



31.7.2021 17



Schon getestet:  
AMD Ryzen 7  
5700G

So retten Sie Hardware vor dem Recyclinghof

# Raspi macht alte Geräte flott

Drucker, Scanner und HiFi-Anlagen vernetzen • SMBv1-Geräte sichern

IM  
TEST

- Transkription für Audio & Videos
- IKEA: Lautsprecher-Bilderrahmen
- RISC-V-Einplatinencomputer
- Hochsicherheits-Mini-PC
- Günstiges ARM-Notebook mit LTE



Personalisiert, manipulativ, intransparent

## Online-Wahlwerbung

c't entlarvt Versender von Phishing-Mails

Basiswissen Windows-Registry

Verschlüsseltes Linux per SSH entsperren

Quantencomputer: 6 Konzepte für den Durchbruch

Kryptogeld: Klimafreundlich durch Proof of Stake?

Café, Camper, Kanaren: Was Sie dürfen und was nicht

# Homeoffice im Grünen

Beratung: Mobilrouter, Datentarife, portable Monitore



€ 5,50

AT € 6,10 | LUX, BEL € 6,50

NL € 6,70 | IT, ES € 6,90

CHF 8.10 | DKK 60,00

## ELEGANZ TRIFFT LEISTUNG

### Das neue bluechip TRAVELline B15W47

Windows 10 Pro

Hochwertiges,  
dünnes und leichtes  
Aluminiumdesign

15,6" FullHD  
IPS Touch-  
Display

Sprachassistent-  
Unterstützung  
mit Lichtleiste

Scan für Video  
und mehr  
Informationen »



**BTO**  
BUILD TO  
ORDER  
KONFIGURIERN

**24**  
MONATE  
GARANTIE

intel.

iRIS<sup>®</sup>Xe

GRAPHICS

intel.

CORE<sup>™</sup>

i5

#### LEISTUNGSSTARKES PREMIUM-NOTEBOOK FÜR HOHE ANSPRÜCHE **bluechip TRAVELline B15W47**

- + Leistungsstarker Intel® Core™ i5-1135G7 Prozessor
- + Windows 10 Pro
- + 15.6" IPS Touch-Dispay im Narrow Bezel Design
- + 8 GB DDR4, 500 GB NVMe SSD
- + Intel® Wi-Fi 6 AX201 und Bluetooth v5.1
- + Beeindruckende Intel® Iris® Xe Grafik
- + Zwei Thunderbolt™ 4-Anschlüsse (USB 4.0, Typ-C)

- + HD-IR-Kamera mit Windows Hello-Unterstützung
- + 15 Millimeter dünnes Aluminium-Gehäuse
- + 73-Wh-Akku für bis zu 16 Stunden Akkulaufzeit
- + Sprachassistenten-Unterstützung mit Lichtleiste
- + hintergrundbeleuchtete Tastatur und Glas-  
Touchpad



## Security: Mit Linux wäre das nicht passiert

Da läuft was schief: Dutzende von Firmen werden via Dienstleister Kaseya mit Malware infiziert und ihre Daten verschlüsselt (S. 14). Zeitgleich gehen Kliniken nach Attacken vom Netz und die Kreisverwaltung Anhalt-Bitterfeld ruft den Notstand aus. Beide Ransomware-Attacken treffen auf ein Umfeld, das oft nicht einmal die elementarsten Sicherheitsregeln beachtet. In vielen Kliniken und Behörden ist ein chronisch unterfinanzierter und unterbesetzter "Fachbereich IT" vollauf damit beschäftigt, die überalterte Hard- und Software (S. 38) am Laufen zu halten.

Während sich Politiker, Dienstleister und Admins gegenseitig die Schuld in die Schuhe schieben, rufen Open-Source-Verfechter hämisch: Mit Linux wäre das nicht passiert! Doch in dem geschilderten IT-Umfeld brächte Linux kaum mehr Sicherheit. Wenn es an ausreichend geschultem und motiviertem Personal fehlt, gibt es niemanden, der die notwendigen Updates einspielt und sich zusätzlich noch um eine adäquate Sicherheitsarchitektur kümmert.

Was wirklich helfen würde, wäre, wenn Behörden, Kliniken, aber auch Unternehmen dem Thema IT-Sicherheit und Datenschutz endlich den erforderlichen Stellenwert einräumen könnten. Natürlich

kostet das Geld, doch unterm Strich dürfte sich diese Investition durchaus lohnen: reibungslose(re) Produktion, störungsfreie Verwaltung, mehr Sicherheit gegen Industriespionage und als Abfallprodukt ein deutlicher Gewinn an Datenschutz.

Wer die IT nach wie vor nur als Kostenfaktor sieht, läuft sehenden Auges in die nächste Katastrophe. Sei es durch noch ausgefeilte Angriffe oder aber durch neue Abhängigkeiten. Microsoft steht mit Windows 365 schon in den Startlöchern (S. 36). Der gemietete komplette PC-Arbeitsplatz in der Cloud, gehostet und gewartet vom amerikanischen Großkonzern, das könnte so manchen Sparfuchs in Unternehmen und Verwaltung in Versuchung führen. Die Folgen des Verlusts an Souveränität und Datenhoheit baden wir dann später aus.



Georg Schnurer

# TERRA MOBILE

# 1470 T

Außergewöhnlich.  
Flach.  
Leistungsstark



## Bringen Sie Ihr Unternehmen auf den neuesten Stand: Mit Windows 10 Pro-Geräten.

Windows 10 Pro unterstützt die weltweit größte Auswahl an Geräten für Unternehmen führender Hersteller und schafft eine Reihe moderner Geräte, die garantiert den höchsten Standards in Bezug auf Leistung, Sicherheit, Design und Erfahrung entsprechen. Dank eines unvergleichlichen

Geräte-Ökosystems können Unternehmen aus einer breiten Auswahl an Geräten wählen. Mit Windows 10 Pro als Grundlage für Ihren modernen Arbeitsplatz erhalten Sie außerdem umfassende Sicherheit, Tools der Unternehmensklasse und eine flexible Verwaltung.

## ERHÄLTLICH BEI IHREM TERRA FACHHÄNDLER

IBN Gesellschaft für Systemtechnik mbH, **14478** Potsdam, Tel. 0331/888400 • Capeletti & Perl GmbH, **20097** Hamburg, Tel. 040/23622 0 • Computer-Service-Buchholz GmbH, **21244** Buchholz i.d.N., Tel. 04181/137373 • Caligrafika, **26133** Oldenburg, Tel. 041/9250095 • T&S Computech GmbH, **30175** Hannover, Tel. 0511/884817 • B.I.T. Datentechnik GmbH, **31675** Bückeburg, Tel. 05722/95040 • Systemhaus Przykopanski, **31848** Bad Münder, Tel. 05042/933160 • MBörso-Computer GmbH, **33100** Paderborn, Tel. 05251/28818-0 • Microtec GmbH, **33649** Bielefeld, 0521/9455274 • bits+bytes Computer GmbH & Co. KG, **35745** Herborn, Tel. 02772/94990 • RODIAC EDV-Systemhaus GmbH, **42551** Velbert, Tel. 02051/989000 • ServeNet Computervertrieb, **42279** Wuppertal, Tel. 0202/266166 • Rose Computer GmbH, **46395** Bocholt, Tel. 02871/244400 • Kortenbrede Datentechnik GmbH, **48161** Münster, Tel. 02533/930802 • Großbecker & Nordt Bürotechnik-Handels-GmbH, **50859** Köln, Tel. 02234/40890 • Franken & Vogel GmbH, **55124** Mainz, Tel. 06131/14406-34 • SURE DataSystems, **57627** Hachenburg, Tel. 02662/95830 • J.S. EDV-Systemberatung GmbH, **63843** Niedernberg, 06028/97450 • Pauly Büromaschinen Vertriebs GmbH, **65555** Limburg, Tel. 06431/500466 • hecom TK + IT Lösungen, **67071** Ludwigshafen, Tel. 0621/6719070 • Lehmann Elektronik, **67346** Speyer, Tel. 06232/28746 • Krieger GmbH & Co KG, **68163** Mannheim, Tel. 0621/833160 • G+S Computer GmbH **68519** Viernheim, Tel. 06204/607921 • KAISYS.IT GmbH, **72793** Pfullingen, Tel. 07121/145330 • Danner IT-Systemhaus GmbH, **72760** Reutlingen, Tel. 07121/56780 • MP-Datentechnik GmbH, **73730** Esslingen, 0711/3609163 • Resin GmbH & Co.KG, **79589** Binzen, Tel. 07261/66660 • Office Komplett, **79664** Wehr Tel. 07762 / 708860 • Schwarz Computer Systeme GmbH, **92318** Neumarkt, Tel. 09181/48550 • K&L electronics GmbH, **95466** Weidenberg, 09278/98610-0.

WORTMANN AG empfiehlt Windows 10 Pro für Unternehmen.



Magnesium-  
gehäuse

35,6 cm (14")  
1920x1080 Non Glare Display

#### TERRA MOBILE 1470T

- Intel® Core™ i5-1135G7 Prozessor [8 MB Cache, bis zu 4.20 GHz]
- Windows 10 Pro
- 8 GB RAM
- 500 GB SSD
- Intel® UHD Grafik

Artikel-Nr.: 1220701

**1.069,-\***

Preis UVP inkl. gesetzl. MwSt.

Dockingstation  
optional

#### TERRA Dockingstation USB-C

Die USB-C Dockingstation ermöglicht den Anschluss von Peripheriegeräten wie z.B. bis zu 2x Bildschirme, Netzwerk, Lautsprecher, Maus und Tastatur. Das TERRA MOBILE 1470T wird beim Betrieb über diese Dockingstation automatisch geladen.

Artikel-Nr.: 1480076

**149,-\***

Preis UVP inkl. gesetzl. MwSt.



\* Änderungen und Irrtümer vorbehalten. Preise in € inklusive gesetzlicher Mehrwertsteuer.  
Es gelten die AGB der Wortmann AG, zu finden unter [www.wortmann.de](http://www.wortmann.de). Solange der Vorrat reicht.  
Keine Mitnahmегарантie.

Ultrabook, Celeron, Celeron Inside, Core Inside, Intel, das Intel-Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, das „Intel Inside“-Logo, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, vPro Inside, Xeon, Xeon Phi, Xeon Inside und Intel Optane sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

© Copyright by Heise Medien.

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

**WORTMANN AG**

IT. MADE IN GERMANY.

## Titelthemen

### Raspi macht alte Geräte flott

- 16 **Upcycling** mit dem Raspberry Pi
- 18 **Drucker und Scanner** ins Netz bringen
- 24 **NAS mit SMBv1** sicher überbrückt
- 30 **Spotify und AirPlay** Raspi als Client
- 32 **3D-Drucker** überwachen und steuern

### Homeoffice im Grünen

- 56 **Mobiles Arbeiten** Die neue Freiheit
- 62 **Vorteile** des „Vertrauensarbeitsorts“ überwiegen
- 64 **FAQ** Recht: Mobiles Arbeiten
- 66 **Router und Datentarife** fürs mobile Büro
- 70 **Monitore** Portabel, flach, leicht, Strom per USB-C
- 72 **Unterwegs videokonferieren** Tipps & Tricks

### Online-Wahlwerbung

- 118 **Microtargeting** Transparent ist nur der Wähler

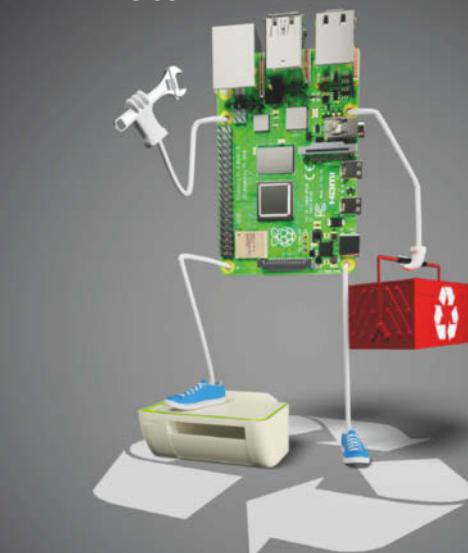
## Aktuell

- 14 **REvil-Trojaner** kam als Sicherheitsupdate
- 36 **Windows 365** Virtuelle Maschinen für Admins
- 37 **Windows** Windows 11, Windows 10 21H2
- 38 **Ransomware** Katastrophenfall ausgerufen
- 39 **Kommentar** Lernen aus Angriffen auf IT
- 40 **Massenüberwachung** durch Abhörsoftware
- 41 **Internet** WhatsApp, Staatstrojaner
- 42 **Videokonferenzen** erschweren Verhandlungen
- 43 **Bildung** Freie Schulsoftware, KI-Förderung
- 44 **Forschung** Displayfolie, Autonome Drohne
- 45 **Zahlungsverkehr** Digitaler Euro, Apple Pay
- 46 **Bit-Rauschen** Intels Fab-Pläne, 128-Kern-CPU
- 47 **Hardware** Workstations, Schlanker CPU-Kühler
- 48 **Server & Storage** DRAM-Mogelei, RZ-Abwärme
- 49 **Netze** Mehr Spektrum für Wi-Fi 6E, QTS 5.0
- 50 **Mobile Spielekonsole** Valve Steam Deck
- 51 **Open Source** Proxmox 7, Pop!\_OS 21.04
- 52 **Web-Tipps** Wissenschaft, Google, Politikeranalyse

## Test & Beratung

- 74 **Chromebook** Acer Spin 513
- 76 **Design-Mini-PC** Bleujour Kubb Gen 11
- 78 **USB-SSD mit Verschlüsselung** Datalocker DL4
- 79 **Audio-Editor** SpectraLayers 8
- 80 **Lüfterloser CPU-Kühler** Noctua NH-P1
- 80 **Luftqualitätssensor** IKEA Vindriktning
- 81 **Ergonomischer Stuhl** Embody Gaming Chair
- 81 **Wi-Fi-6-Router** Tenda TX3
- 82 **IKEA: Lautsprecher-Bilderrahmen**
- 84 **Bluetooth-Headset** Poly Voyager Focus 2 UC
- 86 **Sportuhr** Amazfit T-Rex Pro
- 87 **Lego-App** Bauvorschläge aus Steinchenfoto
- 87 **1-TByte-USB-Stick** Patriot Supersonic Rage Prime
- 92 **RISC-V-Einplatinencomputer**
- 96 **Schon getestet: AMD Ryzen 7 5700G**
- 98 **Günstiges ARM-Notebook mit LTE**
- 100 **OLED versus LCD** Zwei TVs von Sony
- 102 **Hochsicherheits-Mini-PC**
- 104 **High-End-Smartphone** Sony Xperia 1 III

### 16 Raspi macht alte Geräte flott



Der Raspi beschert älteren Geräten einen zweiten Frühling: Er kompensiert fehlende Drucker- und Scannertreiber, motzt 3D-Drucker und analoge Audioverstärker auf und hegt unsichere Protokolle ein.

- 106** **USB-Speicher** mit Schreibschutz  
**110** **Transkription für Audio & Videos**  
**166** **Action-Abenteuerspiel** Metroidvania: Ender Lilies  
**180** **Bücher** E-Auto erklärt, Medienratgeber

## Wissen

- 88** **c't entlarvt Versender von Phishing-Mails**  
**116** **Zahlen, Daten, Fakten** Bluetooth  
**124** **Quantencomputer: 6 Konzepte**  
**128** **Passwortmanager** Interaktion mit Webseiten  
**130** **EncroChat** Hack mit fragwürdigen Mitteln  
**134** **Kryptogeld: Klimafreundlicher**  
**138** **Netzwerk-Tuning** 10 GBit/s für Windows  
**144** **Basiswissen Windows-Registry**  
**168** **Überwachung** Geheimdienste dürfen mehr

## Praxis

- 150** **Chrome OS** auf alter Hardware installieren  
**154** **Hardware-Diagnose** per On-Screen-Display  
**158** **Microsoft Lists** im Team verwenden  
**162** **Verschlüsseltes Linux per SSH entsperren**

## Immer in c't

- 3** **Standpunkt** Mit Linux wäre das nicht passiert  
**8** **Leserforum**  
**13** **Schlagseite**  
**54** **Vorsicht, Kunde** Rücknahme verweigert  
**174** **Tipps & Tricks**  
**178** **FAQ** Multigigabit-Ethernet  
**182** **Story** Cybercrime für Anfänger  
**191** **Stellenmarkt**  
**192** **Inserentenverzeichnis**  
**193** **Impressum**  
**194** **Vorschau 18/2021**



*c't Hardcore kennzeichnet im Heft besonders anspruchsvolle Artikel.*

## 56 Homeoffice im Grünen



Homeoffice muss man nicht wörtlich nehmen:  
Das Büro kann fast überall sein – wenn man die Regeln kennt, die richtige Hardware mitnimmt und eine gute mobile Internetverbindung hat.

## 118 Online-Wahlwerbung



Der Bienenfreund sieht den Artenschutz-Slogan, der Autofahrer „freie Fahrt für freie Bürger“. Wahlwerbung lässt sich präzise auf die Zielgruppe zuschneiden. Was gut ist für die Parteien, ist schlecht für die Demokratie.

# Leserforum

## Schwierigkeiten mit TPM und BitLocker

Standpunkt Microsoft: Der falsche Feind, c't 16/2021, S. 3

Nach unserer Erfahrung [im PC-Service, Anm. d. Red.] behindert die Laufwerkverschlüsselung BitLocker mit TPM die Wiederherstellung von Systemlaufwerken erheblich. Wir mussten schon mehrfach die Festplatten ausbauen, um die Datensicherung nach Löschen aller Partitionen einlesen zu können. Welcher Kunde hat schon den Wiederherstellungsschlüssel für BitLocker notiert und gesichert, um dieses Problem zu lösen?

Bernhard Murra 



Chip des Anstoßes für viele Leser der c't 16/2021: Microsoft verlangt für Windows 11 ein Trusted Platform Module (TPM) wie den abgebildeten Chip von Infineon.

