen wir im November.

Die Präsenzveranstaltung holen wir vom 22. bis zum 24. November 2021 nach. Dann geht es im Kölner Veranstaltungszentrum Komed an zwei Tagen und in drei Tracks wieder um die gesamte Bandbreite der Frontend-Entwicklung: von den Basics der JavaScript- und Webprogrammierung über Frameworks, UX-Design, Workflow und Testing bis hin zu neuen Frontends wie Assistenten, Bots und VR.

# IONOS CLOUD

## Die europäische Cloud-Alternative



**Performant:** Bestes Preis-Leistungs-Verhältnis



**Sicher:** 100 % DSGVO-konform



**Einfach:** Intuitive & flexible Benutzeroberfläche



**Fair:** Pay-per-Minute Abrechnung & kein Vendor Lock-in



**Kundenorientiert:** Kostenloser 24/7 Enterprise-Level-Support

IONOS cloud ist Teil von IONOS, Europas führendem Anbieter von Cloud-Infrastrukturen, Cloud-Services und Hosting-Dienstleistungen. Als einziger Cloud-Computing-Anbieter mit eigenem Code Stack "Made in Germany" wurden wir bereits mehrfach ausgezeichnet.



IONOS by 1&1

# Kasse gesichert – Rechtslage unsicher

## Verzögerungen bei sicheren Kassen

**Bund und Länder streiten um die Umsetzung der gesetzlichen Bonpflicht. Die wichtigen Spezifikationen für Cloud-Kassen kamen zu spät. Das Ergebnis: Rechtsunsicherheit.**

Von Torsten Kleinz

Bei zum 30. September hatten Gewerbetreibende Zeit, ihre Registrierkassen gemäß der 2017 erlassenen Kassensicherungsverordnung mit einem gesicherten Speicher und einer entsprechend aktualisierten Software auszustatten. Doch bereits im Juli schlugen fünf Bundesländer Alarm, dieser Termin sei kaum zu schaffen. Wie die Süddeutsche Zeitung berichtet, haben deshalb außer Bremen inzwischen alle Bundesländer die Übergangszeit verlängert. Betriebe sollen zum Beispiel in Hessen bis zum 31. März 2021 nichts zu befürchten haben, sofern sie die Umstellung auf das System bereits begonnen haben.

Worum geht es konkret? Die Vorschrift des Bundes sieht neben einer durchgängigen Bonausgabepflicht auch vor, dass spätestens ab dem 1. Oktober alle Buchungen auf einem gesicherten Speicher, einer sogenannten TSE (Technische Sicherungseinrichtung), abgelegt und mit einer Signatur ausgedruckt werden. Diese Regelung soll Steuerprüfern die Kontrolle im Rahmen der neu eingeführten Kassennachschauf erleichtern.

### Noch nicht umgesetzt

Doch wer im Herbst 2020 einen kritischen Blick auf einen Kassenbon wirft, wird nur sehr selten eine TSE-Signatur sehen. Selbst große Supermarktketten wie Aldi

oder Lidl haben die Umstellung bisher nicht vollzogen.

Kritiker begründen die Verzögerung zum einen mit der Überlastung des Handels durch die Corona-bedingte Umsatzsteuersenkung. Zum anderen werfen sie der Bundesregierung vor, die technischen Vorschriften zu lange hinausgezögert zu haben. Zwar wurden die ersten TSE-Speicher schon im Februar für den Handel angeboten, nicht aber Lösungen für sogenannte Cloudkassen, die ihre Umsätze über das Internet direkt an ein Rechenzentrum oder einen Dienstleister schicken.

Der österreichische Spezialist für Kassensicherung Fiskaly war im Frühjahr noch optimistisch, bis April seine Lösung rechtskonform ausliefern zu können. Doch Unklarheiten bei den technischen Richtlinien sorgten für Verspätung beim Bundesamt für Sicherheit in der Informationstechnik: Das neue SMAERS-Schutzprofil, (Security Module Application for Electronic Record Keeping Systems), technische Grundlage für die Cloud-TSE, wurde erst am 28. Juli finalisiert – zu spät für eine fristgerechte Umsetzung.

### Fristen-Hickhack

Das Bundesfinanzministerium will diese Einsprüche jedoch nicht gelten lassen. „Nach Kenntnisstand des Bundesministeriums der Finanzen können alle Kassen, ob Registrierkasse oder Cloudkasse, mit den bereits zertifizierten Token-TSE gesichert werden“, erklärt eine Sprecherin auf Anfrage von c't. Verspätungen beim Zertifizierungsprozess lägen nicht in der Hand der Bundesregierung: „Die Dauer der Zertifizierung eines Produktes nach festgelegten Sicherheitsvorgaben ist von vielen Faktoren abhängig, die im Wesentlichen durch den Hersteller und die von diesem beauftragte Prüfstelle beeinflusst sind.“

Auch die Bundesländer wollen den Händlern keinen Freibrief geben. Nach

wie vor gilt die Verpflichtung, die TSE so bald als möglich zu installieren. Wer jedoch bereits eine Cloudkasse installiert hat, soll auf die Bereitstellung durch die Anbieter warten dürfen. Während aber der Bund nur in Härtefällen auf Antrag einen Aufschub geben will, haben die meisten Bundesländer inzwischen einen antragslosen Aufschub in ihre Erlasse geschrieben. Was nun in der Praxis gilt, ist damit auch für Experten unklar.

Fiskaly erwartet unterdessen keine Probleme für seine Kunden, auch wenn die offizielle Zertifizierung länger dauert. Die meisten Steuerfahnder arbeiten nämlich nicht für den Bundesfinanzminister, sondern für seine Länderkollegen. „Da die zuständigen Finanzämter der Bundesländer für die Exekution zuständig sind, gehen wir davon aus, dass diese im Sinne ihrer Erlasse handeln und den Steuerpflichtigen die verlängerte Frist bis 31. 3. 2021 gewähren, soweit die Voraussetzungen eingehalten werden“, erläutert Fiskaly-Gründer und -Manager Simon Tragatschnig gegenüber c't. (hps@ct.de) **ct**

**Literatur und Rechtsquellen:** [ct.de/y3df](http://ct.de/y3df)



Quelle: Bundessteuerberaterkammer

**Claudia Kalina-Kerschbaum, Geschäftsführerin der Bundessteuerberaterkammer, verlangt, Bund und Länder sollen sich einheitlich zu Fristen der Kasseneinführung positionieren.**

# Enquete-Kommission „KI“ stellt eigene Arbeit vor

Die Enquete-Kommission zum Thema „Künstliche Intelligenz“ hat ihre Arbeitsergebnisse präsentiert. Der offizielle Abschlussbericht steht allerdings noch aus.

In einem per Livestream übertragenen Event hat die Enquete-Kommission des Deutschen Bundestages zum Thema „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ das Ergebnis ihrer zweijährigen Arbeit der Öffentlichkeit präsentiert.

Die Kommission setzt sich aus 19 externen Sachverständigen und 19 Mitgliedern des Bundestages zusammen. Vertreter beider Gruppen zeigten sich bei der Präsentation recht zufrieden mit dem Ergebnis. Man habe seine Empfehlungen auf eine breite parlamentarische Basis stellen können. Wer immer in Zukunft regiere, habe am Ergebnis der Kommission mitgearbeitet

und könne es nutzen. Was genau die Empfehlungen sind, wurde allerdings nur anekdotisch genannt. Für einen Überblick wird man auf den offiziellen Abschlussbericht warten müssen, der Ende Oktober dem Bundestag vorgelegt werden soll.

Von Vertretern der Opposition wurde unter anderem bemängelt, dass die Kommission transparenter hätte agieren können, zumal die Notwendigkeit einer frühen und breiten Einbindung der Öffentlichkeit in die Debatte über und in die Entwicklung von KI-Systemen eines der zentralen Ergebnisse der Kommission ist. Die Kritik wurde bereits früher erhoben, aber die Kommission reagierte eher zögerlich. Bei der Abschlusspräsentation konnte die Öffentlichkeit immerhin über ein Online-Tool live Fragen einreichen.

Wie produktiv die gefundenen Empfehlungen politisch sind, wird sich zeigen müssen. So konnte sich im Januar dieses Jahres der Bundestag nicht darauf einigen,



Die Vorsitzende der Kommission, Daniela Kolbe (SPD), eröffnete die Veranstaltung.

autonome Waffensysteme zu ächten – und das, obwohl das zuständige Projekt der Kommission, die Gruppe „KI und Staat“, genau das als Konsens erzielt und bereits veröffentlicht hatte. (syt@ct.de)

Aufzeichnung der Präsentation:  
[ct.de/y6vf](http://ct.de/y6vf)

## WAS AUCH IMMER SIE BRAUCHEN – MIT DER SOURCING PLATFORM BESCHAFFEN WIR DAS!

Bei Conrad finden Sie jetzt Ihren technischen Betriebsbedarf und umfassende Services.



# Desla

## Volkswagens E-Fahrzeug ID.3 getestet

**VW will mit dem batterieelektrischen ID.3 ein E-Auto für jeden an den Start bringen. Das Versprechen: solide Hardware und innovative Software made in Germany. Doch bei letzterer hapert es zwei Wochen nach Auslieferungsstart noch.**

Von Sven Hansen und Stefan Porteck

Einige sehen im ID.3 den Versuch der Deutschen, Tesla zumindest in der Mittelklasse Paroli zu bieten, andere die letzte Chance, in Sachen E-Mobilität überhaupt noch Fuß fassen zu können. So waren auch wir „elektrisiert“, als wir den ID.3 für einige Stunden spontan unter die Finger bekommen konnten. Genug Zeit, um VWs Angriff auf den batterieelektrischen Massenmarkt etwas genauer in Augenschein zu nehmen.

### Konnektivität

VW hat mit der Auslieferung an Kunden bereits begonnen, unser Testwagen schien jedoch noch nicht voll an das Backend angebunden zu sein. Er ließ sich zwar mit der We-Connect-ID-App koppeln, allerdings standen zunächst nur Basisfunktionen wie zum Beispiel die Klimasteuerung bereit. Die Sprachsteuerung funktionierte nur eingeschränkt, die Hotspot-Funktion gar nicht. Eigentlich soll der ID.3 die fest verbaute eSIM gegen Geld auch per WLAN für die Fahrgäste nutzbar machen.

Im praktischen Einschub in der Mittelkonsole verstaut man das Handy, ohne es dabei kabellos laden zu können. Gleich in der Nähe sind zwei USB-C-Anschlüsse eingebaut. Unser ID.3 konnte Medieninhalten vom Handy wiedergeben, verstand sich allerdings weder auf CarPlay noch auf Android Auto. Über das große Mitteldisplay bediente sich das Infotainment-System oft etwas hakelig und ruckelte gelegentlich bei Animationen. In allen Punkten ist da durchaus Luft nach oben.

Das gilt auch für die zugehörige Smartphone-App: Obgleich VW bereits eingeräumt hat, dass diese beim Verkaufsstart nicht den vollen Funktionsumfang haben wird, waren wir doch erstaunt, wie wenig zwei Wochen nach diesem Termin funktioniert. Die Einrichtung geht noch flott von der Hand: In der App einen Account anlegen, das Fahrzeug durch Eingabe der Fahrgestellnummer hinzufügen und dies abschließend auf dem Infotainment-Display bestätigen.

In der Theorie soll die App etwa den gleichen Umfang bieten wie bei anderen Connected-Cars: Dazu zählen Online-Verkehrsdaten, Ver- und Entriegeln per Smartphone sowie die Steuerung der Klimaanlage und des Ladevorgangs aus der Ferne. Zu Beginn unseres Tests war davon lediglich die Steuerung der Klimatisierung verfügbar. Den Versuch, die Temperatur zu verändern, quittierte die App mit einer Fehlermeldung.

### Fahren & Laden

Doch offenbar wird hinter den Kulissen bei VW mit Hochdruck an der Konnektivität gearbeitet. Drei Stunden später zeigte sich in der App plötzlich die Akkuladung nebst Restreichweite. Nun ließ sich zum Beispiel der Ladevorgang per App starten und beenden.

Der ID.3 1st Edition wartet mit mehreren Fahrmodi von sparsam bis sportlich

auf. Auf Wunsch lassen sich die Charakteristik der Dämpfer, der Lenkung und der Gasannahme auch individuell anpassen. Einen deutlichen Unterschied bemerkten wir indes nur bei der Beschleunigung.

Besonders begeisterte uns der kleine Wendekreis von nur 10,2 Meter. Beim Laden lernt man die Wendigkeit des ID.3 zu schätzen: Die CCS-Buchse sitzt hinten rechts, wo man normalerweise die Tanköffnung findet, weshalb man meist rückwärts an die Ladesäulen fahren muss.

In Sachen Fahrassistenz hatte unsere Plus-Variante der 1st Edition wenig zu bieten. Ein adaptiver Tempomat und ein Spurhalteassistent hielten das Fahrzeug auf Abstand zum Vordermann, allerdings nur leidlich in der Spur. Bei ausgeschaltetem Tempomat erhielten wir zudem keine Warnung beim Verlassen der Spur.

Dass Volkswagen mit dem ID.3 durchaus mehr vorhat, zeigt das sogenannte „ID-Light“ im Cockpit. Das unter der Windschutzscheibe platzierte LED-Band dient der Kommunikation mit dem Fahrer. Ein Lichtimpuls über die gesamte Breite des Cockpits zeigt etwa eine Abbiegeaufforderung durch das Navi an. Solch elaborierte Komponenten zur Mensch-Maschine-Kommunikation braucht es eigentlich nur für hochautomatisiertes Fahren.

### Fazit

Dass die Software schlichtweg nicht fertig ist, dürfte zumindest technikbegeisterte Erstkäufer gehörig nerven. Alle anderen bekommen davon vielleicht nicht viel mit, sie werden sich über ihr schickes und wendiges E-Mobil freuen. Der ID.3 bewegt sich flott durch die City und ermöglicht dank hoher Reichweite und CCS-Ladung auch komfortables Reisen auf langen Strecken. (sha@ct.de) **ct**

Auf dem Mini-Display hinter dem Lenkrad ist nicht viel Platz für Informationen.





SAVE  
THE  
DATE

24  
25  
FEBRUAR  
2021



WIR  
STARTEN  
DURCH  
ABER MIT  
SICHERHEIT

# Geborene Konversationistin

## Alexa behält Nutzer im Blick und führt Gruppengespräche

**Das Echo Show 10 ist nicht nur Amazons erstes motorisiertes Smart Display, sein Prozessor soll die integrierte Sprachassistentin auch auf die nächste Evolutionsstufe heben. Für manche dürfte damit aber eine rote Linie überschritten werden.**

Von Nico Jurran

Amazons Ankündigungen zur neuesten Generation seiner smarten Lautsprecher und Displays klangen zunächst wenig spektakulär: Der neue Echo bietet wie der Echo Plus einen integrierten Smart Home Hub mit Unterstützung für ZigBee und Bluetooth Low Energy. Zudem hat er nun – wie auch der neue Echo Dot und der neue Echo Dot mit Uhr – ein „sphärisches“ Design, also eher eine Kugelform.

Das Echo Show 10 (mit 10-Zoll-Monitor) kommt wiederum in der dritten Generation mit integriertem Smart Home Hub, der ZigBee und Bluetooth Low Energy (BLE) unterstützt und beispielsweise Routinen erlaubt, um automatisch das Licht einzuschalten, wenn jemand den Raum betritt.

Doch eben letzteres Smart Display hat es in sich: Dank Motor und Verfolgungsfunktion behält es den Nutzer stets im Blickfeld der neuen 13-Megapixel-Weitwinkelkamera. Dabei erkennt das Gerät über eine Analyse der Audiodaten von seinem Mikrofon-Array und der Videodaten von seiner Kamera, aus welcher Richtung die integrierte Sprachassistentin Alexa angesprochen wird.

Der Motor dürfte sich auch dafür nutzen lassen, die Kamera zu drehen, wenn man von einem anderen Echo Show oder über die Alexa-App auf einen (laut Amazon gesicherten) Live-Feed des Echo Show 10 zugreift. Da man über die Alexa-App auch ferngesteuert zoomen kann, soll sich

so der gesamte Raum überblicken lassen. Und auch die Videotelefonie-Funktion will Amazon ausbauen: Kunden sollen bald mit der neuen Funktion „Gruppenanrufe“ eine Gruppe von bis zu acht Freunden und Familienmitgliedern erstellen und die Konferenz mit einem einfachen Befehl wie „Alexa, rufe meine Familie an“ starten können.

Echo Show 10 wird zum Listenpreis von 243,69 Euro in den Farben Anthrazit und Weiß erhältlich sein. Ein Erscheinungsdatum nannte Amazon noch nicht, Interessenten können sich aber über den Vorverkaufsstart benachrichtigen lassen.

### Gesprächsrunde

Amazon gewährte mit einem kleinen Videoclip auch einen Blick in die Zukunft von Alexa: In einem Demo-Video nahm die nach dem Kommando „Alexa, join our conversation“ an einem Ge-



Im Online-Einzelinterview beantwortete der Chef Scientist der Alexa-KI-Abteilung Rohit Prasad (unten) Fragen zur kommenden Entwicklung der Sprachassistentin.

spräch mit zwei Frauen teil, die darüber diskutierten, welche Pizza sie bestellen sollten – und die sich dabei nur ab und zu an die Sprachassistentin wandten, ohne jedoch nochmals das Aktivierungswort zu benutzen. Dennoch erkannte Alexa, wann sie angesprochen wurde und wann nicht.

Gegenüber c't erläuterte der Chief Scientist der Alexa-KI-Abteilung Rohit Prasad, dass dies unter anderem deshalb funktioniert, weil sich an der Satzkonstruktion und der Betonung erkennen lässt, ob sich eine Person an die Sprachassistentin richtet. Zudem würden Menschen unwillkürlich in Richtung des Echo Show schauen, wenn sie Alexa etwas zu sagen hätten. Daher werte das System auch die Blickrichtungen der Gesprächsteilnehmer aus.

Möglich macht dies Amazons neuer „AZ1 Neural Edge Processor“, den der Hersteller im Echo Show 10 nutzt. Er soll im Vergleich zum aktuell verwendeten Chip unter anderem Spracheingaben doppelt so schnell verarbeiten, dabei aber nur auf ein Zwanzigstel des Stromverbrauchs und 15 Prozent des Speicherbedarfs kommen.

Laut Prasad kann Alexa aktuell an Gesprächen mit bis zu drei Personen teilnehmen. Diese Begrenzung hänge vor allem damit zusammen, dass der Geräuschpegel bei größeren Gruppen üblicherweise beachtlich steigt und es (auch für Menschen) schwieriger wird, der Konversation zu folgen, wenn mehr Personen durcheinander reden.

Der AZ1 wird nach aktuellem Stand daher wohl Voraussetzung für den Konversationsmodus sein; ein Firmware-Update, das den Modus bei älteren Echo-Show-Modellen nachrüstet, ist eher nicht zu erwarten. Unklar blieb bis zum Redaktionsschluss, ob der AZ1 auch in der „Kids Edition“ des Echo Dot zum Einsatz kommt. Sie soll erkennen können, ob ein Kind zu ihr spricht und infolgedessen nur passende Inhalte anbieten.

Den Konversationsmodus und die Kids Edition des Echo Dot wird zunächst

nur auf dem US-amerikanischen Markt angeboten. Eine Einschätzung, wie viel Zeit die Lokalisierung für den deutschen Markt beanspruchen wird, gab Amazon nicht.

### Datenschutzoffensive

Bei der Vorstellung des Echo Show 10 wies Amazon ausdrücklich darauf hin, dass die Verarbeitung der Daten für die Verfolgungsfunktion lokal auf dem Gerät stattfinde und der Datenschutz somit gewährleistet sei. Nutzer können die Bewegungsfunktion zudem jederzeit ausschalten, indem sie die integrierte Kamera-Abdeckung schließen, die Einstellungen am Gerät oder in der Alexa-App anpassen oder einfach den Befehl „Alexa, Bewegung ausschalten“ geben.

Amazon kündigte aber auch an, allgemein die Einstellungen zum Datenschutz seiner Sprachassistentin zu erweitern. So sollen Nutzer die Möglichkeit erhalten, einer Speicherung von Sprachaufzeichnungen zu widersprechen. Sprachbefehle an Alexa werden dann direkt nach der Verarbeitung gelöscht, verspricht der Hersteller.

Bei der ersten Aktivierung dieser Option sollen auch alle zuvor gespeicherten Aufnahmen entfernt werden. Amazon behält nach eigenen Angaben lediglich Transkriptionen der vorherigen Anfragen für 30 weitere Tage. Auf Wunsch könnten Nutzer aber auch diese vorzeitig löschen lassen.

Bisher hatten Nutzer von Alexa die Möglichkeit, Sprachaufzeichnungen einzeln oder je



Bild: Amazon Devices

**Das neue Echo Show 10 ist mit einem bürstenlosen Motor ausgestattet, der das 10-Zoll-Display (laut Amazon geräuschlos) dreht.**

nach Gerät zu löschen. Außerdem gab es eine Option, alle Aufnahmen manuell zu löschen oder einen Löschrhythmus von 3 oder 18 Monaten festzulegen. Diese Optionen bleiben laut Amazon erhalten.

Mit dem Konversationsmodus dürfte für Kritiker, die Sprachassistenten wie Alexa sowieso schon gruselig finden und das Gefühl haben, die Sprachassistentin würde ihre Gespräche aufzeichnen und sie überwachen, dennoch eine rote Linie überschritten sein. (nij@ct.de) **ct**

### Das fliegende Auge

Die Amazon-Tochter Ring hat mit der „Always Home Cam“ eine Mini-Drohne vorgestellt, die Innenräume selbstständig überwacht und Videos der eingebauten Kamera an Smartphones sendet. Sie soll so mehrere stationäre Überwachungskameras ersetzen.

Das Prinzip ist recht einfach: Die pilzförmige Drohne mit vier Motoren und rundum geschützten Rotoren sitzt im Wartezustand in einem Dock, das gleichzeitig als Ladestation dient. Nach der Aktivierung, beispielsweise durch einen unterbrochenen Tür-/Fensterkontakt, fliegt die Drohne selbstständig zuvor definierte Punkte im Haus oder in der Wohnung ab und nimmt über ihre Kamera am unteren Ende ein Live-Video auf, das sie an das Smartphone des alarmierten Nutzers streamt.

Geht der Akku zur Neige, kehrt die Drohne automatisch zum Dock zurück; eine Fernbedienung ist offenbar nicht vorgesehen.

Die Drohne, die zunächst in den USA für rund 250 US-Dollar angeboten werden soll, ist aktuell noch nicht von der zuständigen Zulassungsbehörde Federal Communication Commission (FCC) zugelassen. Daher gibt es auch noch kein Erscheinungsdatum. Ob und wann die Always Home Cam nach Deutschland kommt, lässt sich noch nicht sagen.



Bild: Ring

**In der Ladestation ist die Kamera der „Always Home Cam“-Drohne aus Datenschutzgründen verdeckt.**

## MQTT im Schaltschrank



### Eigenes Netzwerk. Eigener Broker.

Mit der MQTT.box einen eigenen MQTT-Broker betreiben.

Alles in eigener Hand:

- Benutzerverwaltung
- Keine externe Cloud
- On-Prem



[wut.de/mqttbox](http://wut.de/mqttbox)

**W&T**  
www.WuT.de

# Künstliche Intelligenz erkennt Gedankenbilder

**Bestimmte Assoziationen von Testpersonen kann ein KI-System deren Hirnströmen zuordnen. Mit fortgesetztem Training erzeugt es dazu immer treffendere Bilder.**

Bislang nutzen Hirnforscher sogenannte Brain-Computer-Interfaces als Eingabesystem. Ihr Vorteil: Der Proband braucht weder Sprache noch Gestik zu verwenden und kann mit etwas Training direkt durch seine Hirnströme einfache Steuerbefehle geben. Allerdings war man bislang der Ansicht, dass sich keine konkreten Gedanken aus den Hirnströmen ablesen lassen.

Nun hat ein Forscherteam an der Universität von Helsinki ein Brain-Computer-Interface eingesetzt, um bei Testpersonen Vorstellungen aus dem Elektroenzephalogramm (EEG) auszulesen und dazu mit Hilfe eines neuronalen Netzes fotorealistische Abbildungen zu erzeugen. Sie nennen ihre Methode neuroadaptive generative Modellierung. Konkret nutzte das Team um Professor Tuukka Ruotsalo die natürliche Reaktion des Gehirns beim Betrachten von Fotos; in diesem Fall ging es um künstlich generierte Personenbilder. Die Forscher baten zuvor ihre Versuchsteilnehmer, an bestimmte Kategorien zu denken: alt oder jung, ein freundliches Lächeln

oder eine ernste Miene, männlich oder weiblich, blond oder brünett.

Die Vorstellungen des Betrachters korrespondieren mit seinen Reaktionen auf die ihm gezeigten Bilder. Mit diesen EEG-Daten trainierten die Wissenschaftler ein neuronales Netz, das aus den Reaktionen auf die gezeigten Bilder ein neues fotorealistisches Porträt generierte. Dessen Übereinstimmung mit ihren Vorstellungen bewerteten die Tester im Schnitt mit 4,6 von 5 Sternen. Ihre Gedan-

kenbilder erkannten sie demnach ziemlich genau wieder. Die Forscher sehen die neuroadaptive generative Modellierung als ein Instrument der psychologischen Forschung. Es muss nicht auf Porträtbilder beschränkt bleiben. Allerdings könnte auch die Erstellung von Phantombildern von dieser Forschung profitieren.

(agr@ct.de)

**Vorstellungen konkretisieren sich, im Video: [ct.de/y981](http://ct.de/y981)**



Bilder: Universität Helsinki

**Mit jeder Reaktion auf ein vom Tester betrachtetes Bild (rechts, klein) kann ein neuronales Netz dessen ursprüngliche Vorstellung immer genauer wiedergeben (Bild links): in dem Fall ein ernstes Gesicht.**

## Panorama mit flacher Linse

Das sogenannte Fischauge als Ultraweitwinkellinse für Panoramafotos kann mit extremer Wölbung Lichtstrahlen aus einem 180-Grad-Winkel zum Bildsensor leiten. Solche Linsen sind voluminös und entsprechend schwer. Am MIT in Cambridge ist es Forschern gelungen, mit einer absolut flachen Metalinse ebenfalls **Bilder in einem**

**Winkel von nahezu 180 Grad** einzufangen, allerdings zunächst im Infrarot-Wellenlängenbereich. Die Aufnahmen erwiesen sich selbst in den Randbereichen als scharf.

Die Metalinse besteht aus einem Wafer-dünnen Calciumfluoridträger, der einseitig mit einer Schicht Bleitellurid bedeckt ist. Diese Schicht trägt lithografisch erzeugte mikroskopisch kleine Strukturen, die Lichtstrahlen auf einen Bildsensor fokussieren. Das einfallende Licht trifft zunächst auf die glatte unbeschichtete Seite des Calciumfluorids, erst nach dem Durchgang durch dieses Trägermaterial erreichen die Lichtstrahlen die optisch aktiven Strukturen. Die Forscher sind zuversichtlich, ihre Entwicklung auch an das optisch sichtbare Lichtspektrum anzupassen und damit medizinische Endoskope und Smartphone-Kameras zu verbessern. (agr@ct.de)

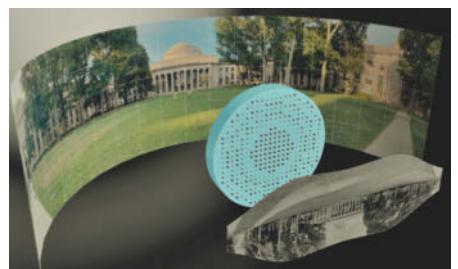


Bild: MIT

**Eine neuartige flache Linse fängt Lichtstrahlen einer 180-Grad-Ansicht ein und leitet sie fokussiert auf den Bildsensor.**

## Warnung vor UV-C-Lampen

Das Bundesamt für Strahlenschutz warnt vor Gefahren bei der Desinfektion mit UV-C-Strahlung. Generell vernichtet ultraviolette Strahlung nicht nur Viren und Keime, sie **schädigt auch Haut und Augen** und gilt als krebserregend. Aktuelle Forschungsergebnisse zeigten, dass kurzwellige Strahlung um 222 Nanometer nicht so tief in den Körper eindringt wie die von einigen Geräten genutzten Wellenlängen um 254 Nanometer. Es ist aber fraglich, ob sich selbst die Strahlung mit kürzerer Wellenlänge gefahrlos in Anwesenheit von Menschen einsetzen lasse. Auf keinen Fall solle man mit dieser Technik den Körper selbst desinfizieren. In der Corona-Pandemie erleben Hersteller von UV-C-Lampen einen regelrechten Hype auch bei Privatanwendern.

(agr@ct.de)

**Video „Selbst am Rand scharf“: [ct.de/y981](http://ct.de/y981)**

# Roboterhand mit Tastsinn

**Neue, elastische Halbleiter weisen den Weg zu einer weichen, dehnbaren Elektronik mit mechanischen Eigenschaften, die man sonst nur von biologischem Gewebe kennt. Die sensorbestückte Roboterhand ist eine der potenziellen Anwendungen.**

Bei Ferndiagnosen könnten medizinische Roboterhände Ärzten helfen, Patienten genauer zu untersuchen. Bisherige Techniken eignen sich dafür aber nur eingeschränkt. Unter anderem sind herkömmliche Halbleiter zu spröde und in elastischen Konstruktionen nur umständlich verwendbar.

Nun beschreibt eine Arbeitsgruppe unter der Leitung von Cunjiang Yu im Fachblatt „Science Advances“ die Konstruktion einer „smarten elektronischen Haut“ und einer „medizinischen Roboterhand“. Die smarte Haut behält ihre elektrischen Eigenschaften selbst dann, wenn sie um 50 Prozent gedehnt wird, betonen die Forscher. Menschliche Haut lässt sich nur um etwa 30 Prozent strecken.

Dehbare Halbleiter sind keine Neuheit. Bisher waren sie aber unter anderem wegen schwacher Ladungsträgermobilität untauglich. Diesem Problem sind Yu und Kollegen bereits 2019 beigekommen. Sie fügten einem elastischen Verbundmate-

rial aus zwei hochkomplexen Polymeren geringe Mengen metallisierter, in PDMS eingelegter Kohlenstoff-Nanotubes hinzu (PDMS = Polydimethylsiloxan, auch als Mittel gegen Kopfläuse oder Gleitbeschichtung bei Kondomen gebräuchlich).

Laut dem Artikel lässt sich der dünne Verbundwerkstoff leicht in großen Mengen produzieren: Ein kommerziell erhältliches wasserabweisendes Halbleitermaterial wird in einer Lösung aufgenommen und

auf eine Wasserfläche ausgegossen. Anschließend verdunstet das Lösungsmittel. Übrig bleibt der ultradünne Halbleiterfilm.

In einer Testschaltung zeigte der Film gute Voraussetzungen für den Einsatz als Tastsensor. Der Widerstand des Materials nahm je nach physischem Druck von rund 200 Megaohm auf nur etwa 8 Ohm ab. Diese smarte Sensorhaut sei auch „hervorragend biegsam und dehnbar“.

(dz@ct.de)

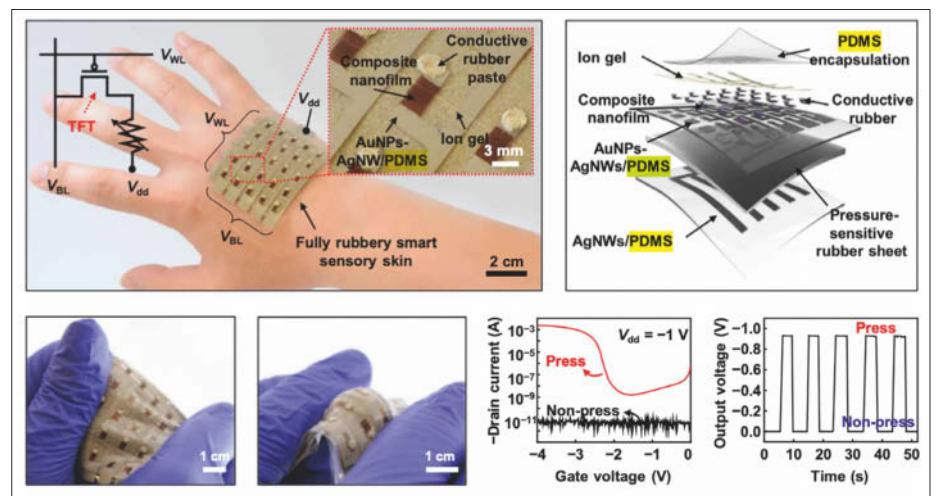


Bild: Universität Houston

**Forscher der Universitäten von Houston und Colorado haben dehbare Transistoren und ein elastisches Verbundmaterial zu einer druckempfindlichen „smartten Haut“ zusammengesetzt.**

## Sensor für den Weltraum

Graphen gilt unter anderem wegen seiner hohen Elektronenbeweglichkeit als attraktives Material für elektronische Bauelemente. Doch unter rauen Bedingungen ließ es sich bisher kaum einsetzen. Die britische Firma Paragraf hat nun einen **Hall-Effekt-Sensor zur Magnetfeldmessung** entwickelt, der sehr gute Eigenschaften für den angepeilten Einsatz in der Raumstation ISS aufweist. In Tests des Analyseinstituts NPL funktionierte der Sensor auch nach einer

Exposition mit einer Neutronendosis von 241 Millisievert pro Stunde. Wie lange der Sensor bombardiert wurde, gibt NPL nicht an. Die Belastung entspreche aber etwa dem 30.000-fachen des in der ISS erwarteten. „Dies ist das erste Mal, dass sich ein kommerziell erhältliches elektronisches Gerät auf Graphenbasis als unempfindlich gegenüber Neutronenstrahlung erwiesen hat“, meldet Paragraf. Silizium-Hallsensoren müsste man deutlich aufwendiger kap-

seln, damit sie unter solchen Bedingungen funktionieren. Der getestete graphenbasierte Sensor wiegt nur 0,8 Gramm.

Bemerkenswert erscheint, dass die Verlustleistung nur im Picowattbereich liegt und der Leistungsbedarf um drei Größenordnungen unter dem von sonst üblichen Sensoren. (dz@ct.de)

## Multisensor-Kit

STWIN SensorTile ist ein von STMicroelectronics konzipiertes Entwicklungskit zur **Zustandsüberwachung in industriellen Anwendungen**. ST hat der drahtlosen Station unter anderem einen Mikrocontroller auf ARM-Cortex-Basis, einen MicroSD-Slot, einen Lithium-Polymer-Akku mit 480 mAh und eine Reihe von Sensoren spendiert. Unter anderem eignen sie sich zur Schwingungsanalyse hochfrequenter Audiospektren bis in den Ultraschallbereich sowie zur Messung von Umgebungstemperatur, Beschleunigung und Luftfeuchte.

An Bord sind Bluetooth und Bluetooth Low Energy sowie ein Anschluss für das optionale WLAN-Modul STEVAL-STWINWVF1. Über einen RS485-Transceiver lässt sich das Kit auch per Kabel ansprechen. Das STWIN SensorTile ist bei Mouser erhältlich. (dz@ct.de)



**Graphenbasierte Sensoren waren für rauhe Umgebungen bisher ungeeignet. Der nebenstehende Magnetfeldsensor hält harter Neutronenstrahlung stand.**

Bild: Paragraf

# Bit-Rauschen

## GeForce-RTX-3080-Probleme, IBM A2O und China-Querelen

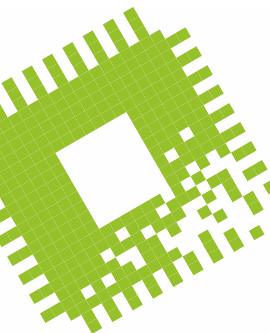
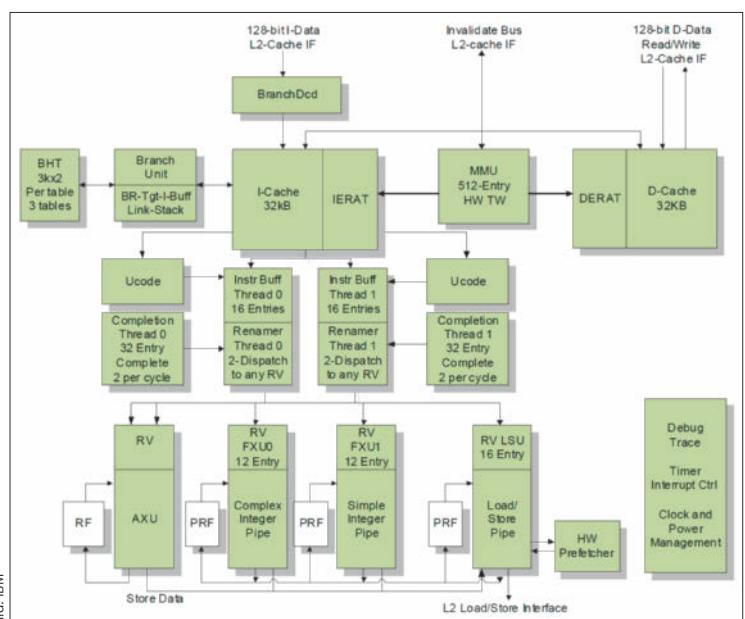
**Bei der Markteinführung von Nvidias GeForce-3000-Grafikkarten läuft einiges schief. IBM bringt einen PowerPC-Kern mit verwirrendem Namen und US-Sanktionen gegen China könnten beliebte Produkte verknappen.**

Von Christof Windeck

Ein Kollege fragte witzelnd, ob Nvidia die kapitalistische Marktwirtschaft nicht ganz verstanden habe: Um ihren Profit zu maximieren, wecken Hersteller ja üblicherweise Bedürfnisse, die sie dann mit manchmal überflüssigen Produkten befriedigen. In diesem Sinne ging der Start der neuen „Ampere“-Grafikkarten GeForce RTX 3080 gründlich schief: Das erweckte Verlangen war groß, doch die immerhin 800 Euro teuren Karten waren nach der Vorstellung sofort ausverkauft. Nicht nur

das sorgte für Verdruss: Einige der Grafikkarten liefen nicht stabil – siehe Seite 44. Die später vorgestellten und noch teureren RTX-3090-Karten waren ebenfalls beim Start kaum erhältlich. Da kann man nur hoffen, dass es bei der RTX 3070 am 15. Oktober besser klappt. Die Instabilitäten der RTX 3080 gehen anscheinend auf simple Kondensatoren zurück; überraschend oft stolpern hyperkomplexe Halbleiter mit Abermilliarden Transistoren über althergebrachte analoge Schaltungstechnik.

Intel brachte Ende September endlich die „Elkhart Lake“-Prozessoren mit „Tremont“-Kernen als Atom x6000E heraus. Interessanterweise bestehen sie aus je zwei Chips in einem gemeinsamen Gehäuse, wobei vermutlich nur der CPU- und GPU-Teil aus der 10-Nanometer-Fertigung stammt. Der zweite Chip dürfte noch 14-Nanometer-Transistoren enthalten, welche die wesentlich verbesserten I/O-Funktionen bereitstellen – siehe Seite 43. Zur sparsamen (Echtzeit-)Verarbeitung von Sensordaten baut Intel zudem einen ARM-Kern ein, nämlich einen Cortex-M7.



Wirklich neu ist die ARM-x86-Kombination aber nicht, denn in sämtlichen AMD-Prozessoren steckt seit Jahren ein Cortex-A5 als Basis des AMD Secure Processor unter anderem für TPM-Funktionen.

### IBM A2O

Ein unaufmerksamer Blick auf die Typenbezeichnung IBM A2O erinnert ältere Semester an Intels legendär vermurkstes A2O-Gate. IBM schreibt A2O aber nicht mit einer Null, sondern mit einem „O“ für Out-of-Order-Verarbeitung – zur Unterscheidung vom In-Order-Kern A2I. IBM hat diese PowerPC-Kerne nach PowerISA 2.06 unter dem Dach der OpenPower-Foundation offen gelegt, sie sind zur Integration in andere Chips gedacht. Allerdings räumen die Entwickler des A2O freimütig ein, dass er noch einige Bugs enthält.

Somit wirkt der anlässlich des OpenPower Summit 2020 vorgestellte A2O wie ein etwas müder Versuch, die OpenPower-Idee am Leben zu erhalten. Sie steht einerseits unter Druck der deutlich lebendigeren RISC-V-Szene, andererseits hat sich der bisher wichtige OpenPower-Partner Nvidia soeben ARM einverleibt.

### Handelskrieg und NOR-Flash

Die US-Regierung unter Nächter Präsident Trump verstärkt den Druck auf die chinesische Halbleiterbranche und hat schärfere Regeln für den Export von Anlagen und Vorprodukten an den wichtigsten chinesischen Auftragsfertiger SMIC beschlossen. SMIC ist bisher die einzige „Fab“ in der Volksrepublik China, die Chips mit 14-Nanometer-Technik produzieren kann, und beliefert damit etwa auch Huawei.

Die Sanktionen gegen SMIC könnten bald auch zu Lieferengpässen bei Smartphones, Smart-Home-Geräten und den derzeit äußerst beliebten Bluetooth-Kopfhörern mit Geräuschunterdrückung führen. Derlei Gerätschaften brauchen nämlich Firmware, die oft in einem winzigen NOR-Flash-Chip steckt. Bei diesen Flash-Chips wiederum hat die chinesische Firma Gigadevice erhebliche Marktanteile ergattert – aber die Fertigung erfolgt bei SMIC. Falls Gigadevice nicht mehr genug NOR-Flashes auf den Markt bringen kann, so reißt das Lücken, die Konkurrenten wie Adesto, Macronix und Winbond vermutlich nicht kurzfristig stopfen können.

(ciw@ct.de)

# Intel Atom x6000E für Autos, IoT, NAS

**Der erste 10-Nanometer-Atom für Embedded Systems bringt höhere Performance sowie neue Funktionen für Echtzeitsteuerung und funktionale Sicherheit.**

Nach langer Verzögerung bringt Intel die mit 10-Nanometer-Strukturen gefertigte Baureihe Atom x6000E mit zwei oder vier „Tremont“-Rechenkernen auf den Markt. Letztere takten höher als die „Goldmont“-Kerne ihrer 2016 eingeführten Vorgänger Atom x-3900E alias Apollo Lake, sollen aber auch bei gleichem Takt deutlich mehr Rechenleistung liefern. Die x6000E-Neulinge tragen den Codenamen Elkhart Lake. Zur gleichen Familie gehören auch billigere Celeron- und Pentium-Typen, denen einige Funktionen fehlen, etwa ECC-Speicherschutz sowie Optimierungen für Echtzeitberechnungen und funktionale Sicherheit. Letztere sind beispielsweise für die Steuerungssysteme in Fahrzeugen (Automotive) wichtig und stecken in den „FE“-Versionen Atom x6200FE und x6427FE. Echtzeitfunktionen wie Time Coordinated Computing (TCC) besitzen auch die „RE“-Typen Atom x6212RE, x6414RE und x6425RE. Die FE- und RE-Typen haben keine Turbo-Funktion, weil ständige Wechsel der Taktfrequenz zu schwankenden Latenzen bei der Verarbeitung von Echtzeit-Steuerungsaufgaben führen.

Elkhart-Lake-Prozessoren bringen noch weitere Verbesserungen, darunter PCI Express 3.0 (statt 2.0), mehrere integrierte Ethernet-Controller auch für 2.5GBase-T sowie einen sparsamen ARM-Cortex-M7-Rechenkern. Der kann einfache Aufgaben erledigen, während die x86-Kerne schlafen.

Den Error Correction Code (ECC) als Schutz gegen RAM-Bitfehler legen die neuen Atoms nicht in separaten Chips ab, sondern nutzen dafür einen Teil der vorhandenen RAM-Kapazität. Dieser „In-Band-ECC“ ist für die Ansteuerung von LPDDR4(X)-SDRAM wichtig, weil es nicht mit der für ECC üblichen x4- und x8-Organisation verfügbar ist, sondern nur mit je 16 oder 32 Datenleitungen pro

Chip (x16/x32). Die Atom x6000E steuern alternativ aber auch zwei DDR4-SODIMMs an mit insgesamt bis zu 32 GByte.

Die Celeron-Versionen N6211 (2 Kerne/6,5 Watt), J6413 (4 Kerne/10 Watt) und die Pentiums J6415/J6425 sind als pinkompatible Alternativen für billigere Geräte gedacht. Es werden noch eng verwandte „Jasper Lake“-Prozessoren als Pentium Silver N6000 und Celeron N6000 erwartet, die in Billig-Notebooks, Chromebooks und NAS zum Einsatz kommen.

Die Hersteller Advantech, Congatec, Kontron, TQ Group und Vecow bieten bereits Produkte mit Atom x6000E an. Intel hat auch Embedded-Versionen der Tiger-Lake-Mobilprozessoren angekündigt, etwa Core i5-1145GRE. (ciw@ct.de)



Bild: TQ Group

**TQ Systems setzt den Intel Atom x6000E auf dem SMARC-2.1-Modul TQMxE40S mit bis zu 16 GByte LPDDR4X-Speicher ein.**

**Digitale Verwaltung**

# Rheinland-Pfalz 2020

Vernetzte Evolution zum Wohle von Bürger/-innen, Wirtschaft und Verwaltung

**24. November 2020, Mainz**

[www.dv-rlp.de](http://www.dv-rlp.de) #dvrlp20

## **Statt Ti und Titan: RTX 3090**

**Nvidias High-End-Grafikkarte GeForce RTX 3090 soll mit 24 GByte Grafikspeicher nicht nur Spieler, sondern auch Kreative und KI-Forscher verzücken. Allerdings kostet sie auch stolze 1500 Euro.**

Um die Titan- und Ti-Modelle der Vorgängergeneration abzulösen, betrieb Nvidia für die RTX 3090 einigen Aufwand. Wie bei der RTX 3080 kommt ein Grafikchip mit aktueller Ampere-Architektur zum Einsatz. Im Vergleich zum Vorgänger Turing hat er neue, flexiblere Tensorkerne für KI-Berechnungen und Raytracing-Kerne, die Schnittpunktberechnungen doppelt so schnell ausführen. Vor allem aber hat Nvidia in die Shader-Multiprozessoren viele zusätzliche Einheiten für Standard-Shader-Berechnungen mit 32

**Gigantisch große RTX 3090: Drei Slots belegt der Kühler der 31,3 Zentimeter langen Founders Edition.**



Bit Gleitkommagenaugkeit eingebaut. Im Grafikchip der RTX 3090 sind nun 10.496 FP32-Shader-ALUs vorhanden, mehr als doppelt so viele wie bei der 1200 Euro teureren Titan RTX. Insgesamt kommt die Karte so auf 36 Billionen Rechenschritte pro Sekunde (FP32-TFlops).

Der mit 24 GByte äußerst üppige Speicher überträgt nun bis zu 936 GByte/s. Spieler können diese Speichermenge selbst mit 8K-Bildschirmen kaum ausreizen, Kreative und KI-Forscher profitieren aber von mehr Freiraum für komplexere 3D-Modelle oder neuronale Netze als noch mit der GeForce RTX 2080 Ti. KI-Vorteile hat die RTX 3090 gegenüber der Titan RTX hauptsächlich durch die neuen Datentypen BF16 und TF32 – bei herkömmlichem KI-Training arbeiten ihre Tensorkerne mit lediglich spärlich besetzten, komprimierbaren neuronalen Netzen deutlich schneller.



Die RTX 3090 hat laut Nvidia eine Leistungsaufnahme von bis zu 350 Watt – keine 10 Prozent mehr als die RTX 3080, sodass sie am Power Limit auch nur um diesen Betrag schneller arbeitet. Als bislang einzige RTX 3000 unterstützt die PCIe-4.0-kompatible RTX 3090 auch die Kopplung via NVLink inklusive der Zusammenlegung der beiden 24-GByte-Speicherpools. (csp@ct.de)

# Business-Rechner mit AMD Ryzen Pro 4000G

Die Kombiprozessoren der Serie Ryzen Pro 4000G vereinen hohe Rechenleistung mit integrierter Grafik und eignen sich deshalb für den Einsatz in Firmen-PCs. Der deutsche Hersteller Exone bietet unter der Bezeichnung **Business S 1301** drei Rechner im Tower-Format mit dem Quad-Core Ryzen 3 Pro 4350G, dem Hexa-Core Ryzen 5 Pro 4650G und dem Octa-Core Ryzen 7 Pro 4750G an. Die günstigen Varianten eignen sich für Textverarbeitung, E-Mail sowie einfache Bild- und Videobearbeitung. Die leistungsfähigeren Prozessoren mit mehr Kernen taugen auch für anspruchsvollere Aufgaben wie das Komprimieren von Code und Finanzanwendungen.

mit größeren Datensätzen. Laut Hersteller liegt die Geräuschentwicklung der Business-PCs bei ungefähr 22 dB(A).

Zur Ausstattung zählen bei den beiden günstigeren Modellen je 8 GByte Arbeitsspeicher, eine SSD mit 250 GByte Kapazität sowie 2 Jahre Garantie. Der leistungsstärksten Variante mit dem Achtkerner spendiert Exone 16 GByte RAM, eine 500-GByte-SSD mit PCI-Express-Anbindung und 3 Jahre Garantie. Per HDMI 2.1 und DisplayPort 1.4 können die Rechner jeweils zwei 4K-Displays mit 60 Hertz ansteuern. Die Office-PCs der Serie Business S 1301 kosten inklusive Windows 10 Pro zwischen 530 und 810 Euro. (chh@ct.de)

## Kurz & knapp

Sowohl Nvidias **GeForce RTX 3080** als auch die **RTX 3090** sind trotz hoher Preise seit ihrem Marktstart am 17. (RTX 3080) und 24. September (RTX 3090) so gut wie nicht zu bekommen. Nachlieferungen an die Händler waren in den ersten Wochen direkt wieder vergriffen.

Mit dem Launch-Treiber plagten **GeForce-RTX-3000-Grafikkarten Stabilitätsprobleme**. Nvidia hat zwischenzeitlich den GeForce 456.55 WHQL herausgebracht, der das Problem mit leichtem Undervolting in den Griff bekommt.

SanDisk frischt die Schnittstellen seiner **USB-SSDs Extreme Portable und Extreme Pro Portable** auf: Die Extreme Portable beschleunigt von 550 MByte/s auf 1 GByte/s, die Pro-Version sogar auf 2 GByte/s. Die SSDs sind mit Kapazitäten zwischen 500 GByte und 2 TByte erhältlich.

Das **PC-Gehäuse Lian Li Lancool 215** ist in der Front mit zwei 20-cm-Lüftern ausgerüstet, die darüber hinaus mit adressierbaren RGB-LEDs versehen sind. Der Midi-Tower mit Glasseitenwand und Platz für E-ATX-Mainboards ist ab Ende Oktober für 70 Euro erhältlich.



Den Office-Rechner Exone Business S 1301 gibt es unter anderem mit dem effizienten Achtkernner Ryzen 7 Pro 4750G zu kaufen

# Erpressungstrojaner kostenlos entschlüsseln

**Verschlüsselungstrojaner spülen Kriminellen nach wie vor viel Geld in die Taschen. Mit den richtigen Tools spart man sich die Zahlung.**

Zum Glück stoßen Sicherheitsforscher immer wieder auf Fehler im Ransomware-Code und bieten kostenlose Entschlüsselungstools an. So zuletzt geschehen beim Windows-Schädling ThunderX. Das Tool kann Schlüssel ableiten und damit Dateien aus den Fängen von ThunderX befreien.

Wer von einer Ransomware betroffen ist, aber nicht weiß, welche es ist und ob es ein kostenloses Entschlüsselungstool gibt, sollte die Website von ID Ransomware (siehe [ct.de/yn6u](http://ct.de/yn6u)) aufrufen. Dabei handelt es sich um ein freies Projekt von verschiedenen Sicherheitsforschern. Alternativ kann man sich in der Datenbank von No More Ransom! (siehe [ct.de/yn6u](http://ct.de/yn6u)) umschauen. Dort findet man Tools inklusive Kurzanleitungen. Bei dem Projekt handelt es sich um eine Zusammenarbeit von unter anderem Kaspersky, Europol und McAfee.

(des@ct.de)

**Trojaner-Datenbanken:** [ct.de/yn6u](http://ct.de/yn6u)



**Die Website ID Ransomware zeigt an, ob es bereits kostenlose Entschlüsselungstools für mehr als 900 Erpressungstrojaner wie AgeLocker oder Ryuk gibt.**

## Attacken auf kritische Lücke in Windows Server

Derzeit haben es Angreifer aktiv auf die Zerlogon getaufte Sicherheitslücke mit Höchstwertung (CVSS Score 10 von 10) in den Windows-Server-Versionen 2008 R2, 2012, 2012 R2, 2016, 2019, 1903, 1909 und 2004 abgesehen. Microsoft rät Admins dringend dazu, ihre Server auf den aktuellen Stand zu bringen und damit abzusichern. Auch Sicherheitsforscher von Cisco Talos haben einen Anstieg von Attacken verzeichnet. Auf einer Website (siehe [ct.de/yn6u](http://ct.de/yn6u)) erläutert Microsoft, wie Admins vorgehen sollten.

Aufgrund von Fehlern beim Einsatz der AES-CFB8-Verschlüsselung beim Netlogon-Prozess könnten entfernte Angreifer ohne Authentifizierung ganze Domänen als Admin übernehmen.

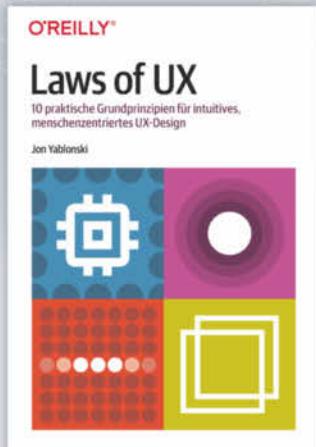
Auch **Samba** ist für Zerlogon anfällig, wenn die Server-Software als Domänencontroller (Active Directory DC, /NT4-style DC) zum Einsatz kommt. Ist das der Fall, sollten Admins sicherstellen, dass mindestens die Version 4.8 vom März 2018 installiert sind. Diese setzt den Samba-Entwicklern zufolge standardmäßig auf einen abgesicherten Netlogon-Prozess.

(des@ct.de)

**Zerlogon Advisory:** [ct.de/yn6u](http://ct.de/yn6u)



**3. Auflage**  
2020, 870 Seiten  
€ 36,90 (D)  
ISBN 978-3-86490-779-1



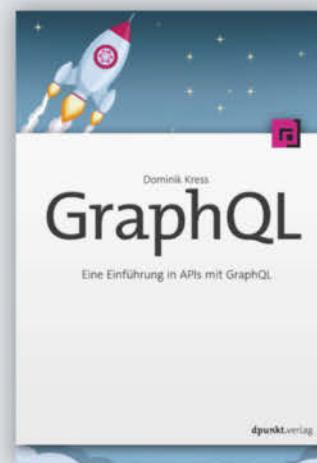
**2020, 140 Seiten**  
€ 24,90 (D)  
ISBN 978-3-96009-156-1  
(O'Reilly)



**2020, 248 Seiten**  
€ 29,90 (D)  
ISBN 978-3-86490-715-9



**2020, 552 Seiten**  
€ 39,90 (D)  
ISBN 978-3-96009-129-5  
(O'Reilly)



**2020, 202 Seiten**  
€ 29,90 (D)  
ISBN 978-3-86490-784-5

**plus+**  
Buch + E-Book:  
[www.dpunkt.plus](http://www.dpunkt.plus)

**dpunkt.verlag**

Wieblinger Weg 17 · D-69123 Heidelberg · fon: 0 62 21 / 14 83 40  
fax: 0 62 21 / 14 83 99 · e-mail: [bestellung@dpunkt.de](mailto:bestellung@dpunkt.de)

**O'REILLY®**

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

# AVM kontra Fritzblock

**Fritz ist ein Vorname – und Teil von Produktbezeichnungen, unter anderem der wohlbekannten FRITZ!Box. Deren Rechteinhaber drängte nun einen Software-Entwickler, sein Tool umzubenennen.**

Um sich lästige Werbeanrufe vom Ohr zu halten, können Fritzboxen unerwünschte Anrufe automatisch abweisen. Dazu muss man die Rufnummern einmal in eine Sperrliste eintragen. Das Windows-Programm SpamBlockUp automatisiert den Prozess, indem es bei eingehenden Anrufen Webdienste nach der angezeigten Nummer fragt, das Ergebnis per Pop-up präsentiert und sie bei hohem „Spam

Score“ auf Wunsch sogar automatisch auf die Sperrliste setzt.

Das Tool hieß bis vor Kurzem noch Fritzblock, was anscheinend AVM nicht gefiel: Laut dem Entwickler Volker Ulle wurde er gedrängt ([ct.de/yebm](http://ct.de/yebm)), sein Programm umzubenennen, womöglich weil AVM befürchtet, es könne wegen seines Namens für ein Produkt des Fritzbox-Herstellers gehalten werden.

Das Berliner Unternehmen hat das gegenüber c't bestätigt. Um das Tool an sich ginge es nicht, aber man halte die Namensähnlichkeit zu eigenen Produkten für zu hoch. Deswegen sei man informell – also ohne Einschalten eines Anwalts – vorgegangen. Die Befürchtung: Fritzblock-Nutzer könnten sich beim AVM-Support melden, wenn das Programm nicht wie erwartet funktioniert, obwohl der gar nicht dafür zuständig sei.

Generell freue man sich selbstverständlich über externe Entwicklungen, die das Fritzbox-Universum bereichern: „Aktivitäten im Bereich Open Source sehen wir bei AVM generell sehr positiv und als wichtig für den IT-Markt insgesamt. Aus diesem Grund bieten wir unter [avm.de/schnittstellen](http://avm.de/schnittstellen) auch entsprechende Schnittstellen an.“ Nur zu Fritz-ähnlich darf der Name des entstehenden Programms oder der App dann wohl nicht werden. (ea@ct.de)

**Fritzbox-Tool SpamBlockUp:** [ct.de/yebm](http://ct.de/yebm)



**Stein des Anstoßes: Das Windows-Tool SpamBlockUp hilft Fritzboxen, unerwünschte Anrufe automatisch abzuwehren. Fritzblock darf es nach dem Willen von AVM nicht mehr heißen.**

## Netzwerktester mit Touchdisplay

Die Netzwerktesterserie „Argus“ von Intec hat erstmalig Nachwuchs mit **Touchscreen** bekommen: Der Argus 260 ist ein **Kombitester** für lokale Netze und Teilnehmeranschlusstechniken, der sowohl über die Tastatur als auch über den Touch-

screen mit 800 × 480 Pixeln Auflösung bedient werden kann. In lokalen Netzen testet das Messgerät **Kupfer-Ethernet bis 1 GBit/s** und liefert umfangreiche Informationen wie Fehlerrate, eventuelle Aderverpolungen und die Leitungslänge. Über Erweiterungen ist außerdem Ethernet bis 2500 MBit/s (2.5GBase-T) möglich.

Der Argus 260 beherrscht weiter alle auf der Telefonleitung üblichen Anschluss-techniken: Die veraltete ADSL-Technik sowie **VDSL bis Super-Vectoring** (Profil 35b), optional auch mit Bonding und G.fast-Analyse (Profile 106 und 212 MHz). GPON- und AON-Glasfaserverbindungen können über ein passendes SFP-Modul geprüft werden. Der Argus 260 kostet ohne Erweiterungen 4630 Euro. (amo@ct.de)



Bild: Intec

**Der Argus 260** hat als erster der Argus-Reihe einen Touchscreen. Er kann Ethernet-, xDSL- und Glasfaserverbindungen prüfen.

## Kurz & knapp: Netze

Das **Mesh-WLAN-Kit Linksys Velop wird zu Apple HomeKit kompatibel**. Laut Belkin kann man mit der Home-App für Apple-Geräte in Kürze über das Mesh-Kit den Zugriff auf HomeKit-fähige Geräte verwalten und festlegen, welche Informationen die Geräte untereinander und über das Internet austauschen dürfen.

Zyxel rundet sein **Wi-Fi-6-Portfolio** mit zwei neuen **Access-Points** ab: Die Modelle WAX610D und NWA210AX funken in beiden WLAN-Bändern gemäß IEEE 802.11ax (Wi-Fi 6) über 2 beziehungsweise 4 Antennen und erreichen so 574 und 2400 MBit/s Bruttodatenrate. Der NWA210AX lässt sich autonom betreiben oder per Nebula-Cloud steuern, der WAX610D zusätzlich per WLAN-Controller.

Der neue **5G-Mobilfunk** wird gerade erst in die Fläche gebracht, doch die Industrie denkt schon an die nächste Technik-generation: Am 20. und 21. Oktober wollen das US-Unternehmen InterDigital und das Institut für „Wireless Internet of Things“ der Northeastern University (Boston, USA) ihr erstes **6G-Symposium** als virtuelle Konferenz abhalten, also online. Es soll die Vision für 6G-Mobilfunk schärfen und klären, welche strategischen, technischen und regulatorischen Hürden zu nehmen sind.

**Netool** bietet für sein gleichnamiges **Netzwerkanalysewerkzeug** (Test in c't 20/2020, S. 88) eine aufgefrischte Firmware an: Die Version 96 zeigt unter anderem mehr Informationen zu den Inventarisierungsprotokollen (LLDP, CDP & Co.) sowie zu Spanning Tree an (Redundanzprotokoll). Außerdem will man Fehler behoben und die Geschwindigkeit des Systems gesteigert haben.

**Schneider Electric** hat eine neue Serie von **Stromverteilungsleisten für 19-Zoll-Gestelle** vorgestellt: Die Easy-PDUs bieten wahlweise Schuko- oder Kaltgerätesteckern Anschluss. Die Leisten sind als einfache Verteiler (Basic), schaltbar (switched) oder mit netzwerk-fähiger Messfunktion (metered) erhältlich.



**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 35 % 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.**



# Speicher für Unternehmen

**Seagate und Western Digital bringen neue Festplatten für Serverracks und NAS-Systeme, Seagate stellt zudem einen neuen Open-Source-Ansatz zur Verwaltung großer Datenmengen vor.**

Western Digital erweitert die Videoplattenreihe Purple und die Oberklasse-NAS-Reihe Red Pro um Modelle mit je 18 TByte Speicherplatz; die Red Pro gibt es zudem nun auch mit 16 TByte. Bei den Red-Pro-Modellen setzt Western Digital auf Schreibköpfe mit zusätzlicher Energieeinspeisung (Energy-enhanced Perpendicular Magnetic Recording, ePMR, siehe c't 17/2020, S. 72). Die Laufwerke drehen mit 7200 Umdrehungen pro Minute, haben 512 MByte DRAM-Cache und übertragen maximal 259 beziehungsweise 272 MByte/s. Sie sollen im Oktober in den Handel kommen.

Details der 18-TByte-Purple-Festplatte hat das Unternehmen noch nicht veröffentlicht. Zur Purple-Serie gehören bei

Western Digital auch MicroSD-Karten, die speziell für die Videoaufzeichnung optimiert sind; diese sind nun mit einer Kapazität von 1 TByte erhältlich.

Seagate setzt die Technik der 18-TByte-Platte Ironwolf Pro (siehe S. 84) nun auch in der Server-Reihe Exos ein. Sie ist auch mit SAS-Anschluss erhältlich. Für Dezember stellt Seagate eine erste Festplatte mit Heat Assisted Magnetic Recording (HAMR) in Aussicht. Die 20-TByte-Festplatte wird ebenfalls in der Exos-Reihe erscheinen.

Weiterhin startet Seagate das Projekt Cortx, eine Objektspeichersoftware zur Verwaltung sehr großer Datenmengen. Cortx steht unter der Apache-2.0-Lizenz, Interessenten können sich an der Entwicklung beteiligen. Details dazu finden sich auf Github (siehe [ct.de/yf3b](https://ct.de/yf3b)). Ebenfalls im Dezember will Seagate Lyve Drive Racks mit einer Speicherkapazität ab 1,34 PByte liefern, die Cortx-Technik sowie HAMR-Festplatten nutzen. (ll@ct.de)



Bild: Western Digital

**Die NAS-Festplatten aus der Red-Pro-Reihe gibt es nun auch mit 16 und 18 TByte Speicherplatz.**

Programmcode zu Cortx: [ct.de/yf3b](https://ct.de/yf3b)

# ARM-Kern mit SVE für Server

ARM hat den **neuen Rechenkern Neoverse V1** für Server vorgestellt, der bisher schon unter dem Codenamen „Zeus“ angekündigt war. Nun erst wurde aber klar, dass Zeus auch die Scalable Vector Extension (SVE) zur schnellen Verarbeitung von Vektordaten bekommt, und zwar zwei Einheiten für je 256 Bit breite Datenwerte ( $2 \times 256$  SVE). Zudem hält das effiziente Datenformat BFloat16 (BF16) Einzug in Neoverse V1, was besonders KI-Algorithmen auf Trab bringen kann. Außerdem können die SVE-Einheiten 8-Bit-Ganzzahlen schnell multiplizieren (8-Bit Integer Matrix Multiplication, I8MM).

Zu den ersten Lizenznehmern für Neoverse V1 gehört die European Pro-

cessor Initiative (EPI) beziehungsweise die EPI-Firma SiPearl. Der für 2022 geplante Entwicklungsprozessor Rhea soll 72 Neoverse-V1-Kerne enthalten. Diese Kerne sind auch mit dem Cortex-A78 und dem leistungsstärkeren Cortex-X1 verwandt.

ARM kündigte zudem als Nachfolger des bereits unter anderem im Amazon Graviton2 eingesetzten Neoverse N1 („Ares“) den Neoverse N2 „Perseus“ für später kommende Serverprozessoren mit bis zu 192 Kernen an. Derartige Chips werden dann auch mit PCI Express 5.0, der kohärenten Schnittstelle Compute Express Link (CXL) und Controllern für DDR5-SDRAM bestückt sein. (ciw@ct.de)

# ARM-Server in der Oracle-Cloud

Oracle will Anfang 2021 in seinen Cloud-Rechenzentren **Server mit neuen Prozessoren** von AMD (Milan, Zen 3), Intel (Ice Lake) und Ampere (Altra mit ARM-Kernen) bereitstellen. Außerdem lassen sich ab sofort Bare-Metal-Instanzen mit Nvidias A100-Rechenbeschleunigern buchen.

Auch Amazon AWS (Graviton2) und einige kleinere Cloud-Dienstleister wie Packet (Ampere eMag) und Verne Global (Marvell ThunderX2) vermieten ARM-Server. In Microsoft Azure kommen sie nur hinter den Kulissen zum Einsatz. Oracles Altra-Maschinen mit bis zu 160 ARM-Kernen sollen besonders kostengünstige Instanzen ermöglichen. Die kommenden E4-Instanzen auf AMD Milan wiederum sollen höhere Performance und eine besonders flexible Konfiguration bringen, beispielsweise viel RAM schon bei wenigen CPU-Kernen. Intels Ice-Lake-Xeons will Oracle hingegen vor allem in Instanzen für rechenintensive Anwendungen einsetzen (High Performance Computing, HPC). Dabei sollen sich mehrere Maschinen zu Clustern mit Remote DMA (RDMA) zusammenschalten. (ciw@ct.de)



# Amazon Luna: Der nächste Dienst fürs Cloud-Gaming

**Amazon steigt mit einem eigenen Dienst in den Markt für Cloud-Gaming ein. Luna soll von der Infrastruktur des Konzerns profitieren.**

Nutzer in den USA können bereits für 6 US-Dollar im Monat eine Reihe von Spielen direkt aus Amazons AWS-Rechenzentren streamen. Luna soll auf PC und Mac, Fire-TV-Geräten sowie im Safari-Browser und damit auf iPhones und iPads funktionieren.



Android-Support soll folgen. Amazon verspricht eine enge Anbindung an den Streamingdienst Twitch und einen speziellen Bluetooth-Controller.

Amazon stellt neben dem eigenen Angebot Luna+ mit dem Dienst vor allem die Infrastruktur bereit, weitere Inhalte sollen aus Kanälen der Spielestudios kommen. Zur Einführung gibt es so einen Kanal lediglich von Ubisoft. Für einen bislang nicht genannten Abopreis lassen sich darin unter anderem Assassins Creed Valhalla, Far Cry 6 und Immortals Fenyx Rising zum Starttermin aus der Cloud spielen. Die Kanalanbieter können Modalitäten anpassen: Der Ubisoft-Kanal erlaubt nur jeweils ein aktives Gerät. Luna+, für den Amazon selbst Inhalte lizenziert, erlaubt zwei gleichzeitig aktive Geräte pro Profil. In Luna+ soll es zum Start unter anderem Resident Evil 7, Control, The Surge 2, GRID und ABZU geben. (mho@heise.de)

## Kurz & knapp: Spiele

Das Weltraumbabenteuer **Empyrian – Galactic Survival** verlässt nach fünf Jahren die Early-Access-Phase. In diesem Open-World-Survival-Spiel erkundet man den Weltraum und seine Planeten, kämpft in unwirtlicher Umgebung ums Überleben und wehrt feindliche Aliens ab.

Die Umweltsimulation **Eco** hat ein großes Update erhalten: Version 9.0 bringt Neues bei Regierungen, bei der Zusammenarbeit in Projekten, neue Tiere, ein In-Game-Wiki, ein neues Biom und eine Überarbeitung der Bedienoberfläche.

Zum zehnjährigen Jubiläum hat Frictional Games sein First-Person-Horrorspiel **Amnesia: The Dark Descent** als Open Source unter der GPL v3 veröffentlicht. Das erleichtert Moddern die Anpassung und Erweiterung des Spiels.



Lesen Sie auch den Test in der  
c't 19/2020 ab Seite 114!

## M215 SC

Auch im Kleinsten ganz GROSS

Bei Snom wird auch auf die Details der Kleinen geachtet – so hat unser Einstiegsmodell M215 kürzlich ein sehr bekanntes Computermagazin beeindruckt.

Lernen Sie uns und unsere hochklassige Produktpalette kennen

**SNOM**

Melden Sie sich noch heute in unserem Partner-Portal als Reseller an und erhalten Sie ein kostenfreies Snom Telefon zum kennenlernen.

# App-Anbieter und Verlage gegen App Store

**Die Lage spitzt sich für den weltgrößten IT-Konzern: Nachdem der Spielehersteller Epic Games gegen die Höhe der App-Store-Provision rebellierte und inzwischen vor Gericht klagt, sammelt er immer mehr Mitstreiter im Kampf gegen Apple, darunter zahlreiche europäische Verlagshäuser.**

Der Streit zwischen dem Spielehersteller Epic Games und Apple, dem einzigen App-Store-Anbieter für iOS-Software, eskaliert weiter und wächst sich zu einem Flächenbrand aus. Epic Games hatte sich im August vehement gegen Apples App-Store-Regeln aufgelehnt und kritisiert die bis zu 30 Prozent hohe Provision für Apple.

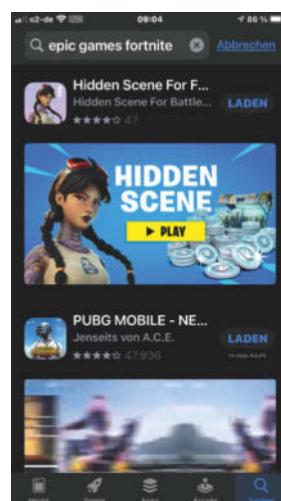
Stillschweigend baute Epic auch eine Funktion in sein Fortnite-Spiel ein, über die Kunden Erweiterungen direkt bei Epic kaufen sollten – was Apple vorhersehbar als Vertragsbruch wertete und zum Anlass nahm, das Spiel noch am selben Tag aus dem Store zu entfernen. Epic zog vor Gericht und warf Apple unfairen Wettbewerb vor. Apple verlangt in einer Gegenklage Schadenersatz.

Seit Ende September stehen Epic mehrere App-Anbieter und Verlagsorganisationen bei, um gemeinsam gegen die App-Store-Regeln vorzugehen: Die Non-Profit-Organisation „Coalition for App Fairness“ fordert „Wahlfreiheit“ und „faire Bedingungen“ rund um den App-Vertrieb, auch von Google.

Zu den Gründungsmitgliedern zählen neben Epic Games die Musik-Streaming-Dienste Spotify und Deezer, die MatchGroup, der auch die Dating-App Tinder gehört, der Verlegerzusammenschluss „Newsmedia Europe“ mit 14 Verlagen und der European Publishers Council (EPC). Unter den 28 Vollmitgliedern des EPC sind Axel Springer SE, Financial Times, Reuters, Verlagsgruppe Georg von Holtzbrinck, Gruner + Jahr, aber auch New York Times und andere App-Store-Betreiber behandelten Verleger „ausbeuterisch“, beklagt der EPC auf seiner Webseite und wendet sich an Regulierungsbehörden weltweit.

In der Folge baute Apple die Startseite seines Webauftritts um und verteidigte den App Store als „sicher und vertrauenswürdig“ für Nutzer und „große Chance“ für Entwickler.

Derweil kündigte Richterin Yvonne Gonzalez Rogers in einer Online-Anhörung Ende September an, dass der Prozess zwischen Epic Games und Apple wohl nicht vor Juli 2021 starten wird. Die gegnerischen Parteien müssen dem Zeitplan noch zustimmen. (dz@ct.de)



**Nur noch letzte Überbleibsel belegen, dass Epic Games sein Spiel „Fortnite“ kürzlich noch über Apples App Store vertrieben hat.**

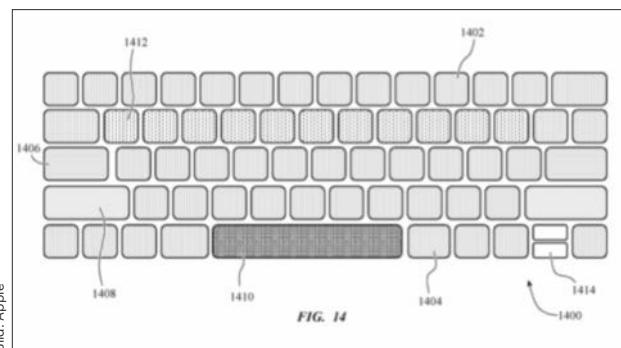
## Vibrationstastatur

Das US-Patentamt hat Apple unter der Nummer 20200303140 ein Patent für eine Tastatur erteilt, an der Nutzer den erwünschten Tastenwiderstand und die Anschlaglautstärke konfigurieren können.

Im zugehörigen Patentantrag schildert der Konzern, wie man mechanische Tasten mit zusätzlichen Elementen ergänzt

zen könnte, um etwa den Tastendruck zu messen und **akustische oder mechanische Rückkopplungen** auszulösen. Die Intensität der Rückmeldung könne per Software konfiguriert werden, beispielsweise in den Systemeinstellungen eines Macs. Unterschiedliche Anschlaglautstärken könnten manuell eingestellt werden oder auch automatisch je nach Vorgaben für die jeweilige Tageszeit.

Weil alle Tasten die Druckstärke dynamisch erfassen, könne die Tastatur ermitteln, welche Taste eigentlich ausgelöst werden sollte, wenn zwei oder mehrere gleichzeitig gedrückt wurden. Dabei geht sie davon aus, dass die mit dem höchsten Druck gemeint war. (dz@ct.de)



**Sensorik gegen Schreibfehler:** In einem US-Patentantrag schildert Apple, wie eine Tastatur selbstständig erkennt, welche Taste gemeint war, wenn zwei oder mehrere gleichzeitig gedrückt wurden.

## Strittige Kameranutzung

Die Instagram-App-Nutzerin Brittany Conditi klagt vor dem US-Bezirksgericht Northern District of California gegen den Facebook-Konzern, dem die Fotoplattform gehört. Sie wirft dem Unternehmen absichtliche, **ungehmigte Zugriffe auf Ihre Kamera** vor. Der Konzern wolle so „lukrative und wertvolle Daten über Nutzer sammeln, auf die er sonst keinen Zugriff hätte“.

Andere iPhone-Nutzer berichteten im Rahmen der Einführung von Apples iOS-Version 14 ebenfalls von unerwarteten Kamerazugriffen durch die Instagram-App. Das iPhone blendet ab iOS 14 in der Statusanzeige ein Signal ein, wenn Apps auf Kamera und Mikrofon zugreifen. Schon beim Betrachten eines Feeds soll Instagram die Kamera aktiviert haben.

Facebook wies die Anschuldigung zurück. Die Benachrichtigung sei fälschlich durch einen Programmfehler ausgelöst worden. (dz@ct.de)

DIGITAL

2020

# ITJOB SUMMIT

by Heise

Attraktive Arbeitgeber • Lebenslaufcheck • Spannende Vorträge

DAS DIGITALE EVENT FÜR IT-FACHKRÄFTE!

**23.10.2020**

FINDE DEINEN  
**TRAUMJOB** ONLINE!

Aussteller

accenture

adesso business people technology



Bundeskriminalamt

BWI  
IT für Deutschland

DEVK

HÄVG RECHENZENTRUM

Heise Gruppe

din tech

KLEMM & Cie.  
TALENT POOL

LEX COM  
LexCom Informationssysteme GmbH

methodpark

MSG

MTAG

ORWARE  
SOFTWARE ENGINEERING

real.digital  
we  digital commerce

SW/M

YESSPRESS

ZITIS

Unser Partner:

Jobware  
... da hab' ich den Job hier!

**JETZT KOSTENFREI REGISTRIEREN**  
**WWW.IT-JOB-SUMMIT.DE**

# Lenovo verkauft Computer mit Ubuntu Linux

**Lenovo will über 20 Geräteserien der ThinkPad- und ThinkStation-Reihen künftig mit Canonicals Ubuntu LTS anbieten.**

Seit geraumer Zeit testet Lenovo den Verkauf von Notebooks mit vorinstalliertem Linux, nun macht der weltgrößte PC-Hersteller Nägel mit Köpfen: Künftig wird man über 20 Gerätebaureihen mit vorinstalliertem Ubuntu Linux LTS von Canonical kaufen können.

Die vorgesehenen Serien umfassen ThinkStation (stationäre Workstation) und ThinkPad (Notebooks). Konkret stehen die ThinkStation-Serien P340, P340 Tiny, P520, P520x, P620, P720 und P920 auf der Liste, bei den ThinkPads sind es L14, L15, P1 Gen 3, P14s, P15, P15s, P15v, P17, T14 (Intel und AMD), T14s (Intel und AMD), T15, T15p, X1 Carbon Gen 8, X1 Extreme Gen3, X1 Yoga Gen 5, X13 (Intel und AMD) und X13 Yoga.

Die ThinkPad-L-Notebooks bekommen Ubuntu LTS 18.04, alle anderen hingegen das neuere Ubuntu LTS 20.04. Die Geräteserien an sich sind nicht neu, sondern wurden bislang nur mit vorinstalliertem Windows 10 verkauft. Lenovo will noch in diesem Monat mit dem weltwei-

ten Vertrieb der Ubuntu-Geräte beginnen, gibt aber an, dass es bis ins Jahr 2021 hinein dauern wird, bis alle Geräte in allen Regionen mit Linux verfügbar sind.

ThinkPad-Notebooks sind als Business-Geräte traditionell bei Linux-Nutzern und -Entwicklern beliebt. In den letzten Jahren hat sich das Bild allerdings gewandelt: Konkurrent Dell verkauft sein Flaggenschiff-Notebook XPS 13 als sogenannte Developer Edition bereits seit etlichen Jahren mit vorinstalliertem Linux und konnte damit viele Linux-Freunde für sich gewinnen. Hierzulande vertreibt außerdem der kleine Anbieter Tuxedo individuell be-

stückbare Notebook-Barebones von Clevo, Tongfang und anderen ODMs mit seinem hauseigenen Linux-System Tuxedo OS, ebenfalls auf Basis von Ubuntu, aber auch mit anderen Distributionen.

Bei besonders günstigen Notebooks unterhalb der 400-Euro-Marke, die laut Produktbeschreibung mit vorinstalliertem Linux angeboten werden, verschleiert die Betriebssystemangabe hingegen häufig lediglich die fehlende Windows-Lizenz. Hardware-Anpassungen und Treiberpflege sucht man dort in der Regel vergeblich; mitunter gibt es nicht einmal eine grafische Bedienoberfläche. (mue@ct.de)

**Das Bild zeigt noch ein Mock-up, aber bald sollen zahlreiche Lenovo-Rechner mit vorinstalliertem Ubuntu zu kaufen sein.**



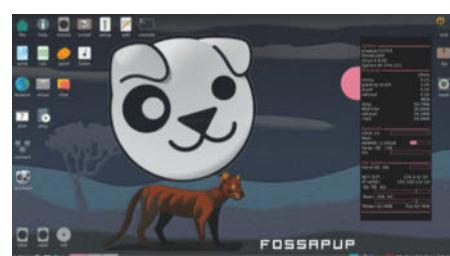
Bild: Lenovo

## Genügsames Live-Linux für betagte Rechner

Die Entwickler der minimalistischen Linux Distribution Puppy Linux haben FossaPup64 in der Version 9.5 veröffentlicht, das auf Ubuntu 20.04 „Focal Fossa“ basiert. Bei Puppy Linux handelt es sich um eine Sammlung genügsamer Live-Linux-Systeme, die auf Debian, Slackware oder Ubuntu basieren. Statt mit einer

Desktop-Umgebung ist FossaPup64 mit dem schlanken Fenstermanager JWM ausgestattet, dessen Bedienung der von älteren Windows-Oberflächen ähnelt. Auch die weiteren Programme sind nach diesem Prinzip ausgewählt: Pale Moon als Browser mit Mozillas älterer Gecko-Engine, die Textverarbeitung AbiWord und die Tabellenkalkulation Gnumeric sowie Deadbeef und MPV als Audio- und Videoplayer. In Puppy Linux laufen normalerweise alle Programme als Root. Ein Konfigurationsdialog stellt das für den Browser ab. Das ISO-Image ist nur gut 400 MByte groß und das System belegt nach dem Start nur etwa 160 MByte RAM. Überraschend für ein auf ältere Geräte ausgerichtetes System unterstützt FossaPup64 allerdings nur x86-64-Bit-Prozessoren, da Ubuntu die 32-Bit-Unterstützung fallengelassen hat.

(David Wolski/ktn@ct.de)



Das Live-System FossaPup64 verwendet den sparsamen Fenstermanager JWM.

## Gnome zählt in Zukunft anders

Mit der Veröffentlichung von Gnome 3.38 (siehe Seite 94) hat Entwickler Emmanuele Bassi eine Änderung des Versionsschemas angekündigt. **Das kommende Release wird Gnome 40 und nicht 3.40 heißen.** Die führende Ziffer 3 entfällt also. Künftig wird bei der halbjährlichen Veröffentlichung die Versionsnummer um eins hochgezählt. Im kommenden Jahr erscheint dann Version 41. Bisher waren die ungeraden Nummern für Entwicklerversionen reserviert. Diese tragen künftig die Beinamen „alpha“, „beta“ und „rc“, beispielsweise „Gnome 40.alpha“. Zwischen-Releases mit Fehlerkorrekturen innerhalb eines stabilen Releases erhalten die Versionsnummern 40.1, 40.2... Die Entscheidung zugunsten des neuen Versionsschemas anstelle von „Gnome 4.0“ fiel laut Bassi auch, um Verwechslungen mit der noch nicht erschienenen Bibliothek Gtk 4.0 zu vermeiden. (ktn@ct.de)

## Sysinternals-Tools für ARM

**Die Werkzeuge der Sysinternals-Suite gelten für viele Windows-Admins als unverzichtbar. Nun gibt es sie auch für Windows on ARM.**

Viele der kostenlosen Windows-Werkzeuge der Sysinternals-Suite hat Programmator Mark Russinovich für Geräte mit ARM-Prozessoren portiert. Sie stecken in einer separaten „Sysinternals Suite for ARM64“, zu finden wie üblich unter <https://sysinternals.com>.

Die ARM-Suite enthält unter anderem die Klassiker „Autoruns“ (zeigt, was Windows beim Hochfahren automatisch mitstartet) und den alternativen Taskmanager „Process Explorer“. Der „Process Monitor“ zeigt alle (!) Zugriffe auf Dateien, Ordner und Registry. Weitere Highlights: „Findlinks“ findet Hardlinks einer Datei. „Handle“ entlarvt, welcher Prozess welche Dateien geöffnet hält. „Junction“ erzeugt und zeigt symbolische Verknüpfungen.

Mit „Streams“ finden Sie heraus, welche Dateien sogenannte Alternate Data Streams (kurz ADS) enthalten – das sind an einer Datei hängende zusätzliche Daten, die im Explorer nicht zu sehen sind. „Sigcheck“ prüft die Signatur einer Datei und gibt Hash-Werte für die untersuchte Datei aus (MD5, SHA256 ...). Es vermag, die Datei im gleichen Abwasch vom Onlinedienst VirusTotal auf Viren prüfen zu lassen – das erlaubt schon vor dem ersten Start einer unbekannten ausführbaren Datei eine Einschätzung, ob man ihr vielleicht besser misstrauen sollte.

„Strings“ zeigt alle in einer Datei enthaltenen zusammenhängenden Zeichenformationen. „ZoomIt“ dient als Bildschirmlupe. Die nutzt nicht nur bei eingeschränkten Sehkräften, sondern auch dann, wenn man etwa bei einer Schulung den Teilnehmern ein wichtiges Detail besonders hervorgehoben zeigen möchte.

(axv@ct.de)

## Edge für Linux

Voraussichtlich noch im Oktober soll Microsoft **Edge für Linux als Testversion** erscheinen. Als Zielgruppe hat Microsoft Webentwickler ausgemacht, die mit Linux arbeiten und die Kompatibilität ihrer Seiten mit Edge prüfen wollen. Da es für Linux auch andere auf der Chromium-Engine basierende Browser gibt, dürfte der Erkenntnisgewinn aber gering sein.

Für Unternehmen, die ihre Mitarbeiter mit Privatgeräten im Homeoffice arbeiten lassen, hat sich Microsoft eine neue Funktion in Edge ausgedacht. In der cloudbasierten Geräteverwaltung Intune sollen Administratoren Edge mit Richtlinien fernverwalten (etwa erlaubte Websites, Startseite oder Plug-in-Verwaltung), ohne den ganzen Rechner in eine Windows-Domäne holen zu müssen. Um Privates und Dienstliches zu trennen, kann der Nutzer mehrere Profile in Edge anlegen.

(jam@ct.de)

T



# Smart meets sound.

Der neue HOLIST

Es gibt viele Bluetooth-Speaker mit Alexa-Sprachsteuerung, aber dieser hier kann noch mehr: Er klingt einzigartig gut. Erlebe deine Playlists mit Dynamore® Technologie für fulminanten 360-Grad-Sound aus jeder Position im Raum. [teufel.de/holist](http://teufel.de/holist)

**Teufel**

# Himmel austauschen mit Adobe Photoshop CC

**Die Bildbearbeitung Adobe Photoshop CC bekommt ein Werkzeug, mit dem sich der Himmel in einem Foto mit wenig Aufwand austauschen lässt. Wann das Update erscheint, steht noch nicht fest.**

Adobe hat ein Werkzeug für Photoshop CC angekündigt, mit dem sich der Himmel in einem Foto auf einfache Weise austauschen lassen soll. Der Filter „Sky Replacement“ steckt demnach künftig im Bearbeiten-Menü. Er stellt verschiedene Hintergründe in den Kategorien „Blue Skies“, „Spectacular“ und „Sunsets“ zur Verfügung, die sich sowohl um eigene Kategorien als auch um eigene Hintergrundfotos ergänzen lassen.

Photoshop CC trennt bei Aufruf des Dialogs automatisch das Motiv vom Hintergrund und erzeugt nach Klick auf eines der vorgegebenen Hintergrundfotos eine Vorschau im Hauptfenster der Anwen-

dung. Zum Maskieren und Abmischen der Farben nutzt Photoshop die künstliche Intelligenz hinter Adobe Sensei.

Über zusätzliche Regler lässt sich die Kante der automatisch generierten Maske verschieben oder weichzeichnen. Außerdem stellt das Werkzeug Regler für Helligkeit, Farbtemperatur und Größe des Hintergrunds bereit. Skalierten Himmel kann man mit dem Bewegen-Werkzeug passend positionieren. Der Farbtemperatur-

regler ändert auf Wunsch die Stimmung des Hintergrundbilds. Das Resultat gibt der Dialog als Ebenengruppe inklusive aller Masken aus.

Adobe hat die Technik nicht erfunden. Skylum stattet seine Bildbearbeitung Luminar mit allerlei KI-gestützten Funktionen aus. Eine der ersten war ein Dialog, zum Ersetzen des Himmels – ebenfalls unter Beachtung der Perspektiv- und Lichtverhältnisse. (akr@ct.de)

**Der Dialog „Sky-Replace-  
ment“ tauscht in Adobe  
Photoshop CC künftig  
einen langweiligen  
Himmel durch einen  
dramatischeren aus.**

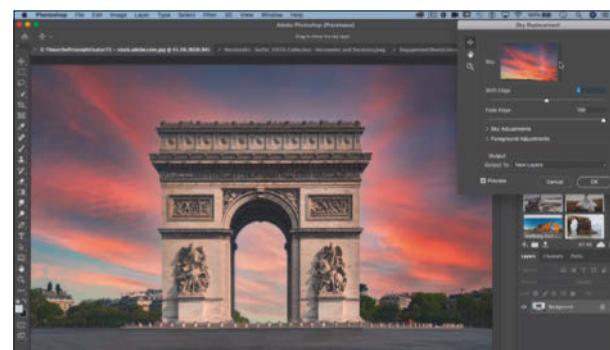


Bild: Adobe

## PicApport 9.0: Fototagging und Reiserouten

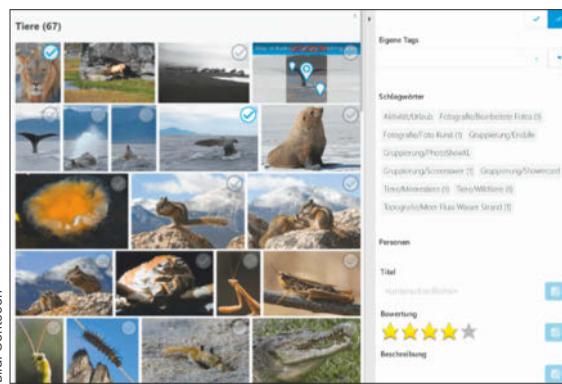
Der kostenlose Private-Cloud-Fotoserver PicApport 9.0 bringt eine Reihe Add-ons mit, die Fotos automatisch mit inhaltlichen Tags versehen. Das Add-on TagYourPhotos ermittelt deutschsprachige Stichwörter über künstliche Intelligenz. PicApport schickt dazu das um technische Metadaten gekürzte Bildmaterial zur Analyse an den Server des Anbieters Somax Software. Deren KI erkennt Gegenstände, Gebäude, Landschaften, Tiere, Sehenswürdigkeiten und anderes.

Zwei neue Hilfsprogramme nutzen den Dienst OpenStreetMap, um in den Metadaten abgelegte GPS-Koordinaten auszuwerten. OSMGeoReverseEncoder versieht Fotos, die Geodaten enthalten, mit aussagekräftigen Metadaten, beispielsweise Bezeichnungen für Land, Stadt und Adresse sowie den Bezeichnungen von Sehenswürdigkeiten wie Museen. Das Add-on OpenrouteGeoJSONRoute generiert Reiserouten anhand von Geodaten in einer Auswahl von Fotos und gibt die Route

als Bild inklusive des Kartenmaterials von OpenStreetMap über den Fotoserver aus.

Zusätzliche Add-ons zeigen Foto-Metadaten über das Hilfsprogramm ExifTool an, verwalten ausgewählte Verzeichnisse als privat und markieren Fotos rot, die nicht im JPEG-Format vorliegen.

PicApport läuft unter Windows, macOS sowie Linux und stellt Fotos über den Web-Browser auf lokalen Endgeräten wie Notebook, Smartphone und Tablet bereit. (akr@ct.de)



Über ein Add-on vergibt PicApport 9 automatisch Schlüsselwörter.

## Bildskalierung mit KI

Die iPad-Bildbearbeitung Pixelmator Photo hat ein neues Werkzeug zur Bildskalierung erhalten. Es heißt ML Super Resolution und restauriert gering aufgelöstes Bildmaterial mit Methoden maschinellen Lernens. Dabei rekonstruiert es Texturen und scharfe Kanten in Fotos, Illustrationen oder Bildern von Gemälden. Beim Upscaling verringert es Bildrauschen und Kompressionsartefakte.

Wie die gleichnamige Anwendung für macOS nutzt auch die iPad-Version einen nichtdestruktiven Ansatz zur Foto-Entwicklung. Neben Reglern unter anderem für Farbtemperatur, Belichtung, Schatten, Lichter, Farbton und Sättigung bietet es KI-gestützte Filter zur Filmsimulation und ein Werkzeug zur Objektretusche. Mithilfe eines Sliders kann man nun Vorher- und Nachheransicht miteinander vergleichen. Zweimaliges Tippen mit dem Apple Pencil löst jetzt eine konfigurierbare Aktion aus, beispielsweise Undo.

Pixelmator Photo 1.4 ist im Apple App Store für 7,99 US-Dollar erhältlich. Für registrierte Kunden ist das Update kostenlos. Die App setzt iOS 11.0 voraus.

(akr@ct.de)

## Teams wird zur Schaltzentrale

Bei den PC-Anwendungen ging es auf der diesjährigen Microsoft-Hausmesse Ignite einerseits um nicht mehr ganz so neue Neuerungen, andererseits um Ankündigungen diverser Erweiterungen für die Konferenzsoftware Teams. Eine interessante Mitteilung zu Microsoft Office versteckt sich im Exchange Team Blog.

Der Trend zur Arbeit im Homeoffice bescherte Microsoft Teams viele neue Nutzer. Der Anbieter rückt nun seine Software für Videokonferenzen in den Mittelpunkt – zum Beispiel mit der neuen **Home Site App**, mit deren Hilfe die SharePoint-Startseite und damit das Firmen-Intranet direkt in Teams zugänglich werden.

Vorhandene Apps will Microsoft nach und nach in Teams integrieren, beispielsweise die **Power BI App**. Hinzukommen neue: Mit **Power Virtual Agents** etwa sollen Anwender direkt in der Konferenzsoftware Apps und Chatbots bauen und veröffentlichen können. Mit der **Power Automate App** lassen sich Arbeitsabläufe automatisieren, beispielsweise Genehmigungsprozesse in Teams einrichten. Vieles, was auf der Ignite angekündigt wurde, wird erst gegen Ende des Jahres verfügbar sein – und auch dann zum Teil nur für englischsprachige Anwender. Das gilt beispielsweise für spezielle Hardware für Teams-Meetings von Lenovo und Yealink sowie die Integration von Cortana zu deren Steuerung.

Neuerungen im eigentlichen Kerngeschäft von Teams, den Besprechungen, wurden größtenteils bereits Anfang Juli vorgestellt. Der **Zusammen-Modus** platziert alle Teilnehmer eines Meetings vor einem gemeinsamen Hintergrund, und mit der Erweiterung der sogenannten **dynamischen Ansicht** können Vortragende in einem Teams-Meeting in benutzer-

Allerlei Neuigkeiten rund um Teams standen bei der Ignite im Vordergrund, so auch der „Zusammen-Modus“ für lustige Gruppenvideos vom Meeting.

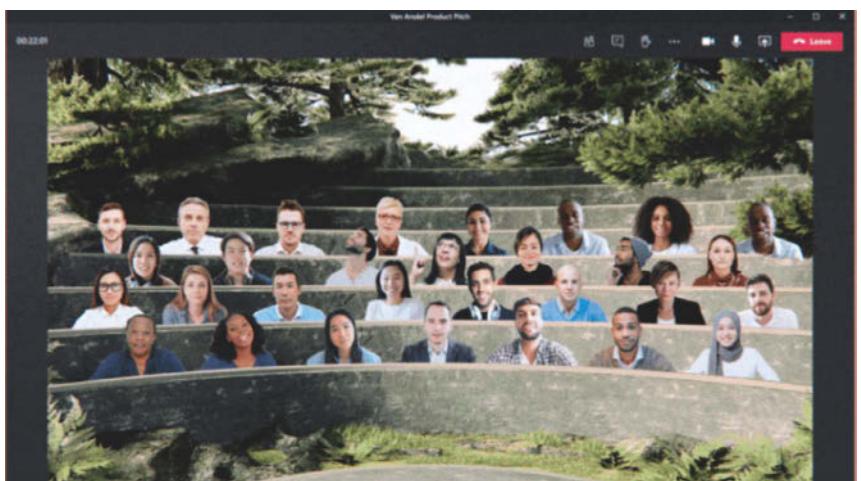


Bild: Microsoft

definierten Layouts festlegen, wie sie Grafiken oder Präsentationsfolien auf dem Bildschirm anordnen.

Im Oktober soll Teams um **Breakout-Räume** erweitert werden, in denen Teilnehmer in Kleingruppen diskutieren können. Nach Ende einer Besprechung soll künftig auf Wunsch eine Zusammenfassung des Meetings zur Verfügung stehen, mit Audio- oder Videoaufnahmen, Transkripten, Chatprotokollen und geteilten Dateien. Eine neue Funktion zur **Teilnehmerregistrierung** mit automatisierter E-Mail-Benachrichtigung soll die Organisation von Webinaren und Kundenpräsentationen erleichtern. Außerdem sollen ab Ende des Jahres Team-Meetings mit 1000 aktiven Teilnehmern und bis zu 20.000 Zuschauern möglich sein.

Für die zweite Hälfte 2021 kündigte Microsoft neue Versionen für Exchange Server, SharePoint Server, Skype for Business Server und Project Server an. Exchange-Kunden wird dieser Versionswechsel erstmals zum Abschluss eines Abos zwingen. Die neue Version soll Admins mit dem **Exchange Admin Center** unterstützen und einen Support-Zugang, Software-Aktualisierungen sowie Sicherheits- und Zeitzonens-Patches bieten. Konkrete Informationen für Nutzer älterer Versionen, insbesondere für Exchange 2016, dessen grundlegender Support am 13. Oktober 2020 endet, gab es auf der Ignite nicht.

Ein einzelner, unauffälliger Satz im Exchange Team Blog bezieht sich auf die Zukunft des Büropakets **Microsoft Office**: „Microsoft Office will also see a new perpetual release for both Windows and Mac, in the second half of 2021.“ Microsoft wird also offenbar die bisher übliche Praxis fortsetzen, parallel zur Abo-Version Microsoft 365 auch eine Kaufversion des Büropakets anzubieten. (dwi@ct.de)

Kentix MultiSensor®

SmartMonitoring

Schützt Ihre  
IT Infrastruktur



Data-Center + IT-Rack +  
kritische Infrastruktur



KLIMA



MONITORING



BRAND



E-MAIL / SMS / SNMP



EINBRUCH



APP

Komplette  
Software integriert!

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

# Vernetzter Terror

## [halle.nsu-watch.info](http://halle.nsu-watch.info)

Vor gut einem Jahr geschah der antisemitische und rassistische Anschlag in Halle auf die dortige Synagoge und einen Imbiss. Zunächst hieß es, der Angriff ginge von einem Einzeltäter aus. Tatsächlich hat der Attentäter zwar allein gehandelt, aber die Tat von Halle hängt durchaus mit rechtem Terror an anderen Orten zusammen. Eindrucksvoll zeigt das die interaktive Karte **Global White-Supremacist Terror: Halle** auf der Webseite von NSU Watch.

Auf zwei Zeitachsen sind die verschiedenen Ereignisse im Zusammenhang mit dem Halle-Attentat zusammengetragen, unterteilt nach Offline- und Online-Aktivitäten. Darunter ist beispielsweise der mutmaßliche Erhalt von 0,1 Bitcoins im Jahr 2013. Der Attentäter behauptet, das Geld bekommen zu haben, um Muslime zu töten. Die Tat selbst sowie die Flucht sind minutiös dokumentiert. Ein Klick auf einen Punkt des Zeitstrahls zeigt den Ort des Geschehens auf der Karte und führt zu weiteren Informationen, verlinkten Videos und anderen Quellen.

Ein dritter Zeitstrahl zeigt globale Ereignisse, die dem Attentat vorangegangen sind und auf die der Täter sich bezog, darunter die NSU-Mordserie sowie die rechtsextremen Attentate von Oslo, München, Pittsburgh und Christchurch. (ktn@ct.de)



# Man or Bro?

## [bropages.org](http://bropages.org)

Unter unixoiden Betriebssystemen bringen die meisten Programme ihre eigene Dokumentation mit, in sogenannten Manpages (von „manual“, also „Anleitung“). Das sind oft sehr umfangliche Texte, die jeden Programmparameter detailliert erklären. Konkrete Beispiele finden sich allerdings nicht immer und wenn, dann meist gegen Ende der langwierigen Lektüre.

„Just get to the point!“, sagen die **bropages**: Die Website listet Beispiele für häufige Programmaufrufe auf, jeweils mit einem kurzen Kommentar, was der Aufruf bewirkt. Die Bropages sind dadurch eine nützliche Ergänzung zu den Manpages, offiziellen Charakter haben sie allerdings nicht: Die Beispiele

```

1  # Create a tar archive
2  tar -cf archive.tar file1 file2 ... fileN
3
4  # Create a tar zipp'd archive
5  tar -zcf archive.tar.gz file1 file2 ... fileN
6
7  # Create multi-part tar archives from a directory
8  tar cf - /path/to/directory|split -b<max_size_of_part>M - archive.tar
9
10 # Extract all files from a tar archive
11 tar -xf archive.tar
12
13 # Extract all files from a tar zipped archive
14 tar -zxf archive.tar.gz
15
16 # Extract one file from a tar archive

```

werden von der Community beigesteuert und bewertet, nicht von den Entwicklern der jeweiligen Software. Es sind einfach Bros – also Kumpel –, die sich hier unverbindlich unter die Arme greifen. (syt@ct.de)

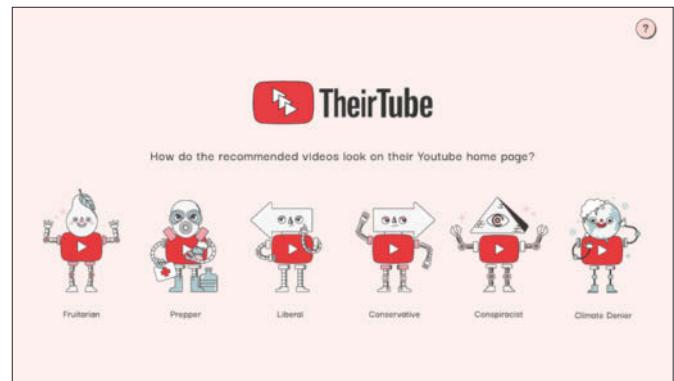
# Fremdsehen

## [their.tube](http://their.tube)

Filterblasen isolieren Gruppen voneinander, verstärken vorhandene (Vor-)Urteile und treiben Nutzer schlimmstenfalls zu immer extremeren Inhalten. Vor allem aber sind Filterblasen kaum wahrnehmbar: Die eigene Blase sieht man nicht und die darin befindlichen Inhalte wirken allzu leicht als objektive Themenauswahl.