## Ziel der TPM-Pflicht

FAQ: TPM 2.0, c't 16/2021, S. 180

Irgendwie kann ich mich nicht des Eindrucks erwehren, dass das die Vorstufe eines geschlossenen Systems ohne vollständige eigene Kontrolle (heute schon schwierig, aber noch halbwegs gegeben) wie bei Android oder iOS auf dem iPhone darstellt.

Ein wirksamer Kopierschutz von Apps und Abkassieren für Inhalte dürfte ohne TPM kaum machbar sein. Wenn ich mich beim technischen Konzept nicht irre, sollte es mit TPM kein großer Schritt dahin sein. Das wäre dann auch ein Grund für eine neue OS-Version, denn man muss dafür den goldenen Käfig über alle Nutzer stülpen, sonst ergibt es keinen Sinn.

Dynamic 

## Interessant für Kriminelle und Geheimdienste

TPM ist zunächst mal ein einheitliches Verschlüsselungsmodul für – wenn es nach Microsoft geht – alle PCs, die Windows in Zukunft als Betriebssystem nutzen. Das macht TPM interessant für Kriminelle und Geheimdienste. Denn wenn man diese Tür knackt, dann hat man erleichterten Zugang zu allen PCs. Einen Bug in einem Chip kann man nicht mal eben mit einem Patch beheben. Wenn man vielleicht schon einen Fuß beim Chip-Hersteller in der Tür hat, wird es noch einfacher. Wäre

nicht das erste Mal, dass Geheimdienste „geimpfte“ Verschlüsselungstechnik an potenzielle Gegner, aber auch an Verbündete verkaufen.

J.Reuther 

## Nicht grundsätzlich falsch

Neue Schnüffelwerkzeuge für Geheimdienste, c't 16/2021, S. 12

Grundsätzlich müssen auch Ermittlungsmethoden zeitgemäß sein – sie dürfen aber nicht ausufern oder eben missbraucht werden (obwohl es dafür wahrscheinlich schon zu spät ist). Ich sehe ein Problem darin, wenn der Verfassungsschutz nicht das Grundgesetz schützt und zum Beispiel nicht gegen diesen Missbrauch vorgeht. Das heißt nicht, dass es grundsätzlich falsch ist, solche Methoden zur Verfügung zu haben. Aber es ist falsch, sie für politische oder persönliche Motive zu nutzen.

botornot 

## PC-Infos statt Windows+Pause

Windows 11: Preise, Termine, Systemvoraussetzungen, Updates und Upgrades, c't 16/2021, S. 20

Sie schreiben, man soll Windows+Pause drücken, um herauszufinden, was man für

einen Prozessor hat. Leider ist die Pause-Taste gerade bei Notebooks immer häufiger gut versteckt (Fn-Tastenkombination) oder überhaupt nicht vorhanden.

Besser: Das Startmenü öffnen, „PC-Infos“ eintippen und in der Ergebnisliste das Symbol mit „i“ im Kreis, gefolgt von „PC-Infos“, auswählen. Wenn man über das Startmenü den Befehl „dxdiag“ ausführt, bekommt man noch ein paar Infos mehr, unter anderem zum Mainboard und zur Grafikkarte.

notting 

## Abgreifen von personenbezogenen Daten

Der digitale EU-Impfnachweis startet mit Einschränkungen, c't 16/2021, S. 38

Im QR-Code ist der Name, der Geburtstag und der Impfstatus vermerkt. Ich befürchte, dass es demnächst nachgebaute Check-Apps geben könnte, die die angezeigten QR-Codes fotografieren, um im Nachhinein doch recht wichtige persönliche Daten abzugreifen.

Diamantiker 

## USB-Odyssee

USB-C: Das leistet die praktische Schnittstelle, c't 16/2021, S. 90

Das deckt sich leider mit meinen Erfahrungen im täglichen IT-Support. Man

## Wir freuen uns über Post

 redaktion@ct.de

 c't Forum

 c't Magazin

 @ctmagazin

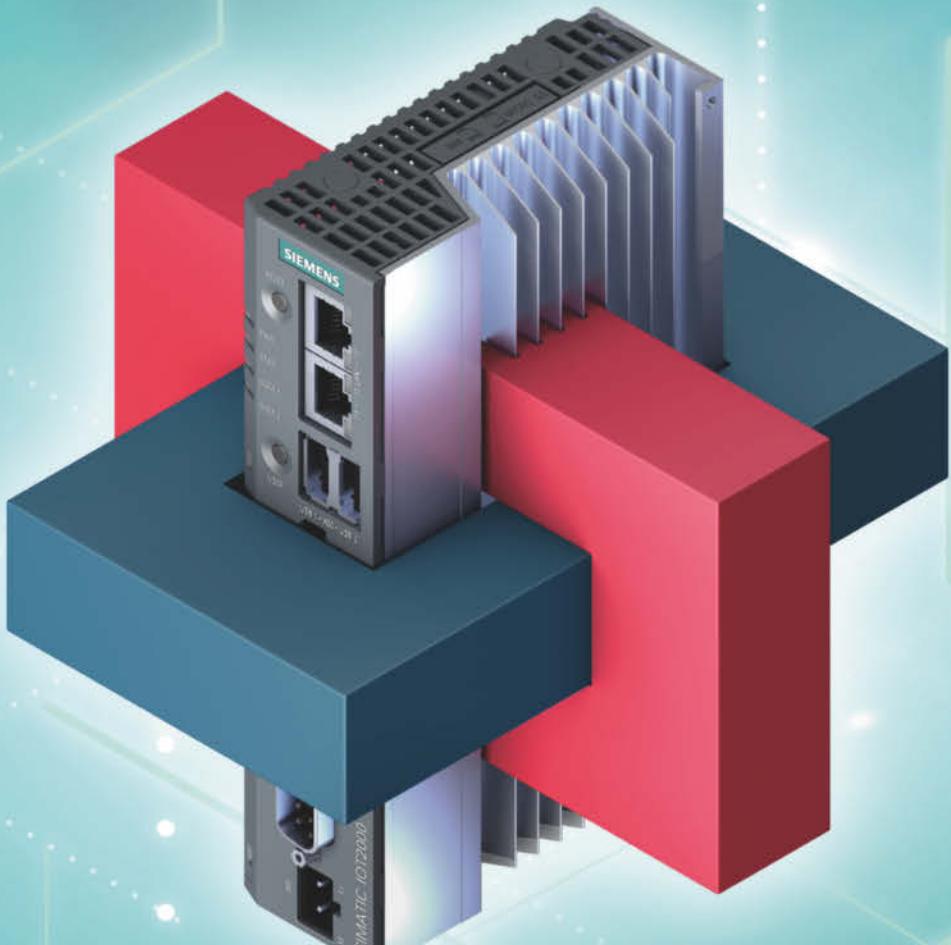
Ausgewählte Zuschriften drucken wir ab. Bei Bedarf kürzen wir sinnwährend.

Antworten sind kursiv gesetzt.

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

**SIEMENS**

Ingenuity for life



- 
- 
- 

## SIMATIC IOT2050 – Ihr Link zu digitalen Dimensionen

Entdecken Sie das smarte IoT-Gate-  
way für IT- und Cloud-Anbindungen.

[siemens.de/simatic-iot2050](http://siemens.de/simatic-iot2050)

sehnt sich zu den Zeiten von USB 2.0 und Firewire 400 zurück. Da war einfach klar: USB für einfache Geräte und Firewire für strombedürftige Peripherie. Die Erfindung des Y-Kabels war vielleicht damals schon der Anfang der USB-Odyssee.

Als USB-C vorgestellt wurde, sollte der Traum vom Dock im Display mit nur einem Kabel wahr werden. Apple hatte etwas Ähnliches mit dem Thunderbolt Display vorgemacht. Jetzt wird alles gut – dachte ich. Dann kam das erste MacBook mit USB-C und der notwendige Adapter war schon mal nicht lieferbar. Beim Einstecken des Kabels rastete dies nicht richtig ein.

Bei einem Dell-Notebook wechselte ich von der bewährten mechanischen Dockingstation auf das Thunderbolt-Dock. Das Notebook dazu hatte nur USB-C. Es gab also jedes Mal beim Start einen Hinweis dazu. Den Hinweis konnte man anfänglich nicht abschalten. Dies wurde später per BIOS-Update behoben. Von der mechanischen Stabilität des alten Docks blieb das Kabel weit entfernt. Sobald das Notebook nur leicht bewegt wurde, gingen alle Verbindungen zu den angeschlossenen Geräten verloren.

Ein Lenovo Dock musste mehrfach an das dazugehörige Lenovo Yoga an- und abgestöpselt werden, bis endlich die externen Bildschirme funktionierten. Nach dem Aufwecken des Notebooks ging immer nur der per HDMI angeschlossene Bildschirm an. Der DisplayPort-Bildschirm bleibt ohne Bild.

An USB-C begeistert mich bisher nur der kompakte und meistens verdrehsichere Stecker und die Verfügbarkeit von günstigen USB-C-auf-A-Adaptoren. Alles andere ist leider Murks.

Michael Bartz 

## DNS nicht vom ISP nutzen

*Privatsphärenschutz: DNS-Verschlüsselung im Feldversuch bei der Telekom, c't 16/2021, S. 128*

Es ist ja läblich, dass datenschutzfreundliche Techniken auch langsam bei der Telekom ankommen. Zurück zum neuen Telekom-DNS werde ich trotzdem nicht wechseln. Mir ist nicht nur ein verschlüsselter DNS wichtig, sondern auch ein zensurfreier. Diese Chance hat die Telekom als Mitglied der CUII (cuii.info) definitiv verspielt. Außerdem halte ich es für grundsätzlich bedenklich, den DNS des

## Fragen zu Artikeln

 **Mail-Adresse des Redakteurs am Ende des Artikels**

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

eigenen ISP zu nutzen. Für ihn ist es ein Leichtes, meinen Surfverlauf mit meinen Vertragsdaten zu verknüpfen. Auch wenn natürlich versprochen wird, dies nicht zu tun.

René S. 

## Rasenmähen per Satellit

*Zentimetergenaue Positionsbestimmung mit Satelliten, c't 16/2021, S. 132*

Es gibt ein Open-Source-Projekt, bei dem der ublox F9P zusammen mit einem Board von ArduSimple zum Einsatz kommt. Unter dem Begriff ArduMower wird in einem Wiki erklärt, wie man sich seinen eigenen Rasenmäher zusammenbauen kann, der dann mithilfe eines RTK-Systems den Rasen ohne Begrenzungsdraht zentimetergenau abfährt und mäht. Ein tolles Projekt mit einer klasse Community!

AF 

**ArduMower: ct.de/yd6v**

## Rolle des Arbeitgebers

*Die private Arbeitsumgebung günstig aufrüsten, c't 15/2021, S. 60*

Das Homeoffice ist unter den Pandemiebedingungen keine wirklich private Umgebung, sondern faktisch ein ausgelagerter Arbeitsplatz und dem Sinne nach auch eine ausgelagerte Arbeitsstätte. Ihre Artikelserie suggeriert und verfestigt die These, dass die Ausstattung und Ausgestaltung im ersten Ansatz beziehungsweise grundsätzlich Privatsache ist und mit privaten Ressourcen zu planen, zu finanzieren und umzusetzen ist. Die eigentlich für Arbeitsstätten zutreffenden Unfallverhütungs- und Gesundheitsschutzzvorschriften (DGUV) wurden

nicht angesprochen, obwohl in diesen hilfreiche und fundierte Hinweise zur Planung einer Arbeitsstätte und somit auch zur Planung des Homeoffice enthalten sind.

Durch Ihr Suggerieren, dass die Einrichtung des Homeoffice mit Privatressourcen zu leisten ist, zementieren Sie die Nichtbeteiligung der Arbeitgeber an der Gestaltung derjenigen Arbeitsplätze, an denen die Arbeit für Ihre Betriebe erbracht wird. Das ist meines Erachtens ungerecht.

Lutz Lyssewski 

## Ergänzungen & Berichtigungen

### Link veraltet

*Apps, Online-Kurse und Videos für das Rückentraining, c't 16/2021, S. 114*

Der Link zur Zentralen Prüfstelle Prävention der Barmer war mit Veröffentlichung des Artikels schon veraltet. Korrekt ist nun: <https://portal.zentrale-pruefstelle-praevention.de/portfolio/barmer/suche>

### Fehlender Kasten

*Windows 11: Preise, Termine, Systemvoraussetzungen, Updates und Upgrades, c't 16/2021, S. 20*

Im gedruckten Artikel ist uns ein Fehler unterlaufen – es fehlte der Kasten „Und was ist mit Windows 10?“. Sie können ihn abrufen unter [ct.de/ytb4](http://ct.de/ytb4).

### Verlustleistung

*USB-C-Kabel ab drei Metern Länge, c't 16/2021, S. 102*

Anders als im Kasten „USB Power Delivery“ beschrieben funktionieren längere Kabel besser bei höheren Spannungen, weil der Strom bei gleichbleibender Leistung sinkt. Bleibt die Stromstärke gleich, bleibt auch der Verlust unabhängig der Spannung gleich.

### Infrarotquelle benötigt

*Nachtsicht im Brillenglas, c't 15/2021, S. 50*

In der Meldung fehlt eine wichtige Komponente: Die geschilderte Nachsichtfunktion einer nanostrukturierten Beschichtung auf dem Brillenglas ergibt sich erst, wenn ein zusätzlicher Nahinfrarot-Laser die Metaoberfläche anregt.



# Shift happens.

Jetzt ist Zeit für neue Ideen.



[www.cronon.net](http://www.cronon.net)

Ihre IT kann mehr, als Sie denken

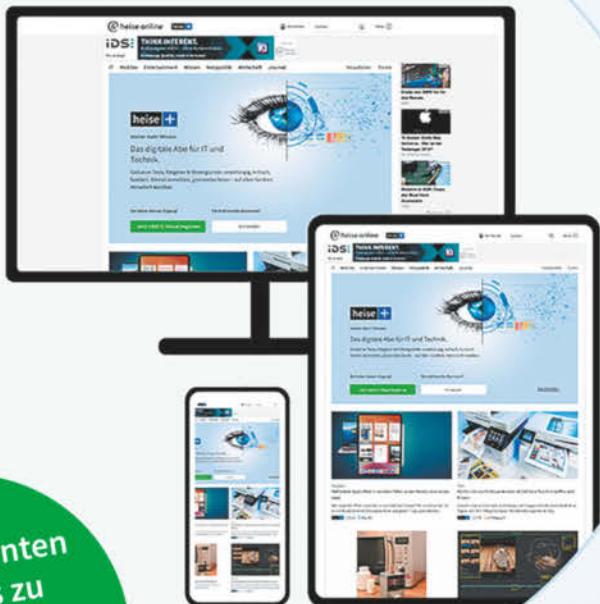
- mit flexiblen Cloud Services und einer spürbaren Entlastung für Ihre IT-Teams
- mit betriebsfertigen Container-Plattformen und echtem Managed Kubernetes
- mit moderner Enterprise Software für intelligentes Datenmanagement

Machen Sie mehr aus Ihrer IT. Machen Sie es jetzt: [shift@cronon.net](mailto:shift@cronon.net)

© Copyright by Heise Medien.

 **Cronon**

c't-Abo-  
nenten  
lesen bis zu  
**75%**  
günstiger



## Das digitale Abo für IT und Technik.

**Exklusives Angebot für c't-Abo-  
nenten:**  
Sonderrabatt für Magazinabonnenten

- ✓ Zugriff auf alle Artikel von heise+
- ✓ Alle Heise-Magazine online lesen: c't, ix, Technology Review, Mac & i, Make und c't Fotografie
- ✓ Jeden Freitag exklusiver Newsletter der Chefredaktion
- ✓ 1. Monat gratis lesen – danach jederzeit kündbar

Sie möchten dieses Exklusiv-Angebot nutzen? Jetzt bestellen unter:

[heise.de/plus-testen](http://heise.de/plus-testen)

✉ [leserservice@heise.de](mailto:leserservice@heise.de) ☎ 0541 80009 120

Ein Angebot von: Heise Medien GmbH & Co. KG • Karl-Wiechert-Allee 10 • 30625 Hannover



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

# 1000 auf einen Streich

## REvil-Verschlüsselungs-Trojaner kam als Sicherheitsupdate getarnt

**Die jüngste Ransomware-Attacke der Hackergruppe REvil führt die Entwicklung böswilliger Software konsequent weiter. Ab jetzt muss jeder davon ausgehen, dass sein Rechner in absehbarer Zeit betroffen sein wird, denn sogenannte Lieferkettenangriffe ziehen immer gleich auf Tausende Rechner auf einmal.**

Von Ingo T. Storm

Anfang Juli gelang es der Hackergruppe REvil, gut 50 Server zu infiltrieren, die Software und Updates an Tausende von Firmenrechnern verteilen – daher der Name Lieferkettenangriff oder Supply-Chain-Attack. Die Hacker platzieren ihre Schadsoftware dabei möglichst weit vorne in der Software-Lieferkette in einem vermeintlichen Update und können sich darauf verlassen, dass dieses an etliche Client-Rechner weitergeleitet wird, denn die wollen ja unbedingt regelmäßige Updates bekommen. Der PC, also das Ende der Lieferkette, ist einem solchen Angriff ziemlich hilflos ausgeliefert. Schließlich muss er seinen Update-Lieferanten vertrauen, denn niemand kann jedes einzelne Update auf Manipulationen untersuchen. VirensScanner helfen meistens auch nicht – wer Updates bringt, genießt Vertrauen und hat daher oft genügend Rechte, um den Virenschutz lahmzulegen. Eine detaillierte Analyse des genauen Ablaufs des Angriffs finden Sie auf heise online (siehe ct.de/yger).

Egal, ob Ihr PC oder Server nun in einer Behörde oder einem Unternehmen steht oder zu Hause nur privaten Zwecken dient: Sie müssen ganz anders als bisher über die

Sicherheit Ihrer Daten nachdenken, denn solche Angriffe werden auch in Zukunft nicht zu verhindern sein. Wer seine Daten nicht so sichert, dass sie die meiste Zeit nicht erreich- und damit auch nicht zerstörbar sind, muss früher oder später mit dem Totalverlust rechnen. Wer zwar brav sichert, aber das Zurückspielen nie durchexerziert, wird im Ernstfall sehr viel Zeit verlieren. Das ist privat nur ärgerlich. Eine Firma, die zu lange braucht, um eine befallene Infrastruktur wieder herzustellen, kann daran aber auch pleitegehen.