Das Projekt **TheirTube** macht zumindest eine Filterblase sichtbar, nämlich die des Empfehlungsalgorithmus der YouTube-Homepage. TheirTube erlaubt die Vorschläge der Video-Plattform aus dem Blickwinkel verschiedener Personas einzusehen. Zur Auswahl stehen sechs Charaktere, vom liberal oder konservativ eingestellten Nutzer über den Doomsday-Prepper zum Klimawandelleugner. Die Personas sind nach echten Individuen modelliert: TheirTube folgt den Kanälen, denen auch diese echten Nutzer folgten, sieht sich Videos an und protokolliert regelmäßig die Empfehlungen von YouTube.

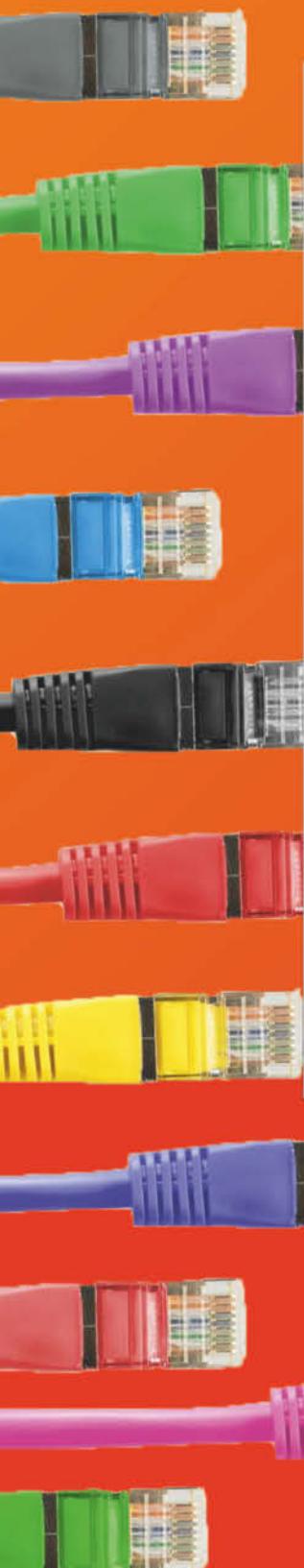
Durch diese Protokolle kann man sich klicken und sie – vor allem das ist interessant – zwischen den Personas vergleichen. Das führt deutlich vor Augen, wie stark Filterblasen die Sicht auf Inhalte verzerrn. Die eigene Blase und ihre Wirkung kann man so zumindest erahnen. (syt@ct.de)



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

NEU

# So läuft alles rund!



## c't ADMIN

IT-Praxis für Heim- und Büronetzwerke

### So läuft alles rund

Windows-Netzwerke tunen  
Netzwerk-Bremsklötze finden und beseitigen

Helpen ohne Hinfahren  
PCs und Mobilgeräte fernwarten

VPN modernisieren  
IPSec-Altlasten raus, WireGuard rein

Nextcloud optimieren  
Tipps für die Gruppenarbeit in der Cloud

Funknetze erweitern  
Mächtige WLAN-Controller  
Privates LTE ergänzt WLAN

Traffic analysieren  
Netzverkehr live beobachten, Störer finden,  
Netzwerkmitschnitte richtig lesen

### Fritzbox optimal

IPv6-Vorteile mit DynDNS nutzen, TK-Anlage erweitern  
Telefonie verschlüsseln, VPN und SMB-Freigaben beschleunigen



Auch als  
Heft + PDF  
erhältlich mit  
29 % Rabatt



### c't Admin 2020

Die alltäglichen Anforderungen eines Admins sind vielfältig und jeder Tag hält neue Überraschungen bereit. Egal ob das WLAN wieder zu lahm ist, die VPN-Techniken dringend modernisiert werden müssen oder das Windows-Netzwerk ein Tuning vertragen könnte, mit hilfreichen Praxis-Tipps erleichtert das neue c't-Sonderheft Ihren Arbeitsalltag. Darüber hinaus schärft die c't-Redaktion den Blick für die aktuellen Entwicklungen in der IT-Praxis.

[shop.heise.de/ct-admin20](http://shop.heise.de/ct-admin20)

Einzelheft  
für nur

14,90 € >



# Aufgeschwatzt

**Klarmobil jubelt Kunden kostenpflichtige Zusatzleistungen unter**



**Damit ein Vertrag wirksam zu-  
stande kommt, muss der Kunde  
deutlich auf die damit für ihn  
verbundenen Kosten hingewie-  
sen werden. Bei Klarmobil ist  
man sich darüber offenbar nicht  
immer ganz im Klaren.**

Von Tim Gerber

**S**einiger Zeit hat Albert R. einen Mobilfunkvertrag mit Klarmobil. Um sich für seine langjährige Treue zu bedanken, rief ihn am 3. Dezember ein Vertriebsmitarbeiter des Providers an. Man wolle ihm die Zusatzoption save.tv einrichten. Damit könne er das Programm von etwa 45 Sendern online und offline nutzen. Zum Kennenlernen erhalte er den Service für einen Monat kostenfrei und könne danach selbst entscheiden, ob er das Angebot für 5 Euro im Monat weiter nutzen wolle. Leicht genervt von dem unvermittelten Anruf sagte Albert A. zu allem Ja und Amen, was der schwatzhafte Kundenberater von ihm wollte. Schließlich hörte es sich für ihn nach einer Werbeaktion ohne Folgekosten

an. Anschließend vergaß er den ungebeuteten Anruf ebenso rasch wieder, wie er die beiden Kurznachrichten wegglickte, die Klarmobil ihm im Anschluss auf sein Telefon schickte.

So war er einigermaßen erstaunt, als Klarmobil ab Februar begann, ihm monatlich 5 Euro für die Option, die er selbst ja gar nicht gebucht hatte, in Rechnung zu stellen. Er monierte dies mit Schreiben vom 14. Februar bei dem Provider, erhielt darauf aber keine Antwort. Also korrigierte er kurzentschlossen selbst den Rechnungsbetrag und überwies nur den unstreitigen Anteil für die Grundgebühr an Klarmobil. Das bescherte ihm in der Folge freilich weitere Rechnungen und Mahnungen.

Anrufe bei der Hotline des Providers brachten auch keine Aufklärung. Das Gespräch mit der Bestellung sei aufgezeichnet und man habe sich das angehört. Demnach gebe es keinen Zweifel, dass er selbst die kostenpflichtige Option gebucht habe. Albert R. bat deshalb darum, ihm die Aufnahme doch ebenfalls vorzuspielen. Das sei aus Gründen des Datenschutzes nicht möglich, teilte man ihm mit.

## Unbewiesen

Da man ihm den Vertragsschluss nicht nachweisen wollte und auf seine schriftlichen Nachfragen keine Reaktion erfolgte, schrieb Albert R. am 26. April erneut an Klarmobil und kündigte nun vorsorglich ganz ausdrücklich die kostenpflichtigen Zusatzoptionen. Auch darauf erfolgte erst einmal keine Reaktion außer weiteren Rechnungen und Mahnungen, denen Albert R. aber nur soweit nachkam, als er sie für berechtigt hielt.

Mit Schreiben vom 15. Juli kündigte ihm Klarmobil dann außerordentlich, weil er seinen vertraglichen Pflichten angeblich nicht nachkäme. Zusätzlich und ohne weitere Vorwarnung schaltete der Provider die genutzten Telefonnummern ab. Für den Rest der Vertragslaufzeit sollte der Kunde an Klarmobil einen Schadenersatz in Höhe der verbleibenden Grundbeträge zahlen.

Auf seinen Vorhalt, die streitige Tarifoption save.tv nie gebucht zu haben, ging Klarmobil auch in dem Kündigungsschreiben nicht ein. Anfang August wandte sich Albert R. mit dem Fall an c't. Wir fragten am 26. August bei der Pressestelle der Freenet AG nach, zu der auch Klarmobil gehört. Merkwürdig kam uns vor allem die Sache mit der Aufzeichnung vor. Deshalb baten wir unter anderem darum, die Aufnahme anhören zu können.

## Abgehört

Dieser Bitte kam der Freenet-Pressesprecher Rüdiger Kubald bereits am folgenden Tag nach und übersandte uns verschlüsselt eine Audiodatei und das zum Öffnen nötige Passwort. Eine Anfrage des Kunden nach dem Mitschnitt läge dem Unternehmen allerdings nicht vor. Zur Sache teilte der Unternehmenssprecher mit, dem Kunden sei in dem Gespräch die Option save.tv angeboten worden. Im Rahmen dieses Angebots sei für ihn der erste

Monat kostenlos gewesen. Mit der Einrichtung habe der Kunde sich einverstanden erklärt.

Vor diesem Hintergrund und da das primäre Interesse von Klarmobil die Zufriedenheit des Kunden mit der Hauptleistung Mobilfunk sei, habe man die Nachfrage von c't zum Anlass genommen mit dem Kunden Kontakt aufzunehmen, um eine individuelle Kulanzlösung zu finden.

Die Interpretation des c't nunmehr im Mitschnitt vorliegenden Gesprächs seitens Klarmobil ist mindestens fragwürdig. Wer am Telefon Leute überrumpelt und ihnen vertraglich bindende Zusagen abringen will, der muss in aller Deutlichkeit auf die wesentlichen Bedingungen hinweisen. Diesen Anforderungen wird das Gespräch mit dem Kunden seitens Klarmobil eher nicht gerecht.

Zwar weist der Mitarbeiter darauf hin, dass eine über den Probemonat hinausgehende Nutzung der Option Kosten in Höhe von 5 Euro im Monat verursachen wird. Es fehlt aber der entscheidende Hinweis darauf, dass die vom Provider initiierte Einrichtung zu einer automatischen Verlängerung führt. Im Gegenteil suggeriert der geschulte Verkäufer dem Kunden mit den Worten „danach entscheiden Sie selbst, ob Sie die Option für vier Euro neunundneunzig im Monat weiter nutzen wollen“, dass er nichts unternehmen muss, wenn er das Angebot nicht kostenpflichtig nutzen will.

# VORSICHT KUNDE!



Bild: Klarmobil.de

**Auf die automatische Vertragsverlängerung nach Ablauf des kostenlosen Testmonats für die Option save.tv werden Kunden von Klarmobil bei Verkaufsgesprächen nicht immer deutlich genug hingewiesen.**

Vor Gericht dürfte sich Klarmobil mit dieser Aufnahme als gültigen Vertragsschluss wahrscheinlich nicht durchsetzen können. Die Formulierung, dass der Kunde am Ende des kostenfreien Probemonats „selbst entscheiden“ könne, obwohl eine automatische Verlängerung vorgesehen ist, kann jedenfalls gehörig in die Irre führen. Das Unternehmen tut jedenfalls gut daran, sich gütlich mit dem Kunden über eine Bereinigung des Vorfallen zu verständigen. Wie die angekündigte individuelle Lösung für Albert R. genau aussehen soll, war zu Redaktionsschluss noch offen. (tig@ct.de) **ct**

## Service im Visier

Immer wieder bekommen wir E-Mails, in denen sich Leser über schlechten Service, ungerechte Garantiebedingungen und überzogene Reparaturpreise beklagen. Ein gewisser Teil dieser Beschwerden ist offenbar unberechtigt, weil die Kunden etwas überzogene Vorstellungen haben. Vieles entpuppt sich bei genauerer Analyse auch als alltägliches Verhalten von allzu scharf kalkulierenden Firmen in der IT-Branche.

Manchmal erreichen uns aber auch Schilderungen von geradezu haarsträubenden Fällen, die deutlich machen, wie einige Firmen mit ihren Kunden umspringen. In unserer Rubrik „Vorsicht,

Kunde!“ berichten wir über solche Entgleisungen, Ungerechtigkeiten und duobiose Geschäftspraktiken. Damit erfahren Sie als Kunde schon vor dem Kauf, was Sie bei dem jeweiligen Unternehmen erwarten oder manchmal sogar befürchten müssen. Und womöglich veranlassen unsere Berichte ja auch den einen oder anderen Anbieter, sich zukünftig etwas kundenfreundlicher und kulanter zu verhalten.

Falls Sie uns eine solche böse Erfahrung mitteilen wollen, senden Sie bitte eine chronologisch sortierte knappe Beschreibung Ihrer Erfahrungen an: [vorsichtkunde@ct.de](mailto:vorsichtkunde@ct.de).

# Lange haltbar

Digitale Daten langfristig zuverlässig speichern



<b>Digitale Daten archivieren</b> .....	<b>Seite 60</b>
<b>Festplatten für die Archivierung</b> .....	<b>Seite 64</b>
<b>Archivmedium M-Disc</b> .....	<b>Seite 68</b>
<b>Archiv in der Cloud</b> .....	<b>Seite 72</b>

# Täglich wächst der Datenberg – aber wie konserviert man digitale Schätze so, dass man selbst oder die Nachfahren damit in 20 oder 30 Jahren noch etwas anfangen können?

Von Christof Windeck

**D**igitalisierung durchdringt allmählich auch die letzten Ecken unseres Lebens: Selbst manchen ärztlichen Befund bekommt man nur noch als Datei, beispielsweise Tomografie- oder Röntgenbilder. Rechnungen, Kontoauszüge und Adressen existieren bloß noch in Smartphone-Apps, als E-Mail-Anhang oder auf Cloud-Speicher. Familienfotos, Videos und Musiksammlungen luntern auf SD-Speicherkarten, USB-Festplatten oder Netzwerk-Speicherboxen (NAS) herum.

Unweigerlich stellt sich die Frage, wie man wichtige digitale Daten über längere Zeiträume sicher aufbewahrt. Firmen sind zur Archivierung verpflichtet, siehe Kasten auf Seite 62. Während es dafür aber klare Fristen und gegen Bezahlung auch passende Lösungen gibt, müssen sich Privateleute selbst ihre eigene individuelle Lösung suchen. Denn nicht nur Art und Menge der persönlich wichtigen Daten unterscheiden sich enorm, sondern auch die Lebensumstände und somit auch die Ziele der Archivierung sowie die Möglichkeiten zum langfristigen Lagern von Datenträgern.

Mit den wichtigsten Aufgabe können Sie aber sofort anfangen: Planen und Sortieren. Ein langfristiges Archiv ist nämlich nicht bloß ein Backup, sondern verlangt mehr Aufwand. Vor allem gilt es, Wichtiges von Überflüssigem zu trennen. Sonst drohen undurchdringliche Datenhaufen, weil man in 20 oder 30 Jahren viele heutige Datenformate nur noch mit enormem Aufwand oder gar nicht mehr lesen können wird. Dann gehen Daten verloren, was dem Sinn eines Archivs widerspricht.

Zum Langzeit-Datenarchiv führen also drei wesentliche Schritte: erhaltenswerte Daten auswählen, anschließend möglicherweise in geeignete Ablageformate konvertieren und schließlich zwecks

Redundanz auf mehreren Archivierungsmedien ablegen. Die nachfolgenden Artikel erklären, wie gut sich Festplatten, Cloud-Speicher und optische Medien für private Archive eignen.

## Backup vs. Archiv

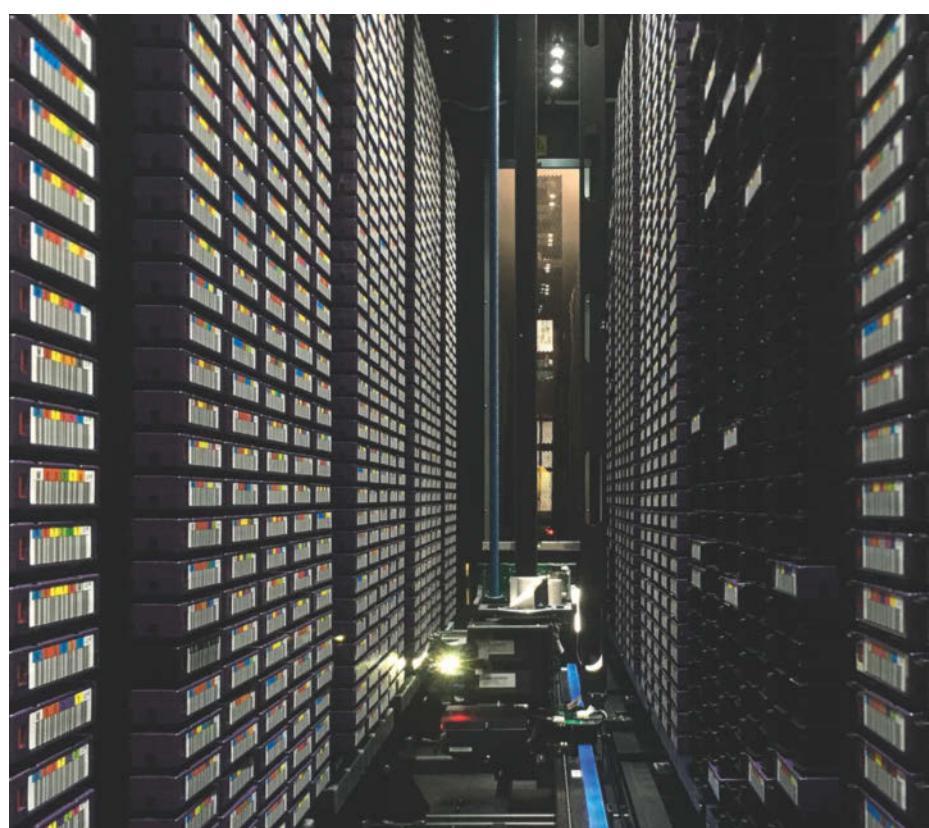
Kurz ein Abstecher zum Thema Backup, weil Sie es ohnehin haben sollten und einige Konzepte auch für die Archivierung gelten. Ein Backup in Form zusätzlicher Sicherungskopien schützt vor Datenverlust. Besonders häufig sind triviale Missgeschicke wie das versehentliche Löschen oder Überschreiben von Daten. Vor allem Mobilgeräte werden aber auch vergleichsweise häufig beschädigt, gestohlen oder

gehen verloren. Sogar ein Desktop-PC im vermeintlich geschützten (Heim-)Büro kann Daten verlieren: durch Überspannung, Blitzschlag, Feuer, Wasserrohrbruch, Einbrecher sowie Schadsoftware wie Emotet.

Grundsätzlich sollte es von jeder Datei mindestens zwei Sicherungskopien geben, die an unterschiedlichen Orten lagern, um sie etwa vor Feuer zu schützen. Hierfür bieten sich NAS-Speicher an oder die verschlüsselte Ablage in der Cloud. Die zugehörigen Passwörter schreibt man auf mehrere Zettel, die wiederum an unterschiedlichen Orten lagern. Für ein Langzeitarchiv kommen weitere Fragen hinzu [1]: Welche Daten lohnen den Aufwand? Wie lange bleiben Speichermedien lesbar? Wird es in 30 Jahren noch USB geben? Welche Dateiformate werden noch lesbar sein? Wohlgere ich Festplatten jahrzehntelang trocken, kühl, staubfrei und gegen unbefugten Zugriff geschützt? Wie konserviere ich Passwörter über Jahrzehnte – auch wenn ich sie mal ändern muss?

## Speichermedien

Denken Sie doch mal zurück ins Jahr 1990: Damals gab es vor allem Floppydisks als



**Magnetband (Tape) kommt nach wie vor zur kostengünstigen Speicherung großer Datenbestände zum Einsatz, aber vor allem in Rechenzentren, wie in diesem Bandroboter der GWDG in Göttingen.**

Bild: Björn Nachwey/GWDG Göttingen



**SATA-SSDs sind mittlerweile mit bis zu 8 TByte Kapazität erhältlich, sind aber zur Langzeitarchivierung nicht empfehlenswert.**

Wechselspeichermedium, für die man heute kaum noch Laufwerke findet. Selbst wenn man eines hat, sind Lesefehler keine Seltenheit. Zip- und Jaz-Drives, MO-Laufwerke, DAT-Bänder und PC Cards waren 1990 noch nicht verbreitet und sind zwischenzeitlich längst wieder vom Markt verschwunden. Es ist also schwierig, die Langzeittauglichkeit von Speichermedien einzuschätzen. Immerhin gibt es beispielsweise noch Adapter, um die ab 1989 eingeführten IDE-Festplatten per USB auszulesen.

Festplatten, die in einwandfreiem Zustand ohne Vorschädigungen eingelagert werden, lassen sich nach 5 Jahren Lagerzeit mit hoher Sicherheit auslesen. Viele kommen auch mit 5 Jahren Garantie. Wahrscheinlich funktionieren die meisten Exemplare erheblich länger. Genaue Untersuchungen dazu kennen wir allerdings nicht. Der Hersteller Western Digital rät dazu, Festplatten unter Raumtemperatur zu lagern, weil höhere Temperaturen Bitfehler bei magnetischen Medien begünstigen. Tipps zur Auswahl von Platten finden Sie ab Seite 64.

Doch nichts hält ewig und nach 5 bis 10 Jahren sollten Sie Ihr Archiv auf dann frische (und größere) Datenträger umkopian. Festplatten erreichen relativ hohe Datentransferraten, aktuelle Exemplare in den schnellsten Zonen über 250 MByte/s, was sich auch via USB 3.0 (USB 3.2 Gen 1) voll nutzen lässt. Bei einer mittleren Transferrate von 150 MByte/s braucht man für beispielsweise 2 TByte im Idealfall (große Dateien) knapp 4 Stunden. Bei 14 TByte dauert eine solche Aktion dann schon länger als einen Tag.

Abseits von optischen Speichermedien (S. 68) und der Cloud (S. 72) wird vor allem noch Bandspeicher (Tape) für Archi-

ve genutzt – aber das ist in der Praxis nur für größere Firmen sinnvoll. Die Bänder selbst sind zwar pro Terabyte günstig und für 30 Jahre Lagerzeit ausgelegt, aber ein aktuelles LTO-8-Laufwerk [2] kostet rund 3000 Euro und verlangt einen SAS-Hostadapter. Doch wie die Erfahrung zeigt [3], drohen trotz sorgfältiger Planung schon nach 15 Jahren erhebliche Probleme. Bei LTO plant man üblicherweise nach spätestens zwei Generationswechseln das Umkopieren der Daten ein.

Immer wieder taucht die Frage auf, wie gut sich Flash-Speichermedien wie SSDs, USB-Sticks und SD-Speicherkarten für die Archivierung eignen. Die Antwort weiß aber niemand. Wir kennen keine aktuelle SSD, deren Hersteller konkrete Aussagen zur Langzeitspeicherung macht. Zudem lassen sich Erfahrungen mit älteren Flash-Medien nicht auf aktuelle Produkte übertragen: Die darin eingebauten NAND-Flash-Speicherchips werden rasch weiterentwickelt, Chips aus dem Fertigungsjahr 2018 unterscheiden sich technisch fundamental von welchen beispielsweise aus dem Jahr 2014. Zudem hängt die sogenannte „Retention Time“ der einzelnen Flash-Zellen davon ab, wie oft sie jeweils schon überschrieben wurden.

Als Archivmedium ist Flash-Speicher folglich ungeeignet, als zusätzliches Backup-Medium aber nutzbar im Sinne von „besser ein mittelprächtiges Backup als gar keins“. Nach dem gleichen Motto taugen auch Ausdrucke von Dokumenten und

Papierfotos als zusätzliche Kopie – aber sie brauchen viel Platz und vertragen ungünstige Lagerbedingungen schlecht.

## Datenformate

Wenn Sie nun abermals ins Jahr 1990 zurückdenken: Wissen Sie noch, welche Datenformate damals aktuelle Programme verwendet haben? Und falls ja: Hätten Sie noch Software, die diese Formate lesen kann, samt dem möglicherweise nötigen Lizenzschlüssel und einem (Betriebs-)System, auf dem das alles funktioniert? Dieser Rückblick zeigt: Dateien müssen in schlau gewählten Formaten abgespeichert sein, wenn sie nach 30 Jahren noch nützlich sein sollen – insbesondere, wenn Sie sie für Ihre Nachfahren aufheben, die ja keine Ahnung haben werden, mit welcher Software die Daten einst erzeugt wurden. Es ist also eine gute Idee, auch Programme mit ins Archiv zu packen, welche die konservierten Dateien lesen und anzeigen können. Besonders gut eignet sich dafür quelloffene Software, die man inklusive Quellcode archiviert, den man notfalls in Jahrzehnten neu kompilieren kann. Außerdem kann man ein Image des aktuell genutzten Betriebssystems mit archivieren.

Für fast alle elektronischen Daten, die Sie auch ausdrucken könnten – also Briefe, Diplomarbeit, Excel-Tabellen, gescannte Dokumente – bietet sich das zur Archivierung gedachte PDF-Format PDF/A an. Es hat eine offengelegte Spezifikation und ist weit verbreitet, was die Chancen erhöht,

## Archive für Firmen: Pflichtaufgabe

Der Gesetzgeber bürdet Unternehmen eine ganze Reihe von Pflichten beim Umgang mit ihren geschäftlichen Daten auf. Dabei geht es einerseits um Datenschutz, andererseits um Archivierung. Je nach Art der elektronischen Firmendokumente gelten unterschiedliche Aufbewahrungsfristen, für Rechnungen etwa 10 Jahre [5]. Je nach Branche, Größe und Umsatz der Firma können unterschiedliche Regeln gelten, stets jedoch die „Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoDB). Digitale Dokumente müssen dabei auch digital konserviert werden – und zwar unverändert und nachvollzieh-

bar. Man spricht von „Revisionssicherheit“.

Was sich kompliziert anhört, ist bei geschickter Planung eine lösbarer Aufgabe: Für die üblichen Office-Dateien und gescannte Dokumente gibt es auch für Kleinfirmen bezahlbare Dokumentenmanagementsysteme [4] sowie Tools zur revisionssicheren Archivierung von E-Mails. Zum Nachweis der Revisionssicherheit genügt allerdings nicht etwa das Zertifikat eines Herstellers. Die Einhaltung der GoDB bleibt vielmehr eine Aufgabe des jeweiligen Unternehmens, das sein Verfahren dokumentieren sollte: Wie genau erfolgt die Datenablage, wer hat dabei welche Pflichten und Zugriffsrechte.

## Speichermedien für die Archivierung

Typ	maximale Kapazität pro Medium	günstigster Preis pro Terabyte (bei Kapazität pro Medium)	Datentransferrate (Kopieren von 4 TByte)	geschätzte Haltbarkeit fabrikneuer Medien bei idealer Lagerung
Festplatte	18 TByte	19 € (6 TByte)	150 MByte/s (8 Stunden)	5 Jahre (eher länger)
SSD (SATA/USB)	8 TByte	80 € (1 TByte)	300 MByte/s (4 Stunden)	unklar
Blu-ray Disc	0,1 TByte	16 € (25 GByte) <sup>1</sup>	45 MByte/s (25 Stunden <sup>2</sup> )	über 10 Jahre, abhängig von Brennqualität
LTO-Magnetband	12 TByte	8,50 € (12 TByte) <sup>3</sup>	360 MByte/s (3 Stunden <sup>4</sup> )	30 Jahre (für Laufwerke nicht spezifiziert)
Cloud-Speicher	–	ab 12 € pro Jahr	6 MByte/s (180 Stunden <sup>5</sup> )	unklar

<sup>1</sup> BD-R mit 100 GByte kosten rund 85 € pro Terabyte und sind nur mit 4X-Geschwindigkeit erhältlich (18 MByte/s)

<sup>2</sup> mit den bisher schnellsten Medien (10X-Brenngeschwindigkeit)

<sup>3</sup> bei LTO-8; LTO-7 kommt auf 300 MByte/s und max. 9 TByte pro Band

<sup>4</sup> ein LTO-8-Laufwerk kostet rund 2900 € plus PCIe-SAS-Adapter

<sup>5</sup> bei 50 MBit/s im Uplink

dass es in vielen Jahren noch lesbar sein wird.

Microsoft Word und LibreOffice können Daten ohne Zusatzsoftware als PDF/A abspeichern. Doch als PDF/A abgelegte Office-Dateien können Sie anders als eine DOCX- oder ODT-Datei nicht einfach erneut öffnen, bearbeiten und wieder abspeichern. PDF/A ist eben ein Archivformat für digitale Dokumente im Originalzustand, also eine Art „digitaler Ausdruck“.

Apropos Ausdruck: Für Programme, die nicht von sich aus im Format PDF/A exportieren können, gibt es virtuelle PDF/A-Drucker. Die funktionieren ähnlich wie das in Windows 10 eingebaute „Microsoft Print to PDF“ – aber das kann leider kein PDF/A. Die Archivierungsfunktion lassen sich viele Firmen gut bezahlen, wir kennen keinen kostenlosen virtuellen Drucker mit PDF/A-Funktion. Für Privatleute gibt es aber etwa das Dokumentenmanagementsystem (DMS) ecoDMS [4] für unter 100 Euro inklusive dieser Funktion. Ein solches DMS erleichtert auch die Klassifizierung der archivierten Dateien anhand von Metadaten. Hinweise wie „Urlaub 2017“ oder „Taufe Susi“ lassen sich auch in andere Dateiformate einbetten, etwa in JPEG-Fotos, und erleichtern die Suche später ungemein.

Bei Multimediadaten ist es schwieriger, das optimale Dateiformat zu wählen. JPEG-komprimierte Fotos lässt man am besten wie sie sind, problematisch sind proprietäre Raw-Formate der Kamerahersteller. So zieht sich etwa die Traditionsmarke Olympus derzeit aus dem Kameramarkt zurück. Wie lange wird kommende Raw-Software also noch Dateien mit der Endung .orf lesen können? Hier steht also eine Konvertierung an, aber ob Adobes offengelegtes Raw-Format DNG tatsächlich noch 30 Jahre durchhält oder doch eher JPEG oder das relativ junge HEIF, lässt sich nicht vorhersagen. Verlustfrei komprimierte PNG-Daten wiederum benötigen relativ viel Festplattenplatz.

Kompromisse gilt es auch bei Musik zu finden. Liegen die Daten unkomprimiert vor, kann man sie etwa als WAV-Datei archivieren, was viel Platz belegt. Der Open-Source-Codec Flac hingegen komprimiert verlustfrei, ist aber wesentlich weniger verbreitet als MP3 und AAC. Hat man ohnehin nur komprimiertes Material in einem dieser Formate, konserviert man am besten das Original [1].

Bei Video gibt es häufiger Neuerungen: Besonders verbreitet ist zurzeit noch MPEG-4 alias H.264 und AVCHD. Mit dem effizienteren Nachfolger H.265 (HEVC) konkurriert VP9, das etwa YouTube bevorzugt verwendet. Doch auch für VP9 tritt schon ein Nachfolger an, nämlich AV1. Ältere Videos in „Standard Definition“ (SD), also einer größeren Auflösung als 720p (1280 × 720 Pixel), haben häufig MPEG-2-Format. Glücklicherweise gibt es Open-Source-Software wie den VLC Player des VideoLAN-Projekts, den man im Quellcode herunterladen und ebenfalls archivieren kann. Unter [ct.de/ym5j](http://ct.de/ym5j) finden Sie detaillierte Erläuterungen und Bewertungen von 52 Datenformaten durch die schweizerische Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen (KOST).

### Komprimieren und verschlüsseln

Wenige große Dateien lassen sich schneller kopieren als eine Ordnerstruktur mit tausenden kleinen Dateien. Solche Ordnerstrukturen kann man komprimiert in eine größere Datei verpacken. Allerdings droht dann ein einzelner Lesefehler, die gesamte Archivdatei unbrauchbar zu machen, und trifft nicht bloß eine einzige Datei. Auch Verschlüsselung hat die Kehrseite, dass der Verlust des Passworts die Daten vernichtet. Falls man dennoch komprimieren und verschlüsseln möchte, bietet sich das Open-Source-Werkzeug 7-Zip an (siehe [ct.de/ym5j](http://ct.de/ym5j)), das man am besten inklusive Quelltext mit archiviert.

Wer seine Archivmedien und Passwortzettel nicht Verwandten oder Freunden anvertrauen möchte, kann auf ein Bankschließfach ab rund 30 Euro jährlich zurückgreifen. Nicht alle Schließfachanlagen sind jedoch klimatisiert. In vielen Städten gibt es Dienstleister, die ab etwa 120 Euro pro Jahr klimatisierte Lagerräume vermieten.

### Sortieren und planen

Das bloße Aufhäufen riesiger Dateiberge ist keine Archivierung: Darin versinken digitale Perlen im Datenmüll. Ein Archiv verlangt vor allem Auswahl und Vorausplanung. Im Abstand von rund fünf Jahren sollte man private digitale Archive prüfen und gegebenenfalls auf andere Speichermedien kopieren. Auch wenn das Arbeit macht, ist es doch weitaus einfacher, als analoge Medien zu konservieren. Denken Sie nur an verstaubte Fotoalben mit verkratzten und vergilbten Papierabzügen. Von einer Festplatte mit tausenden Familienfotos können Sie hingegen problemlos weitere Kopien in Originalqualität anfertigen – Sie müssen es nur auch tun!

(ciw@ct.de) 

### Literatur

- [1] Dieter Brors, Hartmut Gieselmann, Ulrich Hilgefort, André Kramer, Andrea Trinkwalder, Für die Nachwelt erhalten, Das persönliche digitale Archiv gestalten und weitergeben, c't 8/2017, S. 110
- [2] Lutz Labs, Grundlagen Bandlaufwerke, Magnetbänder und Laufwerke für das Backup großer Datensmengen, c't 8/2020, S. 118
- [3] Mirko Dölle, Heikle Datenarchäologie, Tape-Backups nach Jahrzehnten einlesen, c't 22/2016, S. 178
- [4] Peter Schüler, Ordnung im Archiv, Systeme zur privaten und geschäftlichen Dokumentenverwaltung, c't 23/2016, S. 108
- [5] Martin Weigel, Digitale Konserven für den Fiskus, Vorgaben der Finanzbehörde zur Aufbewahrung elektronischer Belege und Dokumente, c't 17/2015, S. 144

**Datenformate für die Archivierung:**  
[ct.de/ym5j](http://ct.de/ym5j)

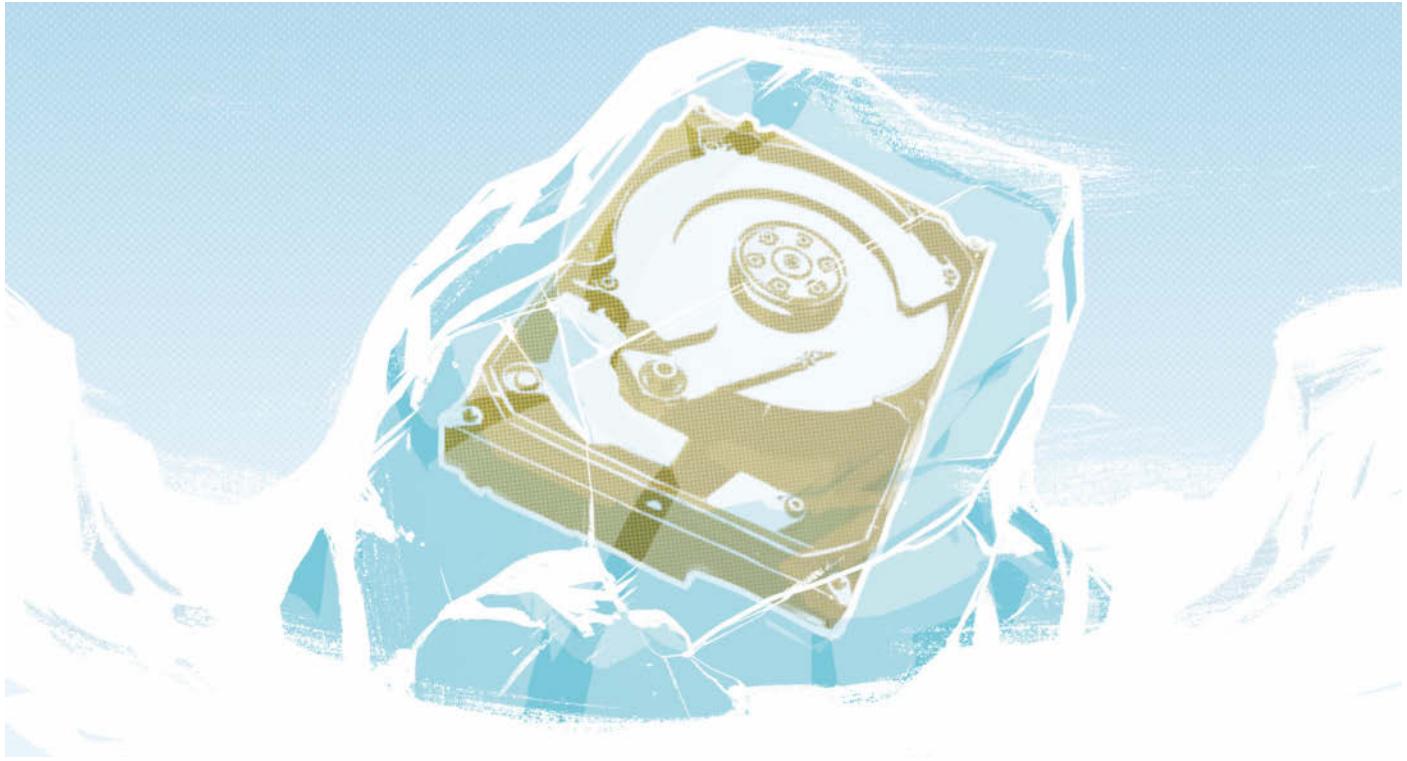


Bild: Albert Huhn

# Stabile Magnetpartikelchen

## Langzeitarchivierung mit Festplatten

**Festplatten sind wohl das beste Mittel, Daten für längere Zeit zu sichern. Sie sind vergleichsweise günstig und die Daten lagern an einem Platz, zu dem man den Zugang selbst kontrollieren kann.**

Von Lutz Labs

**E**ine USB-Festplatte dürfte in vielen Haushalten vorhanden sein, sei es als Backup-Platte oder zum Transport von Daten. Doch taugt eine solche Platte auch, um wichtige Daten über Jahrzehnte aufzubewahren?

Wir haben die drei verbliebenen Hersteller Seagate, Toshiba und Western Digital nach ihren Einschätzungen zur Eignung von Festplatten für die Langzeitarchivierung befragt. Insgesamt sind diese von der Langlebigkeit ihrer Produkte über-

zeugt, eine Garantie für die Lesbarkeit der Daten nach mehr als fünf Jahren möchten sie jedoch nicht geben.

Dennoch sind Festplatten wohl aktuell die beste Möglichkeit zur langfristigen Datensicherung – wenn man sich von der Wunschvorstellung verabschiedet, dass man das Archiv einmal anlegt und sich dann die nächsten 50 Jahre nicht mehr darum kümmern muss.

### Fortschrittstreiber

Festplatten haben in den vergangenen Jahren einige Entwicklungsschritte durchgemacht, die vor allem zu höheren Kapazitäten geführt haben. Dazu gehören unter anderem die Helium-Füllung und die Aufzeichnungstechnik Shingled Magnetic Recording (SMR). Auch unter der Haube gab es Fortschritte: empfindlichere Leseköpfe, rauschärmere Verstärker oder Two Dimensional Magnetic Recording (TDMR). Die letztgenannten Techniken tragen nur indirekt zur Kapazitätserhöhung bei, indem sie die Signalqualität beim Lesen der Magnetpartikel verbessern und damit den notwendigen Platz für die Speicherung

eines Bits verringern. Zudem wurden die Algorithmen zur Korrektur von Lesefehlern durch zusätzliche Informationen optimiert.

### Shingled Magnetic Recording

SMR ist eine Aufzeichnungsmethode, bei der der Schreibkopf einen Teil der gerade eben geschriebenen Spur wieder mit der nächsten überschreibt. Die so geschriebenen Spuren werden also etwas schmäler und es passen bis zu 20 Prozent mehr Bits auf die Scheiben.

Die Technik hat nach Ansicht der Festplattenhersteller keine Auswirkungen auf die Fähigkeiten der Laufwerke zur Langzeitarchivierung: Der Schreibkopf ist um ein Vielfaches größer als der Lesekopf, die verbleibende Spur bleibt immer noch deutlich breiter als der Lesekopf. Es werden also in jedem Fall mehr als genug Partikel magnetisiert, um auch auf lange Sicht die Bits sicher lesen zu können.

Wer der Sache dennoch nicht traut, muss aufpassen: USB-Festplatten im 2,5-Zoll-Format ab 4 TByte dürften allesamt mit SMR arbeiten, bei 3,5-Zoll-Laufwer-

ken ist die Sache allerdings deutlich unübersichtlicher. Dann hilft nur, bei den Preisvergleichern das Häkchen bei „Non-SMR“ zu setzen und sehr genau das Datenblatt zu studieren.

## Helium-Füllung

Eine Helium-Füllung der Gehäuse ist ein weiteres Mittel zur Kapazitätssteigerung. Das Edelgas hat eine geringere Reibung, damit sind dünnerne Scheiben möglich – und das wiederum erlaubt den Einbau weiterer Scheiben.

Manche befürchten, dass das Edelgas im Lauf der Jahre aus den Gehäusen herausdiffundiert. Die Hersteller aber sagen unisono, dass dies sehr selten passiere. Wenn Helium austrete, dann sei dies auf Mikrorisse im Gehäuse zurückzuführen. Doch selbst dann könnten Daten noch gelesen werden.

Western Digital misst den Helium-Gehalt anhand der Flughöhe des Kopfes. Sollte Helium austreten, also Luft eindringen, steigt die Flughöhe und das System wird über das SMART-Attribut 22 darüber informiert. In einem solchen Fall ist das Lesen der Sektoren weiterhin möglich, allerdings kann es beim Schreiben Probleme geben. Die Festplatte überprüft die geschriebenen Daten daher noch einmal, das aber kostet mindestens eine zusätzliche Umdrehung und reduziert damit die Schreibgeschwindigkeit. Seagate nutzt das SMART-Attribut 200 für die Ausgabe des Helium-Gehalts, Toshiba 23 und 24.

Helium-Laufwerke sind nach unserer Ansicht für die Langzeitarchivierung weniger gut geeignet. Sie sind auf eine Laufzeit von fünf Jahren ausgelegt. Ob das Gehäuse noch weitere Jahre dicht hält, ist unklar: Die Garantie ist abgelaufen, es muss den Hersteller nicht mehr interessieren. Aktuelle Seagate-Laufwerke mit 10 TByte oder mehr sind Helium-gefüllt, bei Toshiba und Western Digital beginnen die Helium-Serien bei 12 TByte. In USB-Platten können jedoch auch kleinere Laufwerke stecken, die mit Helium gefüllt sind.

## 1 bis 18 TByte

Wer mit einer Archivkapazität von 1 oder 2 TByte auskommt, kann zu einem 2,5-Zoll-Laufwerk greifen. Diese sind etwas besser gegen Stöße geschützt und benötigen zudem am USB-Anschluss keine zusätzliche Stromversorgung. Bei größerem Platzbedarf teilt man das Archiv auf mehrere 2,5-Zoll-Laufwerke auf oder nutzt Laufwerke im 3,5-Zoll-Format. Lauf-

werke unter 1 TByte sind zwar noch erhältlich, aber pro Terabyte relativ teuer.

## SATA vs. USB

Die meisten Festplatten haben einen SATA-Anschluss für den direkten Anschluss am Mainboard. In viele Rechner, seien es Notebooks oder Mini-PCs, passen sie nicht hinein: kein SATA-Port, kein Platz für 2,5-Zoll-Laufwerke, geschweige denn für die größeren 3,5-Zöller. Da der Trend zu immer kleineren Gehäusen geht, ist eine interne Festplatte als Archivmedium ungeeignet.

Toshiba rät zudem von der Lagerung einer mit Daten gefüllten internen Festplatte ab: Nicht nur, dass diese durch elektrostatische Einflüsse einen Defekt erleiden könnte, auch der Einbau sei relativ fehleranfällig.

Für ein privates Archiv nimmt man deshalb am besten eine externe Festplatte mit USB-Anschluss. Wie diese intern aufgebaut ist, ist zwar zweitrangig, aber dennoch interessant: Während Toshiba und Western Digital bei aktuellen 2,5-Zoll-Modellen den USB-SATA-Wandler bereits auf der Platine der Festplatte integrieren, nutzt Seagate dafür eine zusätzliche Platine. Seagate-Laufwerke lassen sich daher beim Defekt des Wandlers noch über einen Adapter auslesen. Besser ist es jedoch ohnehin, auch ein Archiv redundant zu speichern, also mindestens auch auf einer zweiten Platte; stammt letztere von

einem anderen Hersteller, verringert das das Risiko, dass ein Serienfehler beide Kopien unbrauchbar macht.

Für den USB-Anschluss spricht auch, dass dieser uns wohl noch eine ganze Weile begleiten wird; vielleicht nicht mit den heute bekannten Steckern, aber da wird es sicher Adapter geben. Ein weiterer USB-Vorteil ist der „Air Gap“: Ist die Platte nicht angeschlossen, kann auch kein böswilliger Prozess darauf zugreifen und Daten löschen. Zudem ist das eigentliche Laufwerk im Inneren seines Gehäuses vor elektrostatischen Entladungen (ESD) geschützt.

## Neu und alt

Ausgemusterte Festplatten aus alten PCs wandern in der Praxis häufig in USB-Gehäuse und finden fürderhin Verwendung als Backup-Laufwerke. Für ein (zusätzliches) Backup ist das völlig okay, für ein Langzeitarchiv hingegen absolut ungeeignet.

Zwar sollten die Lager der Laufwerke heute auch einen jahrelangen Stillstand überstehen, die Lagerschmierung kann aber immer noch ausharzen und das Anlaufen behindern. Das ist vor allem ein Problem, wenn man bereits lange genutzte Platten einlagert: Jahrelange Warm-Kalt-Wechsel bekommen dem Schmiermittel nicht gut.

Deshalb sollte man für sein Archiv ausschließlich neue Laufwerke verwenden.

ID	Parametername	Akt. Wert...	Schlecht...	Grenzwerte...	Rohwert (Einh...
01	Lesefehlerrate ↓	100	100	51	000000000000
03	Mittl. Anlaufzeit ↓	82	82	11	000000000182E
04	Start/Stop-Zyklen d. Spindel	85	85	0	0000000003CF1
05	Anz. wiederzugewiesener Sektoren ↓	100	100	10	000000000000
07	Anz. Suchfehler	100	100	51	000000000000
08	Güte der Schuhoperationen ↑	100	100	15	000000000000
09	Betriebsstunden	97	97	0	0000000003607
0A	Anz. ungelungener Spindelanläufe ↓	100	100	51	000000000001
0B	Ans. notwendiger Rekalibrationen ↓	100	100	0	000000000000
0C	Anz. Geräte-Einschaltvorgänge	86	86	0	00000000038FC
0D	Software-Lesefehleranteil ↓	100	100	0	000000000000
B7	Herstellerspezifisch	100	100	0	000000000003
BB	Ende-zu-Ende-Fehler ↓	100	100	0	000000000000
BC	Gemeldete unkorrigierbare Fehler ↓	100	100	0	000000000000
BE	Befehlszeitüberschreitung ↓	100	100	0	000000000000
C2	Temperatur ↓	84	58	0	0000100E0010
C3	Hardware-ECC wiederhergestellt	100	100	0	000000000F05B
C4	Wiederzuweisungsergebnisse ↓	100	100	0	000000000000
C5	Aktuell schwiebende Sektoren ↓	100	100	0	000000000000
C6	Nicht korrigierbare Sektoren ↓	100	100	0	000000000000
C7	UltraDMA-CRC-Fehler ↓	100	100	0	000000000000
C8	Schreibfehlerrate ↓	100	99	0	000000000025
C9	Software-Lesefehlerrate ↓	253	253	0	000000000000

**Die SMART-Werte der 1-TByte-Samsung-Festplatte in diesem Screenshot deuten nicht auf einen kommenden Ausfall hin. Dennoch sollte man diese 13 Jahre alte Festplatte allenfalls noch für das Backup des Backups verwenden.**



**SMART-Werte geben keinen Hinweis auf das Alter der Festplatte. Mit Kaufdatum und Inhalt beschriftet ist sie im Tresor gut aufgehoben.**

Wenn man bedenkt, welche Arbeit man sich mit der Auswahl der archivwürdigen Dateien macht, sollte man nicht bei der Hardware sparen – es lohnt sich nicht: Eine 2-TByte-Festplatte im praktischen 2,5-Zoll-Format bekommt man für 70 Euro.

## Lagerung

Zusätzlich zu den Hinweisen auf Seite 63 gilt für Festplatten natürlich, sie möglichst schonend zu behandeln. Auf Englisch lesen sich die wichtigsten Tipps dazu ganz knackig:

- Don't knock it!
- Don't stack it!
- Don't drop it!
- Don't zap it!

Auf Deutsch klingt das nicht so schön, meint aber natürlich das Gleiche: nicht stoßen, nicht stapeln, nicht fallen lassen und vor elektrostatischen Entladungen schützen.

Die Hersteller empfehlen für die Lagerung eine möglichst konstante Temperatur von 25 °C und eine Luftfeuchtigkeit um 40 Prozent. Bei normalen Festplatten kommt aber noch etwas hinzu: Die Luft sollte weder Staub noch irgendwelche Gase enthalten, auch wenn luftgefüllte Festplatten gegen das Eindringen von Fremdkörpern durch einen Luftfilter geschützt sind. Bei Helium-gefüllten Festplatten spielt das keine Rolle, da sie komplett versiegelt sind.

Seagate rät bei erhöhter Luftfeuchtigkeit noch zur Lagerung der Laufwerke in einer verschlossenen ESD-Tüte, um Korrosion vorzubeugen.

## Fünf Jahre und länger

Nach Angaben von Toshiba sollten die Daten auf einer nagelneuen und optimal gelagerten Festplatte eigentlich ewig halten; die Magnetisierung sei sehr, sehr

stabil. Das sei ähnlich wie bei Magnetbändern, und dort werde eine Haltbarkeit von 30 Jahren angenommen. Defekte könnten in dieser Zeit allerdings an Mechanik und Elektronik auftreten.

Daraus folgt ein Ratschlag aller Hersteller: Schließen Sie die Festplatte mindestens einmal im Jahr an den PC an, damit die Kondensatoren mal wieder geladen werden – auch, wenn durch Alterung ausfallende Kondensatoren inzwischen nicht mehr üblich sind. Dabei sollten Sie die Daten auch einmal von der Platte auf ein anderes Medium kopieren. Die Firmware der Platte merkt beim Lesen der Daten, ob es Probleme gibt und kopiert die Inhalte der betroffenen Sektoren dann in Reservebereiche – sofern die Korrekturmechanismen noch arbeiten. Wenn nicht, ergänzen Sie die betroffenen

Dateien aus einer anderen Quelle (Sie haben doch sicher ein Backup des Archivs).

Schauen Sie dabei auch auf die SMART-Werte der Festplatte: Deuten diese einen nahenden Ausfall an, kopieren Sie die Daten besser gleich auf eine neue Festplatte. Damit Sie einen Vergleich zu den SMART-Werten der Vorjahre haben, sollten Sie diese regelmäßig speichern. Die kostenlose SMART-Software CrystalDiskInfo ([ct.de/ymrw](http://ct.de/ymrw)) bietet dazu das Speichern der aktuellen Werte als Text- oder Bilddatei an.

Alle fünf Jahre kaufen Sie eine neue Festplatte, am besten gleich eine Nummer größer – auch das ist natürlich ein Rat der Hersteller. Kopieren Sie alles auf die neue Platte, aber behalten Sie die alte. Diese können Sie dann an einem anderen Ort lagern, um das Verlustrisiko noch weiter zu minimieren.

Jedes Jahr am 31. März ist World Backup Day, am 30. November Digital Preservation Day. Notieren Sie sich einen dieser Tage im Kalender und schauen Sie dann nach Ihren Daten. Kümmern Sie sich drum. Anders gehts nicht. [ll@ct.de](mailto:ll@ct.de) 

## Literatur

- [1] Boi Feddern, Vergissmeinnicht, Festplatten für die Langzeit-Datenarchivierung, c't 16/2008, S. 124

**Downloads:** [ct.de/ymrw](http://ct.de/ymrw)

## Schreibschutz gegen Trojanerangriffe

Wenn Sie Ihre Archivplatte an den PC stecken, um die Daten auf Lesbarkeit zu prüfen, müssen Sie nicht auf die Platte schreiben. Und wenn die Festplatte schreibgeschützt ist, kann auch kein Trojaner an die Daten heran. Unter Linux kann man Laufwerke einfach im Nur-Lese-Modus mounten, unter Windows hilft das Kommandozeilenutility diskpart. Den Schreibschutz richten Sie am besten gleich nach dem Kopieren der Daten auf die Platte ein. Dazu starten Sie das Programm mit Administratorrechten und lassen sich mittels

`list volume`

die vorhandenen Partitionen anzeigen. Wählen Sie dann über

`select volume 1`

zum Beispiel die Partition mit der Nummer 1 aus. Der Befehl

`attribute volume set readonly`

versetzt sie in den schreibgeschützten Modus. Die Festplatte merkt sich diesen Status. Mittels

`attribute volume clear readonly`

entfernen Sie den Schreibschutz wieder. Statt einer Partition können Sie auch ganze Laufwerke mit einem Schreibschutz versehen, ersetzen Sie dazu `volume` durch `disk`.

Es gibt **10** Arten von Menschen.  
iX-Leser und die anderen.



**Jetzt Mini-Abo testen:**  
3 Hefte + Bluetooth-Tastatur  
nur 16,50 €

[www.iX.de/testen](http://www.iX.de/testen)



[www.iX.de/testen](http://www.iX.de/testen)



49 (0)541 800 09 120



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



MAGAZIN FÜR PROFESSIONELLE  
INFORMATIONSTECHNIK

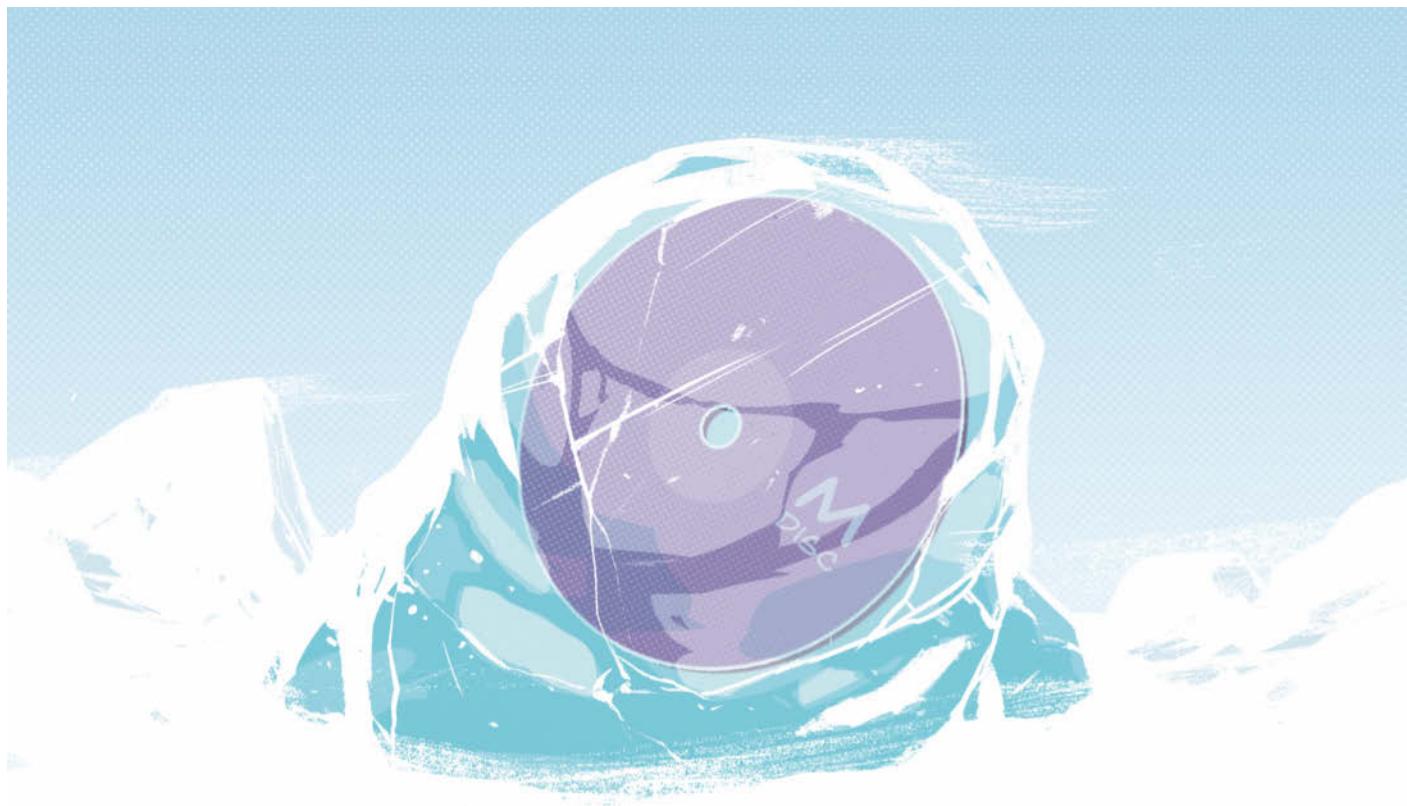


Bild: Albert Hulm

# Elektronische Steintafeln

## Die M-Disc als Langzeitarchiv

**Selbst gebrannte Blu-ray-Discs und DVDs sind als Langzeitarchiv nicht geeignet, weil sie sich in 20 oder 30 Jahren wahrscheinlich nicht mehr lesen lassen. Die M-Disc hingegen soll 1000 Jahre halten – verspricht zumindest der Hersteller.**

**Von Lutz Labs**

**S**ilberscheiben mit Daten sind ja irgendwie 80er: Langsam, umständliche Handhabung, geringe Kapazität, und die Haltbarkeit der Daten ist auch eine große Frage. Dennoch archivieren einige Anwender auch heute noch ihre

Daten auf DVD oder Blu-ray Disc (BD). Und auch wenn sie genauso aussieht: Die M-Disc ist anders, denn sie soll deutlich länger halten.

Die M-Disc ist eine Gemeinschaftsentwicklung des längst insolventen Unternehmens Millenita und Verbatim, einem Unternehmen, das seit vielen Jahren CD-, DVD- und BD-Rohlinge produziert. Das M im Namen steht für Millennium, also Jahrtausend – so lange sollen die Daten darauf halten.

Die erste M-Disc mit einer Kapazität von 4,7 GByte – also eine DVD – hatten wir 2012 im Test [1]. Die Brennergebnisse waren so katastrophal, dass wir uns die später erschienenen BD-Rohlinge gar nicht mehr angeschaut haben. Nun aber wollten wir noch einmal wissen, ob es sich auch heute noch lohnen könnte, auf Silberscheiben als Archivträger zu setzen. Im-

merhin lassen sich diese nicht nachträglich verändern, sind also trojanersicher.

Aufwendiges Testequipment ist für einen ersten Test nicht notwendig; viele BD-Brenner können auch die M-Disc beschreiben, obwohl sie einen stärkeren Laserstrahl benötigt: Die Daten werden, zumindest laut Werbeaussage, quasi in Stein gemeißelt. Die Speicherschicht soll deutlich resistenter gegenüber hoher Temperatur und Luftfeuchtigkeit sowie UV-Licht sein als die einer üblichen DVD oder BD-R. Mit diesen teilt sich die M-Disc also nur das Format, nicht aber die Chemie.

### **Von 4,7 zu 100 GByte**

Die größten Blu-ray-Scheiben fassen heute 100 GByte, vier Lagen à 25 GByte. Größere Kapazitäten, wie sie vor diversen Jahren angekündigt wurden, sind nie er-



Für die Langzeitarchivierung sind nur BD-Rohlinge mit M-Disc-Logo geeignet.

schienen. 500 GByte, gar 1 TByte sollten kommen – damit wäre das Medium vielleicht noch nicht so tief in der Versenkung verschwunden.

Größere optische Medien gibt es durchaus: Sony und Panasonic haben zusammen die Archival Disc entwickelt, die 2015 mit zunächst 300 GByte großen Scheiben auf den Markt kam. Die aktuelle, im vergangenen Jahr vorgestellte Version speichert 5,5 TByte auf einer Cartridge aus 11 Scheiben. Allein das Laufwerk aber kostet knapp 10.000 Euro.

Ein M-Disc-fähiger Blu-ray-Brenner ist deutlich günstiger, er kostet weniger als 100 Euro und die Medienpreise liegen bei rund 16 Cent pro GByte. Ein 25-GByte-M-Disc-Rohling kostet 3,40 Euro, ein 50er 7,70 Euro, ein 100er 13,50 Euro. Teurer sind die DVD-Rohlinge, für die man etwa 2,20 Euro bezahlen muss, 50 Cent pro GByte. Selbst wenn man mit der DVD-Kapazität auskommen würde und sich auch mit den Kosten arrangieren kann: Verbatim hat die Produktion der DVD-Rohlinge bereits eingestellt, beim Neukauf eines Brenners sollte man daher auf jeden Fall zu einem Blu-ray-Modell greifen.

Ein Test von Rohlingen ohne die Überprüfung der Brennqualität ist wertlos – erst recht, wenn es um die Langzeitarchivierung geht. Wir nutzen in diesem Test die Software Opti Drive Control (Download über ct.de/yne1), die die Rohdaten aus bestimmten Laufwerken auslesen kann – nicht aus vielen, und aktuelle sind auch nicht darunter. Daher mussten wir die vierlagigen M-Discs mit 100 GByte aus dem Test herausnehmen: Es gibt keine Möglichkeit, deren Brennqualität zu überprüfen. Ein einfacher Binärvergleich mit den Ursprungsdaten reicht nicht aus, weil dabei Fehler erst auffallen, wenn die Fehlerkorrekturmöglichkeiten des Laufwerks versagt haben.

Da wir die DVDs mangels Zukunftsfähigkeit weglassen und die zweilagige 50-GByte-M-Disc ebenfalls nicht mehr produziert wird, beschäftigen wir uns im Folgenden ausschließlich mit den 25-GByte-Medien. Im Prinzip sollten sich die Ergebnisse auf die größeren Medien

übertragen lassen, die Datensicherheit wird nach Angaben von Verbatim durch die Mehrlagentechnik nicht beeinträchtigt.

### So wie früher

Blu-ray-Brenner haben seit geraumer Zeit nichts mehr dazugelernt: Sie brennen Scheiben bis 100 GByte. Laut früheren Medien-Tests macht der Brenner kaum einen Unterschied bei der Brennqualität. Wir haben daher für die Tests einen Brenner von Verbatim benutzt; Verbatim als der Hersteller der M-Disc sollte die Medien am besten kennen. Interessanterweise steckt in dem USB-Gehäuse ein Pioneer-Laufwerk.

Der Autor musste sich beim Test erst einmal wieder an die Geschwindigkeit eines Blu-ray-Laufwerks gewöhnen: Während eine schnelle PCIe-SSD wie die Samsung 980 Pro mit Schreibgeschwindigkeiten von 5 GByte/s protzt, nimmt ein Blu-ray-Laufwerk die Daten mit nicht einmal 20 MByte/s entgegen – Faktor 250 langsamer. Wer große Datenmengen archivieren möchte, sollte also viel Zeit einplanen.

### Burn it

Mit der passenden Software – beim Verbatim-Laufwerk lag eine ältere Version von Nero Burning ROM Essentials bei – ist das

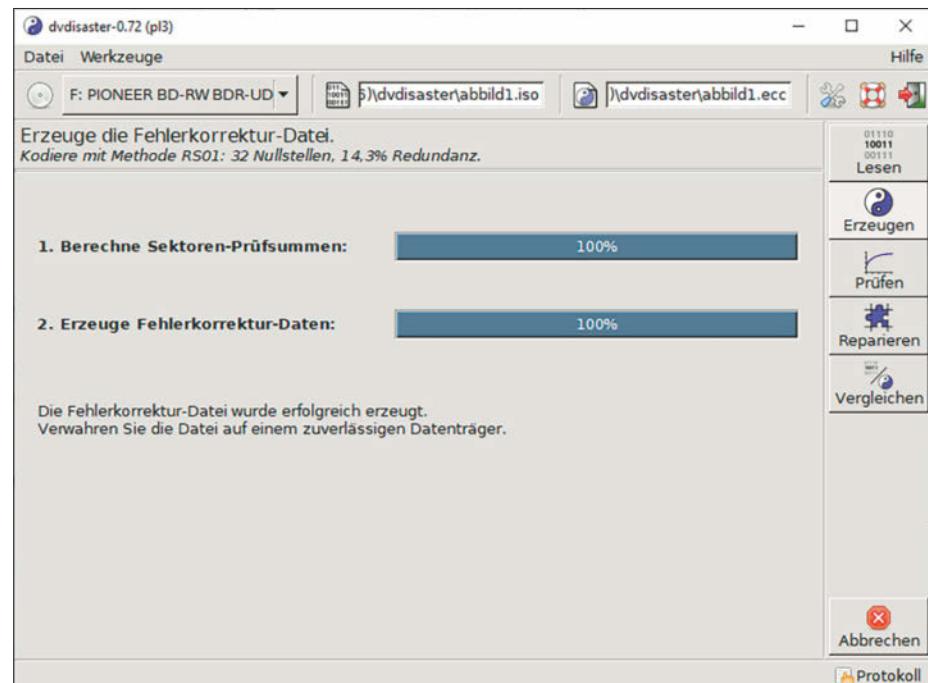
Brennen einer Blu-ray ein Kinderspiel: Dateien auswählen, Brenn-Knopf drücken, warten, fertig.

Bei der Langzeitarchivierung sollte man aber noch zwei Aspekte bedenken. Zum einen beginnt der Zerfall der Medien meistens vom Rand her; diese Spuren werden aber nur bei randvollen Scheiben benutzt. Lässt man etwas Luft, dann steigt die Datensicherheit.

Zum anderen kann man über zusätzliche Fehlerkorrekturdaten die Datensicherheit erhöhen. Solche Dateien erstellt etwa das kostenlose DVDisaster; das in der Standardeinstellung zu einem Datensatz von 20 GByte eine knapp 3 GByte große Fehlerkorrekturdatei erstellt. Diese könnte man zusammen mit einem weiteren Satz Daten auf die nächste BD brennen, davon wieder eine Fehlerkorrekturdatei erstellen und so weiter. Lässt man zusätzlich noch etwas Platz auf den Scheiben, steigen die Chancen auf ein erfolgreiches Lesen der Daten auch in vielen Jahren. DVDisaster sollten Sie dann aber auch mindestens zweifach in das Archiv übernehmen: Sie brauchen die Software später, um defekte Dateien über die Korrekturdaten zu reparieren.

### Check it

Übliche Brennprogramme bieten an, gleich nach dem Schreiben einen Verify-



Reichert man die Daten mit Fehlerkorrekturdaten von DVDisaster an, steigen die Chancen auf die Lesbarkeit in ferner Zukunft.

Lauf anzuhängen. Dabei werden die Daten Bit für Bit verglichen – jedoch nur die Daten, die das Laufwerk liefert. Wie viele Datenfehler das Laufwerk selbst schon korrigiert hat, geht aus dem Vergleich nicht hervor. Daher liefert ein einfaches Verifying wenig Aussagen für die Lagerfähigkeit.

Zur Überprüfung der Brennqualität braucht man nicht nur eine Software, die auf die Daten des Laufwerks zugreift, bevor dessen Fehlerkorrektur diese ausgebessert hat. Man braucht zudem auch ein Laufwerk, dass den Zugriff darauf erlaubt. Während es bei der Software noch einfach ist – wir haben das oben schon erwähnte Opti Drive Control benutzt – ist die Beschaffung eines passenden Laufwerks deutlich schwieriger. Der Programmierer von Opti Drive Control nennt gerade einmal drei Blu-ray-Laufwerke, die die Rohdaten herausgeben: die Lite-On-Modelle DH-401S, iHES106 und iHES208, alle älter als 10 Jahre. Auf eBay haben wir keines der Modelle gefunden, zum Glück aber ein DH-401S in unserem Archiv. Vor einigen Jahren gab es noch spezielle Prüflaufwerke für diesen Zweck – ob diese noch lieferbar sind, haben wir nicht herausfinden können. Preislich lagen diese eh deutlich über dem, was man als Privatanwender für ein Blu-ray-Laufwerk ausgeben möchte.

Opti Drive Control gibt nach der Analyse einer Blu-ray-Disk eine Kurve sowie zwei Werte aus: Long Distance Code (LDC) und Burst Indicator Subcode (BIS).

Bei LDC-Werten unter 15 sowie BIS-Werten unter 13 spricht man von einem guten Brand.

Die BIS-Werte waren bei allen Tests unauffällig, sie lagen immer unter 1. Bei den LDC-Werten aber kamen wir insgesamt nur auf einen Durchschnitt von 19. Bei vielen Blu-rays lag der LDC-Wert zwischen 10 und 15, drei Scheiben mit Werten von 34, 42 und 45 trieben den Durchschnitt hoch. Bei den Tests kamen verschiedene PCs mit Intel- und AMD-CPUs zum Einsatz, auf dem AMD-System entstanden zwei der extrem schlechten Brände, einer auf dem Intel-System – daran kann es also nicht liegen. Eine Erklärung für die unterschiedliche Brennqualität haben wir nicht.

Versuche mit unterschiedlichen Brenngeschwindigkeiten brachten keine Unterschiede beim Brennergebnis. Opti Drive Control bietet zudem an, die Medien mit geringerer Geschwindigkeit auszulesen, aber auch dies hatte keinen nennenswerten Einfluss auf die Fehlerrate.

## Store it

Noch ein Hinweis zur Lagerung der Blu-rays: Diese sollten, wie auch Festplatten, bei Raumtemperatur und einer Luftfeuchtigkeit von rund 40 Prozent aufbewahrt werden. Die DVD-Tütchen aus Papier mit Kunststofffenster, wie man sie gelegentlich in Zeitschriften findet, sind für die Langzeitarchivierung nicht geeignet, da deren Weichmacher die Medien schädigen kann. Nutzen Sie besser Je-

wel-Cases oder übliche DVD-Boxen und lagern sie die Medien möglichst in der Dunkelheit; Schublade oder Schrank sind ausreichend.

## Brauchbar für die Langzeitarchivierung?

Eine Haltbarkeit von 1000 Jahren wäre toll. Ob aber in nur einem Zehntel der Zeit, also in 100 Jahren, noch passende Laufwerke, Anschlüsse und Betriebssysteme verfügbar sind? Zum Konzept eines digitalen Archivs gehört die regelmäßige Prüfung der Daten, damit man sie vor einem eventuellen Datenverlust auf ein frisches Medium übertragen kann. Die allermeisten Anwender haben jedoch kaum die Möglichkeit, die Fehlerraten der gebrannten Scheiben zu ermitteln.

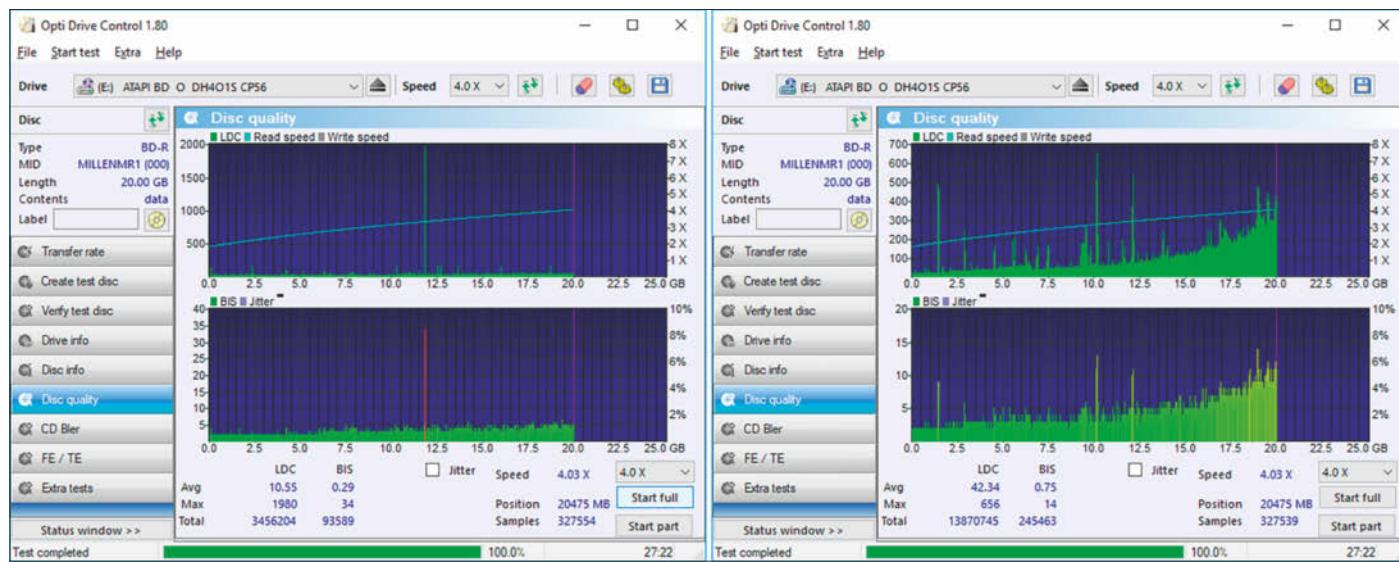
Als alleiniges Archivmedium ist die M-Disc unserer Ansicht nach nicht geeignet. Wer die Hoheit über seine Daten behalten möchte und die Ablage in der Cloud ablehnt, kann sein Archiv zusätzlich auch – und keinesfalls ausschließlich – auf M-Disc brennen. Man muss dabei dann jedoch blind darauf vertrauen, dass die Daten in ein paar Jahren noch lesbar sind.

(ll@ct.de) 

## Literatur

- [1] Hartmut Gieselmann, In Stein gebrannt, c't 12/2011, S. 62

**Download Hilfsprogramme:** [ct.de/yne1](http://ct.de/yne1)



**Ein guter Brand, ein schlechter Brand:** Während die BIS-Werte beim Test unauffällig blieben, lagen die LDC-Werte zwischen 10 und 42 – oberhalb von 15 spricht man von einem eher schlechten Brand.



# storage2day

ONLINE

Sichern Sie sich jetzt noch 1 von  
insgesamt 3 Herbst-Terminen!

DIE KONFERENZ ZU SPEICHERNETZEN UND DATENMANAGEMENT



Mittwoch, 23. September:  
Storage Security & Backup Day

Mittwoch, 7. Oktober:  
Storage-Trends und -Lösungen

Donnerstag, 12. November:  
Ceph Day

Thementag-Sponsor



[www.storage2day.de](http://www.storage2day.de)

Goldsponsoren



Silber- und Security-Day-Sponsor



Veranstalter

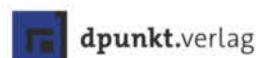




Bild: Albert Hulm

# Auf Eis gelegt

## Daten langfristig in der Cloud sichern

**Cloud-Speicher gilt vielen als Fremdkörper unter den Archivierungsoptionen. Dabei kommen große Unternehmen längst nicht mehr ohne die Langzeitspeicher von Amazon, Microsoft oder anderen großen Cloud-Betreibern aus. Cloudstorage kann eine Archivierungsstrategie sinnvoll ergänzen.**

**Von Holger Bleich**

**B**ei der langfristigen Archivierung digitaler Daten spielen Faktoren wie Medienhaltbarkeit, Temperatur und Lagerort eine große Rolle. Man muss sich damit aber nicht zwangsläufig auseinandersetzen, um die am besten geeigneten Methoden für den eigenen Zweck zu finden. Denn es gibt Anbieter, die diesen Job übernehmen: die Betreiber von Cloud-Speicher.

Cloudstorage lässt sich in diesem Sinne vielleicht als Meta-Medium beschreiben: Zu sichernde Daten gelangen über das Internet an eine definierte Adresse. Hinter dieser Adresse verbirgt sich aber kein konkreter Speicherort, etwa ein bestimmtes Storagesystem in einem Serverrack eines Rechenzentrums. Wo genau die dem Cloudbetreiber anvertrauten Daten liegen, weiß nur dieser selbst. Daraus ergibt sich, dass man bei der Langzeitarchivierung in der Cloud eben nicht dem Medium, sondern dem Betreiber vertrauen muss.

Die Vorteile von Cloudstorage liegen auf der Hand: Alle Archivdaten liegen räumlich getrennt von ihren Originalen. Wohnungsbrände oder andere Katastrophen können den Kopien nichts anhaben – vergleichbar mit der Festplatte im Bankschließfach. Man kann davon ausgehen, dass jeder seriöse Cloudstorage-Anbieter mindestens eine Redundanzebene vorhält – sei es als Hardware-RAID, gespiegelte Storage-Arrays oder in Form von Tape-Kopien.

Der Betreiber als Vertragspartner übernimmt in dem Moment die Verant-

wortung für die Daten, in dem er sie annimmt. Abgestufte Garantien dafür finden Sie übrigens als Privatkunde in den Allgemeinen Geschäftsbedingungen (AGB) und als Geschäftskunde in der Regel im Service Level Agreement (SLA). Meist ist in diesen Vertragsergänzungen auch die aufs Jahr hochgerechnete Verfügbarkeit der gespeicherten Daten garantiert. Hält der Betreiber diesen Prozentwert nicht ein, macht er sich schadenersatzpflichtig.

Allerdings hilft das eher wenig, wenn materiell oder ideell extrem wertvolle Datenarchive in der Cloud flöten gehen, was durchaus schon vorgekommen ist. Deshalb gilt: Cloudstorage darf nie der einzige Baustein einer Archivierungsstrategie sein, sondern dient als Ergänzung.

### Flaschenhals Internet-Zugang

Im Vergleich zu räumlich getrennt gelagerten Datenträgern bietet die Cloud einen weiteren Vorteil: Das Langzeitarchiv ist von überall aus verfügbar. Auch das Zugriffs-Device spielt keine Rolle, weil nicht etwa veraltete Buchsen oder Bussysteme

eingesetzt werden, sondern jeweils aktuelle Internet-Protokolle und Transportverschlüsselungen.

Der ausschließliche Zugriff via Internet bringt allerdings auch mit, dass man abhängig vom eigenen Zugang und der Verfügbarkeit des Betreibers ist. Gerade im Privatbereich stellt der Internetanschluss zu Hause einen Flaschenhals dar, der das Hochladen großer Archivbestände zur Geduldsprobe machen kann.

Dies gilt besonders, wenn das Archiv, wie es üblich ist, auch Multimediateile wie Fotos und Videos umfasst. Für diesen Artikel haben wir einmal defensiv mit einer Archivgröße im Bereich von 100 GByte experimentiert. Geht man bei einem VDSL-Anschluss von 10 MBit/s Upload-Bandbreite aus und nutzt diese komplett aus, dauert es rund 23 Stunden, um dieses Archiv in den Cloudstorage zu übertragen.

Das Gute ist: Da in aller Regel die Download-Bandbreite vielfach höher ist, kommt man umgekehrt schneller ans Archiv. Beim Download mit 50 MBit/s dauert es bei 100 GByte Archivgröße etwa 4,5 Stunden. Allerdings verfügt längst nicht jeder Haushalt über eine VDSL-Leitung. Außerdem können auch andere Faktoren die Übertragung ausbremsen, etwa eine Drosselung auf Anbieterseite.

## Konsumenten-Clouds

Privateute denken bei Cloudspeicher vorwiegend an Apples iCloud, Google Drive oder Dropbox. Solche Angebote dienen allerdings in erster Linie als ausgelagerte Ergänzung zum im Smartphone verfügbaren Speicher und zum Austausch von Dateien zwischen Geräten und Nutzern. In den kostenfreien Versionen stellen sie ohnehin zu wenig Speicherplatz bereit, um als Archiv in Frage zu kommen.

Mitunter lassen sie sich aber kostengünstig erweitern. So kostet es 10 Euro monatlich, Google Drive von 15 GByte auf 2 TByte aufzurüsten. Es bleibt dennoch die Frage, ob man auf kurz- und mittelfristige Speicherung ausgelegten Cloudstorages für Konsumenten sein Langzeitarchiv anvertrauen will.

Auf Datenschutz und Vertraulichkeit sollte man bei Google, Apple & Co. nicht unbedingt setzen. Dass Google hochgeladene Daten maschinell auswertet ist bekannt, und wie bei iCloud gespeicherte Fotos in fremde Hände gelangen, haben in jüngerer Vergangenheit mehrere „Fapenings“ belegt. Wer sein Archiv in

**Strato betreibt seine HiDrive-Cloud mit RAID-Arrays, die den Festplattentausch ohne Datenverlust im laufenden Betrieb erlauben.**



Bild: Strato

US-amerikanische Cloudstorages auslagert, sollte die Daten unbedingt zuvor verschlüsseln (siehe Artikel auf S. 60).

Aus Datenschutzgründen sind deutsche Anbieter die bessere Wahl. Eine allzu große Auswahl an vertrauenswürdigen, lange am Markt agierenden Anbietern gibt es allerdings nicht. Für die Langzeitarchivierung größerer Datenbestände eignet sich beispielsweise HiDrive, der Cloudspeicher von Strato. Auch hier zahlt man monatlich für eine definierte Speichergröße. 1 TByte etwa kostet 7,50 Euro pro Monat, 3 TByte schlagen mit 18 Euro zu Buche – und zwar egal, ob und wie viel man das Angebot nutzt. Übrigens bietet auch die Konzernschwester Ionos Stratos HiDrive an – für etwas mehr Geld.

HiDrive taugt im Vergleich zu den meisten anderen Produkten besser als Langzeitarchiv, weil es mehr sinnvolle Schnittstellen bietet als der Mitbewerber. So lässt es sich nicht nur via WebDAV oder API befüllen, sondern auch über rsync mit dem heimischen NAS-Speicher synchronisieren oder über SFTP und SMB/CIFS erreichen. Der NAS-Hersteller Synology bietet außerdem eine eigene HiDrive-Backup-App für sein Betriebssystem an. Nach Angaben von Strato verzeichnete HiDrive 2019 eine Verfügbarkeit von 99,99 Prozent, garantiert sind 99 Prozent.

Am Beispiel HiDrive lässt sich trefflich diskutieren, ob Konsumenten-Cloudstorage für die Langzeitarchivierung sinnvoll sein kann. Immerhin 90 Euro kostet das 1-TByte-Archiv jährlich. Aber ist es auch langfristig sicher? Dass kann leider niemand garantieren. HiDrive gibt es als eigenständiges Angebot seit 10 Jahren, den Provider Strato wesentlich länger. Aber wird das Produkt auch die nächsten 10 Jahre überleben? Oder gar die nächsten 30?

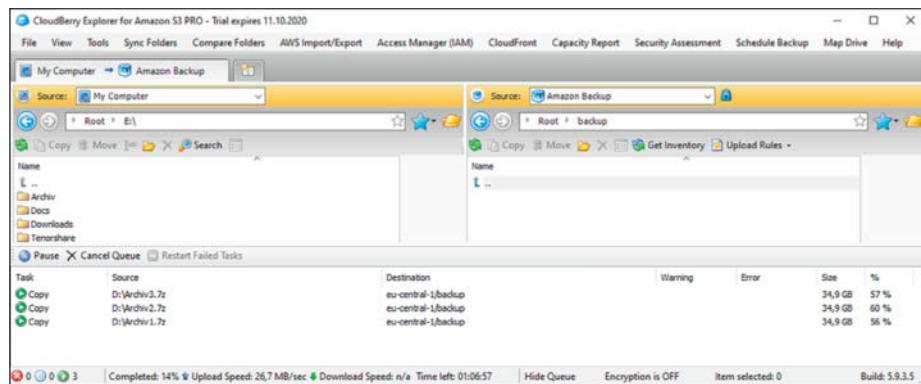
## Cold Storage

Im Business-Bereich hat sich Cloudstorage als Alternative zur lokalen Archivierung von Daten längst durchgesetzt. Das ist angesichts des enormen Speicherbedarfs auch kein Wunder: Ob massenhaft anfallende Sensordaten oder bildgebende Verfahren in der Medizin, Unternehmen müssen für massenhaft unstrukturierte Daten in hohem Tempo Redundanz schaffen. Da sie diese Daten oft ohnehin in der Cloud verarbeiten, bietet es sich an, sie auch dort zu speichern – denn Daten lassen sich in derselben Cloud vergleichsweise schnell übertragen.

Cloudbetreiber haben auf die Bedürfnisse der Industrie reagiert und bieten Storage in verschiedenen Kategorien an: So genannter „warmer“ Speicher ist auf niedrige Latenz, hohe Geschwindigkeit und häufigen Zugriff ausgelegt. Möchte man die Daten häufig ein- und auslesen sowie verarbeiten, ist das der richtige Ablageort.

Je tiefer es in den Archivbereich geht, desto kälter wird es. Daten, die nur selten angetastet, aber verfügbar bleiben sollen, speichern große Cloudbetreiber nicht mehr blockweise ins Dateisystem, sondern behandeln sie als verschiebbare Objekte mit eindeutigen Identifizieren. So kann es etwa sein, dass die Cloud den angelegten Datentresor (Vault) als Objekt aus dem Platten-Array in ein anderes Rechenzentrum oder gleich ins Tape-Archiv verschiebt, wenn er Monate lang nicht abgerufen wurde.

Als weltweit größter Cloudbetreiber gab Amazon innerhalb seiner Amazon Web Services (AWS) 2012 den Startschuss für sogenannten „Cold-Storage“ und benannte das Produkt passenderweise „S3 Glacier“. Später folgte Microsoft dem Beispiel und hob mit „Azure Cool Blob Storage“ ein ähnliches Angebot aus der Taufe.



Cloudberry Explorer lädt Archivdaten parallel zu AWS Glacier hoch.

Im vergangenen Jahr folgte „Google Coldline“. Beim französischen Cloud-Betreiber OVH heißt es „Cloud Archive“, und auch die Telekom Open Cloud und die Ionos Cloud haben ähnlichen objektorientierten Speicher im Sortiment.

Wie in den Business-Clouds üblich verfolgen die Betreiber ein streng nutzungsorientiertes Abrechnungsmodell, ganz anders als es bei den Konsumenten-Clouds üblich ist. Erfreulicherweise bezahlt man nur genau für das, was man auch nutzt.

Bei Cold Storage setzen sich die Kosten meist aus mindestens drei Komponenten zusammen: Für die Lagerung im kalten Archivkeller der Cloud zahlt man einen recht geringen Betrag pro Monat und GByte. Dafür kostet aber jeder Zugriff darauf extra – je nachdem, wie schnell die Antwort kommen muss. Möchte man ein Archiv hoch- oder herunterladen oder auch ergänzen, schlägt außerdem das Datenübertragungsvolumen zu Buche – ganz, als würde man den Archivar aus dem Keller rufen und ihn bitten, diese zehn Aktenordner herunterzuschleppen und einzumotten.

### Beispiel Glacier

Amazon Glacier wird von großen Unternehmen genutzt, um ihre in Amazons S3-Storage aufgelaufenen Daten dauerhaft wegzusichern. Der Anbieter versichert, dass alle Glacier-Archive redundant und physisch getrennt an drei Standorten innerhalb einer „AWS-Region“ gespeichert werden, die sich auswählen lässt. Eine AWS-Region ist beispielsweise EU-Frankfurt. Die Daten verbleiben in diesem Fall also in Deutschland, unterliegen aber dennoch potenziell dem Zugriff des US-amerikanischen Geheimdienstes, weil Amazon ein in den USA beheimateter Konzern ist.

Ein einzelnes Archiv darf bis zu 40 TByte groß sein. Amazon empfiehlt, Dateien zu packen und als Archivdatei hochzuladen. Der Zugriff auf Glacier erfolgt über AWS-APIs. Eine Web-Oberfläche, wie man sie von den Konsumenten-Clouds gewohnt ist, existiert nicht. Dies, kombiniert mit der schwer durchschaubaren Preisstruktur, dürfte Nutzer ohne AWS-Erfahrung abschrecken.

Doch gerade für Glacier existieren mittlerweile eine Reihe von Clients, die den kalten Speicher sehr einfach zugänglich machen, indem sie die API-Sprache in grafische Drag-&-Drop-Kommandos übersetzen. „Fast Glacier“ war das erste dieser Tools. Am besten gefallen uns aber die Produkte von Cloudberry. Der Hersteller ist bekannt für seine Backup-Software.

Interessanter für die Archivierung von Dateien ist aber der „Cloudberry Explorer“. Das für Windows und macOS verfügbare Tool bindet nach Angabe der Account-Schlüssel einen existierenden Glacier-Account in seine FTP-ähnliche Umgebung ein und erlaubt Up- und Downloads direkt aus dem angegebenen Glacier-Vault. Funktionsfähig ist es bereits als Freeware, die Pro-Version für knapp 50 US-Dollar beherrscht On-the-fly-Verschlüsselung, parallel laufende Up- und Downloads und weitere Protokolle wie SFTP.

In unseren Tests klappte die Verbindung zu Glacier reibungslos, nachdem wir uns ein AWS-Konto und einen Glacier-Vault angelegt hatten. Up- und Downloads von 35 GByte großen Archivdateien nutzten die volle Bandbreite der 250-MBit/s-Leitung im glasfaserbundenen Zuhause.

Im Beispiel haben wir 105 GByte ins Glacier-Vault (AWS Frankfurt) geladen (9,45 US-\$ netto). Dafür waren 13 API-Operationen nötig (0,81 US-\$ netto). Für jedes empfangene GByte erhebt Amazon eine

„Retrieval Fee“ von 0,012 US-\$ (zusammen also 1,26 US-\$ netto). Die Speicherung von 1 GByte Daten kostet in der Glacier-Region Frankfurt 0,0045 US-\$ pro Monat (0,47 US-\$ netto). Brutto hat uns also der Upload inklusive den ersten Monat Archivierung rund 12 Euro gekostet.

Dafür liegen die Daten nun in einem dreifach redundanten Archivspeicher auf deutschem Boden. Und der Clou: Solange sie man dort ruhen lässt, kostet jeder weitere Monat weniger als 50 Cent. Bei 1 TByte wären es 5 Euro und damit immer noch wesentlich weniger als bei den Konsumenten-Cloudstorages. Vor allem aber: Der Speicher skaliert und kann problemlos auch Dutzende TByte Archiv verkraften.

Beachten sollte man: Entsprechend der Speicherung kostet auch jede Rückholaktion des Archivs in etwa so viel Geld wie die Einlagerung. Bis die Daten per „Standardarchivabruf“ zum Download bereitstehen, vergehen außerdem drei bis fünf Stunden. Der „beschleunigte Datenabruf“ kostet noch einmal extra.

### Fazit

Cloudstorage eignet sich prinzipiell prima zur ergänzenden, langfristigen Ablage von Archivdaten. Wer nur wenige GByte speichern möchte, kommt mit dem günstigen Angebot von Google gut zurecht. Unverschlüsselt sollte man aber US-Konzernen grundsätzlich keine persönlichen Daten wie Fotos, Urkunden oder Rechnungen anvertrauen. Insbesondere gilt dies für Daten von fremden Personen, da hier auch Verletzungen von Datenschutz- und Persönlichkeitsrechten im Raum stehen. Besser ist es da, einen deutschen Cloudanbieter wie Strato mit seinem HiDrive zu wählen. Für pauschal 90 Euro pro Jahr erhält man 1 TByte Archivspeicher, der sich dank umfangreicher Protokollunterstützung gut nutzen lässt, aber auch als Alltagscloud zur Verfügung steht.

Angebote wie Amazon AWS Glacier scheinen nur auf den ersten Blick Profis vorbehalten zu sein. Mit entsprechender Software werden sie auch für den normalen Nutzer zugänglich, allerdings ändert das nichts am undurchschaubaren Kostenmodell. Sie sind besonders sinnvoll, wenn es um die langfristige Archivierung großer Datenmengen, etwa Raw-Fotografien oder HD-Filmmaterial, geht.

(hob@ct.de) 

**Erwähnte Angebote und weitere Infos:** [ct.de/yp2j](http://ct.de/yp2j)

Exklusiv  
im heise shop!

# Back to BASIC

+ Nano-Axe-  
Board mit  
PICAXE-08M2



## Make Picaxe Special

Noch einfacher als Arduino: Im neuen PICAXE Special der Make dreht sich alles um den Einstieg ins Programmieren mit BASIC. Dazu gibt es ein neu entwickeltes Programmierboard für den Einsatz von PICAXE-Chips, das Nano-Axe-Board mit USB-Anschluss. Damit können Sie sofort starten!

[shop.heise.de/make-picaxe](http://shop.heise.de/make-picaxe)

Einzelheft  
für nur

24,95 € >

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.



heise shop

[shop.heise.de/make-picaxe](http://shop.heise.de/make-picaxe)

# Vorlauter Zwerg

## Asrock Deskmini X300 für Ryzen 4000G

**Mit neuem BIOS macht Asrock die bekannte Hardware in Form des sparsamen Deskmini X300 fit für Ryzen 4000G und erlaubt sogar das Übertakten im Mini-Gehäuse. Es ist zudem das erste X300-System überhaupt.**

Von Carsten Spille

Asrock verbessert den Mini-Barebone Deskmini im Detail, doch die aktuelle Variante X300 bleibt grundsätzlich den Tugenden, aber auch den Schwächen der Reihe treu. Im November soll der milchkartongroße Tausendsassa in den Handel kommen – einen konkreten Preis nannte der Hersteller nicht. Der Vorgänger A300, der auch die Basis des c't-Bauvorschlags für einen 7-Watt-PC bildet, ist zurzeit für etwa 125 Euro zu haben [1,2]. Man sollte mit etwa 30 Euro Aufpreis für den X300 gegenüber dem A300 rechnen. Beim Deskmini-Barebone sind Mainboard, Gehäuse und Netzteil vorhanden, Prozessor, Speicher und SSD muss man selbst beisteuern.

Der X300 ist auch für die aktuellen AM4-Ryzen-Kombiprozessoren aus der 4000G-Reihe ausgelegt. Die gibt es derzeit nur als „Pro“-Version mit bis zu acht Kernen – wir haben für den Test sowohl einen herkömmlichen Ryzen 5 3400G als auch einen Ryzen 5 Pro 4650G genutzt. Beide liefen auf Anhieb und (fast) ohne Probleme im Deskmini X300.

Das Herz des Barebones, Asrocks STX-Mainboard, gleicht dem des A300 bis aufs Haar, auch die Platinenrevision 1.02 ist identisch. Asrock hat allerdings bei AMD die „X“-Lizenz gelöst. Der X300 ist jener „Chipsatz“ ohne Chip, der bereits zum Ryzen-Launch 2018 angekündigt wurde, bis heute aber nirgends zum Ein-

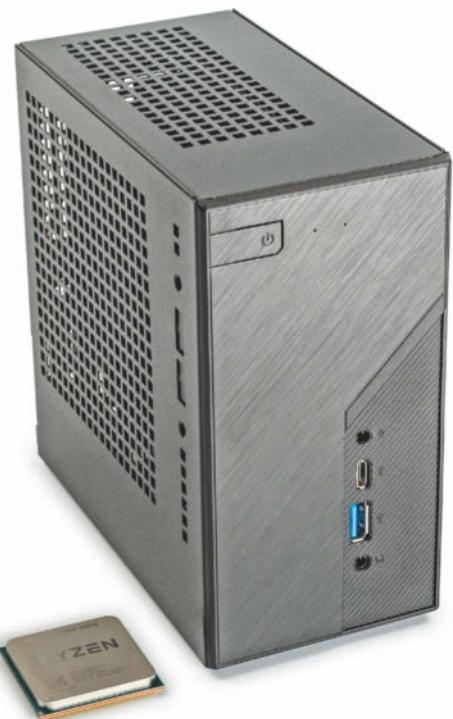
satz kam. Dabei nutzt der PC wie beim A300 die im Ryzen-System-on-Chip integrierten Funktionen, angefangen bei PCI Express über SATA-Ports bis hin zu USB. Nur für Sound und Netzwerk gibt es noch separate Chips auf dem Mainboard.

Unser Testgerät kam ohne WLAN-Option, die Asrock nach wie vor separat verkauft. Wahlweise liegt ein solches der W-Variante des X300 bei. Günstiger und schneller ist allerdings das separat zugekauft AX200-Kit von Intel. Außer Audio- und USB-Buchsen bietet Asrock eine per USB-Header angeschlossene und per magnetischer Rückseite fixierte LED-Leiste als Zubehör, die im Regenbogen-Effekt die Farben durchwechselt und schick durch die Luflöcher im Gehäuse strahlt.

### Zu knapp geschniedert

Beim Gehäuse hat Asrock lediglich kosmetische Änderungen vorgenommen und die Frontverkleidung etwas gediegener gestaltet – aus Kunststoff ist sie nach wie vor. Ansonsten hat sich äußerlich leider nichts getan und mit einer maximalen Kühlerhöhe von 46 Millimeter passt der Boxed-Kühler der Ryzen-G-Modell weiterhin nicht ohne Modifikationen hinein. Auch der beiliegende Winz-Kühler mit seinem lärmenden Lüfter ist geblieben. Er reicht lediglich für Prozessoren mit 35 Watt TDP wie dem Athlon 200GE aus, sofern diese unter Volllast laufen müssen. Für die auf der Rückseite des Mainboard-Trägers montierbaren 2,5-Zoll-Laufwerke fehlen nach wie vor die entscheidenden 3 Millimeter, um auch HDDs mit 15 Millimeter Höhe und damit mehr als 2 TByte einzubauen zu können.

Wer den PC im Wohnzimmer oder im ruhigen Heimbüro einsetzen will, sollte in einen besseren (und vor allem ins Gehäuse passenden) CPU-Kühler wie etwa den Noctua NH-L9a-AM4 investieren. Damit bleiben auch Ryzen 5 3400G und Ryzen 5 Pro 4650G bei Volllast unterhalb der Drossel-



temperatur und der Lüfterlärm erträglich.

Im Leerlauf messen wir mit dem 4650G sehr sparsame 7 Watt, der Ryzen 5 3400G braucht knapp zwei Watt mehr. Mit dem 4650G funktionierten die Stromsparzustände S1 bis S3 nicht. Hier muss Asrock noch das BIOS nachbessern. Die Übertragungsrate der GBit-Ethernet-Schnittstelle sowie der USB-Ports liegen im üblichen Rahmen – schade nur, dass kein USB 3.2 Gen 2 mit 10 GBit/s an Bord ist.

Auch wenn der X-„Chipsatz“ es nun erlaubt, ist das Übertakten im Deskmini ein heikles Thema. Das fängt schon bei der krassen Höhenbegrenzung des Kühlers an. Wirklich leistungsfähige Modelle mit einer Bauhöhe von 46 Millimetern sind Mangelware. Und das mitgelieferte Netzteil kommt mit seinen 120 Watt bereits beim Einsatz eines 65-Watt-Prozessors an seine Grenzen: Wir haben im Turbo-Fenster, bei dem der Prozessor seine TDP überfahren darf, bis zu 140 Watt primärseitig, also inklusive Netzteilverlusten, gemessen. Fürs Tuning inklusive Spannungsabsenkung sind die Optionen im BIOS-Setup jedoch sehr praktisch [3]. Unser Ryzen 5 Pro 4650G wollte ab Werk eine Spannung von 1,3125 Volt für seinen Volllast-Turbo bei 4,2 GHz haben und zog mit Prime95 115 Watt aus der Steckdose. Das schaffte er nach manuellem BIOS-Eingriff auch bei 1,25 Volt, brauchte aber nur noch 98 Watt.

## Fazit

Asrock veredelt den Deskmini in einigen kleineren Punkten, lässt aber Baustellen wie die Stromsparmodi offen. Eine LED-Leiste mag hübsch sein – wichtiger für die meisten Nutzer wäre es aber, dass auch dicke 2,5-Zoll-HDDs oder höhere Kühlern ins Gehäuse passen. So bleibt es bei der schickeren Frontpartie und den Tuning-Optionen im BIOS-Setup. Vor allem aber unterstützt der Deskmini nun die leistungsfähigen, modernen Ryzen-4000-Kombichips und eignet sich damit auch als Basis für einen richtig flotten Mini. (csp@ct.de) 

## Literatur

- [1] Christian Hirsch, Maximal abgespeckt, Kompakte Rechner mit leistungsfähigen Ryzen-Prozessoren, c't 7/2019, S. 100
- [2] Carsten Spille, 7-Watt-Spar-Mini, Sparsamer Einsteiger- und Office-PC für 250 Euro, c't 24/2019, S. 28
- [3] Carsten Spille, Voll entspannt, Mit Undervolting Stromverbrauch, Lärm und Hitze reduzieren, c't 16/2020, S. 144

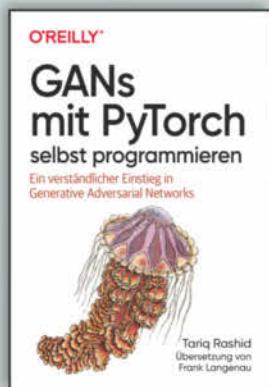
Video zum Deskmini X300: [ct.de/y2e8](http://ct.de/y2e8)

## Asrock Deskmini X300

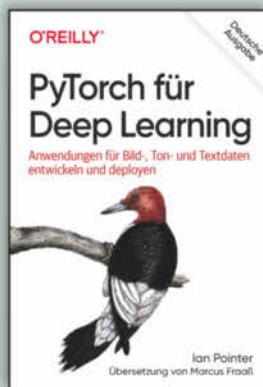
Mini-PC-Barebone für AM4-CPU bis Ryzen 4000G	
Hersteller	Asrock, <a href="http://asrock.com">asrock.com</a>
Prozessor	AMD Athlon 200/3000, Ryzen 3 / 5 2000G / 3000G / 4000G (max. 65 Watt TDP)
Mainboard / BIOS	Asrock X300M-STX / 1.40 (20.08.2020)
RAM (Slots / max.)	2 × SODIMM, DDR4-2933 bis DDR4-3200 (Ryzen 4000G) / 64 GByte (2 × 32 GByte)
Anschlüsse vorn	1 × USB-C 3.2 Gen 1, 1 × USB-A 3.2 Gen 1, 2 × Audio-Klinke
Anschlüsse hinten	1 × DisplayPort 1.2a, 1 × HDMI 2.0, 1 × RJ45, 1 × USB-A 3.2 Gen 1, 1 × USB-A 2.0, 1 × DSub
Festplattenschächte / M.2	2 × 2,5 Zoll (SATA 6G) / 2 × 2280 (M-Key, PCIe 3.0 x4, je 1 × NVMe und 1 × SATA), 1 × 2230 (M-Key, PCIe 2.0 x1, WiFi+BT)
Gigabit Ethernet / Soundchip	1 × Realtek RTL8111 / Realtek ALC233
Netzteil	AcBel ADC027, 19 V/6,32 A (120 W), 15 cm × 3,5 cm × 6,5 cm, Kabel (zum Rechner) 180 cm + Länge Kaltgerätekabel
Abmessungen Gehäuse	15,8 cm × 16,5 cm × 8 cm (inkl. Füßchen & Schlosslasche)
optionales Zubehör	VESA-Halterung, WLAN-Kit, RGB-LED-Leiste
Messwerte (Full-HD-Display, USB-Tastatur/-Maus, Ryzen 5 3400G (Ryzen 5 Pro 4650G))	
Cinebench R20	411 / 1923 (491 / 3609) Punkte
Single- / Multithreading	
3DMark Fire Strike	3411 (3683) Punkte
BAPCo SYSmark 25	909 (1180) Punkte
Leistungsaufnahme Soft-off / Energie sparen	0,4 / 0,9 (– / –) W
Leerlauf / Vollast CPU / GPU / CPU + GPU	8,7 / 81 / 74 / 142 (7,1 / 106 / 53 / 140) W
Geräusch im Leerlauf / CPU-Vollast	⊕ (0,9 Sone) / ⊖ (2,6 Sone)
analoge Signalqualität	Wiedergabe: ⊕⊕/ Aufnahme: ⊖
Preis	noch nicht bekannt
<span style="color: #800000;">⊕⊕</span> sehr gut <span style="color: #008000;">⊕</span> gut <span style="color: #000080;">⊖</span> zufriedenstellend <span style="color: #808000;">⊖</span> schlecht <span style="color: #800080;">⊖⊖</span> sehr schlecht   – funktioniert nicht	

# O'REILLY® Know-how für Praktiker

Noch mehr Auswahl: [www.oreilly.de](http://www.oreilly.de)



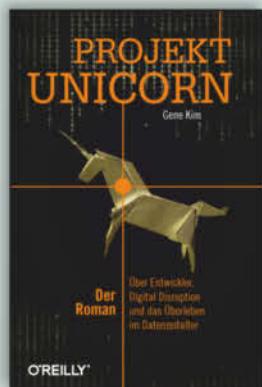
ISBN 978-3-96009-147-9  
Print: 29,90 €, E-Book: 23,99 €



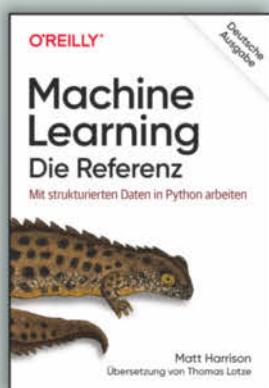
ISBN 978-3-96009-134-9  
Print: 34,90 €, E-Book: 27,99 €



ISBN 978-3-96009-014-4  
Print: 26,90 €, E-Book: 21,99 €



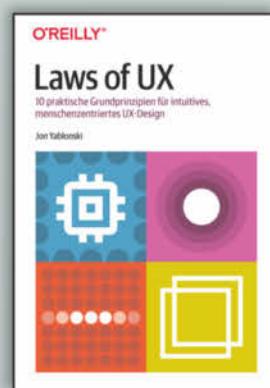
ISBN 978-3-96009-139-4  
Print: 24,90 €, E-Book: 19,99 €



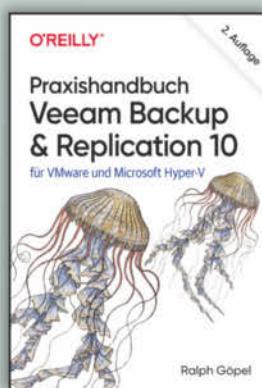
ISBN 978-3-96009-135-6  
Print: 29,90 €, E-Book: 23,99 €



ISBN 978-3-96009-140-0  
Print: 34,90 €, E-Book: 27,99 €



ISBN 978-3-96009-156-1  
Print: 24,90 €, E-Book: 19,99 €



ISBN 978-3-96009-155-4  
Print: 36,90 €, E-Book: 29,99 €



# Flacher Tiger

## Asus-Notebook ZenBook Flip S mit Core i7-1165G7 und OLED-Touchscreen

**Das Asus ZenBook Flip S ist das erste Seriengerät mit Intels elfter Core-i-Generation im c't-Labor. Das Edel-Convertible kommt mit geringem Gewicht, langer Laufzeit und schickem OLED-Bildschirm daher.**

Von Florian Müssig

**B**ei der Vorstellung der elften Core-i-Generation „Tiger Lake“ hatte Intel versprochen, dass Notebooks mit den neuen Prozessoren ab Oktober erhältlich sein sollen. Und tatsächlich trudelte pas-

send dazu das erste solche Gerät im c't-Labor ein: Asus schickte uns sein edles ZenBook Flip S (UX371) – ein 13,3-Zoll-Notebook, das man dank 360-Grad-Scharniere auch als Tablet nutzen kann. Das kurz vor Redaktionsschluss eingetroffene Testexemplar kam noch mit US-Tastenlayout, -Vorinstallation und -Netzteil daher, entspricht laut Asus Deutschland aber ansonsten dem Serienstand. Im hiesigen Handel soll das Notebook vollständig lokalisiert zu finden sein.

Dass die gemessene Rechenleistung der Tiger-Lake-CPU im ZenBook niedriger ausfällt als bei Intels Referenzsystem [1], liegt weniger am etwas schwachbrüstigeren CPU-Modell (Core i7-1165G7 statt Core i7-1185G7) als vielmehr am knapper dimensionierten Kühlssystem. Der Rumpf des

ZenBook ist gerade einmal einen Zentimeter flach, sodass die Kühlung bei anhaltender Last schneller ins Limit läuft als beim Referenzsystem: Dort war das Kühlssystem so bemessen, dass die CPU optional sogar mehr als die maximale „configurable TDP“ (cTDP) von 28 Watt verheizen konnte.

Die Grundtendenz bleibt aber auch beim Zenbook erhalten: Tiger-Lake-CPUs liegen bei Singlethreading-Berechnungen im Vergleich zu allen anderen Mobilprozessoren vorne und legen bei Multithreading-Last gegenüber Ice Lake (zehnte Core-i-Generation) eine Schippe drauf. Wenn alle Kerne gleichzeitig Verwendung finden, schaffen AMDs Ryzen-4000U-Achtkerner weiterhin noch mehr. Die integrierte Grafikeinheit Iris Xe ist bei der 3D-Performance ebenfalls ein großer Schritt nach vorne. Die Treiber liefen stabil; für Spieletests mit bekannten Problemkindern wie Rise of the Tomb Raider blieb vor Druckschluss allerdings keine Zeit mehr.

### Plattform-Plus

Bei den Schnittstellen hat Intel AMD überholt. Wohl gibt es etliche Ryzen-Notebooks mit Wi-Fi-6-Modul, doch Thunderbolt 4 [2] und dessen Basistechnik USB 4 [3] sind derzeit Tiger-Lake-exklusiv. Entsprechende Peripherie sucht man derzeit zwar noch vergeblich, doch die Abwärtskompatibilität umfasst Thunderbolt 3 und ältere USB-Modi inklusive des seltenen USB 3.2 Gen 2 x 2 (20 GBit/s) – und auch die findet man in Ryzen-Notebooks nicht.

PCIe 4.0 ist ebenfalls an Bord, in auf hohe Mobilität getrimmten Notebooks aber sekundär: Aus Stromspargründen dürften in solchen Geräten weiterhin hauptsächlich PCIe-3.0-SSDs zum Einsatz kommen – so auch im ZenBook.

Apropos hohe Mobilität: Mit Tiger Lake ist die zweite Generation von Intels Project-Athena-Spezifikation gestartet, in der Intel Mindestanforderungen für hochwertige Notebooks definiert. Bislang waren diese eher schwammig gehalten und zudem auf Full-HD-Ausstattungsvarianten eines Notebook-Modells beschränkt; und der zugehörige Marketing-Aufkleber mit dem sperrigen Schriftzug „Engineered for Mobile Performance“ fand sich selten [4]. In all diesen Punkten hat Intel nachgelegt: Das Marketing-Programm trägt nun den offiziellen, griffigen Namen „Evo“, der entsprechende Aufkleber ersetzt das herkömmliche Core-i-Logo auf der Handballenablage.

## OLED

Asus baut in sein Evo-Notebook einen 4K-OLED-Bildschirm ein. Das Panel deckt den DCI-P3-Farbraum ab; Bildschirm eingaben sind mittels Finger oder Stift möglich. Der Pferdefuß: Der OLED-Bildschirm hat das herkömmliche Seitenverhältnis von 16:9, während andere Premium-Geräte bereits bei der letzten Gerätegeneration den Schritt hin zu 16:10 oder 3:2 gegangen sind, was ein spürbares Plus an Bildhöhe bringt.

Asus verkauft das ZenBook Flip S (UX371) wie getestet für 2500 Euro oder mit Windows 10 Pro statt Home für 100 Euro mehr. Ausstattungsvarianten mit Full-HD-Touchscreen (modellabhängig IPS oder OLED) statt 4K-OLED heißen ZenBook Flip 13 (UX363) und kosten ab 1800 Euro (8 GByte, 512er-SSD). Alle Konfigurationen verwenden den Core i7-1165G7, abgesehen von der gesteckten SSD gibt es keine Auf- oder Umrüstmöglichkeiten.

Die Tasten der beleuchteten Tastatur sind zwar wie bei Desktop-Tastaturen 19 Millimeter breit, aber nur 16 Millimeter tief – das erfordert Übung, bis man zügig blind ohne Vertipper Texte zu Datei bringt. Die Enter-Taste fällt einzeilig aus. Pos1, Ende, Bild-Auf und Bild-Ab sind hingegen als separate Tasten ausgeführt – das ist selten. Über einen langen Druck in die obere rechte Ecke des Touchpads schaltet man es in einen Ziffernblock-Modus; ein eingeblen detes Raster teilt die Sensorfläche auf. Der Mauszeiger lässt sich auch in diesem Modus noch bewegen; Mehrfingergesten sind hingegen nicht mehr möglich.

Das Kühl system bleibt bei geringer Systemlast und kurzen Lastspitzen lautlos, bei anhaltender Rechenlast rauscht der



**Hinter dem auf dem Aufkleber beworbenen Evo-Programm steckt die zweite Generation des Intel-Marketingprogramms „Projekt Athena“. Das Touchpad lässt sich wahlweise als Ziffernblock verwenden.**

Lüfter mit leisen 0,4 Sone. Der Akku sorgt für bis zu vierzehn einhalb Stunden Laufzeit; das USB-C-Netzteil befüllt den leeren Akku flott. Eine analoge Audio-Klinkenbuchse fehlt; stattdessen legt Asus einen USB-C-Adapter in den Karton.

höchste Performance nach wie vor ein ausgeklügeltes Kühl system, sind für Intel allerdings ein großer Schritt nach vorne.

(mue@ct.de)

## Fazit

Asus hat mit dem ZenBook Flip S ein leichtes Premium-Convertible auf die Standfüße gestellt. Der stiftbedienbare OLED-Touchscreen ist farbstark und hell, mit dem schmalen Seitenverhältnis von 16:9 aber auch der größte Knackpunkt. Die Tiger-Lake-Prozessoren brauchen für

## Literatur

- [1] Nico Ernst, Einzelkämpfer, Erste Benchmarks der Tiger-Lake-CPU Core i7-1165G7, c't 21/2020, S. 42
- [2] Florian Müsseg, USB-Vollausbau, Spezifikation zu Thunderbolt 4 verabschiedet, c't 17/2020, S. 140
- [3] Florian Müsseg, USB, die Vierte, Spezifikation für USB 4 finalisiert, c't 20/2019, S. 26
- [4] Florian Müsseg, Konfusus Athena, Lenovo Yoga C940-14IIL: komfortables Notebook aus Intels Project Athena, c't 10/2020, S. 84

## Asus ZenBook Flip S (UX371): Daten und Testergebnisse

Getestete Konfiguration		90NB0Z2-S00030					
Lieferumfang		Windows 10 Home 64 Bit, Netzteil, USB-C-auf-Audio-Adapter					
<b>Schnittstellen (V = vorne, H = hinten, L = links, R = rechts, U = unten)</b>							
VGA / DVI / HDMI / DisplayPort / Kamera (Hello)	– / – / L / – / ✓ (✓)						
USB 2.0 / USB 3.0 / USB 3.1 / LAN	– / 1 × R / 2 × L (2 × Typ C) / –						
Kartenleser / Strom / Docking-Anschluss	– / – / –						
USB-C: Thunderbolt / USB 3.0 / USB 3.1 / DisplayPort / Laden	✓ / ✓ / ✓ / ✓ / ✓						
<b>Ausstattung</b>							
Display	Samsung ATNA33TP11-1: 13,3 Zoll / 33,7 cm, 3840 × 2160, 16:9, 332 dpi, 4 ... 454 cd/m <sup>2</sup> , spiegelnd						
Prozessor	Intel Core i7-1165G7 (4 Kerne mit SMT), 2,8 GHz (Turbo bis 4,7 GHz), 4 × 1280 KByte L2, 12 MByte L3-Cache						
Hauptspeicher / Chipsatz	16 GByte LPDDR4X-4267 / Intel Tiger-Lake-U						
Grafikchip (Speicher) / mit Hybridgrafik	int.: Intel Iris Xe (vom Hauptspeicher) / –						
Sound	HDA: Realtek ALC294						
LAN / WLAN	– / CNVi: Intel AX201 (Wi-Fi 6, 2 Streams)						
Mobilfunk / Bluetooth (Stack)	– / USB: Intel (Microsoft)						
Touchpad (Gesten) / TPM / Fingerabdruckleser	I2C: HID (max. 4 Finger) / TPM 2.0 / –						
Massenspeicher / optisches Laufwerk	SSD: WDC SN730 (1024 GByte) / –						
<b>Stromversorgung, Maße, Gewicht</b>							
Akku / wechselbar / Ladestandsanzeige	68 Wh Lithium-Ionen / – / –						
Netzteil	65 W, 218 g, 6,5 cm × 6,5 cm × 2,9 cm, Steckernetzteil						
Gewicht / Größe / Dicke mit Füßen	1,23 kg / 30,5 cm × 21,1 cm / 1,5 cm						
Tastaturhöhe / Tastenraster	1 cm / 19 mm × 16 mm						
<b>Leistungsaufnahme</b>							
Suspend / ausgeschaltet	0,6 W / 0,4 W						
ohne Last: Display aus / 100 cd/m <sup>2</sup> / max	1,9 W / 6,6 W / 10,2 W						
CPU-Last / Video / 3D-Spiele (max. Helligkeit)	62,5 W / 16,5 W / 42,9 W						
max. Leistungsaufnahme / Netzteil-Powerfactor	67,2 W / 0,55						
<b>Laufzeit, Geräusch, Benchmarks</b>							
Laufzeit Idle (100 cd/m <sup>2</sup> ) / Video (200 cd/m <sup>2</sup> ) / 3D (max)	14,6 h / 7 h / 2,4 h						
Ladestand / Laufzeit nach 1h Laden	74 % / 10,8 h						
Geräusch ohne / mit Rechenlast	< 0,1 Sone / 0,4 Sone						
Massenspeicher lesen / schreiben	2777 / 2933 MByte/s						
IOPS (4K) lesen / schreiben	86016 / 108288						
WLAN 5 GHz / 2,4 GHz (20m) / MU-MIMO-fähig	35,9 / 20 MByte/s / ✓						
Qualität Audioausgang / Dynamikumfang	⊕⊕ / 100,3 dBa						
Cinebench R20 Rendering (1 / n CPU)	507 / 1713						
3DMark: Night Raid / Sky Diver / Fire Strike / Time Spy	12251 / 10568 / 3584 / 1485						
<b>Preis und Garantie</b>							
Straßenpreis Testkonfiguration	2500 €						
Garantie	2 Jahre						
⊕⊕ sehr gut	⊕ gut	○ zufriedenstellend	⊖ schlecht	⊖⊖ sehr schlecht	✓ vorhanden	– nicht vorhanden	k. A. keine Angabe



# Günstiger Groß-Ryzen

## 16-Zoll-Notebook Honor MagicBook Pro mit Ryzen 5 4600H

**Honor verkauft sein MagicBook Pro ausschließlich in Mittelklasse-Konfigurationen; dank des flotten Ryzen 5 4600H bietet das 16-Zoll-Notebook viel Performance.**

Von Florian Müssig

**M**it dem Notebooknamen MagicBook Pro spielt Honor auf Apples MacBook Pro 16" [1] an, denn auch dort gibt es einen sonst seltenen 16-Zoll-Bildschirm. An dieser Stelle hören die Gemeinsamkeiten allerdings schon wieder auf: Das hier getestete MagicBook Pro kostet 800 Euro, während die Preise des Apple-Geräts erst bei mehr als dem Dreifachen beginnen.

Honor adressiert außerdem eine ganz andere Zielgruppe: Man bekommt das Notebook nur in Mittelklasse-Konfigurationen mit dem Sechs-Kern-Prozessor Ryzen

5 4600H. Das mit 16 GByte Arbeitsspeicher und 512er-SSD sinnvoll bestückte Testgerät ist bei etlichen Händlern für die erwähnten 800 Euro lieferbar. Eine 100 Euro günstigere Konfiguration mit knapperen, weil jeweils halbierten RAM- und SSD-Kapazitäten war bei Redaktionsschluss auf wenige Händler beschränkt. Windows 10 Home ist immer an Bord: Anders als die Smartphones des Honor-Mutterkonzerns Huawei sind die Notebooks nicht vom US-Handelsembargo betroffen.

Der blickwinkelunabhängige 16-Zoll-Bildschirm erfreut mit matter Oberfläche, seine maximale Helligkeit von knapp 300 cd/m<sup>2</sup> reicht selbst an sonnigen Tagen aus. Die Full-HD-Auflösung taugt für alltägliche Aufgaben und lässt sich mit guten Augen auch ohne Windows-Skalierung verwenden. Wie inzwischen bei Notebooks üblich fallen die Ränder um das Panel schlank aus.

Die obligatorische Webcam fand deshalb jedoch keinen Platz an der regulären Position oberhalb des Displays. Honor hat sie stattdessen ausklappbar zwischen F6 und F7 in die Tastatur integriert. Bei Videokonferenzen wird der Nutzer deshalb von unten gefilmt – für den oder die Gegenüber gewöhnungsbedürftig.

Die Webcam-Position hat auch Folgen fürs Tasten-Layout: Alle F-Tasten ab F7 sind um eine Spalte nach rechts verschoben. Wer diese Tasten häufig nutzt, muss sich eingewöhnen, bis er sie blind trifft. Sonst gibt es an der beleuchteten Tastatur nur den in eine Zeile gequetschten Ziffernblock zu bemängeln. Über langes Gedrückthalten der Fn-Taste kann man im Betrieb festlegen, ob die F-Tasten mit Standard- oder Sonderfunktionen belegt sind. Das Touchpad ist groß genug für Gesten mit bis zu vier Fingern; separate Maustasten fehlen. Seitlich der Tastatur findet man die Gitter der Lautsprecher; in den rechten Grill ist der Einschalter samt darin integriertem Fingerabdruckleser eingelassen.

### Ryzen-Power

Im MagicBook Pro arbeitet der Ryzen 5 4600H, der eine hohe Multithreading-Leistung liefert – in etwa das Doppelte dessen, was Intels in Notebooks dieser Preisklasse gängige CPUs (Ice Lake U, 10. Core-i-Generation) erzielen. Selbst die neuen Tiger-Lake-Chips (11. Core-i-Generation, siehe S. 78 und [2]) übertrumpfen AMD nur bei Singlethinger-Berechnungen.

Bei der Grafik verlässt sich Honor auf die im Chip integrierte Radeon Vega 6 und nagelt keine zusätzliche Low-End-GPU dazu. Eine gute Entscheidung: Für vergleichsweise detailarme 3D-Grafik reicht die Radeon aus, für feiner gezeichnete Blockbuster-Welten mit schicken Effekten müsste es dann schon ein Mittelklasse-Grafikchip sein. Für solche Notebooks muss man zwar nur ähnlich viel Geld auf den Tisch legen wie bei Honor, bekommt dort dann aber kein schickes Metallgehäuse.

Honor stattet das MagicBook Pro mit einem Wi-Fi-5-Modul aus. Für noch flotteres Wi-Fi 6 könnte man das gesteckte WLAN-Modul im Geräteinneren tauschen – das Basteln birgt allerdings die Gefahr, dass Honor im Falle eines Defekts die Garantie verweigert. Die SSD ist ebenfalls wechselbar, der Arbeitsspeicher hingegen aufgelöst. Ein im Inneren vorhandener 2,5-Zoll-Schacht kann nicht mit einer Festplatte bestückt werden, weil sowohl das gerätespezifische Anschlusskabel fehlt als auch die Hauptplatine nicht mit dem zugehörigen ZIF-Sockel bestückt wurde.

Außer einer normalgroßen Buchse für HDMI und drei im USB-A-Format findet man einen modernen USB-C-Anschluss vor. Der gibt auf Wunsch DisplayPort-Signale aus und nimmt Strom entgegen, sodass komfortablem USB-C-Docking nichts im Wege steht. Ein Kartenleser fehlt.

Der Lüfter bleibt bei geringer Systemlast unhörbar leise und dreht auch bei kurzer Rechenlast nicht auf. Ist der Ryzen-Chip längere Zeit ausgelastet, so rauscht das Notebook mit erträglichen 1,9 Sone. Der Akku hält bis zu 16 Stunden durch, was für einen Arbeitstag ohne Netzteil ausreicht; mit 1,7 Kilogramm schleppt man aber spürbar mehr Notebook-Gewicht mit



**Wegen der in die Tastatur integrierten, ausklappbaren Webcam erscheint man in Videokonferenzen für die anderen Teilnehmer aus seltsam tiefer Perspektive.**

sich herum als bei einem 13,3-Zöller. Das beiliegende Netzteil verwendet die USB-C-Buchse und lädt einen leeren Akku flott auf. Zudem kann es alle gängigen Spannungen liefern, die USB-C-Smartphones benötigen – dies ist leider nicht selbstverständlich bei Notebook-Netzteilen [3].

## Fazit

Honor hat mit dem MagicBook Pro ein ordentliches Mittelklasse-Notebook im wertigen Metallgehäuse auf die Beine gestellt; größter Knackpunkt ist die schlecht platzierte Webcam. Die Rechenleistung ist dank Ryzen-Sechskerner hoch und es gibt praktisches USB-C-Docking

sowie komfortables biometrisches Einloggen wie bei teureren Geräten. Die Reduktion auf eine verbreitete Ausstattungsvariante schmerzt nicht, weil Honor die Bestückung sinnvoll gewählt hat.

(moe@ct.de) **ct**

## Literatur

- [1] Florian Müssig, Mobile Power mit guter Tastatur, Apple MacBook Pro 16" mit neuer Tastenmechanik, c't 26/2019, S. 72
- [2] Nico Ernst, Einzelkämpfer, Erste Benchmarks der Tiger-Lake-CPU Core i7-1185G7, c't 21/2020, S. 42
- [3] Florian Müssig, An Format gewonnen, Dells Edel-Notebook XPS 15 (9500) mit 16:10-Bildschirm, c't 20/2020, S. 96

## Honor MagicBook Pro: Daten und Testergebnisse

getestete Konfiguration	53011GXD					
Lieferumfang	Windows 10 Home 64 Bit, Netzteil					
<b>Schnittstellen (V = vorne, H = hinten, L = links, R = rechts, U = unten)</b>						
VGA / DVI / HDMI / DisplayPort / Kamera (Hello)	– / – / L / – / ✓ (–)					
USB 2.0 / USB 3.0 / USB 3.1 / LAN	– / 2 × L (1 × Typ C), 2 × R / – / –					
Kartenleser / Strom / Docking-Anschluss	– / – / –					
USB-C: Thunderbolt / USB 3.0 / USB 3.1 / DisplayPort / Laden	– / ✓ / – / ✓ / ✓					
<b>Ausstattung</b>						
Display	Chimei N161HCA-EA3: 16,1 Zoll / 40,8 cm, 1920 × 1080, 16:9, 137 dpi, 4 ... 290 cd/m <sup>2</sup> , matt					
Prozessor	AMD Ryzen 5 4600H (6 Kerne mit SMT), 3 GHz (Turbo bis 4 GHz), 6 × 512 KByte L2, 2 × 4096 KByte L3-Cache					
Hauptspeicher / Chipsatz	16 GByte DDR4-2666 / AMD Renoir-SoC					
Grafikchip (Speicher) / mit Hybridgrafik	int.: AMD Radeon Vega 6 (vom Hauptspeicher) / –					
Sound	HDA: Realtek ALC256					
LAN / WLAN	– / PCIe: Realtek RTL8822CE (Wi-Fi 5, 2 Streams)					
Mobilfunk / Bluetooth (Stack)	– / USB: Realtek (Microsoft)					
Touchpad (Gesten) / TPM / Fingerabdruckleser	I2C: HID (max. 4 Finger) / TPM 2.0 / USB: Goodix					
Massenspeicher / optisches Laufwerk	SSD: WDC SN730 (512 GByte) / –					
<b>Stromversorgung, Maße, Gewicht</b>						
Akku / wechselbar / Ladestandsanzeige	55 Wh Lithium-Ionen / – / –					
Netzteil	65 W, 198 g, 6 cm × 6 cm × 2,9 cm, Steckernetzteil					
Gewicht / Größe / Dicke mit Füßen	1,69 kg / 36,9 cm × 23,4 cm / 2,1 cm					
Tastaturhöhe / Tastenraster	1,4 cm / 19 mm × 19 mm					
<b>Leistungsaufnahme</b>						
Suspend / ausgeschaltet	0,8 W / 0,4 W					
ohne Last: Display aus / 100 cd/m <sup>2</sup> / max	3,2 W / 5,9 W / 8,6 W					
CPU-Last / Video / 3D-Spiele (max. Helligkeit)	67,4 W / 13,8 W / 37,4 W					
max. Leistungsaufnahme / Netzteil-Powerfactor	67,4 W / 0,54					
<b>Laufzeit, Geräusch, Benchmarks</b>						
Laufzeit Idle (100 cd/m <sup>2</sup> ) / Video (200 cd/m <sup>2</sup> ) / 3D (max)	16,3 h / 8,2 h / 2,7 h					
Ladestand / Laufzeit nach 1h Laden	82 % / 13,3 h					
Geräusch ohne / mit Rechenlast	< 0,1 Sone / 1,9 Sone					
Massenspeicher lesen / schreiben	2822 MByte/s / 2537 MByte/s					
IOPS (4K) lesen / schreiben	120832 / 87040					
WLAN 5 GHz / 2,4 GHz (20m) / MU-MIMO-fähig	34 MByte/s / 17 MByte/s / ✓					
Qualität Audioausgang / Dynamikumfang	⊕⊕ / 98,4 dBa					
Cinebench R20 Rendering (1 / n CPU)	431 / 3197					
3DMark: Night Raid / Sky Diver / Fire Strike / Time Spy	12114 / 10530 / 2784 / 1042					
<b>Preis und Garantie</b>						
Straßenpreis Testkonfiguration	800 €					
Garantie	2 Jahre					
⊕⊕ sehr gut	⊕ gut	○ zufriedenstellend	⊖ schlecht	⊖⊖ sehr schlecht	✓ vorhanden	– nicht vorhanden



# Gamer ohne GPU

## Flaches 15,6-Zoll-Notebook Lenovo Legion Y740Si mit Core i7-10750H

**Der 15,6-Zöller Lenovo Legion Y740Si kommt im Gaming-Ornat daher, doch eine spieletaugliche Grafikkarte muss man als externes GPU-Dock dazukaufen. Durch diesen Design-Kniff ist das Notebook selbst extrem flach geraten.**

Von Florian Müssig

**D**ünne Notebooks sind an sich nichts Besonderes mehr, beim Gaming-Notebook Lenovo Legion Y740Si fällt die schlanke Bauform dennoch auf: In dem nur einen Zentimeter flachen Rumpf des 15,6-Zoll-Geräts steckt nämlich kein für flache Notebooks typischer U-Prozessor (15 Watt TDP, Thermal Design Power), sondern mit dem Core i7-10750H eine H-CPU (45-Watt-Klasse) aus Intels zehnter Core-i-Generation. Sie liefert eine für ein Gaming-Notebook ordentliche Rechenleistung, ist aber ein Chip mit betagter Kernarchitektur und 14-Nanometer-Transistoren. An die Multithreading-Performance von AMDs Ryzen-4000-Prozessoren

(siehe S. 80) kommt der Core i7-10750H nicht heran; und bei der Singlethreading-Rechenleistung liegen sogar die U-Modelle der frisch vorgestellten elften Core-i-Generation vorn (siehe S. 78 und [1]).

Die flache Bauweise bringt zwei Besonderheiten mit sich. Um die unter Last anfallende Abwärme abzuführen, sind gleich vier Lüfter notwendig, die schon bei kurzer Last hörbar zu rauschen beginnen. Bei anhaltender Rechenlast wird es mit über 3 Sone sehr laut. Das Kühlsystem schlägt aufs Gewicht durch: Man muss 1,7 Kilogramm herumschleppen.

Obwohl das Notebook Lenovos Gaming-Marke Legion zugeordnet ist, hat es keinen zusätzlichen Grafikchip. Um die Bildschirmansteuerung kümmert sich ausschließlich die im Prozessor integrierte Grafikeinheit UHD, die für alle 3D-Welten jenseits von Google Earth zu schwach ist.

### eGPU

Zum Zocken ist deshalb eine externe Grafikkarte nötig, ein sogenanntes eGPU-Dock. Lenovo hat mit der BoostStation ein ebensolches im Angebot, doch es muss separat gekauft werden. Das Leergehäuse ohne Grafikkarte (82CA0000GGE) kostet rund 390 Euro, mit ab Werk eingebauter Nvidia GeForce RTX 2060 (82CA000H-GE) stehen knapp 550 Euro auf dem Preisschild. Die BoostStation hat ein eigenes Netzteil und kann mit diesem sowohl GeForce- als auch Radeon-Grafikkarten mit bis zu 500 Watt versorgen.

Die Grafikausgabe erfolgt wahlweise auf dem Notebook-Bildschirm oder auf Monitoren, die man an den Ausgängen der Grafikkarte anschließt. Die BoostStation bietet drei USB-A-Buchsen und einen LAN-Anschluss; im Inneren lässt sich eine 3,5-Zoll-Festplatte als stationäres Datengrab einbauen. Ein eingeklappter U-förmiger Metallbügel am hinteren Ende sollte tunlichst nicht als Griff beim Transport verwendet werden: Er dient zum werkzeuglosen Öffnen des Dock-Gehäuses.

Die BoostStation muss unabhängig vom Notebook eingeschaltet werden und lädt nur dann ein per Thunderbolt 3 angeschlossenes Notebook. Das eGPU-Dock verbrät bereits im Leerlauf ohne interne HDD oder angeschlossenes Notebook knapp 11 Watt und befördert diese Abwärme durch einen Lüfter in die Umgebung. Der Ventilator säuselt in ruhigen Umgebungen immer hörbar (0,2 Sone) – und man kann das Dock auch nicht geräuschenmindernd unter dem Schreibtisch platzieren.

ren, weil das beigelegte Thunderbolt-Kabel nur 60 Zentimeter misst.

## Singulär

Lenovo verkauft das getestete Legion Y740Si (konkreter mitunter auch Y740S-15IMH genannt) mit Core i7-10750H, 16 GByte aufgelötem Arbeitsspeicher und einer 1-TByte-SSD für 1700 Euro. Der matte Bildschirm zeigt 4K-Auflösung, ist mit mehr als 500 cd/m<sup>2</sup> sowohl HDR- als auch außentauglich und deckt den Adobe-RGB-Farbraum ab. Das 2500-Euro-Topmodell hat ebenfalls den farbstarken 4K-Bildschirm, jeweils verdoppelte Speicherkapazitäten und den Achtkerner Core i9-10980HK. Das 1300-Euro-Einstiegsmodell kommt mit Core-i5-Vierkern, 512er-SSD, 16 GByte Arbeitsspeicher und einem Full-HD-Panel abgespeckter Farbrillanz daher. Das Gehäuse gibt es ausschließlich in Grau.

Die beleuchtete Tastatur gefällt mit einem gelungenen Layout inklusive großer Cursor-Tasten. Den Tasten des Ziffernblocks liegt allerdings ein engeres Raster zugrunde als beim Haupttastenfeld. Das gestenfähige Touchpad wurde in der Handballenablage nach links verschoben, um trotz Ziffernblocks mittig vor der Leertaste zu liegen.

Oberhalb der Tastatur befindet sich der Einschalter, der gleichzeitig als Fingerabdruckleser für Windows Hello dient. Die über einen mechanischen Schieber abdeckbare Webcam findet man in direkter Umgebung, nämlich mittig an der unteren Kante des Deckels – das sorgt in Videokonferenzen für eine seltsame Untersicht. Angesichts des hohen Bildschirmkinns stellt sich die Frage, ob Lenovo das Display nicht ein wenig tiefer platziert haben könnte, damit die Webcam wie gewohnt darüber



**Wer mit dem Legion Y740Si zocken will, benötigt ein externes GPU-Dock wie Lenovos BoostStation.**

passt. Zudem hätte locker auch ein Panel im arbeitsfreundlicheren 16:10-Format mit mehr Bildhöhe in den Deckel gepasst.

Lenovo hat zwei Thunderbolt- und Docking-fähige USB-C-Buchsen am linken Rand platziert; zwei USB-Buchsen mit herkömmlichem Typ-A-Format sind an die Rückseite gewandert. Der Kartenleser nimmt normalgroße SD-Karten auf, bremst rasante UHS-II-Exemplare allerdings aus. Die Laufzeit fällt mit maximal 10 Stunden ordentlich, aber nicht übermäßig lang aus. Das beiliegende 95-Watt-USB-C-Netzteil lädt den Akku flott.

## Fazit

Lenovo preist das Legion Y740Si als Gaming-Maschine an, doch als solche funktioniert es nur stationär, wenn man zusätzlich in eine eGPU investiert. Ohne sie eignet es sich nur für kreative Nutzer zur Bild- oder Videobearbeitung, erledigt diesen Job als flaches Notebook mit farbstarkem 4K-Bildschirm aber ordentlich. (moe@ct.de) **ct**

## Literatur

- [1] Nico Ernst, Einzelkämpfer, Erste Benchmarks der Tiger-Lake-CPU Core i7-1185G7, c't 21/2020, S. 42

## Lenovo Legion Y740Si: Daten und Testergebnisse

getestete Konfiguration	81YX000VGE					
Lieferumfang	Windows 10 Pro 64 Bit, Netzteil, USB-C-Monitor-Adapter (HDMI, VGA)					
<b>Schnittstellen (V = vorne, H = hinten, L = links, R = rechts, U = unten)</b>						
VGA / DVI / HDMI / DisplayPort / Kamera (Hello)	– / – / – / – / ✓ (–)					
USB 2.0 / USB 3.0 / USB 3.1 / LAN	– / 2 × H / 2 × L (2 × Typ C) / –					
Kartenleser / Strom / Docking-Anschluss	R (SD) / – / –					
USB-C: Thunderbolt / USB 3.0 / USB 3.1 / DisplayPort / Laden	✓ / ✓ / ✓ / ✓ / ✓					
Ausstattung						
Display	CSOT MNF601EA1-2: 15,6" / 39,5 cm, 3840 × 2160, 16:9, 284 dpi, 5 ... 536 cd/m <sup>2</sup> , matt					
Prozessor	Intel Core i7-10750H (6 Kerne mit SMT), 2,6 GHz (Turbo bis 5 GHz), 6 × 256 KByte L2-, 12 MByte L3-Cache					
Hauptspeicher / Chipsatz	16 GByte DDR4-2933 / Intel HM370					
Grafikchip (Speicher) / mit Hybridgrafik	int.: Intel UHD (vom Hauptspeicher) / –					
Sound	HDA: Realtek ALC285					
LAN / WLAN	– / CNVi: Intel AX201 (Wi-Fi 6, 2 Streams)					
Mobilfunk / Bluetooth (Stack)	– / USB: Intel (Microsoft)					
Touchpad (Gesten) / TPM / Fingerabdruckleser	I2C: HID (max. 4 Finger) / TPM 2.0 / USB: Goodix					
Massenspeicher / optisches Laufwerk	SSD: Samsung PM981a (1024 GByte) / –					
Stromversorgung, Maße, Gewicht						
Akku / wechselbar / Ladestandsanzeige	62 Wh Lithium-Ionen / – / –					
Netzteil	95 W, 419 g, 12,5 cm × 6,4 cm × 2,8 cm, Kleeblattstecker					
Gewicht / Größe / Dicke mit Füßen	1,67 kg / 36 cm × 26,1 cm / 1,7 ... 2,2 cm					
Tastaturhöhe / Tastenraster	1,1 cm / 19 mm × 18,5 mm					
Leistungsaufnahme						
Suspend / ausgeschaltet	0,9 W / 0,4 W					
ohne Last: Display aus / 100 cd/m <sup>2</sup> / max	3,8 W / 7,9 W / 13,8 W					
CPU-Last / Video / 3D-Spiele (max. Helligkeit)	52,5 W / 18,7 W / 43,6 W					
max. Leistungsaufnahme / Netzteil-Powerfactor	100,9 W / 0,92					
Laufzeit, Geräusch, Benchmarks						
Laufzeit Idle (100 cd/m <sup>2</sup> ) / Video (200 cd/m <sup>2</sup> ) / 3D (max)	10,3 h / 5 h / 1,8 h					
Ladestand / Laufzeit nach 1h Laden	87 % / 9 h					
Geräusch ohne / mit Rechenlast	< 0,1 Sone / 3,1 Sone					
Massenspeicher lesen / schreiben	3346 MByte/s / 2864 MByte/s					
IOPS (4K) lesen / schreiben	65623 / 55836					
Leserate SD-Karte	78 MByte/s					
WLAN 5 GHz / 2,4 GHz (20m) / MU-MIMO-fähig	24 MByte/s / 13 MByte/s / ✓					
Qualität Audioausgang / Dynamikumfang	⊕⊕ / 103,1 dBA					
Cinebench R20 Rendering (1 / n CPU)	494 / 2506					
3DMark: Night Raid / Sky Diver / Fire Strike / Time Spy / Port Royal	5737 / 4912 / 1202 / 470 / –					
Preis und Garantie						
Straßenpreis Testkonfiguration	1700 €					
Garantie	2 Jahre					
⊕⊕ sehr gut	⊕ gut	○ zufriedenstellend	⊖ schlecht	⊖⊖ sehr schlecht	✓ vorhanden	– nicht vorhanden



**Gute Aussichten für Fotobegeisterte.**

**Sparen Sie 35% im Abo und sammeln wertvolles Know-how:**

- **2 Ausgaben** kompaktes Profiwissen für 14,60 € (Preis in DE)
- **Workshops und Tutorials**
- **Tests und Vergleiche** aktueller Geräte



### Geschenk nach Wahl

z. B. Kamera-Reinigungsset

Jetzt bestellen:

[ct-foto.de/miniabo](http://ct-foto.de/miniabo)

**ct Fotografie**

📞 +49 541/80 009 120

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



## Tausendsassa

**Der AMD-APU Ryzen 5 Pro 4650G hat mit sechs Prozessorkernen, aktueller Zen-2-Architektur und integrierter Radeon-Grafik fast alles, was ein flotter PC braucht.**

Auch Ryzen-Prozessoren für die Desktop-PC-Fassung AM4 bekommen mit der Pro-4000G-Serie nun aktuelle Zen-2-Technik mit bis zu acht Kernen und schneller Radeon-Vega-Grafik. Der Ryzen 5 Pro 4650G hat sechs Kerne und Simultaneous Multithreading für eine bessere Auslastung der Recheneinheiten. Mit 3,7 GHz Basistakt ist er bei 65 Watt TDP sogar minimal flotter als der Ryzen 5 3600 ohne integrierte Grafik, im Turbo sind sie mit 4,2 GHz gleich schnell.

Im Cinebench R20 ist der 4650G so schnell wie der Ryzen 5 3600 und Intels Core i5-10600K. Die integrierte Grafik genügt für ein Spielchen und entlastet die CPU-Kerne bei der Wiedergabe moderner Video-Codecs. Im Leerlauf und unter Volllast ist mit 19 respektive 115 Watt zwar alles im grünen Bereich, aber die aktuellen BIOS-Versionen von drei verschiedenen Boards verweigerten mit dem 4650G die Stromsparzustände S1 bis S3, in denen der Rechner weniger als 1 Watt Leistung aufnimmt. Davon abgesehen ist der Ryzen 5 Pro 4650G ein gelungener Allrounder für alle, die keine Grafikkarte brauchen, und hat genug Leistung für die meisten PCs.

(csp@ct.de)

## AMD Ryzen 5 Pro 4650 G

### Prozessor mit integrierter Grafik für AM4-Fassung

Hersteller, Website	AMD, <a href="http://www.amd.com">www.amd.com</a>
Kerne, Takt	6 (+ SMT), 3,7 GHz (Turbo: 4,2 GHz)
Cinebench R20	491 / 3697 Punkte
BAPCO SYSMark 25	1180 Punkte
3DMark Firestrike	3652 Punkte
Preis	circa 225 € (Tray, ohne Kühlung)

## Maximal konventionell

**Seagate dreht an der Kapazitäts-schraube und steigert die Festplattenkapazität mit konventioneller Aufzeichnungstechnik auf 18 TByte, zuerst bei einer NAS-Festplatte.**

Die Ironwolf Pro ist Seagates erste Festplatte mit einer Kapazität von 18 TByte, eine weitere ist bereits angekündigt (siehe S. 48). Die Kapazitätssteigerung erreicht das Unternehmen durch den Einbau einer neunten Scheibe.

In den Außenzonen erreicht die Ironwolf Pro eine Übertragungsgeschwindigkeit von maximal 280 MByte/s und ist damit die schnellste 3,5-Zoll-Festplatte, die wir je auf dem Prüfstand hatten. Dank Heliumfüllung liegen Leistungsaufnahme (maximal 8,7 Watt im Betrieb) und Lautstärke (0,3 Sone) auf niedrigem Niveau.

Die Ironwolf Pro ist für NAS-Systeme mit bis zu 24 Schächten konzipiert; Vibrationssensoren messen Schwingungen benachbarter Laufwerke, um damit die Kopfsteuerung zu optimieren. Dabei drehen sich die Scheiben mit 7200 Umdrehungen pro Minute. Die Garantie beträgt fünf Jahre, innerhalb dieser Zeit darf das Laufwerk 1,5 PByte Daten verarbeiten.

Vor dem Kauf sollte man die Kompatibilitätslisten der NAS-Hersteller konsultieren. Erste Firmen wie Asustor haben die Platte bereits für einige Modelle freigegeben. (ll@ct.de)

## Seagate Ironwolf NAS

### NAS-Festplatte mit 18 TByte Speicherplatz

Hersteller	Seagate, <a href="http://www.seagate.de">www.seagate.de</a>
Modellbezeichnung	ST18000NE000
Anschluss, Protokoll	SATA 6G, AHCI
Straßenpreis	559 €



## Take Five

**Klipschs multifunktionalen Aktivlautsprecher „The Fives“ wollen das Genre der Regalboxen wieder aufleben lassen.**

Der US-Lautsprecherhersteller Klipsch bietet seine aktiven Regalboxen „The Fives“ in zwei Ausführungen an. Die schwarze Version soll an einen nikotinvergilbten Gitarrenverstärker aus dem Proberaum erinnern, die grob gewebte Vollsynthetik-Bespannung wellt sich deshalb schon ab Werk. Die Variante mit Walnuss-Furnier trägt einen feineren Zwirn, der an graues Leinen erinnert. Die magnetischen Abdeckungen lassen sich entfernen, dahinter kommt der Klipsch-typische Tweeter im Horn zum Vorschein, der von einem 4,5-Zoll-Tiefmittentöner unterstützt wird.

Dass da nicht Opas Boxen im Regal stehen, zeigt spätestens ein Blick auf die Rückseite der Steuerbox, in der die gesamte Technik steckt: Sie bietet Anschlüsse für eine HDMI-Quelle (ARC) sowie einen optischen und einen analogen Eingang. Bei letzterem lässt sich der integrierte Entzerrer-Vorverstärker zuschalten, sodass man einen alten Plattenspieler direkt anschließen kann. Eine USB-B-Buchse ermöglicht den Anschluss an einen PC.

Auf der Oberseite der Steuerbox prangt ein ungewöhnlich wuchtiges Bedienpanel mit zwei dicken Stellrädern. Eines dient der Quellenwahl, mit dem anderen steuert man die Lautstärke. Die Installation ist schnell erledigt, die Steuerbox wird an den Strom gehängt und ihr passives Pendant mit dem 4 Meter langen, proprietären Verbindungskabel angeschlossen. Dieses dürfte zwei Meter länger sein, schließlich will man das Kabel möglichst unsichtbar hinter den Möbeln verschwinden lassen.

„The Fives“ lassen sich per Bluetooth mit dem Smartphone koppeln und unter-

stützen dabei neben SBC und AAC auch den aptX-Codec. Am PC geben sie sich als USB-2.0-Audiointerface zu erkennen und erlauben die Soundausgabe von 16 Bit/44 kHz bis 24 Bit/192 kHz. Eine entsprechende Quelle vorausgesetzt, können sie so auch hochauflöste Musik wiedergeben. Per HDMI am TV-Gerät schließlich nehmen sie 2.0-Ton über den Audio Return Channel an. Die Klipsch-Connect-App für iOS und Android dient lediglich dem Update der Firmware. Vom Sofa aus lassen sich die Speaker über die mitgelieferte Infrarot-Fernbedienung bedienen, dabei sind Lautstärke und Bassintensität veränderbar.

Die Klipsch geben Musik äußerst detailreich wieder, akustische Instrumente und Vocals treten besonders plastisch hervor. So hat man in längst bekannt geglaubten Tracks immer mal wieder ein Aha-Erlebnis durch ein zuvor nicht gehörtes Detail. Einzig nervig: „The Fives“ übertreiben es ein wenig mit den tiefen Tönen und klingen selbst bei minimal eingestelltem Bassboost alles andere als neutral.

Die in den Hörnern versenkten Tweeter liefern präzise Höhen. Die räumliche Darstellung ist – eine korrekte Position im Stereofeld vorausgesetzt – exzellent. Davon profitiert man auch, wenn man die Boxen als TV-Soundsystem nutzt. Da die mittig abgemischten Dialoge tatsächlich vor dem Fernseher im Raum stehen, ist die Sprachverständlichkeit überraschend gut. Allerdings wünscht man sich auch hier eine Subwoofer-Einstellung, die nicht nur die Richtung „mehr Bass“ kennt.

Als neutrale Monitorlautsprecher wird man sich „The Fives“ nicht auf den Schreibtisch stellen, rechts und links neben dem TV-Gerät machen Sie aber durchaus eine gute Figur. Im Stereofeld auf der Couch kann man in vollen Sounds vom Smartphone baden oder druckvolles Action-Kino am TV genießen. Spätestens wenn man die alten Vinylscheiben direkt vom Plattenspieler neu erleben darf, bleibt ein Lächeln im Gesicht. (sha@ct.de)

## Klipsch The Fives

### Aktivboxen mit Bluetooth

Hersteller	Klipsch, <a href="https://de.klipsch.com">https://de.klipsch.com</a>
Lieferumfang	2 x Lautsprecher, Kabel, IR-Fernbedienung
Eingänge	HDMI (via ARC), digital (Toslink), analog Cinch (Line/Phono), analog (3,5-mm-Klinke)
Ausgänge	Subwoofer (analog)
Abmessungen	30,5 cm x 16,5 cm x 23,5 cm
Kommunikation	Bluetooth 5.0
Preis	800 €

**MEINE LIEBSTEN FILMSÜNDEN**  
#ESETgeheimeLeidenschaft



Es muss nicht jeder  
alles von Dir wissen,  
schon gar nicht Deine  
besondere Vorliebe  
für Schnulzen.

Teil nur, was Du willst.  
Alles andere bleibt mit  
Sicherheit (D)ein  
Geheimnis.



**eSET**  
ENJOY SAFER  
TECHNOLOGY™

Jetzt testen unter: [ESET.DE](https://www.eset.de)

# Schnelle R-Serie

## Spiegellose Systemkamera Canon EOS R5

**Die spiegellose Systemkamera Canon EOS R5 schließt mit einer Auflösung von 45 Megapixeln und Bildstabilisator zur Konkurrenz auf. In Details legt sie die Messlatte sogar höher.**

Von Peter Nonhoff-Arps

Die EOS R5 hat das Zeug, die EOS-5D-Reihe abzulösen. Denn ihr Kernstück ist ein neuer CMOS-Sensor mit 45 Megapixeln, und wie Nikon und Sony zuvor hat sich nun auch Canon dazu entschlossen, eine interne Bildstabilisierung einzuführen. Sie ergänzt die optische Bildstabilisierung im Objektiv.

Beachtlich ist die Geschwindigkeit: Bei kontinuierlichem Autofokus und mechanischem Verschluss kommt die EOS R5 auf zwölf Bilder pro Sekunde. Der Zwischenspeicher reicht für bis zu 80 Bilder. Die EOS R5 schließt zudem 8K-Video mit 30 Bildern pro Sekunde in 12 Bit Raw.

### Handhabung

Im Unterschied zu den anderen R-Modellen lehnt sich die Bedienung stark an DSLR-Modelle wie die EOS 5D an. Das



**Die Bedienelemente der Canon EOS R5 orientieren sich an Spiegelreflexkameras. Eher untypisch für diese Klasse ist das schwenkbare Display.**

Mode-Rad hat eine Doppelfunktion: Um einen Aufnahmemodus (P, AV, TV, M) zu wählen, muss man zuvor die Taste am Rad drücken. Zum Videomodus gelangt man durch zusätzliches Drücken der Info-Taste. Schön ist, dass die EOS R5 wieder das große DSLR-typische Einstellrad an der Rückseite mitbringt. Das Display ist dreh- und klappbar und per Touch bedienbar.

Der Dualpixel-Sensor setzt Bildpunkte aus jeweils zwei Subpixeln zusammen. Mit diesem Prinzip ist ein schneller Phasenautofokus auf dem Sensor möglich. Deep Learning unterstützt die Motiverkennung beim Verfolgen und Scharfstellen. Sie erkennt nun außer Menschen und Objekten auch Hunde, Katzen und Vögel. Erkannte Motive verfolgt die EOS R5 mit fast schlafwandlerischer Sicherheit auch bei schlechten Lichtverhältnissen.

Der Akku reichte für gut 600 Aufnahmen. In einer Aufnahmepause ließ sich die Kamera selbsterklärend und ohne Probleme mit einem Smartphone verbinden, um erste Ergebnisse zu sehen und zu teilen. Die erforderliche App ist für Android und iOS erhältlich.

### Messwerte und Bildkritik

Die Canon EOS R5 haben wir zusammen mit dem Canon-Objektiv RF 85mm F1.2L USM DS ins Labor geschickt. In dieser Kombination erreichten wir im Bereich ISO 100 bis ISO 800 zentral 100 Prozent der möglichen Auflösung von 2732 Linienpaaren pro Bildhöhe (Lp/Bh). Bei ISO 12.800 sind es immerhin noch 85 Prozent.

Die Fotos der R5 zeigen kaum sichtbares Rauschen (Visual Noise). Es beginnt bei ISO 100 mit einem guten VN von 0,9 und bleibt bis ISO 6400 unter der Zweiermarke. Selbst bei ISO 12800 haben wir noch ein moderates VN von 2,1 ermittelt. Werte unter 0,8 stehen für Rauschfreiheit, bis zwei ist das Rauschen kaum wahrnehmbar, bei Werten bis drei wird es als mäßig störend empfunden.

Der Dynamikumfang des hochauflösenden Sensors kann sich ebenfalls sehen lassen. Bei ISO 100 lag der Wert bei 13,2

Blendenstufen und hielt sich bis ISO 6400 oberhalb von 10 Blendenstufen, danach fiel er kontinuierlich ab. Damit liegt die EOS R5 auf dem Niveau einer Sony A7R IV oder Nikon Z7.

Für Praxisaufnahmen kam im Test das RF 70-200mm F2.8L IS USM zum Einsatz. Vor allem bei niedrigen ISO-Werten gibt die Kamera Details wie Gefieder, Fell oder Holzmaserung plastisch wieder. Insgesamt zeichneten sich die Aufnahmen durch eine sichere Belichtung aus.

### Fazit

Die EOS R5 ist mit 4300 Euro allein für den Body kein Schnäppchen. Für den gleichen Preis bietet die Sony A7R IV 15 Megapixel mehr. Ein Wermutstropfen ist die kurze Akkulaufzeit. Autofokus und Motiverkennung überzeugen hingegen auch bei schnellen Bildraten. Zusammen mit den neuen RF-Objektiven lässt sich der Sensor bis an seine Auflösungsgrenze ausreizen. Die Fotos sind bis in die Details über alle Zweifel erhaben. Und selbst wenn die Empfindlichkeit mal auf extreme ISO-Werte steigt, bleiben die Ergebnisse noch ansehnlich.

(akr@ct.de) **ct**

*Einen ausführlichen Test dieser Kameras lesen Sie in c't Digitale Fotografie 5/2020.*

### Canon EOS R5

Spiegellose Systemkamera	
Sensortyp	CMOS Dual Pixel, Vollformat (36 mm × 24 mm)
Sensorauflösung	45 Megapixel (8192 × 5464)
Lichtempfindlichkeit	ISO 100 - 25.600 (erw. auf ISO 100 - 51.200)
Bildstabilisierung	5-Achsen (IBIS) und objektivseitig
Autofokustyp / Messfelder	Dual Pixel AF / 5940 (1053 auto section)
kürzeste / längste Verschlusszeit	1/8000 s - 30 s / (Bulb)
Serienbildrate / Raw in Folge	12 B/s (mech.), 20 B/s (elektr.) / 180
Max. Videoauflösung / Format	8192 × 4320 Bildpunkte (30p) / AVC/H.265 (MP4)
Suchertyp / Vergrößerung	0,5" OLED / 0,76x
Sucherauflösung	1600 × 1200 Bildpunkte
Displaytyp / Diagonale	LCD / 8 cm (3,15")
Displayauflösung	1024 × 684 Bildpunkte
beweglich / Touch	✓ / ✓
Speichertyp	1 x CFexpress / 1 x SD (UHS-II)
Akku / Aufnahmen	2130 mA (Li-Ion) / 490 (Monitor), 320 (Sucher)
Gehäusematerial / wetterfest	Magnesium, Carbon / ✓
Bodymaße (B × H × T) / Gewicht	136 mm × 98 mm × 88 mm / 738 g
Anschlüsse	USB 3.1 (Typ-C), HDMI (Typ D), Mikrofon, Kopfhörer, Remote
Wireless	WLAN 802.11a/b/g/n/ac, Bluetooth 4.2
Preis (Body)	4385 €

# PUR – Professional User Rating

## Anwender bewerten Anbieter

Managed Services

12. November 2020, 14 – 18 Uhr

### ONLINE-KONFERENZ

**Jetzt  
Ticket  
sichern!**

- Was professionelle Anwender von Managed Services erwarten
- Worauf es bei der Auswahl des richtigen Dienstleisters ankommt
- Welche Anbieter von 2100 Profis am besten bewertet werden
- Warum Managed Services & Co. Fluch und Segen zugleich sind

Preis: 115,00 Euro inkl. MwSt.

[heise-events.de/konferenzen/pur](http://heise-events.de/konferenzen/pur)

©CoreDESIGN



Partner

 **all for one**  
Group

 **Hewlett Packard  
Enterprise**

 **Trustwave**®



# Riesentafeln

## Stift-Tablets Samsung Galaxy S7+ mit 12,4- und S7 mit 11-Zoll-Display

**Je mehr Displayfläche, desto besser kommen Filme, Zeichnungen und Fotos zur Geltung – das gilt natürlich auch für Samsungs neue Stift-Tablets. Doch wie geschickt Android die Fläche nutzt und wie sich gerade das S7+ im Vergleich zu Notebooks oder dem ähnlich großen iPad Pro 12 schlägt, ist eine andere Frage.**

Von Jörg Wirtgen

**F**ür die 2020er-Generation seiner Top-Tablets traut sich Samsung endlich wieder an 12 Zoll Diagonale heran, zuletzt war das 2014 mit dem NotePro 12.2 der Fall (siehe c't 11/2014, S. 114). Dass das S7+ trotz in jeder Hinsicht besserer Leistungs-werte fast 200 Gramm weniger wiegt und einen dünneren Rahmen hat als das sechs Jahre alte Gerät – geschenkt. Schon interessanter: Die Mobilfunk-Version des S7+ nutzt 5G, und die Tastaturhülle hat gegenüber dem Vorgänger Tab S6 eine gelungene Überarbeitung erfahren.

Das S7+ wirkt dank seines schmalen Rands und flachen Gehäuses modern. Es ist 6 Millimeter dick, aus der planen Rückseite lugt nur ein kleiner Kamerabuckel

hervor. Der mitgelieferte Stift haftet wie beim Vorgänger magnetisch an einer Fläche neben der Kamera. Für den Transport in der Wohnung hält er sicher genug, in Taschen fällt er schnell ab.

Das Display erweist sich OLED-typisch als äußerst farbkräftig und kontraststark, dank hoher Auflösung erkennt man keine einzelnen Pixel. Man kann es auf eine Bildwiederholfrequenz von 120 Hz stellen; dann werden vor allem Scrollbewegungen flüssiger dargestellt.

### Android auf 12 Zoll

Einige Anwendungen machen auf der großen Fläche sofort Spaß, erst recht, wenn man den Stift einsetzen kann: Zeichnen, Mitschreiben oder Korrekturlesen etwa. PDF-Editoren und Magazin-Apps stellen eine DIN-A4-Seite ganz gut lesbar dar.

Auch Videos profitieren, wobei SD- und HD-Videos pixelig wirken; mindestens Full HD sollte man sich auf den 2800 × 1752 Pixel gönnen – oder besser noch 4K. Amazons Prime-App erkannte das S7+ allerdings bis Redaktionsschluss nur als SD-fähig an. Netflix hingegen spielte in 4K. Die Lautsprecher tönen mit leichtem Bass und recht klar.

Andere Apps tun sich schwerer mit der großen Displayfläche. OneNote beispielsweise öffnet Notizen immer im Vollbild mit einem so ungeschickten Zoomfaktor, dass die rechten zwei Drittel des Displays ungenutzt sind; auch wünscht man sich die zusätzlichen Zeichenfunktionen der Windows-Version. In Textverarbeitungen vermisst man eine Zweiseitensicht.

Android bietet immerhin eine „geteilte Bildschirmansicht“, wenn man beim App-Umschalten auf das Icon einer gestarteten App tippt. So bekommt man zwei Apps nebeneinander mit verstellbarem Mittelsteg. So richtig praktikabel ist das aber nicht, beispielsweise fehlt eine Möglichkeit, eine App direkt in diesem Modus zu starten.

Besser gefällt Samsungs spezieller Desktop-Modus DeX (siehe auch S. 106). Der ist seit einigen Generationen in High-End-Tablets und -Smartphones eingebaut und startet, sobald man einen Monitor per USB-C oder Miracast anschließt. Beim S7+ lässt er sich auch auf dem internen Display aktivieren. Apps starten dann in einzelnen Fenstern, die sich per Finger verschieben (hier merkt man die 120 Hz angenehm) und vergrößern lassen. Ähnlich wie unter Windows wird ein Fenster auf die halbe Displaygröße gesetzt, wenn man es an den linken

oder rechten Rand schiebt; an den oberen Rand geschoben wird es maximiert.

## Hardware und Kamera

Die Hauptkamera nimmt ganz ordentliche Fotos auf, solange das Licht reicht. Mit den Kameras von Top-Smartphones hält sie nicht mit, aber um etwa seine Papier-Korrespondenz zu digitalisieren oder Flipcharts festzuhalten, genügt sie.

Dank Snapdragon 865+ gehört das S7+ zu den schnellsten Android-Geräten. In der Praxis sind für alle Apps und 3D-Spiele genügend Leistungsreserven vorhanden. Die Laufzeiten fallen gut, aber nicht rekordverdächtig aus. Der 120-Hz-Betrieb kostet rund 20 Prozent Laufzeit, beispielsweise fällt sie beim Videostreaming von 13,1 auf 10,3 Stunden.

Wie bei den Note-Smartphones kann man bei ausgeschaltetem Display direkt eine Notiz starten. Dort reicht es, den Stift herauszuziehen; bei den Tabs muss man bei gedrückter Taste zweimal aufs Display tippen und beim zweiten Mal losschreiben – wenig intuitiv. Diese Notizen landen in Samsungs Notiz-App. Deren versprochene Synchronisierung mit OneNote fehlt weiterhin, Samsung will sie im November nachliefern.

## Tastatur und Ständer

Für 225 Euro hat Samsung die Tastaturhülle „Book Cover Keyboard“ im Angebot. Sie besteht aus zwei Teilen, einem Ständer (221 g, 3 mm) für die Rückseite des Tablets und einer Tastatur (284 g, 6 mm), die an der Unterseite hängt; beide halten magnetisch und sind einzeln schnell abgenommen. Die Tasten haben einen angenehmen Druckpunkt und liegen in einem für Zehnfingerschreiber noch brauchbaren Raster von 18,3 Millimeter; im Dunkeln wünscht man sich eine Tastenbeleuchtung. Ein recht großes (10 cm × 5,5 cm) Touchpad ist eingebaut; beim Anschließen erscheint der – von Android schon immer vorgesehene – Mauszeiger. Allerdings interpretiert das Touchpad versehentliche Berührungen als Mausbewegung. Das passiert manchmal beim Zehnfingerschreiben mit dem Handballen, aber auch beim Zeichnen, wenn man den Unterarm auf der Tastatur abstützt.

Der Ständer stellt das Tablet stabil in beliebigem Winkel zwischen etwa 5 und 80 Grad auf. An der Oberseite hat er ein kleines Fach für den Stift und ein Loch für die Kamera. Wer ihn auch bei abgenommener Tastatur am Gerät lässt, verliert den Stift beim Transport in der Tasche nicht

mehr und stellt das Tablet bei jeder Gelegenheit von Tisch über Schoß bis Bett einfach auf, statt es halten zu müssen. Der Ständer lässt sich aber auch einfach abnehmen und wieder anklicken – ganz anders als der per Unterdruck haltende und zum Herunterfallen neigende Ständer des Vorgängers Tab S6. Das günstigere „Book Cover“ ohne Tastatur entspricht übrigens nicht diesem Ständer, sondern erlaubt nur zwei feste Aufstellwinkel.

## Galaxy Tab S7

Der kleine Bruder des Tab S7+ ist das Tab S7 – es ist so groß wie bisherige 10-Zoll-Tablets, hat aber dank dünnerem Rand ein 11-Zoll-Display. Das IPS-Panel gehört mit DCI-P3-Farbraum und fast 400 cd/m<sup>2</sup> zu den besten, wird vom OLED des S7+ aber knapp übertroffen: Das ist vor allem dank sattem OLED-Schwarz kontraststärker, zudem heller und minimal farbkräftiger. Die übrige Ausstattung inklusive Kamera und Prozessor ist weitgehend identisch, wobei die Mobilfunk-Variante nur LTE bietet, kein 5G. Die Laufzeiten sind spürbar länger. Ein kleiner Unterschied: Der Fingerabdruckscanner ist im Einschalter an einer Längsseite eingebaut; beim S7+ sitzt er unter dem Display.

Die Tastaturhülle fällt naturgemäß kleiner aus. Sie war bis Redaktionsschluss nicht lieferbar; Produktfotos zufolge dürfen die Tasten im für Zehnfingerschreiber

nicht so gut geeigneten 17-Millimeter-Raster liegen.

## Fazit

Größte Nachteile des Tab S7 und Tab S7+ sind Android selbst – was Samsungs DeX-Modus etwas ausgleicht – und die wenigen Apps, die die Displayfläche sinnvoll ausnutzen. Mehr auf Tablets angepasste Apps gibt es für iPad OS, allerdings kosten die iPads in vergleichbarer Konfiguration mehr als die Samsung-Tablets, erst recht, wenn man Tastaturhülle und Stift dazu rechnet. Das noch größere Software-Angebot der Windows-Tablets wiederum erkaufst man sich mit höherer Komplexität und nicht ganz so touchkonformer Bedienung (siehe c't 15/2020, S. 58).

Somit geben die Samsung-Tablets hervorragende Android-Tablets ab. Wem 11 Zoll reichen, der findet im Tab S7 einen nahezu fehlerfreien, aber mit fast 700 Euro recht teuren Kandidaten. Benötigt man keine Tastaturhülle, bieten auch das deutlich günstigere Tab S6 und unter Abstrichen beim Display das Tab S6 Lite eine Menge.

Faszinierender ist das S7+ mit der riesigen Displayfläche und der Tastaturhülle – im Android-Markt ist es konkurrenzlos. Und auch wenn sich lange nicht alle Android-Apps auf 12 Zoll wohlfühlen, springt der Funke schon bei einigen wenigen Lieblings-Apps über – Filme, Zeichnungen und Fotos.

(jow@ct.de) ct

## Android-Tablets

Modell	Samsung Galaxy Tab S7+	Samsung Galaxy Tab S7
Hersteller / Farben, Varianten	Samsung / Bronze, Schwarz, Silber	Samsung / Bronze, Schwarz, Silber
Betriebssystem / Security Level	Android 10 / Juli 2020	Android 10 / Juli 2020
Display	12,4 Zoll OLED / 267 mm × 166 mm / 2800 × 1752 Pixel / 266 dpi / 2 ... 527 cd/m <sup>2</sup> / Farbraum NTSC	10,9 Zoll IPS / 235 mm × 146 mm / 2560 × 1600 Pixel / 277 dpi / 4 ... 362 cd/m <sup>2</sup> / Farbraum DCI-P3
<b>Kamera</b>		
Hauptkamera	12,8 MP / f/2 / 4128 × 3096	12,8 MP / f/2 / 4128 × 3096
Weitwinkelkamera	5 MP / f/2,2 / 2576 × 1932 (12 mm)	5 MP / f/2,2 / 2576 × 1932 (12 mm)
Frontkamera	8 MP / f/2 / 3264 × 2448	8 MP / f/2 / 3264 × 2448
<b>Ausstattung</b>		
Prozessor / Kerne × Takt / GPU	Qualcomm Snapdragon 865+ / 1 × 3,1 GHz, 3 × 2,4 GHz, 4 × 1,8 GHz / Adreno 650	Qualcomm Snapdragon 865+ / 1 × 3,1 GHz, 3 × 2,4 GHz, 4 × 1,8 GHz / Adreno 650
RAM / Flash-Speicher / Kartenslot	8 GByte / 256 GByte (230 GByte) / ✓ (MicroSD)	6 GByte / 128 GByte (102 GByte) / ✓ (MicroSD)
LTE / 5G / SIM / SAR-Wert <sup>1</sup>	Cat. 20+18 / ✓ / nanoSIM / 1 W/kg	–
USB-Anschluss / Kopfhöreranschluss	USB-C (3.1), OTG, DP / –	USB-C (3.1), OTG, DP / –
Akku / Drahtlosladen	10090 mAh / –	8000 mAh / –
Abmessungen / Gewicht	18,9 cm × 28,5 cm × 0,7 cm / 570 g	16,5 cm × 25,4 cm × 0,7 cm / 504 g
<b>Messungen, Laufzeiten, Benchmarks</b>		
Laufzeiten bei 120 Hz und 200 cd/m <sup>2</sup> Helligkeit	9,5 h lokales Video / 7 h Surfen / 10,3 h Videostream	12,9 h lokales Video / 12,8 h Surfen / 12 h Videostream
Coremark Single / Multi / 3DMark	23326 / 95699 / 7017 (Sling Shot Extreme)	23313 / 97723 / 7197 (Sling Shot Extreme)
Geekbench V4 / V5 (je Single, Multi)	4488, 13065 / 961, 2981	4506, 13139 / 970, 3129
Listenpreis / Straßenpreis	954 € (Wi-Fi/256/8), 1149 € (5G/256/8) € / 899 € (WiFi/128/6)	681 € (Wi-Fi/128/6), 779 € (LTE/128/6) € / –

<sup>1</sup> Herstellerangabe

2x Make testen  
und 6 € sparen!

#### Ihre Vorteile:

- ✓ **GRATIS dazu:** Arduino Nano
- ✓ Zugriff auf Online-Artikel-Archiv\*
- ✓ **NEU:** Jetzt auch im Browser lesen!
- ✓ Zusätzlich digital über iOS oder Android lesen

Für nur 15,60 Euro  
statt 21,80 Euro.

**Jetzt bestellen:**  
[make-magazin.de/miniabo](http://make-magazin.de/miniabo)



## Gadget-Update

**Sony's Noise-Cancelling-Headsets der 1000er-Serie waren schon immer gut. Mit dem WH-1000XM4 wird (fast) alles noch besser.**

Die vierte Generation des WH-1000XM ist von ihrem Vorgänger äußerlich kaum zu unterscheiden. Ein leicht matteres Finish des schwarzen Modells und das nun geprägte statt gedruckte NFC-Logo auf der linken Ohrmuschel fallen kaum auf. Erst wenn man ihn abnimmt, sieht man ein kleines Sensorfenster zum Erkennen des Tragestatus. Nimmt man den 1000XM4 vom Kopf, pausiert die Musikwiedergabe eines per Bluetooth gekoppelten Geräts automatisch. Setzt man ihn wieder auf, geht es weiter.

Der Kopfhörer funktioniert auch ohne Sonys Headphone-App (iOS, Android), aber es lohnt sich, sie zu installieren. Sie versorgt den 1000XM4 mit Updates und erlaubt den Zugriff auf weitere Funktionen. So lassen sich etwa Sound- und Noise-Cancelling-Einstellungen automatisch in Abhängigkeit vom Aufenthaltsort umstellen. Einmal angelernt, optimiert sich der Sound beim täglichen Pendeln somit in Abhängigkeit von der jeweiligen Geräuschkulisse automatisch. Ebenfalls neu: Die optionale Funktion „Speak-to-Chat“, bei der der Kopfhörer die NC-Funktion automatisch ausschaltet und Außengeräusche weiterleitet. Sie aktiviert sich, sobald man einen Ton von sich gibt – leider auch bei Gemurmel oder dem Mitträgern von Liedern.

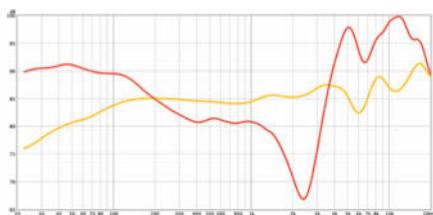
Der WH-1000XM4 lässt sich per Klinkenkabel oder Bluetooth anschließen.

Via Bluetooth 5.0 verbindet man ihn dabei mit bis zu zwei Quellen gleichzeitig. Das ist in Zeiten des Homeoffice besonders praktisch: Hat man beispielsweise Notebook und Smartphone parallel verbunden, wandert der Fokus automatisch von der Videokonferenz zum Handy, sobald man dort einen Anruf annimmt.

Die Steuerung per Touch an der rechten Ohrmuschel ist geblieben. Mit ein wenig Übung lässt sich die Lautstärke justieren oder zwischen Titeln hin und her wischen. Der einzige Taster neben dem Power-Taster ist jetzt als Funktionsbutton „Custom“ gekennzeichnet. Damit wechselt man zwischen den drei NC-Modi (aus, Außengeräusche nach innen, an); alternativ aktiviert man Amazons Alexa oder den Google Assistant.

Der Klang ist hervorragend, vom Vormodell allerdings nicht zu unterscheiden. Nach wie vor kann man die Klangeigenschaften durch das Abfotografieren der Ohrform über die Headphone-App optimieren, sollte dabei allerdings keine zu großen Klangveränderungen erwarten. Mit LDAC unterstützt der Kopfhörer einen Codec, der auch hochauflöste Musik per Bluetooth überträgt. Einziger Pferdefuß: Der ebenfalls recht beliebte aptX-Codec und dessen HD-Variante werden nicht mehr unterstützt.

Guter Tragekomfort, super Klang, effektive Geräuschunterdrückung – der WH-1000XM4 ist ein Fest für die Ohren. Mit den hinzugekommenen Funktionen ist er sogar noch etwas effektiver für den Arbeitsalltag geworden. (sha@ct.de)



Im Vergleich zum neutralen Sennheiser HD-600 (gelb) senkt der Sony WH-1000XM4 (rot) die Mitten deutlich ab.

## Sony WH-1000XM4

Bluetooth-NC-Headset	
Hersteller	Sony, <a href="http://www.sony.de">www.sony.de</a>
Konnektivität	Bluetooth 5.0 (A2DP, HFP), zwei Quellen gleichzeitig
Laufzeit	23 h
Preis	370 €



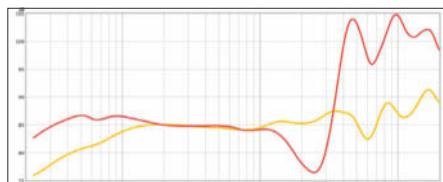
## Detailversessen

**Sennheisers Kopfhörer HD 560S**  
kitzelt extreme Details aus der Musik.

Der HD 560S ist laut Sennheiser ein Kopfhörer für „analytical listening sessions“. Dank einer neuen Polymerblend-Folie im Wandler schält der offene Kopfhörer selbst kleinste Details heraus. Musikfans entdecken neue Feinheiten und Produzenten entlarven schnell Fehler im Mix.

Eine Höhenbetonung von 3 bis 4 Dezibel (im Hörvergleich mit Terzbandrutschen) ab 4 kHz unterstützt die hervorragende Räumlichkeit, lässt den HD 560S im Vergleich zum Sennheiser HD 600 aber recht hart und gnadenlos wirken. Bei der Abstimmung eines Mixes sollten Produzenten das berücksichtigen.

Das geringe Gewicht von 237 Gramm und die weiche, ohrumschließende Polsterung sorgen für hohen Komfort. Das drei Meter lange, glatte Kabel lässt sich leider nicht wechseln. Die Nenn-Impedanz von 120 Ohm eignet sich selbst für mobile Zuschauer. Bislang musste man für eine derartige Akustiklupe weit über 500 Euro ausgeben. Sennheiser verlangt knapp 200 Euro – für solch ein Präzisionswerkzeug ein Schnäppchen. (hag@ct.de)



Im Vergleich zum Sennheiser HD 600 (gelb) betont der 560S (rot) die Höhen ab 4 kHz.

### Sennheiser HD 560S

#### Offener Kopfhörer mit Kabelanschluss

Hersteller	Sennheiser, <a href="http://www.sennheiser.de">www.sennheiser.de</a>
Anschluss	6,3-mm-Stereo-Klinke, Adapter auf 3,5 mm
Preis	199 €

## Flexible Zeiten

**Amazons smarter Lautsprecher „Echo Flex“** lässt sich über seinen USB-Port mit Zusatzmodulen ausrüsten. Nach Bewegungssensor und Nachtlicht ist nun eine Uhr verfügbar.

Um das neue Modul nutzen zu können, mussten wir bei unserem Echo Flex (Test in c't 26/2019, S. 82) mit dem Sprachbefehl „Alexa, suche nach Software-Update“ zunächst die aktuelle Firmware-Version aufspielen. Das dauert rund dreißig Minuten. Danach erkannte der Smart Speaker die Uhr und sie tauchte auch in der Alexa-App auf dem Smartphone auf.

Wie beim Echo Dot mit Uhr (Test in c't 26/2019, S. 82) ist im Flex-Uhrenmodul ein Umgebungslichtsensor integriert, mit dessen Hilfe das Gerät die Helligkeit der Anzeige automatisch reguliert. Und wie dort kann der Nutzer die Helligkeit auch manuell festlegen – was hier aber ausschließlich über Sprachbefehle am Flex läuft und nicht über die App.

Startet man über Alexa einen Timer, zeigt das Modul den passenden Countdown an – wie beim Echo Dot mit Uhr. Der Dot kann darüber hinaus aber auch die aktuelle Temperatur anzeigen, wenn man Alexa danach fragt.

Das Uhrenmodul von Third Reality, das exklusiv von Amazon für rund 20 Euro angeboten wird, ist eine sinnvolle Erweiterung für den Echo Flex, um beispielsweise in der Garage die Zeit im Auge zu behalten. Dank regulierbarer Helligkeit lässt es sich aber auch gut in Wohnräumen einsetzen. Wichtig: An den Echo-Flex-Modulen befindet sich kein USB-Port, sodass sich immer nur ein Zusatzgerät zurzeit nutzen lässt. (nij@ct.de)

## Third Reality Smart Clock

#### Uhrenmodul für Echo Flex

Hersteller	Third Reality, <a href="http://www.3reality.com">www.3reality.com</a>
Display	vierstelliges LCD mit Helligkeitsregulierung
Anschluss	USB-Stecker (Typ A)
Preis	19,99 €

Deutschlands  
größter Kongress für  
Embedded Software  
Professionals

Rund 100 Expertenvorträge –  
15 Kompaktseminare –  
Aussteller-Track



#### KEYNOTE

Software Engineering für  
komplexe Cyber-Physical  
System Designs  
Ralf Reussner, Karlsruhe  
Institute of Technology (KIT)

#### WEITERE VORTRÄGE ZU:

- Architektur & Design
- C/C++ für Embedded
- Open Source & Linux
- Safety & Security
- KI & Machine Learning
- Software-Test & Qualität
- uvm.

Jetzt buchen  
und sparen!  
Frühbisher bis  
31. Oktober

PROGRAMM UND ANMELDUNG UNTER:  
[www.ese-kongress.de](http://www.ese-kongress.de)



Embedded Software Engineering Kongress

# 2020

30. November bis 4. Dezember

VERANSTALTER

ELEKTRONIK  
PRAXIS

MICROCONSULT

GOLDSPONSOREN

axivion  
stopping software erosion

Green Hills  
SOFTWARE

# Micro:Bit-Kumpel

## Kosmos-Experimentierkasten für den Coder-Nachwuchs

**Programmierbare Spielzeugroboter haben oft nur ein Spatzenhirn und ein sehr begrenztes Repertoire an Kunststückchen. Anders beim „Proxi“ von Kosmos: In seinem Kopf steckt ein BBC Micro:Bit. Er bietet vielfältige Möglichkeiten und einen kindgerechten Einstieg in die Programmierung.**

Von Dorothee Wiegand

Wie einen Rucksack trägt der Roboter zwei kleine Elektromotoren an der Rückseite. Sie treiben die sechs Beine an, die den runden Bauch des Proxi tragen. Je drei davon berühren den Boden, während die anderen drei ihre Position ändern – die Art der Fortbewegung erinnert an krabbelnde Spinnen. Auf dem Körper sitzt ein großer Kopf, der eine fest eingebaute Platine beherbergt. Sie dient als Connector für den BBC Micro:Bit. Auch das Batteriefach, ein Buzzer für die Audioausgabe sowie eine Reihe Infrarotsensoren befinden sich in dem etwa apfelformigen Kopf. Um den Micro:Bit in die eingebaute Platine einzusetzen, muss man eine Art Visier aufklappen.



Für die Steuerung des Proxi gibt es im MakeCode-Editor für den Micro:Bit eine eigene Befehlskategorie.

Ein USB-Kabel, über das Programm-Code auf den Micro:Bit überspielt wird, lässt sich auch bei geschlossenem Visier anschließen.

### Bastelstunde

Nach dem Kauf muss der kleine Roboter erst zusammengeschraubt werden. Vier Kunststoffgitter mit teils sehr filigranen Bauteilen liegen im Karton, dazu zwei Beutel mit Zahnrädern und Schrauben sowie die Elektromotoren, Kabel, der Micro:Bit, die Connector-Platine und eine Bauanleitung. Jüngere Bastler brauchen unbedingt Unterstützung, denn während des Zusammenbauens – im Test dauerte es gut vier Stunden – gibt es immer mal wieder knifflige Momente. Die Bauanleitung, ein Heft im DIN-A5-Format, erinnert an Möbelbaupläne von Ikea. Der fertige Roboter ist nicht klapprig, allerdings auch nicht extrem robust. Wir haben es im Test nicht übers Herz gebracht, es auszuprobieren, vermuten aber, dass er bei einem Sturz vom Tisch Schaden nähme.

Wenn alles richtig zusammengebaut wurde und schließlich noch vier AAA-Batterien eingelegt sind, ist der Proxi bereit für einen Funktionstest. Das Programm dafür sowie 14 weitere vorbereitete Micro:Bit-Programme gibt es auf der Kosmos-Website zum Download (siehe ct.de/yxx7). Je nachdem, welches der Programme man auf den Micro:Bit hinter dem Visier überträgt, folgt Proxi beispielsweise einer vorgehaltenen Hand, piepst, blinkt, simuliert einen Spielwürfel oder spielt „Stein, Schere, Papier“. Es gibt auch eine Datei fürs Bluetooth-Pairing mit einem Smartphone. Mit der kostenlosen Proxi-App für iOS und Android kann man das Kerlchen anschließend fernsteuern oder Textbotschaften aufs 5x5-LED-Display schicken.

Alle vorbereiteten Micro:Bit-Programme funktionierten im Test gut. Im Online-Editor von Microsoft, der wahlweise MakeCode-Blöcke oder JavaScript bearbeitet, lassen sie sich hochladen und



Hinter dem Visier des Proxi von Kosmos befindet sich der Standard-Einplatinencomputer BBC Micro:Bit.

modifizieren. Der Proxi gehört zu den von der „Micro:bit Educational Foundation“ anerkannten sogenannten „accessories“. Zur Steuerung seiner Bewegungen hat Kosmos dem Editor die Befehlskategorie „Proxi“ hinzugefügt. Sie umfasst Befehle, mit denen man IR-Werte auslesen und Proxi tanzen oder stampfen lassen kann.

### Fazit

Der kleine Spielzeugroboter verleiht dem BBC Micro:Bit ein Gesicht und eine Gestalt. Die vorbereiteten HEX-Dateien mit Beispielprogrammen erleichtern den Einstieg ins Coden. Sie lassen sich leicht abwandeln, bevor es später an die Umsetzung eigener Programmierideen geht. So wird der Einplatinencomputer auch für jüngere Kinder gut zugänglich. Weil der knuffige Proxi dazu motiviert, ihm immer wieder neue Tricks beizubringen, ist für langen Spaß gesorgt – wenn die Mechanik des Roboterchens es denn mitmacht.

(dwi@ct.de) ct

**Programm-Download:** [ct.de/yxx7](http://ct.de/yxx7)

### Kosmos Proxi

Elektronikbaukasten / Spielzeugroboter	
Hersteller	Kosmos, <a href="http://www.kosmos.de">www.kosmos.de</a>
Systemanf.	PC, Internet-Zugang / App zur Fernsteuerung: Android ab 6.0, iOS ab 11.0
Stromversorgung	4 x 1,5-Volt-Batterie (AAA)
Altersempfehlung	10 bis 16 Jahre
Preis	90 €



## Konferenz-Satellit

**Die Videokonferenzkamera MeetUp von Logitech vereint große Teams in kleinen Konferenzräumen.**

MeetUp bringt Arbeitskollegen, Vereinsmitglieder oder Lerngruppen zusammen. Beim Setup bleiben wenig Fragen offen – man sollte sich nur überlegen, wo man die Kamera anbringen möchte. In der Lieferung enthalten sind eine Tisch- und eine Wandhalterung – um sie direkt mit dem Bildschirm zu verbinden, gibt es eine optionale TV-Halterung für 99 Euro. Hat man einen Ort für die 1,04 Kilogramm leichte MeetUp gefunden, ist sie per Plug & Play in wenigen Minuten einsatzbereit: Dafür verbindet man die Kamera per HDMI- und USB-Kabel mit einem Rechner, auf dem ein Videokonferenzprogramm läuft, und wählt sie anschließend als Kamera, Lautsprecher und Mikrofon aus.

MeetUp funktioniert mit allen gängigen Videokonferenzprogrammen wie Teams, Jitsi oder Skype. Standardmäßig überträgt die Kamera Bilder mit einer Auflösung von 1080p – verbindet man sie per USB 3.0, gehen 4K. Wohin sie zeigt, lässt sich bei Bedarf per Fernbedienung steuern. Zudem erkennt sie, wenn Personen sich bewegen oder neue Konferenzteilnehmer den Raum betreten und stellt diese automatisch scharf. Die automatische Bildeinstellung erfordert Windows 10 oder macOS ab Version 10.14.

Außer mit der Fernbedienung können iPhone-Nutzer die Kamera via Bluetooth mit der App „Logitech Conference-

Cam-Fernbedienung“ steuern. Im Test funktionierte das mit der App -Version 1.0.75 auf einem iPad Pro mit iPados 13.1.1 problemlos. Für Android-Smartphones gibt es keine App.

Das Mikrofon überträgt Frequenzen von 90 Hz bis 16 kHz. Um alle Teilnehmer gut zu verstehen, empfiehlt Logitech maximal sechs Konferierende im Raum. Bei unserem Test hat das in einem circa 6 × 6 Meter großen Konferenzraum gut geklappt – die Teilnehmer waren vier Meter von der Kamera entfernt klar zu sehen und gut zu verstehen. Die empfohlene Teilnehmerzahl lässt sich mit dem Zusatzmikrofon für MeetUp auf acht Konferierende erhöhen. Dieses schlägt noch mal mit 250 Euro zu Buche.

Mit der MeetUp-Videokonferenzkamera sind kleinere Konferenzräume gut für Videokonferenzen ausgestattet. Durch den hohen Preis für die Kamera und optionale Zusatzgeräte ist sie eher für Firmen und Vereine als für Privatpersonen geeignet und das auch nur, solange keine Menschenleben vom Funktionieren der Kamera abhängen: In seiner Software-Lizenzvereinbarung weist Logitech darauf hin, dass die Software nicht für Einsätze in Bereichen wie Atomkraftwerken lizenziert ist, in denen ein Ausfall des Produktes zum Tod oder zu Umweltschäden führen kann. (kim@ct.de)

## Logitech MeetUp

### Videokonferenzkamera

Hersteller	Logitech, <a href="http://www.logitech.com">www.logitech.com</a>
Anschlüsse	USB 2.0 und 3.0, Bluetooth
Betriebssysteme	Windows 7 oder höher, macOS ab Version 10.10
Preis	1099 €

**Mit allen Wassern gewaschen:**



iX Developer  
Moderne Softwareentwicklung  
[shop.heise.de/ix-software20](http://shop.heise.de/ix-software20)  
9,99 €

NEU



iX Kompakt Container 2020  
[shop.heise.de/ix-container20](http://shop.heise.de/ix-container20)  
12,99 €

NEU



iX Developer  
Moderne Softwarearchitektur  
[shop.heise.de/ix-dev-msa20](http://shop.heise.de/ix-dev-msa20)  
12,99 €

NEU

Weitere Sonderhefte zu vielen spannenden Themen finden Sie hier:  
[shop.heise.de/specials-aktuell](http://shop.heise.de/specials-aktuell)

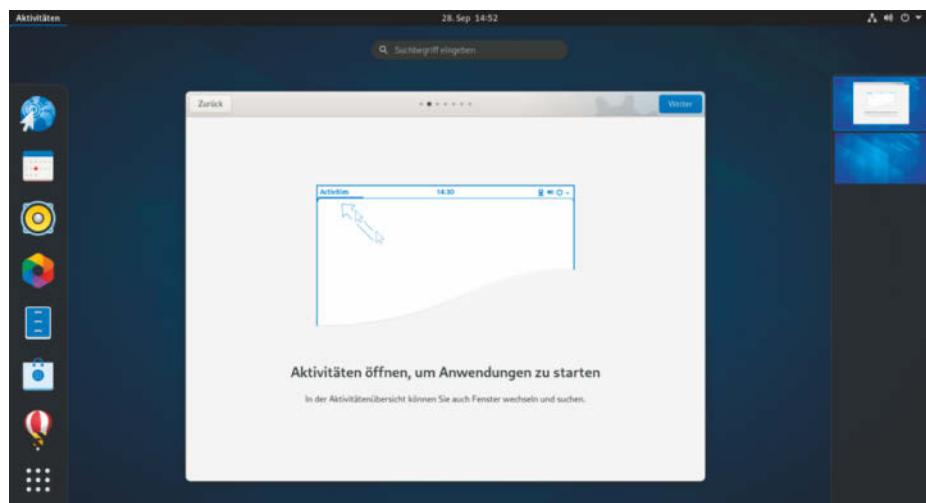
Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.



**heise shop**

[shop.heise.de/specials-aktuell](http://shop.heise.de/specials-aktuell)





# Gnome heißt willkommen

## Linux-Desktopumgebung Gnome 3.38

**Die neue Gnome-Oberfläche wirkt moderner und lässt sich individuell anpassen. Der Browser Gnome Web baut den Trackingschutz aus und es gibt einen verbesserten Multimonitorbetrieb.**

Von Keywan Tonekaboni

**M**it überschaubaren Schritten geht es bei der Gnome-Desktop-Umgebung voran. Die Entwickler der Bedienoberfläche für Linux- und Unix-Systeme haben in Version 3.38 sowohl die sichtbaren Bedienelemente als auch die darunterliegenden Komponenten überarbeitet.

Sind mehrere Monitore angeschlossen, kann Mutter jetzt im Wayland-Modus diese mit individueller Bildwiederholrate ansteuern. Der Window-Manager soll die Inhalte schneller zeichnen, wenn der Bildschirm dies anbietet. Läuft ein Programm oder Spiel im Vollbildmodus, kann der Compositor umgangen werden, um die Inhalte direkt auf den Monitor anzuzeigen, was CPU und Grafikchip entlastet.

Die in die Gnome-Shell integrierte Bildschirmaufzeichnung (Strg+Alt+Shift+R) wurde in einen eigenen Dienst ausgelagert und verwendet jetzt PipeWire und Kernel-Schnittstellen. Davon profitieren derzeit Systeme mit Intelgrafik durch flüssigere Aufzeichnungen.

Gnome 3.38 enthält die Desktopsuchmaschine Tracker zusätzlich in Version 3, mit der sich kontrollieren lässt, auf welche Daten Flatpak-Apps Zugriff haben.

### Flexible Anwendungsübersicht

Nach der ersten Anmeldung in Gnome begrüßt eine Willkommens-Tour und erklärt mit einigen Schautafeln die Besonderheiten der Gnome-Oberfläche und deren Bedienung.

In der Vorversion haben die Gnome-Entwickler den Umbau der starren Anwendungsübersicht begonnen, woran sie bei 3.38 anknüpfen. Die Reihenfolge der App-Starter lässt sich beliebig verändern und ist nicht auf die alphabetische Sortierung festgelegt. Ordner mit mehreren Startern können jetzt auch weitere Unterseiten haben. Statt die Icons am Bildschirmrand abzuschneiden, werden sie abhängig zur Monitorauflösung so angeordnet und skaliert, dass maximal 24 Starter zu sehen sind.

Optisch aufgepeppt wurden die Gnome-Apps „Tonaufzeichner“, das Programm für Bildschirmfotos und die Uhren-App. Die Dialoge wirken deutlich moderner und übersichtlicher. Die Karten-App verfügt nun über Satellitenaufnahmen und einen Nachtmodus. Der Browser Gnome Web, ehemals Epiphany, kann Einstellungen aus Chrome importieren und hat einen verbesserten Trackingschutz, der standardmäßig aktiv ist.

Gnome verbessert die Anmeldung per Fingerabdruck durch einen überarbeiteten Einrichtungsdialog in den Einstellungen. Richtet man einen WLAN-Hotspot ein, werden dessen Daten als QR-Code angezeigt, was bei der Konfiguration auf den Clients Tipparbeit spart.

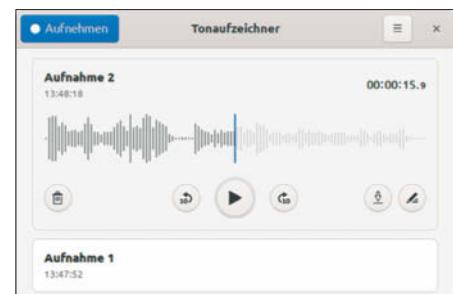
Laut Release Notes gibt es auch einen Schutz vor unberechtigten USB-Geräten bei aktiver Bildschirmsperre sowie eine Kindersicherung, um den Zugriff mit Regeln einzuschränken. Beides konnten wir allerdings weder im neuen Gnome-OS-Image, einer Spezialdistribution zur Vorschau für Entwickler, noch in der Vorabversion von Fedora 33 finden.

Das Systemmenü zeigt jetzt den Akkuladestand auch in Prozent an und verfügt über eine separate Option zum Neustarten des Rechners. Hält man während des Bestätigungsdialogs die Alt-Taste gedrückt, versucht Gnome, in das Computer-Startmenü zu booten.

### Ausprobieren

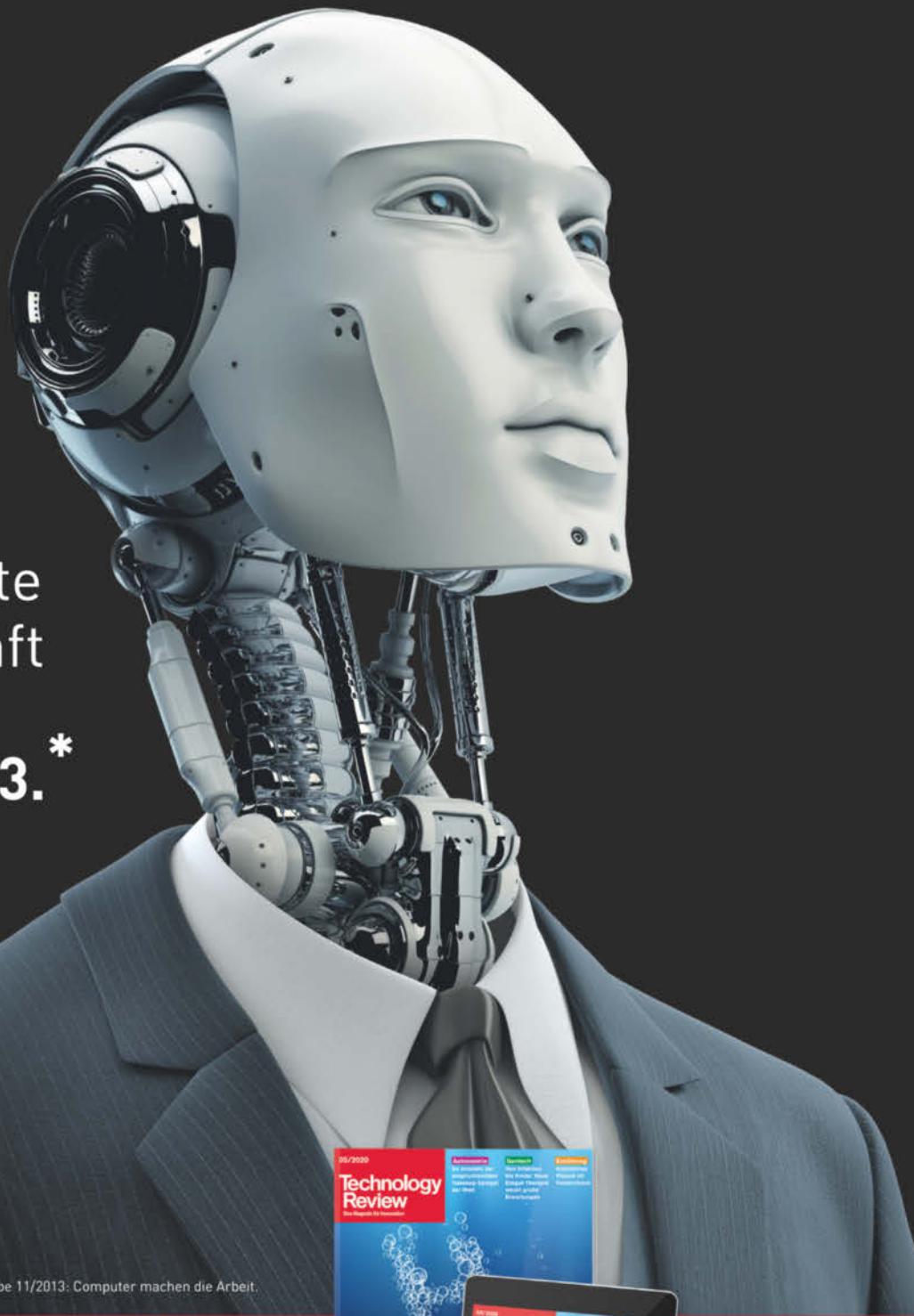
Um Gnome 3.38 zu testen, installieren Sie aus Flathub die Virtualisierungssoftware Gnome Boxen 3.38. Laden Sie dann das Gnome-OS-Image herunter (siehe [ct.de/yau1](http://ct.de/yau1)) und öffnen es in Boxen. Ausgeliefert wird das neue Gnome mit Ubuntu 20.10 und Fedora 33, die diesen Herbst erscheinen, sowie sukzessive in Arch Linux und openSUSE Tumbleweed. (ktn@ct.de) **ct**

**Gnome-OS-Download:** [ct.de/yau1](http://ct.de/yau1)



**Der Soundrekorder lässt sich seit der Neugestaltung einfacher bedienen.**

Alle reden heute  
über die Zukunft  
der Arbeit –  
**wir seit 2013.\***



\*Ausgabe 11/2013: Computer machen die Arbeit.

**Testen Sie 3 Ausgaben Technology Review mit 35 % Rabatt.**

Jetzt bestellen: [trvorteil.de/testen](http://trvorteil.de/testen)

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

 +49 541/80 009 120

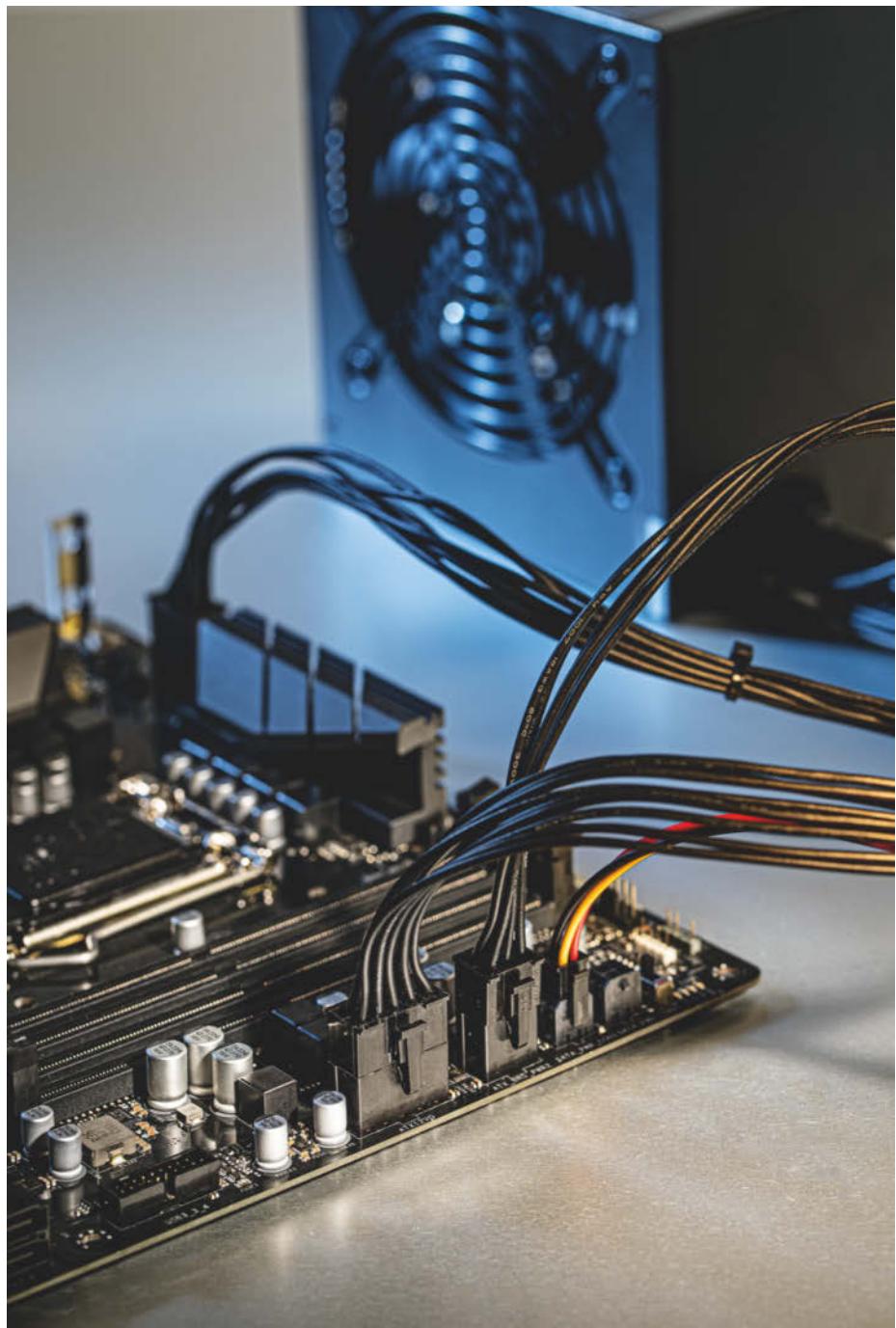


+ Ihr  
Geschenk:



Smartwatch

Lesen, was wirklich zählt in Energie,  
Digitalisierung, Mobilität, Biotech.



**Intel hat eine Alternative zur ATX-Spezifikation entwickelt, bei der Mainboards und Netzteile ausschließlich mit 12 Volt arbeiten – also ohne 5 und 3,3 Volt. Die halbiert nach unseren Messungen den Energiebedarf von Desktop-PCs im Leerlauf auf unter 10 Watt, wovon Umwelt und Geldbeutel profitieren.**

**Von Christian Hirsch**

Die Netzteilnorm Advanced Technology Extended (ATX) für Desktop-Rechner ist inzwischen ein Vierteljahrhundert alt. Zwar wurde sie alle paar Jahre aktualisiert, aus Gründen der Abwärtskompatibilität schleppen ATX-Netzteile aber inzwischen eine Menge unnötigen Ballast aus der Anfangszeit mit. Dieser treibt den Energiebedarf bei schwacher Belastung unnötig nach oben, obwohl moderne Prozessoren dank besserer Energiesparfunktionen immer sparsamer werden.