Ein Ausflug in den Ablauf dieses Angriffs hilft zu verstehen, warum er die Computerwelt nachhaltig durcheinanderbringt. Die Hackergruppe REvil, von der vermutet wird, dass sie aus Russland heraus operiert, nutzte mehrere Sicherheitslücken aus, um Server zu infiltrieren, auf denen die Software Kaseya VSA lief. Einige dieser Lücken waren taufrisch und es gab noch keinen Sicherheitspatch dafür – die Security-Branche nennt das „Zero-Day-Lücke“. Mindestens eine davon war der Firma Kaseya seit April bekannt (siehe ct.de/yger).

### Bären-Dienstleister

Durch diese Lücken gelang es REvil jedenfalls, zwischen 50 und 60 Kaseya-VSA-Server zu kapern. Jeder dieser Server gehört einem „Managed Service Provider“ oder MSP. Das sind IT-Dienstleister, die die Systeme kleinerer und mittlerer Unternehmen warten: Updates einspielen, Benutzer verwalten et cetera. REvil versteckte nun einen Erpressungstrojaner in den Updates, die Kaseya VSA pflichtgemäß an die Kunden-Server und -PCs auslieferte.

Dieses „Sicherheitsupdate“ erledigte zwei Jobs: Es legte den in Windows eingebauten VirensScanner lahm und es verschlüsselte alle erreichbaren Daten. Da das Update von einem scheinbar vertrauenswürdigen Server kam, konnte es besonders viele Daten erreichen und verschlüsseln – viel mehr, als der PC-Nutzer normalerweise sieht. Zu guter Letzt legte die Ransomware die Lösegeldforderung als Klartextdatei auf die Festplatte.

Wohl in der Hoffnung, nicht über 1000 Mal ein fünfstelliges Lösegeld kasieren und dafür Entschlüsselungsinformationen herausgeben zu müssen, forderte REvil über eine eigene Seite im weitgehend anonymen Tor-Netzwerk 70 Millionen US-Dollar für einen Generalschlüssel, der die Daten auf allen betroffenen Rechnern wiederherstellen sollte.

Die Firma Kaseya hatte vielleicht in der Vergangenheit gepatzt und ein Sicherheitsloch nur unzureichend gestopft. Doch nun reagierte sie im Rahmen der Möglichkeiten vorbildlich. Nach rund zwei Wochen waren die meisten MSP, die einen eigenen Kaseya-VSA-Server zur Pflege der Systeme ihrer Kunden einset-

The screenshot shows a ransomware message with the following text:

Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - csruj-Decryptor

Follow the instructions below. But remember that you do not have much time

csruj-Decryptor price

You have 4 days, 00:50:29

- \* If you do not pay on time, the price will be doubled
- \* Time ends on Jul 10, 06:31:27

Current price 203.46792839 XMR = 44,999 USD

After time ends 406.93585678 XMR = 89,998 USD

Monero address: 85.JqgbQT5GLheCvpbQmfXAspl/aZ2WDnA

\* XMR will be recalculated in 1 hour with an actual rate.

INSTRUCTIONS CHAT SUPPORT ABOUT US

zen, wieder arbeitsfähig. Die von REvil letztlich betroffenen Firmen, also die Kunden der Kaseya-Kunden, mussten dagegen alleine zusehen, wie sie ihre vielen tausend Rechner gesäubert und wieder in Gang bekommen. Dass die MSP dabei eine große Hilfe waren, darf bezweifelt werden, denn sie hatten ja mit dem Säubern und Absichern der eigenen Server schon genug zu tun.

REvil hat die Lieferkettenattacke nicht erfunden, aber verfeinert. Die Gruppe geht dabei extrem professionell vor, bis hin zur Support-Webseite, über die die Opfer Hilfe beim Entschlüsseln ihrer Daten erhalten. REvil vermietet ihre Schadsoftware sogar: Wer ein Netz geknackt hat, bekommt auf Wunsch den Trojaner zur Verfügung gestellt. REvil übernimmt auch das Inkasso und behält eine prozentuale Beteiligung ein. Außerdem erhöht REvil den Druck auf die Opfer, indem die Gruppe Daten nicht nur verschlüsselt, sondern damit droht, sie zu veröffentlichen. In den letzten Monaten konnte REvil so zweistellige Millionenbeträge einsammeln.

Die aktuelle Attacke rief die US-Regierung auf den Plan. US-Präsident Biden forderte Russland nicht nur öffentlich dazu auf, strenger gegen Hacker vorzugehen, die aus Russland heraus operieren. Diesmal griff Biden sogar zum Telefon und drohte dem russischen Präsidenten Putin mit weiteren Sanktionen.

Es wird gemunkelt, dass die russische Regierung daraufhin REvil auf die Finger geklopft hat. Vielleicht hat die Gruppe auch nur kalte Füße bekommen oder macht erst mal Pause, um die Millionen aus den vergangenen Fischzügen auch ausgeben zu können. Jedenfalls ist REvil wenige Tage nach dem Präsidententelefonat von der Bildfläche verschwunden. Das mag manchen beruhigen. Sehr ärgerlich ist es jedoch für einige Opfer, die bereits Lösegeld bezahlt haben, mit dem gelieferten Schlüssel aber nur einen Teil der Daten wiederherstellen konnten. Und nun ist der Support nicht mehr erreichbar, der einem beim Entschlüsseln helfen könnte ... Ebenso misslich ist die Lage für diejenigen, die gern bezahlen würden, um ihre Netze wieder hochfahren zu können.

Was bleibt, ist eine ziemlich apokalyptische Vision. Kaseya VSA ist nur eines von vielen Werkzeugen, mit denen Managed Service Provider sich um die Systeme ihrer Kunden kümmern. Und obwohl nur ein kleiner Anteil der Kaseya-VSA-Server ge-

hackt wurde, waren über 1000 Kunden der MSP und damit geschätzt weit mehr als 10.000 Rechner betroffen.

Privatanwender kamen bei diesem Angriff ungeschoren davon, denn sie sind weder an MSP-Systeme angeschlossen noch attraktive Ziele für die Erpresserbanden. Ein Einbruch in Microsofts, Googles oder Apples Update-Server wäre für Otto Normaluser die maximale Bedrohung, bleibt aber unwahrscheinlich, denn es gibt weniger aufwendige Wege in die Netze interessanter Opfer. Zur Software-Lieferkette gehören zum Beispiel auch Grafikkarten- und Druckerhersteller sowie unzählige unabhängige Softwareanbieter. Selbst auf einem wenig genutzten Windows-PC ist eine zweistellige Anzahl von Programmen installiert, für die Updates nicht direkt von Microsoft kommen. Dazu gehören auch in Firmen verbreitete Werkzeuge wie PDF-Reader und -Editoren, Zeichensoftware und Bildbearbeitung. Und so könnten Millionen privat genutzte PCs zum Kollateralschaden werden, wenn sich die nächsten Erpresser ein Allerweltswerkzeug als Einstiegsloke in die Netze ihrer Opfer aussuchen.

PC-Besitzer stecken also in einer Zwickmühle. Wenn sie mit Updates trödeln, könnte ihr Rechner über eine Schwachstelle wie die jüngst aufgetretene PrintNightmare-Lücke verseucht werden. Installieren sie zügig alle Updates, droht eine Lieferkettenattacke. Wir halten Letzteres derzeit für das weit weniger wahrscheinliche Übel. Aber wie gesagt: Sichern Sie Ihre Daten so, dass kein Trojaner sie erreichen kann. Halten Sie alle Informationen parat, die Sie für eine Neuinstallation brauchen. Erstellen Sie zusätzlich regelmäßig ein Systemabbild. Falls es sich um einen Windows-PC handelt, zum Beispiel mit unserem Werkzeug c't-WIMage.

## Hoffnung

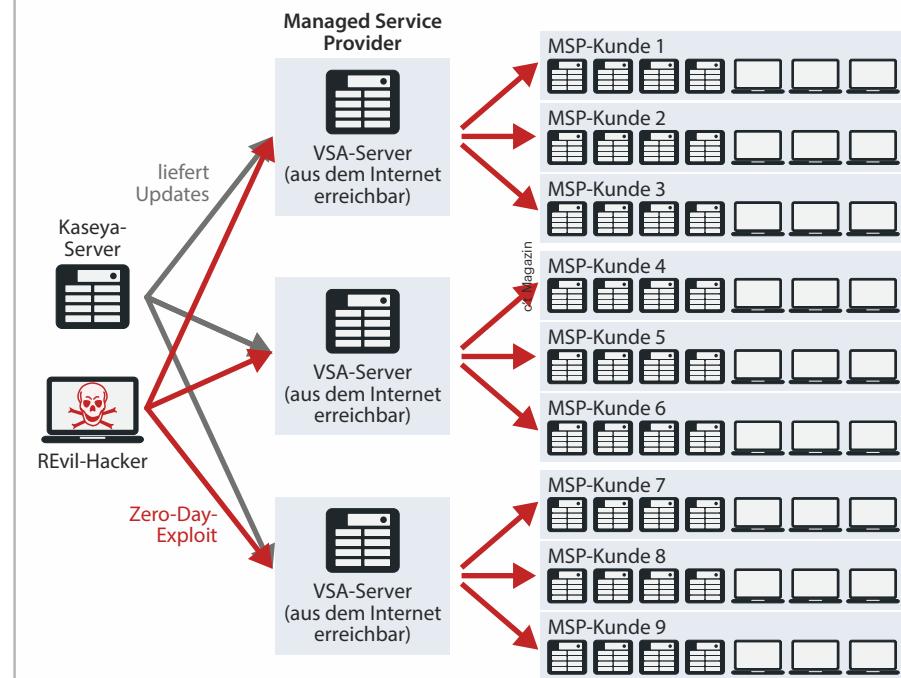
Kurz vor Druckschluss teilte Kaseya mit, von einer ungenannten Quelle einen Generalschlüssel erhalten zu haben. Die Betroffenen könnten also mit einem blauen Auge davonkommen. Aber 19 Tage haben sie auf jeden Fall schon verloren.

(it@ct.de) ct

**Details zu Kaseya, c't-WIMage: [ct.de/yger](http://ct.de/yger)**

## Lieferkettenangriff: 60 Hacks, 1000 Opfer

Managed Service Provider (MSP) sind Dienstleister, die die Netzwerke kleiner und mittlerer Firmen administrieren. Viele von ihnen nutzen dazu eigene Server mit der Software Kaseya VSA. Da Kaseya die VSA-Server mit Updates versorgt, sind sie aus dem Internet erreichbar. Auf diesem Wege konnten die REvil-Hacker knapp 60 Server übernehmen, die dann einen Erpressungstrojaner als Sicherheitsupdate getarnt an rund 1000 Kunden weitergaben.



# Upcycling mit dem Raspi

So lässt der Bastelcomputer alte Technik glänzen



Raspi macht alte Geräte flott .....	Seite 16
Drucker und Scanner ins Netz bringen .....	Seite 18
Sichere Brücke für alte SMBv1-Geräte .....	Seite 24
Digitale Musikstreams für analoge Geräte .....	Seite 30
3D-Drucker aufmotzen .....	Seite 32

# Ein Raspi kann Altgeräten auf die Sprünge helfen: Scannern, für die es keine Treiber mehr gibt. Druckern, denen es an einem Anschluss fürs Netzwerk mangelt. Spezialgeräten, die nur über veraltete, unsichere Protokolle kommunizieren. Audio-Equipment, das noch keine Streams empfängt.

Von Peter Siering

**M**it einem Raspberry Pi hauchen Sie älteren Gerätschaften neues Leben ein, damit die nicht so bald auf dem Recyclinghof landen. Da die Projekte nicht mal den neuesten Raspi voraussetzen, eignen sie sich obendrein gut dafür, älteren Modellen des Bastelcomputers eine sinnvolle Aufgabe zuzuschanzen.

Inspiriert durch einen Themenvorschlag, nach Projekten auch für ältere Modelle des Raspberry Pi zu suchen, entstand dieser Schwerpunkt: Der Kleincomputer ist dank Linux-Betriebssystem sehr kommunaktiv, bringt also auch alte Geräte ins Netz. Obendrein kennt seine Systemsoftware noch Geräte, deren Hersteller längst aufgegeben haben, für aktuelle Versionen von Windows und macOS Treiber herzustellen.

## Raspi-Skills

Die Anleitungen fangen nicht beim Raspi-Einmaleins an. Sie sollten auf dem Raspi aus einer Kommandozeile heraus einen Editor wie nano bedienen können, um Textdateien anzulegen oder zu ändern. Generell sollte es Ihnen nicht vor der Kommandozeile grausen: Ohne gelingt das Einrichten der Software auf dem Raspi nicht. Für die produktive Nutzung der Projekte brauchen Sie die archaische Oberfläche aber nicht mehr.

Das meist obligatorische Kopieren von Pi OS Lite auf die SD-Karte, das Aktivieren des SSH-Zugangs und erste Individualisierungen gelingen besonders flott und komfortabel mit der in [1] vorgestellten Methode; die funktioniert interessanterweise auch mit mancher spezialisierten Raspi-Distribution, wie der für 3D-Drucker auf Seite 32.

Die beiden unmittelbar auf diesen Artikel folgenden Beiträge befassen sich mit der Netzwerkkonfiguration des Raspi: Sie bringen Drucker ins Netz, wiederbeleben Scanner (S. 18) und bauen eine Brücke für alte Netzwerkprotokolle (S. 24). Wir verwenden für die Beispiele IP-Adressen, die einer typischen Fritzbox-Konfiguration entstammen. Achten Sie beim Nachbauen bitte darauf, alle IP-Adressen umzustellen, wenn Sie andere Netze verwenden – besonders bei den verwendeten Firewall-Regeln.

## Viele Wege

Apropos: Die Artikel schlagen konkrete Wege vor, die Konfiguration des Raspi zu beeinflussen, etwa Einträge in /etc/network/interfaces zur Konfiguration des Netzwerks. Raspi- und Linux-Profis ken-

nen weitere Ansätze, das zu bewerkstelligen. Solange sich die Interface-Namen nicht ändern, auf die es bei den Firewall-Regeln ankommt, spricht nichts dagegen, das Netzwerk anders zu konfigurieren. Auch beim Raspi führen oft mehrere Wege zum Ziel.

Die Artikel sparen allerdings ein Feld aus, in dem der Bastelcomputer glänzt: das Smart Home. Wir nutzen den Raspi im c't-Smart-Home-Projekt an vielen Stellen als Brückenbauer, etwa um IKEA-Smart-Home-Gadgets ohne Zentrale zu steuern oder alte Heizkörperventile anzusteuern – alle dort veröffentlichten Artikel finden Sie über ct.de/ydbr.

Auch wenn Sie keines der Projekte direkt anspricht: Jeder Artikel transportiert auch eine Menge Know-how, sei es zur Konfiguration von SMB-Diensten unter Linux, dem Einrichten von Firewall-Regeln oder tückischen Diensten zur Namensauflösung. Für den Fall, dass diesmal für Sie kein Projekt dabei war, Sie aber ein älteres Gerät unbedingt erhalten möchten und eine Chance im Raspi als Upcycling-Helfer sehen, schreiben Sie uns gern. Vielleicht finden wir eine Lösung für ein zukünftiges Projekt. (ps@ct.de) **ct**

## Literatur

- [1] Ronald Eikenberg, Raspi-Schnellstart, Raspberry Pi superschnell einrichten durch Vorkonfiguration, c't 11/2021, S. 132

**c't-Smart-Home-Projektseite:** [ct.de/ydbr](http://ct.de/ydbr)

## Nicht immer nur Raspi ...

Dem Feedback aus Leserbriefen und von unserem Leserbeirat entnehmen wir immer mal wieder, dass die Fokussierung auf den Raspberry Pi manchen stört. Dazu zwei Anmerkungen: Die im Folgenden vorgestellten Projekte lassen sich auch auf anderen Plattformen umsetzen, die eine Raspi-artige Distribution mitbringen – das gilt für die meisten „Bastelcomputer“ auf ARM-Basis. Oft ist es jedoch um die Haltbarkeit und Pflege solcher Distributionen nicht allzu toll bestellt, sodass wir lieber auf den Massenmarkt Raspi setzen. Die Pi Foundation leistet da mit Abstand bessere Arbeit.

Und: Die enge Verwandtschaft von Pi OS zu Debian ist eine große Hilfe. Zum einen kann man ab Raspi 2 auf die ARM-Pakete von Debian zurückgreifen und sich über den Backport-Zweig auch modernere Software fischen, als sie von der Pi Foundation angeboten wird (wovon die folgenden Projekte aber keinen Gebrauch machen müssen). Und, zum anderen, was viel schwerer wiegt: Solange nicht die Hardware-Fähigkeiten des Raspi gefragt sind, etwa die GPIO-Ports, lassen sich die Anleitungen ebenso mit einer Debian-Installation in einer VM auf dem Heimserver oder auf einem Mini-x86-PC umsetzen.