Um die immer strikteren Richtlinien in der EU, den USA und in Japan für den Energiebedarf von Elektrogeräten im Allgemeinen und Desktop-PCs im Speziellen zu erfüllen, hat Intel den Standard ATX12VO (ATX 12 Volt only) aus der Taufe gehoben (Download unter [ct.de/ycj9](http://ct.de/ycj9)). Der Chiphersteller stellt uns für erste Tests Vorserienexemplare des LGA1200-Mainboards Asrock Z490 Phantom Gaming 4SR sowie des Netzteils High Power HP1-P650GD-F12S mit der neuen Technik zur Verfügung.

Hauptänderung zur bisherigen ATX-Norm ist, dass das PC-Netzteil das Mainboard ausschließlich mit 12 Volt Spannung versorgt. Das macht an einigen Stellen im Rechner geänderte Steckverbindungen notwendig. Zudem müssen die ATX12VO-Netzteile mit einem höheren Mindestwirkungsgrad als bisher arbeiten, der vor allem im Schwachlastbetrieb über die 80-Plus-Vorgaben hinausgeht.

#### **Geänderter Spannungsbedarf**

Mit ATX12VO macht Intel einen harten Schnitt. Im PC-Netzteil gibt es nur noch einen einzigen Transformator, der die Netzspannung auf 12 Volt wandelt. Weitere benötigte Spannungen wie 3,3 Volt und 5 Volt erzeugt stattdessen das Mainboard. Das hat den Vorteil, dass die dafür notwendigen

# **Spannungskonzentrat**

## **Der energiesparende PC-Netzteilstandard ATX12VO**

Bauelemente passend für die jeweiligen Anforderungen des Boards wie der Anzahl der USB- und SATA-Ports dimensioniert sind und deshalb effizienter arbeiten.

ATX-Netzteile müssen hingegen auf der 3,3- und der 5-Volt-Schiene Ströme im zweistelligen Amperebereich liefern können, weil vor über 20 Jahren daraus der Prozessor gespeist wurde. Seit Pentium-4-Zeiten treten solche hohen Ströme für die beiden Spannungen aber nicht mehr auf und die üppig dimensionierten Wandler sind überflüssig, denn für die CPU-Kernspannung dient seitdem die 12-Volt-Schiene. Dieser Wechsel hatte den Vorteil, dass bei gleicher Leistung weniger Strom fließt und deshalb Leitungen mit kleinerem Querschnitt ausreichen.

Wandlerschaltungen auf dem Board sind zudem längst gang und gäbe: ATX-Mainboards erzeugen unter anderem die Spannungen für RAM (1,2 bis 1,5 Volt), CPU (0,7 bis 1,5 Volt), Chipsatz und diverse I/O-Chips (2,5 beziehungsweise 1,8 Volt) lokal.

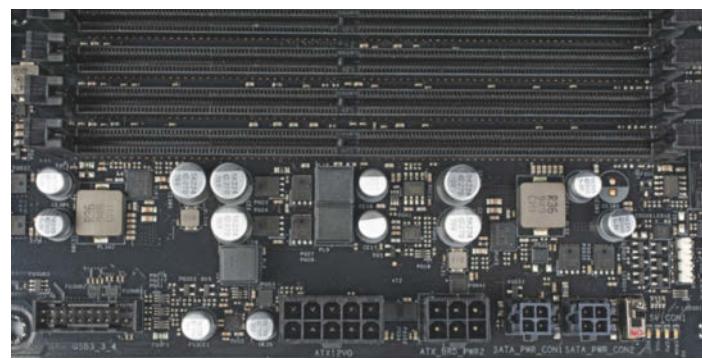
Die Idee von 12-Volt-only-Technik bei Desktop-PCs ist übrigens keine neue. Der PC-Hersteller Fujitsu entwickelte bereits vor rund zehn Jahren zusammen mit dem Netzteilhersteller FSP ein proprietäres 12-Volt-Ökosystem, das in sparsamen Business-PCs zum Einsatz kam.

### Kompakte Stecker

Die bisherige 24-polige ATX-Steckverbindung zwischen Netzteil und Mainboard wird bei ATX12VO durch einen zehnpoligen „Main Power Connector“ ersetzt. Er verwendet das gleiche Raster von 4,2 Millimetern und ist mit kodierten Kontakten ausgerüstet. Diese verhindern, dass man ihn verkehrt herum einsteckt oder andere Stecker anschließt. Drei der fünf Adernpaare des Main Power Connectors versorgen das Mainboard im eingeschalteten Zustand mit 12 Volt. Laut Spezifikation liefert jeder Pin etwa 6 bis 8 Ampere, sodass der neue Stecker bis zu 288 Watt Leistung überträgt.

Ebenfalls im Main-Power-Stecker untergebracht ist die 12-Volt-Standby-Leitung (12VSB), die im Unterschied zu den vorgenannten Adern auch bei ausgeschaltetem PC (Soft-Off) Strom führt. Sie ist notwendig, um den Energiebedarf für Aufweckfunktionen wie Wake-on-LAN, Wake-on-USB, die Erkennung einer unberechtigten Gehäuseöffnung (Chassis Intrusion), aber auch für Standby-Modi wie Suspend-to-RAM zu decken.

**Um Spannungen wie 3,3 und 5 Volt zu erzeugen, sind zusätzliche Wandler in der Nähe der Stromanschlüsse notwendig. Diese arbeiten effizienter als die bisherigen, überdimensionierten im ATX-Netzteil.**



Auf der 12VSB-Leitung muss das Netzteil dauerhaft 1,5 Ampere, also 18 Watt, sowie kurzzeitig Lastspitzen von bis 2,0 Ampere liefern können, denn sie dient auch als Stromquelle für USB-Ports, die Smartphones oder Tablets bei ausgeschaltetem PC laden. Beim bisherigen ATX-Standard beträgt die Spannung für die Standby-Leitung 5 Volt mit bis zu 3 Ampere Stromstärke.

Zwei der bisher im 24-poligen ATX-Stromstecker vorhandenen Leitungen haben es unverändert in den ATX12VO-Standard geschafft. Über den üblicherweise mit einem grünen Kabel markierten Kontaktstift PS\_ON meldet das Board an das Netzteil, dass der Rechner per Taster oder durch eine Aufwachfunktion eingeschaltet wurde und auf allen Leitungen Strom liefern soll. Nachdem das Netzteil hochgefahren ist, meldet es über den Kontakt PWR\_OK, dass alle Spannungen ihre Normwerte erreicht haben.

Mit dem zehnpoligen Main Power Connector ist es jedoch noch nicht getan. Zusätzlich schreibt die ATX12VO-Spezifikation den „Extra Board Connector“ vor. Dieser sechspolige Anschluss ist für High-End-Mainboards gedacht, die zum Beispiel mehrere PEG-Slots tragen oder USB-Ports mit Power Delivery bereitstellen. Der Extra Board Connector ist mechanisch und elektrisch identisch zum sechspoligen PEG-Stromstecker für Grafikkarten. Er stellt wie der Main-Power-Anschluss bis zu 288 Watt Leistung bereit. Bei Multi-Rail-Netzteilen teilen sich alle 12-Volt-Leitungen der beiden Mainboard-Stecker die 12V1-Schiene.

### SATA-Strom direkt vom Board

Unverändert vom ATX-Standard wurde der vier- beziehungsweise achtpolige CPU-Stromanschluss (ATX12V/EPS12V) übernommen, der schon seit 20 Jahren die Wandlerphasen für die Prozessorkernspannung auf dem Mainboard mit 12 Volt

belieft. Typischerweise hängen die Leitungen innerhalb des Netzteils an einem separaten 12V2-Zweig.

Auch bei der Spannungsversorgung von Grafikkarten ändert sich nichts. Über die PCIe-Erweiterungssteckplätze liefert das Board wie auch für alle anderen Erweiterungskarten 12 und 3,3 Volt. Letztgenannte Spannung kommt bei ATX12VO nicht mehr direkt vom Netzteil, sondern vom Board. Bei Karten mit mehr als 75 Watt Leistung sind weiterhin die 6- und 8-poligen Zusatzstecker vorgesehen, die der 12V3 beziehungsweise 12V4-Schiene zugeordnet sind. Der von Nvidia bei der Founders Edition der GeForce RTX 3080 und 3090 verwendete 12-polige Stromstecker ist kein Teil der ATX12VO-Spezifikation, sondern ein proprietärer Anschluss.

Weil ATX12VO-Netzteile keine 5 Volt mehr liefern, fallen auch die bisherigen Stränge mit SATA-Stromanschlüssen vom Netzteil weg. Stattdessen gibt es neue Stecker am Mainboard, von denen die SATA-Kabelstränge starten. ATX12VO führt dafür zwei unterschiedliche Steckverbinder ein: Eine vierpolige Variante stellt bei 12 Volt bis zu 5 Ampere und bei 5 Volt knapp über 2 Ampere bereit, was für zwei SATA-Laufwerke reicht. Eine sechspolige Version mit einem zusätzlichen Leitungspaar für 12 Volt verdoppelt die Zahl der SATA-Stromanschlüsse an diesem Strang auf vier. Verwechslungsgefahr mit dem CPU- und dem PEG-Stecker ist dabei ausgeschlossen, denn es kommt ein kleineres Rastermaß von 3 statt 4,2 Millimetern zu Einsatz.

In der Praxis werden die Mainboards je nach Zahl der vorhandenen SATA-Ports mit mehreren Anschlüssen und Kabelsträngen ausgeliefert. Das von uns getestete Asrock Z490 Phantom Gaming 4SR ist mit zwei vierpoligen Anschlüssen für insgesamt vier Laufwerke ausgerüstet.

Die Spezifikation erlaubt zudem auch klassische Molex-Stecker am Netzteil, al-



**Der bisherige 24-polige Mainboard-Stromstecker (rechts) schrumpft bei ATX12VO auf 10 Kontakte sowie einen 6-poligen PEG-Stecker zusammen.**

lerdings wiederum ausschließlich mit 12 Volt. Sie eignen sich deshalb nicht zum Anschluss von Laufwerken, sondern lediglich für Lüfter, Wasserpumpen oder LED-Leuchtelelemente.

## Sparvorgaben

Im Unterschied zur recht betagten ATX-Netzteilspezifikation diktieren ATX-12VO wesentlich striktere Vorgaben für die Effizienz. Sie sehen mindestens die Werte für 80 Plus Bronze vor: Der Wirkungsgrad bei den Lastpunkten 20, 50 und 100 Prozent muss mindestens 85, 88 beziehungsweise 85 Prozent betragen. Die ATX-Vorgaben sind mit 65, 72 und 70 Prozent wesentlich laxer, obgleich inzwischen der weit überwiegende Anteil der hierzulande verkauften PC-Netzteile die höheren 80-Plus-Vorgaben erreicht.

Vorteile bietet das 12-Volt-only-Design vor allem im Schwachlastbereich. Die allermeiste Zeit haben die Prozessorkerne nichts zu tun und legen sich beispielsweise zwischen zwei Tastaturanschlägen für viele tausend Taktzyklen komplett schlafen. Dank dieser modernen Energiesparfunktionen kommen moderne stationäre PCs je nach Ausstattung mit 7 bis 30 Watt Leistungsaufnahme bei ruhendem Betriebssystem-Desktop aus.

Für diesen Bereich machen die bisherigen Effizienzregularien von ATX und 80 Plus keine Vorgaben. Der niedrigste Lastpunkt von 20 Prozent entspricht bei einem 500-Watt-Netzteil bereits 100 Watt Leistungsaufnahme.

Der ATX12VO-Standard legt hingegen fest, dass Netzteile unter 400 Watt Gesamtleistung bei 10 Watt Last eine Effizienz von mindestens 75 Prozent aufweisen müssen. Bei 400 bis 500 Watt Nennleistung sind es 72 Prozent. Für leistungsstärkere Modelle gilt ein Wirkungsgrad von mehr als 72 Prozent bei 2 Prozent der Nennleistung. Diese Vorgaben sind notwendig, damit Desktop-PCs die ab nächstes Jahr geltenden Tier-II-Richtlinien der California Energy Commission (CEC) einhalten. Ziel ist es, die Leerlaufleistungs-

aufnahme von Desktop-PCs von 2016 bis 2021 um 50 Prozent zu senken.

## Großer Spareffekt

Wir haben sowohl die Effizienz des ATX-12VO-Netzteils der Firma High Power bei ausgewählten Lastpunkten als auch die Leistungsaufnahme des kompletten Systems mit dem Asrock-Mainboard Z490 Phantom Gaming 4SR untersucht. Ein Datenblatt für das Netzteil stand uns nicht zur Verfügung. Anhand unserer Messergebnisse für den Wirkungsgrad (90, 92 und 90 Prozent) bei 20, 50 und 100 Prozent Last erfüllt es die Voraussetzungen von 80 Plus Gold locker und gehört damit zu den sehr effizienten Netzteilen.

Verblüfft waren wir vom deutlich höheren Wirkungsgrad bei geringer Last. Hier kann die ATX12VO-Technik ihre Vorteile voll ausspielen, weil die Wanderverluste für die wenig genutzten 3,3- und 5-Volt-Schienen wegfallen. Bei 10 Watt schafft das Netzteil eine Effizienz von 77 Prozent: Wenn die PC-Komponenten 10 Watt benötigen, schluckt das Netzteil an der Steckdose 13 Watt. In unseren vergangenen Tests von ATX-Netzteilen erreichten die meisten hingegen einen Wirkungsgrad von lediglich 60 Prozent, einige sogar nur von 50 Prozent. Für jedes Watt an Nutzleistung kommt also noch ein weiteres hinzu, das das Netzteil ungenutzt verheizt.

Zudem haben wir das ATX12VO-Mainboard Asrock Z490 Phantom Gaming 4SR

mit dem Zehnkerner Core i9-10900K sowie 16 GByte DDR-2666 und einer SATA-SSD bestückt und zusammen mit dem High-Power-Netzteil getestet. Im Leerlauf schluckte das Gesamtsystem im Auslieferungszustand 14 Watt. Dieser Wert ist für ein LGA1200-System mit dem High-End-Chipsatz Z490 schon recht gut.

Nachdem wir im BIOS-Setup alle CPU-C-States sowie das Link Power Management für SATA und PCI Express aktiviert hatten, konnten wir die Leistungsaufnahme bei ruhendem Windows-10-Desktop auf unter 7 Watt drücken. Das schaffen sonst nur Mini-PCs mit Mobiltechnik wie der Intel NUC. Im Soft-Off- und Suspend-to-RAM-Zustand schluckte das Board mit jeweils rund 2 Watt jedoch ungewöhnlich viel. Vermutlich ist das BIOS noch nicht ausgereift.

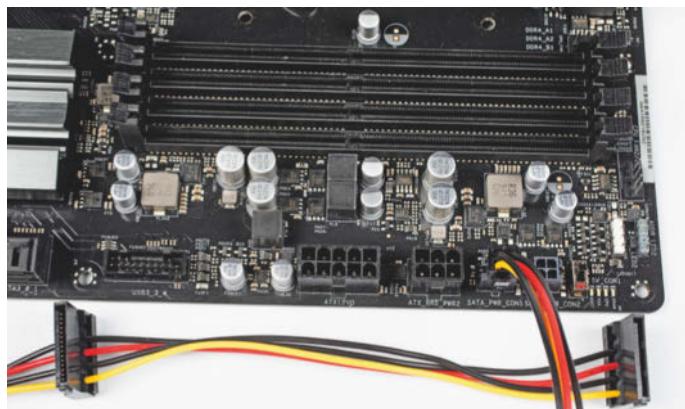
## Fazit

Wir waren überrascht, wie viel Sparpotenzial noch in den Netzteilen steckt. Die ATX-12VO-Norm senkt vor allem die Leistungsaufnahme im Leerlauf, in dem typisch genutzte Desktop-PCs ihre meiste Zeit verbringen. Wie schnell sich der neue Standard bei Netzteilen und Mainboards durchsetzen wird, ist noch unklar. Zunächst wird es wohl hauptsächlich Komplettsysteme großer PC-Hersteller damit geben. Mittelfristig wird ATX12VO auch für PC-Bastler interessant, denn Intel arbeitet mit Netzteilherstellern wie Channel Well, Cooler Master, Corsair, Delta, FSP, High Power und Sea Sonic zusammen. Der ATX-Standard wird wohl aber noch längere Zeit parallel existieren. Aus unserer Sicht ist ATX12VO in jedem Fall ein richtiger Schritt, den Energiebedarf moderner Desktop-PCs zu reduzieren, ohne dabei Flexibilität bei der Ausstattung und bei Aufrüstmöglichkeiten einzuschränken.

(chh@ct.de) ct

**ATX12VO-Standard:** [ct.de/yco9](http://ct.de/yco9)

**Weil der SATA-Stromanschluss auch eine 5-Volt-Leitung enthält, muss bei ATX12VO das Board die Stromstecker für Festplatten und SSDs bereitstellen. Der vierpolige Anschluss liefert je zwei SATA-Geräte.**



# // heise devSec()

Die Konferenz für sichere Software- und Webentwicklung

**ONLINE – 21. UND 22. OKTOBER 2020**

**Jetzt Ticket sichern!**

Sichere Software beginnt vor der ersten Zeile Code ...

## THEMEN SIND UNTER ANDEREM:

- Agile Threat Modeling
- OWASP Top 10 und OWASP API Security Top 10
- Jakarta EE Security und MicroProfile JWT
- Was kann C++ von Rust klauen?
- Cloud-Security auf dem Prüfstand

Nehmen Sie über Ihren Browser bequem vom Büro oder Homeoffice teil, tauschen Sie sich per Text- und Videochat mit Teilnehmern und Referenten aus, und nutzen Sie das Videoarchiv, um im Nachgang alle Vorträge anzuschauen.

[www.heise-devsec.de](http://www.heise-devsec.de)

### GoldspONSOREn



Veranstalter





# Großbildjäger

## Fernseher und Großformat-Displays für Spieler

**Fernseher werden stetig spieletauglicher, Monitore immer größer. Doch welche Variante macht Gamer glücklicher? Vier HDR-taugliche Displays mit 4K-Auflösung und Bilddiagonalen von 48 bis 65 Zoll sollen Antwort geben.**

**Von Benjamin Kraft**

**K**lassischerweise zocken Konsolenspieler auf dem Fernseher. Er gehört als Informationsquelle und Entertainmentzentrale in der Regel ohnehin zum Haushaltsinventar und bietet eine riesige Darstellungsfläche. Doch die schöne neue Streaming-Welt ändert vieles. Um die Lieblingsserie zu genießen, einen Filmabend zu veranstalten oder schlicht die

Tagesschau zu sehen, braucht man nicht mehr zwingend einen Fernseher. Ein großes Display ohne TV-Tuner tut es in Kombination mit einem Media-Center-PC oder einem Streaming-Client auch.

Den Trend haben die Displayhersteller erkannt und bieten deshalb auf Gaming getrimmte Riesenmonitore fürs Wohnzimmer an. Da liegt die Frage nahe, ob man überhaupt einen Fernseher braucht oder ein großes Gaming-Display nicht ausreicht.

Die Fernseher sind dagegen immer smarter geworden und empfangen längst nicht mehr nur digitales Fernsehen per Kabel, Satellit oder Antenne. Aktuelle Geräte bringen auch Streaming-Apps wie Netflix oder Amazon Prime, Sendermediatheken und diverse Sportkanäle gleich mit oder liefern sie über ihren App-Store nach. Außerdem halten sie zunehmend Gamer-Features bereit, unterstützen etwa variable Refresh-Raten und bieten einen Modus für geringe Eingabeverzögerung.

Beispielhaft haben wir für unsere Untersuchung zwei große Gaming-Displays und zwei smarte Fernseher ins Labor geholt, allesamt HDR-tauglich. Von Philips stammt der 55-Zöller Momentum 558M1RY, laut Hersteller ein Monitor für Spieler und mit 1300 Euro das günstigste Gerät im Test. Etwa 300 Euro mehr muss man für den LG-Fernseher OLED 48CX9LB auf den Tisch legen, der mit 48 Zoll der kleinste in der Runde ist. Ab 2100 Euro bekommt man Samsungs GQ65Q90T, einen 65-Zoll-Fernseher, der mit Quantenpunkten besonders strahlende Farben zeigen soll. Teuerster im Bunde ist mit etwa 3800 Euro das Nobel-Display Asus ROG Swift PG65UQ, das zum elitären Kreis der Big Format Gaming Displays (BFGD) gehört.

### Ausstattungsfragen

Mindestens vier Signaleingänge sind überall dabei, wobei sich die Fernseher kom-

plett auf HDMI beschränken. LG unterstützt an allen Ports die noch junge HDMI-Generation 2.1, Samsung immerhin an einem der Eingänge. Damit ist zumindest in der Theorie 4K-Auflösung bei 120 Hz und HDR-Darstellung möglich. Die Gaming-Displays arbeiten noch mit HDMI 2.0, was für 4K mit 60 Hz und HDR reicht. Zusätzlich besitzen die Gaming-Monitore aber einen DisplayPort 1.4 für 4K bis 120 Hz mit HDR.

4K ist auf derart großen Bildschirmen übrigens nicht mehr besonders scharf. Auf 48 Zoll wie bei LGs OLED 48CX9LB ergibt sich eine Pixeldichte von gerade mal 92 dpi, auf 65 Zoll sogar nur 68 dpi. Das entspricht einem 24-Zöller mit 1920 × 1080 Bildpunkten beziehungsweise einem 32-zölligen Full-HD-Display.

An einem USB-Hub kann man Maus und Tastatur oder andere Peripherie anschließen. Der direkte Anschluss schneller Speichermedien ans TV lohnt sich bei den Geräten von LG und Samsung nicht, denn ihre Hubs arbeiten nur mit USB-2.0-Geschwindigkeit – bei 60 MByte/s brutto ist Schluss, netto bleiben meist um die 40 MByte/s übrig. Dafür können sie TV-Sendungen auf externe Medien aufnehmen und von ihnen abspielen; sie verfügen über eingebaute Decoder für aktuelle Audio- und Videoformate in diversen Containern.

Alle Großformatbildschirme werden mit Standfüßen ausgeliefert, die unterschiedlich viel Platz auf der Kommode oder im Regal beanspruchen. Alternativ lassen sich die Displays über Schraublöcher an der Rückseite an einer Wandhalterung befestigen.

Die Lautsprecher liefern in den meisten Fällen ausreichenden bis guten Sound ab. Philips etwa hängt eine Soundbar von Bowers & Wilkens unter dem Display, LG nutzt den Fuß als Soundrutsche, um den Klang zum Publikum zu leiten. Die Asus-Speaker überzeugen indes nicht.

Bei den Gerätemenüs zeigt sich eine Zweiklassengesellschaft: Während die Gaming-Displays die relativ einfachen Bildmenüs ihrer kleineren Geschwister übernehmen, umfassen die Menüs der Fernseher eine Vielzahl an Optionen. Jedes Bildpreset kann mit diversen Optionen nachjustiert werden, darunter Zwischenbildberechnung, HDR-Aufhübung oder Hochskalierung von Inhalten mit geringerer Auflösung. Ein Stück weit geht die Funktionsvielfalt zulasten der Übersichtlichkeit, doch nach ein paar Ver-

suchen hat man sich in die Bedienlogik eingefüchtst.

Dabei helfen auch die guten Fernbedienungen. Während Samsungs minimalistisch gestaltet ist, hat die von LG viele Knöpfe, Zahlentasten und ein Steuerkreuz inklusive Drück-Rollrad. Alternativ navigiert man das Bildmenü mit einem auf dem Fernseher eingeblendeten Pfeil, den man mit der Fernbedienung mit eingebautem Gyroskop über den Bildschirm lenkt.

LG und Samsung bauen in ihre Fernseher jeweils zwei Triple-Tuner ein, die DVB per Satellit (-S/-S2), Antenne (-T/-T2) oder Kabel empfangen. Außerdem beherrschen sie HbbTV und bringen einen CI+-Schacht mit. Ins Heimnetzwerk gelangen sie per 802.11ac-WLAN (Wi-Fi 5) oder kabelgebunden mit Gigabit-Speed, um Futter für ihre Streaming-Apps, Firmware-Updates oder Filmmaterial via DLNA zu bekommen, etwa vom NAS. Schließlich dienen sie noch als Ausgabegeräte für Apples AirPlay 2. LG unterstützt zusätzlich Miracast.

Den smarten Teil übernehmen Betriebssysteme, die in Mobilgeräten ihren Anfang nahmen. LG setzt auf WebOS 5, Samsung auf das Eigengewächs Tizen. Die Fernseher lassen sich nicht nur mit den beigelegten Fernbedienungen dirigieren, sondern gehorchen auch Amazons Alexa,

das LG-TV zusätzlich dem Google Assistant, das Samsung-TV dem hauseigenen Bixby.

### Infos zur Anzeige

Allen Großbildmonitoren ist gemein, dass sie laut Hersteller mindestens 100 Bilder pro Sekunde anzeigen, HDR-Inhalte wiedergeben und 3840 × 2160 Pixel zeigen. Außerdem decken sie zu großen Teilen den Farbraum DCI-P3 ab, der Rot und Grün deutlich satter als das im Web gebräuchliche sRGB darstellt. Asus und Samsung helfen den Farben mit sogenannten Quantenpunkten nach.

Bei Asus, Philips und Samsung kommen VA-Displays zum Einsatz. Diese Panel-Technik steht im Ruf, besonders hohe statische Kontraste zu erzielen. Den verstärken sie mit einem FALD-Backlight (Full-Array Local Dimming), also einer Hintergrundbeleuchtung mit individuell dimmbaren LED-Zonen. Je mehr Zonen, umso feiner lassen sich starke Helligkeitsunterschiede im Bild dosieren.

In einem unserer animierten Testbilder wandert beispielsweise eine dünne weiße Linie von links nach rechts über den ansonsten schwarzen Bildschirm. Bei FALD-Displays ist das Backlight nur in den Zonen an, welche die Linie gerade durchquert – der Rest des Bildschirms bleibt tiefschwarz. Allerdings strahlen die beleuchteten Zonen leicht in benachbarte Bereiche ein, und wenn die weiße Linie von einer Zone in die nächste wechselt, leuchten kurz beide auf, was in diesen Zonen den In-Bild-Kontrast verringert.

Bei einem klassischen Edge-LED-Backlight ist die Hintergrundbeleuchtung in wenige senkrecht verlaufende Zonen aufgeteilt. Wandert die Linie von links nach rechts, leuchtet das Backlight in breiten Streifen dahinter auf. Bewegt sie sich hingegen von oben nach unten, werden alle Zonen aktiviert und der gesamte Bildschirm schimmert, selbst wenn sich die Linie an einem der Ränder befindet.

Einen ganz anderen Weg geht LG mit der OLED-Technik, bei der jedes Pixel selbst leuchtet und individuell gedimmt werden kann. Das organische Display stellt Helligkeitsunterschiede also pixelgenau dar. Beim Linien-Testbild kommt es daher nur zu minimalem Ausstrahlen um die Linie. OLEDs haben jedoch auch Nachteile. Dazu zählt vor allem die Gefahr, dass sich bei statischem Bildinhalt wie



**Philips (rechts) transponiert die Steuerkreuz-Bedienung des Bildmenüs auf die Fernbedienung. Mit eingebautem Gyroskop lenkt man bei LG alternativ einen Zeiger über den Schirm.**



## Asus ROG Swift PG65UQ

Das Asus-Display fällt mit seinem raumgreifenden Spreizfuß und dem nach unten projizierten Logo optisch aus der sonst eher biederer Reihe. Das Gaming-Styling trägt es zu Recht, denn der ROG Swift PG65UQ gehört zur exklusiven Gruppe der BFGDs. Sein Panel deckt den Farbraum DCI-P3 praktisch komplett ab und ist in 384 individuell dimmbare LED-Zonen unterteilt. Dadurch erzielt es hohe In-Bild-Kontraste und ein supertiefes Schwarz. Nominell reicht die Bildwiederholfrequenz bis 120 Hz, im Bildmenü kann man das Panel auf 144 Hz „übertakten“, wie Asus es nennt. Dann reicht die Bandbreite des DisplayPorts bei 4K-Auflösung allerdings nicht mehr für die volle Farbtiefe, sodass das Signal auf YCbCr 4:2:2 reduziert wird. Sichtbare Auswirkungen hatte das indes nicht.

Außerdem beherrscht der Monitor am DisplayPort Nvidias VRR-Technik G-Sync in der Ultimate-Stufe, die Voraussetzung für die Verbindung von VRR und HDR ist und deren Regelbereich von 1 bis 144 Hz reicht; der Lüfter des eingebauten Moduls dreht allerdings dauerhaft hörbar. Die Entscheidung für G-Sync ist automatisch eine gegen Adaptive Sync und damit AMDs FreeSync; da sind die anderen drei Kandidaten flexibler.

In Spielen machte der Asus-Monitor eine sehr gute Figur, wenn die Overdrive-Stufe auf „Normal“ und die Einstellung des variablen Backlights auf „Fast“ stand. Allein der Wechsel von Schwarz auf Dunkelgrau dauerte mit 16 Millisekunden für 120 Hz zu lang. Außerdem differenzierte das Panel sehr dunkle Farbtöne nicht mehr; stattdessen wurden im Spiel Control dunkle Areale durchgehend schwarz dargestellt.

Während in 24p-Filmmaterial wie die Blu-ray „Concussion – Erschütternde Wahrheit“ bewegte Objektkanten mangels Zwischenbildberechnung zerrissen, gefiel die Medienwiedergabe an Streaming-Geräten gut. Sie wollte am Apple TV allerdings nur in Full HD und ohne HDR gelingen, denn obwohl wir es mit diversen Kabeln versuchten, kam keine stabile HDMI-Verbindung mit ausreichender Bandbreite zustande. Offenbar konnten die Geräte auch keine HDCP-Verbindung aushandeln, sodass geschützte Inhalte – etwa Netflix-Serien – nicht abgespielt wurden. Das TV-Programm von Arte gab das Apple TV indes klaglos wieder.

Der Sound des Monitors überzeugt nicht, der Bass ist dünn und die Wiedergabe beginnt bei etwas höheren Pegeln zu scheppern. Besser, man schaltet den HDMI-Receiver davor oder gibt den Ton über die optische Toslink-Buchse an ihn aus.

- ➔ schnelles, farbstarkes Panel
- ➡ Streaming an HDMI unzuverlässig
- ➡ sehr teuer



## LG OLED 48CX9LB

Der superdünne OLED-Fernseher zeichnet ein sehr feines, nuanciertes Bild, der Schirm ist gleichmäßig ausgeleuchtet. Allerdings strahlt er mit maximal 600 cd/m<sup>2</sup> nicht so hell wie die Konkurrenten und eignet sich damit nicht für sehr helle Räume. Seinen vollen Farbumfang zeigt das Panel erst, wenn man den erweiterten Farbraum aktiviert hat. Es erzielt sehr hohe In-Bild-Kontraste, und weil es jedes Pixel einzeln dimmen kann, strahlen helle Bereiche nur minimal in angrenzende dunkle Areale ein. Vollflächiges Weiß schafft er sogar nur mit circa 140 cd/m<sup>2</sup> – das kommt im TV- und Spielealltag allerdings selten vor.

Das Panel schafft den einfachen Bildwechsel fast durchweg in ultraflinken 1,3 Millisekunden. Das würde noch für weit über 400 statt der versprochenen 120 Hz reichen. Nur beim Hin- und Herschalten zwischen Schwarz und Dunkelgrau vergehen rund 10 Millisekunden. Spiele bringt der LG-Fernseher jedenfalls schlierenfrei und knackscharf aufs Display. Damit es keine Eingabeverzögerung gibt, müssen Spieler für den HDMI-Eingang, an dem der PC oder die Spielekonsole hängt, den Modus „Instant Game Response“ im Bildmenü aktivieren. Dann werden Mausbewegungen unmittelbar umgesetzt.

Mit der aktuellen Firmware 5.1.1-3704 umfasst das VRR-Repertoire des LG-OLEDs neben G-Sync auch AMDs FreeSync. Beides klappte im Betrieb problemlos. Doch trotz HDMI-2.1-Eingängen bekamen wir die Kombination 4K mit 120 Hz und HDR nicht hin. Bei einer Radeon RX 5700 XT ließ sich der HDR-Modus nicht aktivieren. Das wiederum klappte bei der GeForce RTX 2080 Ti, die 4K unabhängig von HDR maximal 60 Bilder pro Sekunde ausgab. Die GeForce RTX 3080, eine der ersten Grafikkarten mit HDMI-2.1-Ausgängen, schaffte zwar 4K und 120 Hz, doch sobald wir HDR aktivierten, schaltete Windows auf 1024 x 768 Pixel und 60 Hz um.

Die Medienwiedergabe überzeugte sowohl über die eingebauten Streaming-Apps als auch bei Wiedergabe von Blu-rays. Die Lautsprecher produzieren einen ausgewogenen Sound. Weil die meisten Presets es bei Schärfung und Kontrast übertreiben, empfehlen wir den puristischen Filmmaker Mode zu wählen und Features einzeln zuzuschalten. Für die Blu-ray-Wiedergabe empfiehlt sich beispielsweise, TruMotion auf „Flüssig“ zu stellen.

- ➔ ultrakurze Reaktionszeiten
- ➔ pixelgenaues Local Dimming
- ➡ nur 600 cd/m<sup>2</sup> Spitzenhelligkeit



## Philips Momentum 558M1RY

Das mit rund 1300 Euro günstigste Display im Test bringt eine wohlklingende Soundbar mit dem Logo der Soundschmiede Bowers & Wilkens mit. Die Ambiglow-Beleuchtung an der Bildschirmrückseite orientiert sich am Bildinhalt und hilft speziell in dunklen Räumen, die Stimmung des Spiels oder Films über den Fernseher hinaus auszudehnen. Per Adaptive Sync lässt sich die Panel-Elektronik dynamisch die Bildwiederholrate von AMD- oder Nvidia-Grafikkarten vorgeben. Das Display steht zwar nicht auf Nvidias Liste der G-Sync-kompatiblen Geräte, die Funktion konnten wir aber im Nvidia-Treiber manuell anschalten.

Die Farbdarstellung gefällt gut, das Panel deckt den Farbraum DCI-P3 fast komplett ab. Die Farbsättigung nimmt auch aus großen Einblickwinkeln kaum ab. Das Backlight des Philips-Displays ist in 144 Zonen unterteilt. Die regelt die Elektronik aber so grob, dass der Monitor nicht die hohen In-Bild-Kontraste seiner Mitbewerber im Test erzielt. Außerdem zeigt das Panel anstelle von Tiefschwarz eher ein sehr dunkles Grau, was aber immer noch für einen sehr guten In-Bild-Kontrast von 2006:1 reicht. Allerdings strahlt das Backlight von den Ecken zur Mitte ein. Vollflächiges Weiß geriet hell, aber inhomogen, mit einem großen dunkleren Fleck in der Mitte; zu den Seiten fällt die Helligkeit stark ab. Daran änderte auch der Uniformity-Modus im Bildmenü nichts.

Die versprochenen 120 Hz des Panels lassen sich in der Praxis nicht nutzen. Zwar dauert der Helligkeitswechsel mit der empfehlenswerten Overdrive-Einstellung „Fast“ im Mittel nur 11 Millisekunden, was für 90 Hz reichen würde, doch vergehen beim Wechsel zwischen Schwarz und Hellgrau 21, zu Dunkelgrau gar 32 Millisekunden. In Spielen mit stark unterschiedlich beleuchteter Szenerie, etwa einem dunklen Gang, der in ein helles Zimmer mündet, entstehen dadurch in der Bewegung Schlieren. An den HDMI-2.0-Eingängen des Monitors stellt sich die Frage nicht, denn an ihnen sind ohnehin nur 60 Hz möglich.

Bei der Medienwiedergabe fiel das Bild ebenso gemischt wie bei Asus aus: Bei der Wiedergabe von Kinofilmen mit 24 Hz von Blu-ray-Disc zerrissen bewegte Objektkanten, Streaming-Inhalte mit 60 fps sahen hingegen gut aus, wenngleich etwas weniger knackig als auf den TVs.



## Samsung GQ65Q90T

Der 65-Zöller zeigt ein ähnlich schönes Bild wie das LG-OLED, dessen sattes Rot er trotz Quantenpunkt-Einsatz aber nicht ganz erreicht. Das umfangreiche Menü ist gerade noch übersichtlich, doch viele Optionen sind miteinander gekoppelt. Einen Direktzugriff auf das Einstellungsmenü bietet die Fernbedienung nicht, man muss sich jedes Mal durch die gesamte Smart Hub genannte Menüleiste nach links hangeln, um es aufzurufen. Immerhin kann man einzelne Settings direkt ansteuern. An manchen Quellen stehen nur wenige Bild-Presets zur Verfügung. Erkennt die Elektronik beispielsweise einen PC, darf man nur zwischen Dynamisch und Standard wählen.

Letztere ist eindeutig die bessere Wahl, denn „Dynamisch“ übertreibt es bei Helligkeit, Kontrast und Schärfung. An Konsole und anderen Quellen raten wir zum Filmmaker Modus, in dem man einzeln Features zuschalten kann. Um das volle Farbpotenzial abzurufen, muss man zusätzlich den Farbraum auf „nativ“ stellen. Im Zentrum leuchtet das Display bei vollflächigem Weiß gleichmäßig hell, zu den Seiten fällt die Helligkeit ab.

Zum Zocken ist der Samsung-Fernseher mit aktiviertem Spieldmodus und der Einstellung „Lokales Dimming Hoch“ zummindest theoretisch schnell genug, er bummelte aber beim Wechsel von Schwarz auf Weiß oder Hellgrau mit bis zu 19 Millisekunden. Lieferte eine GeForce RTX 3080 das Signal, wurde der Bildschirm schwarz, sobald wir im Einstellungsmenü unter dem Menüpunkt „externe Geräteverwaltung“ das erweiterte Eingangssignal aktivierten. Diese Einstellung ist aber Voraussetzung für hohe Bildwiederholraten bei 4K. Ob es am Fernseher oder der neuen Grafikkarte lag, war bis zum Redaktionsschluss nicht zu klären. Mit einer AMD Radeon RX 5700 oder Nvidias älterer GeForce RTX 2080 Ti waren maximal 60 Hz möglich; eigentlich müssten mit beiden 100 Hz drin sein.

Filme setzte der Samsung-Fernseher gut in Szene, egal ob per eingebauter App gestreamt oder vom Blu-ray-Player zugespielt. Daran hat auch das lokal dimmbare Backlight seinen Anteil, das mit 120 Zonen aber weniger fein als bei Asus oder LG arbeitet. Das lokale Dimming lässt sich zudem nicht ausschalten. Die Lautsprecher liefern eine angemessene Untermalung, neigen aber zu Schärfe.

⬆️ **guter Sound, satte Farben**

⬇️ **ineffektives Local Dimming**

⬇️ **lahmes, inhomogen ausgeleuchtetes Panel**

⬆️ **schöne Filmwiedergabe**

⬆️ **umfangreiche Einstellmöglichkeiten**

⬇️ **vollgepacktes Menü mit gekoppelten Einstellungen**

dem lange angezeigten Windows-Desktop oder dauerhaft eingeblendeten Elementen wie einer Lebensanzeige im Spiel ein Geisterbild einbrennt. Meist verschwindet das Schattenbild wieder, nachdem ein anderes Muster angezeigt wurde. Inzwischen geben die Hersteller ihren Geräten zudem Gegenmaßnahmen mit oder helfen ihnen beim Selbstschutz [1].

Hochkontrastinhalte können alle Kandidaten wiedergeben, doch ist HDR nicht gleich HDR: Es gibt konkurrierende und sich ergänzende Formate. Die Fernseher von LG und Samsung sind sich bei der Unterstützung von HLG (Hybrid Log-Gamma) und HDR10 einig, zwei von der SMPTE (Society of Motion Picture and Television Engineers) für TV und Video spezifizierte HDR-Standards. LG bringt zusätzlich Dolby Vision IQ mit, Samsung sein eigenes Format HDR 10+.

Die Spiele-Displays von Asus und Philips sind ebenfalls mit HDR10 kompatibel und erfüllen obendrein die anspruchsvollere Norm DisplayHDR 1000 der VESA (Video Electronics Standards Association). Die schreibt neben dem P3-Farbraum und einer Spitzenhelligkeit von mindestens 1000 cd/m<sup>2</sup> auch einen Schwarzwert von maximal 0,05 cd/m<sup>2</sup> vor.

Variable Refresh-Raten-Anpassung (VRR), bei der die Grafikkarte dem Display dynamisch die Bildwiederholrate vorgibt, haben ebenfalls alle Geräte an Bord. Als BFGD setzt das Asus ROG Swift PG65UQ auf Nvidias G-Sync, das in einem Frequenzbereich von 1 und 144 Hz arbeitet. Die Regelung übernimmt ein eigenes, von Nvidia zugeliefertes Modul, das ausschließlich mit Nvidia-Grafikkarten zusammenspielt. Außerdem arbeitet G-Sync nur über DisplayPort.

LG, Philips und Samsung unterstützen Adaptive Sync, das an HDMI und DisplayPort funktioniert. Diesen Standard können sowohl AMDs Radeons als auch Nvidias GeForce-Karten nutzen. Allerdings beginnt der Regelbereich hier meist erst bei 48 Hz, reicht aber bis zur maximalen Bildwiederholfrequenz des Panels. Radeon-Grafikkarten aktivieren automatisch ihren VRR-Modus FreeSync, wenn sie ein Adaptive-Sync-Display erkennen.

Nvidia pflegt eine Liste mit Displays, die es auch ohne Modul als G-Sync-kompatibel einstuft. Der GeForce-Treiber schaltet G-Sync nur dann automatisch an, wenn das angeschlossene Displays auf dieser Liste steht. Das ist bei LGs OLED 48CX9LB der Fall. Andernfalls kann man

G-Sync manuell aktivieren; Nvidia warnt allerdings, dass es zu Bildstörungen wie Flackern oder falscher Farbdarstellung kommen kann.

Die versprochenen hohen Bildwiederholraten von 100 Hz und mehr können nicht alle Kandidaten in der Praxis auch umsetzen. Speziell beim Philips-Gamer dauern die Bildwechsel von Schwarz zu Grautönen mit 20 bis 30 Millisekunden viel zu lang, was ihn für schnelle dunkle Shooter disqualifiziert. Das OLED-TV von LG bewältigt die meisten Helligkeitswechsel dagegen in rasend schnellen 1,2 Millisekunden, nur zwischen Schwarz und Dunkelgrau vergehen im Mittel 10 Millisekunden.

Input-Lag, also die Eingabeverzögerung zwischen einer Mausbewegung und Ausführung auf dem Bildschirm, konnten wir bei den zwei Spiele-Displays nicht feststellen. Die Fernseher bringen in ihren umfangreichen Menüs eine Einstellung mit, die ihn ebenfalls eliminiert. Bei Samsung ist es der Spielemodus, bei LG heißt er Instant Game Response und muss für jeden Signaleingang separat aktiviert werden.

## Kinderkrankheiten mit HDMI 2.1

Die Fernseher von LG und Samsung unterstützen bereits HDMI 2.1 mit einer Bandbreite von 48 GBit/s. Das reicht für 4K-Auflösung bei 120 Hz mit HDR – eigentlich. Im Test klappte das aber noch mit keinem der beiden.

Als Testsystem diente ein Windows-Rechner mit Nvidias neuer GeForce RTX 3080, die als eine der ersten Grafikkarten HDMI-2.1-Ausgänge besitzt [2]. Doch am OLED 48CX9LB schaltete Windows von 4K mit 120 Hz unveränderlich auf XGA-Auflösung (1024 × 768) mit 60 Hz herunter, sobald wir in den Anzeigeeinstellungen den HDR-Schalter umlegten.

Am Samsung QG65Q90T kamen wir gar nicht erst so weit. Wir hängten den Rechner wie von Samsung empfohlen an HDMI-Port 4, der als einziger für hohe Bildraten ausgelegt ist. Sobald wir aber in den Geräteeinstellungen das erweiterte Eingangssignal aktivierten, wurde der Bildschirm schwarz. Wir bekamen erst wieder einen Windows-Desktop zu sehen, nachdem wir den PC mit einem anderen HDMI-Eingang verbunden hatten.

Auf dieses Verhalten angesprochen, reagierten die Hersteller ratlos. Zunächst vermutete Samsung das Kabel als Auslöser. Allerdings hatte es an keinem anderen Fernseher Probleme gemacht. Zudem gibt

es zwar eine offizielle Spezifikation für HDMI-2.1-Kabel; kaufen kann man solche Strippen allerdings noch nirgends. Von LG erhielten wir leider keine Antwort.

Nvidia schließlich verstand unsere Anfrage offenbar falsch und empfahl uns, in Nvidias Systemsteuerung 4K-Auflösung zu wählen und die Nvidia-Farbeinstellungen zu verwenden, um das Ausgabe-Farformat auf YCbCr 4:2:0 umzustellen. Anschließend sollten wir die Auflösung auf 8K erhöhen. Das ist allerdings bloß der Workaround, um 4K mit 120 Hertz auf HDMI-2.0-Displays anzeigen zu lassen. Auf unsere eigentliche Frage bekamen wir bis Redaktionsschluss keine Antwort.

Hier sind die Gaming-Displays mit ihren DisplayPorts klar im Vorteil: War der PC darüber angeschlossen, bekamen wir 4K mit 120 Hz und HDR ohne Verrenkungen und Zickereien auf den Schirm. Für Konsolenspieler ist das ein schwacher Trost, denn die Playstation und Xbox werden auch in der kommenden Generation auf HDMI setzen.

## Fazit

Egal ob Shooter, Rennspiel, rundenbasierte Aufbau-Sim oder Rollenspiel: Großformat-Gaming macht ordentlich Spaß. An einer Spielekonsole der noch aktuellen Generation, die maximal 60 fps erzielen, machen alle der getesteten Geräte eine ähnlich gute Figur. Für 4K müssen allerdings die Voraussetzungen stimmen, was nicht nur eine leistungsfähige Grafikkarte und eine schnelle CPU, sondern auch ein gutes HDMI-Kabel umfasst. Selbst dann klappt die Kombination mit hohen Bildraten und großem Dynamikumfang nicht immer – selbst mit brandaktueller, HDMI-2.1-kompatibler Hardware. Bleibt zu hoffen, dass Treiber- und Firmware-Updates die Lage verbessern.

Kann ein großes Gaming-Display einen Fernseher ersetzen? Wenn die Inhalte primär vom Streaming-Dienst oder aus einer App kommen und sich Zuschauer und Anzeige verstehen, steht dem im Prinzip nichts entgegen. Mit dem Philips Momentum 558M1RY spart man gegenüber den getesteten Fernsehern sogar mächtig Geld, denn zum nächstgünstigsten Gerät, dem LG OLED 48CX9LB, sind es immerhin 300 bis 400 Euro.

Das OLED hat zwar eine kleinere Anzeigefläche, dafür allerdings in Sachen Bildqualität, Ausstattung, Spieleauglichkeit und nicht zuletzt in puncto Medienviedergabe die Nase vorn. Ach ja, und das

## Große Displays und Fernseher von 48 bis 65 Zoll für Gamer

Modell	ROG Swift PG65UQ	OLED 48CX9LB	Momentum 558M1RY	65" QLED 4K Q90T (GQ65Q90T)
Hersteller	Asus, <a href="http://www.asus.de">www.asus.de</a>	LG, <a href="http://www.lg.com">www.lg.com</a>	Philips, <a href="http://www.philips.de">www.philips.de</a>	Samsung, <a href="http://www.samsung.de">www.samsung.de</a>
Displaydiagonale / Auflösung (Pixeldichte)	64,5" (163,8 cm) / 3840 × 2160 (68 dpi)	48" (122 cm) / 3840 × 2160 (92 dpi)	55" (139,7 cm) / 3840 × 2160 (80 dpi)	65" (165 cm) / 3840 × 2160 (68 dpi)
Paneltyp / Seitenverhältnis / max. Bildwiederholfrequenz	VA (AMVA), spiegelnd / 16:9 / 144 Hz	OLED, spiegelnd / 16:9 / 120 Hz	VA (MVA), matt / 16:9 / 120 Hz	VA (QLED), spiegelnd / 16:9 / 100 Hz
Anschlüsse / Tuner	4 × HDMI 2.0, 1 × DisplayPort 1.4, 4 × USB 3.0, 1 × Toslink / n. v.	4 × HDMI 2.1, 3 × USB 2.0, 1 × Kopfhörer, 1 × Toslink / 2 × DVB-T/-T2/-C/-S/-S2 HEVC (H.265), 1 × CI+ 1.4,	3 × HDMI 2.0, 1 × DisplayPort 1.4, 4 × USB 3.0 / n. v.	1 × HDMI 2.1, 3 × HDMI 2.0, 1 × Kopfhörer, 1 × Toslink / 2 × USB 2.0, 2 × DVB-T/-T2/-C/-S/-S2 HEVC (H.265), 1 × CI+ 1.4
Lautsprecher	2 × 15 Watt	2 × 10 Watt + 1 × 20 Watt	2 × 10 Watt + 1 × 20 Watt	2 × 20 Watt + 1 × 20 Watt
LAN / WLAN / Bluetooth	n. v. / n. v. / n. v.	Gigabit-Ethernet / 802.11ac / 5	n. v. / n. v. / n. v.	Gigabit-Ethernet / 802.11ac / 4.2
Farbraum / HDR / VRR	DCI-P3 / DisplayHDR 1000 / Nvidia G-Sync Ultimate	DCI-P3 / HDR 10, Dolby Vision IQ, HLG/ Adaptive Sync	DCI-P3 / DisplayHDR 1000 / Adaptive Sync	DCI-P3 / HDR 10, HDR 10+, HLG / Adaptive Sync
Besonderheiten	Aura Sync, ROG-Logo, FALD-Backlight mit 384 Zonen	Betriebssystem: WebOS 5.0; Sprachassistenten: Amazon Alexa, Google Assistant; Streaming-Clients: Apple AirPlay 2, DLNA-Client, Miracast	AmbiGlow, FALD-Backlight mit 144 Zonen	FALD-Backlight mit 120 Zonen; Betriebssystem: Tizen; Sprachassistenten: Google Assistant, Samsung Bixby; Streaming-Clients: Apple AirPlay 2, DLNA-Client
VESA-Halterung (Lochabstand)	400 mm × 400 mm	300 mm × 200 mm	200 mm × 200 mm	400 mm × 400 mm
Lieferumfang	Fernbedienung, HDMI-Kabel, DP-Kabel	Fernbedienung	Fernbedienung, HDMI-Kabel, DP-Kabel	Fernbedienung
Maße (B × H × T) / Gewicht	144,8 cm × 94,7 cm × 39 cm / 36,8 kg	107,1 cm × 65 cm × 25,1 cm / 18,9 kg	123,2 cm × 83,4 cm × 30,8 cm / 26,5 kg	144,7 cm × 91,9 cm × 28,6 cm / 35 kg
<b>Messwerte</b>				
Leistungsaufnahme Soft-off / im Videobetrieb (bei Helligkeit) <sup>1</sup>	5,5 W <sup>2</sup> / 150 W (517 cd/m <sup>2</sup> )	0,2 / 85,6 W (140 cd/m <sup>2</sup> )	0,13 W / 104 W (496 cd/m <sup>2</sup> )	0,8 W / 199 W (425 cd/m <sup>2</sup> )
Leuchtdichteregelbereich <sup>3</sup>	22 ... 628 cd/m <sup>2</sup>	26 ... 234 cd/m <sup>2</sup>	93 ... 668 cd/m <sup>2</sup>	33 ... 655 cd/m <sup>2</sup>
Reaktionsverhalten (volle Helligkeit, sinnvollster OD-Modus)	3,8 ms	2,2 ms	10,9 ms	8,2 ms
<b>Kontrast</b>				
minimales Sichtfeld <sup>4</sup> / proz. Abweichung	2208:1 <sup>5</sup> / 89,8 %	nicht messbar	2006:1 / 87,5 %	nicht messbar <sup>6</sup>
erweitertes Sichtfeld <sup>4</sup> / proz. Abweichung	1156:1 <sup>5</sup> / 140,3 %	nicht messbar	982:1 / 143,8 %	nicht messbar <sup>6</sup>
Die runden Diagramme geben die Winkelabhängigkeit des Kontrasts wieder. Blaue Farbanteile stehen für niedrige, rötliche für hohe Kontraste. Kreise markieren die Blickwinkel in 20-Grad-Schritten, im Idealfall wäre das gesamte Bild pink.				
winkelabhängiger Kontrast: Kreise im 20°-Abstand				
<b>Bewertungen</b>				
Kontrasthöhe / Blickwinkel-abhängigkeit	⊕⊕ / ⊕	⊕⊕ / ⊕	⊕⊕ / ⊕	⊕⊕ / ⊕
Ausleuchtung / Farbeindruck	⊕ / ⊕⊕	⊕ / ⊕	⊖ / ⊕	⊖ / ⊕⊕
Bedienung / Verarbeitung	⊕⊕ / ⊖	⊕ / ⊕⊕	⊕⊕ / ⊕	⊖ / ⊕⊕
Filmdarstellung / Reaktionszeit	⊖ / ⊕⊕	⊕ / ⊕⊕	⊖ / ⊖	⊕ / ⊕
Preis / Garantie	3800 € / 3 Jahre	1600 € / 2 Jahre	1300 € / 2 Jahre	2230 € / 2 Jahre

<sup>1</sup> gemäß IEC 62087-2 <sup>2</sup> nach zirka 30 Minuten, davor 44,4 W <sup>3</sup> im Desktop-Betrieb <sup>4</sup> Mittelwert und Standardabw. des Kontrasts im min. beziehungsweise erw. Sichtfeld. Das min. Sichtfeld umfasst alle Einblickwinkel, unter denen ein Betrachter das Bild sieht, wenn er aus 60 cm Entfernung frontal auf die Schirmmitte schaut; die Bildecken sieht er dabei unter dem größten Winkel. Im erw. Sichtfeld bewegt er den Kopf parallel zur Schirmfläche bis zu den Displaykanten; der Einblickwinkel auf die gegenüberliegenden Bildränder nimmt zu, der mittlere Kontrast sinkt. <sup>5</sup> gemessen ohne FALD <sup>6</sup> FALD nicht abschaltbar

TV-Programm kann es obendrein auch empfangen und aufnehmen. All das gilt ebenso für den größeren und teureren Samsung-Fernseher, der dem OLED die höhere Spitzenhelligkeit voraus hat. Zudem ist Einbrennen bei ihm kein Thema. Beide gaben allerdings in Verbindung mit HDMI 2.1 kein besonders glückliches Bild ab. Da sie anders als die reinen Gaming-Displays keinen DisplayPort

mitbringen, kann man bei Verbindungsproblemen nicht einfach darauf ausweichen.

Das Asus ROG Swift PG65UQ ist zwar zweifelsohne ein sehr gutes Display, aber nicht nur preislich ein Nischenprodukt. Für weniger als die 3800 Euro, die es derzeit kostet, bekäme man beispielsweise bereits die 65-Zoll-Variante von LGs OLED-Fernseher oder das Samsung-TV

als 75-Zöller. Die haben zwar keinen DisplayPort, sind aber das rundere Angebot. (bkr@ct.de)

## Literatur

- [1] Ulrike Kuhlmann, Ungeliebte Schattenbilder, Maßnahmen gegen das Einbrennen am OLED-TV, c't 23/2018, S. 16
- [2] Carsten Spille, Genug Power für 4K-Gaming, Asus TUF Gaming GeForce RTX 3080 OC, c't 21/2020, S. 44



Bild: Henning Rathjen

# Der Immer-Dabei-PC

## Smartphones am Monitor: Die Desktop-Modi von Huawei und Samsung

**Das Smartphone als Arbeitsgerät: Dank integriertem Desktop-Modus werden einige Smartphones von Huawei und Samsung zum ultramobilen PC. Vor allem Office-Aufgaben lassen sich wunderbar damit erledigen, an anderen Stellen stoßen die Smartphones an Grenzen.**

**Von Robin Brand, Steffen Herget und Jörg Wirtgen**

**H**uawei und Samsung haben ihren Top-Smartphones einen Desktop-Modus spendiert, der startet, sobald man einen Monitor anschließt. Beide verbinden sich mit Smart-TVs sogar drahtlos. Wir haben getestet, wie sich die Desktop-Umgebungen der Smartphones als PC-Ersatz machen, welchen Einsatzszenarien sie gewachsen sind und wo die Grenzen liegen.

Die Hardware selbst ist bei aktuellen Top-Smartphones schon längst nicht mehr der Hemmschuh. Die aktuelle Auflage von Samsungs Note-Serie etwa kommt mit dem schnellen System-on-a-Chip Exynos 990 samt 12 GByte RAM. Multitasking, (einfacher) Videoschnitt, aktuelle 3D-Spiele? Alles kein Problem. Nur arbeiten

will man auf dem kleinen Smartphone-Screen nicht. Hier kommt der spezielle Desktop-Modus zum Einsatz: Einfach per USB-C an einen Monitor angeschlossen, Tastatur und Maus per Bluetooth verbunden, so wird das Smartphone zum Computer.

### Windows lässt grüßen

Voraussetzung dafür ist zunächst einmal, dass das Smartphone über die USB-C-Buchse Displaysignale ausgibt. Diese Fähigkeit spendieren die meisten Hersteller bestenfalls ihren High-End-Smartphones, und selbst dann duplizieren einige Smartphones an einen Monitor angeschlossen schlicht den Inhalt des Smartphone-Displays. Für Streaming und Fotobearbeitung

mag das genügen, doch zum Arbeiten wie an einem Desktop eignet sich das vollbild-orientierte Android nicht.

Daher haben Huawei und Samsung den aktuellen Geräten ihrer P- und Mate-Serie respektive der Galaxy S-, Note- und Z-Serie einen Desktop-Modus eingepflanzt. Sie zaubern eine Desktop-Umgebung auf den Screen, die an eine reduzierte Windows-Oberfläche erinnert und das produktive Arbeiten ermöglichen soll. Bei aktuellen Huawei-Geräten gilt auch im Desktop-Mode die Einschränkung der fehlenden Google-Dienste, dazu später mehr. Eigentlich sollte Android schon mit Version 10 von Haus aus einen Desktop-Modus unter anderem mit einer Taskleiste und einem brauchbaren Fenstermanagement bekommen. Der Code ist im System zwar enthalten, wurde bislang als Funktion jedoch nicht aktiviert. Deshalb mussten die beiden Hersteller dafür eigene Konzepte entwickeln.

Auf dem DeX-Desktop sind Verknüpfungen zu Eigene Dateien, Galerie und Einstellungen abgelegt; außerdem kann man dort nach Belieben neue App-Verknüpfungen hinzufügen oder in der Taskleiste anpinnen. Ähnlich dem Windows-Start-Menü ist unten links ein Icon angelegt, über das alle installierten Apps aufgerufen werden, daneben ist die von Android bekannte Navigationsleiste untergebracht, über die man sich die zuletzt geöffneten Apps (auch die, die man vor dem Start von DeX auf dem Smartphone geöffnet hatte) anzeigen lassen, zum Desktop zurückkehren oder einen Schritt zurückgehen kann. Dazwischen werden die im DeX-Modus aktiven Anwendungen angezeigt, rechts gelangt man zu den Schnelleinstellungen und Benachrichtigungen, kann die Audioausgabe anpassen oder mit einem Mausklick einen Screen-shot aufnehmen.

Ein ähnliches Bild ergibt ein Blick auf Huaweis Desktop-Modus. Auf dem Home-Screen liegen Verknüpfungen zu Dateien, Browser, E-Mail, Memo, Galerie und Huawei Video. In der Taskleiste ist links das Startmenü untergebracht, rechts finden sich Benachrichtigungsmanager und Einstellungsmenü des Smartphones. Per Rechtsklick auf dem Desktop lassen sich zum Beispiel eine neue Datei oder Ordner anlegen, die Bildschirmgröße anpassen oder der Hintergrund ändern. In beiden Umgebungen lassen sich außerdem unterschiedliche Apps an Hintergrund oder Taskleiste pinnen.

**Eine zusammenrollbare Tastatur, das Smartphone als Touchpad, ein Monitor und fertig ist der minimalistische Notfall-PC.**



In beiden Umgebungen starten Apps erst in einem kleinen Fenster, das sich dann verschieben und vergrößern lässt. Auch ein Fullscreen-Knopf ist vorhanden. Mit den ungewohnten Formaten kommen die Apps unterschiedlich gut zurecht. Einige wie Adobe Lightroom nutzen jeden Platz effizient oder öffnen Inhalte wie etwa OneNote in einem sonst den Tablets vorbehalteten, großzügigeren Layout. Andere zeigen Kuddelmuddel und laufen nur zuverlässig, solange man die Fenstergröße unverändert lässt.

### Stolperfalle Hardware

Arbeitet man mit einem USB-C-Dock oder einem Monitor mit USB Power Delivery und eingebautem USB-Hub, erkennt das Smartphone auch darüber angeschlossene Peripherie wie Maus, Tastatur oder USB-Massenspeicher, sogar manche LAN-Ports und USB-Soundchips. Im Test funktionierte das aber nicht mit allen vorhandenen Geräten zuverlässig, weshalb Sie ihr Desktop-Setting vor dem Produktiveinsatz testen sollten.

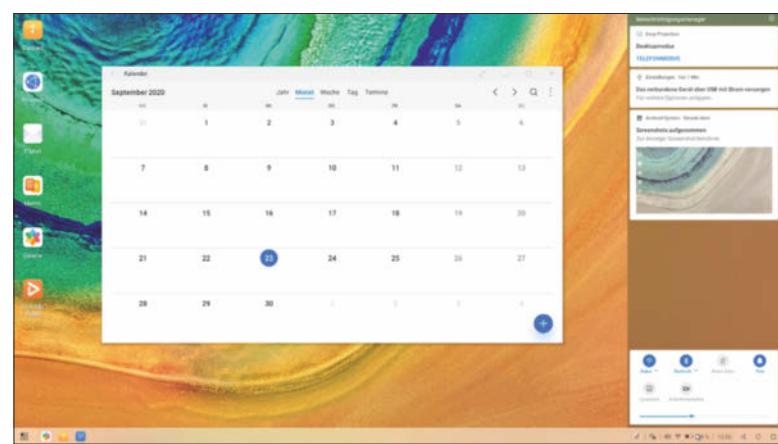
Speziell unsere Huawei-Probanden (P30 Pro und P40 Pro) zeigten sich sehr

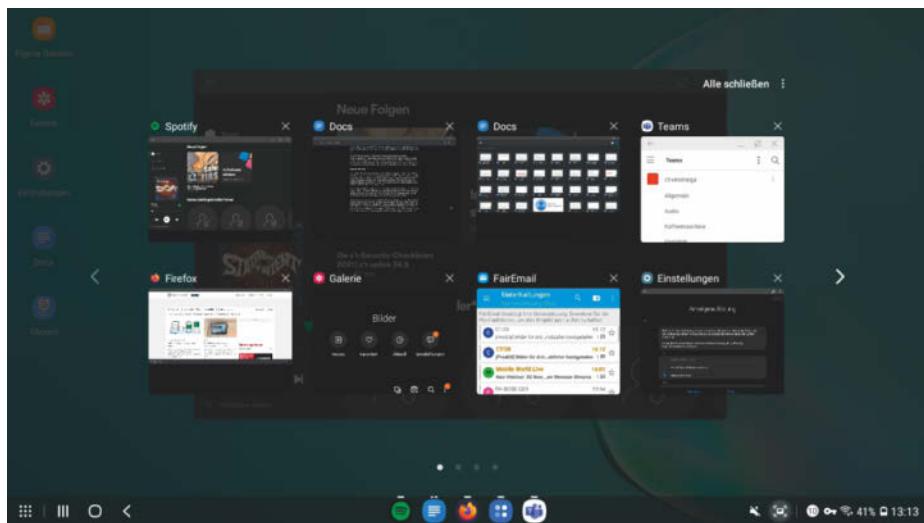
wählerisch, wenn es um die Ansteuerung von Monitoren ging. Über diverse USB-C-Docks, darunter ein Lenovo USB-C-Dock Gen 2 und eines von Anker, wollte es überhaupt nicht funktionieren. Mit Huaweis eigenem MateDock 2 ließen sich die Smartphones dagegen verbinden. Dieses lädt das Smartphone und erweitert es um Anschlüsse für USB Typ A und C sowie VGA und HDMI. Letztere beiden liegen allerdings so eng beieinander, dass sich jeweils nur eins von beiden einstecken lässt. Auch eine direkte Verbindung an einen Monitor per HDMI-auf-USB-C-Kabel klappte. Ohne gleichzeitiges Laden verringerte sich der Ladestand des P40 Pro im Desktop-Modus nur um rund 10 bis 15 Prozent pro Stunde, bei Note 10 und Note 20 Ultra waren es schon mal zwischen 25 und 30 Prozent.

### Angedockt

Auch die drahtlose Verbindung mit Smart-TVs kam einem Glücksspiel gleich. Einen Samsung SmartTV zeigte unser P40 Pro als kompatibles Ausgabegerät an, erfolgreich darstellen ließ sich der Desktop-Mode allerdings nicht darauf. Bei den

**Schön übersichtlich gestaltet Huawei die Desktop-Umgebung.**





Auch mehrere gleichzeitig geöffnete Apps zwingen die modernen Smartphones nicht in die Knie.

Samsung-Testgeräten klappte es – mit Rucklern bei der Übertragung.

Insgesamt verbanden sich die Samsung-Geräte (Galaxy Note 10, Note 20 & Note 20 Ultra) deutlich zuverlässiger. Per USB-C-Dock luden sie, während sie einen Monitor im DeX-Modus ansteuerten. Das klappte mit diversen Monitoren, auch die Ausgabe auf zwei gleichzeitig angeschlossene Displays. Allerdings duplizierte das System dann die Hauptanzeige auf dem zweiten Display; anpassen ließ sich das nicht. Bei einem angeschlossenen Display stehen die Auflösungen HD, FHD und WQHD in verschiedenen Displayformaten zur Auswahl. Mit Note 10 und Note 20 konnten wir Displays allerdings mit maximal FHD betreiben, die Option 3440 × 1440 Pixel blieb auch bei einem 2K-Display ausgegraut. Das Galaxy Z Fold 2 und Galaxy S7+ (siehe Test auf Seite 88) boten im DeX-Modus ein paar mehr Auflösungen an, sie steuerten dasselbe Display mit maximal 3440 × 1440 an.

Eingabegeräte ließen sich kabelgebunden am Dock oder per Bluetooth verbinden, auch das Ethernetkabel und die Audiobuchse des angeschlossenen Displays verwendeten die Samsung-Smartphones. Der Zugriff auf ans Dock angeschlossene USB-Sticks klappte ebenfalls. Andere Peripheriegeräte wie Webcam oder einen Kopfhörer an der Klinkenbuchse des Docks ignorierten die Smartphones.

## Cloud gewinnt

Wer vor allem mit cloudbasierten Diensten wie Microsoft Office 365 oder Google Docs arbeitet, kann in aller Regel mit dem

Desktopbetrieb bei Huawei und Samsung direkt loslegen, nachdem das Smartphone eingestöpselt ist. Eine Anmeldung in der entsprechenden App genügt. Mit dem integrierten Dateimanager der mobilen Office-Apps lassen sich Dokumente schnell finden und öffnen, sodass man sich nicht mit dem für viele Nutzer gewöhnungsbedürftigen Dateisystem von Android auseinandersetzen muss. Man kann auch Dateien direkt aus Clouddiensten wie OneDrive oder Google Drive öffnen.

Der vielleicht größte Vorteil des cloudbasierten Arbeitens: Das Kopieren der Daten auf den Hauptrechner entfällt. Die Daten sind auch dann geräteübergreifend gesichert, wenn das Smartphone verlorengeht.

## Das geht, das nicht

Mails und die bekannten Nachrichten-Apps wie WhatsApp, Telegram und Co. sind so-

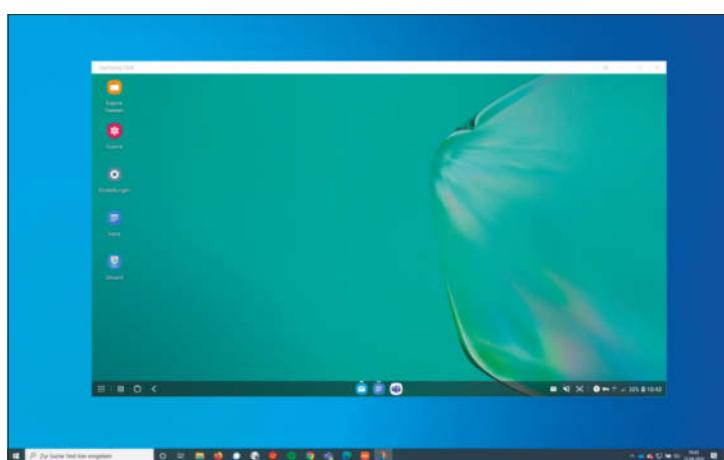
wohl mit DeX als auch mit Easy Projection komfortabel nutzbar. Wenn mehr als ein paar Sätze zu tippen sind, schlägt eine echte Tastatur eben noch immer jeden Smartphone-Touchscreen. Dateien verschicken kann mit GMail und anderen Mail-Apps ein wenig mühsam sein, wenn es sich nicht gerade um Bilder oder Videos handelt. Hier bieten sich die direkten Share-Funktionen der Cloud-Apps an.

Videotelefonie klappt am Ersatz-PC Smartphone prima, wenn der Dienst eine App für Android zur Verfügung stellt – das ist etwa bei Slack, Zoom, Jitsi und Microsoft Teams der Fall. Die funktionieren auch am großen Monitor oder Fernseher, allerdings bleibt die Kamera am Smartphone. Heißt: Das Handy muss während des Anrufs passend in der Hand gehalten oder entsprechend befestigt werden, damit das bei längeren Gesprächen nicht unbequem wird. Häufig ist der Umfang der Videotelefonie-Apps gegenüber der Desktop-Variante eingeschränkt; so kann etwa die Android- (und auch iOS-)Version von Teams keine Gruppenbesprechungen starten.

## Wenig Kompromisse

Bei Office-Arbeiten sind wenige Kompromisse notwendig, solange es nicht allzu weit ins Detail geht. Texte schreibt und bearbeitet man mit Tastatur und Maus über das Smartphone fast wie am PC. Große Tabellen mit vielen Makros und Funktionen sowie aufwendige Präsentationen sind mit den mobilen Apps dagegen nicht so komfortabel zu bearbeiten. Und viele Fähigkeiten der Windows-Versionen fehlen unter Android, beispielsweise die auf großen Monitoren nützliche Mehrseitenansicht von Microsoft Office. Auch benimmt sich die Tastatur häufig anders, so

**DeX lässt sich mit dem passenden Smartphone auch als eigene Anwendung im Windows- oder Mac-Rechner ausführen.**



löscht beispielsweise Strg+Backspace nur in wenigen Apps das vorige Wort.

Auf Huawei-Smartphones neueren Datums gibt es im Desktopmodus ein Problem: Aufgrund des Handelsstreits zwischen USA und China fehlen die auch in vielen Unternehmen genutzten Google-Dienste wie GMail, Google Docs und Google Drive [1, 2].

Die beiden Webbrowser Chrome und Edge arbeiten sauber auf dem großen Bildschirm. Das etwas hakelige Scrollen stört nach kurzer Gewöhnung nicht besonders. Beim Edge-Browser klappt die Bedienung per Tastatur-Shortcuts verlässlicher, Chrome punktet dagegen mit einer übersichtlicheren Multi-Tab-Ansicht. Auch wenn es naheliegt, den Browser für den Einsatz am großen Bildschirm manuell auf „Desktop-Ansicht“ umzustellen, ist das nur eingeschränkt zu empfehlen: In Firefox etwa störte die unten liegende Adresszeile und die Anzeige skalierte nicht zuverlässig. Die eigenen Browser von Huawei und Samsung bereiten ebenfalls keine großen Probleme.

## Grenzen

Im Bereich der Bild- und Videobearbeitung beginnen dann die Schwierigkeiten, und zwar aus zwei Gründen: Software und Performance. Für professionelles Editieren von Bildmaterial fehlen die vollwertigen Desktop-Apps wie Adobe Photoshop, Lightroom oder Premiere. Die Lightroom-App bietet zwar viele wichtige, aber nicht alle Funktionen. Grundsätzliche Dinge schaffen auch die Android-Bordmittel wie Google Fotos oder die eigenen Bildbearbeitungs-Apps von Huawei und Samsung. Bei Videos, vor allem längeren Filmprojekten, stoßen die Exynos- und Kirin-Prozessoren irgendwann an ihre Grenzen.

Bei zahlreichen anderen Anwendungen werden die Grenzen der Software ebenfalls deutlich, nicht zuletzt bei der Bedienung. Smartphone-Apps sind eben für Smartphones und Touch-Bedienung konzipiert und weniger für Maus und Tastatur. Während das bei den Office- und Mail-Programmen keine Schwierigkeiten bereitet, erschwert das Fehlen von Wischgesten und Touch die Bedienung vieler Anwendungen.

## Smartphone im Notebook

Samsungs DeX kann nicht nur Monitor und Peripherie übernehmen, sondern lässt sich auch als Zweit-Desktop auf einem PC verwenden. Dazu installiert

## Smartphones per Miracast ans TV anbinden

Mit einem Smart-TV oder einem entsprechenden Dongle arbeiten die Notfall-PC-Lösungen von Huawei und Samsung auch drahtlos. Die Verbindung über Miracast ist schnell erledigt und im Test stabil. Die Skalierung gelingt mit dem P30 Pro besser als mit dem Note 20 Ultra. Das Huawei-Smartphone merkt sich alle geöffneten Apps und Fenster für das nächste Mal, bei Samsung werden die Anwendungen minimiert. Die Verwendung der Kamera über Miracast leidet mit dem Huawei-Smartphone stärker unter Aussetzern und verzögerten Signalen als bei Samsung.

Wer ein Android-Handy oder iPhone besitzt, hat mit Link to Windows von Microsoft eine weitere Option, Smartphone und PC zu koppeln. Direkt in den Systemeinstellungen vieler Android-Handys integriert, finden darüber Benachrichtigungen, SMS, Fotos und andere Inhalte den Weg vom Android-Handy auf den Windows-Rechner und zurück. Auch Telefone lassen sich bequem am PC

führen, ohne extra zum Smartphone greifen zu müssen. Die Einrichtung erfordert viele Freigaben und Berechtigungen, klappte im Test aber mit dem Galaxy Note 20 Ultra und dem P30 Pro ohne Schwierigkeiten. Die Kopplung der Smartphones erfolgt am Microsoft-Konto und ist somit auf allen angemeldeten Windows-PCs nutzbar. Mit Huawei Share lassen sich Huawei-Smartphones und -Laptops ebenfalls koppeln, Dateiaustausch per Drag & Drop inklusive.

Mit App-Streaming haben aktuelle High-End-Smartphones von Samsung eine Funktion, die andere Hersteller derzeit nicht bieten: Damit können Android-Apps vom Smartphone in einem Windows-Fenster ausgeführt werden. Prinzipiell klappt das mit allen Apps, es gibt jedoch Einschränkungen. Die Ausrichtung im Quer- oder Hochformat gibt die App vor, manuelles Umschalten ist nicht möglich. Actionreiche Spiele leiden zudem unter merklichen Hakkern und einem Zeitverzug in der Anwendung.

man auf Windows-7- und 10- oder Mac-Rechnern (ab Mac OS 10.13) die DeX-Software. Sie startet als eigene Instanz, sobald ein kompatibles Samsung-Smartphone per USB-Kabel angeschlossen wird. Wer zum Beispiel an einem fremden Notebook nicht seine sensiblen Daten im Betriebssystem eingeben möchte, kann einfach per DeX im Vollbild Texte schreiben oder Fotos präsentieren und auf alle anderen Anwendungen des Smartphones zugreifen – sofern der Notebook-Besitzer die Installation der DeX-Software auf seinem Gerät erlaubt.

## Fazit

Hat man keinen PC zur Hand, kann man mit Samsung DeX und Huawei Easy Projection auch auf dem Smartphone arbeiten. Dieser Modus eignet sich aber nicht für den alltäglichen Gebrauch, sondern ist vor allem für den gelegentlichen Gebrauch konzipiert – und selbst dann kommt es darauf an, ob der eigene Workflow und die benutzte Hardware fürs kurzfristige Umsatteln auf das Smartphone taugen. Für den täglichen Einsatz nerven Dinge wie ungewöhnliche Webcam-Perspektiven, nicht erkannte Peripherie oder nicht ans Vollbild optimierte Apps. Wer viel mit

Dateien hantieren und womöglich gar auf verschiedene Firmenserver zugreifen muss, für den ist das Smartphone als Notebook-Ersatz nichts. Doch wenn es darum geht, in der Zeit, bis das Windows-Update eingespielt ist, etwas zu erledigen, lässt sich auf den Desktop-Umgebungen von Huawei und Samsung produktiv arbeiten – vor allem, wenn man vieles mit Clouddiensten erledigt. Selbst lange Texte zu verfassen, ist kein Problem, genauso wenig wie an Videokonferenzen teilzunehmen, mal eben die Präsentation aufzuhübschen oder ein paar Zahlen in eine Excel-Tabelle einzutragen. Für die Büro-Stippvisite oder den Urlaub mag das völlig reichen – und so muss man nur einen USB-C-HDMI-Adapter einstecken und nicht das ganze Notebook. Nützlich ist der Modus auch, um Privates im Büro am Dienstmonitor zu erledigen.

(rbr@ct.de) **ct**

## Literatur

- [1] Robin Brand, Tschüss, Google, Huawei Mate 30 Pro ohne Google-Dienste, c't 5/2020, S. 122
- [2] Jörg Wirtgen, Zeichen-Tablets, Huawei MatePad und MatePad Pro mit Stift, aber ohne Google-Apps, c't 18/2020, S. 82



# Foto-Duell

## Smartphone gegen Kompaktkamera: Sony Xperia 1 II versus Sony RX100 VII

**Smartphone-Kameras können viel – echtes Fotografie-Gefühl ersetzen sie nicht. Sony will das mit dem Xperia 1 II ändern, doch schießt das Smartphone auch bessere Fotos als die Kompaktkamera Sony RX100 VII?**

**Von Sophia Zimmermann**

**D**as Smartphone ist für viele Hobbyfotografen längst zur Immer-dabei-Kamera geworden. Kein Wunder: Mit einem Fingertipp ist der Schnappschuss im Kasten – mit oft brauchbaren Ergebnissen. Nur das Fotografie-Gefühl bleibt auf der Strecke. Das will Sony mit dem

Xperia 1 II ändern und stattet es dafür unter anderem mit einer neuen Photo-Pro-App aus. Sie erinnert stark an das Menü von Sonys Digitalkameras und zeichnet auch Raw-Daten auf. Wir haben den manuellen Modus des 1000-Euro-Smartphones mit der ähnlich teuren Top-Kompakten von Sony verglichen, der RX100 VII – einem äußerst kompakten Allrounder mit festem Objektiv. Den regulären Test des Xperia 1 II lesen Sie in c't 18/2020 auf Seite 80.

Während die Hersteller ihre Smartphones mit immer größeren Sensoren ausstatten, können sie stufenlose optische Zooms nicht bieten. Da ist die Kompaktkamera mit ausgewachsener Optik im Vorteil. Ihr Objektiv deckt einen Kleinbild-äquivalenten Brennweitenbereich von 24 bis 200 Millimetern ( $f/2 - f/4,5$ ) ab und bietet damit einen 8-fachen optischen

Zoom. Die Kamera arbeitet mit einem Typ-1-Zoll-Sensor und einer Auflösung von 20 Megapixeln.

Das Smartphone dagegen arbeitet mit drei Kameras, um verschiedene Brennweiten abzudecken. Die Hauptkamera bildet einen Bildwinkel von 82 Grad ab, was einer Kleinbild-äquivalenten Brennweite von etwa 24 Millimetern entspricht. Die Blende öffnet sich auf  $f/1,7$ . Sony setzt auf seinen 1/1,7 Zoll großen Exmor-RS-Chip. Zur Hauptkamera gesellt sich ein Modul mit Kleinbild-äquivalenter Brennweite von 70 Millimetern (Bildwinkel: 34 Grad) und einer Lichtstärke von  $f/2,4$ . Der eingesetzte Chip ist 1/3,4 Zoll groß. Mit einer Kleinbild-äquivalenten Brennweite von 16 Millimetern deckt das dritte Modul einen besonders großen Bildwinkel ab (124 Grad). Seine Lichtstärke liegt bei  $f/2,2$ , als Sensor dient ein 1/2,55 Zoll großer Exmor-RS-Chip.

### Auflösung: Weniger ist mehr

Auffällig ist, dass Sony anders als viele Konkurrenten nicht mit hohen Auflösungen protzt. Die Module geben die Bilder allesamt mit maximal 12 Megapixeln aus. Tatsächlich ist bei Smartphones weniger mehr, denn die einzelnen Sensorpixel fallen so größer aus. Das ist entscheidend für die Bildqualität. Je größer die Grundfläche der einzelnen Fotodioden, desto mehr

Photonen können sie in derselben Zeit einsammeln und später in Bildinformationen umwandeln. Das wirkt sich positiv auf Rauschverhalten und Dynamikumfang aus.

Im konkreten Fall arbeitet die Hauptkamera des Sony Xperia 1 II mit einer Pixelbreite von etwa 2 Mikrometern. An die RX100 VII reicht sie damit nicht heran. Sie kommt trotz höherer Auflösung auf circa 2,4 Mikrometer breite Pixel.

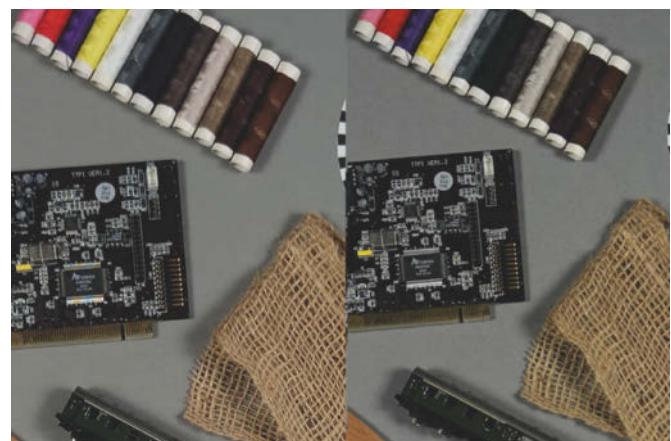
Zum Vergleich: Die Hauptkamera des Samsung Galaxy S20 Ultra besitzt einen größeren 1/1,33 Zoll-Chip (ca. 9,5 mm x 7,2 mm), packt darauf aber 108 Megapixel, die man sich so auch ausgeben lassen kann. Die Pixelbreite liegt bei lediglich 0,8 Mikrometern. Standardmäßig speichert das Smartphone seine Bilddateien allerdings ebenfalls mit 12 Megapixeln, dabei kombiniert es die Informationen mehrerer Fotodioden miteinander. Diese Technik des Pixelbinnings nutzen Telefone, um die Nachteile der Mini-Pixel zu bändigen. Samsung gibt die Größe des so verrechneten Pixels mit 2,4 Mikrometern an.

Wie sich die unterschiedliche Technik im Bild tatsächlich niederschlägt, haben wir in Labor und Praxis überprüft. Dabei haben wir das Xperia 1 II wie eine Digitalkamera behandelt. Alle Aufnahmen entstanden in der Photo-Pro-App mit manuellen Belichtungseinstellungen.

### Besser als die Realität

Die Laborergebnisse des Sony-Smartphones sind überraschend gut – zumindest, was die Messergebnisse anbelangt. Das geht bereits bei Rauschverhalten und Dynamikumfang los. Bei ISO 100 haben wir ein Signal-Rausch-Verhältnis von 78 ermittelt. Das Signal-Rausch-Verhältnis (S/Nx) ist ein Maß für die Störungen („Grieseln“) im Bild, die durch interne Be-

**Kein Rauschen und wenig Details zeigt die Laboraufnahme des Xperia 1 II (links) im manuellen Modus bei ISO 100. Mehr bringt bei diesen Bedingungen die Kompaktkamera RX100 VII zustande (24 mm, ISO 100).**



rechnungen und Effekte wie thermisches Rauschen hervorgerufen werden. Je höher das S/Nx, desto weniger Störungen sind im Bild sichtbar.

Der Visual Noise kommt auf sagenhafte 0,6. Visual Noise (VN) steht für das subjektiv wahrnehmbare Rauschen. Werte bis 0,8 stehen für weitgehende Rauschfreiheit. Werte bis zwei deuten auf einen wenig, Werte bis drei auf einen mäßig und Werte über drei auf einen deutlich störenden Rauscheindruck hin. Dazu kann das Smartphone auf einen beachtlichen Dynamikumfang von etwas mehr als elf Blendenstufen verweisen, durchschnittlich erreichen Digitalkameras einen Umfang von zehn Blendenstufen, wie auch die RX100 VII.

Beim gemessenen S/Nx und VN hält die Kamera nicht ganz mit: Sie startet mit einem Signal-Rausch-Verhältnis von 53 und einem VN von 0,8. Beide Kameras verschlechtern sich mit steigender Signalverstärkung nur moderat. Doch selbst bei ISO 3200 steht beim Smartphone noch ein VN von 1,4 und ein S/Nx von 55. Die Kamera kommt auf einen VN von 2,4. Das S/Nx fällt auf 26. Es dürften die realistischeren Werte

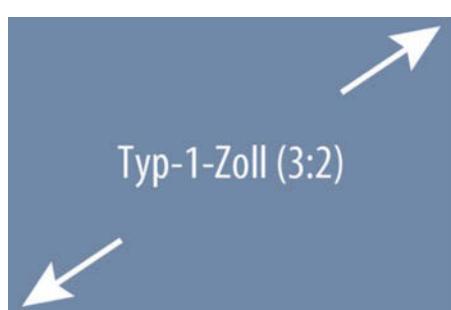
sein, denn die Praxisbilder zeigen nicht die Überlegenheit des Smartphones, die offensichtlich softwarebedingt ist.

Im Gegenteil: Der Fall ist tief. Die Praxisbilder erklären die guten Werte für das visuell wahrnehmbare Rauschen und auch für das Signal-Rausch-Verhältnis. Das ist nämlich selbst bei hohen Empfindlichkeiten tatsächlich nicht sichtbar, allerdings aus einem unschönen Grund: Die Software des Xperia 1 II bügelt die Aufnahmen selbst bei niedrigen Empfindlichkeiten derart glatt, dass praktisch kaum noch Strukturen und Details erhalten bleiben. Dazu schärft sie äußerst großmütig nach, sobald sie kontrastreiche Übergänge „wahrnimmt“. Die RX100 VII rauscht dagegen wahrnehmbar, aber sie erschafft dennoch auch jenseits von ISO 100 einen detailreichen, plastischen Bildeindruck.

### Raw-Dateien mit Potenzial

Ein Blick auf die Raw-Dateien der Kameras zeigt allerdings, dass in den Smartphone-Aufnahmen (ebenfalls aufgenommen über die Photo-Pro-App) etwas mehr Potenzial steckt – obwohl sie einen deutlichen Rotstich aufweisen und Moirés ins Auge fallen. Mit wenig Aufwand erhält man zumindest bei den unteren ISO-Stufen noch einige Details und erreicht so einen natürlicheren Bildlook.

Sony ist durchaus in der Lage, JPEG-Dateien gefällig auszugeben, was der Hersteller mit seinen Digitalkameras wie eben der RX100 VII auch beweist. Die gemeinsame Philosophie, die in Smartphone und Kamera stecken soll, lässt sich in den Bildergebnissen aber nicht erkennen. Bessere Ergebnisse erzielt man mit dem Smartphone oftmals, wenn man die reguläre Foto-App verwendet und sich voll auf die Automatik verlässt – der Reiz der manuellen Fotografie ist dann natürlich dahin.



13,2 mm x 8,8 mm



7,6 mm x 5,7 mm

Der Sensor der Kamera sammelt Licht auf einer deutlich größeren Fläche als der Smartphone-Sensor.



**Bei anspruchsvollen Lichtverhältnissen kämpft das Smartphone mit dem hohen Motivkontrast. Nicht nur helle Elemente fressen aus, auch nicht im Schatten liegende Gräser sind betroffen.**

## Bildqualität in der Praxis

Aber: Labor ist Labor. Um weitere Unterschiede zwischen den Geräten herauszuarbeiten, waren wir auch draußen unterwegs und haben sie in verschiedenen Disziplinen gegeneinander antreten lassen. Die Praxisaufnahmen zeigen weitere deutliche Unterschiede auf.

Wir starten mit Katzenfotos, da sollte das Smartphone eigentlich in seinem Element sein. Tatsächlich eignen sich die Stubentiger dank ihres filigranen Fellkleids auch wunderbar als Testmotive. Unsere Testkatze saß bei schummrigem Lichtverhältnissen im Körbchen. Die RX100 VII erschafft ein vergleichsweise dynamisches Bild. Das Smartphone-Foto wirkt deutlich blasser und weniger plastisch. Auffällig ist, dass beide Kameras ähnlich belichten.

In der Disziplin Landschaftsfotografie haben wir uns für eine detail- und kontrastreiche Szene in einem Flutgraben entschieden, die Sonne im Rücken. Die Lichtverhältnisse sind anspruchsvoll, selbst in der Aufnahme der RX100 VII wirkt der Himmel ausgefressen. Alles Irdische arbeitet sie plastisch heraus. Das Xperia kämpft deutlich stärker mit dem hohen Motivkontrast. Es fressen nicht nur Elemente vor dem Himmel aus, sondern bereits die nicht im Schatten liegenden Gräser und Steine.

Bei der Nahaufnahme einer Blume zeigen beide Probanden eine schöne Freistellung vor dem Hintergrund und eine knackige Schärfe auf den Blumenblättern. Die Naheinstellgrenze der RX100 VII liegt selbst im Weitwinkelbereich lediglich bei acht Zentimetern, sodass sie durchaus auch für Makro-Aufnahmen taugt.

Auch mit dem Smartphone erzielt man einen ansehnlichen Freistell-Effekt bei Nahaufnahmen – ohne spezielle Automatiken zu bemühen. Die Vollansicht wirkt scharf und plastisch. Wer genau hin-

sieht, erkennt Unschönheiten wie überstrahlte Wassertropfen auf der Blüte.

## Stilechte App

Die Photo-Pro-App erinnert in Farbe und Aufbau stark an die Kameramenüs. Auffällig: Ein Softbutton zum Auslösen fehlt. Diese Funktion übernimmt eine zusätzliche physische Taste. Dreht man das Smartphone für Querformat-Aufnahmen, sitzt sie dort, wo bei einer Digitalkamera der Auslöser sitzen würde. Und tatsächlich verhält sie sich dabei auch genauso. Halb durchgedrückt aktiviert sie den Autofokus, ganz durchgedrückt nimmt sie das Bild auf.

Dazu beherrscht die App verschiedene Belichtungsautomatiken – an Bord sind P, S und M. Blendenvoreinstellungen sind nicht möglich. Alle anderen Belichtungsparameter können dagegen angepasst werden. Relativ umfangreich lässt sich der Autofokus konfigurieren. Er erkennt außerdem automatisch Gesichter und Augen und stellt darauf scharf. Allerdings bleibt die Frage, wie viel ein Autofokus wirklich zu tun hat, denn die Schärfentiefe des kleinen Sensors ist in Kombination mit der geringen Brennweite eh schon enorm.

Sony trennt die Photo-Pro-App streng von der normalen Foto-App, die das Xperia 1 II zusätzlich besitzt. Ihr Aufbau entspricht den Anwendungen anderer Smartphones. Hier können Fotografen auch Hintergrundeffekte ins Bild rechnen lassen. Anders als beispielsweise Samsung-Smartphones ist das Xperia dabei allerdings wenig kreativ. Verschiedene Stile gibt es nicht, und das Telefon schwankt ständig zwischen den Befehlen „Bewegen Sie sich näher an das Objekt“ und „Bewegen Sie sich weiter weg vom Objekt“. Das Ergebnis ist ein Unschärfefrei im Hintergrund. Dafür beherrscht das Xperia im Porträt-Modus Kunststückchen wie „Vergrößerte

Augen“ oder „Schmales Gesicht“, mit denen man sich zur Kunstfigur trimmen kann.

Was dem Xperia 1 II gänzlich fehlt, ist ein Nachtmodus. Werden die Lichtverhältnisse schummrig, möchte es still gehalten werden und belichtet dann entsprechend länger. Möglich sind bis zu 30 Sekunden. Bei Nachtaufnahmen kämpft es mit den gleichen Defiziten wie die kleine Digitalkamera und zeigt verwaschene Ergebnisse mit wenigen Details.

## Fazit

Das Sony Xperia 1 II verspricht, „außergewöhnliche Bildqualität“ zu liefern und hofft dabei offenbar auf einen Vertrauensvorschuss, denn die Digitalkameras des Herstellers spielen tatsächlich seit Jahren in der ersten Liga. Die hohen Erwartungen kann das Xperia 1 II nicht erfüllen.

Ja, die Photo-Pro-App bringt echtes Fotografie-Gefühl, die Einstellungsmöglichkeiten sind vielfältig und wirken sehr professionell. Dass Sony sie allerdings strikt von der herkömmlichen Foto-App trennt, ist wenig nutzerfreundlich.

Und dann ist da noch die Bildqualität, die sicher nicht schlecht ist. Aber richtig gut ist sie eben auch nicht. Vor allem fehlt es den Bildern an Tiefe und in den höheren Empfindlichkeiten verwaschen Details. Nicht nur im Vergleich zur RX100 VII muss sich das Smartphone geschlagen geben, auch einige Konkurrenten wie das Huawei P40 Pro oder das Samsung Note 20 Ultra liegen vor dem Xperia 1 II. Aber auch die Bildqualität dieser Top-Smartphones reicht oftmals nicht an die der Sony RX100 VII heran.

(rbr@ct.de) **ct**

*Dieser Artikel erschien ursprünglich auf heise+.*

## Digitalkamera versus Smartphone

Modell	Sony RX100 VII	Sony Xperia 1 II
Art	Digitalkamera	Smartphone
Hauptkamera Auflösung / Brennweite (KB-Äquivalent) / Blende / Sensorgröße / OIS	20 MP / 24-200 mm / f/2...4,5 / 1" / ✓	12 MP / 24 mm / f/1,7 / 1/1,7" / ✓
Ultraweitwinkel Auflösung / Brennweite (KB-Äquivalent) / Blende / Sensorgröße / OIS	–	12 MP / 16 mm / f/2,2 / 1/2,55" / –
Telekamera Auflösung / Brennweite (KB-Äquivalent) / Blende / Sensorgröße / OIS	–	12 MP / 70 mm / f/2,4 / 1/3,4" / ✓
Preis	1100 €	1150 €
✓ vorhanden	– nicht vorhanden	



## Sie suchen einen interessanten und qualifizierten Job in der IT-Branche?

### Attraktive Arbeitgeber warten auf Sie!

heise jobs, die Jobbörse von heise online, und Jobware, der Stellenmarkt für Fach- und Führungskräfte, begrüßen Sie beim IT-Jobtag! Zahlreiche attraktive Arbeitgeber präsentieren sich mit ihren aktuellen Stellenangeboten, Aus- und Weiterbildungsplätzen sowie berufsbegleitenden Studiengängen aus dem ITK-Segment. Im direkten Gespräch können Sie sich informieren, austauschen oder auch eine individuelle Karriereberatung bzw. einen Bewerbungscheck der Jobware Personalberatung in Anspruch nehmen. Verschiedene Vorträge zu spannenden Themen ergänzen das Rahmenprogramm.

### Aus aktuellen Anlass:

- Der IT-Jobtag ist als nationale Veranstaltung ausgelegt.
- Es werden alle notwendigen Hygiene-Vorschriften beachtet.
- Während der Veranstaltung werden an allen Eingängen Desinfektions-Handspender aufgestellt.

### TERMINE 2020

#### STUTTGART

28.10.2020

IHK Region Stuttgart

#### BERLIN

05.11.2020

Spreespeicher

#### LEIPZIG

11.11.2020

Marriott Hotel

#### FRANKFURT

18.11.2020

IHK Gebäude am Börsenplatz

powered by

heise  
jobs

Jobware  
da hab' ich den Job her!



Bild: Thorsten Hubner

# Kioske und Kaufhäuser

## Shopsysteme für angehende Online-Händler

**Shopsysteme sind das A & O im Onlinehandel. Ihre Auswahl entscheidet maßgeblich über die Chancen beim Verkauf im Netz. Wir geben Verkäufern in spe Tipps, worauf sie dabei achten sollten.**

Von Tobias Weidemann

Der E-Commerce boomt – und das nicht zuletzt wegen der Coronakrise, in der Teile des Präsenzhandels die Pforten schließen mussten. Bereits 2019 setzten die deutschen Onlinehändler stolze 72,6 Milliarden Euro um. Und gerade angesichts der Sonderkonjunktur während der Corona-bedingten Einschränkungen konnte der

Onlinehandel punkten: 36,7 Milliarden Euro – und damit 9,2 Prozent mehr als im gleichen Zeitraum des Vorjahres – gaben deutsche Kunden in den ersten zwei Quartalen 2020 aus. Besonders Waren des täglichen Bedarfs wie Lebensmittel, Tierbedarf, Medikamente oder Drogerieprodukte werden inzwischen viel öfter im Internet gekauft als noch vor der Pandemie.

Und noch etwas hat sich in den letzten Monaten geändert: Immer häufiger entdecken auch lokale Händler aus dem Präsenzhandel den Onlinehandel als weiteres Standbein – sei es als virtuelles Schaufenster, als zusätzlichen, weltweit erreichbaren Kanal oder für den Abverkauf bestimmter Bestellwaren, die man früher despektierlich Ladenhüter genannt hätte.

Ähnlich wie Sie als Händler in der Innenstadt die passenden Geschäftsräume finden müssen, entscheidet die Wahl des

richtigen Shopsystems über Ihre Chancen beim Verkauf im Netz – egal, ob Sie ein kleiner oder ein mittelgroßer Händler sind. Über die Jahre haben sich zahlreiche Varianten eingebürgert, die alle ihre Eigenheiten, Vor- und Nachteile haben. Wir präsentieren eine Auswahl, um Ihnen bei der Orientierung zu helfen.

### Worauf achten?

Um es andersherum zu sagen: Die Wahl des falschen Shopsystems ist ungefähr so fatal wie die Wahl der falschen Geschäftsräume. Wenn Sie den Shop zu groß oder an Ihren Anforderungen vorbei wählen, wenn er eine für Ihren eigenen Bedarf benötigte Schnittstelle nicht anbinden kann oder Sie ein anderes wichtiges Element übersehen, können Sie solche Fehler nachträglich meist nur noch schwer ausgleichen. Beim Start in den E-Commerce

sollten Sie daher prüfen, wie flexibel und skalierbar ein Shopsystem ist. Es muss in der Lage sein, mit Ihren Anforderungen und Ansprüchen zu wachsen. Funktionen, die Sie aktuell nicht benötigen, sollten nachrüstbar sein oder selbst entwickelt werden können. Verfügt das Shopsystem über Schnittstellen zu anderen E-Commerce-Modulen (etwa Warenwirtschaftssystemen), ist das ein Indiz für die Zukunftsfähigkeit. Das gilt ebenso, wenn das System eine große Zahl an Erweiterungen bietet, auch für ausgefallene Probleme oder Branchenlösungen.

Großes Augenmerk sollten Sie überdies auf die Handhabung des Backends und die Shop-Performance für Ihre Kunden legen. Begutachten Sie dafür sowohl bestehende Shops anderer Händler, die bereits ein bestimmtes System nutzen, als auch eine Testinstallation. Prüfen Sie außerdem, ob Sie über das Shopsystem bei Bedarf mit Plattformen wie eBay oder Amazon Marketplace zusammenarbeiten können (siehe Kasten auf Seite 116).

Haben Sie einige Systeme in die enge Wahl genommen, sollten Sie sich mit dem Anbieter respektive der Community befassen. Dazu lohnt es sich, sofern möglich, bei größeren Shopsystemen einen Händlertag oder die jährliche Kundenveranstaltung zu besuchen. Dort können Sie meist auch Erfahrungen mit Shopbetreibern austauschen, die Ihnen keine Konkurrenz machen, aber ähnliche Voraussetzungen und Bedürfnisse wie Sie haben.

Im nächsten Schritt müssen Sie sich entscheiden, ob Sie eine Kauf-Software mit einmaligen oder regelmäßigen Lizenzkosten oder ein gemietetes System mit regelmäßigen Kosten auf Abonnement-Basis bevorzugen. Einige Anbieter setzen auf eine regelmäßige Abo-Gebühr. Sie kann entweder eine Pauschale sein oder eine Kombination aus monatlichem Festpreis plus einer umsatz- oder stückzahlbasierten variablen Komponente. Daneben gibt es (zunehmend seltener) das klassische Lizenzmodell, bei dem eine Version einer Software pauschal erworben wird. Allerdings haben Sie gerade damit nicht unbedingt alles abgegolten, weil es bei den aufwendigeren Systemen oftmals nicht ohne eine erfahrene E-Commerce-Agentur geht. Auch sie nimmt ihre regelmäßige Abgebühr („Retainer“) oder einen stundenbasierten Preis.

Unabhängig davon stellt sich die Frage, ob es für Sie sinnvoll ist, wenn Sie den Shop auf einem eigenen Server hosten oder hosten lassen („on Premise“ respek-

tive „off Premise“) oder ob Sie einem cloudbasierten System den Vorzug geben. Im letzteren Fall erhalten Sie als Händler einen fertig konfigurierten Shop, den Sie mehr oder weniger anpassen können. Und nicht zuletzt müssen Sie bei der Shopsoftware die Entscheidung treffen, ob es eine Open-Source-Variante sein soll oder ob Sie auf einen der kommerziellen Anbieter mit Closed Source setzen wollen. Größere Unternehmen bevorzugen oftmals die zweite Variante, binden sich damit allerdings enger an einen Anbieter. Zusätzlich gibt es Shopsysteme, die zwar im Kern Open Source sind, aber Plug-ins, Erweiterungen oder Anpassungen an weitere Systeme erfordern. Für diese zahlen Sie dann wiederum eine monatliche oder einmalige Implementierungsgebühr.