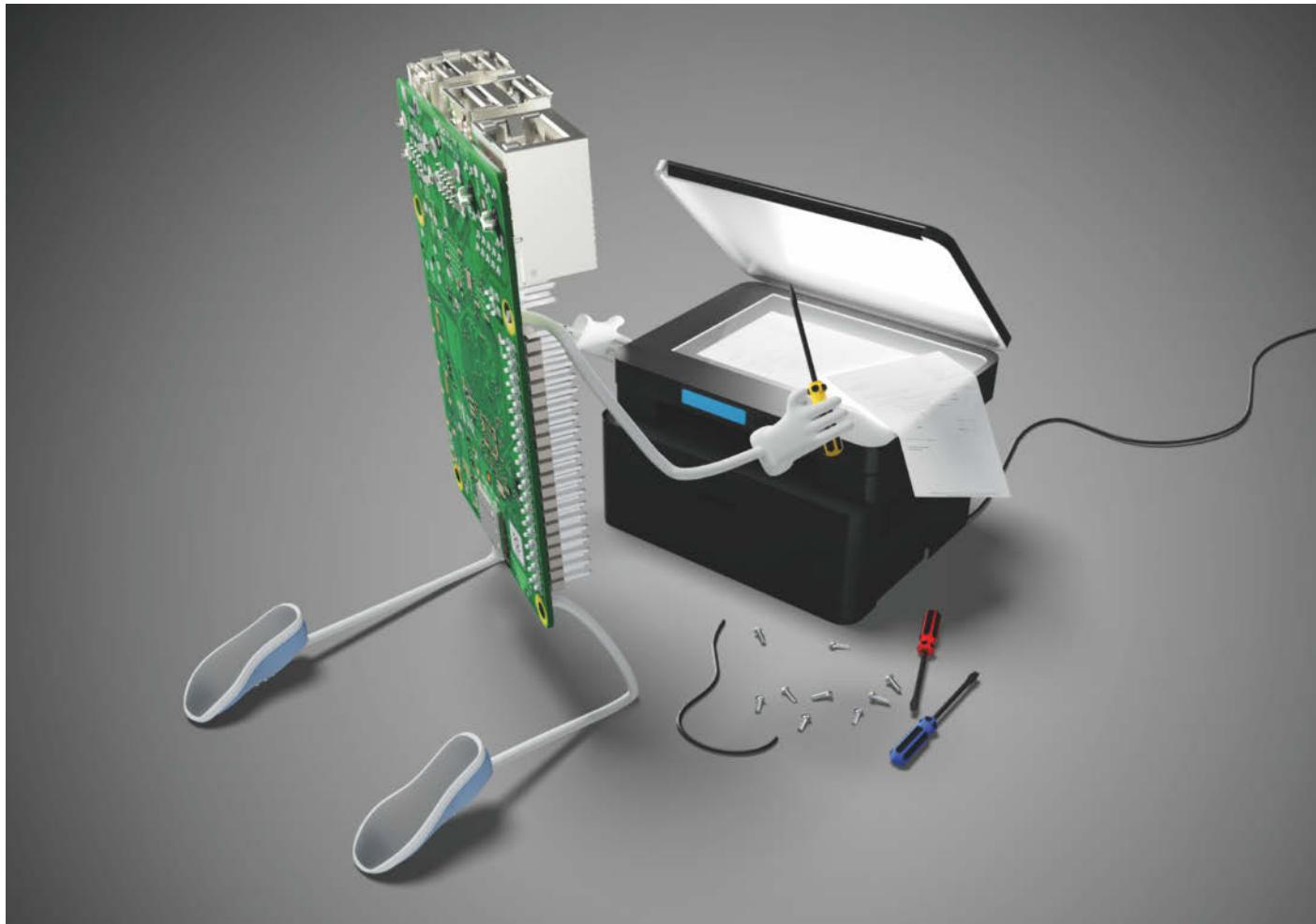


Bild: Andreas Martini

# Am Drucker bleiben

## Raspi als Lebensverlängerung für USB-Drucker und -Scanner

**Drucker und Scanner halten länger, als die Hersteller bereit sind, Treiber für aktuelle Betriebssysteme zu backen. Der Raspi hilft, die Patronen doch noch leer zu drucken, den Scanner weiterhin zu nutzen oder ein älteres Gerät überhaupt netzwerkfähig zu machen.**

Von Peter Siering

**P**i OS, das Betriebssystem des Raspi, hat als Linux-Abkömmling in der Regel Treiberunterstützung, die weniger von wirtschaftlichen Aspekten ge-

trieben wird: So unterstützt sein Drucksystem CUPS noch Modelle, für die Windows und macOS längst keine Treiber mehr liefern. Auch das für Scanner in der Linux-Welt gebräuchliche SANE glänzt mit einem breiten Angebot von Backend-Modulen für verschiedenste Neu-, aber eben auch Altgeräte.

Sowohl CUPS als auch SANE bedienen Netzwerkschnittstellen, sodass sie sich besonders gut dafür eignen, auch reine USB-Geräte in ein Netzwerk zu integrieren. Sie empfangen die gesendeten Daten und ihre Backends rechnen die Daten passend um. Fürs Drucken genügen auf den Clients die dort vorhandenen Treiber. Beim Scannen hilft eine zusätzliche Software, die unter Windows und Linux SANE als Scannerquelle einbindet. macOS kann der Raspi direkt bedienen: Ein Entwickler hat Apples Scan-

protokolle per Reverse Engineering erforscht und als Open Source implementiert.

### Versuch macht kluch

Ob CUPS und SANE ein bestimmtes Drucker-, Scanner- oder Multifunktionsgerät kennen, können Sie über eine Recherche auf den Webseiten der Projekte oft nicht zweifelsfrei ermitteln. Die dort geführten Listen sind meist schlechter gepflegt als die Software selbst. Obendrein bilden sie nicht den Stand der Pakete für CUPS und SANE ab, die in Raspberry Pi OS (und Debian Buster) enthalten sind. Und: Die Tatsache allein, dass ein Modell grundsätzlich funktioniert, heißt noch nicht, dass Sie mit den Druck- oder Scanresultaten und -optionen zufrieden sein werden.

Mitunter nämlich reicht der Leistungsumfang unter CUPS oder SANE

nicht an die Originaltreiber für längst außer Dienst gestellte Betriebssysteme heran: Mal funktioniert die Duplex-Einheit nicht. Mal fehlen Optionen für einen Farbabgleich. Oft liefern die Druckdiensste keine Informationen über Füllstände von Tinten- oder Tonerpatronen. Unter Umständen leidet die Druck- und Scanqualität.

Unser Mantra deshalb: Versuch macht kluch. Ein Aufbau aus Raspi, Altgerät und Client ist mit den im Folgenden beschriebenen Schritten auf Pi-OS-Lite in rund 30 Minuten hergestellt. Quälen Sie den Versuchsaufbau, um abzuschätzen, ob Sie mit den Ergebnissen zufrieden sind. Stecken Sie erst dann Energie in den dauerhaften Betrieb.

Die folgenden Hinweise kümmern sich erst ums Drucken und dann ums Scannen – überspringen Sie, was für Sie uninteressant ist. Für alles Weitere genügt eine Minimalinstallation von Pi OS, die Sie als Lite-Image herunterladen und mit unseren in [1] gezeigten Tipps leicht vorkonfigurieren können. Sie sollten dem Raspi einen Namen geben, da der sich gern in Konfigurationsdateien festsetzt. Exemplarisch verwendet dieser Artikel als Name „printit“. Damit sich alle Dienste darauf einstellen, müssen Sie den Raspi nach dem Namenswechsel neu booten.

## Druck-Server

Noch bevor Sie das Drucksystem CUPS einrichten, sollten Sie den Drucker per USB-Schnittstelle anschließen und einschalten (in der Ausgabe von `lsusb` sollte das Gerät jetzt auftauchen):

```
sudo apt-get install cups \
printer-driver-all hplip
```

Der Befehl fügt nicht nur den eigentlichen Dienst hinzu, sondern neben CUPS selbst gleich noch einige Pakete für gängige Druckermodelle, die aus verschiedenen freien Projekten und zum Teil von Herstellern stammen. Sie decken einen Großteil marktüblicher Modelle ab.

Mit den Paketen „`printer-driver-all`“ holen Sie nach dem Gießkannenprinzip gleich alle in Pi OS enthaltenen Treiber hinzu und mit „`hplip`“ ergänzen Sie noch einige HP-spezifischen Programme und Module. Manche Pakete helfen auch gleich beim Scannerbetrieb von Multifunktionsgeräten – machen also eventuelle Handgriffe unnötig, die der Artikel bei der Scannereinrichtung empfiehlt.

Damit der Drucker im Netzwerk sichtbar wird, muss man CUPS die Freigabe gestatten, gibt ihn im freundlichen Netzwerk auch gleich für den Zugriff aller frei und gestattet administrative Zugriffe auf die CUPS-Weboberfläche:

```
sudo cupsctl --share-printers
sudo cupsctl --remote-any
sudo cupsctl --remote-admin
```

Außerdem ist es nötig, den Benutzer, der die Drucker verwalten soll, der Gruppe „`lpadmin`“ zuzuordnen. Für den Standardnutzer „`pi`“ erledigt das dieser Befehl:

```
sudo usermod -a -G lpadmin pi
```

Jetzt können Sie in einem Browser die CUPS-Weboberfläche erreichen, auf einem Mac durch Eingabe des Namens mit angehängtem .local, also als `http://printit.local:631` – 631 ist der TCP-Port, auf dem CUPS lauscht. Auf einem Windows-PC nehmen Sie die IP-Adresse des Raspi statt „`printit.local`“; die Auflösung des .local-Namens wird dort nicht ohne Weiteres klappen (siehe Ausführungen am Ende des Artikels und im Kasten auf S. 20).

Navigieren Sie nun über die Dachzeile der CUPS-Weboberfläche zu „Verwaltung“ und betätigen Sie den Knopf „Drucker hinzufügen“. Die Administrationsoberfläche wechselt auf eine sichere Verbindung, die Ihnen eine Zertifikatswarnung einbringt. Lassen Sie die Ausnahme zu. Bei erneutem Klick auf „Drucker hinzufügen“ fordert die Oberfläche zur Eingabe von Benutzernamen und Passwort auf. Hier tut es der Standardnut-

zer „`pi`“, wenn Sie ihn wie eben empfohlen in die Gruppe „`lpadmin`“ gepackt haben.

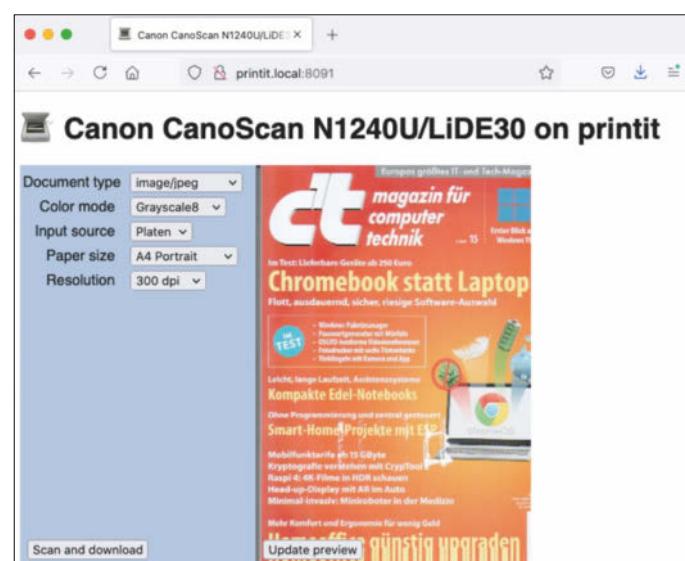
Der fünfschrittige Assistant fragt zuerst Ihr Druckmodell und die zu verwendenden Treiber ab. Die Vorschläge von CUPS liegen meist richtig. Auf der zweiten Seite setzen Sie bitte bei „Drucker im Netzwerk freigeben“ ein Häkchen. Sodann bietet CUPS den Drucker über das IPP-Protokoll im Netz an und kündigt ihn dort auch über das mDNS-Protokoll als „`printit.local`“ an. Sie haben CUPS mit diesen Schritten nähergebracht, wie es den Drucker ansprechen kann (im Windows-Speak: einen Treiber eingerichtet).

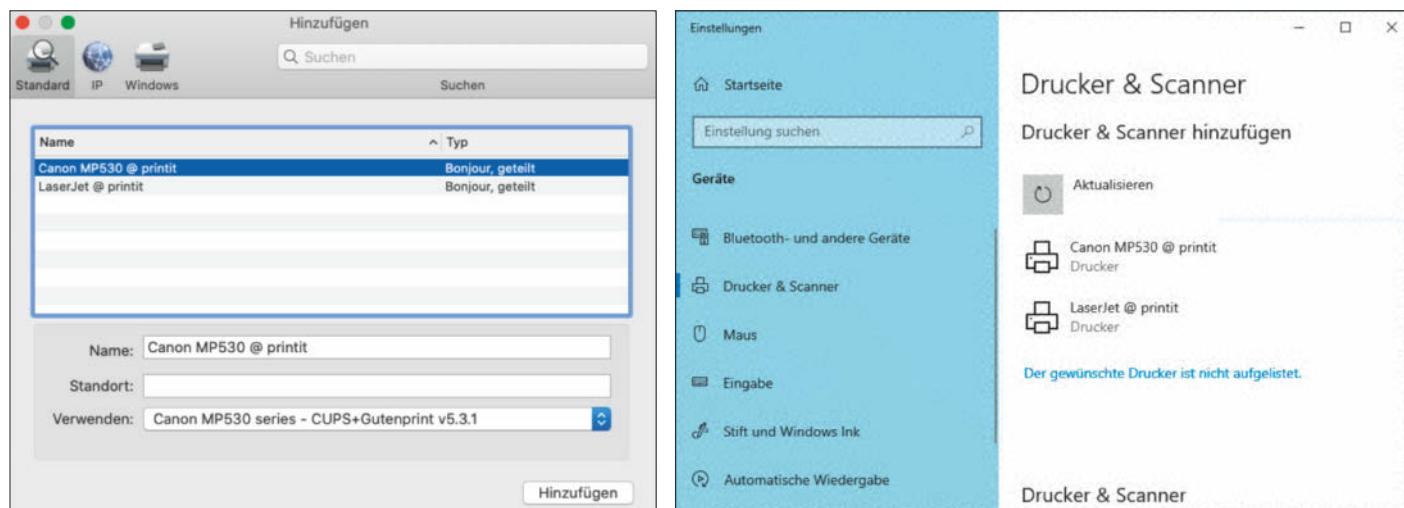
## Druck-Clients

Alle modernen Clients, egal ob unter macOS, Linux, Windows oder iOS, lauschen auf solche Ankündigungen. Sie bekommen den annoncierten Drucker dann mit ihren Einrichtungsassistenten problemlos zu fassen. Üblicherweise übermittelt IPP auch Eigenschaften des Druckers, sodass gängige Betriebssysteme von sich aus einen passenden Treiber wählen. Wenn dem Einrichtungsassistenten Details fehlen, dann deutet das auf Netzwerkprobleme hin. Solange der Client wenigstens den Raspi mit CUPS findet, können Sie manuell einen Treiber auswählen.

Wenn der Client CUPS nicht mal andeutungsweise erkennt, geben Sie bei der Druckersuche die IPP-URL ein. Die können sie für einen in CUPS eingerichteten Drucker auf der Übersichtsseite („Drucker“ in der Dachzeile) in Form eines unter seinem Namen liegenden HTTP-Links finden, etwa als `http://192.168.178.10:631/printers/Canon_MP530`. Die Assistenten

**Das AirSane-Projekt belebt nicht nur alte Scanner für aktuelle macOS-Versionen, sondern bringt auch eine eigenständig nutzbare Weboberfläche mit – genug für gelegentliche Scanaufträge mit allen Betriebssystemen.**





Dank mDNS finden sowohl macOS als auch Windows CUPS-Drucker unkompliziert.

der gängigen Betriebssysteme verarbeiten beim Einrichten von Druckern diese URL.

Wenn Sie den Komfort der automatischen Konfiguration nutzen wollen, etwa um auch per AirPrint die Drucker zu erreichen, müssen Sie sich mit der Konfiguration des Netzwerks auseinandersetzen. Die einfachste Lösung ist: den Raspi in das IP-Netz der Clients hängen. Wer größere Netzwerke am Bein hat: Spendieren Sie dem Raspi mehrere Netzwerkarten und hängen in jedes je eine oder nutzen Sie VLANs. Ein zweiter Raspi, der über seine CUPS-Installation Druckaufträge an einen anderen in einem anderen Netz weiterleitet, kann auch helfen – Sie richten dann das eine CUPS als Drucker im anderen ein.

Wird Ihr Client-System partout nicht schlau aus dem, was CUPS als Druckermodell vorschlägt, können Sie auf einen generischen PostScript-Treiber ausweichen. Unter aktuellen Windows-Versionen wählen Sie als Druckertreiber dann „Microsoft PS Class Driver“ (in älteren Versionen ging es auch mit Auswahl von Apple LaserWriter NTX). Die Daten, die dieser Treiber erzeugt, verarbeitet CUPS normalerweise und rechnet sie passend für das von Ihnen beim Einrichten von CUPS gewählte Backend um. Wenn auch das nicht klappt, dürfte Ihr Drucker reif fürs Recycling sein.

## Scan-Server

Um übers Netzwerk einen alten Scanner weiterhin nutzen zu können, den der Hersteller für Ihr Desktop-System nicht (mehr) mit brauchbaren Treibern versorgt, müssen Sie Software einrichten: auf dem Raspi als Server und bei den meisten Desktop-Betriebssystemen auch auf dem

Client. Nur macOS kann der Raspi direkt versorgen (mehr dazu weiter unten).

Zunächst zur Server-Seite: Ihr Scanner sollte während des Einrichtens am Raspi angeschlossen, eingeschaltet und somit via lsusb auch als USB-Gerät sichtbar sein. Ist das nicht der Fall, begeben Sie sich zunächst auf die Fehlersuche. Das zum Anbinden und Freigeben eines Scanners nötige Scanner Access Now Easy (SANE) lässt sich mit

```
sudo apt-get install sane-utils
```

der Raspi-Softwarekonfiguration hinzufügen; wenn Sie zuvor CUPS zum Drucken eingerichtet haben, ist das Paket schon installiert.

Bevor Sie weiter experimentieren, beachten Sie die Hinweise zu eventuellen Problemen mit Zugriffsrechten im Kasten aus Seite 22. Stimmen die Rechte, können Sie sich mit sudo -u saned sane-find-scanner vergewissern, dass SANE Ihren Scanner erkennt. Im Unterschied zum bereits empfohlenen lsusb prüft der Befehl, ob die Rechte für den aufrufenden

## Avahi zählt Hostnamen hoch

Der Avahi-Daemon implementiert unter Linux die von Apple ursprünglich als Rendezvous vorgestellte Technik, die heute mDNS heißt: Sie schafft einen simplen, benutzerfreundlichen Namensdienst im lokalen Netz. Hosts rufen beim Start ihren Namen ins Netz, der Daemon auf den Hosts registriert diese Namen und Dienste können Namensanfragen stellen. So finden Macs und Windows im Netz Drucker, aber auch Linux-Systeme zueinander.

Die Linux-Implementierung hat leider eine Masse, die gerade beim Einsatz von via mDNS angekündigten Server-Diensten wie Druckern und Scannern nervt: Dann und wann bekommt sie Schluckauf und stolpert beim erneuten Ankündigen des lokalen Hostnamens über die eigenen Ankündigungen – so berichten es Nutzer in zahlreichen Tickets. In neuen Versionen des avahi-Dae-

mon-Pakets sind Patches drin, die das verhindern sollen. Für das derzeit aktuelle Debian Buster, auf dem auch Pi OS aufbaut, sind aber bisher keine aktuellen Pakete verfügbar. Das Patchen der alten Fassung half bei uns nicht dauerhaft.

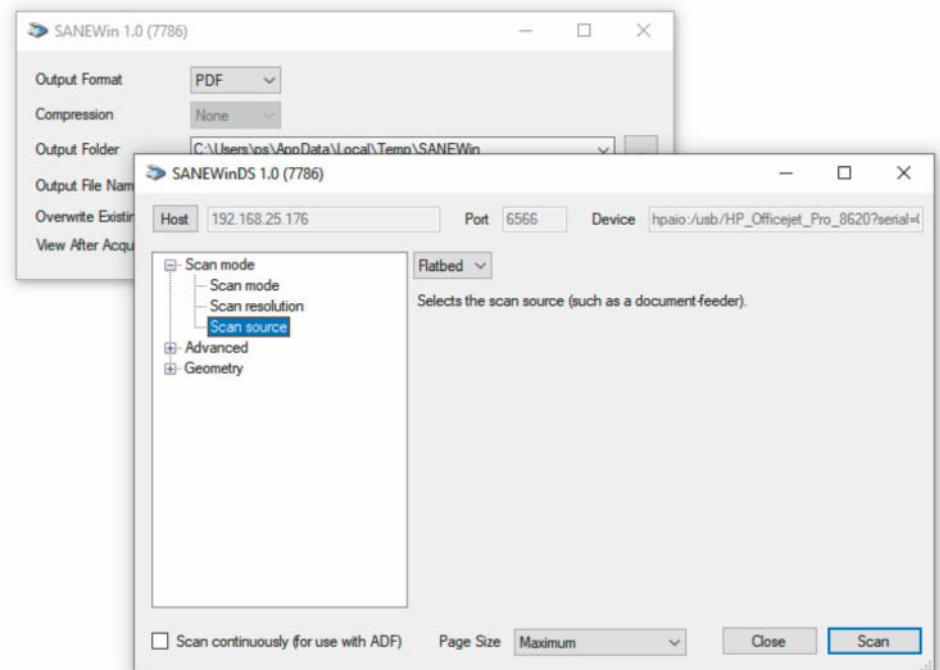
Den Tickets nach sind die von einem avahi-daemon eingefangen eigenen Ankündigungen aber nicht die einzige Ursache für den sich ändernden Namen: Läuft ein mDNS-Reflektor im Netz, etwa ein dafür konfigurierter Avahi-Daemon, der mDNS-Pakete zwischen Sub-Netzen als Proxy weiterleitet, muss man damit rechnen, dass das Hochzählen der Hostnamen erneut beginnt. Andere Nutzer haben Zusammenhänge mit wechselnden dynamischen IPv6-Präfixen beobachtet. Zur Räson bringt den Daemon in der Regel ein Neustart via systemctl restart avahi-daemon.

Nutzer (hier „saned“) passend gesetzt sind – alle SANE-Dienste verwenden diesen Nutzer, um nicht mit Root-Rechten arbeiten zu müssen.

Mehr Klarheit, ob SANE Ihr Scanner-Modell wirklich ansteuern kann, verschafft die Ausgabe von sudo -u saned scanimage -L. Die sieht bei einem erkannten Gerät zum Beispiel folgendermaßen aus: „device 'pixma:04A91712\_1089D0' is a CANON Canon PIXMA MP530 multi-function peripheral“. Kommt lediglich die Meldung „No scanners were identified“, sollten Sie prüfen, ob ein weiteres Paket für Backends bereitsteht – der Raspi kennt zwei: libsane-hpaio für HP-Multi-funktionsgeräte und libsane-extras für zwei exotischere Scanner.

Wenn auch deren Installation keine Scanner zutage fördert, dann kann dieser Artikel momentan nicht helfen, Ihren alten Scanner zu reaktivieren. Es ist durchaus möglich, dass Ihr Scanner in einer moderneren SANE-Version schon unterstützt wird. Das Einrichten einer solchen auf dem Raspi ist aber nur mit großem Aufwand und hohem Risiko möglich, weil man dazu Pakete aus dem Repository-Zweig von Debian-unstable einbinden müsste. Wenn Sie großes Pech haben, hat das SANE-Projekt Ihren Scanner auf eine Blacklist gesetzt – das tun die Entwickler, wenn die Gefahr besteht, dass SANE die Hardware ruiniert.

Die Antwort des Aufrufs von scanimage -L kommt deutlich schneller, wenn Sie in der Datei /etc/sane.d/dll.conf nur die Einträge übriglassen, die für Ihr Scanner-Modul nötig sind. Wie das Modul (im SANE-Jargon Backend) für Ihren Scanner heißt, verrät die Ausgabe von scanimage -L.



**Eher spartanisch: SANEWinDS holt Bilddaten des vom Raspi per SANE bereitgestellten Scanners, stellt aber auch eine TWAIN-Quelle bereit.**

Die Angabe hinter „device“ vor dem ersten Doppelpunkt ist der Name des Backend-Moduls (im obigen Beispiel „pixma“). Dieser Eingriff beschleunigt nicht nur scanimage, sondern auch Zugriffe auf den Scanner übers Netz.

Die Installation von sane-utils richtet nicht nur Programme für das Ansprechen eines Scanners ein, sondern fügt auch gleich einen Dienst (Daemon) hinzu, über den Software auch übers Netzwerk auf den Scanner zugreifen kann. Damit der auf Verbindungen lauscht, müssen Sie ihn zunächst per systemd aktivieren (und gleich starten):

```
sudo systemctl enable saned.socket
sudo systemctl start saned.socket
```

In der Standardkonfiguration lässt der Daemon nur Verbindungen von localhost zu. Damit Ihre Clients im Netz auf SANE zugreifen können, gehören deren IP-Adressen in die Datei zur Konfiguration des Daemon. Wenn Sie als IP-Netzwerk 192.168.178.0/24 nutzen, müssen Sie in /etc/sane.d/saned.conf folgende Zeile ergänzen:

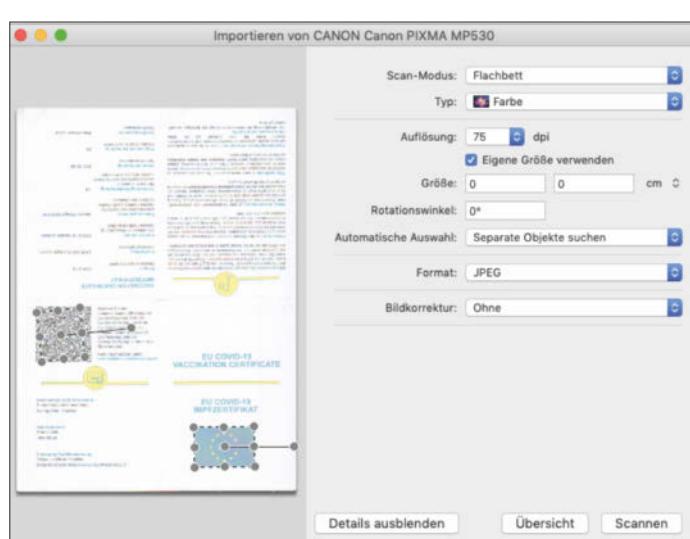
```
192.168.178.0/24
```

Sie dürfen auch sparsamer sein und nur die IP-Adressen ausgewählter Clients dort eintragen.

## Scan-Clients

Diese Handgriffe genügen, um den Scanner von einem Client aus auszuprobieren. Dazu brauchen Sie dort passende Software. Für Windows und Linux gibt es diverse SANE-Frontends. Das Prinzip ist bei beiden gleich: Sie richten die Software ein, tragen die IP-Adresse des Raspi mit dem SANE-Daemon ein und geben einen Scan-Auftrag.

Auf einem Linux-Client ist dafür – wie auf dem Server – SANE zuständig. Auf Debian-artigen Systemen (Pi OS, Ubuntu, Mint u.s.w.) müssen Sie nach dem Installieren der SANE-Pakete in der Datei /etc/saned.d/dll.conf sicherstellen, dass vorm



**AirSane bringt macOS den SANE-Scanner näher, sodass Vorschau direkt das Scannen lernt.**

Eintrag für das net-Backend kein Kommentarzeichen steht.

Außerdem müssen Sie in die Datei /etc/sane.d/net.conf die IP-Adresse Ihres Raspis eintragen. Dann findet der am Client auf einer Kommandozeile abgesetzte Befehl scanimage -L übers Netz normalerweise den Scanner am Raspi. Wenn das klappt, ist der Scanner auch in den gängigen grafischen Anwendungen zum Scannen sichtbar [2].

Für macOS hat sich in den letzten Jahren Erfreuliches getan. Neben dem alten, seit 2017 nicht mehr aktualisierten TWAIN SANE Interface ist ein neuer Ansatz entstanden: die Software AirSane (siehe ct.de/y56g). Sie verbindet SANE mit Apples AirScan-Protokoll. Ein im Netzwerk freigegebener Scanner taucht direkt in der Vorschau-App auf macOS auf und erlaubt das Starten von Scanaufträgen. Je nach Modell werden auch Funktionen wie eine Dokumentenzuführung unterstützt.

Leider gibt es AirSane noch nicht als fertiges Paket für den Raspi – die Debian-Maintainer sind wohl skeptisch, was die Anteile des Reverse Engineerings angeht. Die Hinweise zum Übersetzen und Installieren von AirSane auf seiner GitHub-Seite sind detailliert. Wir käuen sie hier deshalb nicht wieder. Auf einem Raspi 4 dauert das alles nur wenige Minuten. Wenn Sie den Scanner vorher schon auf der Kommandozeile zu sehen bekamen, taucht er nach Einrichten von AirSane nun auch in Vorschau auf.

## Dauerbetrieb

Wenn Ihnen CUPS oder SANE für den Dauerbetrieb zusagen, sollten Sie überlegen, ob Sie den Raspi mit einer festen IP-Adresse versehen und diese beziehungsweise den dafür hinterlegten Namen zur Konfiguration auf den Clients nutzen. Leider hat der für eine dynamische Konfiguration zuständige Avahi-Daemon in aktuellen Versionen von Pi OS eine Mache (siehe Kasten auf S. 20), die den mDNS-Netzwerknamen des Raspi eigenmächtig hochzählt. Das stört für die Ad-hoc-Inbetriebnahme via AirPrint & Co. nicht, aber für den stationären Betrieb eines Mac kann es schon nerven, wenn der für printit eingerichtete Drucker Wochen später nur noch als printit-751 im Netz bekannt ist.

Weitere Unbill droht bei IPv6: Vergibt ein Router offizielle Adressen aus einem vom Provider erhaltenen dynamischen IPv6-Präfix, könnte es sein, dass Druck-

## Rechteverdreher: Spaß mit Geräten, udev, Gruppen und Nutzern

Beim Zugriff auf Scanner und Drucker unter Linux können allerlei Dinge subtil querschießen. Häufig hat es mit Zugriffsrechten zu tun. Beim Anstecken von USB-Geräten legt der udev-Daemon im Dateibaum Pseudodateien an, die für den Zugriff notwendig sind. Der Daemon greift dafür auf ein umfangreiches Regelwerk zurück, das auch beschreibt, wer auf ein Gerät zugreifen darf.

Für Scanner und Drucker gibt es spezielle Gruppen wie lp und scanner. In diese Gruppen kann man reguläre Nutzerkonten wie „pi“ auf dem Raspi einsortieren. Die Gruppen nehmen aber auch spezielle Nutzerkonten auf, die für Dienste eigens erzeugt worden sind, zum Beispiel „saned“ für den SANE-Daemon. Fehlt diese Zuordnung, kann SANE einen Scanner nicht ansteuern.

Wem ein Gerät gehört und welche Gruppe darauf zugreifen darf, findet man recht leicht heraus: lsusb listet alle USB-Geräte auf. Mit der Bus- und Gerätenummer des Scanners oder Druckers baut man den Gerätepfad zusammen und lässt sich die Rechte anzeigen, etwa mit getfacl /dev/bus/usb/001/003.

Viele Konten, Gruppen und Zugehörigkeiten richten SANE und CUPS Pakete beim Installieren von sich aus ein. Aber nicht alle: Wer auf dem Raspi ohne sudo

als Nutzer „pi“ scanimage -L aufrufen will, muss den Nutzer in die Gruppe „scanner“ packen (sudo usermod -a -G scanner pi). Dieser Gruppe gehört üblicherweise der Geräteknoten.

Aber Achtung: Manch ein Multifunktionsgerät (Mufu) weist udev der Gruppe „lp“ zu. Dann liefert scanimage -L erst dann den erstrebenswerten Hinweis aufs Gerät, wenn man „pi“ in diese Gruppe steckt, etwa mit sudo usermod -a -G lp pi. Auch SANE ist davon betroffen: Zum Scannen mit einem Mufu per SANE übers Netz gehört der Nutzer „saned“ in die Gruppe „lp“.

Obendrein verhindert bei einfachen Scannern eine fehlende udev-Regel im aktuellen Pi OS (auf Basis von Debian Buster) den Betrieb. Ohne Eingriff sind die Scanner nur für den Nutzer root zugänglich. Legen Sie deshalb als root unter /etc/udev/rules.d die Datei 65-lib sane.rules an und schreiben Sie dort Folgendes hinein (alles in einer Zeile):

```
ENV{libsane_matched}=="yes", ↵
  RUN+=" /usr/bin/setfacl ↵
    -m g:scanner:rw $env{DEVNAME}"
```

Nach einem Reboot funktionieren die zuvor eingeführten Kommandos sane-find-scanner und scanimage -L auch für einen einfachen USB-Scanner.

oder Scandienste nach einigen Wochen den Dienst einstellen, wenn es ein neues IPv6-Präfix vom Provider gegeben hat. Oft genügt ein Restart von Scan- oder Druckdienst, die Dinge wieder ins Lot zu bringen. Langfristige Abhilfe liegt jenseits dieses Artikels: Konsequenter Verzicht von IPv6 mag helfen, ist aber kontraproduktiv bei den auf IPv6-Autokonfiguration angewiesenen Apple-Scandiensten. Der Einsatz privater lokaler IPv6-Adressen (ULA) mit gezielten gesetzten Routen, die diese Adressen übervorteilen, könnte helfen.

Der Raspi bringt die Altgeräte dank des Linux-Treibers supports nichts nur wieder ins Spiel, sondern eröffnet ihnen auch neue Möglichkeiten, weil sie nun im Netz erreichbar sind. Wenn Sie die Hilfestellungen des Artikels mit allzu neuen Geräten nachspielen, ist Enttäuschung vorpro-

grammiert, weil CUPS und SANE in Pi OS doch schon einige Jahre alt sind. Welches Raspi-Modell Sie am besten nehmen, hängt sicher vom Umfang der Druckaufträge und Ansprüche an die Druckgeschwindigkeit ab. Im Privathaushalt des Autors genügt ein Modell 3 bisher allen Anforderungen – auch denen ungeduldiger Studenten.

(ps@ct.de) **ct**

## Literatur

- [1] Ronald Eikenberg, Raspi-Schnellstart, Raspberry Pi superschnell einrichten durch Vorkonfiguration, c't 11/2021, S. 132
- [2] Rudolf Opitz, Fotos für Pinguine, Scanner mit Linux nutzen, c't 12/2021, S. 146

**AirSane, Kompatibilitätslisten für CUPS und SANE:** [ct.de/y56g](http://ct.de/y56g)



1blu

## Domainregen Homepage Boom

NOCH BIS ENDE AUGUST 2021

Keine Bestellannahme nach  
dem 31.08.2021!

!