Dieser Umstand ist auch der Grund, warum Anbieter preislich nur schwer vergleichbar sind. Denn zum einen ist es mit dem meist monatlichen Preis für die Shopsoftware (egal ob auf dem eigenen Server oder in der Cloud) nicht getan, zum anderen sind die angebotenen Produktvarianten sehr unterschiedlich in der Ausstattung – was bei einer Anwendung selbstverständlich mit dabei ist, kostet bei einer anderen extra. Hinzu kommt als Blackbox das etwaige Budget für eine Agentur; dazu später mehr. Bei kleinen Systemen, bei denen Sie alles aus einer Hand bekommen und auch die Administration selbst erledigen können, haben wir Preise angegeben.

### Klein, fertig, von der Stange

Wenn Sie ein überschaubares Sortiment feilbieten wollen, sollten Sie sich zunächst die kleineren gehosteten Software-as-a-Service- (SaaS-)Shops von der Stange ansehen. **Jimdo**, **Wix Stores** und der **1&1/lonos-Shop** sind gute Beispiele dieser Kategorie. Solche Cloud-Angebote stehen Ihnen für einen geringen monatlichen Betrag fertig vorbereitet und konfiguriert zur Verfügung – und das in einer responsiven Version, die automatisch eine für Mobilgeräte optimierte Version anzeigt, sobald sie ein solches Gerät erkennt. Als Händler geben Sie lediglich im relativ engen Rahmen das Erscheinungsbild des Shops vor, wählen eine Designvorlage oder ein Template, ordnen gegebenenfalls noch nach Ihren Wünschen oder Usability-Geschichtspunkten die einzelnen Elemente neu an und fügen Ihr Waren sortiment ein.

Programmierkenntnisse benötigen Sie nicht: Die Systeme sind baukastenartig gestaltet. Der monatliche Preis unter-

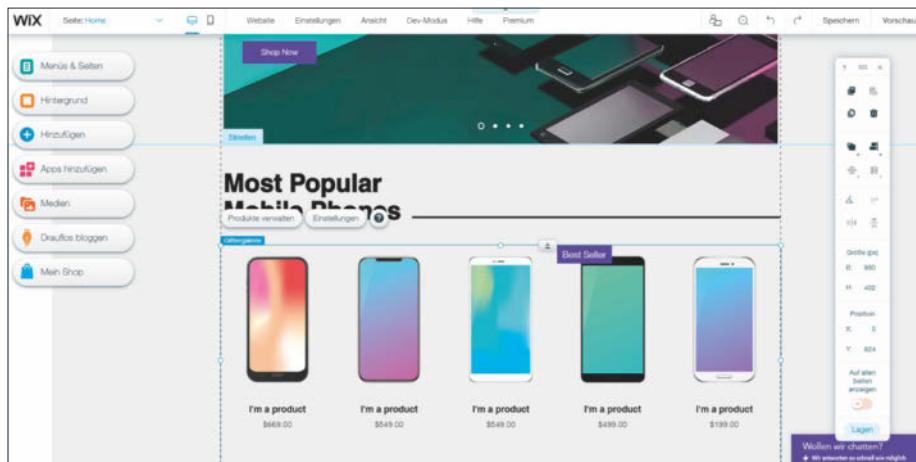
scheidet sich je nach Zahl der Artikel und Funktionsumfang. Er beginnt bei wenigen Euro im Monat für Händler, die online zunächst auf kleiner Flamme anfangen wollen. Die Obergrenze liegt bei rund 40 bis 50 Euro im Monat. Normalerweise können Sie die benötigte Domain gleich mitbuchen, was wir im Interesse einer seriösen Außenwirkung auch zwingend anraten. Achten Sie darauf, dass die Domain in diesem Fall Ihnen gehört und der Betreiber des SaaS-Shops sie nicht nur in Ihrem Auftrag an Sie weitergibt. Ansonsten verlieren Sie bei einem Anbieterwechsel die angestammte URL.

Die Nase rümpfen sollten Sie als Einsteiger oder Onlinehändler, der das Geschäft nur nebenbei betreiben will, über solche Shopsysteme von der Stange nicht. Schauen Sie sich etwa einige Beispiele shops von Wix Stores an, können diese Shops mit großen Systemen von vor einigen Jahren an vielen Stellen mithalten – sowohl bei Designs und Vorlagen als auch beim Funktionsumfang. Zugleich setzen sie nicht das Praxiswissen von E-Commerce-Fachleuten voraus. Wollen Sie sich überhaupt nicht mit der Technik und dem Setup eines Shops befassen, finden Sie bei Wix auch

## Shop-Widgets

Wenn Sie nur ein paar Produkte anbieten wollen, können Widgets eine Art E-Commerce durch die Hintertür sein. Die kleinen Kaufboxen integrieren Sie per Code-Import in beliebige Websites. Sie bereichern beispielsweise eine redaktionelle Website oder ein Blog um E-Commerce-Elemente. Auch als zusätzliches Element auf Landingpages und Microsites sowie in Communitys sind Shopping-Widgets zunehmend populär.

Der gesamte Kaufprozess ist direkt in das Widget integriert, das sich damit beispielsweise auch für den Verkauf wenig erklärbungsbedürftiger Waren wie Gutscheine eignet. Solch eine Kaufbox ist neben dem Fertig-Shop die günstigste und einsteigerfreundlichste Möglichkeit, mit dem Onlinehandel zu starten. Shopping-Widgets bieten beispielsweise **Shopify**, **Versacommerce** und das auf digitale Produkte spezialisierte **Elopage** an.



Mit vielen Vorlagen und einem Baukastenprinzip machen es kleine SaaS-Shopsysteme wie Wix Stores aufstrebenden Händlern leicht, die ersten Schritte zu gehen.

entsprechende Dienstleister – als mäßig technisch gebildeter Nutzer brauchen Sie diese indes nicht. Ein entscheidender Vorteil all dieser Fertigsysteme ist, dass Sie sich als Händler ausschließlich um die Pflege des Sortiments und um das Abarbeiten der Bestellungen kümmern müssen. Der Nachteil liegt darin, dass Sie beispielsweise Warenwirtschaftssysteme aus Ihrem Präsenzgeschäft und einen automatisierten Artikeldatenimport nicht verknüpfen können.

Insbesondere kleinen und mittleren Händlern, die sich ein zusätzliches Standbein im Onlinehandel aufbauen wollen, erleichtern solche Angebote den Einstieg. Zudem sorgen sie für eine deutlich kürzere „Time to market“. Während der

Coronakrise haben auf diesem Weg zahlreiche Geschäfte auf die Schnelle einen Webshop eröffnet. Dafür bieten solche einfachen Shops nur begrenzte Möglichkeiten in der Anpassung und der Produktpräsentation – und wie schon angedeutet können Sie Handels-APIs und andere Systeme kaum anbinden. Da neue Funktionen vom Anbieter des Shopsystems bereitgestellt werden, müssen Sie sich als Händler mit dem begnügen, was Sie vorfinden. Wenn Sie bestehende eigene Systeme integrieren wollen, werden Ihnen schnell die damit verbundenen Einschränkungen auffallen.

Niedrigschwellig sind diese Angebote überdies, wenn Sie Logistikunternehmen und Zahlungsdienstleister einbinden wol-

len. Die Shopsysteme unterstützen alle gängigen Verfahren dafür, also etwa Versand-Vorankündigungen an Speditionen oder Bezahlschnittstellen. Nur um entsprechende Verträge müssen Sie sich selbst kümmern. Beim Thema Rechtskonformität sind Sie ebenfalls schon ein gutes Stück auf der sicheren Seite, zumindest was die Gestaltung des eigentlichen Shops betrifft. Das entbindet Sie allerdings nicht von der Pflicht, bei der werblichen Darstellung auf die Begrifflichkeiten zu achten, auch um sich vor Abmahnungen missgünstiger Mitbewerber zu schützen [1]. Nachdem das Privacy-Shield zwischen der EU und den USA gekippt ist, müssen Sie außerdem generell darauf achten, wo sich der Hauptsitz des Unternehmens befindet und ob persönliche Kundendaten auf Servern in den USA fließen können. Das kann etwa bei Wix Stores zum Problem werden, obwohl Israel als „sicheres Drittland“ gilt [2].

### Shoplösungen mit individuellerem Ansatz

Bei den individuelleren Lösungen, die vor allem ambitionierte Zweitstandbeinhändler und reine Onlinehändler des klassischen Mittelstands ansprechen, gibt es inzwischen ein Nebeneinander von Cloud-Lösungen und selbst gehosteten Shops. Mit dem Siegeszug der Cloud-Infrastrukturen haben diese auch im Onlinehandel zugenommen und sind mittlerweile selbst bei größeren Onlinehändlern eher die Regel als die Ausnahme. Sie haben handfeste Vorteile: Gerade bei größeren Händlern kommt es vor, dass die Besucherzahl stark schwankt. Wenn Ihre

## Bereit für die Plattform: Warum eBay, Amazon & Co. relevant sind

Zahlreiche E-Commerce-Riesen betreiben ihre eigene Plattform. eBay und Amazon Marketplace sind die Klassiker, aber auch Zalando, Otto, Real oder Galeria spielen mit. Zahlreiche Plattformen haben jedoch eine problematische Doppelrolle: Sie sind einerseits Onlinehändler und betreiben andererseits den Marktplatz. Schlecht für Sie, wenn Amazon über Ihre Verkaufszahlen Bescheid weiß, Sie aber nicht deren konkretes Zahlenwissen kennen.

Als Ersatz für einen eigenen Webshop sollten Sie solche Plattformen nicht sehen. Sie erlauben Ihnen nur wenig Freiheit in der individuellen Warenpräsenta-

tion. Zudem verlangen sie eine stattliche Provision für die Reichweite und den Platz im virtuellen Schaufenster. Doch gerade darin liegt ein Argument, warum Sie dort zusätzlich präsent sein können. Verstehen Sie die Provision in dem Fall als Marketing-budget, mit dem Sie Ihre Kundenzahl vergrößern und sich einen Namen in ihrem Handelssegment erarbeiten können.

Machen Sie sich aber bewusst, dass die Betreiber die Regeln vorgeben. Im schlimmsten Fall drehen sie nicht nur an der Provisionsschraube, sondern schließen Händler vom Verkauf aus. Dafür reichen schon wenige Unstimmigkeiten mit

Kunden. So ist Amazon bei Reklamationen seinen Kunden gegenüber extrem kulant und fordert dies auch von den Marketplace-Händlern ein – durchaus ein Nachteil für Sie als Händler. Zudem können Amazon und andere Ihnen bei gut laufenden Produkten schnell Konkurrenz machen.

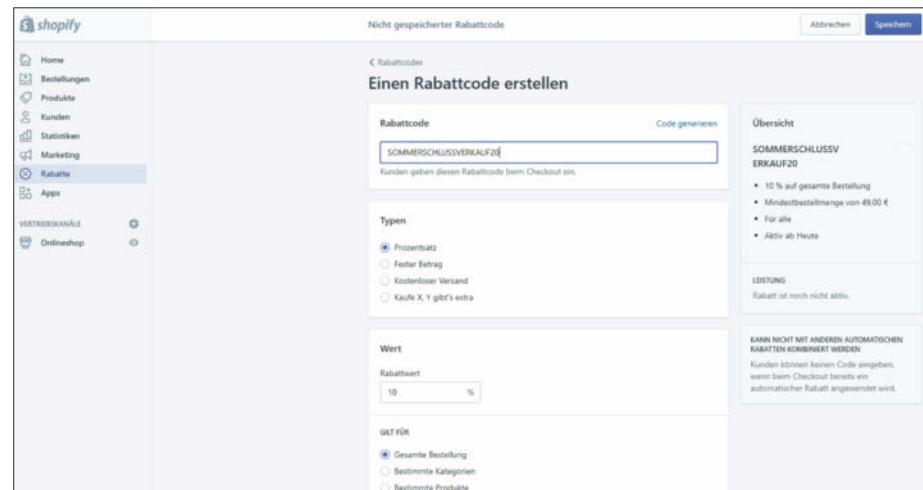
Trotzdem sollten Sie sich bei der Wahl einer Shoplösung den Weg in die Plattformen über entsprechende Export- und Importschnittstellen offenhalten. Fehlt der Abgleich mit der Warenwirtschaft und den Logistiktools, stößt Ihre Bestellabwicklung gerade in Spitzenzeiten schnell an Grenzen.

Besucher aber bei großem Andrang nach einer Werbeaktion nicht bestellen können, ist das im Sinne der Conversion – der „Umwandlung“, bei der Ihr Besucher zum zahllenden Kunden wird – der größte anzunehmende Unfall. Mehr noch, es hinterlässt einen schlechten Eindruck bei den gerade mühevoll gewonnenen Besuchern und Kunden. Individuell skalierbare Cloud-Lösungen federn kurzfristigen Ansturm besser ab als das statische On- oder Off-Premise-Rechenzentrum. Sie bieten sich daher auch für die Shoplösung an.

Es gibt inzwischen viele erfolgreiche Cloud-Systeme für den E-Commerce. Eines der bekanntesten und erfolgreichsten ist **Shopify**. Sie können dort Shops für Vertriebskanäle wie Web und Mobile, aber auch für soziale Netzwerke und Marktplätze gestalten. Nicht nur Einsteiger erhalten für 29 US-Dollar im Monat einen vollwertigen Shop; große, international aufgestellte Webshops bekommen für 299 US-Dollar im Monat das Maximum an Funktionsumfang. Plattformen wie Shopify lassen sich nach Bedarf unterschiedlich skalieren.

Zum Grundpreis kommen bei Shopify variable Entgelte für die Zahlungsabwicklung, die zwischen 1,8 und 2,4 Prozent des Brutto-Verkaufspreises liegen. Sie als Händler und der Shopsystemanbieter haben also gleichermaßen Interesse daran, dass der Shop gut läuft. Funktionen wie Rabattcodes, Geschenkgutscheine oder Zählung von Kaufabbrüchen mit nicht ausgecheckten Warenkörben stellt Shopify in allen Versionen bereit, ebenso Schnittstellen. Ein ausführlicheres Be richtswesen und Monitoring steht aber erst in den größeren Varianten zur Verfügung. Shopify bietet Ihnen zudem die Möglichkeit, es als Bestellsystem im eigenen Ladengeschäft etwa über ein Tablet zu nutzen. Das können Sie via Shopify POS einbinden.

Eine Alternative unter den SaaS-Lösungen ist ein modular aufgebautes System wie **Plentymarkets**. Es bringt zusätzlich zum reinen Onlineshop auch Lösungen für das ERP-System zur Unternehmensplanung mit. Dafür stellt es beispielsweise Kundenpflege- (CRM-), Kassenterminal- (POS-), Fulfillment-, Marketing- und Marktplatzanbindung bereit. Die einfachste Variante mit sämtlichen Softwaremodulen kostet ab 39 Euro, hinzu kommen in diesem Fall aber noch als variables Entgelt 0,5 Prozent des Brutto-Auftragsvolumens. Die Ein-Mandanten-Lösung kann außer-



Cloudanbieter wie Shopify haben ein intuitiv zu bedienendes Backend, in dem sich auch Neulinge relativ schnell zurechtfinden.

dem bis zu fünf Kassen im Laden verwalten und enthält einen Shop-Builder, mit dem Sie einfach nach dem Baukastenprinzip Seiten erstellen können. Mit dem „Shop-Booster“ sollen Sie das Einkaufserlebnis und die Ladezeiten optimieren können. Mithilfe eines REST-API, das kompatibel zum Open-API-Standard 2.0 ist, können Sie Plentymarkets außerdem an andere Softwaresysteme wie Warenwirtschaft anbinden.

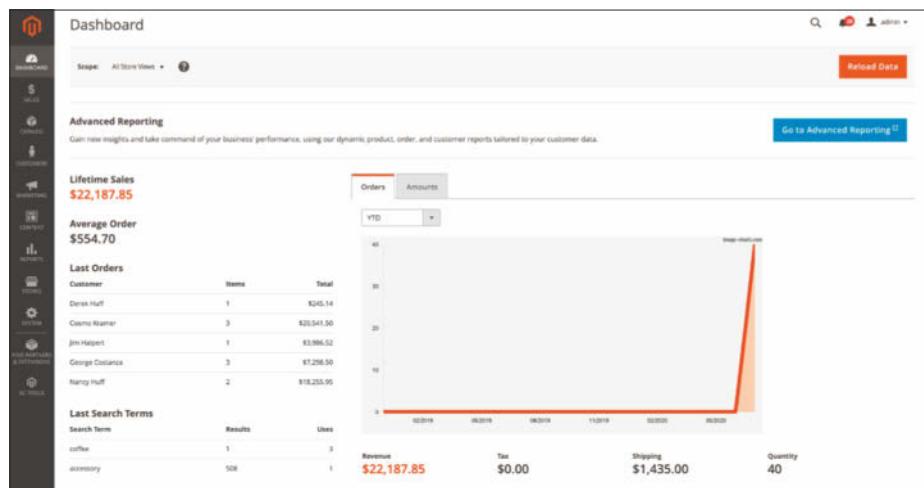
Zusätzlich gibt es für erfahrene Händler und Großunternehmen auch noch weitere Versionen, die auf individuelle Anforderungen in Sachen Funktionsumfang und Abrechnung zugeschnitten sind. Plentymarkets bietet sich vor allem an, wenn Sie alles aus einer Hand haben wollen, ohne sich dabei Gedanken um das Zusammenspiel der Komponenten machen zu müssen.

E-Commerce-Produkte aus der Cloud und im Umfang eines Shopify oder Plentymarket sind somit ein Kompromiss zwischen selbst gehosteten Shops, die Ihnen noch mehr Individualisierungspotenzial bieten, und den einfachen SaaS-Shops von der Stange. Sie sind dazu in aller Regel auch optimal an die Suchmaschinenoptimierung (SEO) angepasst. Zudem können Sie sie komfortabel über Schnittstellen mit CRM- oder Versandsystemen verbinden. Zu den weiteren Vorteilen der Cloud gehören regelmäßige Updates und Anpassungen sowie Skalierbarkeit. Nicht zuletzt in der Vorweihnachtszeit wissen viele Mittelstands-Onlinehändler und ambitionierte Präsenzhändler mit Online-Zweitstandbein dieses Modell zu schätzen.

## Shopsoftware: von Open und Closed Source

Dass softwarebasierte Shopsysteme so häufig dem Open-Source-Gedanken folgen, hat mit dem Geschäftsmodell ihrer Anbieter zu tun: Auf diese Weise bekommen sie eine große Reichweite, eine starke Stellung am Markt sowie Support aus der Entwicklerszene. So entstehen viele Erweiterungen und Brückenschläge zu anderen Systemen, etwa aus der Payment- und ERP-Welt. Auch spezielle Zusatzfunktionen, die nur einzelne Shops benötigen (etwa Aboverkauf), werden Sie im Open-Source-Bereich eher finden. Im Open-Source-Sektor haben Sie außerdem große Zukunftssicherheit, weil die Community populäre Features oder Anbindungen häufig auch dann weiter pflegt, wenn ein Unternehmen sie nicht mehr anbietet. Doch Open Source heißt nicht, dass Sie alles kostenlos nutzen dürfen. Häufig erhalten Sie neben dem quelloffenen Grundsystem angepasste, kostenpflichtige Systeme für Ihr Einsatzszenario, oder Sie nutzen Erweiterungen gegen Entgelt – Preise sind Verhandlungssache.

Oftmals stehen hinter Open-Source-Shopsystemen große Unternehmen, etwa **Magento**, das seit 2018 Teil der Adobe Experience Cloud ist. Magento ist derzeit das verbreitetste reine Shopsystem. Sie können es an vielen Stellen erweitern und anpassen. Auf einem Marktplatz für Plugins und Extensions, genannt „Magento Connect“, erhalten Sie Module für nahezu alles Denkbare im E-Commerce-Kontext – etwa Artikelempfehlungen oder eine interne Suche. Allerdings brauchen Sie umfangreiche Vorkenntnisse und Zeit,



**Selbst gehostete Shopsoftware (hier: Magento) ist trotz aller Übersichtlichkeit nichts mehr für den schnellen Einstieg. Aufgrund der komplexen Möglichkeiten empfiehlt sich die Hilfe eines Freelancers oder einer Agentur.**

um so einen Shop auf dem eigenem Server oder Webspace einzurichten und zu betreiben. Das gilt auch für andere Systeme dieser Art. Planen Sie solch ein größeres E-Commerce-Projekt, sollten Sie daher bei der Strategiedefinition wie auch beim Aufbau des Shops auf die Dienste einer erfahrenen E-Commerce-Agentur oder (in kleinerem Rahmen) eines guten Freelancers setzen.

Neben Magento Open Source (ehemals „Community Edition“) gibt es auch Magento Commerce. Diese lizenpflichtige, erweiterte Version enthält deutlich mehr Funktionen, etwa einen besseren Editor, sowie Gewährleistung und Support. War Magento ursprünglich ein reiner Shop, ist es inzwischen auch mit Anbindungen an andere Händlersysteme ausgestattet. Neben den Softwareversionen erhalten Sie Magento außerdem als Teil der Magento Commerce Cloud von Adobe. Das Hosting übernimmt Amazon Web Services (AWS) – deshalb müssen Sie sich

mit der DSGVO-Konformität auseinandersetzen.

Ebenfalls häufig anzutreffen ist **Shopware**. Sie bekommen es auf Open-Source-Basis und in einer kommerziellen Lizenzversion mit weiteren Features. Auch für das browserbasierte System deutschen Ursprungs erhalten Sie etliche Module und Plug-ins; zudem bietet es Schnittstellen zu allen gängigen Warenwirtschaftssystemen und Payment-Dienstleistern. Das PHP-basierte System setzt eine MySQL-Datenbank voraus, lässt sich aber ohne Programmiererfahrung einrichten und betreiben.

Auch Shopware bietet seit Juni 2020 eine Cloud-Edition namens „Shopware Starter Edition“ an. Sie wendet sich vor allem an Einsteiger. Dabei soll sie so einfach wie die kleineren Shops von der Stange sein und zugleich gewährleisten, dass Sie bei größerem E-Commerce-Engagement einigermaßen reibungslos in die größere Shopware-Edition wechseln können.

nen. Diese umfassendere Version soll es zukünftig nicht nur als selbst gehostete Variante, sondern auch als individuelleren Cloud-Shop geben. Doch der identische Preis von monatlich 199 Euro Grundgebühr für die jeweilige Professional Edition täuscht: Im Fall der Cloud-Edition kommen noch 0,5 Prozent Umsatzbeteiligung hinzu. Welche Variante sich unter Kosten- gesichtspunkten für Sie lohnt, hängt von Ihrer Kundenstruktur und Ihren Umsätzen ab. Mehr Flexibilität und geringere Investitionskosten erhalten Sie auf jeden Fall mit der Cloud.

Das Beispiel zeigt noch etwas anderes: Als Händler haben Sie ein Interesse daran, möglichst in einem einmal gewählten Shop-Ökosystem zu bleiben, auch wenn die Umsätze zunehmen oder beispielsweise neue Märkte im Ausland hinzukommen. Bei Magento und Shopware haben Sie große Sicherheit, dass Sie mithilfe des Shopsystem-Anbieters einen Relaunch ohne umfangreichere Anpassungen realisieren können: Ihre bestehenden Schnittstellenanbindungen, Erweiterungen und vielleicht sogar speziell programmierte individuelle Lösungen werden weiterhin funktionieren.

Ein (in der Grundversion) prinzipiell kostenloses Open-Source-E-Commerce-System ist **WooCommerce**. Hierbei handelt es sich ebenfalls um eine vollwertige Shopsoftware, die vollständig auf Wordpress basiert, dem weltweit meistgenutzten Content-Management-System. Wenn Sie als fortgeschrittenener Einsteiger oder Mittelständler bereits über eine entsprechende Wordpress-Umgebung für Ihre Website verfügen, können Sie diese Shopsoftware integrieren. Auch auf der Bedienoberfläche werden Sie sich schnell zurechtfinden.

Neben einer großen Zahl an Design-Templates, die Sie individuell anpassen können, stehen Ihnen auch viele Plug-ins

## Shopsysteme (Auswahl)

	Commercetools	Intershop	Ionos MyWebsite Shop	Jimdo	Magento	osCommerce	OXID eShop	Plentymarkets
Anbieter	commercetools GmbH / REWE Digital GmbH	Intershop Communications AG	1&1 Ionos SE	Jimdo GmbH	Magento, Inc. / Adobe, Inc.	-	OXID eSales AG	plentysystems AG
URL	commercetools.com	intershop.com	ionos.de	jimdo.com	magento.com/de	oscommerce.de	oxid-esales.com	plentymarkets.eu
Lizenzmodell	kommerziell	kommerziell	Abonnement	Abonnement	Open Source, kommerziell	Open Source	Open Source, kommerziell	Abonnement
Hauptsitz	Deutschland	Deutschland	Deutschland	Deutschland	USA	-	Deutschland	Deutschland
Technik	SaaS	gehostet, SaaS	SaaS	SaaS	gehostet, SaaS	gehostet	gehostet	SaaS
Zielgruppe	Mittelstand bis Großunternehmen	Großunternehmen	Einsteiger	Einsteiger	fortgeschritten Einsteiger bis Großunternehmen	fortgeschritten Einsteiger bis Mittelstand	Mittelstand	fortgeschritten Einsteiger bis Mittelstand

<sup>1</sup> Plug-ins z. T. kommerziell

<sup>2</sup> Starter

<sup>3</sup> Spryker Now

zur Verfügung. Diese decken sämtliche Eigenheiten des deutschen Onlinehandels ab und sind auf einem Marktplatz für Erweiterungen erhältlich. Zusätzlich lassen sich auch zahlreiche Wordpress-Erweiterungen verwenden, die das System insbesondere bei der Content-Erstellung vielseitiger machen. Eine Herausforderung kann es hier wie überall sein, sämtliche rechtlichen Vorgaben im deutschen Onlinehandel einzuhalten (beispielsweise zu Mengenangaben und Kennzeichnungspflichten). Die Erweiterung „Woo Commerce Germanized“ deckt in dieser Hinsicht immerhin viele Themen ab. Sie sollten sie als erste installieren.

Ebenfalls verbreitet und vor allem unter Open-Source-Anhängern mit kleinen und mittleren Shops sehr beliebt ist **osCommerce**. Das Shopsystem kann auf rund 20 Jahre Entwicklungszeit zurückblicken und verfügt über eine große, sehr rege und hilfsbereite Community. Gut 9000 Erweiterungen und mehr als 21.000 Shops, in denen osCommerce zum Einsatz kommt, stellen dessen Zukunftsfähigkeit sicher. Neben einer umfassenden Dokumentation und umfangreichen Foren finden Sie beispielsweise von 1&1 vorbereitete Hosting-Pakete. Dennoch ist osCommerce wohl das genaue Gegenteil von den Shopsystemen, bei denen Sie auch mit rudimentärem IT-Wissen sofort loslegen können. Es ist vielmehr ein System, das zum Basteln und Optimieren einlädt. Deshalb eignet es sich für Nutzer, die Erfahrungen mit der Technik sammeln wollen.

Bei den vorgestellten großen Open-Source-Systemen werden Sie, wie schon angedeutet, in aller Regel einen E-Commerce-Dienstleister benötigen. Er passt Ihren Shop im Detail an die Workflows Ihres Unternehmens an. Durch die weite Verbreitung der vorgestellten Systeme gibt es jeweils eine große Auswahl an solchen

## Großsysteme

Am oberen Ende der Skala stehen Anbieter komplett kommerzieller Systeme wie SAP, IBM oder Salesforce. Je nach Anforderungen an einen Shop kann es sich bei großen E-Commerce-Projekten lohnen, auf ein solches kommerzielles System zu setzen, insbesondere, wenn in Ihrem Unternehmen bereits andere Komponenten des jeweiligen Unternehmens zum Einsatz kommen. Allerdings liegen die Projektkosten für einen solchen Shop schnell im sechsstelligen Bereich – mit entsprechenden Folgekosten. Als zweites Standbein eignen sie sich auf keinen Fall.

Dienstleistern. Sie unterstützen Sie auch dabei, Templates und Layouts an Ihr Corporate Design anzupassen, Microsites und Landingpages zu erstellen sowie die Rubrikseiten aufzubauen, die Sie mithilfe einer Agentur für Suchmaschinen optimieren müssen.

## Die Qual der Wahl

Vom kleinen Online-Schaufenster bis zum multinationalen E-Commerce-Kaufhaus gibt es eine Vielzahl von Shopsystemen. Das macht es für Entscheider im E-Commerce so schwierig, das Passende zu finden. Obwohl Sie beim Start meist noch keine in sich stimmige E-Commerce-Strategie haben dürften, sollten Sie zumindest die eingangs aufgeworfenen Fragen klären, bevor Sie sich als Onlinehändler für ein Shopsystem entscheiden – am besten tun Sie das schon vor einer Demo-Tour oder Beratung durch die Vertreter der infrage kommenden Shops.

Generell gilt: Wenn Sie nur mit wenigen Produkten anfangen und zunächst

Erfahrungen mit den Backends und der Abwicklung von Bestellungen mitsamt Bezahlprozessen und Logistik sammeln wollen, sind Sie mit einer der kleinen SaaS-Varianten gut beraten. Größere Cloud-Systeme wie Shopify sind ein guter Kompromiss zwischen einer großen Zahl an Möglichkeiten und schneller Time to Market. Demgegenüber sind die Open-Source-Programme deutlich flexibler zu erweitern – ein Muss für ambitioniertere E-Commerce-Projekte, bei denen Sie möglicherweise auch auf bestehende ERP- und Warenwirtschaftssysteme zurückgreifen wollen.

Ab einem bestimmten Komplexitätslevel werden Sie als Onlinehändler nicht mehr ohne das Know-how einer Agentur oder eigener Fachkräfte auskommen. Der Vorteil einer Agentur (oder eines Freelancers) ist, dass sie weitere Projekte betreut und daher den E-Commerce-Markt gut kennt und beobachtet.

Bei Systemen ausländischer Anbieter, etwa Wix Stores, Woo Commerce oder Shopify, sollten Sie mithilfe einer Rechtsberatung unbedingt prüfen, ob sämtliche deutschen Vorgaben eingehalten werden (etwa Datenschutzrecht, Grundpreisangaben oder Kennzeichnungspflichten bei bestimmten Warenkategorien). Zwar gilt das auch für inländische Anbieter. Für einen deutschen Onlinehändler ist es aber generell kein Schaden, sich für ein System aus Deutschland zu entscheiden, etwa Jimdo, Shopware oder Plentymarkets. Sie haben viele deutsche Rechtsnormen bereits umgesetzt. (mon@ct.de) **ct**

## Literatur

- [1] Nick Akinci, Joerg Heidrich, Die Abmahnern lauern, Wie wettbewerbsrechtliche Unterlassungsansprüche die Existenz von Shop-Neulingen gefährden, c't 17/2020, S. 176
- [2] Holger Bleich, FAQ: Das Ende des Privacy Shields, c't 21/2020, S. 178

PrestaShop	Salesforce Commerce	SAP Hybris	Shopify	Shopware	Spryker	VersaCommerce	Wix Stores	WooCommerce	Xt:Commerce
PrestaShop SA	salesforce.com, Inc.	SAP SE	shopify Inc.	shopware AG	Spryker Systems GmbH	Versacommerce GmbH	Wix.com	Automattic Inc.	xt:Commerce GmbH
prestashop.com/de	salesforce.com/de	sap.com	shopify.de	shopware.com	spryker.com/de/	versacommerce.de	de.wix.com	woocommerce.com	xt-commerce.com
Open Source	kommerziell	kommerziell	Abonnement	Open Source	kommerziell	Abonnement	Abonnement	Open Source <sup>1</sup>	einmalige Lizenz
Frankreich	USA	Deutschland	Kanada	Deutschland	Deutschland	Deutschland	Israel	USA	Österreich
gehostet	SaaS	gehostet, SaaS	SaaS	gehostet, SaaS <sup>2</sup>	gehostet, SaaS <sup>3</sup>	SaaS	SaaS	gehostet	gehostet
fortgeschritten	Großunternehmen	Großunternehmen	Einsteiger bis Mittelstand	Einsteiger bis Mittelstand	Mittelstand bis Großunternehmen	Einsteiger	Einsteiger	Einsteiger bis Mittelstand	fortgeschritten
Einsteiger bis Mittelstand									



Bild: Rudolf A. Blaha

# Kuratiert ins Postfach

## Die Renaissance der Newsletter

**Newsletter prägen journalistische Dickschiffe wie die New York Times mit, bilden die Kristallisierungskerne neuer Medienunternehmen und ermöglichen es jedermann, Kleinstpublikationen mit spitzer Zielgruppe herauszubringen. Wer für frische, interessante, sorgfältig zusammengestellte Inhalte aufgeschlossen ist, kann so manche spannende Entdeckung in seinem Postfach machen.**

Von Jo Bager

E-Mail-Newsletter? Das ist doch Spam“, so werden wohl viele Menschen denken, wenn man sie auf das Thema anspricht. Und tatsächlich steht der Begriff meistens für etwas, das man nicht haben will: etwa für Supersonderangebote, die man nur erhält, weil man irgendwo etwas bestellt und den Newsletter mit untergeschoben bekommen hat. Oder unambitioniert zusammenkopierte Überschriften und Vorlauftexte von Zeitungen. Mit so etwas holt man niemanden hinter dem Ofen hervor.

Aus dem Wust solch liebloser und nerviger digitaler Postwurfsendungen stechen schon seit ein paar Jahren wesentlich bessere Angebote heraus. Einige Journalisten zäumen das Medium E-Mail-Newsletter neu auf, stellen täglich oder wöchentlich ein fein auf das Zielpublikum abgestimmtes Nachrichtenpaket zusam-

men und bereiten es passend für das Medium auf – mit viel Erfolg.

Beispiele gefällig? Bei **Fever Pit'ch** von Sportjournalist und Chefredakteur bei Sport1 Pit Gottschalk dreht sich alles um Fußball. Jeden Freitag informiert **Finanztip.de** die fast 800.000 Abonnenten seines kostenlosen Newsletters über aktuelle ökonomische Entwicklungen, erklärt Grundlagen und gibt konkrete Tipps zum Thema „persönliche Finanzen“. Am anderen Ende des Preisspektrums liegt der Tagesspiegel, der unter der Marke **Tagespiegel Background** mehrere hochspezialisierte Newsletter zu Themen wie Klima & Energie oder Digitalisierung & KI herausbringt – und zwar für jeweils 179 Euro pro Monat. Während Newsletter hierzulande meist (noch?) andere Medien begleiten und ergänzen, gibt es in den USA bereits journalistische Angebote und Plattfor-

men, die ausschließlich auf E-Mail-Newsletter setzen, etwa **The Hustle** und **Substack**.

## Auf den Punkt

Laut dem Digital News Report, für den das Reuters Institute Menschen in 40 Ländern interviewt hat, empfangen rund 16 Prozent der Befragten mindestens einen Newsletter pro Woche (Deutschland: 18%). Das klingt noch nicht so spektakulär, aber: Knapp die Hälfte dieser Nutzer gab an, dass E-Mail ihre Hauptquelle für Nachrichten ist. Newsletter-Empfänger sind tendenziell älter und besser situiert als der Durchschnitt. Häufig ist von Millennials als *der Zielgruppe* für Newsletter die Rede, aber nicht immer – es gibt auch welche, die sich an jüngere Menschen richten.

Auf den ersten Blick bietet das Medium wesentlich weniger als Websites und Apps. So lassen sich viele dynamische und interaktive Elemente nicht in E-Mails darstellen: Ein reduziertes Layout, ein wenig Typografie, mal ein Bild, ein paar Icons – das wars. Zudem kann man Newsletter nicht schnell updaten.

Die Eingeschränktheit von Mails lässt sich allerdings auch als Vorteil sehen. E-Mails sind endlich, im Unterschied zum schier grenzenlosen und unübersichtlichen Internet. Der Empfänger hat das Gefühl, einen guten Überblick zu bekommen. Er wird nicht mit Informationen erschlagen, sondern auf den Punkt informiert (wenn es gut gemacht ist).

In diesem Zusammenhang ist häufig von Skimmable Content die Rede, auf Deutsch also etwa „gut durch querlesen oder überfliegen erfassbare Inhalte“: Kurze Absätze und kurze Sätze sind Trumpf. Der Newsletter enthält oft eine für sich stehende Zusammenfassung eines Sachverhalts; wer das Thema vertiefen will, findet den Link dazu.

Überschriften und Hervorhebungen stellen wichtige Punkte heraus; Spiegelstriche oder Listen strukturieren komplexe Informationen; Infografiken und Videos werden nur eingebettet, wenn sie Informationen besser aufbereiten können. Das Layout unterstützt die Übersichtlichkeit mit viel Weißfläche und indem Abschnitte mit Karten oder Kästchen voneinander abgetrennt sind.

Aus Betreibersicht sind Newsletter attraktiv, weil sich über die Mail-Adresse ein direkter Kanal zum Leser öffnet. Die Nutzung lässt sich etwa über das Nachladen von Bildern sowie über Mailbugs oder geklickte

Links gut tracken. Newsletter-Tools registrieren jede Nutzeraktion genau, liefern gute Statistiken etwa zur Konversion von Werbung. Aus Sicht des Datenschutzes ist das allerdings bedenklich.

## Eine langsame Welle

Die Renaissance der E-Mail-Newsletter läuft im Grunde schon seit Beginn der 2010er-Jahre. Genauso wenig wie es den einen Grund für den neuen Erfolg des alten Mediums gibt, gab es auch nicht das eine Ereignis oder Medium, das die neue Popularität anfachte.

Zulauf bekamen digitale Rundbriefe zum Beispiel durch die Betreiber und Leser von Blogs. Im Jahr 2013 hat Google seinen RSS Reader eingestellt, das bis dahin am weitesten verbreitete Hilfsmittel, um Inhalte von Blogs und Nachrichtensites zu sammeln und zu lesen. Newsletter empfahlen sich als Alternative, die zudem einen persönlicheren Kanal zwischen Autor und Lesern aufbauten.

Manchmal sind E-Mail-Newsletter auch schlicht per Zufall entstanden. Sam Parr zum Beispiel kam die Idee zu The Hustle im Jahr 2015, als er mit einem Mailing die Konferenz HustleCon beworben hat. Daraufhin wurde er von Antworten quasi überrollt. Offensichtlich hatte er die richtige Ansprache für seine Empfänger gefunden. Seither betreibt er The Hustle mit großem Erfolg: Mehr als 1 Million Abonnenten erhalten täglich seine „business and tech in 5 minutes or less“.

Nur noch 29 Prozent der Befragten des Digital News Reports greifen direkt auf Nachrichten-Websiten oder -Apps zu, und dieser Anteil geht weiter zurück. So gut wie jeder dagegen nutzt E-Mail – auch auf dem Smartphone. Und in ihr E-Mail-Postfach schauen Anwender mehrmals am Tag. Von dort lassen sie sich dann wieder gut in andere Medien abholen.

Seit Dezember 2019 darf WhatsApp nicht mehr als Nachrichtenticker verwendet werden, weil der Massenversand von Nachrichten gegen die Nutzungsbedingungen des Anbieters verstößt. Unternehmen experimentieren seit dem Wegfall auch verstärkt (wieder) mit E-Mail-Newslettern. Der Tagesspiegel zum Beispiel brachte als Ersatz für sein WhatsApp-Angebot den E-Mail-Newsletter **Fragen des Tages** heraus.

## Newsletter-Großbaustelle

Zu journalistischen Medien gehören Newsletter einfach dazu. Sie sind ein eta-

**Gut strukturierte, auf den Punkt formulierte Texte, klar abgegrenzte Blöcke: Die wichtigsten Inhalte von The Morning Brew lassen sich gut beim Überfliegen erfassen.**

bliertes Mittel, um Leser bei der Stange zu halten. Viele große Medien haben erkannt, dass es schon lange nicht mehr genügt, einfach nur Überschriften und Vorlauftexte zusammenzukopieren – dafür gibt es RSS-Feeds. Sie experimentieren schon seit etlichen Jahren mit dem Format und gehören zu den Vorreitern bei der Weiterentwicklung des neuen Formats.

Was für die New York Times einen guten Newsletter ausmacht, hat sie bereits 2018 beschrieben (siehe ct.de/xyu8). So sind speziell für die Newsletter verfasste Berichte und Essays Pflicht: „Bieten Sie etwas Wertvolles an, das Sie nirgendwo sonst bekommen können.“ Wichtig sei es auch, den Newsletter ansprechend zu gestalten. Last, not least ist persönliche Ansprache essenziell.

Der wichtigste Newsletter, **The Morning**, erreicht städtische 17 Millionen Abonnenten. Das Publikum ist somit fast dreimal so groß, wie die New York Times

zahlende Abonnenten hat (6,5 Millionen). Ein gut gemachter Newsletter ist also auch für sich interessant genug, obwohl die Nicht-Abonnenten die hinter der Paywall verborgenen Artikel nicht mal zu sehen bekommen. Es gehört sicher zum Kalkül der New York Times, dass die Newsletter so neue Abonnenten an das Blatt heranführen sollen.

Die New York Times setzt aber nicht nur auf The Morning, sondern betreibt ein riesiges Angebot von knapp 70 Newslettern. Sie experimentiert gerne und viel und bringt zu aktuellen Themen und Gegebenheiten schnell neue Newsletter an den Start. Im Mai, als die Corona-Pandemie in New York den ersten Höhepunkt erlebte und es am sichersten war, zu Hause zu bleiben, startete die Zeitung **At Home**, mit vielen Beiträgen, die man auch auf den Kultur- und Gesellschaftsseiten einer Zeitung erwartet: Buch-, Serien-, Film- und andere Empfehlungen, Koch- und ganz generell Tipps, um das Zusammenleben im Lockdown angenehmer zu gestalten. At Home erzählt die Geschichten aber aus einer persönlicheren Perspektive, als man sie sonst von Zeitungen erwarten würde. Und das kommt offenbar an: At Home hat mittlerweile einen festen Platz auf der Startseite der Zeitung und auch in The Morning (Briefing).

## Plattformen und Apps

Der Erfolg mancher Webdienste ist ohne einen Newsletter schwer vorstellbar. Auf der US-Website **Product Hunt** zum Beispiel können Benutzer neue Produkte teilen, entdecken – und darüber abstimmen. Täglich veröffentlicht der Dienst eine Bestenliste der am häufigsten positiv bewerteten Produkte. Per Newsletter verbreitet Product Hunt täglich die am besten bewerteten Produkte, heizt so den Wettbewerb ständig an und zieht seine Nutzer regelmäßig auf die eigene Webseite.

Andere Newsletter wiederum existieren als eigenes Angebot oder bilden selbst den Mittelpunkt einer journalistischen Plattform. Das eingangs vorgestellte **the Hustle** ist ein Beispiel dafür. Neben dem Newsletter veröffentlicht Parr auch zwei Podcasts und ein geschlossenes Business-Netzwerk, Trends. Die Teilnahme an Trends kostet 299 US-Dollar pro Jahr.

**Morning Brew**, ein werbefinanzierter Business-Newsletter, hat mehr als eine Million Abonnenten. Das Team besteht

mittlerweile aus 29 Personen und bringt weitere Newsletter zu den Themen Retail, Tech und Quarantine sowie einen Podcast heraus. Bei **theSkimm** ist schon die Kernzielgruppe, junge Frauen aus Großstädten, bemerkenswert. Die letzte, 2018 veröffentlichte Abonnentinnenzahl liegt bei über 7 Millionen. Längst gibt es auch Apps sowie Facebook- und andere Social-Media-Kanäle von theSkimm. Das wichtigste Medium ist aber nach wie vor der Newsletter.

## Newsletter-Pressen

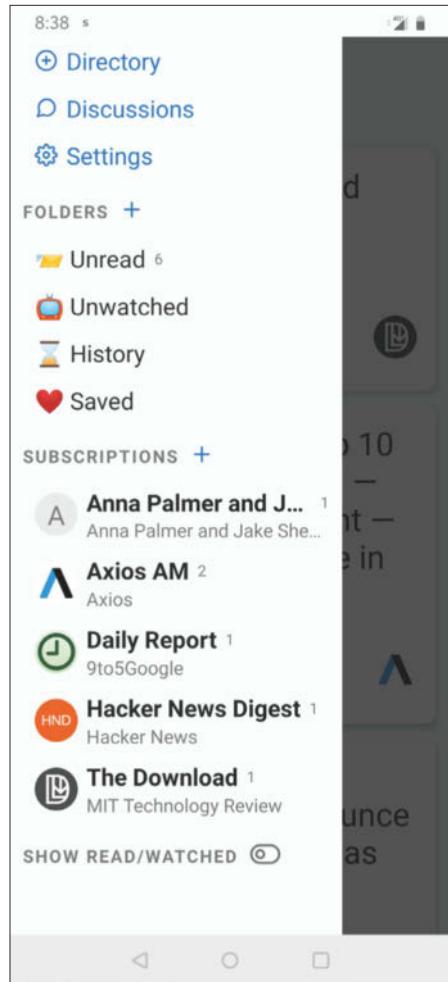
Der Newsletter-Trend wird auch durch Plattformen vorangetrieben, die es jedermann einfach machen, eigene Rundmails zu publizieren. Lange Zeit war **TinyLetter** die führende Plattform. Beim bereits 2010 gegründeten und später vom E-Mail-Dienstleister MailChimp übernommenen Anbieter kann jeder kostenlos Newsletter mit bis zu 5000 Abonnenten veröffentlichen.

Heute gibt es **TinyLetter** immer noch, aber es spielt eine kleinere Rolle. Das hat mit **Substack** zu tun. Substack ist 2017 an den Start gegangen, und es brachte ein wichtiges Alleinstellungsmerkmal mit sich. Autoren können auf der Plattform ihre Newsletter monetarisieren, sprich: sich ihre Arbeit bezahlen lassen. Das gibt Spezialisten mit Nischenthemen die Chance, sich mit ihrem Publikum zu vernetzen – und auf diese Weise Geld zu verdienen: Für Lindsay Gibbs' Newsletter **Power Plays** über Sexismus im Sport sind mehr als 1000 Abonnenten bereit, 72 US-Dollar pro Jahr zu bezahlen.

Mehr als 100.000 Menschen, so meldete Substack kürzlich, bezahlen auf der Plattform für Newsletter. Substack behält zehn Prozent der Abgebühren ein. Insgesamt soll es „tausende“ Newsletter auf der Plattform geben, auch kostenlose. Neben Substack bedienen noch weitere Dienstleister den Markt der (monetarisierbaren) Klein-Newsletter, darunter **ButtonDown** und **Revue**.

## Verzeichnisse und Reader

Apropos Revue: Der Dienst betreibt mit **Discover** ein Verzeichnis englischsprachiger Newsletter mit Suchmaschine. Es hat sich auf „editorial newsletters“ spezialisiert, Newsletter, die von Autoren herausgebracht werden, welche bestimmte Nischenthemen im Detail behandeln. Dabei berücksichtigt das Verzeichnis nicht nur bei Revue selbst gehostete Newsletter – ein



Der Reader Stoop hilft, das normale Postfach frei von Newslettern zu halten.

guter Startpunkt, um sich über spezialisierte Newsletter aus dem englischsprachigen Raum zu informieren.

Es gibt auch eigene Reader-Apps für Newsletter, das für Android und iOS verfügbare **Stoop** zum Beispiel. Wer die App einrichtet, erhält eine eigene E-Mail-Adresse unter der Domain [stoopinbox.com](http://stoopinbox.com). Praktisch: So kann man problemlos Dutzende Newsletter abonnieren, ohne befürchten zu müssen, dass das normale Postfach von Newslettern überschwemmt wird.

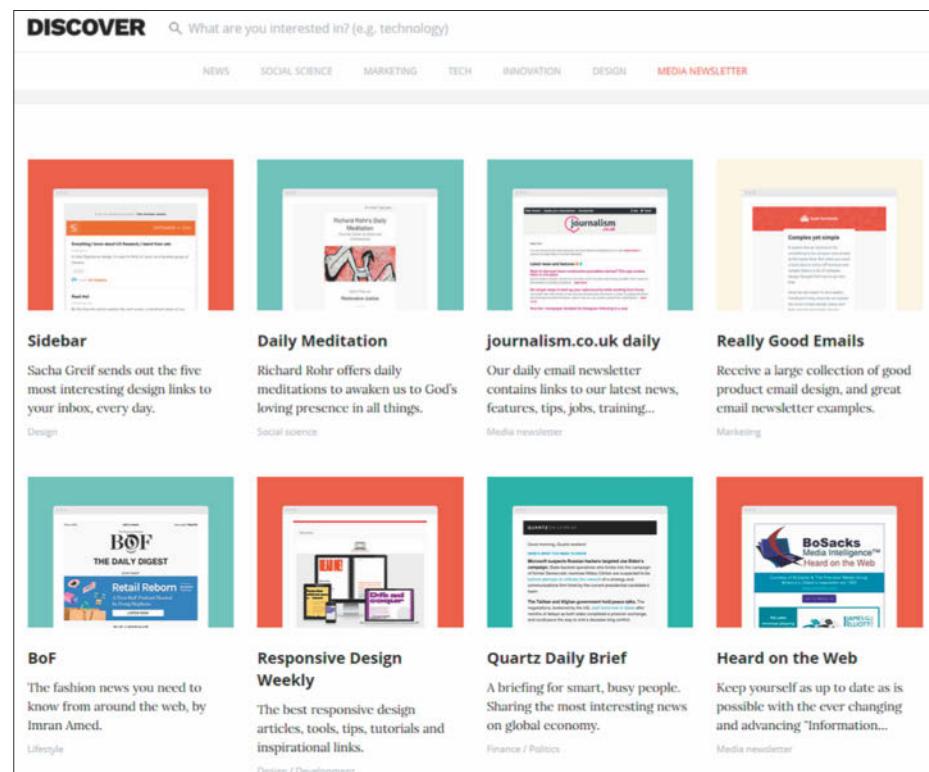
Im integrierten Verzeichnis findet der Nutzer eine Vorauswahl hunderter englischsprachiger Newsletter zu den verschiedensten Themen. Will er einen abonnieren, sendet ihn die App zur Subskriptionsseite und trägt in vielen Fällen gleich die Mailadresse ein. Die eintreffenden Mails versammelt die App unter einer schicken Oberfläche. **Slick Inbox** (Android und iOS) sowie **Meco** für iOS funktionieren ähnlich.

Wer dagegen keine neue App für Newsletter installieren will, sondern seine News gerne per RSS-Reader konsumiert, der findet in **Kill the Newsletter!** das Hilfsmittel dazu. Der kostenlose Dienst erzeugt für jede Newsletter-Anmeldung eine individuelle E-Mail-Adresse, sammelt anschließend die eintrudelnden Nachrichten ein und stellt sie als RSS-Feed zur Verfügung. Wer RSS per Feedly konsumiert, benötigt Kill the Newsletter! nicht mehr. Der RSS-Dienst kann seit dem September Newsletter ähnlich wie Stoop einsammeln.

## Stilbildend

Schlankes Layout, kein unnötiger Schnickschnack, gut erfassbare Inhalte, persönliche Ansprache: Das sind alles Zutaten, die nicht nur Newsletter aufwerten, sondern ganz grundsätzlich publizistische Praxis vieler Sites sein sollten und sind: So betreibt The Verge zum Beispiel eine eigene TL;DR-Seite, die Nachrichten auf eine Zeile herunterbricht.

An manchen Stellen erweckt es sogar fast den Anschein, dass sich Websites das Newslettern zugrunde liegende Design zum Vorbild genommen haben. Fast schon prototypisch etwa setzt die US-amerikanische Website Axios die Newsletter-Prinzipien um. Die Startseite enthält nicht viel mehr als eine Spalte mit kurzen Teasern zu den neuesten Meldungen: Autor, Überschrift, ein, zwei kurze Absätze. Der Link auf den gesamten Artikel



The screenshot shows the Discover platform interface. At the top, there's a search bar with the placeholder "What are you interested in? (e.g. technology)". Below the search bar is a navigation bar with links: NEWS, SOCIAL SCIENCE, MARKETING, TECH, INNOVATION, DESIGN, and MEDIA NEWSLETTER. The main content area is divided into four columns, each featuring a different newsletter thumbnail and a brief description:

- Sidebar**: Sacha Greif sends out the five most interesting design links to your inbox, every day. (Design category)
- Daily Meditation**: Richard Rohr offers daily meditations to awaken us to God's loving presence in all things. (Social science category)
- journalism.co.uk daily**: Our daily email newsletter contains links to our latest news, features, tips, jobs, training... (Media newsletter category)
- Really Good Emails**: Receive a large collection of good product email design, and great email newsletter examples. (Marketing category)
- BoF**: The fashion news you need to know from around the web, by Imran Amed. (Lifestyle category)
- Responsive Design Weekly**: The best responsive design articles, tools, tips, tutorials and inspirational links. (Design / Development category)
- Quartz Daily Brief**: A briefing for smart, busy people. Sharing the most interesting news on global economy. (Finance / Politics category)
- Heard on the Web**: Keep yourself as up to date as is possible with the ever changing and advancing "Information...". (Media newsletter category)

**Discover** ist ein Verzeichnis von „editorial newsletters“, also Newslettern mit exklusiven Inhalten.

informiert, auf wie viele Minuten Lesezeit sich der Besucher einstellen muss.

## Hierzulande

Auch hierzulande gehören E-Mail-Newsletter zum normalen News-Sortiment großer Medienhäuser. Alleine die Süddeutsche bringt gut zwei Dutzend Newsletter heraus; kaum ein großes Medium, das kein Morning Briefing oder eine anders geartete Tageszusammenfassung anbietet.

Newsletter zu aktuellen Anlässen sind ebenfalls weit verbreitet. Viele deutsche Medien bringen regelmäßige Mail-Updates zur Corona-Krise und zur US-Wahl heraus. Das Zeit Magazin hat zusätzlich Mitte März den **Morgen-Newsletter** gestartet, um Kulturschaffenden eine Bühne zu bieten. Lokalblätter stellen ihre regionale Kompetenz mit Newslettern zu Veranstaltungen und Freizeittipps heraus, die Hannoversche Allgemeine Zeitung etwa mit **HAZ mal raus**.

Der Grimme-Preis-gekrönte **Checkpoint** des Berliner Tagesspiegels ist so erfolgreich, dass ihn die Zeitung ausgebaut hat. In eingeschränkter Form als **Checkpoint-Kurzstrecke** ist der Newsletter kostenlos. Die Vollversion mit exklusiven Inhalten kostet 6,99 Euro pro Monat oder 60 Euro pro Jahr.

Ein im März in Münster gestartetes journalistisches Projekt setzt sogar primär auf tägliche Newsletter, beziehungsweise „Briefe“, wie sie dort genannt werden. **RUMS** steht für „Rund um Münster“ und soll die journalistische Monokultur um die Stadt aufbrechen. Ein Abo kostet 8 Euro pro Monat.

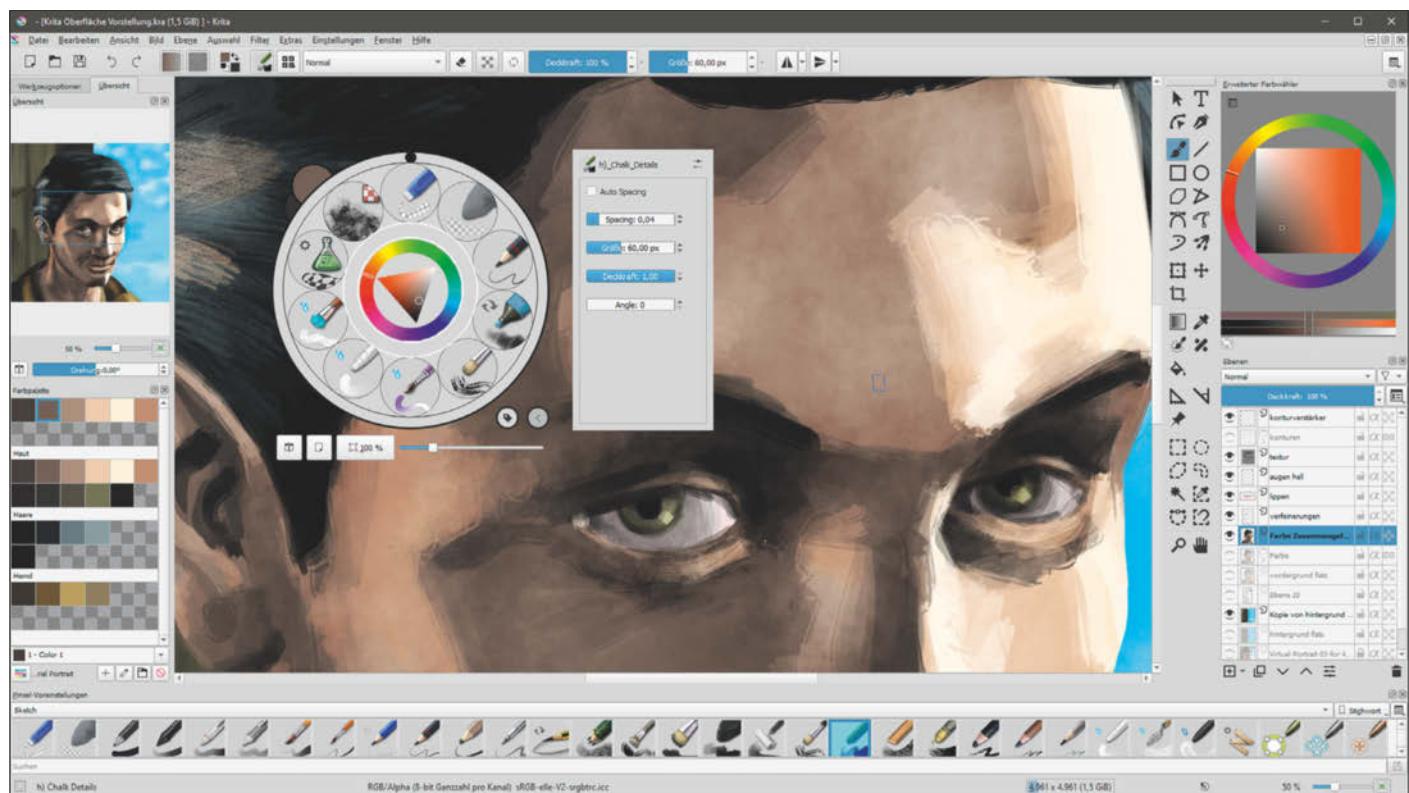
Und auch Klein-Newsletter von Einzelpersonen gibt es hierzulande, etwa das eingangs erwähnte Fever Pit'ch. Autor und re:publica-Mitgründer Johnny Haeusler bringt den Newsletter **Spreeblick** heraus. Und Fabian Reinbold, der Washington-Korrespondent von t-online.de, berichtet in seinem Newsletter **Post aus Washington** aus der US-amerikanischen Hauptstadt.

## Ausprobieren!

Alle erwähnten Newsletter und ein paar mehr finden Sie über [ct.de/yxu8](http://ct.de/yxu8). Entdecken Sie doch einfach mal das neue, alte Medium wieder. Das ist heute glücklicherweise möglich, ohne dass man sich einem erhöhten Spam-Risiko aussetzt – der DSGVO sei Dank. Ein Abonnement, das nicht zu einem passt, lässt sich auch schnell wieder kündigen.

(jo@ct.de) **ct**

**Links zu den Newslettern:** [ct.de/yxu8](http://ct.de/yxu8)



# Kreativ frei malen

## Einstieg in die Malsoftware Krita

**Das freie Malprogramm Krita kann in vielen Bereichen mit etablierten Größen wie Painter und SAI mithalten. Mit ein paar Wegweisern finden sich auch Einsteiger schnell zurecht.**

Von Gerald Himmlein

**S** seit sich die Open-Source-Anwendung Krita von einer Bildbearbeitungssoftware in Richtung kreative Malerei umorientiert hat, holt sie schrittweise zu etablierten Größen wie Painter und Paint Tool SAI auf. In der Open-Source-Welt hat Krita längst seinen eigenen Platz an der Seite der Bildbearbeitungssoftware Gimp und dem Vektorgrafikprogramm Inkscape gefunden.

Da Krita intern SVG-Vektoren verarbeitet, lassen sich viele Vektorformen verlustfrei zwischen Inkscape und Krita hin- und herköpfen. Neben Text und geometrischen Formen bietet Krita auch ein Freihandwerkzeug, das sowohl Druck als auch Neigung von Grafiktablett-Stiften auswerten kann.

Für Animationen stellt Krita eine eigene Animations-Palette, eine Timeline sowie bunte Onion Skins bereit – letztere mit bis zu 10 Instanzen in beide Richtungen. Was fehlt, ist eine Errechnung von Zwischenframes (Tweening). Diese Funktion ist zwar eingeplant, aber noch ohne Termin.

Kritas Oberfläche sieht aus wie eine Mischung aus OpenCanvas, Painter, Photoshop und SAI. An Painter erinnert insbesondere die Unterteilung der Werkzeuge in eigene „Pinsel-Engines“. Die Komplexität der Werkzeuge bleibt zwar deutlich hinter den Pendants in Painter zurück, dafür sind sie einfacher zu handhaben und anzupas-

sen. Wie alle ernst zu nehmenden Malprogramme ist Krita darauf ausgelegt, mit einem Grafiktablett oder einem Stifttablett bedient zu werden. Arbeiten mit einer Maus ist zwar möglich, aber mühselig.

### Neue Funktionen

Das für diese Tage angekündigte Krita 4.4 erscheint zu spät für unseren Test, der sich auf die zu Redaktionsschluss aktuelle Version 4.3 bezieht. In dieser erweitert Krita den Funktionsumfang um Wasserfarben-Malwerkzeuge und die Möglichkeit, die Farbauswahl mit vordefinierten Masken auf ausgewählte Bereiche einzuschränken.

Die Arbeitsfläche lässt sich jetzt vom Rest der Programmoberfläche abtrennen, um sie etwa auf ein Stift-Tablet auszulagern (Menü „Ansicht/Detach Canvas“). Der Snapshot-Docker kann Zwischenstadien eines Motivs speichern, damit man unkompliziert zu früheren Versionen des Motivs zurückkehren kann.

Das neue magnetische Lasso erleichtert die Auswahl entlang klar definierter Ränder („Magnetic Selection Tool“) und der Zauberstab („Zusammenhängenden Bereich auswählen“) erkennt Bereiche jetzt auch ebenenübergreifend.

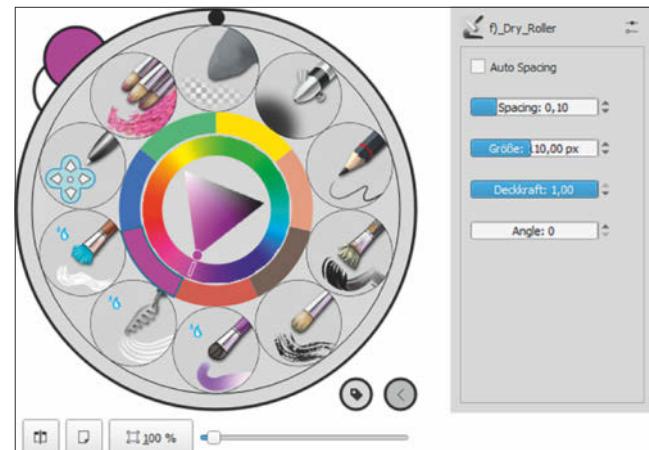
## Krita kennenlernen

Krita besitzt eine relativ konventionelle Programmoberfläche mit Menüs und andockbaren Paletten. Alle Paletten können entweder frei schweben oder an den Rändern des Hauptfensters einrasten. Insgesamt stehen 33 andockbare Dialoge zur Auswahl. Die Tabulator-Taste blendet alle Dialoge auf einen Schlag ein beziehungsweise aus.

Über „Fenster/Arbeitsbereich“ lassen sich vorgegebene Arbeitsbereiche auswählen, die auf bestimmte Aufgaben optimiert wurden. „Einstellungen/Andockbare Dialoge“ bietet die Möglichkeit, Schwebefenster einzeln aus- und abzuwählen. Der im Titelbild gezeigten Oberfläche liegt der Arbeitsbereich „Default“ zugrunde, mit den zusätzlichen Schwebefenstern Farbpalette und Übersicht am linken Rand und unten der Pinselauswahl („Pinsel-Voreinstellungen“).

Im gezeigten Layout der Oberfläche passen alle relevanten Elemente auf ein Full-HD-Display. Wesentlich bequemer ist die Handhabung von Krita jedoch auf einem Multimonitorsystem – mit der Ar-

**Das mit der rechten Maustaste aktivierte HUD bietet schnellen Zugriff auf Farben und Pinsel.**



beitsfläche auf einem Display und den Paletten auf dem anderen.

Das Verschieben der Dialoge ist in Krita etwas fummelig. Um den Werkzeugkasten vom linken an den rechten Fensterrand zu verschieben, muss man erst den Werkzeugkasten rechts neben einer der dort angedockten Paletten platzieren. Der Werkzeugkasten hat zunächst nur die Höhe der benachbarten Palette. Anschließend muss man die anderen Paletten unter diese neu positionieren. Um zu verhindern, dass ein Schwebedialog an anderen Paletten oder am Fensterrand einrastet, muss man vor dem Verschieben die Strg-Taste drücken.

Ein Rechtsklick auf die Arbeitsfläche öffnet das kreisförmige Head-up-Display (HUD). Das HUD ist die Geheimwaffe von Krita, um die Bedienung zu beschleunigen, da wichtige Werkzeuge und Einstellungen gleich zur Hand sind. Von innen nach außen zeigt es einen Farbwähler, die letzten zwölf verwendeten Farben, die ersten zehn Pinsel der aktiven Werkzeugfamilie, einen Ring zum Drehen der Arbeitsfläche sowie die aktive Vordergrund- und Hintergrundfarbe. Unter den Ringen liegen Tools zum Spiegeln der Ansicht, zum Ausblenden der Paletten, Zoom-Werkzeuge, ein Knopf zur Auswahl der Pinselfamilie und eine Schaltfläche, um

## Zusätzliche Pinsel

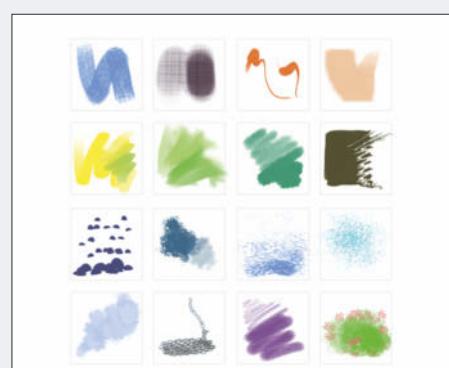
Krita stellt einen ordentlichen Grundstock an Pinseln bereit, der aber weit hinter dem Umfang der Pinselbibliotheken anderer Malprogramme zurückbleibt. Der Gedanke dahinter ist wohl, Anwender zu motivieren, auf Basis des Lieferumfangs eigene Lieblingswerkzeuge zu erstellen.

Auch wenn der Pinseleditor von Krita lang nicht so komplex ist wie etwa die überbordende Palettenorgie von Corel Painter, werden sich Einsteiger zunächst etwas überfordert fühlen. Dankenswerterweise führt die Krita-Dokumentation unter „Resources“ diverse Pinsel-Presets erfahrener Anwender auf (siehe ct.de/y91q). Weitere Pinsel finden sich im Krita-Forum krita-artists.org unter „Tutorials & Resources“. Darüber hinaus kann Krita auch Photoshop-Pinsel laden, sofern sie im ABR-Format vorliegen.

Einige Krita-Bundles sind stark spezialisiert, etwa die Filtereffekte von Woltnera oder das „Concept art“-Pack von Pyteo. Wer Bob Ross schätzt, wird die Landschaftspinsel von IForce73 lieben.

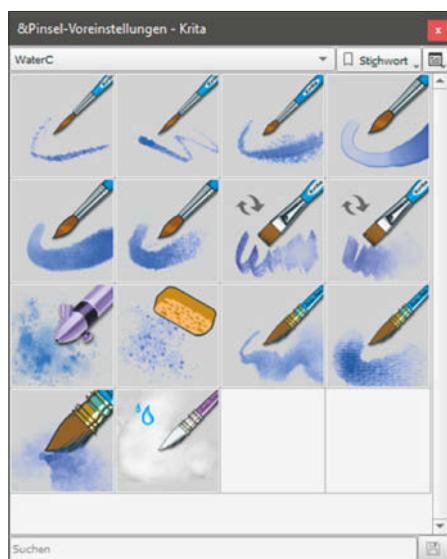
Pinselpakete werden meist als „bundle“ bereitgestellt, die eventuell noch einmal gezippt wurden. Die Bundles lädt man erst im Browser herunter, um sie dann in Krita über „Einstellungen/Ressourcen verwalten“ zu importieren. Es öffnet sich ein englischsprachiger Dialog, in dem die Schaltfläche „Import Bundles“ zum „Datei öffnen“-Dialog des Betriebssystems führt. Navigieren Sie von hier aus zum Download-Ordner und wählen Sie ein oder mehrere Bundles aus.

Über die Pfeilknöpfe zwischen den Unterfenstern „Active Bundles“ und „Inactive Bundles“ lassen sich Pinselpakete aktivieren und deaktivieren. Im unteren



**Erfahrene Krita-Anwender stellen zusätzliche Pinsel, wie hier eine Auswahl von GDQuest, kostenlos zum Download bereit.**

Bereich des Fensters „Manage Resource Bundles“ lassen sich Bundles auch bearbeiten, um etwa nur einzelne Pinsel zu verwenden.



**Mit den passenden Stichwörtern wählt man schnell den gewünschten Pinsel aus. Pinsel lassen sich auch unter mehreren Stichwörtern ablegen.**

die Basis-Werkzeugeinstellungen auszuklappen.

Krita ist zwar eingedeutscht, die Lokalisierung hat aber diverse Lücken. Das führt dazu, dass in grundsätzlich deutschsprachigen Dialogen und Menüs plötzlich englische Texte vorkommen. Die Online-Dokumentation ist ausschließlich in englischer Sprache verfügbar.

Von sich aus legt Krita alle 15 Minuten ein Backup des bearbeiteten Bildes an. Stört dies bei großformatigen Motiven den Arbeitsfluss zu sehr, kann man das unter „Einstellungen/Krita einrichten/Allgemein/Dateiverarbeitung“ anpassen oder ausschalten. Bei der Gelegenheit kann man auch die Zahl der Rückgängig-Schritte vom Standardwert 30 auf 50 hochsetzen („Allgemein/Verschiedenes/Stapelgröße für Zurücknehmen“) – gerade wenn man viel strichelt, geht der Undo-Funktion anderenfalls zu früh die Puste aus.

Die Online-Dokumentation enthält Abschnitte, um Umsteigern von Photoshop und Paint Tool SAI bei der Orientierung zu helfen. Da sich viele Malprogramme eng an Photoshop orientieren, lohnt sich der zugehörige Abschnitt für fast alle Umsteiger.

## 15 Pinsel-Engines, unendliche Möglichkeiten

Der wesentliche Kern von Krita sind die 15 Pinsel-Engines. Jede davon arbeitet nach eigenen Prinzipien: Die Borsten-Engine

simuliert sich spreizende Pinsel, die Schraffur-Engine erzeugt Strichmuster und die Skizze-Engine erzeugt prozedurale Muster zwischen benachbarten Linien.

Über den Pinseleditor (Tastenkürzel: F5) lassen sich die Parameter jedes Pinsels bis ins Detail justieren; das HUD (Rechtsklick) stellt die wichtigsten Schieberegler bereit. Angepasste Pinsel lassen sich als neue Presets speichern. Die meisten Malwerkzeuge verwenden die Pixel-Engine, darunter sowohl die Radierer und Bleistifte als auch die Kreiden und Wasserfarben. Einige Malwerkzeuge kommen ihren realen Vorbildern schon recht nahe, andere sehen ziemlich künstlich aus. Online stehen diverse „Bundles“ mit zusätzlichen Pinsel-Presets bereit, darunter Spezialwerkzeuge für Gebüsch oder Wolken (siehe Kasten „Zusätzliche Pinsel“).

## Eine Kategorie für sich

Bevor es ans Malen geht, sei empfohlen, die Werkzeugpalette ein bisschen aufzuräumen. Die mitgelieferten Malwerkzeuge sind acht Stichwörtern wie „Erasers“ und „Sketch“ zugeordnet; zusätzlich gibt es das Stichwort „My Favorites“.

Auf den ersten Blick erscheinen die Stichwörter funktional identisch zu den in anderen Malprogrammen üblichen Kategorien. Der Ansatz mit den Stichwörtern hat jedoch einen entscheidenden Vorteil: In Painter & Co. kann ein Malwerkzeug nur zu einer Kategorie gehören. Krita-Malwerkzeuge lassen sich problemlos auch mehreren Stichwörtern zuordnen – oder gar keinem.

Die in Version 4.3 hinzugekommenen Wasserfarben-Presets geben eine gute Gelegenheit, das Potenzial der Stichwörter zu verdeutlichen: Sie sind im Auslieferungszustand nämlich noch keinem Stichwort zugeordnet. Das können Sie gleich ändern. Hierfür klicken Sie in den Pinsel-Voreinstellungen mit der rechten Maustaste auf einen der „WaterC“-Pinsel und öffnen im Kontextmenü den Eintrag „Diesem Stichwort zuweisen“. Tippen Sie in das Eingabefeld am Ende des Auswahldialogs „WaterC“ ein und klicken Sie auf den „+“-Button.

Weisen Sie jetzt über denselben Dialog nacheinander allen anderen Wasserfarbenpinseln das Stichwort „WaterC“ zu. Wenn Sie in den Pinsel-Voreinstellungen aus der Dropdown-Liste anschließend das Stichwort „WaterC“ auswählen, zeigt Krita nur noch die Wasserfarbenwerkzeuge an.

Spielen Sie ein bisschen mit den Wasserfarbenpinseln herum, bis Sie einen gefunden haben, der Ihnen besonders zusagt. Rechtsklicken Sie dann auf das Pinsel-Preset und weisen Sie ihm über „Diesem Stichwort zuweisen“ den Eintrag „My Favorites“ zu. Ab sofort taucht das Werkzeug sowohl unter „My Favorites“ als auch unter „WaterC“ auf.

So lassen sich mit Stichwörtern leicht projektbezogene Werkzeugsammlungen anlegen: Ordnen Sie jeden Pinsel, den Sie in einem Motiv verwenden, einem passenden Stichwort zu (z. B. „Portrait“, „Comic“ oder „Landschaft“), dann sind dieselben Malwerkzeuge beim nächsten Projekt ähnlicher Art sofort wieder parat.

## Pinsel anpassen

Abgesehen vom Pinseleditor und dem Ausklappbereich des HUD bietet Krita mehrere Möglichkeiten zur direkten Anpassung grundsätzlicher Pinselparameter: Die Strichgröße verändert man über einen Schieberegler in der Symbolleiste oder zieht die Maus oder den Stift bei gedrückter Umschalttaste nach rechts oder links. Die Deckkraft des aktiven Werkzeugs lässt sich mittels Schieberegler oder Tastenkürzeln (O und I) justieren. Nach einem Rechtsklick auf den Regler lassen sich auch exakte Werte eingeben.

Wer die Strichstärke einiger Pinsel stark vergrößert, mag feststellen, dass sich die Striche zu einem fleckigen Stempelmuster auflösen. In diesem Fall ist eine Vergrößerung des Parameters „Abstand“ im Pinseleditor nötig.

## Fazit

Mit seinen Animations- und Vektorfähigkeiten hebt sich Krita von der Konkurrenz ab. Funktional bleibt das Programm allenfalls hinter dem japanischen Clip Studio Paint (ehemals Manga Studio) zurück. Der nachfolgende Artikel beleuchtet die Möglichkeiten von Krita im Rahmen eines konkreten Projekts: einem Porträtbild.

(ktn@ct.de) **ct**

**Krita-Dokumentation und zusätzliche Pinsel:** [ct.de/y91q](http://ct.de/y91q)

## Krita 4.3

Malsoftware	
Hersteller	Krita Foundation, <a href="http://www.krita.org">www.krita.org</a>
Systeme	Linux, macOS, Windows
Preis	kostenlos (Download, FlatHub, Snap-Store), 9,79 € (Microsoft Store), 9,99 € (Steam)
Lizenz	Open Source (GPL v3)

NEU

# Das ultimative Kompendium für Mac-User!

Auch als PDF sofort zum Download!



NEU

## Mac & i Special

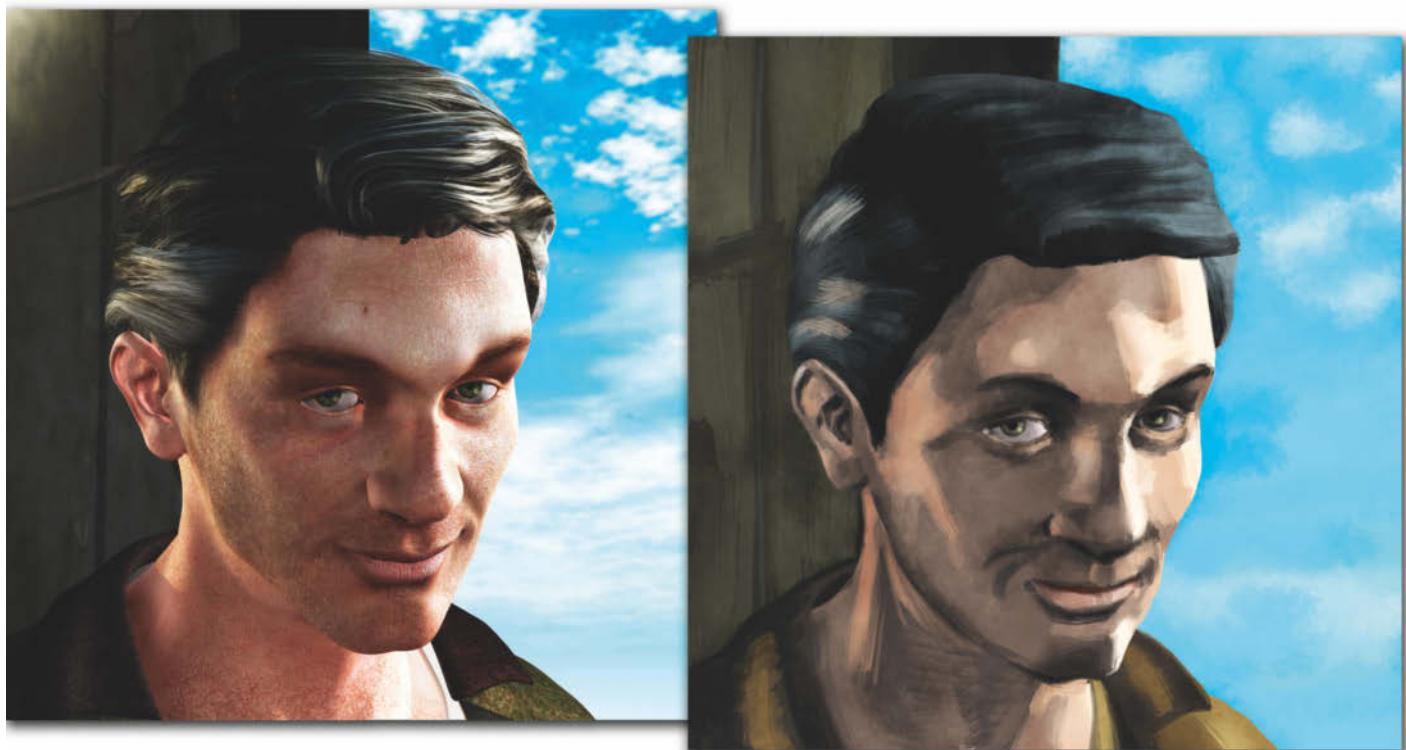
Ist der Mac Ihr Arbeitsgerät Nr. 1? Dann wird es höchste Zeit, macOS individuell an Ihre Arbeitsweise anzupassen und mittels Tools und Apps um vermisste Funktionen zu erweitern. In diesem Mac & i-Sonderheft lesen Sie wie's geht. Außerdem liefern aktualisierte Artikel der letzten drei Jahre 370 Tipps zum Finder, zu Systemprogrammen wie Fotos, Kontakte, Erinnerungen, Nachrichten, Musik/iTunes und Terminal sowie zu Apples Office-App Pages. Dieses Heft ist ein Muss für jeden Mac-User!

[shop.heise.de/mactipps20](http://shop.heise.de/mactipps20)

Einzelheft  
für nur

12,90 € >





# Gesicht zeigen

## Malen lernen mit Krita 4.3

**Das Open-Source-Malprogramm Krita bietet viel, ist für Einsteiger aber etwas unübersichtlich. Am besten lernt man die Software kennen, indem man sich eine konkrete Aufgabe stellt. Ein Porträt ist da ein dankbares Beispiel: Das Motiv ist überschaubar und stellt nicht viele Fallen. Ein paar digitale Abkürzungen sparen viel Zeit – Traditionalisten mögen die Stirn runzeln, aber letztlich haben die großen Meister auch alle Mittel benutzt, die ihnen zur Verfügung standen.**

Von Gerald Himmeltein

Porträts gelingen am einfachsten, wenn die Vorlage zum Durchpausen starke Kontraste und somit klare Konturen bietet. Gefragt sind also ein starkes Licht von einer Seite und eine schwächere Lichtquelle aus der Gegenrichtung, die den Schattenbereich aufhellt. Das Motiv sollte nur aus Kopf, Hals und vielleicht noch den Schultern bestehen. Am besten ist eine Aufnahme in Dreiviertelansicht: Bei frontalen Porträts sieht die natürliche Asymmetrie des Gesichts oft „krumm“ aus, obwohl das Bild die Vorlage akkurat wiedergibt. Wer kein Fotostudio im Keller hat, der fotografiert das Porträt am besten bei gutem Wetter im Freien neben einer hellen Wand: Die Sonne spendiert das Hauptlicht, die Wand spielt Reflektor.

Um Probleme mit Persönlichkeitsrechten zu umschiffen, benutzt dieses Tutorial einen virtuellen Kopf als Modell. Instagram-freundlich ist das Porträt bereits quadratisch zugeschnitten; dement-

sprechend verwendet auch das Tutorial eine quadratische Arbeitsfläche (21 cm × 21 cm bei 600 dpi, also 4961 × 4961 Pixel). Erzeugen Sie mit Strg+N eine neue Datei und tragen Sie die gewünschten Dimensionen ein. Das Farbmodell belassen Sie auf „RGB/Alpha“.

Zum digitalen Malen brauchen Sie ein Grafiktablett oder ein Stifttablett (auch als Pen Tablet oder Pen Display bekannt). Mit der Maus lassen sich kaum gerade Striche ziehen, geschweige denn kontrollierte Kurven. Davon abgesehen greift dieses Tutorial ausschließlich auf den mit Krita 4.3 ausgelieferten Grundstock an Malwerkzeugen zurück.

Zuerst wird die Vorlage per Drag & Drop in die Arbeitsfläche gezogen. Über ein Menü fragt Krita nach, was mit dem Bild passieren soll; wählen Sie „Als Referenzbild einfügen“ und machen Sie das selbe noch einmal, wählen diesmal aber die Option „Als neue Ebene einfügen“.

Das erste Bild schwebt dauerhaft als Referenz für Farbwerte und Konturen über der Arbeitsfläche, das zweite dient zum Durchpausen. Schieben Sie zuerst die Referenzebene mit dem „Reference Images Tool“ aus dem Weg – das ist im Werkzeugkasten die Reißzwecke. Im nächsten Schritt wählen Sie in der Ebenen-Palette das importierte Bild aus und vergrößern es mit dem Transformieren-Tool (Bilderrahmen) bei gedrückter Umschalttaste, bis es die gesamte Arbeitsfläche ausfüllt. Probieren Sie ruhig aus, was ohne Umschalttaste passiert: Genau für so etwas gibt es die Rückgängig-Funktion.

### Konturen und Kontrastlinien nachziehen

Im nächsten Schritt werden die Konturen der Vorlage nachgezogen. Hierfür legen Sie eine neue Ebene über der Bildebene an. Öffnen Sie mit der rechten Maustaste die Eigenschaften der neuen Ebene und setzen deren Modus von „Normal“ auf „Multiplizieren“. Dieser Modus stellt sicher, dass die Striche auf jeden Fall sichtbar bleiben. Andernfalls kann es vorkommen, dass sich etwa rote Linien nicht ausreichend von der Fotovorlage abheben. Ist das Foto sehr kontrastreich, kann es helfen, die Deckkraft der Vorlage auf 75 Prozent zu reduzieren.

Im Beispiel wurden die Konturen mit dem „Pencil-2“ mit einer Strichstärke von 50 Pixeln und dunkelgrauer Farbe nachgezogen – grundsätzlich eignen sich auch andere Werkzeuge, etwa „Sketching-3 Leaky“ oder „Charcoal pencil large“. Die Strichstärke passen Sie entweder über den „Größe“-Regler in der Symbolleiste an oder über das HUD (Rechtsklick).

Konturen sind in diesem Kontext alle Bereiche, in denen starke Kontraste aufeinandertreffen, sowie die Ränder der Bildbestandteile, etwa der Rand des Gesichts vor dem Himmel oder der Hemdkragen.

Um die nachfolgende Arbeit etwas zu erleichtern, empfiehlt es sich, auch die Umrisse der dunklen und hellen Bereiche nachzuziehen, am besten auf zusätzlichen Ebenen. Umrahmen Sie die dunklen Bereiche mit kräftigem Rot und die hellen mit einem kräftigen Dunkelblau.

Abschließend zeichnen Sie auf einer weiteren Ebene in etwas hellerem Grau grob die Konturen des Hintergrunds nach. Das Ganze sollte nicht länger als eine Viertelstunde dauern.

Das war es dann aber auch mit dem Durchpausen: Ein Klick auf das Auge-Symbol



Zuerst werden die Konturen der Vorlage durchgezogen.

bol links neben dem Ebenennamen macht die Vorlage unsichtbar. Grundsätzlich ist das Motiv jetzt fertig – der restliche Prozess besteht nur noch daraus, diese Führungslinien passend auszumalen.

### Ordnung behalten

Ebenso wie bei analoger Malerei sollte man auch seine digitalen Anstrengungen etwas strukturieren. Das bedeutet erst einmal, den Ebenen sinnvolle Namen zuzuweisen (Konturen, Dunkel, Hell, Hintergrund) und sie zu gruppieren. Namen weisen Sie in Krita zu, indem Sie auf den Namen einer Ebene doppelklicken. Zum Gruppieren markieren Sie erst die oberste der gewünschten Ebenen, dann mit gedrückter Umschalttaste die unterste. Jetzt wählen Sie im Menü „Ebene/Gruppe/

Schnellgruppierung“ (Strg+G). Auch diese Gruppe sollte einen sprechenden Namen erhalten.

Eigentlich kann man die Ebene mit der Bildvorlage an dieser Stelle löschen. Die Erfahrung lehrt jedoch, dass es gelegentlich praktisch ist, noch einmal auf das Foto zurückzugreifen – etwa, wenn erst beim Ausarbeiten der hellen Bereiche deutlich wird, dass ein Bereich nicht oder unvollständig markiert wurde. Ohne Not sollten Sie das Foto aber nicht mehr einblenden: Jetzt kommt der kreative Teil.

### Flächen füllen

Kommerzielle Comics werden meist in Fließbandarbeit gezeichnet: Bleistiftzeichnung, Tusche, Farbgebung, Sprechblasen – üblicherweise führt jede dieser Aufgaben eine andere Person durch, vor allem aus Zeitgründen. Bei der Farbgebung gibt es zusätzlich zu den eigentlichen „Colorists“ noch „Flatter“, die Comic-Panels grob einfarbig vorfärbten. Diese Flächen benutzen die Colorists als Grundlage für Auswahlen, die sie mit dem Zauberstab (in Krita: „Zusammenhängenden Bereich auswählen“) aktivieren und mit komplexen Schattierungen füllen.

Diese Flats-Technik lässt sich auch für das Porträt einsetzen, als digitales Pendant zur klassischen Grundierung. Zuerst legen Sie dafür unterhalb der Gruppe mit den Konturen zwei weitere Ebenen an: „Hintergrund Flats“ und „Vordergrund Flats“.

Krita stellt zum Füllen von Flächen unter den Pinseln das extrem praktische

Farbige Linien markieren die hellen und dunklen Bereiche.





**Farbflächen trennen Haare, Haut, Augen und Hemd voneinander.**

Malwerkzeug „Shapes Fill“ bereit. Es erstellt Auswahlen und füllt sie sofort. So entfällt ein wesentlicher Schritt gegenüber der Flats-Methode in Photoshop (erst Auswahllasso, dann Füllfunktion).

Wichtig: Shapes Fill arbeitet normalerweise mit Kantenglättung. Die sollten Sie ausknipsen, damit die Übergänge sauber bleiben. Dazu klicken Sie im Pinsel-Editor (F5) unter „Allgemein“ auf „Experimentelle Einstellungen“ und aktivieren „Harte Kanten“. Gleichzeitig haben Sie so Ihr erstes Malwerkzeug angepasst. Drücken Sie die Escape-Taste, um den Pinsel-Editor zu schließen.

Die Flats müssen die finalen Farben des Motivs nicht widerspiegeln: Wichtig ist nur, dass sich die Bereiche farblich klar

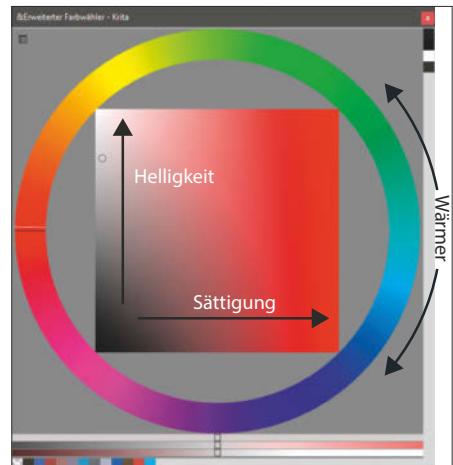
voneinander abheben. Beginnen Sie am besten mit dem Hintergrund, der im Beispiel aus zwei einfachen Farbflächen besteht. Dann nehmen Sie sich auf der Ebene „Vordergrund Flats“ die Elemente der Figur vor. Hier fangen Sie am besten mit den außen liegenden Bereichen an, die teilweise überlappt werden: also erst die Haut von Gesicht und Hals, dann das weiße Shirt, dann das Hemd und die Haare. Zum Schluss sind die Augen und die Pupillen dran.

Das Flatten gelingt am besten, wenn Sie mit unterschiedlichen Zoom-Stufen arbeiten: Die groben Bereiche lassen sich bequem in der Übersicht abdecken, die Konturen besser aus nächster Nähe nachziehen. Das Ganze ist zwar todlangweilig, sollte aber nicht länger als eine Viertelstunde dauern.

Wenn Sie an den Rändern der Figur über das Ziel hinausschießen, können Sie ein wunderschönes Krita-Feature verwenden: Die Taste „E“ versetzt jeden Pinsel in den Radiermodus. Mit Shapes Fill können Sie also auch Formen erzeugen, die Farbe abtragen.

### Farben wählen

Ist die Flats-Arbeit abgeschlossen, füllen Sie die Bereiche mit dem Füllungswerkzeug mit Grundfarben, die besser zum Motiv passen. Diese sollten möglichst nicht zu intensiv sein – das Hintergrund-Blau im Beispiel wäre für den Vordergrund viel zu dominant. Empfehlenswert sind blasses, mittlere Farbtöne: für die



### Das Farbwähler mit quadratischem Mittelfeld und seine Bedeutung

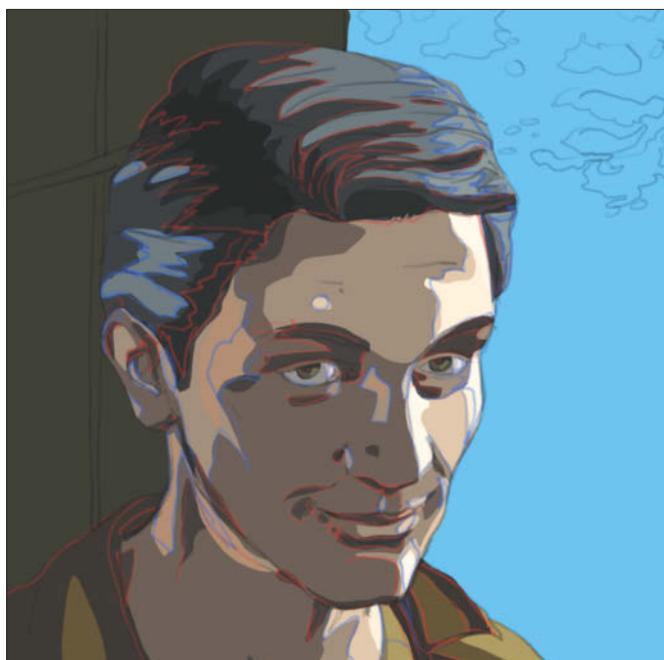
Haut ein blasses Rosa, für das Hemd ein mittleres Braun, für die Haare ein blasses Blau, für die Pupillen ein blasses Olivgrün. Im nächsten Schritt duplizieren Sie die Flats-Ebenen und ergänzen das Duplikat um helle und dunkle Farbtöne, die zur jeweiligen Grundfarbe passen. Das ist zugegebenermaßen nicht ganz einfach, deshalb erst ein kurzer Ausflug in die Theorie.

Welche Farbtöne Sie aussuchen, ist Geschmackssache. Für die abgedunkelten Bereiche eignen sich Farben, die dunkler, weniger gesättigt und kälter sind als der Flats-Mittelton. Für die Bereiche im Sonnenlicht empfehlen sich hellere, wärmere und eventuell etwas stärker gesättigte Farbtöne.

Für eine ordentliche Farbenlehre fehlt hier der Platz, deshalb nur ganz grob: Die „wärmste“ Farbe ist Rotorange, die „kälteste“ Farbe ist Türkis. In Krita gibt es eine große Auswahl an Farbwählern, die mit unterschiedlichen Modellen arbeiten. Klicken Sie auf das kleine Symbol oben links neben dem Farbwähler, um den Typ zu wechseln. Beim HSV-Farbwähler mit quadratischem Mittelfeld, bei dem Schwarz unten links liegt, lassen sich Ton, Sättigung und Helligkeit dank größerer Bereiche besonders bequem ansteuern.

Von Türkis aus führen im Farbring beider Richtungen zu wärmeren Farbtönen – welche besser passt, hängt ganz vom Motiv ab. Das quadratische Farbfeld im Ring dient zur Anpassung der Sättigung (links-rechts) und Helligkeit (unten-oben) der im Ring gewählten Grundfarbe.

Wenn Sie einen dunkleren, kälteren und weniger gesättigten Farbton brau-



**Die Flächen werden anhand der farbigen Linien verfeinert.**

chen, wählen Sie zuerst im Farbring einen kälteren Ton und klicken dann im Quadrat auf ein Feld, das tiefer und weiter links liegt als der Kreis, der Ihren bisherigen Farbton zeigt.

Wer sich mit Ring und Quadrat schwertut, der kann die drei darunterliegenden Schiebe-Regler ausprobieren: Der obere ändert den Farbwert, der mittlere die Sättigung und der untere die Helligkeit.

Zusätzlich bietet Krita die Möglichkeit, per Tastenbefehl zu passenden Farbtönen zu springen: K wählt einen dunkleren Ton, L einen helleren. Die Verschiebung zu einem wärmeren oder kälteren Farbton übernimmt die Automatik allerdings nicht.

### Schreiende Farben sind out

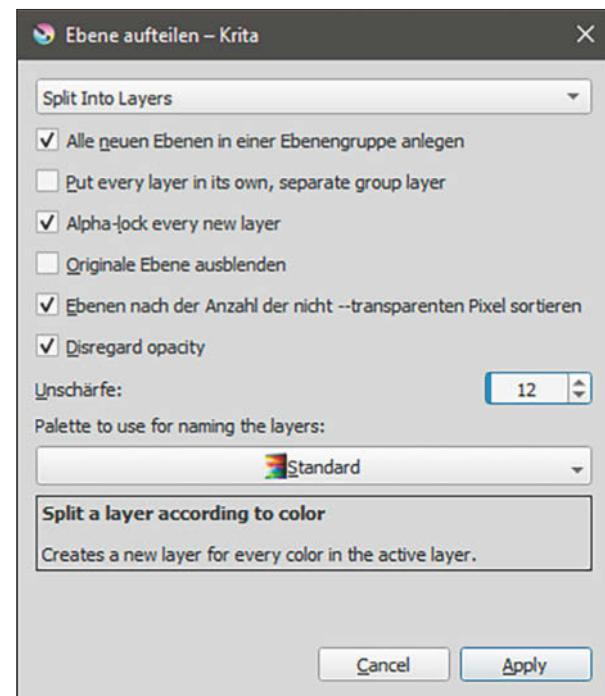
Bei den Mitteltönen können Sie es sich leicht machen, indem Sie diese mit dem Farbauswahlwerkzeug, auch als Pipette bekannt (P oder Strg+Mausklick), aus dem schwebenden Referenzbild extrahieren. Vorher sollten Sie den Radius des Werkzeugs über den Dialog „Werkzeugoptionen“ auf 10 bis 20 Pixel erweitern, um nicht immer wieder ausgerechnet das eine Pixel zu treffen, das die falsche Farbe besitzt. Bei den dunklen und hellen Tönen führt die Pipette nur selten zum Erfolg; hier ist Handarbeit angesagt.

Damit sich die Farben nicht gegenseitig zu übertönen versuchen, sollten Sie frühzeitig festlegen, welche Farben das Motiv dominieren sollen. Diese Vorgabe grenzt den Farbumfang ein. Anfänger erkennt man oft daran, dass sie von allen Farbtönen die sattesten Varianten einsetzen: Das Ergebnis schreit einen förmlich an. So etwas kann ein Stilmittel sein (siehe Keith Haring), wirkt aber meistens nur grell und irgendwie daneben.

Zuerst muss man also entscheiden, ob insgesamt eher kältere oder wärmere Farben dominieren sollen. Fällt die Entscheidung auf eine warme Farbpalette, bedeutet das, dass die kalten Farben nicht so stark gesättigt sein dürfen. Ein starkes Blau bedingt also ein blasses Gelb, ein intensives Gelb bedingt hingegen ein graues Blau.

Krita bietet als Hilfestellung die Palette „Gamut Masks“, die Sie über das Menü „Einstellungen/Andockbare Dialoge“ einblenden. Die Nutzung setzt allerdings einen Farbwähler mit kreisförmigem Mittelfeld voraus. Wechseln Sie also zuerst den Farbwähler und wählen Sie dann eine

**Krita separiert die Inhalte einer Ebene mit dem Werkzeug „Ebene aufteilen“ automatisch in verschiedene Ebenen.**



Gamut Mask, etwa „Dominant Hue With Accent“ oder „Split Complementary“. Über dem Farbwähler erscheint ein Regler „Drehung“, um die bevorzugten Bereiche freizulegen. Wichtig: Wenn Sie sich einmal für einen Farbbereich entschieden haben, sollten Sie die Maske nicht mehr drehen – sich an die Maske zu halten ist ja Sinn der Sache. Das Ergebnis wirkt erst einmal etwas restriktiv, bietet aber eine gute Orientierung. Um gezielt Akzente mit Farben außerhalb der Maskenbereiche zu setzen, lässt sich die Maske an- und ausknipsen. Hierfür stellt der Farbwähler oben links den Knopf „Toggle gamut mask“ bereit.

Sofern man nicht gerade Comics zeichnet, sollte man absolutes Weiß eben-

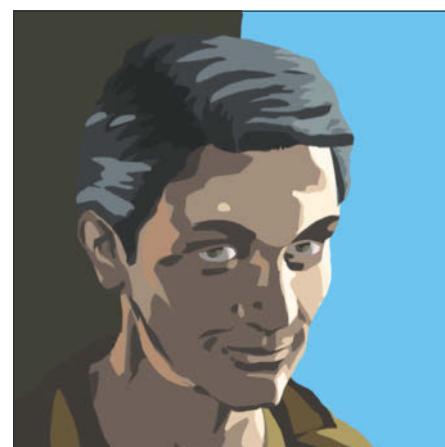
so vermeiden wie absolutes Schwarz: Von diesen Extremen aus gibt es keine Steigerung mehr, weißer als weiß gibt es nur in der Werbung. Schwarz und Weiß sollte man allenfalls mit Malwerkzeugen mit reduzierter Deckkraft einsetzen.

### Flats auftrennen

Momentan liegen alle Vordergrund-Flats auf derselben Ebene. Um die definierten Bereiche weiter zu verfeinern, teilen Sie diese auf separate Ebenen auf. Hierfür bietet Krita ein großartiges Werkzeug: „Ebene/Teilen/Ebene aufteilen...“ öffnet einen nicht ganz übersetzten Dialog. Markieren Sie darin die im obenstehenden Bild gezeigten beziehungsweise in der folgenden Liste aufgeführten Optionen:

- Split Into Layers
- Alle neuen Ebenen in einer Ebenengruppe anlegen
- Alpha-lock every new layer
- Ebenen nach der Anzahl der nicht-transparenten Pixel sortieren
- Disregard opacity
- Unschärfe: 12

Ein Klick auf „Apply“ und Krita geht ans Werk. Es entsteht eine Ebenengruppe mit einem Stapel an Ebenen, für jeden Farbbereich eine. Diese sollten Sie jetzt passend umbenennen, zum Beispiel in Haut, Haare, Augen, Pupillen oder Hemd. Klicken Sie bei der Gelegenheit rechts neben den Ebenennamen auf das Schachbrett-muster-Symbol, sodass darin ein Vorhang geschlossen erscheint. Das begrenzt alle



**Zwischenstand: die Farbbereiche ohne die Hilfslinien**



**Halbtransparente Pinsel geben dem Ganzen ein organisches Aussehen.**

weiteren Striche auf die jeweils eingefärbte Fläche.

### Früchte ernten, Frust schieben

Jetzt geht es an die Verfeinerung der Schattierungen. Das Beispielbild verwendet für die Haut sechs Schattierungen: zwei dunkle Farbtöne der Grundfarbe, zwei helle Schattierungen für die von der Sonne direkt beschienenen Bereiche, eine sehr helle Farbe für Glanzlichter und dann noch eine gesättigtere und wärmere Variante des Grundtons für die Bereiche, die das sekundäre Licht aufhellt. Ähnlich schattiert sind die Haare (vier Farbstufen), das Hemd (fünf Stufen), die Augen und die Pupillen (je drei Stufen).

Je nach Motiv können mehr oder weniger Schattierungsstufen nötig sein. Verteilen Sie diese Farbtöne anhand der blauen und roten Linien auf den Ebenen. Stellen Sie dazu die Konturengruppe auf 50 Prozent Deckkraft ein und setzen Sie mit Shapes Fill die gewünschten Farbakzente. Endlich ernten Sie die Früchte der vielen Vorbereitungen!

Der folgende Satz wird Sie womöglich frustrieren: Weder für die Wahl der Schattierungsstufen noch für deren Platzierung gibt es eine präzise Anleitung, weil das Vorgehen relativ ist. Das liest sich in einem Tutorial sehr unbefriedigend, aber manche Sachen gelingen nur mit Erfahrung beziehungsweise geduldigem Ausprobieren. Es ist nichts verkehrt daran, sich dem Ziel in mehreren Anläufen zu nähern: Probieren Sie erst unterschiedliche Mitteltöne aus, dann andere Töne für die Schattie-

rung. Speichern Sie das Bild immer mal wieder unter neuem Dateinamen ab, um keine Fortschritte zu verlieren. Krita bietet dafür die Funktion „Inkrementelle Version speichern“ (Strg+Alt+S) an, die dem Dateinamen eine Zahl hinzufügt und schrittweise bei jedem Speichern um eins hochzählt.

Orientieren Sie sich an den roten und blauen Linien und ziehen Sie an kniffligen Stellen das schwebende Referenzbild zu rate. In der Übersicht-Palette sehen Sie, ob das Ergebnis sich dem Ziel annähert. Knipsen Sie zwischendurch die Ebenengruppe mit den Konturlinien aus und ein, um sicherzugehen, dass Sie Fortschritte machen.

Es empfiehlt sich, mit einfachen Bereichen anzufangen (Hemd, Haare) und das Gesicht erst in Angriff zu nehmen, wenn Sie sich warm gearbeitet haben. Nicht verzagen, wenn das Ergebnis zwischendurch absolut schrecklich aussieht: Das ist ganz normal; im Bau befindliche Häuser sehen auch nicht gemütlich aus.

Bei jedem Porträt gibt es den Moment, in dem es total misslingen zu sein scheint. Entweder sieht die Person viel zu hässlich aus oder zu wenig nach sich selbst. Meistens fehlt dabei nur eine Schattierung an einer ausschlaggebenden Stelle. In solchen Momenten der Unsicherheit empfiehlt es sich, das Bild mit der Taste „M“ horizontal zu spiegeln (oder über „Ansicht/Leinwand/Spiegelansicht“) – das gibt einen neuen Blick auf das Motiv, der häufig offenbart, wo der Fehler liegt.

Korrekturen probieren Sie am besten auf einer neuen Ebene aus – da können Sie besser radieren (E) und Flächen verfeinern. Passt das Ergebnis, sollten Sie Korrektur- und Farbebene miteinander verschmelzen. Dazu klicken Sie in der Ebenenpalette mit gedrückter Umschalttaste beide Ebenen an und drücken Strg+E oder gehen über den Menüpunkt „Ebene/In untere Ebene einfügen“.

### Verfeinern, bis es passt

Zu diesem Zeitpunkt sollte das Bild dem Motiv schon ziemlich ähnlich sehen, zumindest in der Übersichts-Palette. Die harten Übergänge sehen zwar mehr nach Pop Art aus als nach Gemälde, aber das Gröbste ist geschafft.

Bevor es weitergeht, blenden Sie die Konturengruppe aus, duplizieren zur Sicherheit die Gruppe mit den Farbebenen und blenden das Original aus. Alle weiteren Arbeitsschritte finden auf den duplizierten Farbebenen statt, die Originale dienen als Backup.

Es gibt digitale Künstler, die Farbflächen mit „Blender“-Werkzeugen butterweich ineinanderfließen lassen. Das Ergebnis wirkt aber meistens glatt und erinnert an Airbrush-Kitsch. Für ein natürlicheres Ergebnis wählen Sie für die Übergänge stattdessen einen Pinsel mit reduzierter Deckkraft. Welche Pinsel Sie für die weitere Bearbeitung wählen, ist Geschmackssache.

Im Beispiel wurden die Farbbereiche zunächst mit der „Wet Bristles Brush“ zusammengeführt, mit Pinselgrößen zwischen 100 und 120 Pixeln. Zur Ausarbeitung der Haarsträhnen diente „Dry Brushing“. Hierbei kamen abwechselnd die



**Verfeinerungen auf separaten Ebenen geben dem Motiv den letzten Schliff.**

zuvor gewählten dunklen und hellen Farben zum Einsatz, bis das Ergebnis organisch aussah. Zur Verfeinerung der Hautbereiche kam durchgehend „Bristles-2 Flat Rough“ zum Einsatz, mit wechselnden Strichbreiten.

Ganz wichtig: Verzetteln Sie sich nicht in unnötigen Details! Niemand, außer vielleicht ein anderer Künstler, wird Sie dafür bewundern, wie formvollendet das Ohr abgebildet ist. Jeder sieht hingegen sofort, wenn die Kontur der Nase nicht stimmt oder der Mund schief sitzt. Der wichtigste Bereich sind aber die Augen: Hier kann ein Strich an der falschen Stelle alles verunstalten. Konzentrieren Sie sich also auf die wichtigen Bereiche des Porträts; die unwichtigen können ruhig skizzenhaft bleiben.

Für Korrekturen empfiehlt es sich auch hier, neue Ebenen anzulegen, um nicht versehentlich zu ruinieren, was man bisher geschafft hat. So mancher digitale Künstler hat fröhlich herumexperimentiert, bevor er erst feststellte, dass es nicht besser wurde, und dann, dass der Rückgängig-Verlauf nicht mehr weit genug zurückreichte, um den Schaden ungeschehen zu machen.

Das ist schließlich der große Vorteil digitaler Malerei gegenüber analoger Kunst: Das Digitale bietet die Freiheit, zu gucken, ob eine Anpassung das Motiv verbessert oder verschlimmert, und notfalls zu einem früheren Zustand zurückzukehren.

Davon abgesehen sei nachdrücklich empfohlen, die Datei vor jeder signifikanten Änderung unter einem neuen Namen abzuspeichern. Zählen Sie ruhig einfach durch: „Porträt 01“, „Porträt 02“, ... oder verwenden Sie das inkrementelle Speichern. Festplattenplatz ist billig, Nerven sind kostbar.

Blicken Sie auch in der Verfeinerungsphase immer mal wieder auf die Übersicht-Palette und spiegeln Sie gelegentlich das Motiv: Das entlarvt Schwachstellen sofort.

## Die letzten Handgriffe

Irgendwann werden Sie merken: Das Bild verändert sich noch, es wird aber nicht mehr besser. Sie sind fertig.

Womöglich sieht das Ergebnis noch etwas arg digital aus: Die Striche sind etwas zu glatt, die Farbe zu gleichförmig; es fehlt eine Körnung. Dem lässt sich relativ leicht abhelfen: Legen Sie eine neue Ebene über allen anderen Ebenen an,

**Eine überlagerte Textur lässt das Bild weniger digital aussehen.**



füllen Sie diese mit 50-prozentigem Grau („Bearbeiten/Mit Vordergrundfarbe füllen“) und setzen Sie den Ebenenmodus auf „Ineinanderkopieren“. Danach sollte alles wieder wie vorher aussehen – „Ineinanderkopieren“ wertet mittleres Grau als neutral aus.

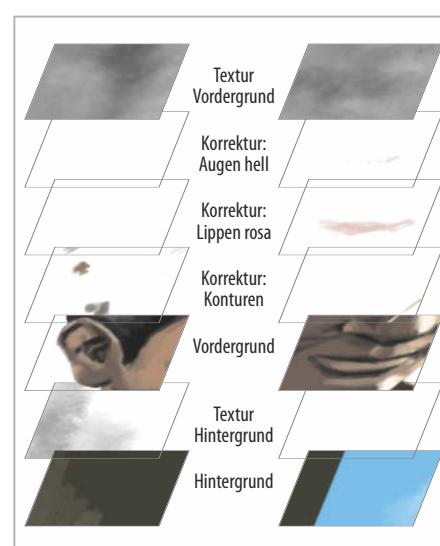
Nehmen Sie jetzt das Malwerkzeug „Texture Big“ und überlagern Sie das Motiv abwechselnd mit schwarzen und weißen Tupfern. Da, wo Sie mit Schwarz arbeiten, wird die Sättigung etwas zunehmen; mit Weiß bearbeitete Bereiche werden etwas blasser. Geschickt eingesetzt, lässt sich dem Motiv so etwas zusätzlicher Pepp verleihen.

Zum Schluss ist der Hintergrund dran. Bleiben Sie hier bei der Ausarbeitung ruhig vage, um nicht vom Vordergrund abzulenken.

Bei einigen Motiven fällt zum Schluss auf, dass immer noch etwas fehlt. Hier kann es helfen, mit wohlplatzierten Linien zusätzlichen Kontrast zu erzeugen. Nehmen Sie hierfür am besten einen Kohlestift oder eine Kreide, etwa „Charcoal pencil large“ oder „Chalk Details“, und wählen Sie für die Striche markante Akzentfarben – für Hautbereiche etwa ein dunkles, blasches Braun oder ein helles Beige. Wenn diese Striche zu stark dominieren, reduzieren Sie die Deckkraft der Ebene oder schwächen die Linien mit dem Radiergummi ab, bis Sie mit dem Ergebnis zufrieden sind.

Zum Abschluss noch ein paar Ratschläge für Leute, bei denen sich partout keine Zufriedenheit einstellen will: Oft hilft es, die Sache zu überschlafen und am Folgetag erneut anzugehen. Mit frischen Augen kommt man oft weiter, wo man am Vortag noch verzweifelt ist. Gelegentlich hilft auch längerer zeitlicher Abstand: Was heute noch misslungen wirkt, sieht zwei Wochen später plötzlich annehmbar, wenn nicht sogar verflucht gut aus. Und wenn's partout nicht gelingen will: Legen Sie den ersten Versuch beiseite und fangen Sie neu an. Jetzt wissen Sie ja, was beim letzten Mal schief lief, und werden das im zweiten Anlauf hinbekommen. Und dabei gewiss neue Fehler machen, daraus lernen und immer mehr Erfahrung sammeln.

(ktn@ct.de) ct



**Der Aufbau des fertigen Bildes: Vorsichtshalber finden alle Korrekturen auf separaten Ebenen statt.**

# Zahlen, Daten, Fakten

## Telefonie

Der altehrwürdige Telefondienst, im 18. Jahrhundert eingeführt, hat sich in den vergangenen 20 Jahren rasant gewandelt. Noch bis weit in die 10er-Jahre gab es ein eigenes physisches Telefonnetz. Das ist inzwischen abgeschaltet, VoIP hat das Rennen gemacht und bietet mit HD-Voice Hifi-Qualität beim Telefonieren.

Telefonie ist seitdem eine Internetanwendung unter vielen. Wo früher Staaten ihr Fernmeldemonopol verteidigten und Mitarbeiter der Bundespost Beamtenstatus genossen, herrscht inzwischen ein lebhafter Wettbewerb und ein heftiger Preisdruck.

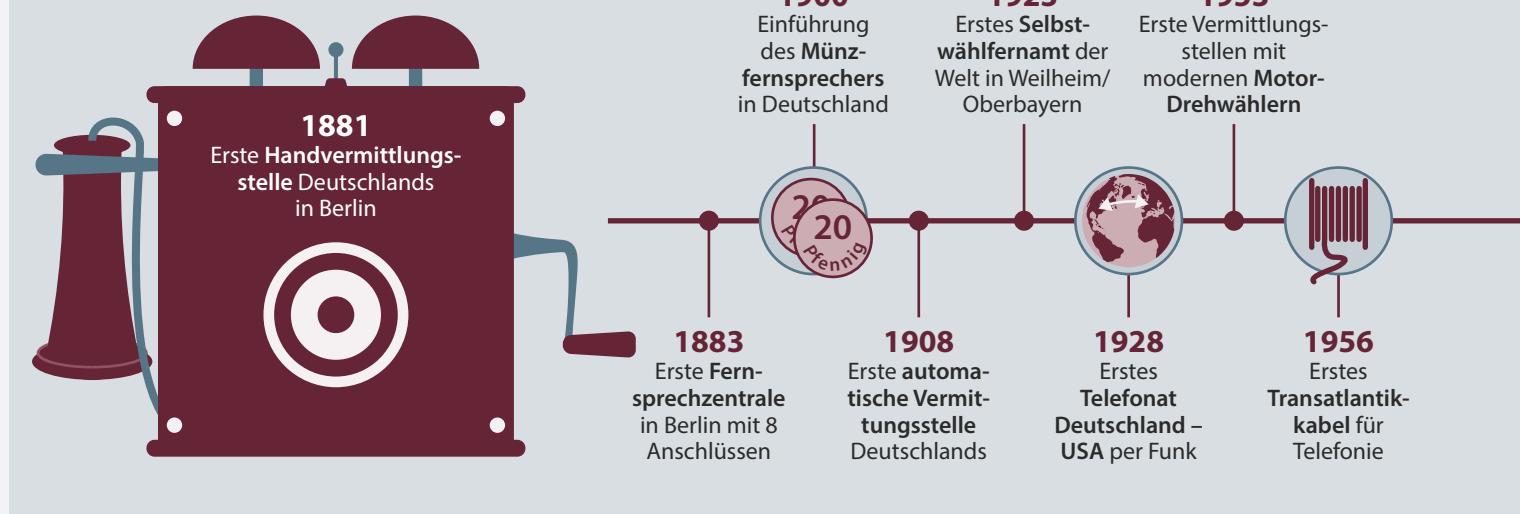
Mobilfunk ist durch billige Geräte und ständig fallende Preise zum globalen Mas-

senmarkt geworden und hat dem Festnetz schon lange den Rang abgelaufen, insbesondere in Entwicklungs- und Schwellenländern.

Das Festnetztelefon ist ein Auslaufmodell; telefoniert wird da, wo es gerade passt, also mobil und in Messengern auf dem Smartphone. (uma@ct.de) **ct**

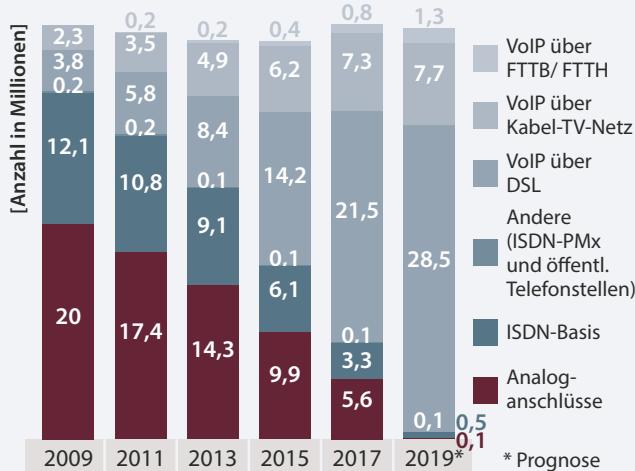
## ► Die Geschichte des Telefons

... Wichtige Meilensteine auf dem Weg vom Kurbeltelefon mit Handvermittlung zu modernen VoIP-Anlagen.<sup>1</sup>



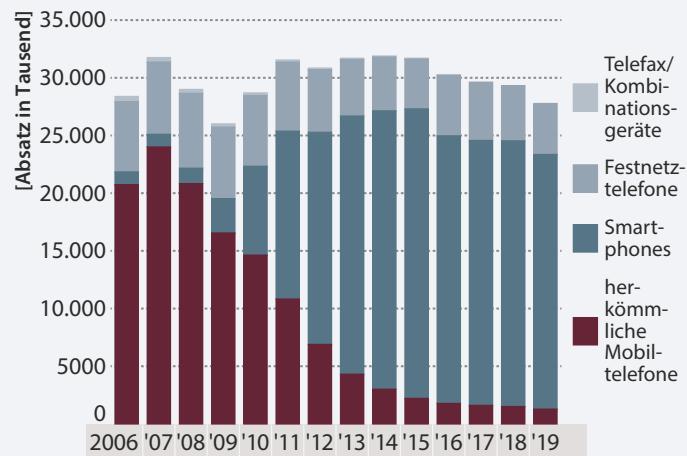
## ► Anschlussarten

... Klassische Festnetztelefonanschlüsse in Deutschland sind inzwischen fast komplett auf VoIP umgestellt.<sup>2</sup>



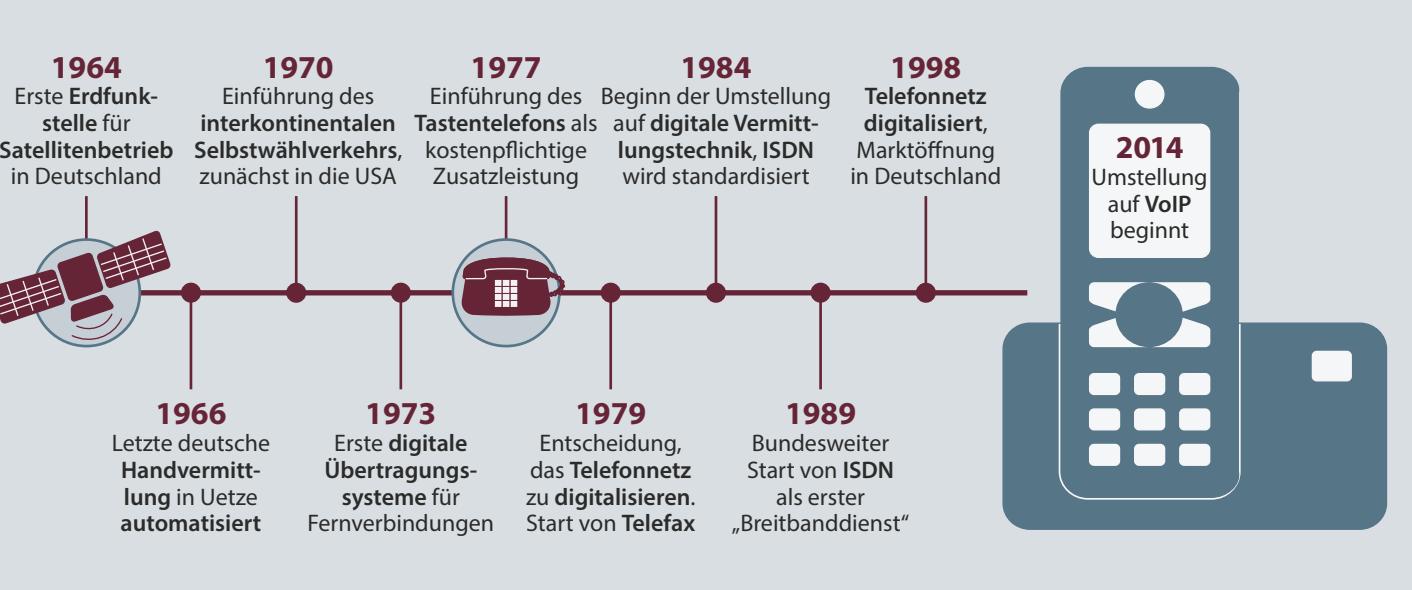
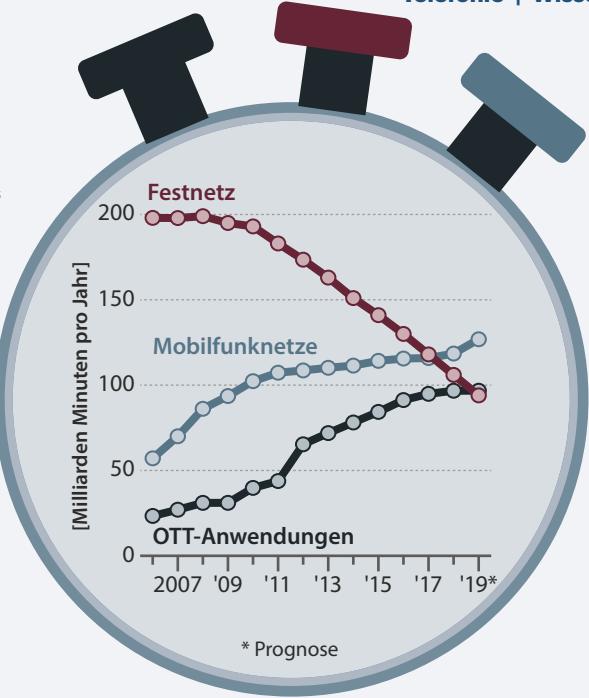
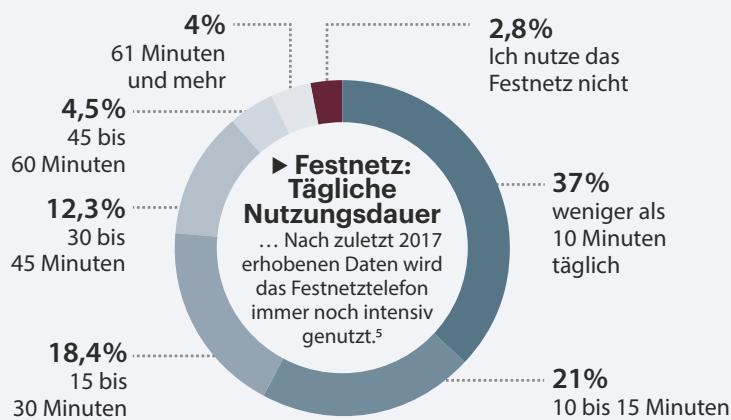
## ► Verkaufte Telefone

... Smartphones verdrängen konventionelle Mobilfunk- und Festnetztelefone zügig aus dem Markt.<sup>3</sup>



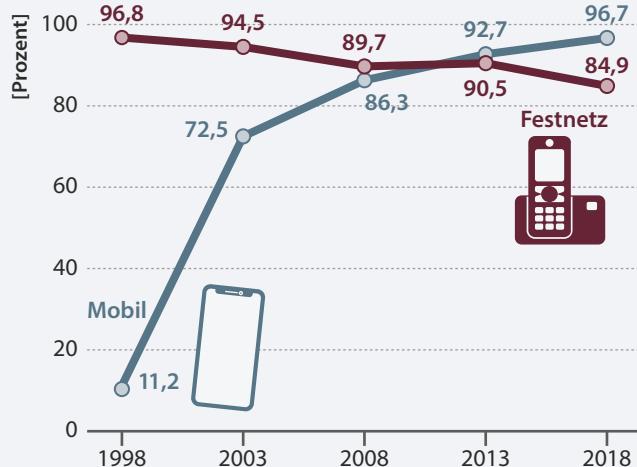
## ► Gesprächsminuten (abgehend)

... Immer mehr Telefonkunden nutzen Over-the-Top-Telefonie (OTT) in Deutschland, also telefonieren in Apps wie Skype, WhatsApp oder anderen Messaging-Diensten.<sup>4,5</sup>



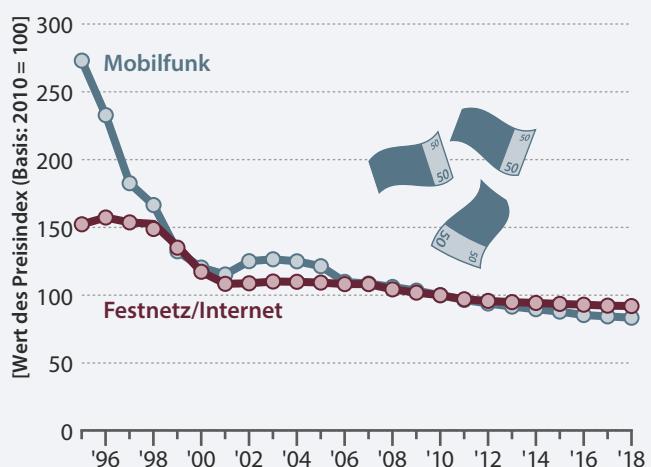
## ► Ausstattung mit Telefonen

... Mobil einsetzbare Handys und Smartphones ersetzen in immer mehr Haushalten das ortsgebundene Festnetztelefon.<sup>6</sup>



## ► Preisentwicklung

... Die Digitalisierung 1998 hat einen Preisrutsch bei Festnetztelefonie und Internetzugang ausgelöst. Und die Preise bröckeln weiter.<sup>7</sup>



# (Zu) stiller Alarm

## App-Desaster am Warntag

**Im September blieben am bundesweiten Warntag viele Handys stumm. Die Warn-Apps Nina, Katwarn und Biwapp benachrichtigten viele Nutzer zu spät oder gar nicht über den ersten bundesweiten Probealarm. Die Ursachen dafür liegen in der Infrastruktur.**

Von Urs Mansmann

Der 10. September sollte die Nagelprobe für die Warnung der Zivilbevölkerung im Katastrophenfall werden. Bundesweit sollten Sirenen ertönen, Warntafeln aufleuchten und Smartphones Alarm schlagen. Um genau 11 Uhr sollte das Spektakel beginnen, die Entwarnung war für 11:20 Uhr angesetzt.

Warn-Apps, die Meldungen an die Anwender pushen, sind inzwischen ein wichtiger Baustein des Zivilschutzes. Der gut vorbereitete Test scheiterte jedoch vollkommen überraschend und drastisch, denn viele Smartphones gaben keine Alarrrmeldung aus.

Das wäre nicht so fatal, wenn Deutschland nicht nach dem Ende des Kalten Kriegs entschieden hätte, die vielerorts fest installierten Warnsirenen abzubauen. Nur noch wenige Kommunen unterhalten ein Sirenennetz, das die Bevölkerung im Ernstfall zeitnah alarmieren könnte. An deren Stelle sollten schon lange moderne technische Lösungen getreten sein, die aber nicht so funktionieren, wie sie sollen.

Deshalb warnt man heute vielerorts noch so wie vor vielen Jahrzehnten: Tritt überraschend eine dringende Notlage ein, wird die Polizei mit Lautsprecherwagen in Marsch gesetzt. Allerdings gibt es große Unterschiede, wie die Länder und Kommunen das Thema angehen: Das stets von Sturmfluten bedrohte Hamburg beispielsweise unterhält auch heute noch ein funk-

tionierendes Sirenennetz und warnt bei drohenden Sturmfluten im Hafengebiet zusätzlich durch Böllerschüsse.

### Wichtiger Weckeffekt

Warn-Apps sind ein wichtiger Baustein, weil sie auch bei stummgeschaltetem Handy mitten in der Nacht Krach schlagen, wenn etwa wegen eines Brandes Fenster geschlossen werden müssen oder ein Hochwasser droht. Gerade nachts ist der Weckeffekt sehr wichtig; Durchsagen im Rundfunk oder Warnungen auf Anzeigetafeln erreichen niemanden, der gerade im Bett liegt. Allerdings hängt die Wirksamkeit der Warn-Apps davon ab, dass möglichst viele Anwender sie auch installieren und korrekt konfigurieren.

Ideen, wie man im Ernstfall Weckrufe auf anderem Wege absetzen könnte, gibt es viele. Beispielsweise könnten eines Tages die Hupen smarter Autos oder vernetzte Rauchmelder in den Haushalten die Betroffenen aus dem Schlaf reißen. Da Smart-City-Anwendungen in Deutschland aber noch nicht so richtig weit verbreitet sind und standardisierte Schnittstellen zu solchen Systemen oft fehlen, wird es noch viele Jahre dauern, bis das in die Praxis umgesetzt werden kann.

Die Warn-Apps sind ebenfalls eine Smart-City-Anwendung im weiteren Sinne. Sie arbeiten standortbezogen und stellen die Warnungen gezielt zu – deswegen benötigen sie Zugriff auf die Standortdaten des Smartphones, um dynamisch für den jeweiligen Aufenthaltsort zu warnen. Für die meisten Nutzer dürfte es sinnvoll sein, zusätzlich die Koordinaten des Wohnorts oder Arbeitsplatzes anzugeben, um auch dafür Warnungen zu erhalten, wenn man gerade woanders unterwegs ist.

### Zentrales Warnsystem

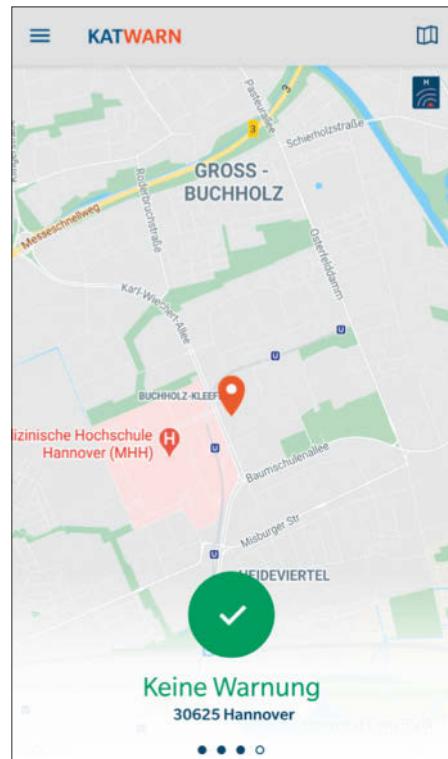
Die Warnmeldungen von den Katastrophenschutzbehörden in den Landkreisen und kreisfreien Städten sowie den Lagezentren der Bundesländer und des Bundes werden zentral im MoWaS (Modulares Warnsystem) des Bundesamtes für Bevöl-

kerungsschutz und Katastrophenhilfe (BBK) ausgelöst und verteilt. Warnungen erfolgen dabei stets nur für einen begrenzten Zeitraum und ein genau bezeichnetes Gebiet. Bundesweite Alarme wie der Probealarm am Warntag waren dabei in der Praxis erstmals bei der Corona-Pandemie zu verzeichnen.

In Deutschland sind derzeit drei etablierte Warn-Apps am Start: Nina, Katwarn und Biwapp. Alle drei tauschen seit Februar 2019 untereinander Nachrichten aus. Auf diesem Wege erreichen alle Meldungen, egal wie sie in eines der Systeme gelangt sind, alle betroffenen Nutzer aller drei Apps.

Die Systeme hinter den Warn-Apps haben Schnittstellen, über die sie Warnmeldungen direkt erfassen und verarbeiten können, etwa von Behörden und Wetterdiensten. Bei Katwarn gibt es einen Redaktionsdienst, der diese Eingaben betreut und das System beaufsichtigt.

Wer sichergehen will, sollte im Webauftakt seines Landkreis beziehungsweise seiner Stadtverwaltung dennoch eruieren, mit welcher der drei Warn-Apps diese direkt Daten austauscht und diese App installieren. Das erhöht die Wahrscheinlichkeit, dass man Warnungen für den jewei-



Die Warn-Apps arbeiten stets standortbezogen und verschicken die Meldungen gezielt nur an Betroffene.

ligen Standort zeitnah und zuverlässig zugestellt bekommt.

Genau das machte auch am Warntag den entscheidenden Unterschied: Wer beispielsweise in einem Kreis unterwegs war, der Katwarn nutzt, und Katwarn als Warn-App einsetzte, erhielt die Alarmmeldung schlimmstenfalls mit einigen Minuten Verzögerung. Andere warteten lange auf die Alarmmeldung – wenn sie denn überhaupt eintraf.

## Mobilfunknetze lastfest

An den Mobilfunknetzen lag es jedenfalls nicht: Selbst wenn Warnungen innerhalb kürzester Zeit an zahlreiche Anwender zugestellt werden, können 3G- und 4G-Mobilfunkzellen die dafür notwendigen Datenmengen ohne Probleme schultern. Eng könnte es erst nach der erfolgreichen Zustellung werden, wenn derart aufgeschreckte Nutzer gleichzeitig und zahlreich auf dem Alarm reagieren und beispielsweise zum Telefon greifen oder Daten im Internet abrufen.

Katwarn ist ein Projekt der öffentlichen Versicherer, die Programmierung liegt beim Fraunhofer-Institut für Offene Kommunikationssysteme, kurz Fokus. Projektleiter Daniel Faust erklärte im Gespräch mit ct, warum lange nicht alle Warnungen ankamen: „An unserem System sind zahlreiche Kommunen direkt angeschlossen. Am Warntag kamen darüber zahlreiche Meldungen herein, die wir innerhalb von Minuten alle zugestellt haben. Allerdings übergab das bundesweite System MoWaS seine Alarmierungen nur teilweise an Katwarn. Deshalb haben viele Anwender keine oder verspätete Warnung erhalten, obwohl unser System einwandfrei funktionierte.“

Dass die Probleme an MoWaS lagen, bestätigte uns auf Nachfrage auch der Sprecher des Bundesinnenministeriums, Björn Grünwälder, der auch für die Warn-App Nina des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) zuständig ist: „Der fehlgeschlagene bundesweite Warntag am 10. 9. 2020 steht nicht im Zusammenhang mit der Warn-App Nina.“

Probleme mit Nina habe es lediglich beim ersten Warntag 2018 in Nordrhein-Westfalen gegeben. Dabei hätten sich „Schwächen in der Bewältigung von Lastspitzen“ gezeigt. Das habe man umgehend behoben, beim ebenfalls noch auf NRW beschränkten Warntag 2019 habe die App die Lastspitze problemlos verar-

**Die Warn-App Biwapp verarbeitet nicht nur Warnmeldungen, sondern auch Service-Meldungen der Kommunen wie Verkehrshinweise oder Schulausfälle.**

beiten können. Derzeit werde die App von geschätzt 9,2 Millionen Anwendern genutzt, die Kapazität reiche aber für 40 Millionen aus.

Grund für die aktuellen Probleme sei ein Designfehler in der Programmierung von MoWaS. Grünwälder führt aus: „Gemäß Angaben des Dienstleisters für den Betrieb des modularen Warnsystems führt ein hohes Aufkommen gleichzeitiger Datenbankabfragen der Anwender zu der Systemüberlastung, die ursächlich für die verzögerte Meldungsverarbeitung war.“ Nachdem die Warnung von MoWaS verspätet erfolgt sei, habe Nina die Warnungen innerhalb weniger Sekunden ausgeliefert.

Offenbar entwickelte die Situation dann zusätzlich eine fatale Eigendynamik: Als die Verantwortlichen im Katastrophenhafen feststellten, dass ihre Meldungen nicht ankamen, schickten einige sicherheitshalber wohl noch weitere Meldungen hinterher, was das akute Lastproblem noch zusätzlich verschärft, berichteten einige Medien.

Eine lastfeste Alternative zu einer App-Lösung wären Cell Broadcasts, wie sie in anderen EU-Ländern eingesetzt werden, etwa den Niederlanden oder Rumänien. Solche Nachrichten werden für alle

Teilnehmer in einer Funkzelle ausgestrahlt. Das funktioniert aber nur für den aktuellen Standort. Durch zyklische Wiederholung der Nachrichten bekommen auch Teilnehmer eine Meldung, die ihr Gerät später einschalten, vorübergehend keinen Empfang hatten oder im Warngebiet eintreffen.

Die deutschen Netzbetreiber nutzen Cell Broadcast aber schon seit vielen Jahren nicht mehr; man müsste also zunächst einmal die Technik dazu installieren. Eine Alarmierung per SMS wiederum scheitert an den Kapazitäten im Mobilfunk, weil sie jedem Nutzer einzeln zugestellt werden müsste. Wollte man alle Nutzer in einem dicht besiedelten Gebieten per SMS warnen, würde der Versand der Nachrichten zu lange dauern.

## Konsequenzen aus dem Fehlschlag

Der krachende Fehlschlag zog bereits personelle Konsequenzen nach sich: Der Chef des BBK, Christoph Unger, der das Warn-Desaster zu verantworten hat, muss seinen Posten vorzeitig räumen. Ihm soll der CDU-Bundestagsabgeordnete Armin Schuster nachfolgen. Innenminister Horst Seehofer kündigte grundlegende Reformen beim BBK an.

Die erkannten Mängel sollen nun zügig beseitigt werden. Ein Systemtest soll sicherstellen, dass das erfolgreich war. Und offenbar will das BBK damit nicht bis zum nächsten turnusmässigen Warntag im September 2021 warten.

Wenn nächstes Mal alles funktioniert, kann auch der Twitterer @OomenBerlin durchschlafen, der am 11. September um 3:53 Uhr morgens darüber klagte, dass ihn eine 17 Stunden verspätete Pushnachricht vom Warntag gerade aus dem Schlaf gerissen habe. (uma@ct.de) ct



Bild: Fraunhofer FOKUS/O. Lang

**Warnungen erfolgen stets für ein bestimmtes Gebiet. Bundesweite Alarne kommen in der Praxis fast nie vor.**



Bild: Geothermieanlage Bruchsal, EnBW

# Schatz im Oberrheingraben

## Heimisches Lithium als Nebenprodukt von Erdwärmestrom

**Lithium-Ionen-Technik treibt mobile Endgeräte an, deshalb ist das importierte Alkalimetall ein teures Gut. Geologen in Karlsruhe erschließen erstmals Quellen in Deutschland – das Tiefenwasser von Geothermieranlagen.**

**Von Markus Strehlitz, Arne Grävemeyer**

**G**emeinhin gelten ja Daten als das Öl des 21. Jahrhundert. Aber ein Rohstoff hätte ebenfalls Anspruch auf diesen Titel: Lithium. Es ist elementarer Bestandteil von Lithium-Ionen-Akkus und macht damit Smartphones, Laptops und Elektrofahrzeuge erst mobil. Zudem gibt es die nicht wieder aufladbaren Lithiumbatterien, die sich vor allem in Kleinstelektronik durchgesetzt haben. Lithiumtechnik ist leicht, kompakt und bietet eine hervor-

ragende Energie- und Leistungsdichte. Ernstzunehmende Alternativen wie Natrium-Ionen-Akkumulatoren und Magnesium-Schwefel-Batterien befinden sich derzeit noch im Laborstadium.

Eine Wissenschaftlergruppe am Karlsruher Institut für Technologie (KIT) hat nun ein Verfahren ausgetüftelt, bei dem Lithium quasi als Abfallstoff bei der Energieerzeugung in Geothermieranlagen anfällt. Eine Pilotanlage soll noch bis Jahresende Lithium aus Deutschland fördern.

Heute ist die Gewinnung von Lithium problematisch. Es wird derzeit vor allem aus Salzseen im südamerikanischen Länderdreieck Chile, Argentinien und Bolivien abgebaut [1] sowie aus Festgestein – hauptsächlich in Australien.

### Salzwüsten entstehen

In Südamerika wird der Rohstoff gewonnen, indem lithiumhaltiges Wasser in großen Salzseen verdunstet. Der Prozess kann über ein Jahr in Anspruch nehmen. Das vorrangige Problem: Man braucht viel Wasser, um Lithium in der Konzentration

zu erhalten, die für eine Batteriezellenproduktion notwendig ist. Wasser ist allerdings in den betroffenen Gebieten ein mindestens genauso kostbarer Rohstoff wie das zu gewinnende Lithiumsalz für die Industrie. „Da die Abbaugebiete beispielsweise in der Atacama-Wüste sehr trocken sind, können Auswirkungen auf die Hydrologie schwerwiegend sein“, heißt es dazu in einer Studie des Freiburger Öko-Instituts. Die Wasserreserven am Salar de Atacama in Chile seien zwischen 2002 und 2017 mit einer Rate von 1,16 Millimetern pro Jahr zurückgegangen, was auch die letzten Flussläufe und Wiesen vertrocknen lässt.

Die Gewinnung aus Festgestein in Australien erfordert hingegen viel Energie und erzeugt eine große Menge Abraum. Weite Transportwege zu Produktionsstätten für Batterietechnik in Europa sind ein weiteres ökologisches und ökonomisches Problem.

Doch die Transportwege könnten sich künftig verkürzen. Jens Grimmer, Geologe am KIT, und seine Kollegin Florence Saravia haben ein vergleichsweise einfaches

Verfahren entwickelt, um Lithium am Oberrheingraben zu fördern. Dort stehen Geothermieanlagen, die heißes Wasser aus dem tiefen Untergrund nach oben befördern, um daraus Strom zu produzieren. Die unterirdischen Thermalwasser-Reservoirs liefern aber nicht nur Energie, in ihnen ist auch Lithium gelöst – und das in beträchtlichen Mengen. Grimmer geht von 200 Milligramm pro Liter aus. Das gesamte Potenzial im Oberrheingraben beläuft sich auf mehrere tausend Tonnen an förderbarem Lithium pro Jahr.

## 800 Tonnen Lithium in Bruchsal

Die KIT-Wissenschaftler wollen bereits vorhandene Geothermieanlagen nutzen, von denen es auf deutscher und französischer Seite derzeit insgesamt fünf gibt, und zwar an den Standorten Bruchsal, Landau, Insheim, Soultz-sous-Forêts und Rittershoffen. Allein durch die Geothermieanlage Bruchsal strömen seit 2010 sekündlich 28 Liter Thermalwasser. Damit werden derzeit überschlägig etwa 800 Tonnen Lithiumchlorid pro Betriebsjahr gefördert und ungenutzt wieder reinjiziert, wie der Anlagenbetreiber EnBW mitteilt.

Jede dieser Anlagen besitzt prinzipiell zwei Wasserleitungen in die Tiefe. Durch die eine strömt das Thermalwasser in einen Wärmetauscher und gibt dort einen Teil seiner Energie ab. Anschließend fließt es durch die sogenannte Schluckleitung wieder in den tiefen Untergrund zurück. Genau hier wollen die Wissenschaftler ansetzen und mit einer Anlagenergänzung Lithiumionen herausfiltern.

Für diesen Teil des Verfahrens setzen die KIT-Experten auf eine halbdurchlässige Membran, durch die sie das Wasser mit hohem Druck pressen. Auf diese Weise überwinden sie den osmotischen Druck, der der Konzentration von gelösten Ionen entgegenwirkt. Die Methode lässt sich vereinfacht mit der von Meerwasserentsalzungsanlagen vergleichen. Im Ergebnis trennt die KIT-Membran Wasser mit gelösten Lithiumionen vom restlichen Thermalwasser.

Insgesamt erfordert dieser Verfahrensschritt eine ganz erhebliche Membranfläche, in einer vollständigen Anlage voraussichtlich mehrere Hundert Quadratkilometer. Allerdings lässt sich diese Membran raumsparend aufwickeln und in mehrere Module verpacken. „Das ist der Grund, weshalb wir wahrscheinlich nicht viel Platz benötigen“, sagt Grimmer.

Die im ersten Schritt erzielte Lithium-Konzentration reicht noch nicht aus, um das Lithium chemisch auszufällen. Um die Konzentration dafür auf 5000 bis 6000 Milligramm pro Liter zu steigern, erhitzten die Forscher das Wasser in einem zweiten Verfahrensschritt. Die dafür benötigten zusätzlichen Energiemengen sind überschaubar, da selbst die Temperatur des abgekühlten Thermalwassers vor der Re-injektion in die Tiefen der Gesteinsschichten noch 60 bis 70 Grad Celsius beträgt.

Das Ergebnis aus diesen beiden Verfahrensschritten ist Lithiumkarbonat – ein Zwischenprodukt, das die Industrie weiterverarbeiten kann. Grimmer rechnet damit, dass dieses Endprodukt noch in einer weiteren Verfahrensstufe zu reinigen ist. Doch die Frage nach dem dafür benötigten Wasser dürfte hierzulande nicht so heikel sein wie in den Salzwüsten Südamerikas. In Zukunft könnte eine zentrale Anlage für den gesamten Oberrheingraben das gewonnene Lithiumkarbonat zusammenführen und reinigen.

## Schnelle Gewinnung

Das KIT-Verfahren ist im Vergleich zu anderen Abbauförmen sehr schnell: Während die Gewinnung aus Salzseen Monate in Anspruch nimmt, gehen die KIT-Wissenschaftler davon aus, dass sich das Lithium im Thermalwasserzyklus der Geothermieranlage kontinuierlich innerhalb von Stunden extrahieren lässt. Europa müsste geringere Mengen an Lithium

importieren, was das Risiko des Ausfalls von Lieferketten senkt.

Ein weiterer Vorteil des neuen Verfahrens ist die gezielte Ausfilterung der Lithiumionen. Alle weiteren Inhaltsstoffe strömen mit dem genutzten Thermalwasser wieder zurück in die Tiefe. So verursachen sie keine Probleme in der Anlage – etwa indem sie in Form von Ausfällungen Rohre verstopfen und Wartungsarbeiten verursachen. Das Prinzip des Verfahrens von Grimmer und Saravia lautet: Dem Wasser werden nur die Lithiumionen entnommen.

Das ist gleichzeitig aber auch eine wichtige Bedingung, die das Verfahren erfüllen muss. „Das Wasser, das für die Geothermie verwendet wird, enthält auch Stoffe, die man nicht an der Oberfläche haben möchte“, erklärt Grimmer. Dazu zählen zum Beispiel Schwermetalle. „Wir wissen, dass keine Probleme entstehen, wenn wir das Wasser so, wie es ist, wieder nach unten schicken. Wir wissen aber nicht, welche Reaktionen wir im Reservoir hervorrufen, wenn wir es wesentlich verändern würden.“ Dies technisch umzusetzen ist eine der Anforderungen an die künftige Pilotanlage.

Eine andere besteht darin, mit den hohen Fließraten des Thermalwassers rechtkommen. Diese sind überhaupt die Voraussetzung, um wirtschaftlich Geothermie zu betreiben. Lithiumkonzentration und Fließgeschwindigkeit sind die entscheidenden Größen, denn das Produkt aus

## Lithium aus dem Rückstrom

Zusatznutzen der Geothermie: Nachdem das Thermalwasser in einem Wärmetauscher Energie abgegeben hat und bevor es wieder in die Tiefe zurückfließt, filtern aufgewickelte Membranen die in Wasser gelösten Lithiumionen heraus.

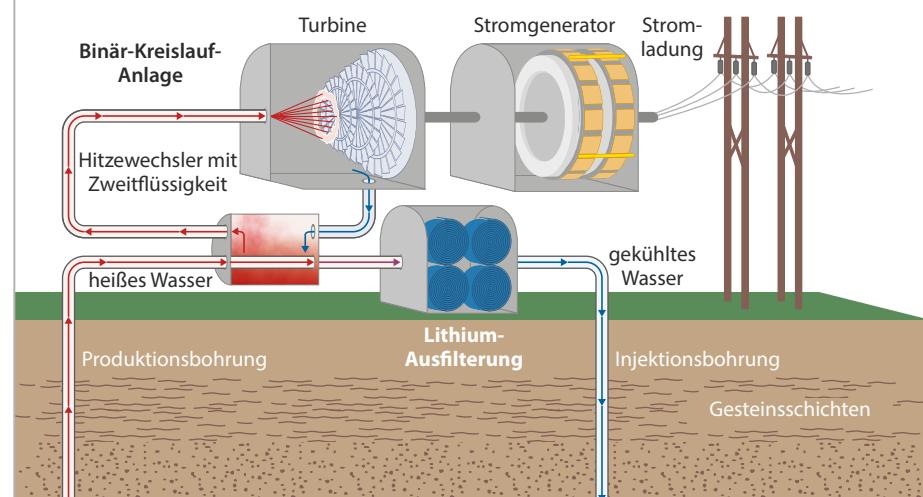




Bild: Amadeus Bramsiepe / KIT

beiden ergibt das Potenzial, das die teilnehmenden Partner heben können. Letztlich habe man sich wegen der hohen Fließraten für die Membrantechnologie entschieden.

Herausforderungen gibt es aber nicht nur bei der Technik. „Sobald man in den Thermalwasserkreislauf eingreift, bedarf das immer einer Zustimmung der Bergämter“, sagt Grimmer. Es gibt also auch administrative Hürden zu überwinden.

## Steigende Nachfrage erwartet

Martin Wedig weiß, dass sich solche Genehmigungsverfahren hinziehen können. Er ist Geschäftsführer der Vereinigung Rohstoffe und Bergbau, ein Wirtschaftsverband der deutschen Rohstoff gewinnenden Industrie. Und seiner Meinung nach sind die regulatorischen Hürden einer der Gründe, weshalb es solche Projekte hierzulande schwer haben, Investoren zu finden. Aber grundsätzlich sieht er die Aktivitäten der KIT-Wissenschaftler positiv. „Jedes Vorhaben, in Deutschland oder Europa eine eigene Lithiumgewinnung aufzubauen, ist unterstützenswert“, sagt Wedig. Er befürworte alles, was dazu führe, weniger abhängig von ausländischen Lieferungen zu sein. Die Coronakrise habe gezeigt, wie schnell Lieferketten reißen können.

Die KIT-Forscher gehen davon aus, dass die Lithiumerzeugung mit ihrem Verfahren günstiger sein wird als die Förderung aus Festgestein oder mit Salzseen – wenn sich das Verfahren an bestehende Geothermiekraftwerke ankoppeln lässt.

Zwar ist der Weltmarktpreis für Lithiumkarbonat seit einigen Jahren großen Schwankungen unterlegen und derzeit mit etwa 7,25 US-Dollar an der Londoner

Metallbörse relativ niedrig – unter anderem, weil der Ausbau der Elektromobilität nicht so schnell vorankommt wie erwartet. Aber die deutsche Rohstoffagentur erwartet für die kommenden Jahre eine deutlich ansteigende Nachfrage.

## Weitere Projekte

Die Möglichkeit, Lithium aus Thermalwasser zu gewinnen, hat daher noch andere Interessenten gefunden. So hat etwa Pfalzwerke geofuture, eine Tochter des Energieversorgers Pfalzwerke aus Ludwigshafen, mit dem australischen Unternehmen Vulcan eine Absichtserklärung zur Lithiumgewinnung unterzeichnet. Die beiden Partner wollen dafür das Geothermiekraftwerk Insheim nutzen. Hier strömen in der Sekunde 50 bis 80 Liter Heißwasser aus der Tiefe, mit bis zu 200 Milligramm Lithiumsalzen pro Liter.

Weitere Interessenten an der Lithiumgewinnung im Oberrheingraben haben bereits Schürfrechte beantragt, darunter die Deutsche Erdwärme aus Karlsruhe und auf französischer Seite das Unternehmen Fonroche.

Noch befindet sich dieses Projekt der Pfalzwerke in einem sehr frühen Stadium, man startet gerade mit Laborversuchen. Jörg Uhde, Geschäftsführer von Pfalzwerke geofuture, geht davon aus, dass in etwa zwei Jahren die Voraussetzungen für erste Pilotversuche im Geothermiekraftwerk vorliegen können. Die Partner rechnen damit, allein am Standort Insheim etwa 190 Tonnen Lithium jährlich fördern zu können. Mit neuen Bohrungen in der Ortenau am rechten Oberrhein könne das Unternehmen noch zehnmal so viel Lithium fördern, erwartet man bei Vulcan.

Allein durch die Leitungen der Geothermieranlage Bruchsal strömen mit dem Thermalwasser im Jahr etwa 800 Tonnen Lithiumchlorid, die bislang ungenutzt bleiben.

In zwei Jahren soll das Verfahren des KIT längst erprobt sein. Die Wissenschaftler aus Karlsruhe wollen ihre Pilotanlage schon bis Jahresende 2020 in den Thermalwasserkreislauf in einem der existierenden Geothermiekraftwerke im Oberrheingraben installieren. Damit wollen sie nicht nur die Machbarkeit beweisen, sondern auch ermitteln, zu welchen Kosten die Lithiumgewinnung möglich ist. „Dieser Prototyp ist relativ klein und im Prinzip könnte man ihn auf einen Schreibtisch stellen“, erklärt Grimmer. „Wir werden dabei zunächst auch nur mit geringen Fließraten von zehn Litern pro Minute arbeiten.“

Mit der Pilotanlage werden dann verschiedene Experimente durchgeführt. Unter anderem wollen die Wissenschaftler unterschiedliche Druckstärken sowie Membrantypen testen. Die Daten des Prototyps sollen auch aufzeigen, ob das Verfahren wirtschaftlich sein kann. Die Pilotphase werde etwa ein halbes Jahr dauern.

Wenn der Betrieb im Prototyp-Maßstab funktioniert, könne man eine Großanlage planen und aufbauen. Das Verfahren sei so angelegt, dass sich auch diese auf der Fläche der existierenden Geothermiekraftwerke unterbringen lasse. Grimmer schätzt, dass der Aufbau der Großanlage ein Jahr dauern wird. Wenn alles gut läuft, könnten die Projektpartner bereits in zwei Jahren signifikante Mengen Lithiumkarbonat liefern. (agr@ct.de) **ct**

## Literatur

- [1] Christian Wölbert, Bolivien träumt vom Lithium-Boom, Wie das ärmste Land Südamerikas eine Akku-Industrie aufbauen will, c't 15/2014, S. 72



## **Servermanagement mit SaltStack**

Installation, Konfiguration, Automatisierung

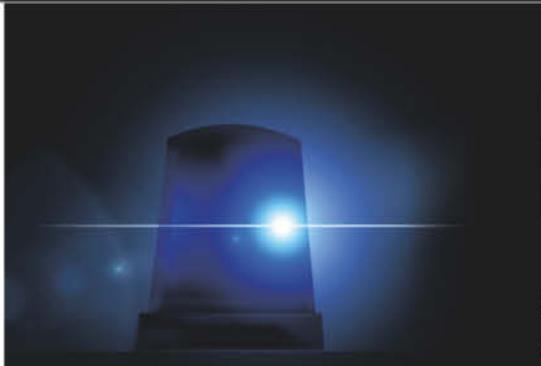
26. – 28. Oktober 2020

online



## **Single-page Applications mit Angular**

02. – 05. November 2020  
online



## **Parallele Programmierung in Java**

11. – 13. November 2020  
Hannover

## **IT-Sicherheit: Notfallplanung und Notfallübungen**

09. – 11. November 2020  
online



## **OWASP Top 10**

16. November 2020  
online



Weitere Infos unter:  
<http://www.heise-events.de/workshops>





Bild: Henning Rathjen

# Die ELFE und das Bürokratiemonster

## E-Government: Warum Software allein nicht ausreicht

**Eine in Bremen erdachte App vereinfacht den Antragsprozess für Kinder- und Elterngeld radikal. Für den Erfolg mussten allerdings zahlreiche Gesetze geändert werden – ein Aufwand, den die Bundesregierung selten treibt.**

Von Christian Wölbert

**K**ommt ein Kind auf die Welt, haben die Eltern Besseres zu tun, als Formulare auszufüllen. Aber es muss ja sein: Die Geburt muss angemeldet werden, Elterngeld muss beantragt werden, Kindergeld ebenfalls, eventuell auch der Kinderzuschlag. Allein der Antrag auf Elterngeld umfasst (in Niedersachsen) neun Seiten. Beizufügen sind diverse Nachweise, darunter eine Geburtsurkunde, die jüngsten zwölf Gehaltsabrechnungen und eine Bescheinigung der Krankenkasse.

Doch wenn alles glatt geht, hat dieser Papierkrieg bald ein Ende. Künftig sollen El-

tern in Deutschland Elterngeld und Kinder- geld innerhalb von fünf Minuten mit einer Web-Anwendung beantragen können. Ohne komplizierte Formulare, ohne Nachweise. Bremen will das unter dem Titel „ELFE – Einfache Leistungen für Familien“ noch in diesem Jahr online stellen. Die restlichen Bundesländer sollen folgen.

Es wäre ein kleines Wunder. Im aktuellen E-Government-Ranking der EU-Kommission liegt Deutschland auf Rang 22 von 29 – hinter Ländern wie Zypern und Slowenien. Schließlich geht man in der Bundesrepublik auch im Jahr 2020 meist

noch persönlich zum Amt oder schickt einen Brief. Und selbst die wenigen vorhandenen Online-Anwendungen, etwa für die Steuererklärung, machen das Leben nicht wirklich leichter: Nutzer sparen Papier und Porto, aber nicht viel Zeit, weil online dieselben Formulare ausgefüllt werden müssen wie offline.

### Win-Win-Win-Situation

ELFE ist anders. Die Anwendung fasst ertens mehrere Anträge zusammen, die bislang an verschiedene Behörden geschickt werden müssen. Zweitens müssen die Eltern nur noch wenige Informationen eintippen und keine Nachweise anhängen. Die Behörden besorgen sich die nötigen Daten dann – wenn die Antragsteller zustimmen – einfach bei anderen Behörden.

Davon profitieren nicht nur die Bürger. Die Bundesregierung schätzt, dass der Staat durch das neue Verfahren rund 5 Millionen Euro pro Jahr einspart, weil Sachbearbeiter weniger Daten abtippen und seltener fehlende Unterlagen nachfordern müssen. Die Wirtschaft wird demnach um rund 100.000 Euro im Jahr entlastet, weil Eltern ihre Arbeitgeber seltener um zusätzliche Unterlagen bitten. Eine Win-Win-Win-Situation.

### Sechs Gesetzesänderungen für eine App

Die Geschichte von ELFE zeigt aber auch, welcher Aufwand getrieben werden muss, um wirklich praktische E-Government-Anwendungen zu schaffen. Design-Thinking-Workshops und agile Entwicklung reichen nicht. Nötig sind auch politische, juristische und organisatorische Schwerstarbeit. Allein für die erste Ausbaustufe von ELFE mussten sechs Gesetze und Verordnungen geändert werden.

Wer mehr darüber erfahren möchte, muss mit Martin Hagen sprechen. Der offizielle Titel des Diplom-Politologen lautet „Staatsrat für Haushalt, Personal und IT beim Senator für Finanzen der Freien Hansestadt Bremen“. Manchmal wird er aber einfach „Vater der ELFE“ genannt.

Vor vier, fünf Jahren stellten Hagen und seine Kollegen fest, dass die meisten

Bremer E-Government-Anwendungen kaum genutzt wurden. Es erschien ihnen deshalb wenig sinnvoll, weitere Antragsverfahren eins zu eins online zu stellen. Um diese Zeit herum wurde Hagen zum fünften Mal Vater, füllte zum fünften Mal die entsprechenden Formulare aus. Er setzte sich in den Kopf, einen besseren Prozess zu erfinden: „Wir mussten uns fragen, was eigentlich die Nutzerinnen und Nutzer wollten.“

### Sinnloses Abtippen

Im November 2017 veranstalteten die Bremer einen Workshop mit einem Dutzend Behörden, die mit dem Thema „Geburt“ befasst sind. Schnell kam man zu der Erkenntnis: Formulare und Nachweise sind für Elterngeld und Kindergeld eigentlich überflüssig. Denn rund 95 Prozent der Informationen, die Behörden bislang von den Eltern verlangen, liegen längst bei der Verwaltung vor.

Die Standesämter zum Beispiel können bezeugen, dass das Kind existiert. Die Rentenversicherung kann Informationen zum Gehalt der Eltern bei den Arbeitgebern elek-

tronisch abfragen. Die Krankenkassen wissen, wie viel Mutterschaftsgeld sie bezahlt haben. „In Wirklichkeit haben wir die Daten schon, bevor die Eltern sie uns geben“, betont Hagen.

Allerdings dürfen die Behörden die Daten bislang nicht untereinander austauschen. Allein deshalb müssen Eltern sie selbst beschaffen und einreichen. Und die Sachbearbeiter in den Elterngeldstellen müssen sie wieder abtippen. Erst danach kann eine Software die Höhe des Elterngelds berechnen. „Eigentlich ist das Verfahren ein gigantischer Algorithmus“, sagt Hagen.

Die Bremer entwickelten einen Prototypen der ELFE-Anwendung. Sie liest den Personalausweis über die NFC-Schnittstelle des Smartphones aus und verifiziert so die Identität des Antragstellers. Im nächsten Schritt fragt sie, wie Vater und Mutter die Elterngeldmonate untereinander aufteilen wollen. Dann sammelt ein



Bild: Freie Hansestadt Bremen / Der Senator für Finanzen

**Der Bremer Staatsrat Martin Hagen gab den Anstoß für die Entwicklung der ELFE-App.**

Webdienst die nötigen Daten ein – Geburtsbestätigung, Gehaltsinfos und so weiter – und speist sie in die richtigen Kanäle.

### Fünf Ministerien mussten mitziehen

Doch umsetzen konnte Bremen das System nicht, die App blieb erst einmal ein Dummy. Zunächst musste der Bund die gesetzlichen Grundlagen für den Datenaustausch zwischen den Behörden schaffen. Die Einwilligung der Eltern genügte nicht. Die Behörden mussten dazu auch vom Gesetzgeber berechtigt und verpflichtet werden.

Die Bremer sicherten sich zunächst die Unterstützung der anderen Bundesländer. Im September 2018 forderte der Bundesrat den Bund mit 16:0 Stimmen auf, „geeignete Gesetzesvorschläge für die Umsetzung des Projektes ELFE zu unterbreiten“.

Nun lief die Berliner Gesetzesmaschinerie an. Doch das Vorhaben entpuppte sich als komplex. Nicht weniger als fünf Ministerien mussten zusammenarbeiten: Inneres, Familie, Arbeit, Gesundheit und Justiz. Außerdem waren das Bundeskanzleramt und der Bundesbeauftragte für den Datenschutz beteiligt. Angepasst werden mussten die Personenstandsverordnung, das Einkommensteuergesetz, die Abgabenordnung, das Elternzeitgesetz sowie das Vierte und das Fünfte Buch Sozialgesetzbuch. „Es reicht nicht, mit nur einem Ministerium die Digitalisierung zu besprechen. Man muss alle an einen Tisch bringen“, sagt Hagen.

**Das Konzept für ELFE entstand im November 2017 auf einem Workshop in Bremen. Ende 2020 soll die Familien-App einsatzbereit sein.**



Bild: Freie Hansestadt Bremen / Der Senator für Finanzen

Am 24. Juni 2020 beschloss das Bundeskabinett den „Gesetzentwurf zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen.“ Voraussichtlich im November werden sich Bundestag und Bundesrat mit dem Entwurf befassen, ihre Zustimmung gilt als sicher. Der Workshop in Bremen wird dann genau drei Jahre zurück liegen.

### Vorerst nur für Angestellte

Parallel zu den Gesetzesänderungen trieben die Bremer und der Bund die technische Umsetzung voran. Zusammen mit technischen Dienstleistern wurden Standards für den Datenaustausch definiert und Schnittstellen in die Systeme der Rentenversicherung und der Krankenkassen eingebaut. Noch bis Ende des Jahres will Bremen sein ELFE-System freischalten.

Trotzdem bleiben noch Baustellen: Das Elterngeld ist zwar bundesweit einheitlich geregelt, die Länder bearbeiten die Anträge aber eigenständig – und setzen zum Teil andere Software ein als Bremen. Diese Anwendungen müssen nun ebenfalls noch an das neue Konzept angepasst werden. Einige Länder werden dem Bremer Beispiel voraussichtlich schnell folgen. Doch bis ELFE bundesweit läuft, kann es durchaus noch ein, zwei Jahre dauern.

Und das ist nicht das einzige Problem: Vorerst werden nur Angestellte die ELFE-App nutzen können, denn nur deren Einkommen wird von der Rentenversicherung erfasst. Damit auch Selbstständige Elterngeld auf diesem Weg beantragen

können, müssen die Finanzämter an das neue System angebunden werden. Dazu sind wiederum neue Rechtsanpassungen nötig. Auch Besoldungsstellen für Beamte müssen noch integriert werden.

Trotzdem gilt ELFE bereits jetzt als Vorzeigbeispiel, nicht nur bei der Bundesregierung und in Bremen. Auch der Normenkontrollrat, ein unabhängiges Expertengremium für Bürokratieabbau, lobt das neue System. Er vermutet sogar, dass künftig 80 Prozent der Eltern es nutzen werden – nicht nur 40 Prozent, wie die Bundesregierung schätzt.

### Bleibt ELFE die Ausnahme?

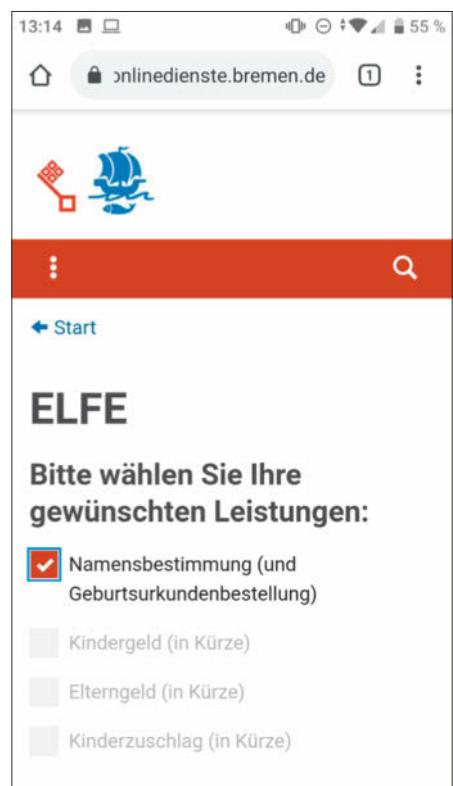
Mittlerweile sind zig weitere E-Government-Projekte angelaufen. Treiber ist das Online-Zugangsgesetz (OZG), mit dem sich Bund und Länder dazu verpflichtet haben, bis Ende 2022 die knapp 600 wichtigsten Verwaltungsleistungen online zu stellen. Landauf, landab fanden in den vergangenen Jahren zahlreiche ähnliche Workshops statt wie 2017 in Bremen.

Laut dem Normenkontrollrat wurden in solchen Laboren mittlerweile rund 40 „Rechtsänderungswünsche“ für nutzerfreundliche E-Government-Apps nach dem Vorbild von ELFE identifiziert. Doch die Bundesministerien würden sich „schwertun“, diese Gesetzesvorhaben anzupacken. Abgesehen vom ELFE-Paket sei bislang nur ein weiteres Gesetz, das Meldegesetz, für E-Government optimiert worden. „Der Weg vom Labor zum digitalisierungsfreundlichen Gesetz scheint ein sehr weiter zu sein“, schreibt der Rat in seinem Bericht.

Zu befürchten ist also, dass ELFE eine Ausnahme bleibt. Dabei sei es seit Langem eine Binsenweisheit, dass es nicht ausreiche, Verwaltungsverfahren „eins zu eins zu elektrifizieren“, mahnt der Normenkontrollrat.

(cwo@ct.de) **ct**

**ELFE-Gesetzentwurf, Bericht des Normenkontrollrats: [ct.de/y48q](http://ct.de/y48q)**



**Prototyp der ELFE-App: Anträge werden zusammengefasst und vereinfacht.**

# Faszination Geschichte –

## Großartige Leistungen früherer Zivilisationen

### Top-Themen:

- Das Leben im alten Rom
  - Im Reich der Inka
  - Die Varusschlacht - Sieg der Germanen
  - Die Geheimnisse von Stonehenge
- ...und viele mehr!



Jetzt am Kiosk oder unter: [shop.heise.de/wissen-geschichte20](http://shop.heise.de/wissen-geschichte20)



Mit dem Security Advisory ADV190023 hat Microsoft viele Administratoren verunsichert. Dabei sollen die darin enthaltenen Empfehlungen eigentlich nur für mehr Sicherheit in der Kommunikation mit Active-Directory-Domain-Controllern sorgen und ungesicherte Verbindungen verhindern. Wir haben zusammengefasst, was Admins jetzt wissen müssen, wenn sie mit einem AD und LDAP arbeiten.

Von Thorsten Scherf

Mitte August 2019 hat Microsoft das Advisory ADV190023 herausgebracht. Darin empfehlen die Redmonder, die beiden Einstellungen „LDAP-Channel-Bindung“ und „LDAP-Signaturen“ auf Active-Directory-Domain-Controllern zu aktivieren. Diese sollen eine „sicherere Kommunikation zwischen LDAP-Clients und Active Directory-Domain-Controllern“ garantieren. Weiter kündigt Microsoft an, dass diese Einstellungen in einem späteren Update (zwischenzeitlich war mal vom März 2020 die Rede) automatisch aktiviert werden könnten. Und genau hier fängt das Problem an: Da Microsoft bewusst oder unbewusst sehr schwammig formuliert hat und nicht genau auflistet, welche Verbindungen genau „sicher“ sind, entstand viel Aufregung. Fälschlicherweise nahmen viele Admins an, dass hiermit der Einsatz von SSL/TLS für Verbindungen zum Domain-Controller zwingend vorgeschrieben werde – wer eine Hard- oder Software nutze, die das nicht beherrscht, so die Angst, werde ausgesperrt. Doch ganz so drastisch sind die Änderungen gar nicht. Administratoren sollten sich aber schon jetzt mit den Optionen sicherer LDAP-Verbindungen beschäftigen, auch wenn es aktuell keinen konkreten Termin für Änderungen durch ein Update mehr gibt. Nicht alle Details in diesem Artikel sind in jeder Umgebung von Interesse. Admins reiner Windows-Umgebungen zum Beispiel müssen sich nicht mit allen Feinheiten von TLS-Verbindungen auseinandersetzen.

Bild: Albert Huin

# Sicher, aber ausgesperrt?

## Was Microsofts Sicherheitsempfehlungen fürs Active Directory für Admins bedeuten

## Begriffsklärung

Mit den Empfehlungen und den für die ferne Zukunft angekündigten Änderungen der Standardeinstellungen will Microsoft das Herzstück von Windows-basierten Firmenumgebungen besser schützen. Die beiden Sicherheitseinstellungen „LDAP-Signierung“ und „LDAP-Channel-Bindung“ beschreibt Microsoft recht dürftig in zwei Dokumenten (alle Texte finden Sie über [ct.de/yqb2](http://ct.de/yqb2)). Die eigentliche Idee dieser Einstellungen ist, Replay- und Man-in-the-Middle-Angriffe zu verhindern. Bei dieser Art von Attacken versuchen Angreifer, Daten durch Abhören der Netzwerkkommunikation abzufangen und in veränderter Form an das eigentliche Ziel weiterzuleiten. Mithilfe von LDAP-Signaturen wird sichergestellt, dass Daten auf dem Weg vom Absender zum Empfänger nicht verändert wurden – der Absender signiert sie kryptografisch, der Empfänger kann die Signatur verifizieren. Ein Angreifer kann die Inhalte unterwegs nicht verändern und eine gültige Signatur erzeugen.

Bei der LDAP-Channel-Bindung geht es darum, dass Angreifer keine Identitätsinformationen eines Benutzers abfangen können, um diese dann innerhalb einer anderen Verbindung erneut zu verwenden – etwa, um in fremdem Namen Aktionen im Firmennetz auszuführen. Im Englischen wird für solche Angriffe gerne der Begriff des „Impersonating“ verwendet. Bei LDAP besteht diese Schwachstelle nur in dem kurzen Moment, in dem ein TLS-Kanal zu einem Domain-Controller aufgebaut wird – die Lücke wurde 2017 bekannt und hat die CVE-Nummer CVE-2017-8563 bekommen. Bei aktivierter LDAP-Channel-Bindung findet eine Art Verknüpfung des TLS-Layers mit dem Anwendungs-Layer statt, in diesem Fall also LDAP. Dabei wird der Fingerabdruck des TLS-Layers mit dem LDAP-Protokoll verbunden. Das Ergebnis dieser Verknüpfung ist eine eindeutige Prüfsumme, die verhindert, dass Pakete einer solchen Verbindung zu einem späteren Zeitpunkt erneut wieder verwendet werden können, da sich der Fingerprint und damit die Prüfsumme mit jeder neuen TLS-Sitzung ändert.

## Was ist schon sicher?

Grundsätzlich gibt es mehrere Wege, um den Verkehr zwischen Client und Domain-Controller zu sichern: Der RFC 2251 für LDAP v3 definiert zwei Methoden, um

einen BindRequest durchzuführen, also eine Anmeldung an einem LDAP-Server: per Simple Bind oder per „Simple Authentication and Security Layer Bind“ (SASL Bind). Ein Simple Bind findet mit einem Active-Directory-Domain-Controller üblicherweise auf dem Standard-LDAP-Port 389 statt. Bei einem solchen findet die Authentifizierung des Benutzers mit Benutzername und Passwort statt. Bei einem Simple Bind werden die Daten weder signiert noch verschlüsselt übertragen. Solche Verbindungen gehören nicht zu den sicheren und sind leicht zu missbrauchen. Eine Möglichkeit ist es, diesen Verkehr per SSL/TLS-Tunnel zu sichern – dazu später mehr.

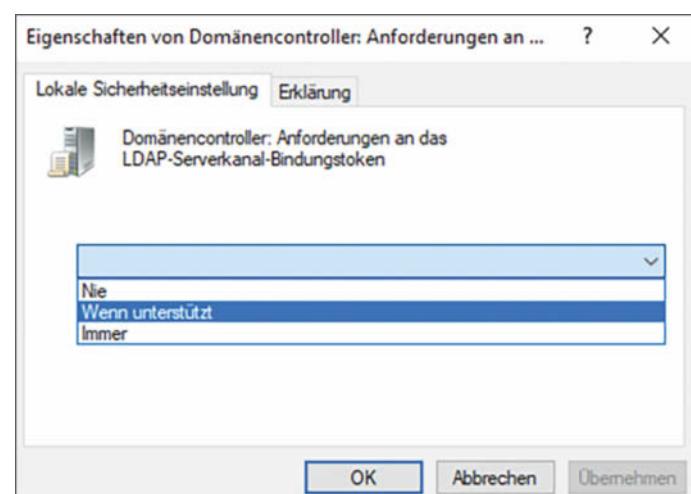
Dem gegenüber steht der SASL Bind. Bei SASL handelt es sich um ein komplexes Security-Framework, bei dem die beiden Kommunikationspartner untereinander vereinbaren können, welche Art der Authentifizierung zum Einsatz kommen soll. Stark vereinfacht dargestellt, kann ein SASL-Verbindungsaufbau wie folgt ablaufen:

- Der Client greift auf den Service zu und teilt mit, dass er SASL unterstützt und nun wissen möchte wie die Authentifizierung ablaufen soll.
- Der Server antwortet und erklärt, dass er auch SASL versteht und beispielsweise die SASL-Mechanismen GSSAPI, GSS\_SPNEGO, EXTERNAL und DIGEST-MD5 unterstützt.
- Der Client teilt dem Server mit, dass doch bitte GSSAPI zum Einsatz kommen soll.

- Der Server akzeptiert den Wunsch und teilt dem Client mit, dass mittels GSSAPI sowohl eine Kerberos- als auch NTLM-basierte Authentifizierung möglich sei.
- Der Client entscheidet sich für Kerberos und schickt dem Server ein entsprechendes Kerberos-Ticket, um die eigentliche Authentifizierung zu starten.

Sowohl Simple Bind als auch SASLBind lassen sich in einem SSL/TLS-Tunnel einsetzen. Hierbei wird die Integrität,

Authentizität und Vertraulichkeit der Daten über den SSL/TLS-Layer sichergestellt, so wie das zum Beispiel auch ein TLS-Layer für HTTP gewährleistet. Das Protokoll selbst wird nicht verändert. Der Standard-Port für LDAP over SSL/TLS (LDAPS) ist 636, alternativ können die beteiligten Kommunikationspartner einen Tunnel mit Hilfe von StartTLS auch auf dem LDAP-Port 389 aufbauen. Microsoft verwendet für die Authentifizierung von Benutzern innerhalb einer Domäne seit Windows 2000 das Protokoll Kerberos v5, das in RFC 4121 beschrieben ist. Der Zugriff auf das Active Directory erfolgt zumeist über das „Generic Security Service Application Program Interface“ (GSSAPI), welches eine weitere Abstraktionsebene innerhalb des SASL-Frameworks darstellt. Die genaue Implementierung mit allen Microsoft-spezifischen Erweiterungen ist in dem Dokument MS-KILE beschrieben (siehe [ct.de/yqb2](http://ct.de/yqb2)). Ein SASL Bind unterstützt grundsätzlich das Signieren und auch das Verschlüsseln der Daten.



SASL und LDAPS darf man teilweise auch kombinieren: Die Authentifizierung eines Benutzers gegenüber dem LDAP-Server kann auch innerhalb eines per SSL/TLS-gesicherten Tunnels sowohl mit einem Simple Bind als auch mit SASL erfolgen. Microsoft erlaubt aber kein Signieren oder Verschlüsseln der Daten auf dem SASL-Layer, wenn bereits ein SSL/TLS-Tunnel zum Einsatz kommt.

### Was tun?

Mit diesem Hintergrundwissen ausgestattet, sollten Sie sich als Administrator auf die Suche nach Verbindungen machen, die bisher über ungesicherte Wege am Domain-Controller ankommen. Zunächst brauchen Sie einen Überblick, welche Geräte und Anwendungen in Ihrem Netzwerk überhaupt mit dem Domain-Controller per LDAP kommunizieren – das sind neben Windows-Clients möglicherweise auch Linux-Clients oder Macs, die eine Benutzeranmeldung am Active Directory anbieten. Weitere Kandidaten sind Desktop- und Web-Anwendungen, die sich ins Active Directory integrieren und zum Beispiel Benutzer und Gruppen auslesen und daraus Berechtigungen innerhalb der Software ableiten. Möglicherweise nutzen auch Appliances (wie etwa Firewalls) oder Ihre Drucker und Kopierer das Active Directory – zum Beispiel für eine Anmeldung oder für das Adressbuch der drucker-eigenen Scan-to-Mail-Funktion.

Um herauszubekommen, welche Systeme mit welcher Methode auf die Active-Directory-Domain-Services zugreifen und ob es in Ihrem Netzwerk ein Problem wäre, wenn LDAP-Signaturen und Channel-Bindung verpflichtend wären, sollten Sie für einige Tage oder Wochen das Logging für Zugriffsversuche auf den Domain-Controllern einschalten. Dieses aktivieren Sie per Registry-Schlüssel:

```
reg add HKLM\SYSTEM\CurrentControlSet\services\NTDS\Diagnostics /v "16 LDAP Interface Events" /t REG_DWORD /d 2
```

Anschließend finden Sie in der Ereignisanzeige Einträge mit einer ID im Bereich von 2886 bis 2889 für Probleme mit der LDAP-Signatur und 3039 bis 3041 für Probleme mit der LDAP-Channel-Bindung. Tauchen hier nach dem Aktivieren des Loggings keine Einträge auf, weil Sie zum Beispiel eine reine Windows-Umgebung haben, können Sie die im Security

Advisory empfohlenen Einstellungen gefahrlos einschalten, ohne jemanden auszusperren.

### Sicherheit aktivieren

Wie sich die beiden Anforderungen auf Domain-Controllern umsetzen lassen, beschreibt Microsoft detailliert. Die Einstellungen für LDAP-Signaturen und LDAP-Channel-Bindung können in Registry-Schlüsseln gesteuert werden. Diese legen Sie unterhalb von

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

auf den Domain-Controllern an. Der Schlüssel `LDAPServerIntegrity` kann dabei die Werte 1 (keine Signierung notwendig) und 2 (Signierung immer notwendig) annehmen.

Für die LDAP-Channel-Bindung (CB) brauchen Sie den Schlüssel `LdapEnforceChannelBinding`. Dieser kann drei Werte enthalten: 0 (kein CB notwendig), 1 (CB erforderlich, wenn der Client es unterstützt) und 2 (CB immer erforderlich). Die meisten Administratoren werden diese Einstellungen per Gruppenrichtlinien setzen wollen: Die entsprechenden Richtlinien liegen unter „Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen“. Auf all Ihre Windows-Clients sollten Sie die Richtlinie „Netzwerksicherheit: Signuranforderungen für LDAP-Clients“ anwenden. Empfohlener Wert ist „Signatur erforderlich“. Die Domain-Controller setzen eine Signatur voraus, wenn Sie die Richtlinie „Domain-

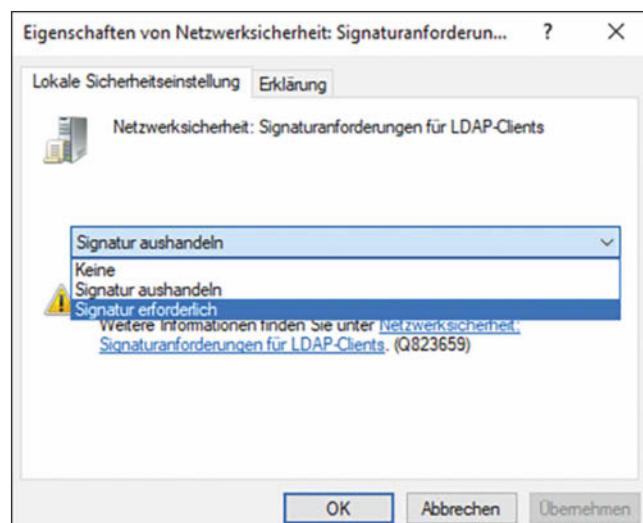
Controller: Signuranforderungen für LDAP-Server“ mit der Einstellung „Signatur erforderlich“ anwenden. Die Channel-Bindung aktivieren Sie mit der Richtlinie „Domain-Controller: Anforderungsgruppenrichtlinie für LDAP-Serverkanalbindungstoken“, empfohlener Wert ist „Wenn unterstützt“.

Alle Windows-Clients, die aktuell noch Support bekommen, verwenden bereits signierte LDAP-Verbindungen, die Domain-Controller erzwingen solche Verbindungen aber erst, wenn Sie als Administrator die oben stehenden Änderungen vornehmen. Die Anforderungen für LDAP-Channel-Bindung sind hingegen vergleichsweise neu und wurden erst zusammen mit einem Update für CVE-2017-8563 eingeführt [4]. Wenn Sie nur Windows 10 mit allen aktuellen Updates nutzen, sind Ihre Clients bereit dafür. Probleme gibt es nur, wenn Sie seit dem Jahr 2017 keine Updates mehr installiert haben und das Update für CVE-2017-8563 fehlt.

### Gemischte Umgebungen

Wenn Sie in den Logs Einträge finden, weil Sie Nicht-Windows-Clients, also beispielsweise Linux, andere Unix oder Appliances im Einsatz haben, müssen Sie unweigerlich etwas tiefer in die Materie einsteigen, bevor Sie die Richtlinien aktivieren. Solche Clients greifen oftmals in den Standardeinstellungen mit einem Simple Bind auf die Domain-Controller zu oder verwenden teilweise auch SASL, ohne aber für die Integrität der Daten zu sorgen.

Um herauszufinden, welche Verbindungsarten erlaubt sind, nachdem Sie die Signaturen im Domain-Controller erzwungen haben, können Sie die Richt-



Die signierte Übertragung in LDAP-Verbindungen kann man per Gruppenrichtlinie erzwingen. Empfohlener Wert ist „Signatur erforderlich“.

linien in einer Testumgebung aktivieren und auf einer Linux-Kommandozeile mit dem Werkzeug `ldapsearch` etwas experimentieren.

Zuerst eine Abfrage per Simple Bind (aktiviert durch die Option `-x`), also komplett ungesichert:

```
ldapsearch -xLLL -H ldap://ad1.win2016.test
-b 'DC=win2016,DC=test'
-D 'CN=Administrator,CN=Users,DC=win2016,DC=test'
-W samaccountname=Administrator DN
```

Der Server fragt zunächst nach dem Kennwort und beklagt sich dann erwartungsgemäß, weil keine Signierung stattfindet: `ldap_bind: Strong(er) authentication required (8).`

Im nächsten Schritt können Sie einen SASL Bind mit GSSAPI ausprobieren. Das aktivieren Sie mit der Option `-Y GSSAPI` und den SASL-Optionen „sign“ und „seal“, eingeschaltet durch `-O maxssf` mit

einem Wert größer 1. Damit ein SASL-Zugriff funktioniert, brauchen Sie zuerst auf dem Client ein gültiges Kerberos-Ticket. Ein solches erhalten Sie auf der Kommandozeile mit dem Werkzeug `kinit`:

```
kinit Administrator@WIN2016.TEST
```

Das Ticket liegt bereit und Sie können eine Suche auf dem Server anstoßen:

```
ldapsearch -LLLY GSSAPI
-O maxssf=256 -H ldap://ad1.win2016.test
-b 'DC=win2016,DC=test'
-W samaccountname=Administrator DN
```

Der Domain-Controller meldet:

```
SASL/GSSAPI authentication started
SASL username: Administrator@ [...]
SASL SSF: 256SASL data security
layer installed.
dn: CN=Administrator [...]
```

Der Zugriff war erfolgreich, da die Daten sowohl verschlüsselt als auch signiert übertragen werden. Da die Anforderung aus dem ADV190023 aber lediglich besagt, dass die Daten signiert sein müssen, sollte also ein Zugriff auch dann funktionieren, wenn lediglich die SASL-Option „sign“, also ohne „seal“ zum Einsatz kommt (`-O maxssf=1`):

```
ldapsearch -LLLY GSSAPI
-O maxssf=1
-H ldap://ad1.win2016.test
-b 'DC=win2016,DC=test'
-W samaccountname=Administrator DN
```

Wie erwartet klappt der Zugriff auch in diesem Fall. Versuchen Sie nun jedoch, auch auf das Signieren der Daten zu verzichten (`-O -maxssf=0`), so wird der Domain-Controller sich weigern, mit `ldapsearch` zu kommunizieren.

Festhalten kann man also, dass alle Clients, die eine Signierung der Daten auf dem SASL-Layer durchführen können,

DIE ONLINE-KONFERENZ VON HEISE

13.10.2020 | 10-17 UHR

# Agile Software-entwicklung im Unternehmen

Praxisvorträge von Expert\*innen

Softwareentwicklung

Inspect & Adapt

Softwarearchitektur

Remote Work

Usability Engineering

Schätzungen

Unternehmensweite Agilität



## Windows und Linux: SSL/TLS-Konfiguration

Ein Windows-Server, der als Domain-Controller arbeitet und LDAPS anbieten soll, benötigt zuerst ein X.509-Zertifikat. Dieses muss zuvor von einer Zertifizierungsstelle (CA) unterzeichnet werden und in der Konfiguration des LDAP-Dienstes hinterlegt werden. Häufig nutzt man in einer Domäne die Windows-eigene Zertifizierungsstelle. Eine detaillierte Anleitung, wie Sie den Domain-Controller mit SSL/TLS absichern können, finden Sie über ct.de/yqb2. Der Client, der nun eine gesicherte Verbindung durch einen SSL/TLS-Tunnel zum LDAP-Dienst aufbauen möchte, muss ebenfalls eine Kopie des öffentlichen Schlüssels besitzen und dem Zertifikat ausdrücklich vertrauen. Wie dies

genau abläuft, hängt stark von dem eingesetzten Client-System ab. Bei Hardware-Appliances kann man den öffentlichen Schlüssel zum Beispiel oft über eine Weboberfläche hinterlegen. Im Folgenden kommt als Beispiel ein Linux-System mit Red Hat Enterprise Linux um Einsatz.

Unter Linux kopieren Sie das CA-Zertifikat in den OpenLDAP-Ordner /etc/openldap/cacerts und legen eine weitere Kopie in /etc/pki/ca-trust/extracted/openssl/ ab. Als Dateiname für das Zertifikat der CA wird in diesem Beispiel ad-ca.crt verwendet. Anschließend fügen Sie in der OpenLDAP-Konfigurationsdatei /etc/openldap/ldap.conf die folgende Zeile hinzu:

```
TLS_CACERT /etc/openldap/cacerts/➥
➥ad-ca.crt
```

Damit weiß die OpenLDAP-Bibliothek, auf welches Stammzertifikat sie zurückgreifen muss, um beim Aufbau eines SSL/TLS-Tunnels das Zertifikat des LDAP-Servers zu verifizieren. Abschließend rufen Sie noch den folgenden Befehl auf:

```
update-ca-trust
```

Hiermit wird das neue CA-Zertifikat dem systemweiten Zertifikatsspeicher hinzugefügt, sodass auch andere Applikationen, die auf Basis von OpenSSL arbeiten, dieser Zertifizierungsstelle vertrauen.

aus dann ohne Probleme mit dem Active-Directory kommunizieren können, wenn auf den Domain-Controllern die Option für die LDAP-Signierung erzwungen wird. Eine Verschlüsselung der Daten mithilfe von SSL/TLS ist nicht zwingend erforderlich.

Wie sieht es aber aus, wenn ein Client absolut kein SASL unterstützt, wie es beispielsweise bei diversen (alten) Hardware-Appliances der Fall ist? Im schlechtesten Fall unterstützt der Client weder SASL noch eine Verbindung über einen SSL/TLS-Tunnel. Dann sollten Sie sich überlegen, ob es nicht an der Zeit ist, sich vom lieb gewonnenen Gerät zu trennen. Eine ungesicherte Verbindung ist nicht mehr zeitgemäß!

Im günstigen Fall wird eine LDAP-Verbindung zu einem Domain-Controller per Simple Bind mit zusätzlichem SSL/TLS-Tunnel angeboten. Hierfür sind allerdings einige zusätzliche Anforderungen sowohl auf der Server- als auch der Client-Seite zu erfüllen. Weitere Informationen hierzu finden Sie im Kasten „Windows und Linux SSL/TLS-Konfiguration“.

Wenn Sie sich für LDAP über SSL/TLS entschieden haben und die Zertifikate auf Server und Client eingerichtet sind, sollten Sie sich mit der LDAP-Channel-Bindung auseinandersetzen. Diese können Sie in Richtlinie oder Registry-Schlüssel in zwei Stufen aktivieren: entweder immer, oder nur dann, wenn es der Client unterstützt. Letzteres empfiehlt Microsoft aktuell.

Zum Experimentieren können Sie auf einem Linux-System wieder ldapsearch auf der Kommandozeile benutzen. Aktivieren Sie in der Testumgebung zunächst die verpflichtende Channel-Bindung, um zu sehen, was dann noch möglich ist. Um zu sehen, wie ältere Clients reagieren, sollten Sie zunächst Versionen von openldap und cyrus-sasl ausprobieren, die vor Juni 2020 veröffentlicht wurden. Probieren Sie mit den etwas älteren Paketen zunächst einen Simple Bind über LDAPS auf Port 636:

```
ldapsearch -LLLx ↵
➥-H ldaps://ad1.win2016.test ↵
➥-b 'DC=win2016,DC=test' ↵
➥samaccountname=Administrator DN ↵
➥-D 'CN=Administrator,CN=Users,➥
➥DC=win2016,DC=test' -W
```

Dieser Aufruf ist genauso erfolgreich wie ein Simple-Bind über StartTLS auf Port 389:

```
ldapsearch -LLLx -ZZ ↵
➥-H ldap://ad1.win2016.test ↵
➥-b 'DC=win2016,DC=test' ↵
➥samaccountname=Administrator DN ↵
➥-D 'CN=Administrator,CN=Users,➥
➥DC=win2016,DC=test' -W
```

Ein Simple Bind über SSL/TLS-Tunnel funktioniert immer, unabhängig von der Channel-Bindung. Eine hilfreiche Erkenntnis, denn eine solche Verbindung ist hinreichend sicher. Anders hingegen sieht

es aus, wenn Sie versuchen, sich mithilfe von SASL und Kerberos durch den SSL/TLS-Tunnel anzumelden. Beschaffen Sie sich erst ein Kerberos-Ticket:

```
kinit Administrator@WIN2016.TEST
```

Dann erfolgt der eigentliche Zugriff auf den LDAP-Server mit Hilfe von GSSAPI/Kerberos:

```
ldapsearch -LLL GSSAPI ↵
➥-H ldaps://ad1.win2016.test ↵
➥-b 'DC=win2016,DC=test' ↵
➥samaccountname=Administrator DN ↵
➥-O maxssf=256
```

Der Server beklagt sich über vermeintlich ungültige Zugangsdaten, auch über StartTLS haben Sie keinen Erfolg. Setzen Sie die Richtlinie für Channel-Bindung im Domain-Controller dagegen auf „Wenn unterstützt“, funktionieren diese Zugriffe wieder.

Wenn Sie SSL/TLS mit verpflichtender Channel-Bindung nutzen wollen, um Angriffe durch diese Lücke zu unterbinden, brauchen Sie aktuelle Client-Software. Die beiden Software-Pakete openldap und cyrus-sasl unterstützen erst seit Juni 2020 die LDAP-Channel-Bindung und können seitdem auch mit Channel-Binding-Tokens (CBT) umgehen. Weitere Informationen hierzu finden Sie in den entsprechenden Feature Requests in den Bug-Trackern der beiden Komponenten (siehe ct.de/yqb2). Wenn

Sie das letzte Experiment mit aktuellen Softwarepaketen wiederholen und die Bindung im Domain-Controller erzwungen haben, können Sie problemlos zugreifen.

Wichtig ist, dass bei diesen SASL-Zugriffen über SSL/TLS die Signierung der LDAP-Daten ausschließlich auf dem TLS-Layer stattfindet und auf dem SASL-Layer explizit durch den Einsatz der Option `-0 maxssf=0` deaktiviert wurde. Versuchen Sie, die Daten sowohl auf dem SASL-Layer als auch mit Hilfe von SSL/TLS zu signieren und zu verschlüsseln, so wird dies zu einer Fehlermeldung führen, wie das folgende Experiment zeigt:

```
ldapsearch -LLL GSSAPI ↵
↳-H ldap://ad1.win2016.test ↵
↳-b 'DC=win2016,DC=test' ↵
↳samaccountname=Administrator DN ↵
↳-0 minssf=256
```

Der Server antwortet mit dem Fehler:

```
SASL data security layer installed.
ldap_result: Can't contact LDAP server
```

Das Zwischenergebnis: Wenn Sie nur Simple Binds über SSL/TLS durchführen, brauchen Sie sich um Channel-Bindung nicht zu kümmern. Wenn Sie dagegen SASL auf SSL/TLS einsetzen möchten und gleichzeitig die Channel-Bindung verpflichtend machen wollen, brauchen Sie unter Linux sehr frische Softwarepakete.

## Fazit

Die Panik rund um das Advisory ADV190023 ist unbegründet. Wann und ob Microsoft überhaupt die Anforderungen durch ein Update automatisch auf allen Domain-Controllern aktiviert, steht aktuell nicht fest. Die Ankündigung wurde schon mehrfach verschoben und Microsoft selbst schreibt, dass diesbezüglich keine Änderungen in der nahen Zukunft zu erwarten sind. Sicher ist in jedem Fall: Wenn Sie die Richtlinien einmal bearbeitet haben, werden sie nicht überschrieben. Linux und Appliances auszusperren war keinesfalls das Ziel der Empfehlungen.

Die Hinweise aus Redmond sind aber eine gute Gelegenheit, sich mit dem Thema zu befassen und sichere Übertragungen zum Domain-Controller verpflichtend zu aktivieren – alles andere ist heute nicht mehr zeitgemäß. Dafür müssen Sie herausfinden, was Ihre Clients können. Die häufigste Angst können die Experimente auf alle Fälle nehmen: Der Einsatz von SSL/TLS ist nicht zwingend notwendig, um auch in Zukunft erfolgreich mit einem Active Directory kommunizieren zu können. Auch der Einsatz von SASL wird weiterhin zum Erfolg führen, solange sichergestellt ist, dass die Daten auf dem SASL-Layer signiert sind. Beherrscht auch nur einer Ihrer Clients ausschließlich Simple Bind, kommen Sie aber nicht umhin, SSL/TLS einzurichten. Richtig kompliziert wird es, wenn SASL innerhalb eines Tunnels zum Einsatz kommen soll. Dann müssen Sie sich auch mit der LDAP-Channel-Bindung im Active Directory auseinandersetzen. In jedem Fall erhöhen Sie die Sicherheit Ihres Netzwerks und machen es Angreifern schwerer, wenn Sie ungeschützten LDAP-Verkehr verhindern.

(jam@ct.de) 

**Dokumentation und ADV190023:** [ct.de/yqb2](http://ct.de/yqb2)

# Workshops 2020

## Vertriebsperformance 4.0

19. Oktober 2020 / Hannover

Erfahren Sie in diesem Workshop, weshalb alte Vertriebssteuerungsmodelle nicht mehr funktionieren werden und was es braucht, damit wir für Vertrieb 4.0 gerüstet sind.



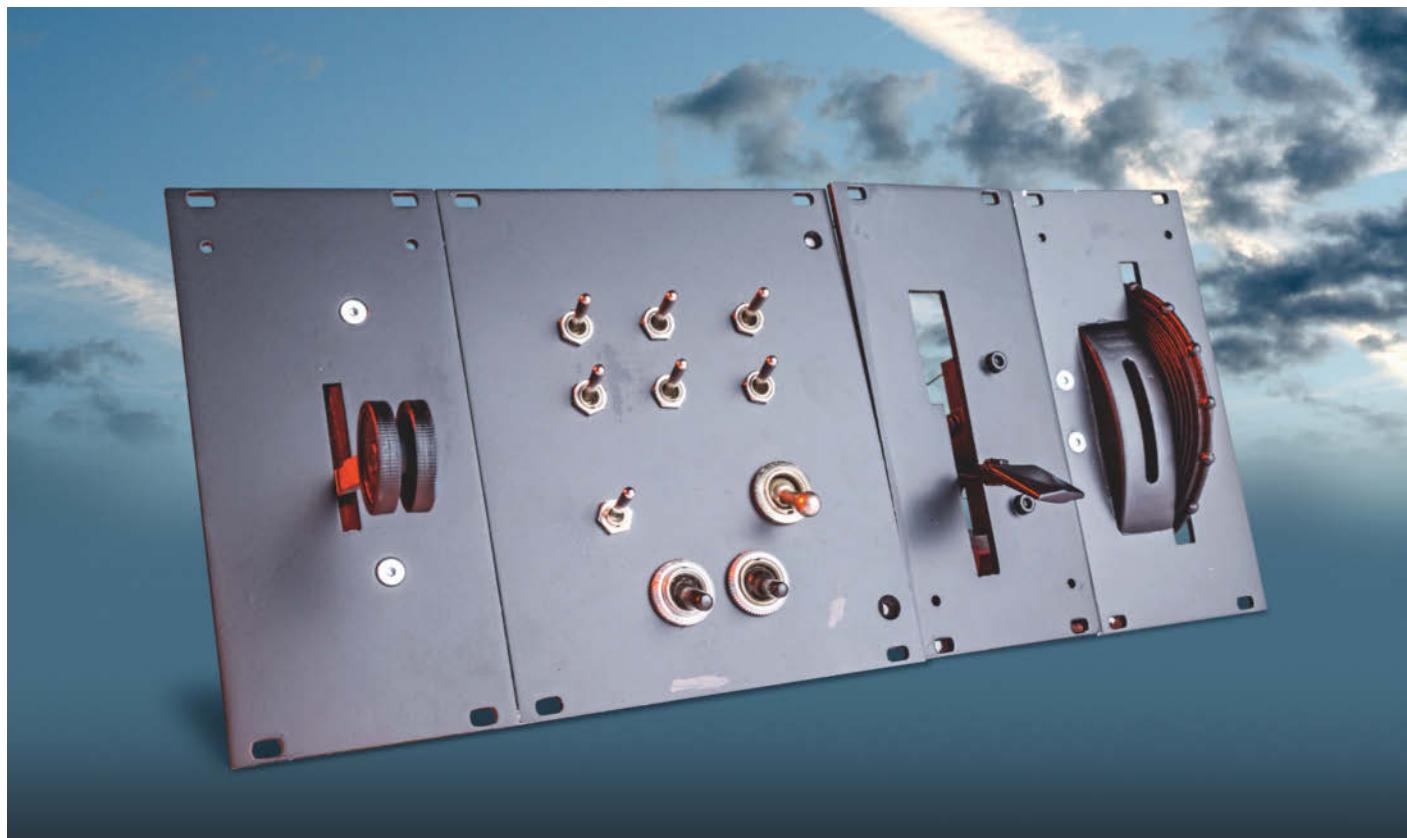
## Social Selling im B2B

27. Oktober 2020 / Hannover

In diesem Workshop lernen Sie, Ihre eigene Social Selling-Strategie zu entwickeln und diese erfolgversprechend mit den bestehenden Sales Aktivitäten zu verknüpfen.



Weitere Infos unter:  
<http://www.heise-events.de/workshops>



# Fliegender Frederick

**Ein selbst gebauter Controller für den Flugsimulator auf Basis des Arduino Micro**

**Mit den richtigen Knöpfen und Hebeln fühlt sich Fliegen mit dem Microsoft Flugsimulator 2020 noch authentischer an. Ein passender USB-Controller mit Arduino Micro ist schnell gebaut und bindet Trimmrad, Landeklappen- und Fahrwerkshebel einer Cessna an den Rechner an.**

**Von Pina Merkert**

**B**aut man Bedienelemente eines Flugzeug-Cockpits mit physischen Hebeln, Rädchen und Schaltern nach, holt man den virtuellen Raum des Flugsimulators ein Stück weit in die Realität. Die Simulation fühlt sich authentischer an und das Fluggefühl wird intensiver. Da jeder virtuell fliegende Pilot ein anderes Flugzeug mag, hat jeder auch andere Vorstellungen für die perfekte Form der Bedienelemente – und die setzt man am besten mit einem selbst gebauten Controller um. Mit einem Arduino Micro als Herzstück geht das einfach und kostengünstig.

Gibt sich der Arduino als Tastatur aus [1], kann man jedes Mal, wenn am selbst gebauten Controller ein Schalter umgelegt wird, einen Tastendruck oder eine Tasten-

kombination an den Rechner schicken. Moderne Betriebssysteme brauchen für solche „Human Interface Devices“ (HID) keine besonderen Treiber und über die Einstellungen im Flugsimulator und in anderen Spielen kann man bequem definieren, was passieren soll, wenn der Arduino in die Tasten haut.

Ein Mikrocontroller kann sich nur dann als HID ausgeben, wenn er die USB-Kommunikation selbst abwickelt. Steckt wie beim Arduino Uno oder Nano für USB ein Extra-Chip auf dem Board, lässt sich damit kein HID emulieren. Ein Atmel MEGA 32U4, der als HID arbeiten kann, ist auf einem Arduino Micro, Leonardo oder auf dem inoffiziellen 3,3-V-Klon „Pro Micro“ verlötet. Wir haben einen

Arduino Micro verwendet, der 16 GPIO-Pins zur Verfügung stellt. Die waren uns aber nicht genug, weshalb wir per I<sup>2</sup>C einen MCP23017 angebunden haben, der weitere 16 GPIO-Pins zur Verfügung stellt (für I<sup>2</sup>C gehen dafür am Arduino zwei GPIO verloren).

Wir haben unseren Controller „Fliegender Frederick“ getauft. Wenn Sie wollen, können Sie ihn gern nachbauen – Vorlagen und Beispiele dazu finden Sie auf ct.de/yrpp. Alle einzelnen Punkte in einer Schritt-für-Schritt-Anleitung aufzulisten würde aber den Umfang dieses Artikels sprengen. Da Ihre Werkstatt wahrscheinlich anders als unsere ausgestattet ist, müssen Sie für einen Eins-zu-eins-Nachbau eigene Wege finden, die Fronten auszuschneiden oder die Befestigungen herzustellen. Außerdem macht das Projekt ohnehin mehr Spaß, wenn Sie unseren Frederick nur als Vorlage benutzen und Ihren Controller an die Fundstücke in der eigenen Bastelkiste und die eigenen Bedürfnisse anpassen. Vielleicht ist Ihr Lieblingsflugzeug ja gar keine Cessna und die Hebel müssen etwas anders aussehen.