12 .de-Domains inklusive

Kostenlose SSL-Zertifikate

- > Webbaukasten inklusive
- > SSL-Certs von Let's Encrypt für alle Domains per Mausklick
- > 100 GB SSD-Webspace
- > Zusätzlicher Onlinespeicher (30 GB)
- > 4 externe Domains
- > 1.000 E-Mail-Adressen
- > 100 GB E-Mail-Speicher
- > 100 aktuelle 1-Klick-Applikationen
- > 100 SSD MySQL-Datenbanken

2,29  
€/Monat\*

Dauerpreis

\* Preis/Monat inkl. 19% 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/boom](http://www.1blu.de/boom)

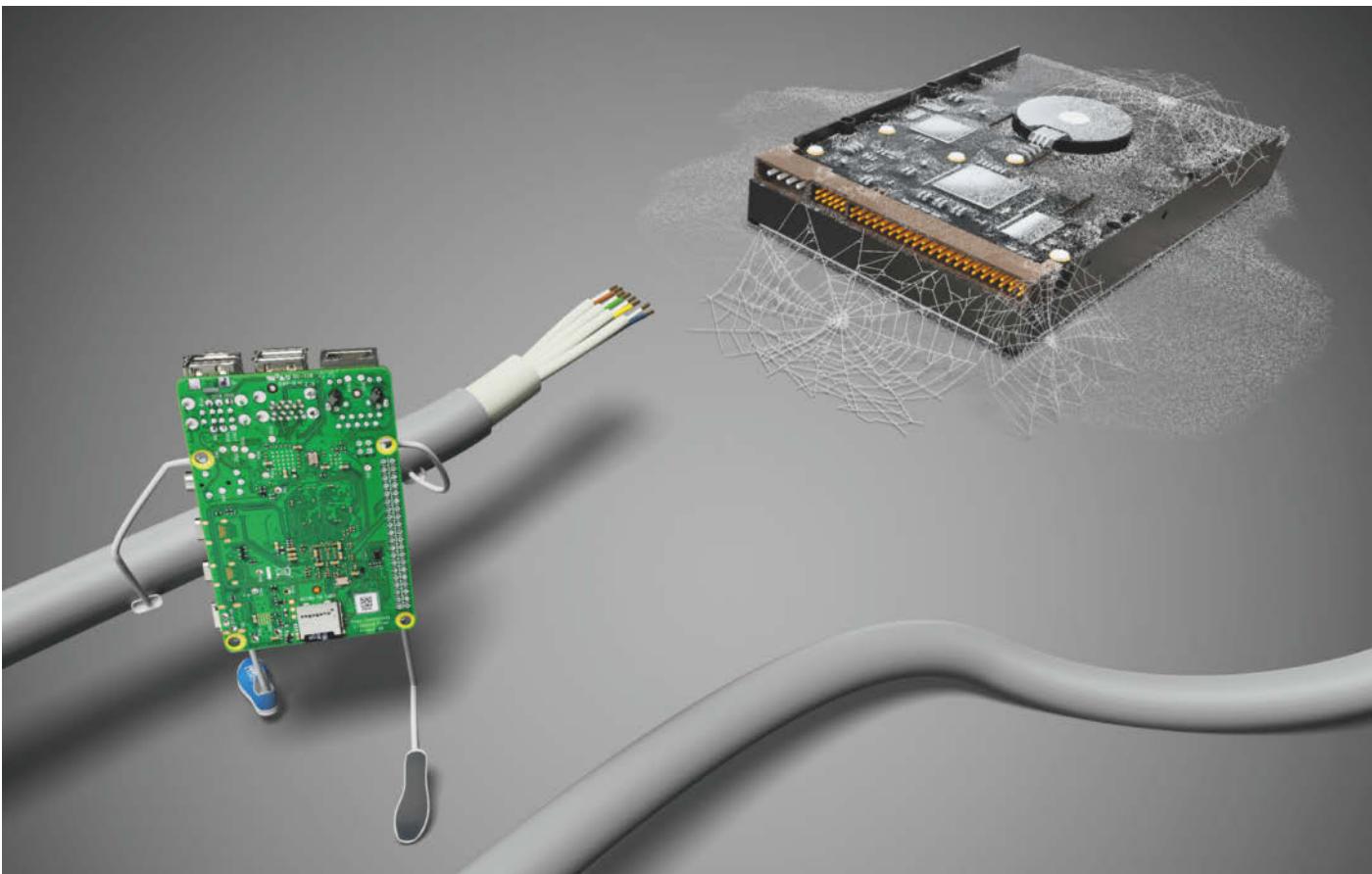


Bild: Andreas Martini

# Brückenbau

## Raspberry Pi als Brücke zu SMBv1-Gerätschaften

**Manches Gerät, zum Beispiel ein Scanner, kann Dateien im Netz abladen und benutzt dafür das SMB-Protokoll. Wenn es ungünstig läuft, versteht es sich nur auf das wegen vieler Sicherheitslücken verpönte SMBv1. Wer auf das Gerät nicht verzichten will, muss entweder das unsichere SMBv1 in seinem Netz erlauben oder kann einen Raspi als Protokollbrücke einsetzen.**

Von Peter Siering

**D**ass das SMBv1-Protokoll unsicher ist und in keinem Netzwerk heute mehr benutzt werden sollte, ist schon seit einigen Jahren sehr klar: Lücken in der Implementierung des Serverdienstes in Windows führten zu einer rasanten Verbreitung von Würmern. Auch die Clients sollte man heutzutage meiden, weil sie keine sicheren Verbindungen herstellen und sich leicht Zugangsdaten entlocken lassen.

Dennoch werden noch heute Geräte in Umlauf gebracht, die nur SMBv1 für den Dateiaustausch kennen. Und: In manchem kostspieligen Gerät steckt eben auch ein Netzwerkstack, der nur das alte Protokoll beherrscht, ohne dass es eine Aussicht auf eine Aktualisierung durch den Hersteller gibt. Mit einem Raspberry Pi können Sie sich als Betreiber solcher Altgeräte selbst helfen und brauchen die Sicherheit eines Produktivservers durch Aktivieren von SMBv1 nicht weiter zu gefährden.

Die Grundidee dieser Praxisanleitung ist, das Altgerät so einzuhügeln, dass es allein mit einem Raspi Daten über das verpönte SMBv1-Protokoll austauscht. Der Raspi reicht die Daten dann an einen Produktivserver weiter, zu dem er per SMBv2/3 spricht. Weiterreichen beschreibt dabei keinen aktiven Kopierprozess, sondern lässt sich schlicht über das Durchreichen eines freigegebenen Verzeichnisses realisieren.

Der Raspi verbindet sich also als Client mit dem Produktivserver, auf dem die Daten des Geräts, etwa Scans, landen sollen – er mountet dazu via SMBv2/3 die Freigabe an einem lokalen Verzeichnis, etwa /reshare. Dieses lokale Verzeichnis gibt der Raspi seinerseits als SMB-Laufwerk für den Zugriff des Geräts frei – diese Freigabe lässt sich so konfigurieren, dass sich nur das SMBv1-Altgerät verbinden kann. Wer es perfekt will, geht noch einen Schritt weiter und sperrt Raspi und Alt-

gerät in ein separates Netz weg – dann wären im Produktivnetz keine SMBv1-Clients und -Server mehr aktiv.

Klingt einfach, wenn man regelmäßig mit Samba hantiert. Hat aber auch dann diverse Tücken: Es müssen Benutzerkonten passend eingerichtet, Rechte angemessen gesetzt und bei höherem Sicherheitsbedarf Netze konfiguriert sein. Und man sollte bei all dem nicht aus den Augen verlieren, dass der Raspi keine Performancewunder vollbringen wird und dass sich das Verfahren nur dann wirklich eignet, wenn es um simple Dateiübertragungen geht. Ein gemeinsamer gleichzeitiger Zugriff auf Dateien, die das Gerät gerade schreibt, gibt früher oder später Datensalat.

## Client-Seite

Schnappen Sie sich einen Raspi, idealerweise einen modernen mindestens mit Ethernet-Port. Bespielen Sie eine Speicherkarte mit Pi OS in der Lite-Ausgabe. Booten und konfigurieren Sie das Image passend durch (Spracheinstellungen, SSH et cetera). Die weiteren Hinweise gehen der Einfachheit halber davon aus, dass Sie alle Schritte als Nutzer „root“ ausführen (also nach der Anmeldung als „pi“ zunächst einmal `sudo su` ausführen).

Die IP-Adressen und Namen für die Benutzer sind Beispiele, passen Sie diese an Ihre Geräte und Netzwerk an. Der Übersicht halber die hier verwendeten Adressen: 192.168.178.2 ist der Produktivserver, auf dem die Dateien schließlich landen sollen. 192.168.178.5 ist die Adresse des Altgeräts. Der Raspi könnte die Adresse 192.168.178.3 erhalten.

Um den Raspi als Datenumschlagplatz zu verwenden, brauchen Sie ein Verzeichnis, in dem diese Daten liegen. Dieses Verzeichnis heißt in unserem Beispiel `/reshare`. Dateien, die dort landen, müssen einem Benutzerkonto zugewiesen sein, das unser Beispiel „reuser“ nennt. Verzeichnis und Konto müssen Sie auf dem Raspi anlegen, was mit einem Befehl gelingt (alle Befehlszeilen und Konfigurationsdateiexample aus diesem Artikel finden Sie auch zum einfachen Kopieren in einem Gist auf GitHub, siehe ct.de/ytej):

```
adduser reuser --disabled-password \
--gecos "" --home /reshare --quiet
```

Der Befehl erstellt obendrein eine Gruppe namens „reuser“. Verbinden Sie dieses Verzeichnis dauerhaft mit einer Freigabe auf

dem Produktivserver, indem Sie in der Datei `/etc/fstab` folgenden Eintrag ergänzen:

```
//192.168.178.2/scans /reshare cifs \
uid=reuser,gid=reuser, \
credentials=/root/cred
```

Der UNC-Pfad („//192 ...“) verweist auf die Freigabe im Produktivnetz. Es schließt sich der Ort an, wo der Raspi die Freigabe einhängen soll. Mit „cifs“ erfährt er, welche Art von Dateisystem es ist. Die Angaben „uid“ und „gid“ sorgen dafür, dass das Raspi der Meinung ist, dass die Dateien auf der Freigabe dem lokalen Nutzer „reuser“ und seiner Gruppe gehören.

Die in `/etc/fstab` referenzierte Datei mit den Zugriffsparametern (`/root/cred`) muss wie folgt aussehen:

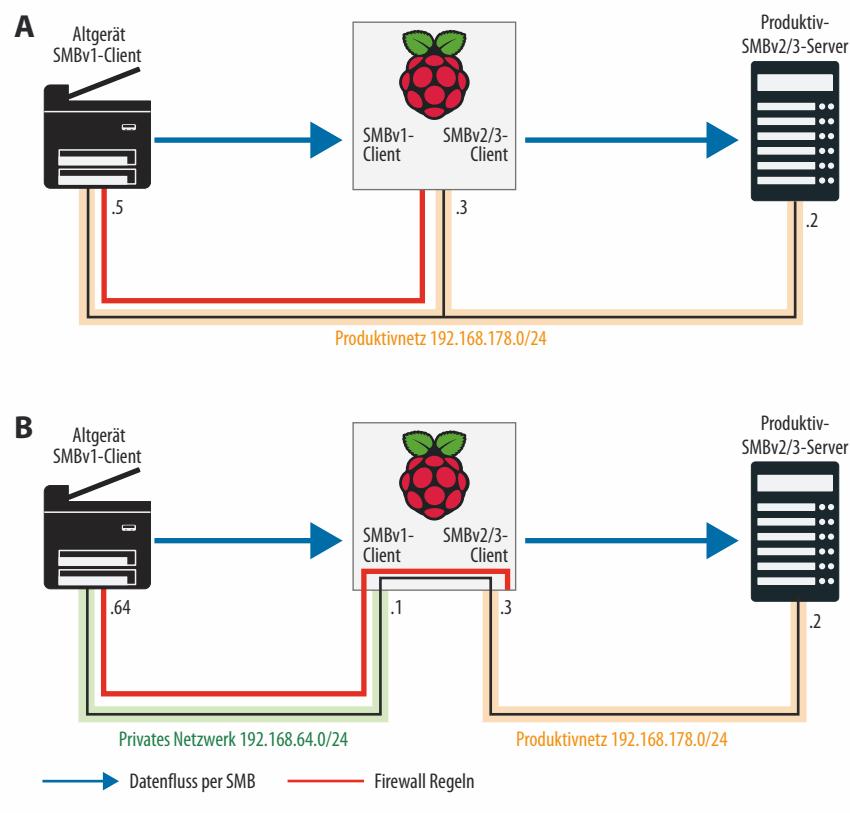
```
username=upuser
password=uppassword
domain=example
```

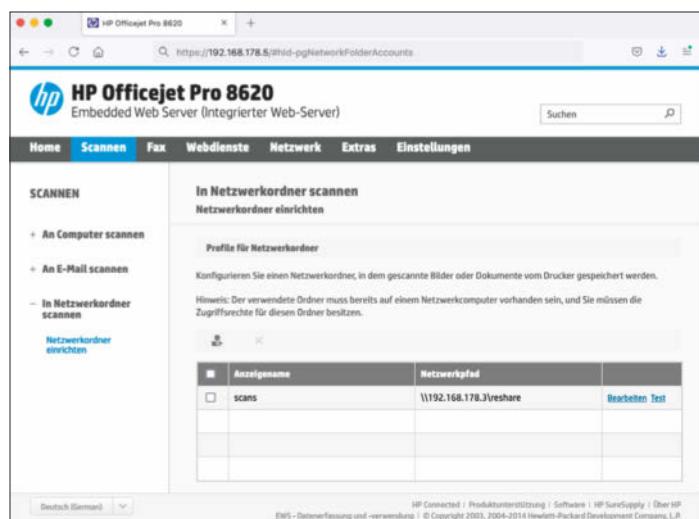
„upuser“ und „uppassword“ sind Benutzername und Passwort, die für den Zugriff auf die Freigabe des Produktionsservers nötig sind; diese können Sie durch die bisher von Ihrem Gerät verwendeten Zugangsdaten ersetzen. Die Zeile mit „domain“ ist nur notwendig, wenn es sich dabei um einen Server handelt, der in einem Active Directory hängt; sie kann sonst entfallen.

Nach Erweitern beziehungsweise Anlegen der Dateien können Sie den Raspi mit `mount -a` anweisen, alle Mounts einzubinden. Jetzt sollten Sie in `/reshare` vorhandene Dateien auf der Freigabe auf dem Zielserver sehen. Bleibt das Verzeichnis leer, obwohl auf dem Server Dateien liegen, die der Nutzer „upuser“ sehen kann, prüfen Sie die einzelnen Konfigurationsstufen auf eventuelle Fehler. Versuchen Sie auch, die Freigabe nebst Dateien mit einem anderen Client zu erreichen, um grundsätzliche Zugriffsprobleme auszuschließen.

## SMB-Brücke mit Raspberry Pi

Je nach Sicherheitsanspruch gibt es zwei Varianten, eine Brücke zwischen einem alten SMBv1-Gerät und einem sicheren SMBv2/3-Server zu bauen. Bei A hängen alle Geräte in einem Netzwerk. Firewallregeln auf dem Raspi stellen sicher, dass nur das Altgerät per SMBv1 zugreifen darf. Für andere Geräte ist der verpönte SMBv1-Server nicht sichtbar. Bei B versorgt der Raspi wie ein Router ein zusätzliches Netz für den SMBv1-Verkehr. Das ist sicherer, weil der SMBv1-Client nur für den Raspi sichtbar ist. Für den Zugriff auf weitere Dienste des Altgeräts erfordert das aber aufwendigere Firewallregeln.





## Server-Seite

Um auf dem Raspi eine SMBv1-Freigabe einzurichten zu können, brauchen Sie dort Samba:

```
apt-get install samba
```

Schlagen Sie die eventuell angebotenen Hilfen zur Konfiguration bei der Paketinstallation aus (drücken Sie einfach Return, bis die Nachfragen aufhören). Überschreiben Sie die Konfigurationsdatei /etc/samba/smb.conf für den Serverdienst mit folgender Minimalversion:

```
[global]
workgroup = SMBONE
ntlm auth = ntlmv1-permitted
interfaces = eth0
[reshare]
path = /reshare
root preexec = mount /reshare
writeable = yes
force user = reuser
force group = reuser
veto files = .ssh
```

Im Abschnitt [global] sorgt die Option ntlm auth = ntlmv1-permitted dafür, dass Samba überhaupt SMBv1-Verbindungen annimmt. Die für das Weiterreichen von Dateien in [reshare] beschriebene Freigabe lässt alle angelegten Dateien „reuser“ und seiner Gruppe gehören.

Die Option veto files verhindert, dass sich der „reuser“ über das Anlegen einer .ssh/authorized\_keys-Datei Zugang zum Raspi via SSH erschleicht. Eine interaktive Anmeldung per Benutzername und Passwort ist ihm ohnehin schon untersagt, da sein Konto mit der Option --disabled-password angelegt worden ist.

Beim Verbindungsaufbau eines Clients lässt root preexec vorsichtshalber das /reshare-Verzeichnis mounten. Das automatische Mounten beim Booten des Raspi klappt trotz Eintrags in der /etc/fstab-Datei nicht zuverlässig. Die verwendete Samba-Option erspart elendiges Gefummel mit systemd.

Damit das Altgerät auf die Samba-Freigabe zugreifen kann, müssen Sie für den angelegten Nutzer „reuser“ noch ein Samba-Passwort setzen. Das erledigt der folgende Befehl, indem er zweimal zur interaktiven Eingabe des Passworts auffordert:

```
smbpasswd -a reuser
```

Starten Sie den Samba-Server neu, um sicherzustellen, dass alle Änderungen so weit auch einen Neustart überleben und dass der Samba-Server mit den eingestellten Parametern läuft:

```
systemctl restart smbd
```

```
iptables -I INPUT -i eth0 -p tcp -m multiport --ports 445,137,139 -j DROP
iptables -I INPUT -i eth0 -p udp -m multiport --ports 137,139 -j DROP
iptables -I INPUT -i eth0 -p tcp -m multiport --ports 445,137,139 -s 192.168.178.2 -j ACCEPT
iptables -I INPUT -i eth0 -p udp -m multiport --ports 137,139 -s 192.168.178.2 -j ACCEPT
iptables -I INPUT -i eth0 -p tcp -m multiport --ports 445,137,139 -s 192.168.178.5 -j ACCEPT
iptables -I INPUT -i eth0 -p udp -m multiport --ports 137,139 -s 192.168.178.5 -j ACCEPT
```

**Bevor Sie SMBv1 auf Ihrem Produktivserver abschalten können, müssen Sie dem Altgerät den als Brücke arbeitenden SMB-Server auf dem Raspi näherbringen.**

Auf dem Altgerät müssen Sie dann „reuser“ als Konto und das soeben eingegebene Passwort hinterlegen, damit es auf die Freigabe „reshare“ zugreifen kann (über den UNC-Pfad //192.168.178.3\reshare). Dateien, die das Altgerät auf der Freigabe via SMBv1 ablegt, tauchen auf dem SMBv2/3-tauglichen Server unmittelbar auf. Sie haben erfolgreich eine Brücke geschlagen.

Noch ist der für SMBv1 konfigurierte Server aber für alle Systeme im Netzwerk sichtbar. Mit einigen Extra-Firewallregeln können Sie dafür sorgen, dass der Raspi nur mit dem Altgerät und dem Produktivserver SMB spricht und sich dem restlichen Netz gegenüber zugeknöpft gibt – die Regeln (siehe Listing im Kasten unten) braucht es aber allenfalls dann, wenn Sie auf weitere Schutzmaßnahmen verzichten wollen.