Unser Controller nutzt genau wie der Lautstärkeregler aus c't 18 [2] einen Drehencoder. Der registriert Drehungen am Trimmrad, mit dem man die Nase des Flugzeugs nach oben oder unten neigt. Die Verschaltung haben wir eins zu eins vom Lautstärkeregler übernommen, da die dort beschriebene kleine Platine unübersichtlichen Kabelverhau an den Anschlüssen verhindert. Die restlichen Bedienelemente sind elektrisch gesehen einfache Schalter, sehen aber teilweise anders aus.



**Den Fahrwerkshebel einer Cessna haben wir originalgetreu nachgebaut. Damit der Hebel genug Hub bekommt, bewegt er keinen Kippschalter, sondern einen Schiebeschalter.**

Für den Hebel fürs Ausfahren des Fahrwerks haben wir beispielsweise einen Schiebeschalter mit einem langen Hebelarm verheiratet und ans Ende zwei 3D gedruckte Kunststoffscheiben geschraubt. Das Ergebnis sieht dem Fahrwerkshebel einer Cessna täuschend ähnlich.

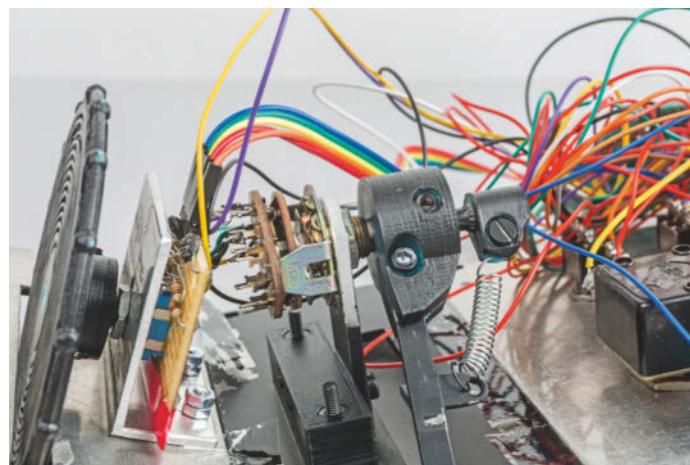
Für die Landeklappen hat eine Cessna einen Hebel, der vier Stellungen annehmen kann. Ihn haben wir mit einem um 90° gedreht eingebauten Drehschalter umgesetzt. An seiner Welle setzt ein Hebelarm an, der eine Besonderheit aufweist: Offensichtlich als Schutz vor versehentlich zu extrem gehobenen Landeklappen kann man ihn mit einer geraden Bewegung nach unten nur auf die erste Stufe stellen. Für größere Bremswirkung muss der Pilot ihn etwas zur Seite schieben und dann nach unten drücken. Damit unser Schalter in der geschützten Stellung einrastet, zieht eine Zugfeder den Hebel-

arm zur Welle. Eine Stufe im Ausschnitt für den Hebel in der Frontplatte sperrt den Hebel für unüberlegte Bewegungen. Der Flugsimulator-Pilot muss den Hebel also gegen die Federkraft nach rechts drücken, um Stufe 2 oder 3 zu erreichen.

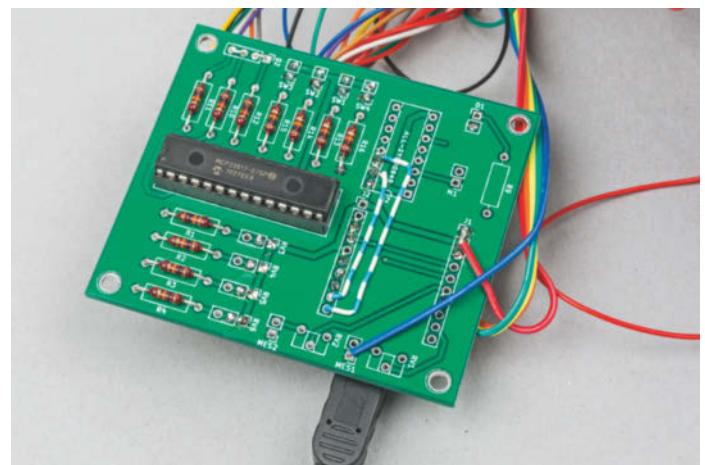
### Platinen-Recycling

Die beiden Drähte für die I<sup>2</sup>C-Verbindung zum MCP23017 und die Pulldown-Widerstände an allen GPIO-Pins baut man leicht auf einer Lochrasterplatine auf. Wir hatten jedoch für ein anderes Projekt in der Redaktion vor einiger Zeit Platinen fertigen lassen, die einen MCP23017 und diverse Widerstände aufnehmen können. Da man bei Platinenfertigern immer gleich einen ganzen Stapel bekommt, lagen noch mehrere dieser Platinen ungenutzt im Lager. Wir haben sie, wo es sinnvoll war, bestückt und auf einige ungenutzte Bohrlöcher huckepack den Arduino Micro aufgelötet. Die übrigen Platinen in unserem Lager verschenken wir an die ersten zehn Leser, die mit einer netten Mail an pmk@ct.de Bedarf anmelden. Die Gerber-Files für das Platinenlayout finden Sie unter ct.de/yrpp – da die Platine aber nur halb passt, lohnt es sich allerdings nicht, sie ohne Änderung fertigen zu lassen. Falls Sie größer in die Controllerproduktion einsteigen möchten, können Sie aber gern unsere KiCAD-Datei als Basis nehmen.

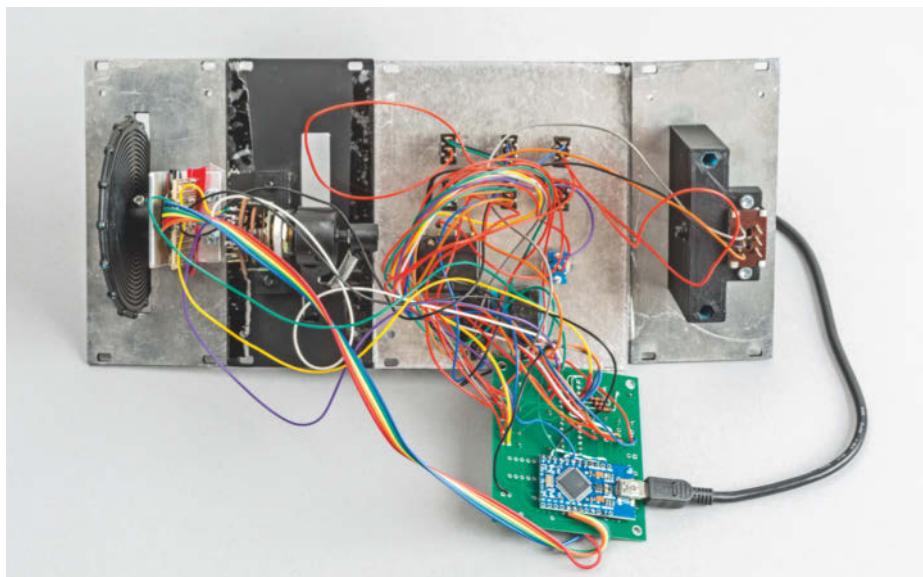
Außer beim Drehencoder (die Schleifkontakte sind besonders anfällig für Prelen) haben wir die Schalter alle in Software entprellt und auf Kondensatoren verzichtet. Falls Ihnen eine Hardware-Lösung



**Der Hebel für die Landeklappen verhindert Fehlbedienungen mit einer mechanischen Sperrung: Die Feder zieht den Hebel nach rechts, sodass er bei Stufe 1 auf einer Kante des Ausschnitts in der Frontplatte aufliegt. Wer weiter schalten will, muss ihn erst nach links und dann nach unten bewegen.**



**Unsere zweckentfremdete Platine mit dem MCP23017 trägt die meisten Pulldown-Widerstände. Nötig ist sie aber nicht. Eine etwas breitere Loch- oder Streifenrasterplatine reicht ebenfalls. Wir verschenken je eine Platine an die ersten zehn Leser, die uns per Mail fragen.**



**Drehencoder, Drehschalter und Schiebeschalter sind in ungewöhnlicher Orientierung hinter den Aluminium-Frontplatten verschraubt.**

lieber ist, können Sie sich an den Kapazitäten und Widerstandswerten unserer Entprellung für den Raspi orientieren [3].

## Mechanik

Trimmrad, Fahrwerkshebel und der Landeklappen-Wahlschalter haben wir jeweils mit einer eigenen Frontplatte aus 2 Millimeter dickem Aluminium verschraubt. So entstehen Module, die man beliebig anordnen und bei Bedarf auch noch erweitern kann. Eine vierte, etwas breitere Aluplatte nimmt noch zehn zusätzliche Kippschalter auf, die weitere Funktionen des Flugzeugs schalten können. Sechs der Kippschalter haben eine kompakte Bauform und passen so in zwei Reihen zu je drei Stück. Darunter finden drei größere Kippschalter Platz, die wir aus alten Geräten ausgebaut haben. Die etwas antiken Schalter bieten ein sehr befriedigendes Schaltgefühl, da sie etwas schwerer gehen und mit Macht in der neuen Stellung einrasten. Das Schalter-Recycling spart nicht nur Geld, die unterschiedlichen Druckpunkte sorgen auch für haptische Abwechslung und somit mehr Spaß. Aus denselben Gründen haben wir als zehnten Schalter keinen Umschalter eingesetzt, sondern einen Taster, allerdings mit einem Hebel zum Herunterdrücken, statt eines Knopfs zum Eindrücken. Dadurch sieht er aus wie die anderen Kippschalter, fühlt sich aber anders an.

Die Schalter und Regler sind teilweise anders eingebaut, als ihre Datenblätter spezifizieren. Beispielsweise hängen

Drehencoder und Drehschalter jeweils horizontal hinter der Frontplatte. Die Welle ragt nicht wie üblich vorn aus dem Gehäuse, stattdessen interagiert der Pilot mit einem angeschaubten Rad oder Hebel. Beim Fahrwerkshebel schiebt der Hebel einen Schiebeschalter in seine Endstellungen. Da sich der Hebel entlang einer Kreisbahn bewegt und sich der Schiebeschalter linear verschiebt, gleicht ein über den Zapfen des Schiebeschalters gestülpter Schuh die Ungenauigkeit aus. Die Drehachse von Hebel und Schuh bildet jeweils eine Schraube.

Um die Bauelemente so ungewöhnlich zu befestigen, haben wir diverse Bauteile entworfen und 3D-gedruckt. Alle CAD-Dateien der Designs und fertige STLs für den 3D-Drucker finden Sie über [ct.de/yrpp](http://ct.de/yrpp). Unsere Bauteile stammen alleamt aus der Bastelkiste. Wenn Sie einen eigenen Controller bauen wollen, müssen Sie die Designs also eventuell an Ihre Bauteile anpassen. Eine Einführung in OpenSCAD finden Sie in [4], für einen Block am Trimmrad haben wir auch FreeCAD [5] verwendet. Wir haben ein Video zum Bau aufgenommen, das Sie ebenfalls über [ct.de/yrpp](http://ct.de/yrpp) finden.

## Programmcode

Den Programmcode der Firmware für den Frederick finden Sie im GitHub-Repositorium über [ct.de/yrpp](http://ct.de/yrpp). Die Architektur ist Arduino-Standardkost: In `setup()` konfiguriert der Code die vielen GPIOs für die

Schalter als Eingang. Die `loop()`-Funktion pollt die Schalter und speichert deren gemeldete Stellung zwischen, um per Software zu entprellen. Wegen der Prellung lohnt es sich auch nicht, auf Interrupts zu setzen; außerdem hat der Arduino ohnehin wenig zu rechnen. Den endlichen Automaten für den Drehencoder haben wir einfach von [2] übernommen.

Um die Kommunikation mit dem MCP23017 per I<sup>2</sup>C kümmert sich die Wire-Bibliothek [6]. Die Funktion `i2cDigitalRead(unsigned short pinNo)` in `i2cMCP.cpp` filtert einzelne Bits aus den Bytes, die der MCP23017 für seine Eingänge liefert. Der Code in der `loop()` in `main.cpp` nutzt `i2cDigitalRead()` und `digitalRead()` für die direkt am Arduino angeschlossenen Schalter im gleichen Format.

## Entprellen per Software

Wir haben uns die Widerstände und Kondensatoren fürs Entprellen der Schalter gespart und erledigen das per Software. Zur Erinnerung: Beim Prellen schaltet ein Schalter nicht einmal um, sondern wechselt in schneller Folge zwischen hohem und niedrigem Pegel, bis sich nach üblicherweise maximal 250 Millisekunden ein stabiler Pegel eingestellt hat. Da der Code die Schalter alle 25 Millisekunden abfragt, registriert er beim Umschalten ein wildes Auf und Ab, das sich nach einer Weile stabilisiert. Die Software macht bei dieser Hektik nicht mit, sondern wartet, bis sie acht Mal den gleichen Wert gelesen hat. Erst dann geht sie von einem gekippten Schalter aus. Das verzögert die Reaktion um circa 1/4 Sekunde – ausreichend schnell, dass es einem noch so vorkommt, als würde der Controller sofort reagieren.

Für das Warten auf stabile Pegel enthält der Code zusätzlich zur Stellung ein `history`-Byte für jeden Schalter. In C++ sieht das für den ersten Schalter so aus:

```
unsigned char switchA0History = 0;
bool switchA0State = false;
```

Um Protokoll kümmert sich die Funktion `debounce()`. Damit sie mit jedem Schalter funktioniert, nimmt sie einen Zeiger auf ein `history`-Byte und einen Zeiger auf den Status an, außerdem den gerade gelesenen Wert (die Rückgabe von `i2cDigitalRead()` oder `digitalRead()`). Das `history`-Byte verwendet die Funktion, um 8 Werte als einzelne Bits zu speichern. Daher schiebt sie mit einer Shift-Opera-

tion ( $\ll 1$ ) alle Bits zunächst um eine Stelle nach links. Das älteste Bit fällt dabei weg und Bit 0 ist dafür eine 0. An dieser Stelle (Bit 0) speichert sie nun den gelesenen Wert. C stellt boolesche Variablen intern als Integer 0 oder 1 dar. Konvertiert man das zu einem Byte, kommen also nur die Werte 0b00000000 und 0b00000001 vor. Bit 1 bis 7 sind bei diesem Byte also immer 0. Verrechnet man die verschobene history also über ein bitweises Oder | mit dem Boolean, können sich Bit 1 bis 7 also nicht verändern. Da die verschobene history an Stelle 0 aber garantiert eine 0 stehen hat, schreibt das Oder dort nur die 0 oder 1 aus dem Boolean hin.

Mit einem so geführten Protokoll ist es einfach, auf eindeutige Schalterveränderungen zu warten. Solange in der History Nullen und Einsen gemischt vorkommen, bleibt `debounce()` beim alten Wert für state. Wenn aber nur Nullen oder nur Einsen in der history stehen, setzt die Funktion state neu und gibt auch den geänderten Wert zurück:

```
bool debounce(unsigned char* history,
  bool* state, bool reading) {
  *history = (((*history) << 1) |
    (unsigned char) reading);
  switch (*history) {
  case 0b00000000: *state = false;
    break;
  case 0b11111111: *state = true;
    break;
  }
  return *state;
}
```

Der Code überwacht für alle Schalter, ob sich der state ändert und ruft bei Bedarf eine Funktion auf. Um die Überwachung kümmert sich `detectSwitchToggle()`. Um duplizierten Code zu vermeiden, nutzt sie ebenfalls Zeiger auf history und state und für den Funktionsaufruf beim Umschalten einen Zeiger auf eine Callback-Funktion:

```
void detectSwitchToggle(
  unsigned char* history,
  bool* state,
  bool reading,
  void (*callback)(bool state)) {
  bool oldState = *state;
  if (oldState != debounce(history,
    state, reading)) {
    callback(*state);
  }
}
```

## Arduino tippt

Was beim Umschalten passiert, steht in der Datei `keypresses.cpp`. Die Reaktion aufs Umschalten des ersten Kippschalters sieht beispielsweise so aus:

```
void switchA0(bool state) {
  if (state) {
    Serial.println("A0 ON");
    Keyboard.press(KEY_LEFT_ALT);
    Keyboard.press('A');
    Keyboard.releaseAll();
  } else {
    Serial.println("A0 OFF");
    Keyboard.press(KEY_LEFT_ALT);
    Keyboard.press(KEY_RIGHT_SHIFT);
    Keyboard.press('A');
    Keyboard.releaseAll();
  }
}
```

Die Funktion nutzt das per `Keyboard.begin()` initialisierte Tastatur-Objekt aus der HID-Project-Bibliothek. Der Arduino „tippt“ hier Tastenkombinationen: Ein `Keyboard.press()` entspricht dem Herunterdrücken einer Taste einer Tastatur. Die Funktion nimmt entweder Integer-Konstanten für Sondertasten wie `KEY_LEFT_ALT` entgegen (die Arduino-Doku zu `Keyboard.h` listet auf, welche Konstanten zur Verfügung stehen, siehe ct.de/yrpp) oder druckbare Zeichen wie 'a' oder '0'. Die Funktion `Keyboard.releaseAll()` lässt alle Tasten wieder los. Die Arduino-Beispiele bauen zwischen dem Drücken und dem Loslassen stets noch ein `delay()` ein. In unseren Tests hat es aber auch ohne `delay()` einwandfrei funktioniert.

## Abfrageintervall

Um eine schnelle Reaktion auf Eingaben zu garantieren, verzichtet der Code in `loop()` auf Aufrufe von `delay()`. Stattdessen protokolliert er in Timern wie `unsigned long debounceTimer`, wann die letzte Interaktion stattfand. Es reicht dann ein Vergleich mit zwischen der von `millis()` gelieferten Zeit mit der um ein Offset erhöhten Zeit der letzten Interaktion:

```
if (millis() > debounceTimer + 25) {
  debounceTimer = millis();
  detectSwitchToggle(
    &switchA0History,
    &switchA0State,
    digitalRead(SWITCH_A_0_PIN),
    switchA0);
}
```

Ohne Warten braucht der Arduino weniger als 5 Millisekunden für einen Durchlauf der `loop()`. Die Schalter fragt der Code aber frühestens alle 25 Millisekunden ab, sodass fürs Entprellen genug Zeit verstreicht.

Stattdessen hätten wir auch mit je einer 4 Byte langen `history` arbeiten können, 8 gelesene Werte im Abstand von 25 Millisekunden reichten im Test aber bereits für ein fehlerfreies Entprellen.

Das gleiche Vorgehen mit einem anderen Timer nutzt der Code auch, um den Status aller Schalter außer dem Trimmrad alle 20 Sekunden auf die serielle Schnittstelle zu schreiben. Zum Debuggen ist die Ausgabe praktisch und den Flugsimulator stört das zusätzliche serielle Interface nicht.

## Spaßige Bastelei

Egal, ob Sie den fliegenden Frederick nachbauen oder nur als Ideengeber nutzen: Die Bastelei macht Spaß, weil sie viel Modellbau umfasst und die überschaubare Elektronik wenig Stolperfallen auslegt. Das Grundprinzip bleibt nämlich für alle Varianten gleich: Der billige Arduino Micro übernimmt die USB-Kommunikation als HID und tippt als virtuelle Tastatur bei jeder Hebelbewegung. Für eine Handvoll Schalter reichen die Arduino-GPIOS aus, sodass Sie sich für kleine Interfaces den MCP23017 und die Platine sparen können. Wir haben am fliegenden Frederick mit Unterbrechungen circa sechs Wochen lang gebastelt. Planen Sie also ausreichend Zeit für das Projekt ein. Dafür dürfen Sie sich auf doppelte Freude einstellen: zuerst Bastelspaß, bis alle Spezialschalter funktionieren, und danach der Spaß am Fliegen mit jeder Menge haptischen Schaltern. (pmk@ct.de) ct

## Literatur

- [1] Tim Gerber, Anschläge, PC-Programme mit Arduino steuern, c't 8/2016, S. 156
- [2] Pina Merkert, Drehknopf bis 11, Arduino Micro lernt Lautstärkeregler, c't 18/2020, S. 154
- [3] Pina Merkert, Versuchs-Hut, So verdrahten Sie Schalter, Taster und LEDs am Rasp, c't 17/2020, S. 26
- [4] Pina Merkert, OpenSCAD, Modelle für den 3D-Druck programmieren, c't 12/2017, S. 172
- [5] Christoph Schmitt, CAD-Content, 3D-Konstruktion mit FreeCAD, c't 13/2018, S. 140
- [6] Pina Merkert, Mehr I/O zum Basteln, Sehr viele GPIO-Pins an Arduino, Raspi und ESP, c't 15/2020, S. 146

**Repository bei GitHub, 3D-Designs,**  
**Link zum Video: ct.de/yrpp**



# Geregelter Zutritt

## Flexible Autorisierung mit dem Open Policy Agent

**Was ein Anwender in einer Software darf, wird traditionell anhand eines Rollenmodells entschieden. Für die vielen Regeln in einem Unternehmen ist das aber meist zu starr. Mit dem Open Policy Agent steuern Sie flexibler, wer was darf.**

Von Jan Mahn

**J**ede Anwendung, auf die mehr als ein Anwender zugreifen soll, muss immer wieder die folgende, alles entscheidende Frage beantworten: Darf dieser Benutzer

die gewünschte Aktion wirklich ausführen? In Unternehmensanwendungen hängt von der richtigen Beantwortung dieser Frage viel ab. Wer was darf, entscheidet meist nicht der Entwickler der Software selbst – er bekommt vielmehr die Regeln, die im Unternehmen gelten, in ganzen Sätzen auf den Tisch und hat die Aufgabe, sie für die Anwendung zu übersetzen. Solche Regeln können etwa so aussehen:

- Mitarbeiter aus der Einkaufsabteilung dürfen Aufträge bis 1000 Euro freigeben.
- Der stellvertretende Leiter darf bis 10.000 Euro freigeben.
- Der Leiter der Einkaufsabteilung darf alles freigeben.

Um sich dem Problem zu nähern, greift man meist zu einem Modell, das solche Berechtigungen vereinfacht. Viele Ent-

wickler entscheiden sich für ein rollenbasiertes Modell (Role Based Access Control, RBAC). In einem solchen System gibt es Benutzer, Gruppen und Rollen. Ein Nutzer kann Mitglied mehrerer Gruppen sein. Benutzern und Gruppen kann man Rollen zuweisen – die Anwendung entscheidet dann jeweils, ob die Rolle vorhanden ist, die zum Ausführen einer Aktion notwendig ist. Im besten Fall kann man die Berechtigungsprüfung sogar an eine eigene RBAC-Komponente auslagern, sodass sich Code der Anwendung und die Regeln des Unternehmens nicht vermischen.

Für die drei oben formulierten Regeln bräuchte man bereits drei Rollen, zum Beispiel `purchase_employee`, `purchase_deputy` und `purchase_head`. An die Grenzen von RBAC stößt man aber spätestens, wenn sich die Entscheider eine weitere

Regel ausgedacht haben und sie dem Entwickler auf den Tisch legen:

- Mitarbeiter der Einkaufsabteilung dürfen Aufträge beliebiger Höhe freigeben, wenn der Lieferant in der Liste der Stammlieferanten steht.

Ein System, das nur die Rollen des Benutzers auswertet, kann eine solche Entscheidung unmöglich treffen – es müssen weitere Attribute des Auftrags ausgewertet werden, einige sprechen dann von „Attribute-based Access Control“ (ABAC). Wenn bisher nur auf die Existenz einer Rolle geprüft wurde, muss der Entwickler hier also mitten in der Anwendung tricksen und zusätzlich zur Prüfung auf die Rolle `purchase_employee` den Auftrag unter die Lupe nehmen und dann mit einer `if`-Anweisung auf unterschiedliche Lieferanten reagieren. Hat man einmal damit begonnen, sol-

che Entscheidungen in den Code der Anwendung zu integrieren, wird das sicher immer wieder passieren. Vorbei ist es mit der Trennung zwischen RBAC-Komponente und Anwendung – ändert sich später eine Vorgabe des Unternehmens, muss immer ein Entwickler, der sich in den Untiefen der Anwendung auskennt, die Änderungen an der richtigen Stelle vornehmen. Noch schwieriger ist es, aus dem Code eine Übersicht herauszufiltern, wer welche Rechte hat. Möchte man eine Unternehmenssoftware an mehrere Kunden verkaufen, kommen solche Tricks nicht infrage. Die Trennung von Programmcode und individuellen Regeln ist dann eine unumstößliche Vorgabe.

## OPA bringt frischen Wind

Um eine Lösung für solche Probleme zu schaffen, hat sich das Unternehmen Styra den Open Policy Agent (OPA) ausgedacht. Die Erfinder kommen aus dem Bereich Software-Defined Networking sowie aus dem Cloud- und Container-Umfeld und so sind Container-Umgebungen (mit Docker oder Kubernetes) ein möglicher, aber längst nicht der einzige Einsatzbereich für OPA. 2019 hat Styra das Projekt an die Cloud Native Computing Foundation, einer Stiftung unter dem Dach der Linux Foundation, gespendet. Seitdem wird die Open-Source-Software von Programmierern aus vielen Unternehmen weiterentwickelt. Zu den Nutzern von OPA zählen Energie- und Telekommunikationsunternehmen sowie Banken und Versicherun-

gen – das Auswerten von Regeln gehört hier zum Kerngeschäft.

Der Open Policy Agent ist ein Dienst, der Regeln und Daten entgegennimmt und auf dieser Grundlage eine Entscheidung zurückgibt. Die Macher bezeichnen Ihre Erfindung als universelle Policy-Engine. Im einfachsten Fall lautet eine solche Entscheidung `allow: true` oder `allow: false`. Zurück kommen könnte aber beispielsweise auch eine gefilterte Liste. Berechtigungsprüfungen sind also nur ein möglicher Einsatzbereich.

Wenn Sie OPA in Ihrer Software einsetzen möchten, haben Sie verschiedene Optionen. Nutzen Sie eine klassische Infrastruktur ohne Container, können Sie die

OPA-Binärdatei herunterladen und OPA im Server-Modus starten (siehe [ct.de/yc54](http://ct.de/yc54)). OPA stellt dann ein REST-API bereit, an

dem Ihre Anwendung per HTTP-Anfrage um Entscheidung bittet. Ebenfalls per API übergeben Sie ein oder mehrere Textdokumente mit den Regeln, die OPA zur Laufzeit für Sie verwahrt. Die Integration in bestehende Systeme ist so in jeder Programmiersprache möglich, für die es einen HTTP-Client gibt (was auf jede relevante Sprache zutreffen dürfte).

Nutzen Sie eine Container-Umgebung, in der auch Ihre Anwendung containerisiert ist, können Sie OPA ebenfalls als Container starten und per HTTP mit ihm kommunizieren. Das Container-Image im Docker-Hub heißt `openpolicyagent/opa:latest`.

Planen Sie gerade eine Anwendung in Go, haben Sie eine dritte Möglichkeit, OPA zu integrieren: Weil Open Policy Agent in Go geschrieben ist, können Sie die Policy-Engine auch als Go-Paket einbinden:

```
import (
  "github.com/open-policy-agent/opa/rego"
)
```

Mit der Funktion `query.Eval()` befragen Sie OPA dann direkt – in diesem Fall müssen Sie sich selbst darum kümmern, die Regeln im Arbeitsspeicher oder in Dateien zu verwalten. Die Dokumentation gibt einige Anregungen dazu (siehe [ct.de/yc54](http://ct.de/yc54)).

## Es gibt Regeln

Bevor Sie sich mit der Integration in Ihre Anwendung befassen, müssen Sie einen

Blick auf die Regeln werfen. Die Entwickler haben sich dafür entschieden, eine eigene Sprache zum Verfassen solcher Regeln zu erfinden – sie heißt Rego und orientiert sich bei der Syntax teilweise an Go, entsprechende Kenntnisse sind aber nicht nötig. OPA ist nicht der erste Ansatz, um flexible Regeln in ein maschinenlesbares Format zu bringen – seit 2003 gibt es etwa XACML, basierend auf XML. Viele Freunde hat dieser Ansatz aber nicht gefunden, auch weil die XML-Fragmente für Menschen kaum lesbar sind. Rego-Regeln dagegen sind leicht zu erfassen.

Um die Flexibilität von Rego auszuprobieren, müssen Sie nichts herunterladen und keine komplizierte Container-Infrastruktur starten. Nutzen Sie zum Experimentieren den Online-Spielplatz unter [play.openpolicyagent.org](http://play.openpolicyagent.org). Im Fenster links ist Platz für die Regeln, rechts finden Sie einen Bereich für Eingabedaten (Input) in Form von JSON-Objekten. Im Feld darunter können Sie weitere Daten (Data) als JSON-Objekt übergeben, die zur Entscheidungsfindung herangezogen werden sollen. Unten rechts kommt das Ergebnis zurück, sobald Sie die Schaltfläche „Evaluate“ betätigen. Wenn Sie ein Experiment im Online-Sandkasten speichern oder mit Kollegen teilen möchten, klicken Sie oben rechts auf „Publish“.

Als Beispiel zeigen wir nun Stück für Stück, wie Sie die oben formulierten Regeln für die Einkaufsabteilung in Rego übersetzen. Dabei lernen Sie die wichtigsten Teile der Rego-Syntax kennen. Bereinigen Sie zunächst die drei Eingabefelder in der Browser-Umgebung. Füllen Sie dann das Feld für die Eingabewerte:

```
{
  "operation": "create_purchase",
  "user": "bob",
  "roles": ["purchase_employee"],
  "order": {
    "company_id": "123", "sum": 1000
  }
}
```

Wenn Sie die Beispiele nicht abtippen möchten, finden Sie den Playground zum Artikel über [ct.de/yc54](http://ct.de/yc54). In diesen Eingabewerten finden Sie bereits den Benutzernamen (`bob`) und eine Liste seiner Rollen (`purchase_employee`). Der Einsatz von Rollen aus einem klassischen RBAC-System und OPA schließen sich also keinesfalls aus – wenn es sich bewährt hat, können Sie weiterhin mit Rollen arbeiten und die

Rolleninhaber zum Beispiel in einer SQL-Datenbank verwalten.

Ihre Anwendung, die eine Entscheidung von OPA erwartet, muss diese Informationen lediglich als JSON-Objekt zusammenbauen. Nicht zuständig ist OPA für die Authentifizierung – wenn sich die Nutzer beispielsweise mit Benutzernamen und Kennwort anmelden, muss ein anderer Teil Ihrer Anwendung diese Kombination prüfen und den Benutzernamen als Teil der Eingabedaten OPA übergeben.

Im Feld links formulieren Sie jetzt Ihre erste Regel:

```
package purchase.example

import input
import data
default allow = false

allow {
  input.operation == "create_purchase"
}
```

Jedes Rego-Dokument beginnt mit einem Namen, eingeleitet von `package`. Das ist wichtig, wenn Sie später Regeln in anderen Rego-Dokumenten wiederverwenden möchten. Es folgen zwei `import`-Befehle. Mit diesen stellen Sie sicher, dass die Eingabedaten (`input`) und die weiteren Informationen (`data`) benutzt werden können. Anschließend wird ein Standardwert für den Rückgabewert `allow` festgelegt. Standardmäßig soll der Zugriff mit `"allow": false` verboten werden. Der Name `allow` für den Rückgabewert ist keinesfalls festgelegt, Sie könnten ihn auch anders nennen – `allow` werden Sie aber in allen Dokumentationen, in denen es um Autorisierung geht, als Beispiel finden.

Es folgt die erste richtige Regel. Übersetzt bedeutet sie „Wenn der Wert für `operation` in den Eingabewerten `create_purchase` ist, gib `"allow": true` zurück.“ Diese Regel ist aber noch viel zu großzügig, bisher fehlt die Prüfung auf die Rolle `purchase_employee` und die Bestellsumme. Einen Operator für die UND-Verkettung von Bedingungen gibt es in Rego nicht. Stattdessen gibt OPA nur dann `true` für eine Regel zurück, wenn alle Zeilen innerhalb der `{ }` erfüllt sind. Weitere Bedingungen fügen Sie also einfach in neue Zeilen ein:

```
allow {
  input.operation == "create_purchase"
```

```
  input.order.sum <= 1000
  some i
  input.roles[i] == "purchase_employee"
```

Normale Mitarbeiter der Abteilung dürfen nur Aufträge bis 10.00 Euro erstellen. Um das zu prüfen, reicht eine Zeile aus: Innerhalb des JSON-Objekts können Sie mit der Punkt-Syntax (die zum Beispiel aus JavaScript bekannt sein dürfte) bis zum gesuchten Wert navigieren und darauf einen Vergleich anstellen.

Da ein Nutzer mehrere Rollen haben kann (und in einer echten Anwendung sicher auch haben wird), liegen diese in einem JSON-Array. Auf ein Element in einem solchen Array greifen Sie in Rego genau wie in JavaScript mit Angabe des Indizes in `[ ]` zu. Die erste Rolle des Benutzers bekommen Sie zum Beispiel mit `input.roles[0]`. Weil Sie sich auf die Reihenfolge nicht verlassen können, müssen Sie über alle Rollen iterieren. Dafür brauchen Sie in Rego keine `for`- oder `while`-Konstrukte. Definieren Sie stattdessen eine Variable mit dem Schlüsselwort `some` und verwenden Sie diese als Index. OPA prüft dann selbstständig, ob diese Bedingung erfüllbar ist. Besonders hilfreich ist das, wenn Sie tiefer verschachtelte Datenobjekte haben und mit mehreren Index-Variablen gleichzeitig arbeiten. In einer beliebigen Programmiersprache enden solche Suchen schnell in undurchsichtigen verschachtelten Schleifenformationen.

Jetzt ist es an der Zeit, OPA in Aktion zu testen. Werten Sie die Regel mit der Schaltfläche „Evaluate“ aus und experi-

mentieren Sie etwas mit den Eingabewerten. Aufträge jenseits von 1000 Euro lehnt OPA nun ab.

## Mehr Daten nutzen

Drei weitere Regeln fehlen noch – zunächst sollen Stellvertreter und Abteilungsleiter das Recht bekommen, höhere Beträge freizugeben. Für die Entscheidungsfindung bekommt OPA ein weiteres JSON-Objekt im Feld `data`. Im Online-Sandkasten kopieren Sie die Daten in das zweite Feld auf der rechten Seite. Ein echter OPA-Server nimmt solche Daten per REST-API entgegen. Alle Statusinformationen Ihrer Anwendung, die für Entscheidungsfindungen infrage kommen, sollten Sie hier abladen. Für die gewünschten Regeln brauchen Sie folgende Daten:

```
"departments": {
  "purchase": {
    "deputy": "alice",
    "head": "bob",
    "workers": [
      "peter",
      "marie"
    ]
  },
  "trusted_companies": ["123", "456"]
}
```

Dieses Objekt enthält die Information, wer in der Abteilung `purchase` als normaler Mitarbeiter, Stellvertreter und Abteilungsleiter arbeitet. Außerdem gibt es eine Liste

The screenshot shows the 'The Rego Playground' interface. The left panel contains the Rego code. The right panel shows the 'INPUT' and 'DATA' sections. The 'INPUT' section contains a JSON object with an 'operation' field set to 'create\_purchase', an 'order' object with a 'sum' field of 1000, and a 'roles' array containing 'purchase\_employee'. The 'DATA' section contains a JSON object with a 'departments' object, which in turn contains a 'purchase' object with 'deputy' (alice), 'head' (bob), and 'workers' (peter, marie). It also contains a 'trusted\_companies' array with values '123', '456', and '789'. The bottom panel shows the 'OUTPUT' section, which displays the result of the evaluation: a single object with 'allow' set to true and 'is\_purchase' set to true.

Im Rego Playground können Sie erste Erfahrungen bei der Arbeit mit Open Policy Agent sammeln. Die Umgebung läuft ohne Installation im Browser.

aller Stammlieferanten. Die Regel für Stellvertreter sieht so aus:

```
allow {
  input.operation == "create_purchase"
  some i
  input.roles[i] == "purchase_employee"
  data.departments.purchase.deputy
  & == input.user
  input.order.sum < 10000
}
```

Eine Syntax für ODER brauchen Sie in Rego auch nicht. Legen Sie einfach eine weitere Regel für `allow`, gefolgt von den Bedingungen in `{ }` an. OPA wird sie nacheinander prüfen und beim ersten Treffer `allow: true` zurückgeben. Im Online-Spielplatz können Sie gut verfolgen, welche Regel zum Einsatz kam und an welcher Zeile es möglicherweise scheiterte. Setzen Sie oben rechts den Haken bei „Coverage“. Grün eingefärbte Zeilen wurden erfolgreich ausgewertet. Bevor Sie weitere Regeln für den Abteilungsleiter und die Stammlieferanten schreiben, sollten Sie den Code etwas aufräumen. Die ersten drei Zeilen kommen immer wieder vor. Für diese sollten Sie eine wiederverwendbare Regel bauen:

```
is_purchase {
  input.operation == "create_purchase"
  some i
  input.roles[i] == "purchase_employee"
}
```

Sind diese beiden Bedingungen erfüllt, nimmt `is_purchase` den Wert `true` an. Diese Hilfsregel können Sie gleich einsetzen, die Regel für den Abteilungsleiter sieht dann so aus:

```
allow {
  is_purchase == true
  data.departments.purchase.head
  & == input.user
}
```

Diese Schreibweise können Sie noch weiter verkürzen und `== true` weglassen. OPA prüft dann automatisch, ob ein Wert `true` ist.

Die letzte Regel, die ein reines RBAC-System an die Grenzen gebracht hätte, ist ebenfalls schnell formuliert:

```
allow {
  is_purchase
  some j
  data.trusted_companies[j]}
```

## Autorisierung ist nicht Authentifizierung

Eine Anwendung, die Zugriffe steuert, muss zwei Aufgaben lösen: Der erste Schritt ist die **Authentifizierung** – der Nutzer muss sich gegenüber der Anwendung ausweisen. Noch immer das häufigste Verfahren zur Authentifizierung ist die Anmeldung mit Benutzername und Kennwort. Nutzer und Server sind dabei im Besitz eines gemeinsamen Geheimnisses, dem Kennwort. Alternativ könnte der Nutzer sich zum Beispiel mit einem Zertifikat ausweisen oder einen FIDO2-Stick verwenden. Nach erfolgreicher Authentifizierung sammelt der Server Informationen über den Nutzer. Das können zum Beispiel Gruppenmitgliedschaften sein, in Unternehmensumgebungen ist oft Microsofts Active Directory die zen-

trale Quelle für solche Informationen. Diese Aufgaben fallen nicht in den Bereich von Open Policy Agent.

OPAs Aufgabe liegt im Bereich der **Autorisierung**, also in der Entscheidungsfindung, ob ein vorher authentifizierter Nutzer zu einer Aktion berechtigt ist. Dafür muss der Authentifizierungs- server vorher zweifelsfrei sichergestellt haben, dass sich niemand als jemand anders ausgibt. Auf keinen Fall sollten Sie OPA mit seinem API ins Internet hängen – dieses API ist dafür gedacht, dass über ein internes Netz eine Komponente Ihrer Software für eine Entscheidung anfragt. OPA ist also nur ein Baustein für Ihre Anwendung, keine komplette Autorisierungs- und Authentifizierungslösung.

```
& == input.order.company_id
}
```

Ein gewöhnlicher Mitarbeiter darf jetzt beliebig viel Geld ausgeben, solange er nur bei einem Stammlieferanten bestellt.

Mit diesen grundlegenden Funktionen haben Sie Open Policy Agent und Rego noch lange nicht ausgereizt. Einen Überblick über eingebaute Funktionen finden Sie in der Referenz über [ct.de/yc54](https://ct.de/yc54) – eingebaut sind zum Beispiel Funktionen zum Zählen von Elementen (`count()`) oder ein Zugriff auf die aktuelle Uhrzeit und das Datum (über das Objekt `time`). Außerdem gibt es Funktionen, um zusätzliche Daten beim Auswerten von Regeln nachzuladen.

## Integrieren

Mit diesem Grundwissen ausgestattet, müssen Sie sich eine sinnvolle Architektur für Ihre Software ausdenken, in die Sie OPA integrieren können. Ihr bisheriges RBAC-System müssen Sie dafür nicht abschaffen. Bestehende Rollen können Sie OPA als Daten oder Eingabewerte übergeben und in Ihre Regeln einfließen lassen. Inspirations für eigene Integrationen liefert die OPA-Dokumentation (siehe [ct.de/yc54](https://ct.de/yc54)). In den Beispielen finden Sie unter anderem ein HTTP-API, eine der häufigsten Anwendungen für OPA. Es gibt auch bereits fertige Integrationen für einige Anwendungen. So können Sie mit OPA in Verbindung mit Linux-PAM zum Beispiel genau steuern, wer auf einer Linux-Maschine welche Ope-

rationen ausführen darf. Auch einen Docker-Host können Sie mit einer fertigen OPA-Integration um ein Berechtigungskonzept erweitern.

## Regeln sind Code

Zu den Vorteilen von Open Policy und Regeln im Rego-Format gehört, dass Sie die Regeln, die in Ihrer Organisation existieren, wie Code behandeln können. Rego-Regeln kann man dokumentieren (mit `#` am Zeilenanfang) und in Git-Repositories versionieren. Einmal in Git abgelegt, können Sie zum Beispiel einen Review-Prozess in Ihre CI-Lösung einbauen, damit Änderungen nur im Vieraugenprinzip möglich sind. Auch an Unit-Tests für Regeln ist gedacht. Dafür formulieren Sie erwartete Ergebnisse und lassen OPA diese automatisch testen.

Der Einstieg in Open Policy Agent lohnt vor allem, wenn Sie eine neue Anwendung planen – gerade in einer Microservice-Architektur haben Sie ihn schnell eingebaut, weil er per HTTP arbeitet. Bei großen bestehenden Anwendungen ist der Kraftakt nicht zu unterschätzen – wenn Sie Ihre Entscheidungen bisher tief vergraben im Code vornehmen, müssen Sie nicht nur OPA integrieren, sondern all diese Code-Zeilen wieder herausoperieren. Belohnt werden Sie mit einer flexiblen und gut zu wartenden zentralen Stelle für alle Formen von Entscheidungsfindung.

(jam@ct.de) 

**Dokumentation:** [ct.de/yc54](https://ct.de/yc54)



Wenn bei einem technischen Bericht oder einer Studienarbeit Chemie ins Spiel kommt, stoßen klassische Textverarbeitungsprogramme an ihre Grenzen. Dagegen können Sie mit LaTeX chemische Notationen mit einfachen Kommandos direkt im Dokument erzeugen.

Von Zacharias Steinmetz

Bei der Verbrennung von Erdgas entsteht  $\text{CO}_2$ . Solch ein Satz lässt sich ohne Weiteres in jedes gängige Textverarbeitungsprogramm tippen, enthält er doch mit „ $\text{CO}_2$ “ bloß eine einfache chemische Summenformel. Möchte man hingegen Kohlenstoffdioxid als Strukturformel darstellen, die komplette Verbrennung in einer chemischen Reaktionsgleichung abbilden oder gar mehrstufige Reaktionsmechanismen zu Papier bringen, ist Spezialsoftware gefragt.

Mit dem Makropaket LaTeX und dem zugrunde liegenden Satzsystem TeX lassen sich Texte mitsamt Formeln komplett aus einem Guss im LaTeX-Editor oder sogar in der gewohnten Office-Suite erstellen. Dagegen eignen sich eigenständige Formeleditoren für Android, die wir kürzlich getestet haben, vor allem für schnelle Skizzen, verweigern aber vielfach die Zusammenarbeit mit Microsoft Office, LibreOffice & Co. [1].

Kommerzielle Werkzeuge wie ACD/ChemSketch, ChemDraw oder ISIS Draw sind da leistungsfähiger, doch auch mit diesen gerät es leicht zum Geduldsspiel, die Ergebnisse mit geeigneten Darstellungs- und Exportparametern an die Formatvorlagen des Textdokuments anzupassen. Demgegenüber stellt die Einarbeitung in LaTeX kaum einen Mehraufwand dar, erschließt Ihnen aber weit mehr Möglichkeiten.

### Im Labor

Wie man mit LaTeX erste eigene Dokumente erzeugt, haben wir schon detailliert beschrieben [2]. Ungeduldige laden sich über die Website des LaTeX-Projekts (für alle erwähnten Webadressen: siehe [ct.de/ytkl](http://ct.de/ytkl)) eine TeX-Distribution ihrer Wahl für Windows, macOS oder Linux herunter. Darin wird stets auch LaTeX unterstützt.

# Chemiebaukasten

## Chemische Formeln und Reaktionsgleichungen in LaTeX

Zum Schreiben bewährt sich ein auf LaTeX spezialisierter Editor wie TeX-studio, indem er dem Benutzer viel Tipparbeit abnimmt und zudem auf Knopfdruck das fertig layoutte Arbeitsergebnis anzeigt. Einen Zwischenweg beschreitet das LibreOffice-Plug-in TexMaths. Dieses erzeugt, eine lokale LaTeX-Installation vorausgesetzt, aus Formelbefehlen PNG- oder SVG-Grafiken undbettet sie direkt in ein Writer-Dokument ein. Um das zu nutzen, müssen Sie außer den wenigen hier vorgestellten Kommandos nicht einmal den allgemeinen LaTeX-Wortschatz einstudieren.

## LaTeX pur

Die folgenden Zeilen, die man am bequemsten in einem LaTeX-Editor eingibt, kodieren ein erstes Vorschaudokument:

```
\documentclass{scrartcl}
\usepackage[utf8]{inputenc}
\usepackage[T1]{fontenc}
\usepackage[ngerman]{babel}
\begin{document}
Bei der Verbrennung von Erdgas
entsteht CO2.
\end{document}
```

Im Editor erscheint dabei nur dieser Quellcode, den Sie per Kopfdruck zu einem DVI-Dokument kompilieren können. Darin findet sich das von TeX erzeugte Layout in einem geräteunabhängigen, maschinenlesbaren Format. Den Inhalt bekommen Sie automatisch als fertiges Layout auf dem Bildschirm angezeigt und typischerweise als PDF-Datei gespeichert.

Um LaTeX den Umgang mit chemischen Elementen beizubringen, verwenden wir in diesem Beitrag zusätzlich die Pakete chemmacros und chemfig jeweils in ihrer aktuellen Version, die allerdings noch nicht ihren Weg in alle TeX-Distributionen gefunden haben und womöglich manuell hinzugefügt werden müssen. In diesem Fall müssen Sie die Zip-Archive herunterladen, in gleichnamige Verzeichnisse entpacken und diese dann in das Erweiterungsverzeichnis Ihrer TeX-Distribution kopieren. Für TeX Live und Windows ist das normalerweise texlive/texmf-local. Das für Windows empfohlene MikTeX installiert fehlende Pakete automatisch nach, wenn sie in der Präambel eines Dokuments erwähnt werden.

Während chemmacros hilft, chemische Summenformeln und Reaktionsgleichungen aufzustellen, lassen sich mit chemfig zweidimensionale Strukturformeln und Darstellungen von Reaktionsmechanismen wiedergeben.

Über den jeweiligen Befehl `\usepackage{<Paketname>}` werden die jeweiligen Pakete geladen und stellen die enthaltenen Befehle für die TeX-Verarbeitung bereit. Zusätzlich schaltet `\chemsetup{modules = all}` alle Zusatzmodule des chemmacros-Pakets frei. Diese Statements gehören zusammen mit anderen Angaben, deren Defaultwerte Sie nur in Sonderfällen anpassen müssen, in die Präambel des LaTeX-Dokuments.

## Die Grundbausteine

Mithilfe des Kommandos `\ch` lassen sich im Hauptteil des Dokuments nach `\begin{document}` chemische Formeln definieren. `\ch{CO2}` erzeugt „CO<sub>2</sub>“. Der tiefgestellte Index wird automatisch als solcher interpretiert, sodass es anders als im nativen Mathemodus keiner expliziten Formatierung bedarf.

Möchte man die Formel um Oxidationszahlen ergänzen, gelingt dies mit `\ox{4,C}\ox{-2,O2}`, hier wohlgernekt ohne `\ch`-Makro. Erst wenn der Ausdruck in Anführungszeichen gesetzt wird, lässt sich dieser in die `\ch`-Notation einbinden: `\ch{"\ox{4,C}\ox{-2,O2}"}`. Auf diese Weise sind Mischkonstruktionen umsetzbar, in denen nur einzelne Abschnitte der Summenformel mit Oxidationszahlen versehen werden sollen. In beiden Fällen lautet das Ergebnis hier C<sup>IV</sup>O<sub>2</sub><sup>-II</sup> gemäß den Nomenklaturvorgaben der International Union of Pure and Applied Chemistry (IUPAC).

Dem `\ox`-Befehl nachgestellte eckige Klammern nehmen davon abweichende Optionen auf. So erzwingt `[roman=false, pos=top, explicit-sign=true]` die ebenso gebräuchliche Darstellung CO<sub>2</sub><sup>+4-2</sup>, bei der die Oxidationszahlen in arabischen Ziffern direkt über den Elementsymbolen stehen. Im Unterschied dazu werden echte Ladungen, wie sie etwa in den Anionen der Kohlensäure vorkommen, analog zum Mathemodus mit einem Zirkumflex erzeugt, also `\ch{HCO3^{\pm}}`. Ein optional übergebenes `[circled=all]` umringt die Ladungszeichen zur besseren Übersicht: HCO<sub>3</sub><sup>0</sup>. Zahlreiche weitere Funktionen wie die Notation von Radikalen oder Isotopen verrät die Paketdokumentation des TeX-Repositories CTAN.

## In Reaktion

Möchte man nun veranschaulichen, dass bei der vollständigen Verbrennungsreaktion des Erdgas-Bestandteils Propan drei Teile Kohlenstoffdioxid und vier Teile Wasser entstehen, lautet die Eingabe:

```
\ch{C3H8 + 5 O2 ->[ $\Delta$ ]}
3 CO2 ^ + 4 H2O}
```

Der LaTeX-Compiler erzeugt daraus folgende Reaktionsgleichung:



Gleich bleibt die Verwendung des Makros `\ch`. Neu ist neben den vorangestellten Stoffmengenverhältnissen der Reaktionspfeil und das alleinstehende Zirkumflex, das einen vertikalen Pfeil generiert. Dieser gibt explizit an, dass CO<sub>2</sub> während der Reaktion entweicht.

Je nach Bedarf ist eine Vielzahl weiterer Pfeilarten wählbar, zum Beispiel zur Darstellung eines chemischen Gleichgewichts. Dem Reaktionspfeil nachgestellte eckige Klammern nehmen zudem über oder unter dem Pfeil stehende Beschriftungen auf. In diesem Beispiel handelt es sich um ein Delta, das die Freisetzung von Energie anzeigt.

„chemmacro“-Befehl	Typ
<code>-&gt;</code>	A → B
<code>&lt;-</code>	A ← B
<code>-/→</code>	A → B
<code>&lt;-&gt;</code>	A ↔ B
<code>&lt;=&gt;</code>	A ≡ B
<code>&lt;=&gt;&gt;</code>	A ≡ B
<code>&lt;&lt;=&gt;</code>	A ↔ B

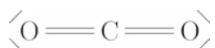
## Gib mir Struktur

Selbst einfache Strukturformeln lassen sich noch mittels `\ch`-Kommando umsetzen. Einfach-, Doppel- und Dreifachbindungen werden dabei jeweils mit einem Minus-, Gleichheits- und Pluszeichen kodiert. Aus `\ch{O=C=O}` wird also O=C=O. Für komplexere Strukturen samt Darstellung freier Elektronenpaare oder ganzer Reaktionsmechanismen bedarf es aber des Pakets und gleichnamigen Befehls chemfig.

Mit `\chemfig{O=C=O}` bleibt die Schreibweise zum Erzeugen der Molekülformel zunächst identisch zu `\ch`. Der Befehl

\charge fügt der Strukturformel unter Angabe der Winkel die freien Elektronenpaare als Striche hinzu:

```
\chemfig{\charge{135=|,-135=|}{O}C=\charge{45=|,-45=|}{O}}
```



Ersetzt man | durch einen Doppelpunkt, werden die freien Elektronen als einzelne Punkte dargestellt. Mit derselben Syntax lassen sich auch partielle Ladungen darstellen. Die Angabe 4pt definiert den jeweiligen Abstand zum betreffenden Atom. 90 steht für eine Winkelangabe von 90°:

```
\chemfig{\charge{90:4pt=$\delta-$}{O}=\charge{90:4pt=$\delta^+$}{C}=\charge{90:4pt=$\delta-$}{O}}
```

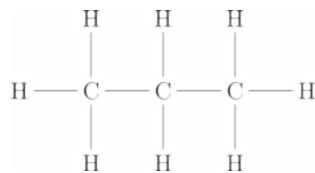


Damit liegt bisher lediglich ein lineares Molekül im Chemiebaukasten. Für Moleküle mit komplexeren Verzweigungen, wie sie im Propan aus der dargestellten Verbrennungsreaktion vorkommen, verlangt die chemfig-Notation nach der Definition von Substituenten. Das sind Moleküluntergruppen und diese stehen eingeschlossen in runden Klammern nach dem Atom, an das sie binden sollen. Damit sich die Substituenten beim Zeichnen nicht überlagern,

muss deren Position explizit angegeben werden. Dies gelingt am einfachsten über die Angabe einer ganzen Zahl zwischen 0 und 7 in eckigen Klammern, die einem Vielfachen von 45° relativ zur Horizontalen entspricht. Das Kommando

```
\chemfig{H-C(-[2]H)(-[6]H)-C(-[2]H)(-[6]H)-H}
```

erzeugt die Valenzstrichformel von Propan:



## Mit einem Minimum an TeX

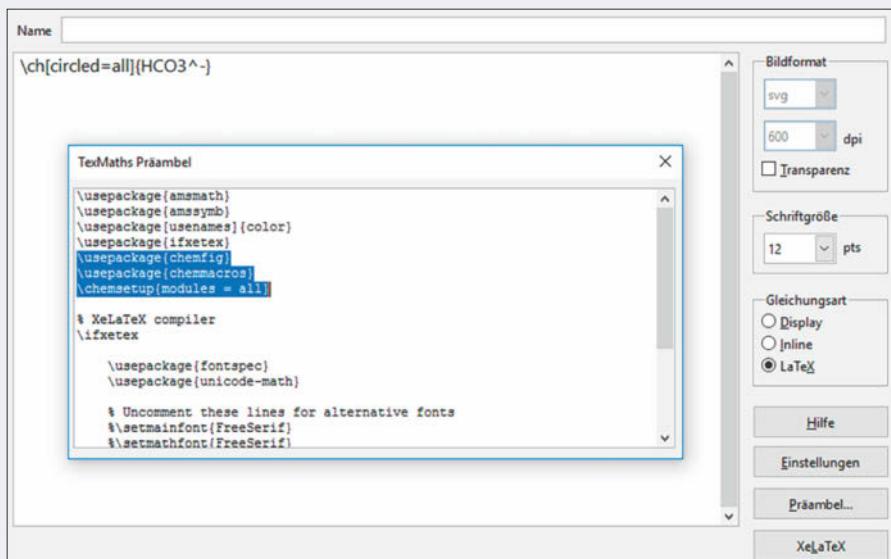
Wenn Sie sich nicht in die komplexe Struktur von LaTeX-Dokumenten einarbeiten möchten, können Sie die hier vorgestellten Funktionen auch einstiegsfreundlich mit der Bürosuite LibreOffice nutzen. Dafür müssen Sie außer einer TeX-Distribution und den vorgestellten TeX-Packages außerdem das LibreOffice-Plug-in TexMaths installieren. Das gelingt im LibreOffice Writer unter „Extras/Extension Manager“ über den Download-Link für weitere Extensions.

Beim Einsatz unter Linux beklagt sich das Plug-in je nach verwendeter Linux- und TeX-Distribution über fehlende TeX-Kernelfunktionen oder ein zu altes Hilfsprogramm namens dvipng und verweigert erst einmal den Dienst. Dann wird es womöglich erforderlich, eine andere TeX-Distribution aufzuspielen.

Nach dem anschließenden Neustart präsentiert Writer in der Befehlsleiste vier neue Symbole für Formeln, nummerierte Formellisten, Plug-in-Einstellungen und für LaTeX-Compiler-Einstellungen. Davon muss man sich nur mit dem ersten Symbol beschäftigen: Dieses öffnet einen Dialog, in dem Sie Ihre LaTeX-Befehle eingeben

und mit dem Compiler LaTeX oder XeLaTeX kompilieren können. Beim ersten Gebrauch sollten Sie allerdings zuerst die Präambel-Schaltfläche anklicken. Daraufhin erscheint ein Grundgerüst des Codes. Dieses enthält auch die vorformulierte LaTeX-Präambel, die schon ohne Ihr Zutun ganz bequem die Voraussetzungen für die Formulierung mathematischer Ausdrücke schafft. Damit die Software auch die erwähnten Chemie-Pakete berücksichtigt, müssen Sie die zugehörigen \usepackage- und \chemsetup-Befehle in die Präambel einfügen und einmal speichern.

Nach dieser Vorarbeit übersetzt ein Klick auf die LaTeX- oder XeLaTeX-Schaltfläche im Dialog die eingetippte Formel in eine TeX-gerenderte Grafik und fügt diese im LibreOffice-Dokument ein. Es entsteht ein ganz normales Dokument, das sich ohne Zusatzsoftware mit LibreOffice anzeigen und etwa auch als PDF exportieren lässt. Word kann solche Dokumenten nur in den Formaten DOC und DOCX lesen und rendert die vom Plug-in eingebundenen Formeln nur als unscharfe Bilder, taugt also nicht als Werkzeug für die Veröffentlichung.



Das Plug-in TexMaths gibt sich mit vier neuen Symbolen in der Writer-Befehlsleiste zu erkennen.

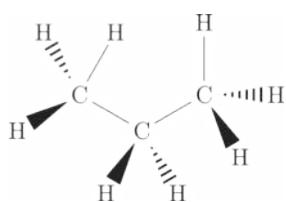
Damit LibreOffice chemische Formeln rendert, muss man mit \usepackage die Module chemmacros und chemfig einbinden.

Direkt lassen sich absolute Winkelangaben durch einen vorangestellten Doppelpunkt übergeben. Der Befehl

```
\chemfig{H-C(-[:90]H)(-[:-90]H)
         -C(-[:90]H)(-[:-90]H)-H}
```

gibt also dieselbe Valenzstrichformel aus.

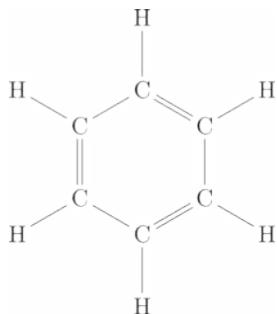
Eine leichte Anpassung der Winkelangaben und Bindungstypen bringt den Chemieinteressierten von der zuvor erstellten Valenzstrichformel zur Keilstrichformel. Diese verdeutlicht die räumliche Anordnung der Atome im Molekül:



Sie sehen: chemfig interpretiert Winkelangaben als Gradzahlen für die Drehung entgegen dem Uhrzeigersinn, beginnend bei 0 für die Ausrichtung von links nach rechts. Auch Ringstrukturen erschließen sich zwangslässig aus passend verketteten Bindungs- und Winkelangaben, etwa mit

```
\chemfig{C(-[:90]H)
         =[:330]C(-[:30]H)
         -[:-270]C(-[:330]H)
         =[:210]C(-[:270]H)
         -[:-150]C(-[:210]H)
         =[:90]C(-[:150]H)-[:-30]C}
```

für die konventionelle Strukturformel des Benzolmoleküls:



Schnell zeigt sich, wie mit dem Umfang der zu zeichnenden Moleküle die Komplexität der chemfig-Syntax wächst. Den Einstieg erleichtert das Webtool mol2chemfig, mit dessen Hilfe man Molekülstrukturen händisch vorzeichnen oder aus einer Datenbank abrufen kann. Diese lassen

sich im Anschluss in die chemfig-eigene Struktur konvertieren und in LaTeX übernehmen.

Für weitere Details lohnt ein Blick ins chemfig-Kompendium. Neben zahlreichen Beispielen, wie sich besonders komplizierte Strukturen elegant umsetzen lassen, enthält es auch Anleitungen, die verschiedensten Formatierungseinstellungen feingranular anzupassen und eigene Vektorgrafiken mithilfe des Pakets TikZ einzubinden.

## Viele weitere Möglichkeiten

LaTeX kann noch mehr Chemie. Wem nach diesem Artikel noch nicht der Kopf raucht, der kann etwa mithilfe des LaTeX-Pakets bohr Bohr'sche Atommodelle visualisieren. Beim Zeichnen von Energie-diagrammen hilft endiagram, und ghsystem nimmt dem Benutzer die Recherche und Übernahme von Risiko- und Sicherheitssätzen sowie Gefahrensymbolen gemäß dem global harmonisierten System zur Einstufung und Kennzeichnung von Chemikalien (GHS) ab. Um anzugeben, dass Propan leicht brennbar ist, fügt man mit `\ghspic{flame}` das entsprechende Piktogramm ein. Der Befehl `\ghs{h}{220}` spuckt gemäß GHS die Warnung „H220: Extrem entzündbares Gas“ auf Deutsch, Englisch, Französisch, Italienisch oder Spanisch aus, je nachdem, welche Sprache in der Präambel festgelegt ist, etwa mit `\usepackage[ngerman]{babel}` für Deutsch mit Silbentrennung.

Zusätzlich zu den allgemeinen Funktionen für professionellen Textsatz bietet



**Wenns brenzlig wird: ghsystem stellt Gefahrstoffsymbole bereit.**

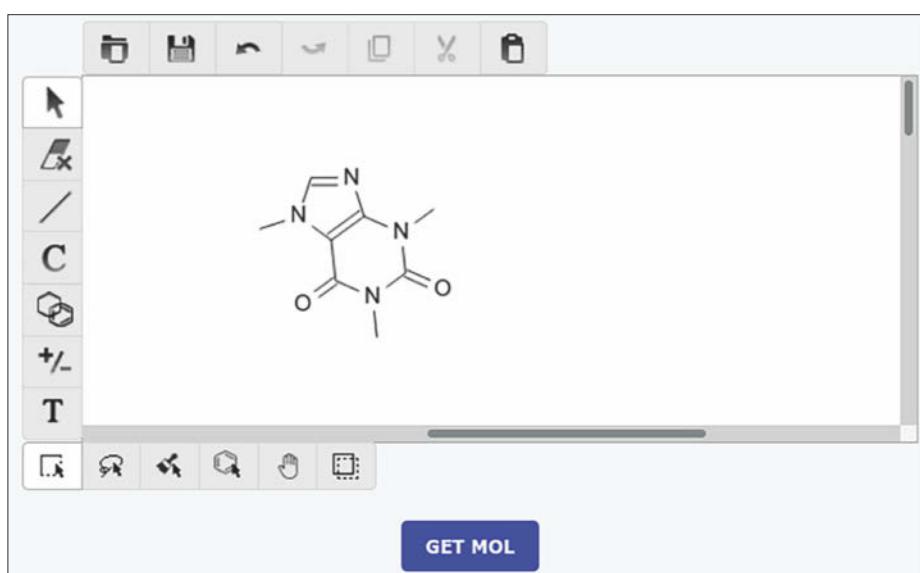
LaTeX speziell für Chemiker viele Werkzeuge, die ohne TeX allenfalls in komplizierter Spezialsoftware zu finden wären. Auch wenn spezielle Editoren den ungewohnten Umgang mit TeX und LaTeX schon vereinfachen, können Sie sich die Einarbeitung mit dem beschriebenen LibreOffice-Plug-in TexMaths noch weiter erleichtern.

([hps@ct.de](mailto:hps@ct.de))

## Literatur

- [1] Peter Schüler, Molekül-Baumeister, Android-Editoren für chemische Strukturformeln, c't 24/2018, S. 156
- [2] Zacharias Steinmetz, In Form gegossen, Anspruchsvolle Texte mit LaTeX schreiben und gestalten, c't 9/2019, S. 152

**Software-Quellen und Dokumentationen:** [ct.de/ytk1](http://ct.de/ytk1)



Mit mol2chemfig kann man Strukturformeln im MDL-Format anfertigen oder aus einer Datenbank holen.

# Für Wissenshungrige

## Ausgewählte Fachliteratur

[shop.heise.de/buecher](http://shop.heise.de/buecher)



### Michael Bonacina **Python 3: Programmieren für Einsteiger**

Dieses Buch legt besonderen Fokus auf die Objekt-orientierte Programmierung (OOP) und das Erstellen von grafischen Oberflächen. Nach dem Durcharbeiten der Übungsaufgaben des Buches kann der Leser eigene komplexere Python Anwendungen inklusive grafischer Oberfläche programmieren.

ISBN 9783966450072

[shop.heise.de/python3-einsteiger](http://shop.heise.de/python3-einsteiger) 13,90 € >



### Christian Solmecke, Sibel Kocatepe **DSGVO für Website-Betreiber**

Ihr Leitfaden für die sichere Umsetzung der EU-Datenschutz-Grundverordnung. Experten erklären Schritt für Schritt, wie Sie Ihren Webauftritt vollständig rechtskonform gestalten – gut verständlich auch für Nichtjuristen.

ISBN 9783836267120

[shop.heise.de/dsgvo-websites](http://shop.heise.de/dsgvo-websites) 39,90 € >

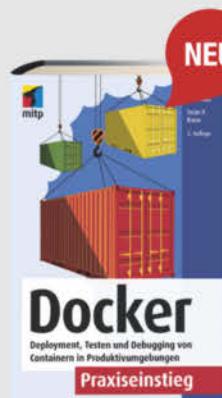


### Jörg Frochte **Maschinelles Lernen (2. Aufl.)**

Maschinelles Lernen ist ein interdisziplinäres Fach, das die Bereiche Informatik, Mathematik und das jeweilige Anwendungsgebiet zusammenführt. In diesem Buch werden alle drei Teilgebiete gleichermaßen berücksichtigt.

ISBN 9783446459960

[shop.heise.de/maschinelles-lernen](http://shop.heise.de/maschinelles-lernen) 38,00 € >

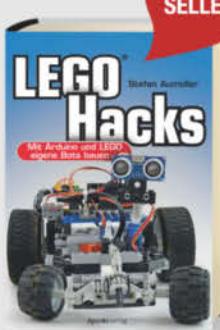


### Karl Matthias, Sean P. Kane **Docker Praxiseinstieg (2. Aufl.)**

Lernen Sie, wie Sie Docker-Images Ihrer Anwendungen erstellen, testen und deployen sowie skalieren können, und wie Sie die Container in der Produktivumgebung pflegen und warten. Die Einrichtung und das Testen von Docker-Anwendungen kommen ebenso zur Sprache wie das Debugging eines laufenden Systems.

ISBN 9783958459380

[shop.heise.de/docker-praxis2](http://shop.heise.de/docker-praxis2) 25,99 € >

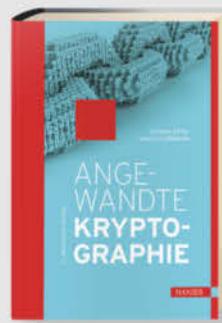


### Stefan Aumüller **LEGO® Hacks**

Dieses Buch zeigt, wie aus LEGO und dem Arduino faszinierende Modelle werden. Lernen Sie, Sensoren und Aktoren, mit LEGO-Elementen zu verbinden und daraus viele neue spannende Projekte aufzubauen. Auch Grundlagen der Elektronik werden Ihnen vermittelt.

ISBN 9783864906435

[shop.heise.de/buch-legohacks](http://shop.heise.de/buch-legohacks) 29,90 € >

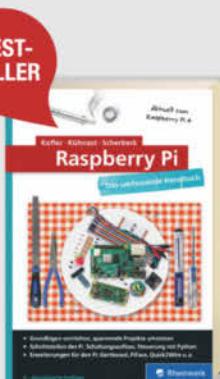


### Wolfgang Ertel, Ekkehard Löhmann **Angewandte Kryptographie (6. Aufl.)**

Ziel des Buches ist es, Grundwissen über Algorithmen und Protokolle zu vermitteln und kryptographische Anwendungen aufzuzeigen. Mit so wenig Mathematik wie nötig, aber vielen Beispielen, Übungsaufgaben und Musterlösungen.

ISBN 9783446463134

[shop.heise.de/kryptographie6](http://shop.heise.de/kryptographie6) 34,99 € >



### Michael Kofler, Charly Kühnast, Christoph Scherbeck **Raspberry Pi (6. Aufl.)**

Das umfassende Handbuch mit über 1.000 Seiten komplettem Raspberry-Wissen, um richtig durchzustarten zu können. Randvoll mit Grundlagen und Kniffen zu Linux, Hardware, Elektronik und Programmierung.

Aktuell für alle Versionen, inkl. Raspberry Pi 4!

ISBN 9783836269339

[shop.heise.de/raspberry-6](http://shop.heise.de/raspberry-6) 44,90 € >



### Simon Monk **Der Maker-Guide für die Zombie-Apokalypse**

Bereiten Sie sich vor: mittels 20 Survival-Projekten mit einfacher Elektronik, Arduino und Raspberry Pi werden Sie Ihren eigenen Strom erzeugen, unverzichtbare Bauteile vor dem Zombie-Zugriff retten und lebensrettende Elektronikschaltungen bauen, um Untote aufzuspüren.

ISBN 9783864903526

[shop.heise.de/zombies](http://shop.heise.de/zombies) 24,90 € >

# und Maker!

## Zubehör und Gadgets

[shop.heise.de/gadgets](http://shop.heise.de/gadgets)

NEU



### ParkLite

ParkLite denkt mit. Die elektronische Parkscheibe stellt automatisch nach ca. 20 Sekunden die Parkzeit ein. Damit ist Schluss mit Bußgeldern! Hitze- und kältebeständig, inklusive Reinigungstuch und Klebepads.

[shop.heise.de/parklite](http://shop.heise.de/parklite)

29,90 € >

NEU



### 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.

[shop.heise.de/flirc](http://shop.heise.de/flirc)

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.

[shop.heise.de/musegear](http://shop.heise.de/musegear)

24,90 € >



### Raspberry Pi-Kameras

Aufsteckbare Kameras, optimiert für verschiedene Raspberry Pi-Modelle mit 5 Megapixel und verschiedenen Aufsätzen wie z. B. Weitwinkel für scharfe Bilder und Videoaufnahmen.

[shop.heise.de/raspi-kameras](http://shop.heise.de/raspi-kameras)

ab 18,50 € >

### Komplettset Argon ONE Case mit Raspberry Pi 4



NEUER PREIS!

Das Argon One Case ist eines der ergonomischsten und ästhetischsten Gehäuse aus Aluminiumlegierung für den Raspberry Pi. Es lässt den Pi nicht nur cool aussehen, sondern kühl auch perfekt und ist leicht zu montieren. Praktisch: alle Kabel werden auf der Rückseite gebündelt ausgeführt – kein Kabelsalat!

117,60 €

[shop.heise.de/argon-set](http://shop.heise.de/argon-set)

99,90 € >

### ArduiTouch-Set



NEUER PREIS!

Setzen Sie den ESP8266 oder ESP32 jetzt ganz einfach im Bereich der Hausautomation, Metering, Überwachung, Steuerung und anderen typischen IoT-Applikationen ein!

69,90 €

[shop.heise.de/arduitouch](http://shop.heise.de/arduitouch)

36,90 € >

NEU



### 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.

[shop.heise.de/pokit](http://shop.heise.de/pokit)

94,90 € >

### NVIDIA Jetson Nano B01

Die neue Revision B01! Die Leistung moderner KI für Millionen Geräte. Mit dem Jetson Nano von NVIDIA können Sie als Heimbastler oder Entwickler platzsparend und effizient in die Welt der KI eintauchen. Ideale Voraussetzung für die Programmierung neuronaler Netze dank vier A57-Kerne und einem Grafikprozessor mit 128 Kernen. Inklusive Netzteil!



[shop.heise.de/jetson](http://shop.heise.de/jetson)

134,90 € >

### „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. Versilbertes Gewebe im Inneren der Tasche aus recycelter Fallschirmselde bildet nach dem Schließen einen faradayschen Käfig und blockiert so alles Signale.



[shop.heise.de/no-signal-sleeve](http://shop.heise.de/no-signal-sleeve)

29,90 € >



28% RABATT

### Make Family + Makey-Paket

Darüber freut sich die ganze Familie: „Make Family“ – das vollgepackte PDF-Magazin mit 21 Anleitungen zum kreativen Basteln mit Kids auf über 200 Seiten. Dazu: der knuffige Makey-Plüschorpfer und der Makey-Lötausatz mit LEDs und Batterie.

27,70 €

[shop.heise.de/makey-paket](http://shop.heise.de/makey-paket)

19,90 € >



# Herzlose Action

## Marvel's Avengers: ohne viel Spielwitz

**Das Action-Rollenspiel Marvel's Avengers zeigt, dass große Namen kein tolles Spiel garantieren. Die unterhaltsame Superheldensaga geht in wüstem Gekloppe und unnützen Mikrotransaktionen unter.**

Von Andreas Müller

Die Geschichte beginnt mit einem großen Knall: Bei einer Feier zu Ehren der Avengers explodiert eine gefährliche Chemikalie und macht aus den Einwohnern San Franciscos sogenannte Inhumans-Menschen mit Superfähigkeiten. Da es viele Todesopfer gibt, werden die Avengers schnell zu Sündenböcken abgestempelt. Aus Scham verstecken sich Iron Man, Hulk & Co. und müssen mitansehen, wie die geheimnisvolle Organisation AIM die Macht an sich reißt. Die Schurken haben aber nicht mit Kamala Khan alias Ms. Marvel gerechnet, die das alte Team der Avengers wieder zusammensammelt.

Wie sich die junge Heranwachsende Kamala als erste muslimische Superheldin

im Marvel-Universum unter den alten Haudegen behauptet, ist dann auch das Interessanteste an der holprig erzählten Geschichte. Spielerisch wird das geboten, was schon aus anderen Superheldenspektakeln wie Batman oder zuletzt Spider-Man bekannt ist: wilde Schlägereien gegen große und kleine Bösewichte, bei denen die Helden reichlich ihre Superfähigkeiten einsetzen können.

Neben Ms. Marvel schlüpft der Spieler auch in die Rollen der anderen fünf Avengers und zieht mit menschlichen oder computergesteuerten Mitstreitern in den Kampf. Jeder besitzt andere Fähigkeiten: Kamala kann ihren Körper verformen, Iron Man bekämpft die Gegner aus der Luft mit Raketen und Black Widow wirbelt im Nahkampf flink die Gegner durcheinander. Zusammen mit Thor, Hulk und Captain America steht theoretisch eine breite Palette an Kampfstilen zur Verfügung, die Upgrades und Ausrüstung noch verfeinern können.

### Eintönige Missionen

In der Praxis ist egal, ob die Avengers Agenten befreien oder feindliche Stützpunkte zerstören. Das endet stets in Prügeleien, denen es an Übersicht fehlt. Präzise Atta-

cken sind in dem Chaos kaum möglich. Nur bei den Bosskämpfen gegen riesige Roboter, fliegende Festungen oder im wahrhaft epischen Finale blitzt der Spielwitz auf, an dem es in den eintönigen Missionen fehlt.

Am Ende der rund 15-stündigen Story-Kampagne geht es im sogenannten Endgame weiter. Von Abwechslung ist hier nichts zu spüren. Wenn die Superhelden zum wiederholten Mal die gleichen Gegner auf die gleiche Weise in ähnlicher Umgebung besiegt haben, sinkt die Motivation zum Weiterspielen.

Was bleibt, ist die Jagd nach neuer Ausrüstung. Die findet man auf dem Schlachtfeld oder bei Geschäftsleuten, aber bis das dafür nötige Geld gesammelt ist, dauert es sehr lange. Schneller geht es mit Mikrotransaktionen, bei denen man Ingame-Währung für Echtgeld kauft, um sie im Spiel einzusetzen.

Mittlerweile scheint es schon fast üblich, große Spieletitel nicht nur über ihren Verkauf, sondern auch über spätere Umsätze im Spiel zu finanzieren. Auch in Marvel's Avengers führt dieses Spielprinzip dazu, dass der Spieler entweder stundenlang die gleichen monotonen Missionen ausführt oder sich den Stress spart und mit ein paar Euros nachhilft. Origineller oder spannender wird das Spiel dadurch nicht. Für die Zukunft haben Entwickler Crystal Dynamics und Publisher Square Enix immerhin Zusatzinhalte angekündigt, wie den neuen Helden Hawkeye oder den Playstation-exklusiven Spider-Man. Für Marvel's Avengers wird es dennoch ein weiter Weg sein, um die Herzen der Fans zu erobern.

### Fazit

Marvel's Avengers ist ein Spiel der verpassten Möglichkeiten. Die Geschichte geht in wilder Superheldenaction unter und schickt den Spieler auf eintönige Missionen. Nur wer bis zum Ende durchhält, wird mit einem tollen Finale teilweise entschädigt. Der Rest ist eine auf Gewinnmaximierung ausgerichtete Videospielmarke, der es an Spielwitz und dem Herz der Vorlage fehlt. Ein Spiel nur für beinharte Superheldenfans.

(lmd@ct.de) **ct**

### Marvel's Avengers

Action-Rollenspiel	
Vertrieb	Square Enix, <a href="https://avengers.square-enix-games.com/de/">https://avengers.square-enix-games.com/de/</a>
Systeme	Windows ab 7, PS4, Xbox One
Preis	70 €
USK	ab 12 Jahre

# SMART LOSLEGEN

mit dem Node-RED Special von Make!

Jetzt auch  
komplett digital  
erhältlich!



## Make Special: Node-RED

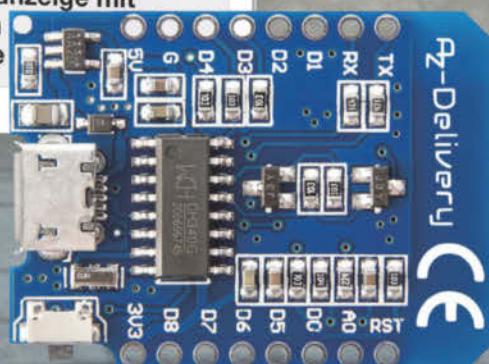
Für Einsteiger ohne tiefergehende Programmier-Kenntnisse bietet Node-RED die ideale Lösung. Man verknüpft fertige grafische Bausteine zu einem „Flow“ und kann so komplexe Anwendungen für IoT und Smart Home entwerfen.

Im neuen Make Node-RED Special bietet die deutsche Make-Redaktion Anfängern und Fortgeschrittenen einen leichten Einstieg in die Programmierung von Smart Homes. Das Heft wird portofrei inklusive eines ESP8266 D1 Mini mit WLAN geliefert!

[shop.heise.de/ma-nodered](http://shop.heise.de/ma-nodered)

24,95 € >

inkl. D1 Mini



Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.



heise shop

[shop.heise.de/ma-nodered](http://shop.heise.de/ma-nodered)



# Businessmodell DSGVO-Schadensersatz?

## Immer mehr Verbraucher klagen auf Schmerzensgeld wegen Datenschutzverstößen

**Mittlerweile gibt es in Deutschland Tausende von Verbrauchern, die von Unternehmen Schadensersatz wegen Verstößen gegen die DSGVO fordern. Falls Gerichte diese Forderungen bestätigen, könnte sich eine arbeitsteilig organisierte Klageindustrie entwickeln, die sich auf Datenschutzverstöße spezialisiert.**

Von Tim Wybitul

Massenklagen von Verbrauchern haben Konjunktur. Bei Aktionärsklagen oder den sogenannten Dieselprozessen sprechen Medien manchmal sogar von einer „Klageindustrie“. Oft arbeiten Verbraucheranwälte, Prozessfinanzierer, Legal-Tech-Firmen und andere spezialisierte Anbieter eng zusammen. Auch Datenschutzklagen sind ein attraktives neues Geschäftsmodell geworden.

Nach Artikel 82 der Datenschutz-Grundverordnung (DSGVO) haben natürliche Personen bei Datenschutzverstößen nicht nur einen Anspruch darauf, Anwaltskosten oder ähnliche materielle Schäden ersetzt zu bekommen, sondern auch sogenannte immaterielle Schäden, also Schäden, die jemandem an seiner Gesundheit, Ehre oder Freiheit zugefügt werden. Letztlich geht es um eine Art Schmerzensgeld für die Verletzung von Persönlichkeitsrechten.

In der Praxis kommt es zu solchen Schadensersatzklagen oft dann, wenn Datenpannen oder andere Security-Unfälle bekannt werden. Die Kläger argumentieren in diesen Fällen, dass das von dem

Vorfall betroffene Unternehmen die nach Artikel 32 DSGVO vorgeschriebene Datensicherheit nicht gewährleistet habe. Aufgrund dieses Verstoßes seien die Daten der Kläger rechtswidrig offengelegt worden – häufig stellen Hacker derartige Daten nach einem erfolgreichen Zugriff auf Firmensysteme schließlich auch ins Netz.

Nach Ansicht der Kläger stellt schon die Offenlegung ihrer Daten einen zu erstattenden Schaden dar. Demnach führe beispielsweise bereits die Verbreitung personenbezogener Daten zu einem Verlust der Kontrolle über die eigenen Daten, der nach den Erwägungsgründen zur DSGVO einen erstattungsfähigen Schadensposten darstellt. Zudem argumentieren Verbraucheranwälte und ihre Mandanten, dass insbesondere Erwägungsgrund 146 zur DSGVO einen weiten Schadensbegriff vorsehe. Richter sollten daher den Schadensersatz nach Art. 82 DSGVO „wirksam“ im Sinne der Rechtsprechung des Europäischen Gerichtshofs (EuGH) – und damit abschreckend – auslegen.

Um eine solche abschreckende Wirkung zu erzielen, müssten Gerichte den Klägern allerdings hohen Ersatz für immati-

terielle Schäden zusprechen. Dies ginge in die Richtung eines Strafschadensersatzes nach US-amerikanischem Vorbild, die sogenannten „Punitive Damages“. Auch wenn es für deutsche Verhältnisse ungewöhnlich klingt, hat das Arbeitsgericht Düsseldorf mit dieser Argumentation einem Kläger nach Art. 15 DSGVO immateriellen Schadensersatz von 5000 Euro zugesprochen. Sein ehemaliger Arbeitgeber hatte ihm eine Datenschutzauskunft verspätet und nur unvollständig übermittelt [1]. Gegen das Urteil ist der Arbeitgeber allerdings in Berufung gegangen, eine endgültige Entscheidung steht noch aus.

### Wer spielt mit?

Allein in Deutschland gibt es derzeit mehrere tausend Anspruchsteller, die von Unternehmen Schadensersatz nach Art. 82 DSGVO fordern. Das Modell der Klagen wegen vermeintlicher oder tatsächlicher Verstöße gegen die DSGVO ist aber nicht nur für möglicherweise geschädigte Verbraucher sehr interessant: Auch Prozessfinanzierer, Klägeranwälte und Legal-Tech-Firmen sehen hier große Chancen auf finanziellen Profit.

**Sind Sie vom easyJet Datenleck betroffen? Dann haben Sie Anspruch auf Schadensersatz!**

**MIT UNS GELD SICHERN**

**Was Ihnen zusteht**

- Ein monetärer Ausgleich Ihres Schadens.
- Eine Auskunft darüber, welche Ihrer Daten veröffentlicht wurden.
- Ein Anspruch darauf, dass eine Veröffentlichung jetzt und zukünftig unterbleibt.

**Was Sie tun können**

Die Ihnen zustehenden Rechte mit unserer Hilfe einfordern, indem Sie unser Formular ausfüllen.

Wenn ein möglicher Datenschutzverstoß mit vielen potenziell Betroffenen bekannt wird, schalten manche Anbieter schnell Werbung, posten Infos auf ihren Social-Media-Konten und bieten Onlineformulare auf ihren Websites, damit sich Kläger registrieren können. Oft bieten diese Anbieter dann an, die Anwälte zu stellen und den Prozess komplett auf eigene Kosten zu führen.

Einige Anbieter versprechen dem Verbraucher im Erfolgsfall dann beispielsweise 75 Prozent der eingeklagten Schadenssumme – den Rest kassiert der Anbieter. Teilweise kaufen auch Legal-Tech-Unternehmen Ansprüche aus einem DSGVO-Schaden auf, um diese dann in eigenem Namen gebündelt geltend zu machen. Deutschland steht da eher am Anfang. In Großbritannien dagegen haben auf Massenklagen spezialisierte Kanzleien und Prozessfinanzierer bereits Milliardenklagen erhoben, um Schadensersatzansprüche wegen Datenschutzverstößen durchzusetzen.

### Sechsstellige Beträge

Bevor sie Klagen einreichen, schicken die Anwälte der Anspruchsteller Schreiben, in denen sie teilweise sehr hohen Schadensersatz geltend machen. Gegebenenfalls fordern sie das Unternehmen auch auf, die Daten des potenziellen Klägers nicht mehr zu verarbeiten, und drohen mit Unterlassungsverfügungen. Manche Klägeranwälte nutzen Eilverfahren auf Erlass einer einstweiligen Unterlassungsverfügung dann auch als Testfall. Sie wollen erfahren, welche Gerichte dazu neigen, für Kläger positive Entscheidungen wegen festgestellter DSGVO-Verstöße zu fällen. In aller Regel fordern die Kläger zudem umfangreiche Auskünfte über die Verarbeitung ihrer Daten auf Basis von Art. 15 DSGVO. Sie möchten so in Erfahrung bringen, wie die Verarbeitung abgesichert war und wo ihre Daten überall gelandet sein könnten.

Wenn es zum Gerichtsverfahren kommt, machen die Kläger dann vor allem immateriellen Schadensersatz geltend. In Deutschland liegen solche eingeklagten Forderungen pro Fall zwischen wenigen Hundert Euro bis hin zu sechsstelligen Beträgen. Im Prozess muss das Gericht dann erst einmal herausfinden, ob überhaupt ein DSGVO-Verstoß vorliegt – und wer einen solchen Verstoß beweisen muss.

Stellt das Gericht einen Verstoß fest, muss es dann klären, ob der Kläger einen immateriellen Schaden darlegen kann.

### Tipp: Der c't-Datenschutz-Podcast

Rechtsanwalt Tim Wybital, der Autor dieses Artikels, war auch Guest im c't-Datenschutz-Podcast „Auslegungssache“. In Episode 21 erläuterte er die rechtlichen Grundlagen zu Schadensersatzforderungen, seine Bewertung davon und beispielhaft auch bereits ergangene Urteile.

Alle 14 Tage bespricht c't-Redakteur Holger Bleich mit c't-Autor und Verlags-



justiziar Joerg Heidrich im Podcast aktuelle Entwicklungen rund um den Datenschutz. Alle Folgen des Podcasts finden Sie unter [ct.de/auslegungssache](http://ct.de/auslegungssache). Außerdem können Sie ihn kostenlos über Podcast-Verzeichnisse wie iTunes, über Spotify oder direkt über den Feed auf der Homepage abonnieren. Das Team erreichen Sie unter [auslegungssache@ct.de](mailto:auslegungssache@ct.de).

Nach den meisten einschlägigen Urteilen ist hierfür eine spürbare Beeinträchtigung von einiger Erheblichkeit nötig, etwa durch eine öffentliche Bloßstellung oder die Weitergabe sensibler oder sogar intimer Daten. Deutschen Richtern reichen wegen dieser sogenannten Erheblichkeitsschwelle rein subjektiv empfundene Beeinträchtigungen bislang meistens nicht aus.

### Zunehmender Druck

Eine einheitliche Linie gibt es in der Rechtsprechung aber bislang noch nicht. Viele potenzielle Kläger hoffen darauf, dass die Gerichte in kommenden Verfahren beim immateriellen Schaden und bei weiteren Prozessfragen weniger strenge Maßstäbe anlegen werden. Diese Hoffnung beruht unter anderem darauf, dass manche Instanzgerichte und vor allem der EuGH in den letzten Jahren sehr „datenschutzfreundliche“ Entscheidungen gefällt haben, die oft zugunsten der jeweiligen Kläger ausgingen. Zum Schadensersatz nach Art. 82 DSGVO selbst hat der EuGH bislang keine Entscheidung gefällt. Es ist zumindest nicht ausgeschlossen, dass das höchste EU-Gericht künftig gute Rahmenbedingungen für Schadensersatzklagen nach Datenschutzverstößen schaffen wird.

Der Druck auf datenverarbeitende Unternehmen hat auf jeden Fall bereits deutlich zugenommen. Ganz im Sinne des Gesetzgebers sorgt der Anspruch auf Schadensersatz in der DSGVO dafür, dass zumindest in vielen Firmen mehr Sorgfalt im Umgang mit personenbezogenen Daten herrscht und Prozesse überdacht und neu dokumentiert werden.

Denn: Eine gute Vorbereitung auf Schadensersatzklagen nach Art. 82 DSGVO

kann in Gerichtsverfahren sehr hilfreich sein. Unternehmen sollten bereits dann tätig werden, wenn sie Indizien für eine Datenpanne oder einen sonstigen möglichen Datenschutzverstoß feststellen. Eine schnelle und gut – also gerichtsfest – dokumentierte Sachverhaltsaufklärung hilft dabei. Sehr nützlich ist auch, wenn man zeitnah eingeleitete Maßnahmen zur Schadensminderung nachweisen kann.

### Fazit

Massenklagen wegen Datenschutzverstößen könnten sich in Deutschland zu einem ernsthaften Risiko für Unternehmen entwickeln. Fehler beim Datenschutz betreffen oft eine große Anzahl von Kunden, Mitarbeitern oder sonstigen betroffenen Personen. Verliert man ein einziges Verfahren vor Gericht, muss man damit rechnen, dass Klägeranwälte, Prozessfinanzierer und andere Anbieter dies nutzen, um weitere Kläger anzuwerben.

Derzeit ist noch nicht absehbar, ab welcher Erheblichkeitsschwelle Gerichte künftig Klagen auf immateriellen Schaden wegen Datenschutzverstößen stattgeben. Auch andere wichtige prozessuale Fragen solcher DSGVO-Klagen sind noch ungeklärt. Unternehmen sind daher gut beraten, schnell zu reagieren, wenn sie in ihrem Geschäftsbetrieb Anhaltspunkte für mögliche relevante Verstöße gegen datenschutzrechtliche Vorgaben feststellen. Das hilft nicht nur ihnen, sondern jedem davon Betroffenen.

(hob@ct.de) ct

### Literatur

[1] Arbeitsgericht Düsseldorf, Urteil vom 5.3.2020, Az. 9 Ca 6557/18

# Tipps & Tricks

# Sie fragen – wir antworten!

## Netzwerkpfad mit Laufwerksbuchstaben einbinden

Ich arbeite ständig auf einem Server und möchte einen dort liegenden Unterordner dauerhaft mit einem Laufwerksbuchstaben im Explorer einbinden. Der bietet mir aber nur das Einbinden von \\Server, nicht jedoch von \\Server\Pfad\ zum\Ordner an. Kann der Explorer das nicht?

Mit dem Windows-Explorer geht das in der Tat nicht, aber mit der Eingabeanforderung. Starten Sie die und tippen Sie dort Folgendes ein:

```
net use u: \\Server\Pfad\ zum\Ordner ↵
    ↵/persistent:yes
```

Statt u: können Sie auch einen beliebigen anderen (freien) Laufwerksbuchstaben von d: bis z: angeben. Der Parameter /persistent:yes sorgt dafür, dass das Laufwerk nach einer Neu-Anmeldung an Windows wiederhergestellt wird. Ist das neue Laufwerk einmal angelegt, erscheint es auch im Explorer. Los werden Sie es durch net use u: /delete, mehr zum Befehl spuckt net help use aus.

(axv@ct.de)

## Linux: Bitte-nicht-stören-Modus für den Xfce-Desktop

Manche Desktop-Umgebungen bieten einen Nicht-Stören-Button, mit dem sich alle Benachrichtigungen abschalten lassen. Wie mache ich das unter Xfce?

Der Nicht-Stören-Modus des Xfce-Desktops verbirgt sich in den Systemeinstellungen unter „Benachrichtigungen“. Schieben Sie hier im Register „Allgemein“ den Schieberegler neben „Bitte nicht stören“ nach rechts.

Schneller ist der Regler zur Hand, wenn Sie ein Icon dafür auf der Bild-

Bitte nicht stören:  
Über das eigens hinzugefügte Glockensymbol im Panel schalten Sie auf dem Xfce-Desktop die Benachrichtigungen ab und wieder an.



schirmleiste hinterlegen. Klicken Sie das Xfce-Panel dazu mit der rechten Maustaste an und wählen Sie „Leiste/Neue Elemente hinzufügen“. Suchen Sie hier nach „Benachrichtigungserweiterung“, markieren Sie den Eintrag und bestätigen Sie mit „Hinzufügen“.

Ein Klick auf das Glockensymbol öffnet nun einen kleinen Dialog mit dem Schieberegler, sodass Sie den Nichtstören-Modus schnell an- und wieder abschalten können. Am ausgegrauten Glockensymbol erkennen Sie, dass der Modus aktiv ist. Hier finden Sie auch ein Protokoll der Benachrichtigungen, die Sie verpasst haben.

(lmd@ct.de)

in der Fritzbox gehandhabt; es bekommt eine \*\*62X-Nummer, die Sie für interne Rufe an alle anderen angeschlossenen Telefone, unabhängig von der Anschluss-technik (analog/SIP/DECT), nutzen können. Das Telefonbuch der DECT-Station ist mangels passender Schnittstelle leider nicht nutzbar.

(amo@ct.de)

## Bookmarks gegen Phishing

Um gefälschten Links beim Phishing zu entgehen, wird häufig empfohlen, Homebanking und andere kritische Seiten nur über Bookmarks aufzurufen. Können Lesezeichen aus der Ferne nicht manipuliert werden?

Theoretisch sind Szenarien zur Manipulation von Lesezeichen denkbar. Mögliche Wege wären etwa bösartige Add-ons oder Lücken in der Lesezeichen-Synchronisierung zwischen verschiedenen Browser-Installationen. Uns ist aber derzeit kein solcher Fall bekannt.

Praktisch überwiegen die Vorteile eines Lesezeichens jedenfalls ganz eindeutig: Manipulierte Links setzen häufig auf den Austausch einzelner Zeichen (zum Beispiel O statt O) und darauf, dass Sie diesen Austausch nicht bemerken. Ein Lesezeichen zu nutzen, statt auf einen zugesandten Link zu klicken, schützt zuverlässig vor solchen Tricks.

Selbst beim händischen Abtippen der URL kann es Ihnen passieren, dass Sie sich vertippen. Angreifer nutzen auch gefälschte Domains, die absichtlich häufige Tippfehler enthalten (etwa Buchstabendreher, wie in googel.com oder mircosoft.com). Auch in solchen Fällen schützen Bookmarks. (mon@ct.de)

## Registry-Eintrag nach jedem Upgrade verschwunden

Ich habe in meiner Windows-10-Installation in der Registry einen Eintrag geändert. Doch nach jedem Einspielen eines der halbjährlich erscheinenden Upgrades, die Microsoft als „Funktionsupdates“ bezeichnet, ist die Änderung wieder weg. Gibt es einen Weg, das zu verhindern?

Leider nicht: Bei jedem Upgrade wird Windows frisch installiert und anschließend übernimmt das Setup-Programm Dateien, Anwendungen und Einstellungen aus der alten Installation in die neue – allerdings nur jene, von denen es weiß. Dieses Wissen zu erweitern, vermag nur Microsoft selbst.

Was Sie aber machen können, um die Änderungen nicht nach jedem Upgrade erneut durchspielen zu müssen: Exportieren Sie den geänderten Schlüssel über dessen Kontextmenü in eine REG-Datei. Nach einem Upgrade reicht dann ein Doppelklick auf diese Datei, um die Änderung wieder im System zu haben.

Obacht: Es lassen sich nur ganze Schlüssel, aber keine einzelnen Einträge exportieren. Die REG-Datei dürfte daher in meisten Fällen mehr Einträge enthalten als nötig. Das können Sie leicht ändern: Starten Sie Notepad.exe und ziehen Sie die exportierte REG-Datei per Drag & Drop hinein. Die obersten zwei Zeilen („Windows Registry Editor Version 5.00“ sowie eine Leerzeile) müssen bleiben. In der

nächsten Zeile steht in eckigen Klammern der Schlüsselname, darunter Zeile pro Zeile die einzelnen Einträge. Löschen Sie einfach alle überflüssigen Zeilen und speichern Sie die Datei, fertig.

Sie können auch die Inhalte mehrerer REG-Dateien zusammenkopieren: Einfach jeweils die Zeile mit dem Schlüsselnamen in eckigen Klammern und darunter die Zeile für den Eintrag ans Ende einer anderen REG-Datei kopieren. (axv@ct.de)

Fragen richten Sie bitte an

 [hotline@ct.de](mailto:hotline@ct.de)

 [c't Magazin](#)

 [@ctmagazin](#)

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter [www.ct.de/hotline](http://www.ct.de/hotline).

## Viren-Samples

Zum Testen meiner Schutzmaßnahmen bräuchte ich ein paar Viren und/oder Trojaner. Kann c't so etwas zur Verfügung stellen?

Nein, das können wir leider nicht. Es gibt aber eine Reihe von Diensten im Internet, bei denen man – meist nach einer Registrierung – Malware-Samples bekommen kann. Eine Übersicht über solche Dienste bietet etwa der Blog von Lenny Zeltser (alle Links unter [ct.de/yx4t](http://ct.de/yx4t)).

Falls es darum geht zu prüfen, ob Virenscanner anschlagen, sind EICAR-Testdateien die bessere Wahl. Sie sind harmlos, Virenscanner erkennen sie vereinbarungsgemäß aber trotzdem, um genau solche Tests zu ermöglichen. Über den Emailcheck von heise Security können Sie sich auch Mails mit diesen Dummy-Viren zuschicken lassen. (ju@heise.de)

**Sample-Provider und EICAR-Dateien:**  
[ct.de/yx4t](http://ct.de/yx4t)

## FAT32 gleich exFAT?

Meine externe Toshiba-Festplatte lässt sich unter Windows nur mit NTFS (Standard) oder exFAT formatieren. Ich brauche aber FAT32. Wird das eventuell unter exFAT angeboten?

Nein, dabei handelt es sich um verschiedene Dateisysteme. FAT32 wird vom Betriebssystem wahrscheinlich nicht angeboten, weil die Festplatte dafür „offiziell“ zu groß ist; Microsoft setzt bei Partitionen über 32 Gigabyte auf NTFS. Für Laufwerke bis etwa 2 Terabyte helfen Tools wie der Fat32Formatter oder H2-Format (siehe [ct.de/yx4t](http://ct.de/yx4t)). Darüber geht FAT32 nur noch mit nativen 4K-Sektoren, die sind aber eigentlich nur bei Server-Festplatten üblich. (ll@ct.de)

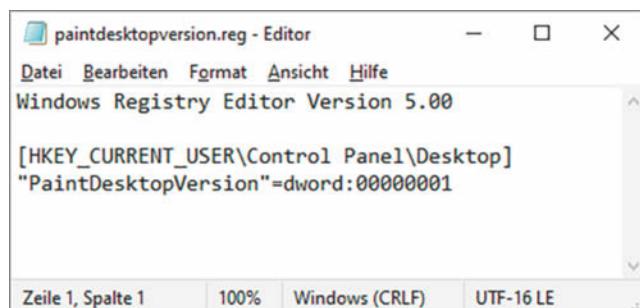
**Formatierungs-Tools:** [ct.de/yx4t](http://ct.de/yx4t)

## DoH über VPN

Seit einigen Monaten habe ich in meinem Firefox für „DNS über HTTPS“ (DoH) den DNS-Server der „Digitalen Gesellschaft“ hinterlegt. Gelegentlich nutze ich aber zusätzlich einen VPN-Anbieter. Was passiert in diesem Fall? Auf welchem Server geschieht dann die DNS-Auflösung?

Die DNS-Auflösung läuft beim DoH-Anbieter ab. Dafür müssen Sie auch nichts ändern, wenn Sie einen VPN-Tunnel in Betrieb nehmen. Der Firefox-Browser baut dann eben seinen TLS-Tunnel innerhalb des VPN-Tunnels auf, um den konfigurierten DoH-Server zu erreichen.

Nachteilig ist daran, dass es (ein wenig) mehr Rechenaufwand kostet und die Pakete länger unterwegs sind, weil ja die DoH-Pakete des Firefox-Browsers zunächst zum Endpunkt Ihres VPN-Anbieters reisen und erst von dort zum DoH-Server. Das hat zur Folge, dass komplexe Webseiten, für deren Aufbau zahlreiche DNS-Anfragen erforderlich sind, langsamer aufgebaut werden. (dz@ct.de)



Dass Windows bei einem Upgrade nicht all Ihre Registry-Änderungen übernimmt, kann nur Microsoft selbst ändern. Mit einer exportierten REG-Datei sind Änderungen nach dem nächsten Upgrade aber ruckzuck restauriert.

## Thunderbird 78 verbindet sich nicht

❓ Nach einem Update von Thunderbird auf Version 78 kann ich auf eines meiner IMAP-Konten nicht mehr zugreifen. Es sieht so aus, als würde der Zugriff eine Weile versucht und dann passiert nichts weiter; es kommt nicht einmal zur Abfrage des Passworts. Hätten Sie eventuell eine Idee, was da schiefläuft?

❗ Es könnte daran liegen, dass Thunderbird seit Version 78 die veralteten Verschlüsselungsstandards TLS 1.0 und 1.1 nicht mehr unterstützt. Falls der IMAP-Server nur diese Versionen unterstützt, kommt es zu dem beschriebenen Fehler. Eine deutliche Fehlermeldung zeigt Thunderbird leider nicht an.

Ob das bei Ihnen der Fall ist, können Sie prüfen, indem Sie temporär wieder TLS 1.0 und 1.1 erlauben. Dazu gehen Sie wie folgt vor:

1. Scrollen Sie in Thunderbirds Programmeinstellungen ganz nach unten, drücken Sie auf die Schaltfläche „Konfiguration bearbeiten“ und bestätigen Sie die Warnung.
2. Suchen Sie die Einstellung „security.tls.version.min“ und ändern Sie ihren Wert auf „1“.
3. Schließen Sie das Fenster und starten Sie Thunderbird neu.

Falls die Mail-Abfrage so funktioniert, sind tatsächlich die TLS-Versionen das Problem – und damit vermutlich Ihr Mailprovider, der wohl ausschließlich veraltete Versionen unterstützt. An ihn sollten Sie sich wenden, um das Problem dauerhaft zu beheben.