Damit diese Regeln dauerhaft aktiv bleiben, installieren Sie anschließend unbedingt die Hilfskripte zum Speichern der Firewall-Regeln:

```
apt-get install iptables-persistent
```

Die Installation des Pakets fragt gleich, ob Sie die Regeln speichern wollen. Nehmen Sie das Angebot an. Ihre SMB-Brücke ist jetzt betriebsbereit und genügt grundlegenden Sicherheitsanforderungen. Wenn Sie mehr wollen, lesen Sie weiter, wenn Ihnen das genügt, beachten Sie auch die Hinweise am Ende des Artikels unter „Extra-Tipps“.

## Netz auswerfen

Bei der so weit beschriebenen Konfigurationsmethode bleibt das Altgerät als SMBv1-Client im Netzwerk sicht- und somit angreifbar. Wenn Sie auch das vermeiden wollen, können Sie den Raspi ein zusätzliches Netzwerk versorgen lassen, das allein zur privaten SMBv1-Kommunikation mit dem Altgerät dient. Sie sperren das Altgerät letztlich in einem privaten Netzwerk weg.

Das verursacht weitere Arbeit für den Fall, dass das Altgerät nicht nur per SMB Daten abliefern soll, sondern auch der Zugriff darauf über andere Protokolle aus dem Produktivnetz heraus möglich sein

**Diese Firewall-Regeln sorgen dafür, dass der Raspi SMB-Verbindungen nur mit dem Altgerät und dem Produktivserver eingehet, Anfragen anderer Geräte per SMB aber verwirft.**

# IT FÜR DIE INDUSTRIE. MADE IN GERMANY.



Industrie-Prozesse digitalisieren mit  
spezieller High-End Hardware.  
Jetzt mehr erfahren:

[exone.de/  
ct15](http://exone.de/ct15)



individuelle, passgenaue  
inhouse Assemblierung



Sicherheit und Qualität  
für höchste Ansprüche



persönlicher, kompetenter  
Ansprechpartner

Unsere Industrie IT Marken

**calmo®**  
Industrial IT made in Germany

**Pokini**  
*IT for rough environments*

**exone®**  
IT für Unternehmen

Sie sind auf der Suche nach einem zuverlässigen Partner um das Sortiment Ihres Systemhauses zu erweitern oder um ein IT-Großprojekt umzusetzen? Dann lassen Sie sich von uns überzeugen.

**07322 96 15 - 288 | [www.extracomputer.de](http://www.extracomputer.de) | [info@extracomputer.de](mailto:info@extracomputer.de)**

EXTRA Computer GmbH · Brühlstraße 12 · 89537 Giengen | Irrtum und Änderung vorbehalten. Nur solange der Vorrat reicht.



muss, zum Beispiel das Aufrufen einer Weboberfläche oder das Übermitteln von Druckdaten. Doch das können Firewall-Regeln auf dem Raspi lösen.

Die eben zur minimalen Absicherung des SMBv1-Servers gesetzten Firewall-Regeln sind dafür allerdings kontraproduktiv. Wenn Sie diese gesetzt haben sollten, verwerfen Sie sie jetzt gleich mit:

```
netfilter-persistent flush
```

Jeder Raspi ab Modell 3 hat sowohl eine Ethernet- als auch WLAN-Schnittstelle. Das Folgende geht davon aus, dass Sie ein solches Modell verwenden und das WLAN benutzen, um den Raspi mit Ihrem Produktivnetz zu verbinden (die Adresse 192.168.178.2 weiterhin für den Produktivserver angenommen). Sie können bei einem frischen Pi-OS-Image zum Beispiel raspi-config verwenden, um den Raspi ins WLAN zu bringen oder das gleich beim Bespielen der Speicherkarte erledigen [1].

Die Ethernet-Schnittstelle hingegen verbinden Sie mit dem Altgerät. Neuere Raspis erkennen automatisch den Kabeltyp (Auto-MDI-X), Sie brauchen also meist kein Cross-Connect-Ethernetkabel oder einen Switch zwischen Altgerät und Raspi.

Die Vorgabe für die Schnittstellen hat Gründe: Im Produktivnetz werden Sie tendenziell einen WLAN-Access-Point vorfinden, im privaten Netz müssten Sie den erst einrichten. Sie können statt des WLANs ebenso gut eine zweite USB-Ethernet-Schnittstelle nutzen. Die Namen der Netzwerkgeräte müssen Sie dann entsprechend anpassen (etwa eth1 anstelle von wlan0 verwenden).

Für den Einsatzzweck empfehlen sich feste IP-Adressen. Die können Sie über die Datei /etc/network/interfaces vorgeben. Die Adressen für wlan0 müssen Sie an Ihr Netzwerk anpassen. Wenn Sie auf den zweiten Block verzichten (alles ab allow-hotplug wlan0), läuft das Folgende auch mit einer dynamischen IP-Adresse aus dem WLAN:

```
allow-hotplug eth0
iface eth0 inet static
  address 192.168.64.1
  netmask 255.255.255.0

allow-hotplug wlan0
iface wlan0 inet static
  address 192.168.178.3
  netmask 255.255.255.0
  gateway 192.168.178.1
```

```
dns-nameservers 192.168.178.1
wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

Wenn Sie sich per WLAN mit dem Produktivnetz verbinden und eine statische IP-Konfiguration bevorzugen, ist die Zeile wpa-conf wichtig. Der dort referenzierten Datei entnimmt der Raspi die Zugangsdaten für das Funknetz. Sie sieht so aus, wenn Sie für das initiale Einrichten des WLAN den Assistenten von raspi-config bemühen (die Angaben in den Anführungszeichen hinter ssid und psk müssen Sie an Ihr WLAN anpassen):

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=DE
network={
  ssid="meinwlan"
  psk="meinepassphrase"
}
```

Die Netzwerkkonfiguration des Altgeräts müssen Sie so umstellen, dass es sich im vom Raspi versorgten Netz wiederfindet. Entweder Sie vergeben eine feste IP-Adresse (passend zur obigen Konfiguration für eth0 zum Beispiel die Adresse 192.168.64.50) oder Sie lassen einen Dienst auf dem Raspi diese Aufgabe übernehmen. Für letzteres bietet sich dnsmasq an. Den Dienst richten Sie auf dem Raspi mit

```
apt-get install dnsmasq
```

ein. Damit dnsmasq im privaten Netzwerk zwischen Raspi und Altgerät IP-Adressen verteilt und DNS-Anfragen des Geräts in die weite Welt schickt, braucht dnsmasq in der Konfigurationsdatei /etc/dnsmasq.conf zwei angepasste Zeilen (sie finden sich dort nach der Installation nur in ähnlicher, auskommentierter Form):

```
interface=eth0
dhcp-range=192.168.64.50,192.168.64.50,12h
```

Den Bereich für DHCP-Adressen ist bewusst eng gewählt. Sie können ihn natürlich anders belegen. So ist jedenfalls sicher gestellt, dass das Altgerät genau diese eine Adresse erhält.

Egal, ob mit fester oder dynamischer IP-Adresse: Mit der so weit ausgeführten Konfiguration können nach einem Reboot Raspi und Altgerät via IP Pakete austau-

schen. Ein auf dem Raspi aufgerufenes ping 192.168.64.50 sollte Antwortpakete des Altgerätes bringen. Wenn das Altgerät wie eingangs beschrieben für die Dateiablage auf dem Samba-Server des Raspi konfiguriert ist, sollte jetzt auch der Dateiaustausch gelingen.

## Altgerät in die Welt

Soll das Altgerät sich ausschließlich mit dem Raspi unterhalten können und selbst nicht ins Internet gelangen, überspringen Sie die folgenden Hinweise bis „Welt an Altgerät“. Wenn das Altgerät weiterhin Dienste im Produktivnetz und im Internet erreichen soll, muss der Raspi aktiv Pakete weiterleiten. Das erreichen Sie durch Anlegen der Datei /etc/sysctl.d/97-ipfw.conf mit folgendem Eintrag:

```
net.ipv4.ip_forward=1
```

Rufen Sie zum Einlesen der neuen Kernel-einstellung hinterher sysctl --system auf. Damit die Antworten aus entfernten Netzen zurückfinden, sollte der Raspi außerdem alle Verbindungen nach außen via Network Address Translation (NAT) hinter seiner IP-Adresse verstecken. Das ist mit einer Firewall-Regel getan, die abgehende Pakete vom Altgerät (192.168.64.50) auf das Produktionsnetz umschreibt (an wlan0):

```
iptables -t nat -I POSTROUTING \
-o wlan0 -j MASQUERADE \
-s 192.168.64.50/32
```

Um das Altgerät daran zu hindern, via SMBv1 auf Geräte im Produktivnetz zuzugreifen, sperren Sie mit folgenden Firewallregeln die dafür benutzten Ports und Protokolle, wenn die Pakete aus dem privaten Netz kommen (eth0) und in andere Netze gerichtet sind (FORWARD):

```
iptables -I FORWARD -i eth0 -p tcp \
--dport 445 -j DROP
iptables -I FORWARD -i eth0 -p tcp \
-m multiport --ports 137,139 -j DROP
iptables -I FORWARD -i eth0 -p udp \
-m multiport --ports 137,139 -j DROP
```

Speichern Sie die neuen Firewallregeln:

```
netfilter-persistent save
```

Wenn Sie auf das Einrichten von dnsmasq verzichtet haben, tragen Sie auf dem Altgerät die IP-Adresse des im Produktivnetz genutzten DNS-Servers ein, etwa die

IP-Adresse Ihrer Fritzbox. Jetzt kann das Altgerät reguläre Dienste im Internet erreichen, nicht jedoch SMB-Server. Der Raspi dient als Router dorthin.

Mit einer feiner dosierten NAT-Konfiguration für ausgehende Verbindungen vom Altgerät ins Internet könnten Sie ihm weitere Maulkörbe über SMB hinaus verpassen. Sie könnten nur ausgewählte Ports freischalten, etwa nur Zugriffe auf die Server des Geräteherstellers erlauben oder auch gezielt unterbinden. Was und ob das notwendig ist, müssen Sie selbst entscheiden. Wenn SMBv1 das einzige bekannte Problem ist, sollten die so weit genannten Schritte genügen.

## Welt an Altgerät

Was hingegen für manches Altgerät sinnvoll sein dürfte, sind Firewallregeln auf dem Raspi, um gezielt Verkehr dorthin zu leiten, etwa die Weboberfläche des Altgeräts oder seinen SSH-Server zugänglich zu machen. Dazu muss der Raspi an ihn gerichtete Netzwerkanfragen als Stellvertreter an bestimmte Ports des Altgeräts weiterleiten. Solche Regeln für Webzurufe und SSH könnten wie folgt aussehen:

```
iptables -I PREROUTING -t nat -p tcp \
--dport 80 -j DNAT \
--to-destination 192.168.64.50
iptables -I PREROUTING -t nat -p tcp \
--dport 23 -j DNAT \
--to-destination 192.168.64.50:22
```

Beachten Sie den subtilen Unterschied der Regeln: Die erste reicht Zugriffe auf Port 80 des Raspi direkt an das Altgerät auf Port 80 durch. Die zweite empfängt SSH-Verbindungen auf Port 23 und leitet sie dann auf Port 22 aus – so muss man den SSH-Server auf dem Raspi nicht auf einen anderen Port zwingen.

Probieren Sie die Regeln aus, so solche für Ihr Altgerät überhaupt nötig sind, und speichern Sie diese bei Bedarf mit

```
netfilter-persistent save
```

## Extra-Tipps

Die Beispiele verwenden nur IPv4. Das ist für lebensverlängernde Maßnahmen zugunsten eines Altgeräts vertretbar, auch weil die Autokonfiguration von IPv6 gern mal querfunkt beziehungsweise eigene Regeln für die Firewall benötigen würde. Deswegen sollten Sie für den

The screenshot shows the 'Netzwerk' (Network) tab selected in the top navigation bar. Under 'NETZWERK', there are several collapsed sections: 'Allgemein', 'Verkabelt (802.3)', 'Wireless (802.11)', 'HP Wireless direkt', 'AirPrint™', and 'Erweiterte Einstellungen'. The 'Verkabelt (802.3)' section is expanded, showing the 'Status' sub-section. It lists network interface details: Netzwerkschnittstelle (Aktiviert), Host-Name (HPD341B3), Verbindungsstatus (Verbunden), Verbindungsstatus (AUTO), Hardware (MAC)-Adresse (A0D3C1), and an IPv4 table. The table includes fields for Domain-Name, Konfiguriert von (DHCP), IP-Adresse (192.168.64.50), Teilnetzmaske (255.255.255.0), Standard-Gateway (192.168.64.1), DNSv4, Konfiguriert von (DHCP), Bevorzugte DNS-Adresse (192.168.64.1), Alternative DNS-Adresse, and WINS.

**Wenn Sie das Altgerät hinter dem Raspi verstecken, müssen Sie auch seine Netzwerkkonfiguration anfassen. Der Vorteil: Der SMBv1-Server ist nur in einem privaten Netzwerk sichtbar, das Raspi und das Altgerät teilen.**

dauerhaften Betrieb dieses Brücken-Raspi IPv6 entweder ganz verbieten, indem Sie die Datei /etc/sysctl.d/96-noipv6.conf anlegen und dort Folgendes hineinschreiben:

```
net.ipv6.conf.all.disable_ipv6=1
```

Wenn Sie auf dem Interface im Produktionsnetz IPv6 brauchen, können Sie die Einschränkung auch milder auslegen und auf die „private“ Schnittstelle begrenzen:

```
net.ipv6.conf.eth0.disable_ipv6=1
```

Diese Änderungen wirken, sobald Sie den Raspi neu gestartet haben.

Wenn Sie etwa mit einem Notebook unter Linux mit smbclient das Altgerät simulieren, um zu überprüfen, ob Ihre SMB-Brücke funktioniert, müssen Sie ein Detail beachten: smbclient liest die standardmäßig installierte Samba-Konfigurationsdatei /etc/samba/smb.conf auf dem Notebook aus. Die lässt aber SMBv1 in der Regel nicht zu.

Sie sollten deshalb smbclient beim Aufruf die obige smb.conf-Datei oder Ihre Variante davon zur Verfügung stellen. Andernfalls erhalten Sie womöglich Meldungen à la NT\_STATUS\_INVALID\_PARAMETER\_MIX. Angenommen, besagte smb.

conf-Datei liegt im aktuellen Verzeichnis, dann lautet der Testaufruf

```
smbclient //192.168.64.1/reshare \
-s ./smb.conf -m NT1 -U reuser
```

Je nachdem, welche der beiden Konfigurationen Sie testen, müssen Sie die IP-Adresse des SMBv1-Servers auf dem Raspi angeben – der obige Befehl nutzt die aus dem zweiten Konfigurationsbeispiel.

Mit welcher SMB-Version sich Geräte mit einem Samba-Server verbinden, ermittelt der Befehl smbstatus. Die Versionsangabe NT1 entspricht SMBv1. So können Sie sich auf dem Raspi vergewissern, dass Ihre Konfigurationsarbeiten gelungen sind, und schließlich Ihren Produktivserver so konfigurieren, dass er kein SMBv1 mehr anbietet muss. Der Aufwand lohnt sich, weil Sie Ihr Netzwerk damit gegen lästige Schädlinge immunisieren.

(ps@ct.de) ct

## Literatur

- [1] Ronald Eikenberg, Raspi-Schnellstart, Raspberry Pi superschnell einrichten durch Vorkonfiguration, c't 11/2021, S. 132

**GitHub-Gist zum Kopieren der Befehlszeilen: [ct.de/ytej](https://ct.de/ytej)**

# Audio-Aufrüster

## Raspi als Client für Spotify und AirPlay einrichten



**Ein Raspi Zero reicht aus, um unsmarten AV-Receivern oder analogen Verstärkern Musikstreaming-Fähigkeiten zu verleihen. Mit Raspotify und Shairport Sync klappt das mit wenig Aufwand.**

Von Dennis Schirrmacher

Wenn der AV-Receiver (AVR) seinen Dienst noch zuverlässig verrichtet, aber kein Audio-streaming beherrscht, müssen Sie das Gerät nicht gleich durch ein aktuelles ersetzen. Sogar die Leistung eines Raspberry Pi Zero W (ca. 15 Euro) reicht aus, um einen AVR oder Stereoverstärker aufzurüsten und Musik via WLAN zu streamen.

### Vorbereitungen

Als Basis genügt das schlanke Betriebssystem Pi OS Lite. Damit Smartphones den Raspi als Spotify-Connect-Client im Netzwerk erkennen, gibt es die Open-Source-Software Raspotify. Dafür ist ein Spotify-Premium-Account nötig. Raspotify installieren Sie mit

```
curl -sL https://dtcooper.github.io/raspotify/install.sh | sh
```

Das Skript installiert nicht nur Raspotify, sondern fügt auch das Repository des Entwicklers hinzu. Das hat den Vorteil, dass die Paketverwaltung neben dem Betriebssystem auch den Spotify-Client aktualisiert. In der Spotify-App taucht der Raspi sofort nach der Installation als „raspotify (raspberrypi)“ auf und lässt sich als Ziel für die Wiedergabe auswählen.

Damit der Raspi als AirPlay-Client „Raspberrypi“ im Netzwerk erscheint, müssen Sie Shairport Sync installieren. Das ist etwas aufwendiger, da dafür benötigte Pakete in Pi OS veraltet sind. Auf

GitHub erklärt der Entwickler verständlich, wie das Übersetzen und die Installation Schritt für Schritt ablaufen (siehe [ct.de/yd1x](https://ct.de/yd1x)).

### Klang-Tuning

Um die Soundqualität für Spotify zu optimieren, müssen Sie die Konfigurationsdatei `/etc/default/raspotify` bearbeiten. Die folgenden Zeilen aktivieren Sie, indem Sie das Doppelkreuz-Zeichen am Zeilenanfang löschen. Ändern Sie in der Zeile `BITRATE` den Wert von `160` auf `320`. Erst dann streamt Spotify Musik in der bestmöglichen Qualität mit einer Bitrate von `320 kbit/s`.