(syt@ct.de)

## Schriftart zerstört Systemüberwachung

❓ Ich habe in meinem Gnome-Desktop die Schriftart für Monospace-Text auf „JetBrains Mono“ umgestellt, sowie Sie es in den Tipps der Ausgabe 20/2020 beschrieben haben. Alles ist wunderbar, bis auf meine Ubuntu-Systemüberwachung. Da sind alle Zeichen durch ein Rechteck ersetzt. Ein Zurückwechseln auf „Ubuntu Mono Regular“ oder ein Neustart des Systems hilft nichts. Habe ich mir mein gesamtes Font-System zerschossen?

❗ Nein, das Problem lässt sich wohl relativ einfach beheben. Die Ubuntu-

Systemüberwachung hat sich anscheinend am Variable-Font verschluckt, der in Version 2 von „JetBrains Mono“ dazugekommen ist. Diese variablen Varianten der Schriftart brauchen Sie aber auch nicht unbedingt. Sie können sie einfach entfernen, indem Sie JetBrainsMono-Variable.ttf und JetBrainsMono-Variable-Italic.ttf aus dem Installationsort der Schriftart löschen (üblicherweise in /usr/share/fonts/). Danach sollte sich die Systemüberwachung wieder lesbar präsentieren. (syt@ct.de)

## Wochentag in Windows-Taskleiste

❓ In meiner Taskleiste stehen ganz rechts die Uhrzeit und darunter das Datum. Ich würde dort auch gern den Wochentag anzeigen lassen, aber anscheinend gibt es in den Einstellungen keine passende Option?

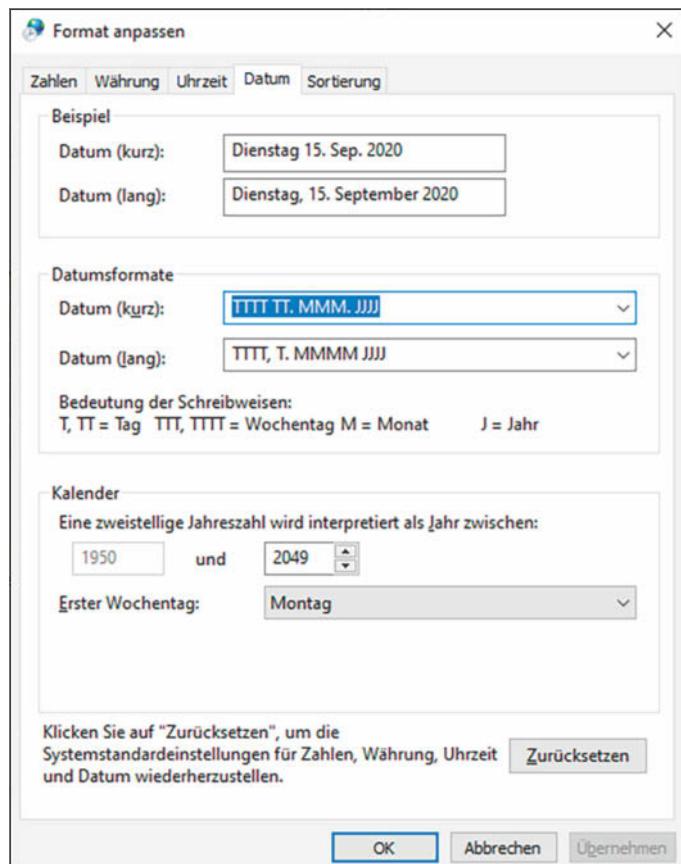
❗ Es gibt zwei Möglichkeiten. Die einfachere: Vergrößern Sie Ihre Taskleiste auf mindestens zwei Zeilen, dann erscheint der Wochentag als Zeile zwischen Uhrzeit und Datum. Dazu klicken Sie erst mit der rechten Maustaste auf einen leeren Bereich der Leiste und stel-

len sicher, dass im Kontextmenü „Taskleiste fixieren“ *nicht* ausgewählt ist. Dann positionieren Sie den Mauszeiger am oberen Rand der Leiste, sodass er zu einem Doppelpfeil wird. Nun können Sie die Leistenhöhe mit gedrückter linker Maustaste ändern.

Falls die höhere Taskleiste nicht Ihrem Geschmack entspricht, ist die zweite Möglichkeit vielleicht eher was für Sie: Drücken Sie Windows+R und tippen Sie ins „Ausführen“-Feld intl.cpl ein. Es öffnet sich ein Dialog namens „Region“, in dem Sie im Reiter „Formate“ unten auf „Weitere Einstellungen“ klicken. Es erscheint der nächste Dialog, in dem Sie im Reiter „Datum“ den Cursor ins Feld „Datum (kurz)“ setzen, um von Hand vorne TTTT zu ergänzen (Leerzeichen dahinter nicht vergessen). Nach einem Klick auf „Übernehmen“ erscheint der Wochentag in der Taskleiste neben dem Datum. Falls Sie den Wochentag nur abgekürzt anzeigen lassen wollen („Mi“ statt „Mittwoch“), setzen Sie nur TTT statt TTTT an den Anfang.

Hinweis: Diese Änderung gilt für alle Stellen im System, an dem das kurze Datumsformat verwendet wird, etwa bei den Datumsanzeigen in der Detailansicht des Explorers.

(axv@ct.de)

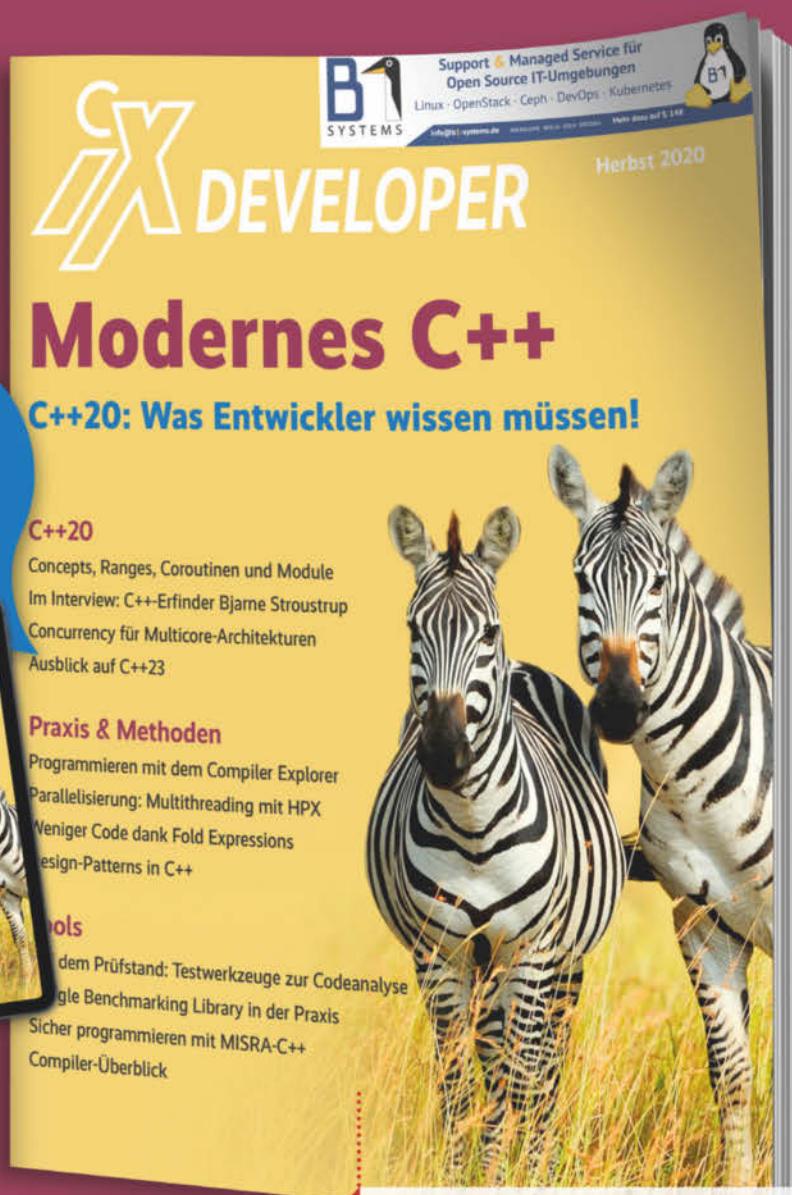


Damit Windows den Wochentag in der Taskleiste anzeigt, kann man sie vergrößern oder die Anzeige für „Datum (kurz)“ ändern.

# C++20: Was Entwickler wissen müssen!

NEU  
im heise shop

Auch  
digital  
als PDF!



## IX DEVELOPER Modernes C++

Noch in diesem Jahr soll **C++20** erscheinen, der neue Standard für C++. Das IX-Sonderheft stellt die **zentralen Features** des Standards vor und liefert einen spannenden Einblick in die **vier großen Neuerungen**. Zusätzlich gibt das Heft eine Übersicht zur Kernsprache, der Bibliothek und Concurrency. ix-Artikel der letzten 2 Jahre zu C++ geben außerdem einen umfassenden Überblick für Entwickler.

[shop.heise.de/ix-dev-c++20](http://shop.heise.de/ix-dev-c++20)

Einzelheft  
für nur

14,90 € >



# FAQ

# Windows kaufen

**Viel Geld zu sparen beim Windows-Kauf ist verlockend, doch welche Schnäppchen stellen gültige Lizenzen dar? Darüber gibt es immer wieder heftige Diskussionen und sogar juristische Auseinandersetzungen, wie auch die kürzlichen Hausdurchsuchungen beim Billiganbieter Lizengo zeigen.**

**Von Axel Vahldiek**

## Das Problem

FAQ Eine FAQ zum Kauf von Windows?  
Was ist daran so schwierig?

! Wenn man Software kaufen möchte, findet man kaum etwas Komplizierteres als die Produktpolitik von Microsoft in Bezug auf Windows 10. Das geht schon damit los, dass es diverse Editionen mit unterschiedlichem Funktionsumfang gibt (Home, Pro, Enterprise und je nach Zählweise noch Hunderte weitere). Eine Übersicht über die Editionsvielfalt haben wir in [1] zusammengetragen.

Microsoft vertreibt Windows zudem mit sehr unterschiedlichen und komplexen Lizenzmodellen, beispielsweise vorinstalliert auf neuen oder gebrauchten Rechnern, in Schachteln unterschiedlichen Inhalts, per Mail, in Bündeln entweder pro Nutzer oder pro Rechner lizenziert („Volumenlizenz“), und so weiter und so fort. Die Angebote für Privatkunden sind

dabei noch relativ einfach zu durchschauen, Firmen beispielsweise üben hingegen einen ständigen Spagat zwischen „so viel wie nötig“ und „nicht mehr als nötig“ – geht der schief, bezahlen sie entweder zu viel oder zu wenig, und im letzteren Fall droht dann sogar juristischer Ärger. Ein besonders weites Feld ist der Handel mit Gebrauchtlizenzen: Prinzipiell ist es zwar durchaus zulässig, Software gebraucht zu handeln – sogar solche, die ursprünglich per Download ausgeliefert wurde –, es gibt aber eine Menge Wenns und Abers.

## Was man bekommt

FAQ Was genau bekomme ich, wenn ich Windows kaufe?

! Das unterscheidet sich von Fall zu Fall. Nur eines bekommen Sie grundsätzlich: Eine Lizenz, also das Recht, Windows nutzen zu dürfen. Der Verkäufer muss dazu

allerdings seinerseits das Recht besitzen, Ihnen dieses Nutzungsrecht einräumen zu dürfen. Zusätzlich erhalten Sie üblicherweise die Software, entweder bereits vorinstalliert auf einem PC oder aber separat zum Selbstinstallieren, etwa in Form einer DVD, eines USB-Sticks oder eines Downloads. Schließlich bekommen Sie einen Installationsschlüssel, wobei Ihnen dieser bei vorinstallierten PCs großer Anbieter nicht in ausgedruckter oder digitaler Form ausgehändigt wird, sondern im Klartext in der ACPI-Tabelle MSDM der Firmware des Mainboards steckt.

## Was ist eine Lizenz?

FAQ Was genau bedeutet denn dieses Nutzungsrecht für mich?

! Das hängt von der Lizenz ab. Für Privatkunden gilt die Faustregel: Eine Lizenz berechtigt Sie zum Betreiben genau einer Windows-Installation auf genau einem Rechner, mehr nicht. Es gibt allerdings Grauzonen. Bei einer Parallelinstallation beispielsweise ist zwar sichergestellt, dass immer nur eine der Installationen läuft, während die andere inaktiv auf dem Datenträger liegt. Will man beide Installationen abwechselnd betreiben, will Microsoft als Urheber das nicht erlauben. Der Haken daran: Es ist ungeklärt, ob man in diesem Fall überhaupt die Erlaubnis des Urhebers braucht. Das kann nur ein Gericht entscheiden. Doch das setzt wiederum eine entsprechende Klage voraus, und die ist nicht in Sicht.

Anders sieht es beispielsweise mit einer virtuellen Maschine (VM) aus: Die läuft gleichzeitig mit dem Wirtsbetriebssystem und benötigt daher unstrittig eine separate Lizenz.

Microsoft bietet auch Lizenzen an, die andere Nutzungsformen erlauben, doch sind die für spezielle Zielgruppen gedacht

**Wer bei Microsoft die deutschsprachigen Lizenzbestimmungen („Product Terms“) herunterlädt, erhält ein 148 Seiten langes Textdokument, das wohl kaum jemand durchliest.**

(Firmen, Behörden, Bildungseinrichtungen) und meist nur unter bestimmten Voraussetzungen zu erwerben und einzusetzen.

## Wozu eine Lizenz?

Was soll ich mit einer Lizenz? Die Installationsdateien kann ich doch einfach mit dem Media Creation Tool von [microsoft.com/software-download/windows10](https://microsoft.com/software-download/windows10) herunterladen. Was mir fehlt, ist doch bloß der Installationsschlüssel.

Technisch gesehen mag das stimmen, rechtlich sieht es anders aus. Der Urheber einer Software, im Falle von Windows also Microsoft, hat zunächst einmal alle Rechte daran. Er kann im Rahmen der gesetzlichen Vorgaben frei entscheiden, unter welchen Bedingungen und zu welchem Preis seine Software von anderen eingesetzt werden darf. Erfüllen Sie die Bedingungen, räumt er Ihnen das Nutzungsrecht ein, sprich er erteilt Ihnen eine Lizenz. Der Einsatz von Windows ohne Lizenz ist daher ein Verstoß gegen Microsofts Rechte und kann juristisch verfolgt werden.

Das gilt im Übrigen auch für andere Software: So dürfen Sie unter der GNU General Public License (GPL) stehende Software kostenlos einsetzen und sogar vertreiben. Bei Letzterem müssen Sie aber die Lizenzbedingungen einhalten, die für diesen Fall vorschreiben: Den Quellcode mitgeben oder einen Hinweis beilegen, dass man den Code auf Anforderungen erhalten kann. Verstoßen Sie dagegen, kann Ihnen auch hier juristischer Ärger drohen. Es gibt zwar Software, mit der man tatsächlich machen kann, was man will, doch selbst dazu muss der Urheber zuvor die Erlaubnis erteilt haben. Um es deutlich zu sagen: Es besteht kein Recht auf Software, die möglichst billig oder gar umsonst ist.

## Schlüssel gleich Lizenz?

Wenn ich einen Schlüssel kaufe, habe ich damit nicht automatisch eine Lizenz erworben?

Leider nein. Installationsschlüssel dienen zwar als Nachweis für den Besitz einer Lizenz, aber nicht jeder Schlüssel taugt dazu. So gibt es beispielsweise generische Schlüssel, die zwar vom Windows-Setup-Programm, aber nicht von Microsofts Aktivierungsservern akzeptiert



Ganz legal und trotzdem kostenlos kann man die Insider-Vorabversionen sowie die 90-Tage-Testversionen von Windows nutzen. Wenn auf einem neuen PC Windows 10 bereits vorinstalliert ist, zahlt man gefühlt ebenfalls nichts dafür – ist zwar nicht korrekt, aber dennoch die günstigste Art des Windows-Kaufs.

werden. Zudem könnte der Schlüssel geklaut oder unerlaubt mehrfach genutzt sein, und dann hat man trotz Schlüssel kein Nutzungsrecht.

## Aktivierung als Beweis?

Bei mir hat mit dem erworbenen Installationsschlüssel nicht nur das Installieren von Windows geklappt, sondern auch das Aktivieren. Das sollte doch nun reichen als Beweis der Gültigkeit meiner Lizenz, oder?

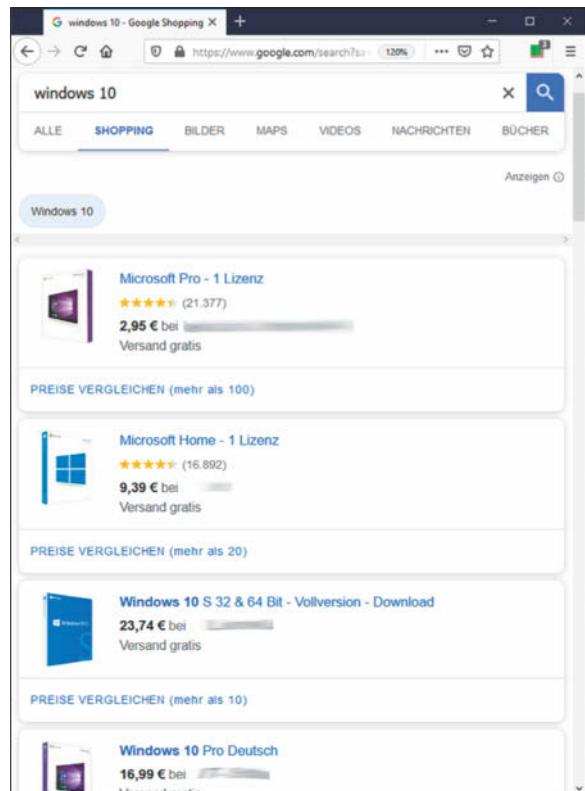
Ärgerlicherweise lautet die Antwort auch hier: Nein. Denn Microsoft stellt keineswegs technisch sicher, dass ein Schlüssel nur dann aktiviert wird, wenn eine gültige Lizenz dahintersteckt. „Aktivierung auf Vertrauensbasis“ nennt Microsoft das. Als Folge könnte ein Händler denselben Schlüssel gleich an mehrere Kunden verhökern, und deren Installationen könnten sich anfangs sogar erfolgreich aktivieren lassen. Dennoch hätten die Käufer kein Nutzungsrecht erworben. Das bekommen sie aber üblicherweise erst nach einiger Zeit zu spüren, etwa beim nächsten Upgrade auf eine neuere Windows-10-Version, denn dabei wird der Schlüssel erneut überprüft und gegebenenfalls gesperrt. Windows verliert dadurch die Aktivierung und lässt sich mit diesem Schlüssel nicht mehr erneut aktivieren.

Es gibt auch Installationsschlüssel, die für Wirtschaftsräume außerhalb der EU bestimmt sind. Deren Verkauf ist hierzulande nicht erlaubt, und wenn Sie trotzdem so einen Schlüssel kaufen, erwerben Sie damit keine Lizenz – dennoch klappt üblicherweise das Aktivieren. Ähnlich sieht es beispielsweise mit Schlüsseln aus, die aufgrund geschlossener Verträge nur von Angehörigen von Bildungseinrichtungen genutzt werden dürfen – gehören Sie nicht dazu, wird das Aktivieren zwar klappen, doch haben Sie dennoch kein Nutzungsrecht. Lizizenzen aus Visual-Studio-Abonnements (ehemals MSDN) dürfen größtenteils nur für Testzwecke genutzt werden, auch hier sagt also das erfolgreiche Aktivieren erst mal nichts aus über das Nutzungsrecht.

## Lizenzgültigkeit erkennen

Wenn weder der Installationsschlüssel noch eine erfolgreiche Aktivierung als Beweis der Gültigkeit meiner Lizenz dienen, was dann? Es muss doch Möglichkeiten geben, das irgendwie zu erkennen.

Und wieder lautet die Antwort: Nein. Leider weigert sich Microsoft bis heute, Nutzern gangbare Wege zu eröffnen, mit denen sie die Gültigkeit ihrer Lizenz überprüfen können. Auch für so manchen seriösen Händler ist das fatal, denn so fehlt



**Das Internet ist voll von billigen Windows-Angeboten. Doch ob man für den Kaufpreis auch wirklich eine Lizenz bekommt, ist vom Einzelfall abhängig.**

[3]. Das Angebot ist zwar offiziell eigentlich schon seit Jahren ausgelaufen, doch meinte Microsoft das Ende offensichtlich nicht ernst. So akzeptiert das Windows-10-Setup-Programm bis heute die Schlüssel der alten Windows-Versionen, doch diese Fähigkeit hat Microsoft dem Setup-Programm erst nach Auslaufen des Angebots beigebracht, was nur mit Absicht zu erklären ist. Zudem erkennen Microsofts Aktivierungsserver, zu welcher Version ein Installationsschlüssel gehört. Dass Windows-10-Installationen dennoch bis heute mit alten Schlüsseln aktiviert werden, ist ebenfalls nur mit Absicht zu erklären. Falls Sie gern volle Rechtssicherheit in dieser Frage hätten: Die könnte nur eine Gerichtsentscheidung bringen. Doch die Indizien sprechen sehr dafür, dass Microsoft an einer solchen Entscheidung gar kein Interesse hat, und Sie nichts zu befürchten haben, wenn Sie das Gratis-Upgrade nutzen. Achtung: Die Aktivierung beim Gratis-Upgrade ist mitunter tückisch, den Details haben wir eine separate FAQ gewidmet [4].

ihm eine Möglichkeit, einem Kunden zu beweisen, dass er ihn nicht betrügt. Microsofts Ziel ist dabei offensichtlich, vor allem Firmen- und andere Großkunden dazu zu bewegen, direkt bei Microsoft oder bei offiziell autorisierten Partnern einzukaufen – was im Vergleich zu anderen Anbietern oft teurer kommt. Es freuen sich allerdings auch schwarze Schafe unter den Händlern, denn der Kunde hat ja kaum eine Chance, Händler sicher einschätzen zu können.

bei Microsoft und deren Partnerunternehmen.

### Ich will es gratis

Was ist, wenn ich kein Geld für Windows ausgeben kann oder will?

Sofern Sie eine Windows-Lizenz dann weder von Freunden noch von Bekannten oder Verwandten geschenkt bekommen, stehen Ihnen zwei Optionen offen. Sie können die 90-Tage-Testversion von Windows 10 Enterprise nutzen, die jedermann ganz legal und kostenlos bei Microsoft herunterladen und nutzen darf. Der Haken: Die Installation ist nur 90 Tage nutzbar und lässt sich nicht in eine dauerhaft nutzbare umwandeln – es bleibt also nur die Neuinstallation. Die zweite Option ist der Einsatz von Vorabversionen aus dem Insider-Programm [2], was ebenfalls jedermann kostenlos möglich ist. Allerdings sind die nicht immer ganz stabil. Zudem übermitteln sie an Microsoft in erheblichem Umfang Daten, zu denen auch sehr private gehören können – Sie zahlen letztlich also doch, nämlich mit Ihren Daten.

Sofern Sie noch eine Lizenz von Windows 7, 8 oder 8.1 besitzen, die Sie nicht mehr verwenden, können Sie die per Gratis-Upgrade in Windows 10 umwandeln. Eine unverändert gültige Anleitung finden Sie in

### Ich will es rechtssicher

Und wie kaufe ich nun Windows, ohne dabei rechtlichen Ärger zu riskieren?

Als Privatkunde kaufen Sie am bequemsten und günstigsten Windows 10 Pro oder Home, wenn Sie sich für einen neuen PC entscheiden, auf dem Windows vorinstalliert ist. Es gibt auch Anbieter, die Microsofts Erlaubnis haben, gebrauchte PCs mitsamt vorinstalliertem Windows zu verkaufen („Microsoft Authorized Refurbisher“, MAR, sowie „Microsoft Registered Refurbisher“). Ohne neuen PC greifen Sie zur System-BUILDER-Lizenz, die Sie bei einem seriösen Anbieter erwerben, der auch selbst PCs zusammenbaut (übliche Preise sind 90 Euro für Home und 140 für Pro).

Enterprise-Lizenzen hingegen gibt es nur im Paket und mit speziellen Verträgen

### Ich will es gebraucht

Kann ich Windows auch gebraucht kaufen? Man liest ja immer mal wieder, dass das verboten sei.

Anderslautenden Gerüchten zum Trotz ist der Kauf und Verkauf gebrauchter Software hierzulande sehr wohl erlaubt, und das gilt auch für Windows [5]. Sie dürfen beispielsweise einen gebrauchten Komplett-PC mit vorinstalliertem Windows erwerben und bekommen so eine Lizenz, die vorher jemand anderem gehörte. Auch einzeln kann man Windows ganz legal gebraucht kaufen: Eine System-BUILDER-Lizenz lässt sich handeln, sofern nur sichergestellt ist, dass der Verkäufer keine Kopie zurückbehält. Der Haken: Als Käufer können Sie oft nicht einschätzen, ob der Verkäufer korrekt vorgeht.

Was hier übrigens keine Rolle spielt, ist der gern zitierte „Erschöpfungsgrundsatz“. Es ist zwar durchaus korrekt, dass Microsoft nach dem erstmaligen Verkauf nicht mehr frei bestimmen kann, was man mit einem erworbenen Windows-Exemplar tun darf, doch das bedeutet keineswegs, dass Microsoft gleich alle Rechte daran verliert. So dürfen Sie zwar die erwähnte System-BUILDER-Lizenz weiterverkaufen, aber nur das ursprünglich erwor-

# EGAL WO... SPACE FASZINIERT!



## DAS IST SPACE

Vollgepackt mit informativen Artikeln und atemberaubenden Fotos berichtet Space über die Technik der Weltraumfahrt, ebenso wie über Astronomie und kosmische Phänomene.

## Testen Sie 2x Space mit 30 % Rabatt!

Nur 11,90 €\* statt 17,00 €\* im Handel!

Zusätzlich digital als PDF im Kundenaccount verfügbar.

Jetzt bestellen unter:

**[www.emedia.de/space-mini](http://www.emedia.de/space-mini)**

0541 80 009 126 [space-abo@emedia.de](mailto:space-abo@emedia.de)

eMedia Leserservice, Postfach 24 69, 49014 Osnabrück

\*Preise in Deutschland.

bene Exemplar und keine Vervielfältigungen davon.

## Ich will es billig

Ich will möglichst viel Geld sparen.  
Wie erkenne ich seriöse Händler?

Gemeinerweise gar nicht, denn Händler haben kaum eine Möglichkeit, Ihnen gegenüber ihre Seriosität nachzuweisen. Bei Gebrauchthändlern sollten Sie darauf achten, dass sie Quelle und Vorgeschichte der angebotenen Software offenlegen.

Hingegen können Sie mitunter schwarze Schafe erkennen. Einige Tipps dazu in Kurzform.

Angesichts von System-BUILDER-Preisen um die 100 Euro pro Lizenz können Sie davon ausgehen, dass Sie bei dramatisch billigeren Angeboten vielleicht eine zumindest vorerst gelingende Aktivierung bekommen, aber wohl kein echtes Nutzungsrecht.

Wenn ein Händler garantiert, dass das Aktivieren wirklich klappt, lügt er: Das Aktivieren erledigen Microsofts Server, und auf die hat er keinen Einfluss.

Verspricht der Händler Ersatzschlüssel bei Problemen, sollte das misstrauisch machen: Als Ihr Vertragspartner ist er ohnehin in der Pflicht bei Problemen mit der Ware, und das gilt auch, wenn das Aktivieren nicht klappt. Warum aber sollte er extra darauf hinweisen, dass es Probleme geben könnte?

Das Versprechen von „Original“-Schlüsseln sollte Ihre Warnlampen anhen lassen: Das Problem sind heutzutage keine gefälschten Schlüssel (die gibt es nach unserem Kenntnisstand nicht mehr), sondern geklauter oder unerlaubt mehrfach verwendete. Die sind zwar Original, doch hilft Ihnen das nicht.

Wenn Sie die Installationsdateien vom Server des Händlers herunterladen können, ist das ein Alarmsignal: Die Dateien darf er nur mit Erlaubnis von Microsoft zum Download bereitstellen, und die bekommen Billigheimer nicht.

Manche Händler versprechen Firmenkunden, sie durch „schriftliche Haftungsfreistellung“ von „allen Kosten“ freizustellen, die durch Lizenzprobleme auftreten könnten, doch das ist Humbug. Man denke nur an Folgekosten von Hausdurchsuchungen, womöglich inklusive Beschlagnahme von Hard- und Software, was womöglich noch Konventionalstrafen

nach sich zieht – die wird der Händler Ihnen kaum erstatten (können). Wenn den Verantwortlichen beispielsweise in einer Firma Geldstrafen auferlegt werden, darf sie der Händler schon von Gesetzes wegen nicht übernehmen.

Wer Lizizenzen aus Volumenverträgen als eigenständige anbietet, disqualifiziert sich. Denn solche sind stets Upgrade-Lizenzen, setzen also eine Basislizenz voraus. Meiden Sie Händler, die vermeintliche OEM-Enterprise-Lizenzen anbieten – die gibt es nicht.

## Ich will's noch billiger

Mir ist dieser ganze Juristenkram völlig wurscht, ich will es nur so billig wie möglich.

In aller Deutlichkeit: Wenn Sie alle rechtlichen Bedenken beiseite wischen, können Sie zwar viel Geld sparen, doch Sie handeln auf eigenes Risiko. Wenn es nur um eine Lizenz geht, wird der Kauf zwar gemäß des alten Prinzips „Wo kein Kläger, da kein Richter“ vermutlich folgenlos bleiben. Doch mit steigender Zahl der erworbenen Exemplare steigt auch die Wahrscheinlichkeit, dass man für fehlende Lizizenzen geradestehen muss, inklusive strafrechtlicher Konsequenzen [5]. Gera de Unternehmen sollten sicherstellen, dass sie nicht auf zwielichtige Geschäftemacher reinfallen.

Wenn Sie sich bewusst auf dubiose Händler einlassen, haben Sie zudem bei

Kaufproblemen keinerlei Hilfe von Dritten zu erwarten. Im Gegenteil: Sollten Sie einem Betrüger aufsitzen, könnte eine Anzeige bei der Polizei sogar dazu führen, dass Sie selbst Ärger bekommen.

## Aktivierungsproblem

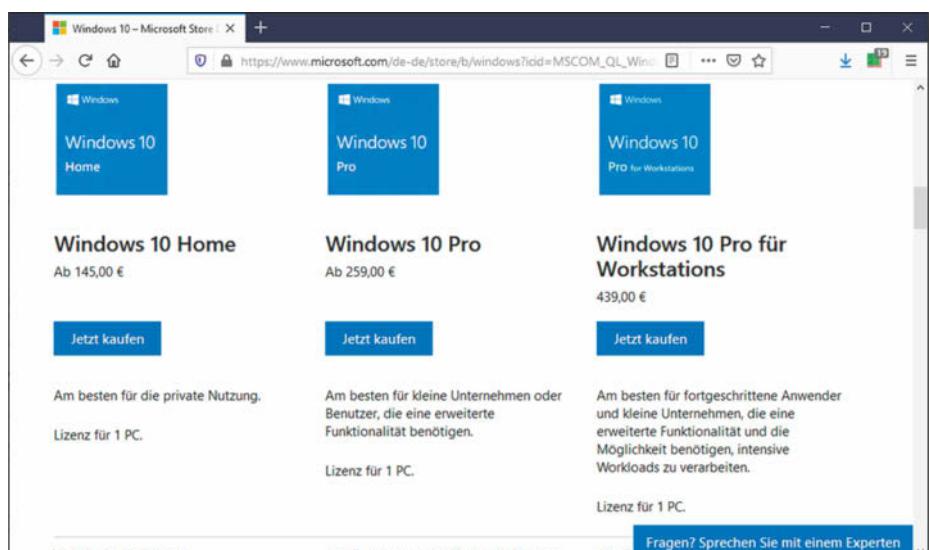
Meine gekaufte Windows-Lizenz lässt sich nicht aktivieren.

Prüfen Sie in diesem Fall zuerst, ob die Aktivierung korrekt abläuft: Gerade Schnäppchenjäger können auf die unterschiedlichsten Aktivierungsverfahren stoßen, und einige erfordern andere Handgriffe als andere. Eine Übersicht finden Sie in [6].

## Weiterhin Aktivierungsproblem

Das Aktivieren klappt immer noch nicht, ich verklage jetzt Microsoft!

Das wird in den meisten Fällen nichts bringen. Es ist immer der Verkäufer, der garantieren muss, dass eine verkauftte Ware funktioniert. Er ist dafür verantwortlich, dass die verkaufta Lizenz legal ist und funktioniert, und dazu gehört das erfolgreiche Aktivieren. Gibt es nach dem Kauf Probleme, muss der Verkäufer für eine Lösung oder Ersatz sorgen. Microsoft ist bei Aktivierungsproblemen also nur dann zuständig, wenn Sie die



Microsoft verkauft Windows gern an jedermann, allerdings zu horrenden Preisen – kein Wunder, dass sich viele da nach günstigeren Alternativen umsehen.

Lizenz direkt beim Konzern erworben haben.

Obacht: Nur weil der Verkäufer dafür verantwortlich ist, dass die Lizenz legal ist und funktioniert, bedeutet das keineswegs, dass Sie nach dem Kauf damit machen können, was Sie wollen. Wenn Sie beispielsweise eine legale Einzelplatzlizenz unerlaubt mehrfach verwenden, ist das nicht mehr Sache des Verkäufers, sondern ganz allein Ihre Verantwortung.

## Reingefallen

Ich habe den Verdacht, dass meine gekaufte Windows-Lizenz in Wirklichkeit gar keine ist. Und nun?

Sofern die Gewährleistungsfrist noch läuft, ist der Verkäufer der erste Ansprechpartner, doch ob das was bringt, steht auf einem anderen Blatt.

Bleibt der Gang zu einem Anwalt. Sofern es nur um eine einzelne Lizenz geht, dürfte der Streitwert allerdings so gering sein, dass das nicht lohnt – es läuft darauf hinaus, dass der Kaufpreis verloren ist. Immerhin brauchen Sie in diesem Fall wohl nicht zu befürchten, dass Microsoft oder sonst jemand Ihnen juristisch auf die Pelle rückt.

Haben Sie hingegen Lizizen in größerem Umfang womöglich gar für den kommerziellen Einsatz in einem Unternehmen oder Ähnliches erworben, sollten Sie vorsorglich mit Ihrem Anwalt sprechen.

## Lizengo

Sie erwähnten eingangs die Hausdurchsuchung bei Lizengo. Sind dort erworbene Lizizen also illegal?

Die Hausdurchsuchung hat noch keine rechtlichen Fakten geschaffen. Das kann erst eine Gerichtsentscheidung, die noch aussteht. Bislang ist daher unklar, wie die Sache ausgeht. Wir empfehlen jedoch, bis dahin nicht darauf zu vertrauen, dass bei Lizengo erworbene Lizizen rechtlich sicher sind.

## Lizengo in c't

Sie haben in 21/2019 Lizengo schon in der Überschrift bescheinigt, das Unternehmen vertreibe „Einwandfreie

Software legal erwerben: Schauen Sie in die Tipps.

Insbesondere im Internet kursieren viele auffällig günstige Software-Angebote. Diese müssen nicht zwangsläufig illegal sein. Seien Sie trotzdem vorsichtig. Ein extrem günstiger Preis kann ein Hinweis auf illegale Software sein.

Wie können Sie sich schützen? Die folgenden Punkte geben wichtige Hinweise, wie Sie legale von illegalen Angeboten unterscheiden können.

Alle erweitern | Alle zuklappen

- > Gefälschte Datenträger.
- > Der Verkauf einzelner Microsoft Echtheitszertifikate (COAs) ist per se illegal!
- > Verkauf von Microsoft COAs zusammen mit nicht zugehörigen PCs/Datenträgern ist per se illegal!
- > Der Verkauf von Microsoft COAs ist per se markenrechtlich unzulässig zusammen mit:
- ▽ Der Verkauf von „gebrauchter“ Software ist unter bestimmten Voraussetzungen zulässig.

Es ist rechtlich zulässig, „gebrauchte“ Microsoft Software zu verkaufen und zu nutzen, wenn die folgenden Voraussetzungen erfüllt sind, für die Ihr Verkäufer und Sie im Streitfalle die volle Beweislast tragen:

- Das Computerprogramm muss ursprünglich mit Zustimmung von Microsoft im Gebiet der EU oder eines anderen Vertragsstaates des Europäischen Wirtschaftsraums (EWR) in den Verkehr gebracht worden sein.

**Microsoft räumt selbst ein, dass der Handel mit gebrauchten Lizizen unter bestimmten Voraussetzungen erlaubt ist.**

Microsoft-Schnäppchen aus dem Supermarkt“. Und nun die Probleme?

Es passiert uns zum Glück zwar recht selten, aber in diesem Fall mussten wir unsere Einschätzung revidieren. Als Folge haben wir dem Thema in c't 5/2020 einen ganzen Schwerpunkt gewidmet und sind darin auch deutlich auf die revidierte Einschätzung zu Lizengo eingegangen [7, 8, 5].

## Lizenz tauschen

Ich habe einen Installationsschlüssel bei einem jetzt wieder verschwundenen Hökerer auf einem Online-Marktplatz erworben und mittlerweile so meine Zweifel, ob das eine gute Idee war. Also habe ich eine System-Builder-Lizenz erworben, die ich stattdessen nutzen will. Muss ich Windows dafür neuinstallieren?

Kommt drauf an: Sofern Sie dieselbe Edition wie die ursprüngliche erworben haben (Home, Pro ...), brauchen Sie nur den Installationsschlüssel auszutauschen. Dazu drücken Sie die Tastenkombination Windows+Pause und klicken auf „Product Key ändern“. Sie landen in den Tiefen der Einstellungs-App, wo Sie ebenfalls auf „Product Key ändern“ klicken. Hier geben Sie den neu erworbenen Schlüssel ein und folgen den weiteren Dialogen, bis Windows aktiviert ist.

Achten Sie beim Kauf darauf, welche Edition genau Sie erwerben: Es gibt Editionen mit sehr ähnlich klingenden Namen, beispielsweise „Home“ und „Home N“, die jedoch unterschiedliche Schlüssel haben und Schlüssel der jeweils anderen Edition nicht akzeptieren. Welche derzeit installiert ist, können Sie ebenfalls per Windows+Pause ablesen. Was scheitert, ist das Einpflanzen eines Home-Schlüssels in eine Pro-Edition. In der Gegenrichtung hingegen klappt es: Sofern Sie ein Home ohne N installiert haben, können Sie den Schlüssel einer Pro-Edition ohne N eingeben (funktioniert wie der Schlüsseltausch) und sitzen dann nach einem Neustart vor einem Pro. Haben Home und Pro jeweils ein N im Namen, klappt es genauso. (axv@ct.de)

## Literatur

- [1] Axel Vahldiek, Inflation der Editionen, Über die scheinbar simple Frage, wie viele Ausgaben von Windows 10 es gibt, c't 13/2018, S. 148
- [2] Jan Schüßler, FAQ: Windows Insider, c't 5/2020, S. 178, auch online unter ct.de/-3281564
- [3] Axel Vahldiek, Bombenräumung, Tipps zum immer noch kostenlosen Umstieg von Windows 7 auf 10, c't 26/2019, S. 20
- [4] Axel Vahldiek, FAQ: Aktivierung beim Gratis-Upgrade, c't 4/2018, S. 144, auch online unter ct.de/-3953069
- [5] Nick Akinci, Abenteuer Softwarekauf, Rechtliches zur Nutzung von Betriebssystemen und Standardprogrammen, c't 5/2020, S. 72
- [6] Axel Vahldiek, Lauter Freischalter, Was die Windows-Aktivierungsverfahren für Schnäppchenjäger bedeuten, c't 24/2019, S. 138
- [7] Axel Vahldiek, Einkaufs-Labyrinth, Geld sparen beim Windows-Kauf, c't 5/2020, S. 64
- [8] Axel Vahldiek, Labyrinth nach Microsoft-Art, Windows-10-Kauf ohne Risiko, c't 5/2020, S. 68



James Bridle  
**New Dark Age**

Der Sieg der Technologie und  
das Ende der Zukunft

C. H. Beck, München 2020 (2. Aufl.)  
ISBN 978-3-4067-4177-7  
320 Seiten, 25 €  
(Epub-/Kindle-E-Book: 19 €)

## Willkommen zurück, Mittelalter!

**Sichern technischer Fortschritt und Informationswachstum die Zukunft der menschlichen Gesellschaft? James Bridle glaubt, dass der Menschheit die Technik längst entglitten ist und ihren Spielraum tatsächlich immer stärker einengt, statt ihn zu erweitern.**

Der Autor, von Pressestimmen als „Vordenker“ und gar als „Popstar der Digitalisierungskritik“ apostrophiert, blickt mit den geschärfsten Augen eines Künstlers auf viele Weichenstellungen der letzten Jahre. Die alltägliche Informationsflut führt Bridle zufolge dazu, dass Menschen zwar potenziell immer mehr wissen, aber immer weniger tun können, um als richtig erkannte Ziele zu erreichen. Als Paradebeispiel dient ihm der Klimawandel, den eine informierte Menschheit aufgrund von Daten, die durch Computernetzwerke reisen, immer besser versteht. Der dadurch bedingte Energieverbrauch treibt aber seinerseits den Klimawandel voran.

Umgekehrt machen Extremwetterlagen der technischen Infrastruktur zu schaffen. Überhaupt weist Bridle auf Rückkopplungseffekte in vielen Wirkungsketten hin, wobei er gelegentlich mit dem groben Stift zeichnet: Ein erhöhter CO<sub>2</sub>-Gehalt in der Luft verlangsamt das menschliche Denken. So kommt es zu weniger neuen Erkenntnissen, aber zugleich beeinflusst die Informationsflut die Qualität der Forschung: Es entstehen zwar Unmengen an wissenschaftlichen Arbeiten, diese münden aber kaum noch in wirklich bahnbrechenden Forschungsergebnissen, so Bridle.

Der automatische Hochfrequenzhandel krempelt die Finanzwelt um; Rückkopplungen sorgen für absurd erscheinende Effekte an den Börsen. Unternehmen wie Amazon und Uber sind auf dem Weg zur vollständigen Automatisierung; Mitarbeiter werden zu temporären Lückenbüßern für die kommenden autonomen Systeme. Künstliche Intelligenz überträgt diese Mechanismen auf immer weitere Berufsfelder. Manch lebenswichtige Entscheidung treffen künftig Maschinen, deren interne Abläufe niemand mehr versteht – das sieht der Autor schon beinahe als unvermeidlich an. Er findet bisweilen verblüffende Zusammenhänge und belegt seine Erkenntnisse mit vielen beklemmenden Beispielen, größtenteils aus der jüngeren Vergangenheit.

Bridle bietet selbst keine Lösungen an – er will nur Denkanstöße geben und auf Missstände hinweisen. Was er sagt, lässt Leser nicht gleichgültig, sondern provoziert sie dazu, eine eigene Haltung zu finden. (Maik Schmidt/psz@ct.de)

## Gute Grundlagen

**Die grafische Programmiersprache Scratch richtet sich an Kinder und Jugendliche. Wie man damit eigene kleine Spiele entwickelt, erklärt dieses gut durchdachte Lehrbuch für Kids ab 8 Jahren mit viel Witz. Und auch die Theorie kommt nicht zu kurz.**

Im Online-Editor von Scratch puzzelt man vorgegebene Programmierblöcke ineinander und baut so den Code fürs eigene Projekt zusammen. Klingt einfach – aber die ersten Schritte in der grafischen Programmierumgebung sind gerade für jüngere Kinder ungewohnt. Auch für Eltern, die vielleicht Erfahrung mit klassischen Programmiersprachen mitbringen, ist der Scratch-Editor mit Bühne, Figuren und Kostümen Neuland.

Anhand von fünf vorbereiteten Projekten ebnen die Autoren Scratch-Einsteigern den Weg in diese Welt. Mit einer interaktiven Grußkarte geht es ganz einfach los. Das fünfte Projekt, ein Quizspiel, besteht dann schon aus mehr als 100 Programmierblöcken. Zu allen fünf Beispielen gibt es Links direkt zu den Projekten im Scratch-Editor. Sie lassen sich dort anschauen, ausprobieren und später auch nach eigenen Vorstellungen ändern und erweitern; zu solchen „Remixes“ ermuntern die Autoren ausdrücklich. Über QR-Codes gelangt man schnell zu den Projekten, weitere Codes führen zu YouTube-Videos mit allgemeinen Tipps zur Scratch-Programmierung.

Außer der Praxis vermittelt das Buch auch einiges an Theorie. Wer die knappen, kindgerechten Texte vollständig studiert, weiß anschließend, was ein Algorithmus ist und kennt den Unterschied zwischen Internet und World Wide Web. Für den nötigen Spaß sorgen die „Bugs“ – quietschbunte Monster aus der Feder des Illustrators Jan Radermacher. Sie wuseln über sämtliche Buchseiten und sind auch die Protagonisten der vorgestellten Programmierprojekte.

Gerade weil das Puzzlestein-Prinzip von Scratch Syntaxfehler weitgehend ausschließt, lernen Kinder damit nicht automatisch die besten Grundlagen für späteres textbasiertes Coding. Dazu bedarf es einer fundierten Einführung. Das Buch von Diana und Philipp Knodel macht alles richtig: Schritt für Schritt und sinnvoll aufeinander aufbauend erklären die Autoren bedingte Anweisungen, Variablen, Schleifen, Listen und vieles mehr. Beispielprojekte und Erklärvideos ergänzen den Inhalt dieses soliden Lehrbuchs perfekt.

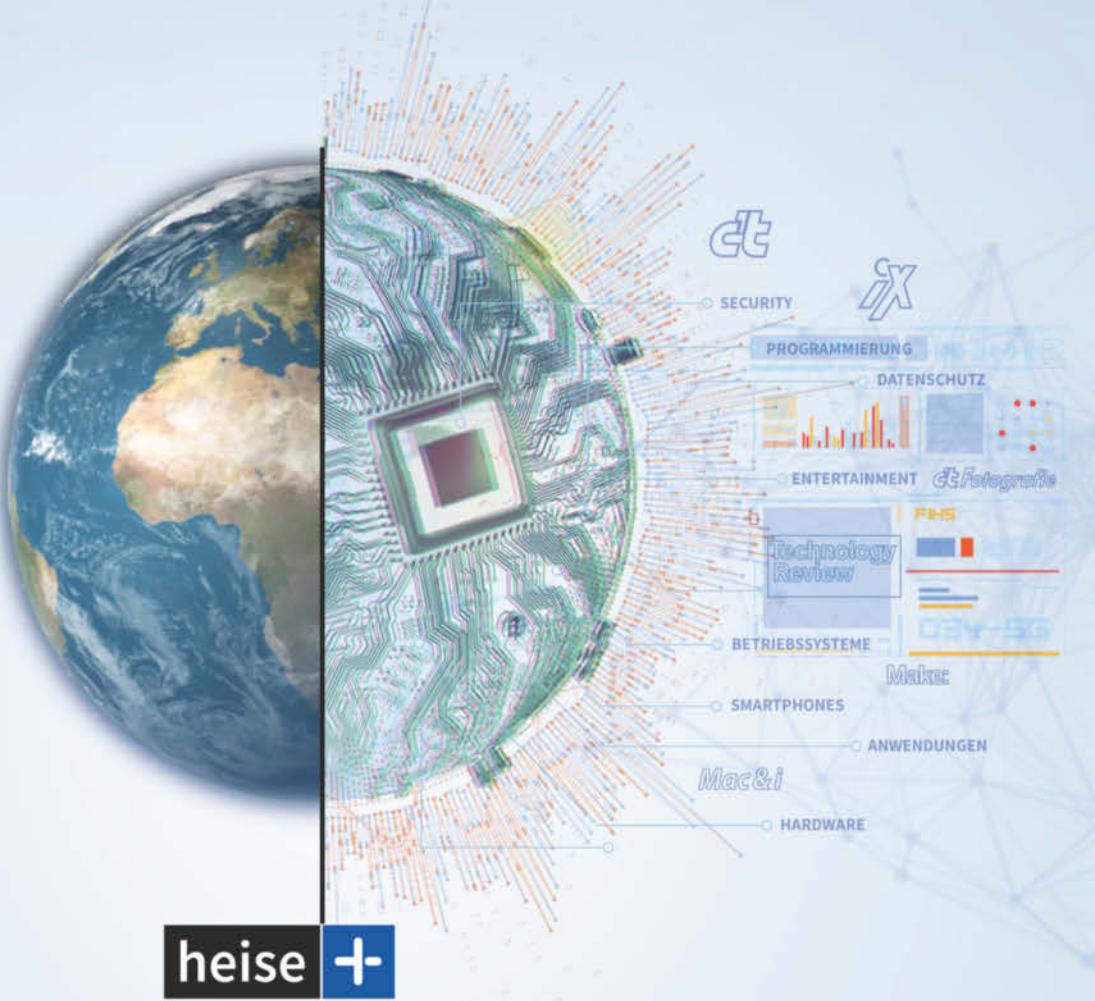
(dwi@ct.de)



Diana Knodel, Philipp Knodel,  
Jan Radermacher

**Einfach Programmieren lernen mit Scratch**

Carlsen, Hamburg 2020  
ISBN 978-3-5512-2083-7  
96 Seiten, 15 €  
PDF-/Epub-/Kindle-E-Book: 10 €



## Das digitale Abo für IT und Technik.

**Exklusives Angebot für c't-Abonnenten:** Lesen Sie zusätzlich zum c't-Magazin unsere Magazine bequem online auf [heise.de/magazine](http://heise.de/magazine) und erhalten Sie Zugang zu allen heise+ Artikeln.

- ✓ Für c't-Plus-Abonnenten 3 €/Monat für alle anderen c't-Abonnenten 5 €/Monat
- ✓ Jeden Freitag Leseempfehlungen der Chefredaktion im Newsletter-Format
- ✓ 1. Monat gratis lesen – danach jederzeit kündbar
- ✓ c't, iX, Technology Review, Mac & i, Make, c't Fotografie direkt im Browser lesen

**Sie möchten dieses Exklusiv-Angebot nutzen?  
Unser Leserservice hilft Ihnen gern beim Einrichten.**

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

📞 0541 80009 120



Weitere Informationen zum Abo-Upgrade finden Sie unter:

**[heise.de/plus-info](http://heise.de/plus-info)**



# EINE AUFGABE FÜRS LEBEN

VON DANIEL SCHLEGELE

Über ihr wölbte sich die azurne Kuppel – an den Rändern ausgebleicht, im Zentrum geschwärzt, als läge das Universum blank. Darunter ein zu Sand kristallisiertes Meer, das bis an den Horizont reichte. Die Dünen flüsterten dunkel, Myriaden Sandkörner rannen herab, spülten übereinander wie Perlen aus Silizium. In der Ferne flimmerte die Luft und erschuf spiegelnde Pfützen. Es roch abgestanden. Und vertraut.

Mit einem weiteren Atemzug zerstob die Illusion.

Irene löste den Blick von der Wand und richtete ihn auf das Bett, auf die Frau, die unter der ockerfarbenen Bettdecke ruhte. „Guten Morgen, Mama.“

Schlaftrige Augen musterten sie. „Musst du los?“

„Gleich. Hab noch ein bisschen. Frühstück habe ich dir gemacht.“

„Wann kommst du wieder?“

„Spätestens heute Abend. Dann können wir noch *Sky-city Detective* schauen.“

„Gerne.“

Gedankenvoll betrachtete Irene ihre Mutter, dann strich sie ihr, einem Impuls folgend, sanft über die Haare. Leise schloss sie hinter sich die Tür. Durch einen Korridor aus Farnen und Bäumen bog sie ins Wohnzimmer; mit einer Geste zum Sensor rodete sie den Urwald – zurück blieb ein silbergraues Tuch, das die Wände bespannte. Der Geruch von frisch gemähtem Gras hing noch für einen Moment in der Luft, bevor auch er entschwand.

Schriftzeichen wanderten über ihre Brillengläser. Stiller Anruf. Judith. Ihr implantierter Chip nahm das Gespräch an.

„Hallo“, flötete es in ihrem Ohr.

„Schon wach?“

„Immer noch! Nachschicht ist vorbei.“

„Tja, ich muss gleich los – der Kreislauf des Lebens, was?“

„Wohl eher des Arbeitens. Du bist noch auf der Suche?“

„Eifrig. Und demotiviert.“

Ihre Freundin lachte. „Was steht heute an?“

„Vorstellungsgespräch bei der Datenagentur Cheng“, entgegnete Irene und wählte eine dunkelblaue Bluse aus ihrem Kleiderschrank.

„Persönlich oder per Netz?“

„Persönlich. Man besteht drauf.“

„Tatsächlich? Wird die Agentur von Dinosauriern geleitet?“

Irene zögerte mit der Antwort. „Deren Annonce klang auch ein wenig ... ungewöhnlich? Also, man sucht jemanden, der Netzingenieure überwacht. Klasse-vier-Netzingenieure, um genau zu sein. Das soll angeblich nicht übers Netz gehen.“

„Aha. Und was sind Klasse-vier-Netzingenieure? Haben die ganz, ganz besondere Bedürfnisse?“

„Nicht den blassensten Schimmer. Noch nie mit denen zu tun gehabt.“

„Wahrscheinlich 'ne inoffizielle Bezeichnung. Aber wenn man der Nomenklatur folgt: Klasse-zwei sind KIs, die Dreier Algorithmen – dann stehen die Vierer also noch unterhalb deiner geliebten Algorithmen. Ha, sind's vielleicht Rechenschieber?“

„Man sagte mir lediglich, es seien Umgeschulte. Klingt für mich vielmehr, als müsse ich mich um die Wünsche verwirrter Neunetzer kümmern. Kaffee kochen, Geschichten vorlesen, Händchen halten.“

„Vermutlich auch füttern und den Mund abwischen?“

„Wie gesagt, keinen Schimmer, wirklich nicht.“ Irene betrachtete sich im Spiegel. „Passt.“ Sie griff zum Make-up und folgte den Anweisungen, die ihr das Display einblendete.

„Ansehen kann man es sich ja zumindest.“

„Klar. Scheint zudem eine Netzfirma mit eher wissenschaftlich angehauchtem Hintergrund zu sein. Wenn die nicht seriös ist, weiß ich auch nicht.“ Irene trat vom Spiegel zurück. Sie zog die Stirn kraus. „Keine Ahnung, wann ich mich das letzte Mal geschminkt habe ...“

„Wie geht's eigentlich deiner Mutter?“

„Ganz gut. Sie erholt sich langsam vom Unfall.“

„So schnell wird sie bestimmt nicht mehr ins Netz abtauchen.“ Judith blieb für einen Moment still. „Bleibende Schäden hat sie aber nicht davongetragen, oder?“

„Nein, nein, der Arzt meinte, dass sie vollständig genesen wird. Aber einen neuen Anschluss, den braucht sie auf jeden Fall. Gibt's noch mal eine Rückkopplung, brennt der wahrscheinlich durch ... und brät ihr Gehirn gleich mit.“

„Hat sie schon einen Termin?“

„In dieser Woche noch. Bis dahin meidet sie das Netz ... Sie schläft viel. Und sie schaut sich mit mir *Sky-city Detective* an!“

„Tatsächlich?“

„Ja, sie fiebert sogar richtig mit!“

Über die hellgrauen Tücher wanderte eine Kolonne aus Ziffern und Buchstaben.

„Hör zu, ich muss los.“

\* \* \*

Irene scheiterte daran, den Respirator in ihrer Tasche zu verstauen. Beim erbosten Versuch, ihn wieder herauszuziehen, verhakte sich der Aufsatz für die Duftaromen am Reißverschluss, wodurch ihr das Gerät beinahe aus der Hand rutschte. Sie ächzte, verkniff den Mund, errötete.

„Sieht hübsch aus“, bemerkte der Rezeptionist, ein junger Mann in weißem Anzug. Seine beiden Schläfensteckplätze hatten die Gestalt goldener Sterne. „Selbst verziert?“

Irene hielt mit einem scheuen Lächeln inne. Rote und gelbe Farbwirbel bedeckten das Atemgerät. „Sonderedition.“

„Hübsch“, bekundete er erneut. „Man hat jetzt Zeit. Ich bringe dich rüber.“

Ehe sie sich versah, hatte er sie durch den Korridor in einen Konferenzraum geführt, verabschiedend genickt und sie allein gelassen.

Blanke Wände, leere Bildrahmen als Ausdruck eines absonderlichen Kunstverständnisses, zweifarbiges, verwaist wirkendes Mobiliar. In seiner Sterilität erwies sich das Innere der Datenagentur Cheng als geradezu erfrischend gegenüber der abgasvernebelten Stadt. Dem Raum haftete ein chemischer Zitrusgeruch an, der olfaktorische Rückstand des verwendeten Putzmittels. Irgendwo schnarrte die Klimaanlage.

Auf der Irene gegenüberliegenden Raumseite öffnete sich eine Tür. Eine Frau und ein Mann traten ein. Irene begrüßte sie mit einer Verbeugung.

„Willkommen bei der Datenagentur Cheng“, begann die Frau breit lächelnd. „Dies ist Herr Cheng, ich bin Frau Marchand. Sie müssen Irene Ablett sein, die Bewerberin auf die Technikerstelle. Wie geht es Ihnen?“

„Persönlich hier zu erscheinen, das ist schon ein wenig ungewöhnlich, muss ich gestehen.“

## „DIE NETZINGENIEURE SIND DAS KAPITAL DIESER AGENTUR.“

„Wir betreiben mit unseren Ingenieuren ein separates Netz, abgekoppelt vom globalen. Das dient der Sicherheit, um der Gefahr überschwappender Instabilitäten vorzubeugen. Daher können Sie nur von hier aus auf die Daten zugreifen. Und wer nicht gewillt ist, bereits für ein Vorstellungsgespräch hierherzukommen, nun, der ist ungeeignet für den Job, finden Sie nicht auch? Haben Sie Erfahrung im Umgang mit Klasse-eins-Netzingenieuren?“, fügte Marchand beiläufig an.

„Klasse-eins? Menschen? Oh, also ...“

„Oder mit etwas Vergleichbarem?“

Irene presste die Lippen zusammen, während sie ihr Gedächtnis nach etwas durchforstete, was den freundlichen, beschämend bohrenden Blick der Frau mildern konnte. „Ich habe mal nebenher auf einige Zweier aufgepasst. Während der Uni habe ich das gemacht, hin und wieder für ein paar Stunden in der Nacht. Quasi als Aushilfe für die Profis. Also den Quellcode kontrollieren und aufpassen, dass die ihn nicht selbst umschreiben, Stichproben durchführen, ob die Arbeit nach den Richtlinien erfolgt ist. Solche Dinge.“

„Für wie lange war das?“

„Hm ... Ein, zwei Semester bestimmt.“

Marchand nickte. „Klasse-vier-Netzingenieure sind eine Neuheit, sollten Sie wissen, eine kleine Rarität zwischen all den professionellen Netzen und den Hochleistungs-KIs. Die Arbeit hier erfordert ein Fingerspitzengefühl, das das nüchterne Abarbeiten gegenüber einem Klasse-Zweier deutlich übersteigt. Von Algorithmen ganz zu schweigen. Angesichts Ihrer fehlenden Erfahrung in diesem Bereich weiß ich jedoch

nicht, ob wir Ihnen guten Gewissens die Obhut über unsere Netzingenieure überlassen können. Was meinst du?“

„Die Netzingenieure sind das Kapital dieser Agentur“, meinte Cheng stolz. „Ihre Überwachung benötigt viel Intuition, viel Einfühlungsvermögen. Geht man zu unbedarf an die Sache heran, kann der Arbeitsprozess empfindlich gestört werden. Uns schwebt daher eine Technikerin vor, die bereits Erfahrungen mit diffizilren Überwachungsobjekten vorweisen kann.“

Irene seufzte resigniert. „Ich verstehe.“

„Dennoch bedanken wir uns für Ihren Besuch“, meinte Marchand. „Wir melden uns bei Ihnen.“

„Da Sie nun schon einmal hier sind“, setzte Cheng an, „hätten Sie Interesse, unsere Umgeschulten einmal kennenzulernen?“

Irene knetete ihre Finger, gedanklich noch mit der Enttäuschung ringend. „Nun ... ja. Ja, gerne, warum nicht?“

Cheng führte sie in einen Trakt, an dessen Ende ein Körperscanner sowie zwei Wachleute standen. Nach der Überprüfung des implantierten Personalchips ließ man sie passieren. Über eine Treppe gelangten sie in eine verglaste Kanzel etliche Meter über dem Erdboden. Den Großteil des hell erleuchteten Raums nahm eine Konsole ein.

„Das ist unsere Technikerin Yana“, sagte Cheng. „Sie wacht am Tage über unsere Netzingenieure.“

Eine Frau schielte über die Kontrollanzeigen hinweg. „Erfreut“, grüßte sie und richtete ihr Augenmerk wieder auf die Monitore. Statt Haare bedeckten mehrere Steckplätze ihre linke Kopfhälfte, von denen ein einzelner mit der Konsole verbunden war.

Irene schaute durch das Glas auf das Innere einer umgebauten Lagerhalle. In regelmäßigen Abständen reihten sich metallene Objekte aneinander – aufrecht stehende Kästen, die wie Sarkophage anmuteten. Aus ihnen wucherten Kabelbündel gen Hallendecke.

„Die Netzingenieure sind in den Containern?“

„Genau. Wir bezeichnen dies übrigens nicht als Container, sondern als Kammern.“

„Ist das so etwas wie eine neue Generation von KIs?“

„Nein, nein. Das sind echte Menschen dort drinnen. Wir können uns gerne einen ansehen. Sofern Sie nicht zu empfindlichen Gemüts sind. Viele unserer Netzingenieure sind körperlich versehrt. Kriegsveteranen, Kryounfälle, Strahlvergiftungen. Eine Handvoll musste mit Stammzellen aufgezüchtet werden, um überhaupt ein funktionsfähiges Nervensystem zu schaffen.“

Ahnungslos, was sie erwartete, folgte sie Cheng in die Halle. Zuerst bemerkte sie den sanften Luftzug, der den unaufdringlichen, flüchtigen Duft von Wacholder brachte, und daraufhin die langsam, beruhigenden Klänge einer Sinfonie.

Cheng spazierte durch die Reihen und blieb plötzlich stehen. Er winkte zur Kanzel hinüber.

„Die Nummer siebzehn, bitte!“

Der Metallsarg spaltete sich in der Mitte, klappte aus einander und offenbarte einen gläsernen, mit Flüssigkeit gefüllten Tank. Eine Silhouette, entfernt menschlich und unvollständig, kam zum Vorschein. Die rechte Körperhälfte fehlte, das Gehirn war teilweise entblößt, Muskelstränge, Organe und Knochen lagen frei. Mehrere Kabel waren mit

dem Leib verbunden, ein Anschluss mit dem Durchmesser eines Taus spross aus dem Hinterkopf. Obgleich der Mann grauenvoll entstellt war, wirkte er seltsam friedlich. Seine geschlossenen Augenlider zuckten, als erlebte er einen Traum.

„Das sind die fleischlichen Überreste von Viktor Brauer“, erklärte Cheng. „Im Krieg hat ihn eine Granate schwer verwundet, sodass man ihn kryokonservierte und später in solch eine Kammer legte.“

„Dieser Mensch lebt noch?“, argwöhnte Irene.

„Sehen Sie das Lidzucken? Mitunter öffnen sie auch die Augen, aber sie sehen nichts. Es sind nur Muskelreflexe. Was lebt, ist eben das Restbewusstsein. Stunden nicht der Tank und die Flüssigkeit zwischen ihm und der Außenwelt, würde er sterben. Hier ist er vor Bakterien und Viren geschützt sowie generell vor dem weiteren Verfall bewahrt.“

„Und die Musik?“

„Ohne die Sinneseindrücke funktioniert es nicht. Ihr Verstand verödet sonst, kollabiert, stirbt ab. Obgleich sie ausschließlich im Netz leben, nehmen sie dennoch mit ihren Sinnen die weltliche Umgebung wahr. Mit Musik oder elektrischer Stimulanz kann man sie gewissermaßen erden, sie daran erinnern, dass sie noch leben. Oder die Luft, die ihre Kammern umweht und ihnen so etwas wie Körperlichkeit verleiht. Die Kammern sind daher mit einer Vielzahl von Sensoren ausgestattet, die die Reize an das Nervensystem weitergeben – sozusagen ihr Anker in der echten Welt.“

„Herr Cheng?“, hallte es aus den Lautsprechern.

„Hm?“

„Kommen Sie rauf, die Sensoren schlagen aus. Und nehmen Sie Ihren Besuch mit.“

In der Kanzel empfing Yana sie mit verschränkten Armen und düsterer Miene. Vorwurfsvoll deutete sie auf die Konsole. „Sehen Sie?“

Cheng beugte sich über die Anzeigen, beäugte sie wie eine Sammlung Diamanten. „Sonderbar“, murmelte er, mehr fasziniert als verärgert. „So leid es mir tut, aber ich muss unseren Rundgang hiermit beenden.“

Nachdem er Irene zur Rezeption begleitet hatte, räusperte er sich und verstaute die Hände in den Hosentaschen. „Eins noch – und verzeihen Sie, falls Ihnen diese Frage seltsam erscheint: Tragen Sie ein Parfüm?“

„Ähm ... ja.“

„Welches? Wenn ich fragen darf?“

„Belsa. Mit Fliederduft.“

„Es ist nur wegen der Netzingenieure. Sie haben auf irgendetwas reagiert.“

„Ja ... nun, danke für die Führung“, sagte Irene, verbeugte sich und schritt zum Ausgang. Hinter der Entlüftungsschleuse zog sie sich ihren Respirator über das Gesicht, warf den Plastikmantel über und trat hinaus auf die Straße.

\* \* \*

Alles bebte, als sich der Zug in die Kurve legte; dumpfes Fluchen hallte wie ein Echo durch die Menge der Fahrgäste. Irene umklammerte die Haltestange. Wie beiläufig wanderten ihre Augen über die Leute und deren Respiratoren. Etliche Standardausführungen, pragmatisch gehalten, kaum Farben oder Verzierungen. Allenfalls zwei, drei beeindru-

ckende Modelle, geformt zu japanischen Samuraimasken, dazwischen ein Selbstbau in Form eines Ritterhelms. Ansonsten nur Plastikhartschalen mit Kunststoff- oder Gummischläuchen. Problemlos fügten sie sich in das farbliche Gesamtbild aus Handschuhen und schmucklosen Plastikmänteln, die über der Kleidung getragen wurden, damit der Gestank sich dort nicht hineinlegte. Sie bemerkte die Blicke, die ihren Respirator liebkosten – die Halbmaske verbarg ihr breites Lächeln.

Auf der Straße drang ein fauliges Miasma in ihre Nase, das selbst der Filter nicht zu neutralisieren vermochte. Reflexartig drehte sie an ihrem Aromaauflsatz und speiste die Maske mit einem Kirschparfüm. In den Häuserschluchten versickerte derweil eine senfgelbe Wolke – die Wolken, die in der Ferne über den Elektrowerken aufstiegen, wölbten sich hingegen in einem olivfarbenen Spektrum.

„Wie lief's?“, empfing Judiths Stimme Irene.

„Absage“, antwortete sie stumm, von einem Chip aus ihren Gehirnwellen ausgelesen.

„Och, schade.“ Ein Seufzen. „Aber bestimmt gibts irgendwo noch eine Stelle in der Algorithmen-Sparte.“

Irene schnaufte mit desillusioniertem Amusement. „Man kann Zweier darauf abrichten, einen Dreier zu überwachen und zu optimieren. Schneller und besser als ein Mensch das kann. Also spart man die Dreier-Techniker ein und beschäftigt stattdessen lieber einen Zweier-Techniker mehr.“

„Um Produkte noch verkaufen zu können, bleibt denen wohl keine Wahl. Außer man schuftet für den Staat oder für eine Forschungseinrichtung, aber das ist eher was für Idealisten. Ohnehin sterben die Algorithmen aus, KIs sind effizienter, Menschen vielseitiger. Letztlich ist das doch der Grund, warum wir Maschinen bauen, nicht wahr? Damit sie uns die leidige Arbeit abnehmen.“

„Vielen Dank für dein Mitgefühl.“

„Nichts als die Wahrheit.“

„Ich weiß ... Ich brauch erst mal 'nen freien Kopf.“

Zu Hause, noch bevor sie in den Flur getreten war, zog Irene den Plastikmantel aus und warf ihn in den Müllschlucker neben der Tür. Kurz darauf erschien ihre Mutter und überschüttete sie mit Fragen zu ihrem bisherigen Tag. Anschließend durchstöberten sie die digitalen Datenbanken nach neuen Wandmotiven. Später am Abend kramte Irene einen alten Respirator hervor, den sie mit ihrer Mutter gemeinsam modifizierte und dekorierte.

Während sie in der Küche das Abendessen zubereiteten, leuchtete eine Benachrichtigung in Irenes Brillengläsern auf. Ein Anruf.

„Frau Ablett?“

„Ja?“

„Hier ist Khalid Cheng von der Datenagentur Cheng.“ Seine Stimme klang aufgereggt. „Wunderbar, dass ich Sie erreiche. Können Sie noch mal herkommen?“

\* \* \*

Dass sie die Kontrollkanzel des Datenverarbeitungskomplexes wiedersehen würde, hatte Irene eigentlich nicht vermutet. Jetzt aber lauschte sie dort den Ausführungen Chengs, der ihr mit flatteriger Gestik umriss, was den Netzingenieuren widerfahren war – und dabei so ekstatisch wirkte wie die

Umgeschulten in seinen Beschreibungen. Von signifikanten Leistungssteigerungen war die Rede, von sprudelnden Hirnaktivitäten, von neuralen Feuerwerken. Und von der Möglichkeit einer neuen Arbeitsstelle.

„Sie haben etwas an sich, worauf manche der Netzingenieure reagieren; sie empfinden Ihre Gegenwart ganz offenbar als angenehm.“ Chengs Hände rotierten, während er nach Worten suchte. „Dafür war nicht das Parfüm verantwortlich, das Sie trugen, wir haben es getestet. Ihr eigener, natürlicher Körpergeruch könnte es sein. Vielleicht versteckt sich darin irgendwo die Möglichkeit, den Umgeschulten ein angenehmeres Dasein zu ermöglichen. Wir haben schon früher bemerkt, dass ein angenehmer Duft dazu beiträgt, sie zu beruhigen, was natürlich verständlich ist – niemand mag die Absonderungen, die durch die städtischen Gassen wehen. Aber dies hier könnte womöglich der Durchbruch sein.“ Seine Hände verlangsamten sich, rollten aus wie ein Wagen, der langsam zum Stehen kommt. „Können Sie sich das vorstellen? Also ... wären Sie bereit, das zu tun?“

## „WIE VIEL MENSCH STECKT IN DIESEN ÜBERRESTEN AUS NERVENBAHNEN UND SYNAPSEN?“

„Ja, denke schon“, antwortete Irene nach kurzem Zögern – sonderlich schwer klang die Aufgabe jedenfalls nicht.

„Wunderbar! Sie können sofort beginnen. Ja, gehen Sie ruhig, drehen Sie Ihre Runde. So können wir gleich sehen, ob es funktioniert.“

Mit langsamem Schritt durchwanderte Irene die Halle. Durch die neoklassische Musik zwangte sich vielfaches elektrisches Summen. Der Anblick der stehenden Metallsärgen, dem sie bei ihrem Vorstellungstermin mit Gleichmut begegnet war, flößte ihr wider Erwarten etwas Unbehagen ein. In ihrem kalten, abweisenden Äußeren ließen sie jegliche Spur menschlichen Daseins vermissen; zu seltsam, zu bizarr erschien ihr das alles plötzlich. Wie sollten die Kreaturen da drin tatsächlich leben? Erinnerungen an Leute, die im Netz umhergegeistert waren, bis ihr weltlicher Leib zu verrotten begann, kamen ihr in den Sinn. Sie erinnerte sich an Predigten der Lehrer, an die abschreckenden Bilder der Lehrfilme, an die Geschichten von Freunden – *Netzleichen*, wie man sie nannte.

„Hat's geklappt?“, fragte Irene, nachdem sie in die Kanzel zurückgekehrt war. Cheng war indessen verschwunden, lediglich Yana überwachte noch die Anzeigen.

„Sie mögen dich wohl. Zumindest irgendein durchlöcherter Rest ihres Unterbewusstseins.“

„Sie reagieren also tatsächlich?“

„Klar. Hier, die Anzeigen.“

Irene zog die Augenbrauen hoch.

Yana lachte. „Siehst unzufrieden aus.“

„Find's nur sonderbar. Zwischen Toten umherwandeln, als wäre ich auf einem Friedhof.“

„Tot sind die nicht. Die haben nach wie vor Hirnaktivität.“

Irene starre für einen langen Augenblick auf die sich windenden Graphen der Kontrollanzeigen. „Wie viel Mensch steckt in diesen Überresten aus Nervenbahnen und Synapsen?“

„Ehrlich? Haben mehr Ähnlichkeit mit 'nem Schwamm als mit 'nem richtigen Menschen ... Nun, irgendwo mag in denen noch ein Teil ihrer Persönlichkeit stecken. Den zu finden ist jedoch – nun, sagen wir: spekulativ. Ihre Handlungen im Netz sind größtenteils instinkt- und triebgesteuert, da steckt kein großer Geist mehr dahinter.“ Yana grübelte. „Zumindest erleichtert es so die Arbeit“, schloss sie und zuckte mit den Schultern. „Solange das Gehirn noch irgend eine Aktivität aufweist, kann man sie als Netzingenieure einsetzen. Instinktiv basteln die dir ein Netz zusammen, das von keiner schlechten Qualität ist. Muss eben nur stabil sein. Womöglich werden die irgendwann Netzer und KIs überflüssig machen.“ Nachdenklich rührte sie in ihrer Kaffeetasse. „Willst du hinschmeißen?“

„Ehrlich gesagt ... Ich bin unschlüssig.“

„Kein Problem. Geh nach Hause, schlaf eine Nacht drüber. Und entweder stehst du morgen hier wieder vor der Tür oder – so wie ich ihn kenne – wird der Chef sich sofort auf die Suche nach einem Ersatz für dich machen.“

„Ich überleg's mir.“

„Wie gesagt, die Schwämme finden dich toll. Und sie sind nicht tot, klar?“

Ein verschmitztes Lächeln wand sich über Irenes Gesicht. „Klar.“

(psz@ct.de) **ct**

*Zweiter und letzter Teil im nächsten Heft*

## Jetzt gibts was auf die Ohren!

Wenn Ihnen das Lesen dieser Story Lust auf mehr gemacht hat, möchten wir Ihnen unsere Podcast-Reihe **ct SciFiCast** ans Herz legen: Unter [heise.de/-4491527](http://heise.de/-4491527) warten kostenlose Hörfassungen ausgewählter Geschichten aus dem c't-Story-Fundus auf Sie!



Unsere „pechschwarzen Technikmomente“ gibt es zum Herunterladen oder als direkte Audiostreams – professionell eingesprochen und ideal als Begleiter für Fahrten oder auf Laufstrecken, wenn Sie Smartphone und Kopfhörer dabei haben.

Hören und per RSS-Feed abonnieren können Sie die Storys unter anderem auch auf Player.FM, Spotify und iTunes:

- [www.heise.de/ct/rss/ctstories.rss](http://www.heise.de/ct/rss/ctstories.rss)
- [open.spotify.com/show/37UbzCwzzCiju8501HUwL](http://open.spotify.com/show/37UbzCwzzCiju8501HUwL)
- [de.player.fm/series/ct-scificast](http://de.player.fm/series/ct-scificast)
- [podcasts.apple.com/de/podcast/ct-scificast/id1480700673](http://podcasts.apple.com/de/podcast/ct-scificast/id1480700673)

Auf Wiederhören!



**NACH UNS DIE  
SYN-FLOOD**

**IX**  
MAGAZIN FÜR PROFESSIONELLE  
INFORMATIONSTECHNIK

## Fernstudium IT-Security

Aus- und Weiterbildung zur Fachkraft für IT-Sicherheit. Vorbereitung auf das **SSCP- und CISSP-Zertifikat**. Ein Beruf mit Zukunft. Kostengünstiges und praxisgerichtetes 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)

# Talk nerdy to me!

**ct** magazin für  
computer  
technik

**LC-POWER™**  
[www.lc-power.com](http://www.lc-power.com)

# M.2 NVMe

PHENOM SERIE - bis zu 1 TB  
PHENOM PRO SERIE - bis zu 2 TB



Langsames Booten war gestern! Machen Sie die NVMe-M.2-SSD aus unserer neuen Phenom-Serie mit einer Lesegeschwindigkeit von bis zu 1800 MB/s zu Ihrem blitzschnellen und zuverlässigen Begleiter.

Darf es noch etwas schneller sein? Die Phenom Pro-Serie für High-Performer begeistert mit einer atemberaubenden Lesegeschwindigkeit von bis zu 3400 MB/s und bringt Ihr Gaming-Erlebnis sowie Ihren Arbeitsalltag auf das nächste Level.

NEU

# So bleiben Ihre Daten im Netz sicher und privat

AKTION! c't-Raspion-Set 30 Euro günstiger: Entlarvt Datenspione im Haushalt!

## c't Daten schützen

So bleiben Ihre Daten im Netz sicher und privat

### Privatsphäre sichern

Social Media aufräumen • Spuren in Fotos verwischen  
Daten richtig anonymisieren



### Spione enttarnen

c't-Raspion einrichten  
Datenlecks im Haushalt identifizieren

### Verfolger abschütteln

Inkognito im Netz • Tracking aushebeln  
Google entkommen • Maulkorb für Windows

### Daten verschlüsseln

Sicher mailen mit PGP und S/MIME  
Dateien & System mit Bitlocker und VeraCrypt sichern

## Die 13 wichtigsten Privacy-Checklisten

Mehr Schutz für PC, Smartphone, Homeoffice & Social Media

### c't Daten schützen

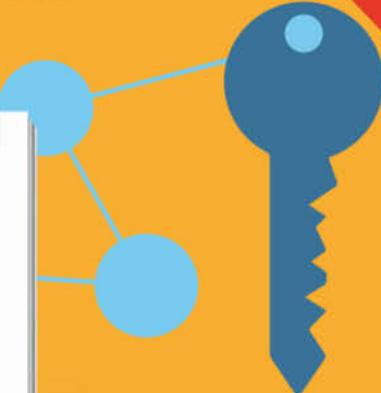
Halten Sie Schnüffler fern und Ihre privaten Daten sicher mit dem neuen c't-Sonderheft Daten schützen 2020! Privacy-Checklisten geben Hinweise für mehr Schutz in Ihrem Netz-Alltag und das nötige Rüstzeug um Tracking auszuhebeln, Google zu entkommen und Windows einen Maulkorb zu verpassen. Dazu: mit dem c't-Raspion-Projekt Spione enttarnen!

[shop.heise.de/ct-datenschutz20](http://shop.heise.de/ct-datenschutz20)

Einzelheft  
für nur

12,90 € >

Auch als  
Heft + PDF  
erhältlich mit  
22% Rabatt



11523



Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.



heise shop

[shop.heise.de/ct-datenschutz20](http://shop.heise.de/ct-datenschutz20)



ORACLE Feuerwehr [www.oraservices.de](http://www.oraservices.de) 

Embarcadero Delphi / C++, Festgefahren? Auf Fehlersuche? Troubleshooting sofort unter [solutions@provigor.de](mailto:solutions@provigor.de), Tel.: +49 1522-1 61 05 02 

DATENRETTUNG v. HDD, RAID, SSD – Erfolg >99% [www.datarecovery.eu](http://www.datarecovery.eu) – 24h-Tel.: 0800-073 88 36 

EDELSTAHL LED SCHILDER: [www.3D-buchstabe.com](http://www.3D-buchstabe.com)  
HAUSNUMMERN nobel 230V~: [www.3D-hausnummer.de](http://www.3D-hausnummer.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) 

**WWW.DRAW-A-MOUNTAIN.COM**

nginx-Webhosting: [timmehosting.de](http://timmehosting.de) 

Lust auf Java? [WWW.TQG.DE/KARRIERE](http://WWW.TQG.DE/KARRIERE) 

Ihr Internetauftritt: Video und Textanimation <https://deltodigit.jimdofree.com> 

[www.patchkabel.de](http://www.patchkabel.de) - LWL und Netzwerk Kabel 

WLL-Breitband Netz Ruhrgebiet – [schneeweiss.de](http://schneeweiss.de) 

Embarcadero Delphi: Migration und Modernisierung von Anwendungen und Komponenten. Zügiges Fresh up unter [solutions@provigor.de](mailto:solutions@provigor.de) Tel.: +49 1522 1 61 05 02 

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 

xxs-kurze Daten- & Netzkabel: [kurze-kabel.de](http://kurze-kabel.de) 

**Anzeigenschluss  
für die nächsten  
erreichbaren Ausgaben:**

**24/2020: 20.10.2020**

**25/2020: 03.11.2020**

**26/2020: 17.11.2020**

## 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,-)

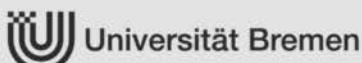
€ 66,- (132,-)

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.





Im Fachbereich 3 (Mathematik und Informatik) der Universität Bremen sind in der Arbeitsgruppe Rechnerarchitektur (vorbehaltlich der Stellenfreigabe) **befristet, voraussichtlich bis zum 31.05.2025, zwei Stellen:**

## Wissenschaftliche/r Mitarbeiter/in (w/m/d)

mit abgeschlossener überdurchschnittlicher Promotion im Rahmen des DFG-Projektes PolyVer  
Informatik – Entgeltgruppe 14 TV-L (100%)

zum nächstmöglichen Zeitpunkt zu besetzen. Eine Besetzung in Teilzeit ist möglich.

Die international renommierte Arbeitsgruppe Rechnerarchitektur der Universität Bremen entwickelt Entwurfswerkzeuge für den computergestützten Schaltkreis- und Systementwurf. Bei der Stelle geht es um die **Entwicklung innovativer Methoden zum Nachweis der Korrektheit beim Entwurf eingebetteter Systeme**. Die Stelle ist in einem von der Deutschen Forschungsgemeinschaft (DFG) für 5 Jahre genehmigten **Reinhart Koselleck-Projekt, "PolyVer: Polynomiale Verifikation elektronischer Schaltungen"**, angesiedelt.

Die Arbeitsgruppe kooperiert im Rahmen von Transferprojekten, die u.a. vom Bundesministerium für Bildung und Forschung (BMBF) gefördert werden, eng mit Partnern aus der Industrie. Im Graduiertenkolleg **System Design** (SyDe) der Universität Bremen werden neue Methoden und Verfahren entwickelt und im praktischen Umfeld auf ihre Verwertbarkeit hin analysiert. Eine enge Kooperation mit diesen Projekten ist erwünscht.

Verbunden sind u.a. mit der Stelle der Aufbau und die Leitung einer Arbeitsgruppe zum Thema „Theorie der formalen Verifikation mit beschränkten Ressourcen“ bzw. zum Thema „Implementierung von Algorithmen zur formalen Verifikation mit beschränkten Ressourcen“.

Weitere Informationen zum Anforderungsprofil und zu den Aufgaben finden Sie unter: [www.karriere.bremen.de](http://www.karriere.bremen.de)

Rückfragen an: Prof. Dr. Rolf Drechsler, Tel:0421-218-63932, E-Mail: [drechsler@uni-bremen.de](mailto:drechsler@uni-bremen.de).

Senden Sie Ihre aussagekräftigen und vollständigen Bewerbungsunterlagen (Lebenslauf, Diplom- oder Masterzeugnis etc.) **unter Angabe der Kennziffer A227/20 bis zum 12.11.2020** an:

Universität Bremen  
Fachbereich 3 Informatik/Mathematik  
Prof. Dr. Rolf Drechsler  
Bibliothekstraße 5  
28359 Bremen

oder elektronisch in einer Datei im PDF-Format an [drechsler@uni-bremen.de](mailto:drechsler@uni-bremen.de)



B u n d e s  
rechnungshof

Der Bundesrechnungshof ist eine oberste Bundesbehörde. Er prüft die gesamte Haushalts- und Wirtschaftsführung des Bundes und ist als Organ der Finanzkontrolle nur dem Gesetz unterworfen.

Wir suchen für das Prüfungsgebiet

„Informations- und Kommunikationstechnik und IT-Sicherheit“

im Bundesrechnungshof in Bonn

**Master/Diplom (Univers.)-Absolventinnen/-Absolventen (w/m/d) der (Wirtschafts-)Informatik, (Wirtschafts-)Mathematik, Physik, Wirtschaftswissenschaften, des (Wirtschafts-)Ingenieurwesens oder einer vergleichbaren Fachrichtung**

- Ausschreibung „BRH 2020-0062B“ -

Weitere Informationen finden Sie im Internet unter: [www.bundesrechnungshof.de](http://www.bundesrechnungshof.de)



 Heise Gruppe

# 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).





## Bringen Sie uns ins digitale Zeitalter!



IT-Systemhaus

Das IT-Systemhaus verantwortet als IT-Dienstleister der Bundesagentur für Arbeit (BA) den kompletten digitalen Auftritt einer der größten deutschen Bundesbehörden und stellt bundesweit über 100 Anwendungen und IT-Lösungen für die Arbeitsagenturen und Jobcenter sowie ein umfassendes Online-Portal bereit. Softwarelösungen im IT-Systemhaus werden mit innovativen Technologien und Architekturen auf Basis offener Standards entwickelt und in redundanten, hochverfügbaren Rechenzentren als Private Cloud betrieben. Das IT-Systemhaus betreibt mit über 170.000 vernetzten PC-Arbeitsplätzen und der dazugehörigen Infrastruktur eine der größten IT-Landschaften Deutschlands und entwickelt diese ständig weiter.

Wir suchen zum nächstmöglichen Zeitpunkt für unseren Standort in Nürnberg eine/n

### Vorsitzende/n der Geschäftsführung des IT-Systemhauses zugleich Bereichsleiter/in im Geschäftsbereich Informationstechnologie und Digitale Prozesse (ITDP) in der Zentrale (w/m/d)

Sie sind verantwortlich für ca. 1.600 Mitarbeiterinnen und Mitarbeiter in den Bereichen Systementwicklung, Produktion und Zentrales Projektmanagement. Gemeinsam mit den Führungskräften dieser Bereiche verantworten Sie den umfangreichen Dienstleistungsauftrag des IT-Systemhauses und nehmen dabei eine zentrale Rolle bei der agilen, digitalen Transformation der BA ein. Vergleichbar der Funktion eines „Chief Digital Officers“ sind Sie Garant für den Output des IT-Systemhauses als IT-Dienstleister für die BA, gestalten die IT-Strategie mit und setzen diese um. In Ihrer Funktion sind Sie der/m Generalbevollmächtigten der BA – zugleich Geschäftsführer/in Informationstechnologie und Digitale Prozesse (ITDP) – unterstellt und nehmen als Bereichsleiter/in in der Zentrale eine zentrale Brückefunktion zwischen IT- und Business-Seite im Headquarter der Zentrale wahr.

#### Ihre Aufgaben und Tätigkeiten:

- Führung und Steuerung des IT-Systemhauses (mit Personalverantwortung für ca. 1.600 Mitarbeiterinnen und Mitarbeiter und einem Budget von ca. 690 Millionen Euro jährlich)
- Verantwortung für die Zielerreichung und Vertretung des IT-Systemhauses nach innen und außen
- Verantwortung für die Umsetzung der Geschäftspolitik der BA im IT-Systemhaus
- Verantwortung für die Umsetzung der digitalen Agenda der BA und damit Garant für den Output des IT-Systemhauses als IT-Dienstleister der BA
- Mitgestaltung und Umsetzung der IT-Strategie
- Strategische Steuerung von externen Dienstleistern und Lieferanten des IT-Systemhauses
- Beratung der Vorstands- und obersten Führungsebene zu Fachthemen der IT der BA und des IT-Systemhauses

#### Sie überzeugen durch:

- Einen Hochschulabschluss oder vergleichbare Qualifikation (vorzugsweise Informatik, Wirtschaftsinformatik)
- Langjährige einschlägige Berufserfahrung in herausgehobenen Führungspositionen im IT-Umfeld
- Umfassende Erfahrung in den Bereichen Veränderungsmanagement und Transformation großer Organisationen
- Berufserfahrung in der Projektsteuerung
- Fundierte Kenntnisse und Erfahrung im Umfeld Betriebswirtschaft und Controlling
- Fundierte IT-Kenntnisse mit der Fähigkeit, das agile Zusammenwirken von IT- und Business-Seite auszustalten

#### Wir bieten Ihnen:

- Eine interessante, technikorientierte und zugleich fachlich vielseitige Tätigkeit
- Attraktive außertypische und leistungsorientierte Bezahlung im Rahmen des öffentlichen Dienstes
- Perspektivisch vielfältige Möglichkeiten der Personalentwicklung mit umfangreichen Qualifizierungsangeboten
- Flexible und familienfreundliche Arbeitszeitmodelle
- Standortgarantie (Metropolregion Nürnberg)

Bewerbungen von Frauen begrüßen wir besonders. Wir wollen den Anteil von Schwerbehinderten in der BA erhöhen und fordern daher schwerbehinderte Menschen auf, sich zu bewerben.

Bitte beachten Sie, dass Sie nach einer Einstellungszusage gemäß dem Sicherheitsüberprüfungsgesetz (SÜG) geprüft werden.

Für Rückfragen können Sie sich gerne telefonisch an Frau Silvia Rau (Leiterin Fachbereich Obere Führungskräfte, Tel.: +49 911 179-4847) wenden.

**Sind Sie interessiert?** Dann bewerben Sie sich bitte mit Ihren vollständigen Bewerbungsunterlagen (s. Rubrik „FAQ“) und unter Angabe des Referenzcodes 2020\_E\_003384 online unter [www.arbeitsagentur.de/ba-bewerbungsportal](http://www.arbeitsagentur.de/ba-bewerbungsportal). **Bewerbungsende:** 07.11.2020

Weitere Informationen erhalten Sie unter [www.ba-it-systemhaus.de/karriere](http://www.ba-it-systemhaus.de/karriere) oder allgemein zur BA unter [www.arbeitsagentur.de/karriere](http://www.arbeitsagentur.de/karriere).

Die Bundesagentur für Arbeit ist eine Arbeitgeberin, die Chancengleichheit und Vielfalt ihrer Mitarbeiterinnen und Mitarbeiter fördert. Hierbei unterstützen wir auch die Beschäftigung von Menschen mit Behinderung. Für diese vorbildliche Personalpolitik sind wir zum wiederholten Male ausgezeichnet worden.



# Inserenten\*

1&1 IONOS SE, Montabaur	33	<b>Stellenanzeigen</b>
1blu AG, Berlin	9	Bundesagentur für Arbeit, Nürnberg
AUDI AG, Ingolstadt	2	Bundesrechnungshof, Bonn
Conrad Electronic SE, Hirschau	35	Freie Hansestadt Bremen, Bremerhaven
dpunkt.verlag GmbH, Heidelberg	45	
DZ BANK AG, Frankfurt	31	
ESET Deutschland GmbH, Jena	85	
Fernschule Weber, Großenkneten	187	
Hetzner Online GmbH, Gunzenhausen	196	
Hiscox Europe Underwriting Limited, München	17	
Kentix GmbH, Idar-Oberstein	55	
Lautsprecher Teufel GmbH, Berlin	53	
O'Reilly, dpunkt.verlag GmbH, Heidelberg	77	
Platinion GmbH, Köln	195	
Silent Power Electronics GmbH, Willich	187	
Snom Technology AG, Berlin	49	
Thomas-Krenn.com, Freyung	7	
Vogel Communications Group GmbH & Co. KG, München	91	
Wiesemann & Theis GmbH, Wuppertal	39	

secIT by Heise	heise Events	37
IT-Job-Summit	heise Events, Jobware	51
storage2day	iX, dpunkt.verlag	71
PUR - Professional		
User Rating	heise Events, techconsult	87
heise devSec	heise security, heise developer, dpunkt.verlag	99
IT-Jobtag	heise jobs, Jobware	113
iX Workshops	iX, heise Events	141
Agile Softwareentw.		
im Unternehmen	Heise Knowledge	149
Vertriebsperformace 4.0 +		
Social Selling	iX, heise Events	151
data2day	iX, heise developer, dpunkt.verlag	192

Ein Teil dieser Ausgabe enthält Beilagen von REWE Digital, Köln, und Heise Medien GmbH & Co. KG, Hannover

\* Die hier abgedruckten Seitenzahlen sind nicht verbindlich.  
Redaktionelle Gründe können Änderungen erforderlich machen.



Die Konferenz für Big Data,  
Data Science und Machine Learning

Vorträge und Workshops zu den Themen:

- Methoden & Tools: Von den Rohdaten zur Analyse und Visualisierung
- Rollenverteilung: Data Scientist, Domänenexperte und Developer
- ML-Projekte: DevOps, DDD und Design Canvas
- ML-Modelle: NLP, Forecasts & ML as a Service

Jetzt  
Ticket  
sichern!

[www.data2day.de](http://www.data2day.de)

Silbersponsoren

@codecentric

**HMS**  
analytical software

OPITZ CONSULTING

Veranstalter

**h**

heise Developer

dpunkt.verlag

# 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:** „Fritzbox sicher und privat“:  
Dušan Živadinović ([dz@ct.de](mailto:dz@ct.de)), „Backup für die Ewigkeit“: 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)), Ingo T. Storm ([it@ct.de](mailto:it@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 ([apoi@ct.de](mailto:apoi@ct.de)), Arne Grävemeyer ([agr@ct.de](mailto:agr@ct.de)), André Kramer ([akr@ct.de](mailto:akr@ct.de)), Markus Montz ([mon@ct.de](mailto:mon@ct.de)), Peter Schmitz ([psz@ct.de](mailto:psz@ct.de)), Kim Sartorius ([kim@ct.de](mailto:kim@ct.de)), Dr. Hans-Peter Schüler ([hps@ct.de](mailto:hps@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))

**Redaktion:** Mirko Döll ([mid@ct.de](mailto:mid@ct.de)), Liane M. Dubowy ([lmd@ct.de](mailto:lmd@ct.de)), Ronald Eikenberg ([rei@ct.de](mailto:rei@ct.de)), Thorsten Leemhuis ([thl@ct.de](mailto:thl@ct.de)), Jan Mahn ([jam@ct.de](mailto:jam@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)), Merlin Schumacher ([mls@ct.de](mailto:mls@ct.de)), Jan Schüßler ([js@ct.de](mailto:js@ct.de)), Keywan Tonekaboni ([ktm@ct.de](mailto:ktm@ct.de)), Axel Vahldiek ([axv@ct.de](mailto:axv@ct.de))

### Ressort Hardware

**Leitende Redakteure:** Christof Windeck ([cw@ct.de](mailto:cw@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)), Tim Gerber ([tig@ct.de](mailto:tig@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 Müsigg ([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)), Ulrich Hilgefort ([uh@ct.de](mailto:uh@ct.de)), Nico Jurran ([nij@ct.de](mailto:nij@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 ([Ltg](mailto:Ltg), [uk@ct.de](mailto:uk@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))

**Redaktionsassistenten:** 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 Assistenten:** Ralf Schneider ([Ltg](mailto:Ltg), [rs@ct.de](mailto:rs@ct.de)), Hans-Jürgen Berndt ([hjb@ct.de](mailto:hjb@ct.de)), Denis Fröhlich ([df@ct.de](mailto:df@ct.de)), Christoph Hoppe ([cho@ct.de](mailto:cho@ct.de)), Stefan Labusga ([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)), 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:** Nicole Judith Hoehne ([Ltg](mailto:Ltg)), Martina Fredrich, Jürgen Gonnermann, Birgit Graff, Angela Hilberg, Jessica Nachtigall, Astrid Seifert, Dieter Wahner, Ulrike Weis

**Art Direction:** Nicole Judith Hoehne (Leitung & Weiterentwicklung)

**Junior Art Director:** Martina Bruns

**Fotografie:** Andreas Wodrich, Melissa Ramson

**Videoproduktion:** Johannes Börnsen

**Digitale Produktion:** Melanie Becker, Anna Hager, Pascal Wissner

### Illustrationen

Jan Bintakies, Hannover, Rudolf A. Blaha, Frankfurt am Main, Thorsten Hübner, Berlin, Albert Hulm, Berlin, Sven Huth, Schülp, Thomas Kuhlenbeck, Münster, Michael Luther, Berlin, Andreas Martini, Wettin, Henning Rathjen, Oberursel

**Editorial:** Hans-Jürgen „Mash“ Marhenke, Hannover, **Schlage Seite:** 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: 2BAE3C6F6DAFFB000

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 58E8 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: [sq4lecqyx4izcpk.onion](https://sq4lecqyx4izcpk.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, Dr. Alfons Schräder

**Mitglieder der Geschäftsleitung:** Beate Gerold, Jörg Mühle

**Verlagsleiter:** Dr. Alfons Schräder

**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. 37 vom 1. Januar 2020.

**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:**

VU Verlagsunion KG  
Meßberg 1  
20086 Hamburg  
Tel.: 040/3019 1800, Fax: 040/3019 145 1800  
E-Mail: [info@verlagsunion.de](mailto:info@verlagsunion.de)

### c't erscheint 14-täglich

Einzelpreis 5,20 €; Österreich 5,70 €; Schweiz 7.60 CHF; Dänemark 57,00 DKK;  
Belgien, Luxemburg 6,00 €; Niederlande 6,30 €; Italien, Spanien 6,50 €

**Abonnement-Preise:** Das Jahresabonnement kostet inkl. Versandkosten: Inland 122,85 €, Österreich 130,95 €, Europa 141,75 €, restl. Ausland 168,75 € (Schweiz 175,50 CHF); ermäßigtes Abonnement für Schüler, Studenten, Auszubildende (nur gegen Vorlage einer entsprechenden Bescheinigung): Inland 89,10 €, Österreich 95,85 €, Europa 108,00 €, restl. Ausland 135,00 € (Schweiz 140,40 CHF). c't-Plus-Abonnements (inkl. Zugriff auf das c't-Artikel-Archiv sowie die App für Android und iOS) kosten pro Jahr 18,90 € (Schweiz 22,95 CHF) Aufpreis. Ermäßigtes Abonnement für Mitglieder von AUGE, BvDW e.V., /ch/open, GI, GUUG, ISACA Germany Chapter e.V., JUG Switzerland, VBIO, VDE und VDI (gegen Mitgliedsausweis): Inland 93,15 €, Österreich 98,55 €, Europa 112,05 €, restl. Ausland 139,05 € (Schweiz 132,30 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 2020 by Heise Medien GmbH & Co. KG

ISSN 0724-8679 AWA ACTA



# Vorschau 23/2020

Ab 24. Oktober im Handel und auf ct.de



## Der c't-Sicherheitsreport

Viele Unternehmen, Behörden und Privatpersonen treffen zu wenig oder gar keine Schutzmaßnahmen gegen Angriffe aus dem Internet. Wir haben das Netz systematisch nach Lücken durchsucht und sind an Dutzenden Stellen auf ungeschützte Server und vertrauliche Daten gestoßen. Schuld sind häufig Konfigurationsfehler.



## Vom Drohnen-Foto zum 3D-Modell

Fotos von einem Gebäude, die man mit einer Drohne aus verschiedenen Perspektiven geschossen hat, kann die Software Metashape zu einem 3D-Modell zusammensetzen. Mit minimaler Nachbearbeitung lässt es sich auf einem 3D-Drucker ausdrucken.

# Vorschau c't-Retro 2020

Ab 20. Oktober im Handel und auf ct.de



## Das PC-Märchen

In der Retro-Ausgabe der c't 2020 gehen wir der legendären Erfolgsgeschichte des IBM PC und seines Entwicklerteams „The Dirty Dozen“ nach. Wir reisen zurück zu den ersten Windows-Versionen und zeigen, wie man Windows 3.1, 95 & Co. ausprobieren kann – und die Software, die es damals dafür gab. Außerdem: haufige Tipps, wie man seine Daten von alten Festplatten, Disketten und CDs rettet.

Als Abonnent finden Sie die Extra-Ausgabe ab dem 19. Oktober in Ihrem Briefkasten. Am Kiosk gibts c't Retro 2020 ab dem 20. Oktober für 6,90 Euro.

## Noch mehr Heise-Know-how



Mac & i 5/2020 jetzt im Handel und auf heise-shop.de



Make 5/2020 jetzt im Handel und auf heise-shop.de



Technology Review 11/2020 jetzt im Handel und auf heise-shop.de

# SIE DENKEN BEI PYTHON NICHT AN SCHLANGEN?

## BCG Platinion sucht IT Architects.

Bei BCG Platinion fragen wir uns nicht, wie die digitale Welt ist – sondern wie sie sein sollte. Bei uns arbeiten kleine, hochmotivierte Teams an der Umsetzung geschäftskritischer IT-Themen renommierter Industrie- und Dienstleistungsunternehmen. Dabei ist uns eine enge Zusammenarbeit mit dem Kunden genauso wichtig wie die persönlichen Aufstiegs- und Entwicklungschancen unserer Mitarbeiter. Sie haben Interesse an einer führenden IT-Beratung und wollen von den Chancen des globalen BCG-Netzwerks profitieren? Dann freuen wir uns auf Ihre Bewerbung.

Mehr Infos auf [karriere.bcgplatinion.de](http://karriere.bcgplatinion.de)





### z.B. Managed Server MX93

- ✓ Intel® Xeon® E5-1650 v2 Hexa-Core inkl. Hyper-Threading-Technologie
- ✓ 64 GB DDR3 ECC RAM
- ✓ 2 x 500 GB SATA 6 Gb/s SSD (Software RAID 1)
- ✓ 100 GB Backup Space
- ✓ Unbegrenzter Traffic
- ✓ Standort Deutschland
- ✓ Keine Mindestvertragslaufzeit
- ✓ Setupgebühr 103,24 €

monatlich **103,24 €**

### z.B. Managed Server MA120

- ✓ AMD EPYC 7401P 24-Core "Naples" (Zen) Simultaneous Multithreading
- ✓ 128 GB DDR4 ECC RAM
- ✓ 2 x 960 GB NVMe SSD (Software RAID 1)
- ✓ 100 GB Backup Space
- ✓ Unbegrenzter Traffic
- ✓ Standort Deutschland
- ✓ Keine Mindestvertragslaufzeit
- ✓ Setupgebühr 138,04 €

monatlich **138,04 €**