Standardmäßig spielt Raspotify alle Songs mit einer gleichbleibenden Lautstärke ab (Normalisation). So muss man nicht ständig zum Lautstärkeregler greifen. Leider beeinflusst das die vom Künstler beabsichtigte Dynamik eines Songs negativ. Um das abzuschalten, müssen Sie in der Zeile `VOLUME_ARGS=`, die Option `enable-volume-normalisation` entfernen. Außerdem empfiehlt es sich, in der gleichen Zeile die digitale Lautstärkeregelung zu deaktivieren, indem Sie `volume-ctrl linear` durch `fixed` ersetzen. Das hat zwar den Nachteil, dass man die Lautstärke nur noch am AVR und nicht mehr am Smartphone regeln kann, dafür kommt das Musiksignal mit vollem Dynamikumfang am AVR an. Das sollte man unter `/etc/shairport-sync.conf` mit der Option `ignore-volume-control="yes"` auch für AirPlay machen. Dafür muss man in der Zeile nur die Zeichen `//` am Anfang entfernen.

Dank bei beiden Clients standardmäßig aktivem Gapless Play laufen Live-Alben ohne Unterbrechung zwischen Songs. Um den Namen des Spotify-Clients anzupassen, tippen Sie die gewünschte Bezeichnung hinter `DEVICE_NAME=` ein. Bei AirPlay geht das bei `name=`.

### Richtig anschließen

Um das Audiosignal vom Raspi Zero und 1 bis 4 digital an einen AVR zu leiten, benötigen Sie lediglich ein HDMI-Kabel. Steht im Wohnzimmer noch ein analoger Stereo-Ver-

stärker, kommt das Audiosignal beim Raspi 1 bis 4 nach einer Digital-Analog-Konvertierung (DAC) via 3,5-mm-Klinke aus dem Kleinstcomputer in den Verstärker. Die Audioqualität des Ausgangs ist aber nicht sehr gut und anspruchsvolle Ohren sollten einen externen DAC einsetzen. Da der Raspi Zero keinen analogen Audioausgang hat, ist ein DAC obligatorisch.

Das Aufrüsten gelingt kostengünstig für rund 15 Euro mit dem HifiBerry DAC+, den man via 40-Pin-GPIO-Anschluss mit einem Raspi verbindet. Wer noch hochwertigeren Sound möchte, muss mehr Geld ausgeben. Wir haben das mit dem Qudelix 5K (120 Euro) und dem RME ADI-2 DAC FS (960 Euro) ausprobiert.

Da viele DACs USB Class Compliant sind, erkennen Raspis sie ohne Treiberinstallation. Damit die Wiedergabe klappt, schließen Sie den DAC via USB als externe Soundkarte an und ändern unter `/usr/share/alsa/alsa.conf` das Ausgabegerät. Passen Sie dafür die Einträge wie folgt an: `defaults.ctl.card 1, defaults.pcm.card 1` Falls die Lautsprecher stumm bleiben, ziehen Sie das HDMI-Kabel ab und probieren Sie es noch mal.

Mit dem Qudelix 5K klappte die Wiedergabe problemlos. Beim RME ADI-2 DAC FS störten mit einem Raspi Zero Knackser den Hörgenuss. Raspis können diesen DAC nur mit 32 Bit ansprechen. Das überfordert den Zero offensichtlich. Auch eine selbst kompilierte Raspotify-Version mit verbesserter 32-Bit-Kompatibilität konnte das Problem nicht lösen.

### Fazit

Fernab von dieser speziellen Problematik liefen der Spotify- und AirPlay-Client auf einem Raspberry Pi Zero W in unserem Test über mehrere Wochen absolut stabil. Die Musikübertragung via WLAN gelang stets ohne Aussetzer. Es muss also nicht immer gleich ein neuer AVR sein, wenn man smarte Funktionen vermisst. (des@ct.de) **ct**

**Installationsanleitung AirPlay:** [ct.de/yd1x](https://ct.de/yd1x)

# Mehr Zugang. Mehr Chancen.

Cisco hat sich verpflichtet, bis 2025 insgesamt 1 Milliarde Menschen positiv zu beeinflussen. Wir setzen uns ein für eine Welt, in der alle Zugang zu Information und Bildung haben. Um voranzugehen. Um mutig zu sein. Um teilzuhaben.

Das ist die inklusive Zukunft. Wenn alle und alles miteinander verbunden sind, ist alles möglich.

[cisco.de/bridgetopossible](https://cisco.de/bridgetopossible)



The bridge to possible

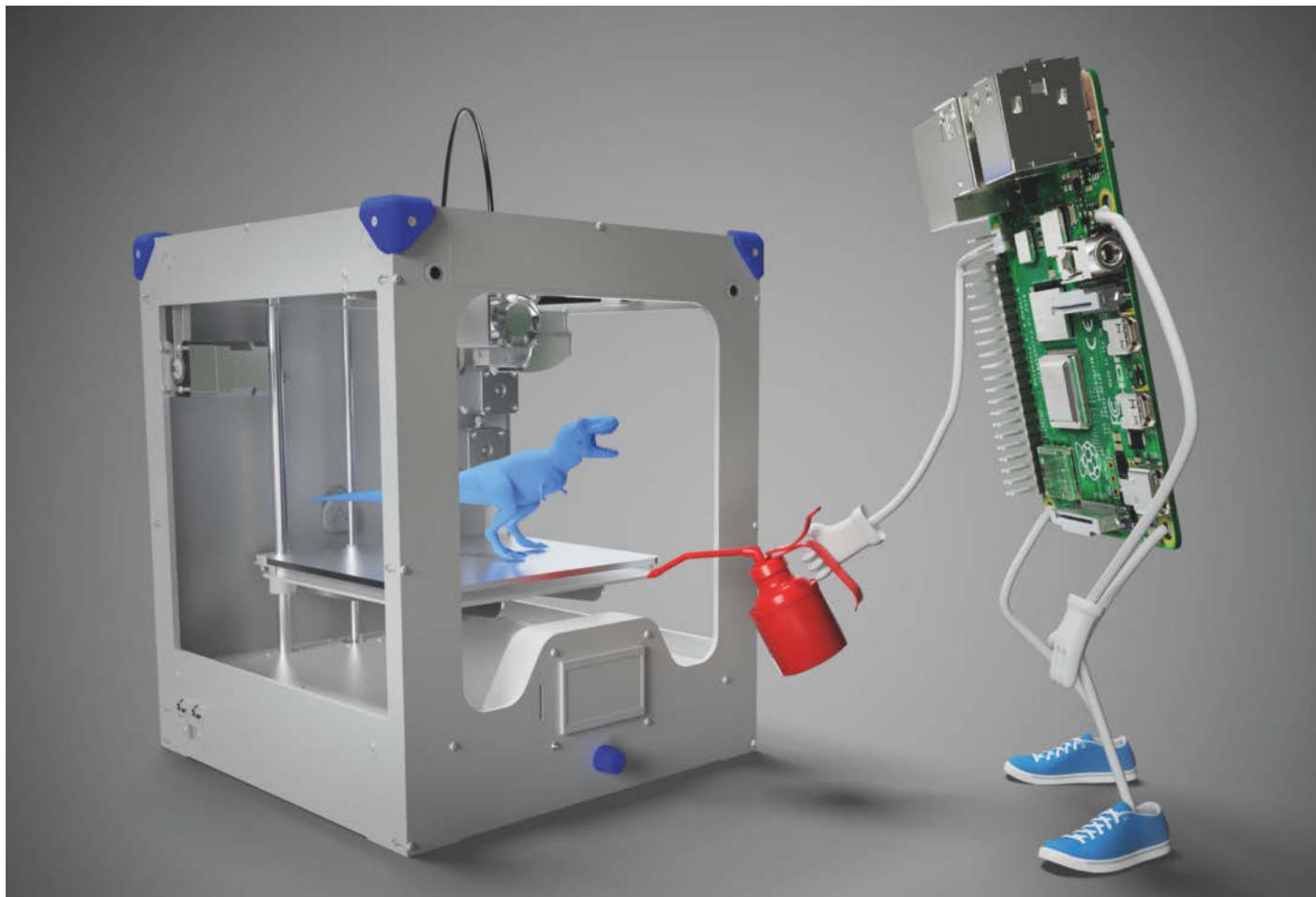


Bild: Andreas Martini

# 3D-Druckserver

## 3D-Drucker ins Netzwerk bringen mit Raspi und Octoprint

**3D-Drucker machen über viele Stunden Lärm, weshalb man sie meist in eine entlegene Ecke der Wohnung verbannt. Damit man da nicht für jede Temperaturanpassung hinlaufen muss, gehört der Drucker ins Heimnetz. Mit Octopi lässt sich das leicht und günstig nachrüsten.**

Von Pina Merkert

man für jede Einstellung zum Drucker laufen, der aus Lärmschutzgründen im Keller oder in einem Abstellraum steht, fallen viele Wege an. Möchte man den Druck zudem im Auge behalten, beispielsweise weil man mit einer neuen Filamentsorte experimentiert und Zweifel hat, ob die Betthaftung ausreicht, fallen noch viel mehr Wege an und jeder zusätzliche Meter nervt.

Abhilfe schafft da ein Raspberry Pi (gern auch ein älteres Modell) mit Octoprint, einer browserbasierten 3D-Drucker-Oberfläche, die den Drucker von überall im Heimnetz steuerbar macht. Weil die Kombination so naheliegend ist, gibt es sogar eine Raspi-Distribution namens „Octopi“. Drucker-Mainboard per USB-Kabel mit Raspi verbinden – und los geht's.

Eine Steuerung über USB unterstützen nahezu alle jemals verkauften 3D-Drucker.

Octoprint erlaubt, Bett und Düse vorzuheizen, stellt die aktuelle Temperatur als attraktives Diagramm dar, bietet Tasten, um den Drucker manuell zu bewegen und erlaubt G-Code hochzuladen und Drucke zu starten. Wer neu kalibrieren muss, freut sich über eine integrierte Konsole, ein gut bestücktes Plug-in-System rüstet diverse Spezialfunktionen nach. Besonders attraktiv ist das Plug-in „Octolapse“, das mit einer Raspi-Kamera schicke Zeitraffer-Videos vom Verlauf der Drucke aufzeichnet. Mit diesem Artikel gelingt Ihnen die Einrichtung in wenigen kurzen Minuten.

### Installation

Octopi laden Sie als gezippte IMG-Datei von octoprint.org herunter (siehe ct.de/ypwc). Auf der Webseite finden Sie auch eine Anleitung, um Octoprint auf anderer Hardware wie einem Heimserver zu installieren. Für den Raspi ist die Installation aber am einfachsten: Archiv auspacken, Raspi-Imager öffnen, „Betriebssystem/eigenes Image“ auswählen, IMG-Datei im Downloads-Ordner auswählen und die SD-Karte beschreiben. Octopi basiert auf dem offiziellen Raspberry Pi OS, weshalb

**B**eim 3D-Druck gibt es immer wieder Wartezeiten, beispielsweise, um das Druckbett vorzuheizen. Muss

The screenshot shows the 'Setup Wizard' step 'Konfiguriere dein Druckerprofil'. It includes fields for 'Formfaktor' (Rectangular selected), 'Ursprung' (Left selected), 'Heizbett' (Heated Bed checked), 'Beheizte Kammer' (Heated chamber unchecked), and build volume dimensions (Width X: 250 mm, Depth Y: 210 mm, Height Z: 210 mm). A note states: 'Wenn der Druckkopf des Druckers sich außerhalb des Druckvolumens bewegen darf (z.B. für Nozzlerereigungslinien) kannst du hier eine als gefahrlos geltende Bounding Box für seine Bewegung definieren.' Below this is a section for 'Individuelle Bounding Box' which is unchecked. At the bottom, it says: 'Diese Informationen werden für das Temperaturab, den Bounding-Box-Check, den GCODE-Viewer und/oder beim Slicen aus OctoPrint heraus verwendet.' A 'Zurück' (Back) button is on the left, and a 'Weiter' (Next) button is on the right.

die mit dem Raspi-Imager einstellbaren Voreinstellungen funktionieren. Das Menü mit den Voreinstellungen öffnet sich mit der Tastenkombination Strg+Um-schalt+X (wie das funktioniert haben wir in [1] beschrieben).

Statt des Raspi-Imagers können Sie auch Balena Etcher oder den „Schreiber von Laufwerksabbildern“ beziehungsweise das „Festplattendienstprogramm“ benutzen. Dann müssen Sie die Einstellungen fürs WLAN aber nach dem ersten Start mit angeschlossenem Display und Tastatur nachholen oder in die Datei `octopi-wpa-supplicant.txt` im Verzeichnis `/boot` eintragen.

Die SD-Karte stecken Sie anschlie-ßend in den Raspi und verbinden auch gleich den Drucker mit dem Minirechner. Meist ist beim Drucker beziehungsweise dessen Mainboard ein Kabel mit USB-A und USB-B dabei. Manche Drucker kön-nen Sie auch mit einem alten Handy-Lade-kabel (USB-A- und Micro-USB-Stecker) mit dem Raspi verbinden.

## Drucker verbinden

Nach dem ersten Start sollte sich der Raspi in Ihrem Heimnetz melden und vom Router eine IP bekommen. Diese können Sie im Webinterface vom Router nachsehen. Statt der IP funktioniert meist auch der Hostname, den Sie in den Raspi-Vorein-stellungen vergeben haben. Wir haben für den Artikel einen Prusa i3 netzwerkfähig gemacht, weshalb wir als Hostname „prusa13“ eingestellt haben. Unser Router ließ sich für die Namensauflösung einspannen,

**Ein Einrichtungsassis-tent hilft beim ersten Start, die wichtigsten Einstellungen vorzu-nehmen. Das „Drucker-profil“ enthält bei-spielsweise Angaben zur Größe des Druck-betts.**

Raspi (der hat ja neben Octoprint noch Kapazitäten für andere Aufgaben frei) wechselt die Nummerierung der Devices je nachdem, welches vom Kernel beim Boot zuerst erkannt wird. Sollte Sie das stören, können Sie wie in [2] beschrieben eine UDEV-Regel für den Drucker erstellen. Eigene Namen für Devices müssen Sie in den Einstellungen im Bereich „Drucker“ auf der Seite „Serielle Verbindung“ im Textfeld „Zusätzliche serielle Ports“ hinzufügen.

Die Baudrate, mit der Ihr Drucker kommunizieren möchte, sollte in der Beschreibung zum Gerät benannt werden. Falls Sie dort keine Angabe finden, probieren Sie einfach mal 115200 aus. Das ist die Voreinstellung in der Konfiguration der Marlin-Firmware und auf der basieren die meisten Firmwares günstiger Drucker.

Das Druckerprofil ist normalerweise schon vorausgewählt, weshalb Sie anschließend nur noch den Haken bei „Verbindungseinstellungen speichern“ setzen wollen und anschließend auf den großen „Verbinden“-Knopf drücken. Nach ein

weshalb der Raspi nach wenigen Sekun-den unter <http://prusa13> erreichbar war. Klappt die Namensauflösung nicht, nutzen Sie die IP-Adresse aus der Heimnetz-Über-sicht im Router-Interface, beispielsweise <http://192.168.178.68>.

Beim ersten Aufruf begrüßt Sie ein Assistent, der diverse Fragen zum Druckernamen et cetera stellt. Die Erklärtex-te sind automatisch auf Deutsch, wenn der Browser in deutscher Sprache installiert ist. Da Gina Häußge, die Hauptentwickle-rin von Octoprint, Deutsche ist, gibt es keine Übersetzungsfehler und die Be-schreibungen sind gut verständlich.

Im Einrichtungsassistent legen Sie auch ein Profil für Ihren Drucker an, in dem Sie den Namen und die Größe des Druckraums festlegen. Octoprint nutzt diese Angaben beispielsweise für eine Prü-fung, ob geladener G-Code überhaupt in den Druckraum passt. Alle Angaben kön-nen sie später selbstverständlich in den Einstellungen anpassen. Die Verbindung zum Drucker nehmen Sie erst auf, nachdem Sie den Assistenten fertig durchge-klickt haben.

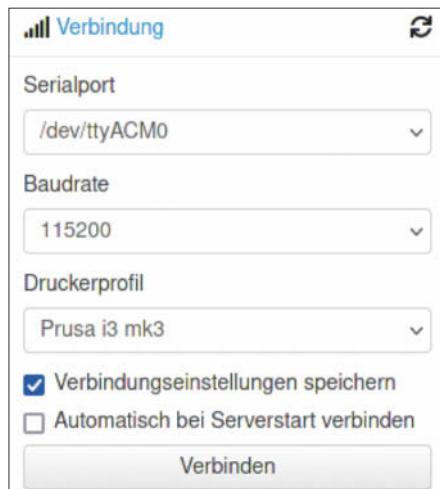
Dann nämlich erscheint in der linken oberen Ecke der Weboberfläche ein Kas-ten mit Verbindungseinstellungen. Die bestehen aus Drop-down-Menüs für den Port, die Baudrate und das im Assistenten erstellte Druckprofil. Der Name des Ports ist der Pfad zum seriellen Interface in üblicher Linux-Benennung. Zur Auswahl steht üblicherweise `/dev/ttyUSB0` oder `/dev/ttyACM0` wie bei unserem Prusa. Stecken noch mehr serielle USB-Geräte am



**Der kleine Raspi ist unter dem 3D-Dru-cker-Gehäuse versteckt. Seine Kamera hängt als kleines Rechteck an der Vor-derkante der Seitenscheibe.**

paar Sekunden wechselt dessen Beschriftung auf „Trennen“ und im Temperatur-Reiter füllt sich das Diagramm mit Messwerten der Temperaturfühler von Heizbett und Hotend.

„Automatisch bei Serverstart verbinden“ sollten sie nur auswählen, wenn Sie immer nur mit Octoprint drucken und nie von SD-Karte und außerdem Drucker und Raspi stets gemeinsam einschalten. Dann spart das Häkchen dort einen Knopfdruck. Für mehr Übersicht in der linken Leiste können Sie den Kasten mit den Verbindungseinstellungen mit einem Klick auf die Überschrift einklappen.



**Steuern kann Octoprint den 3D-Drucker erst, wenn die Serielle Verbindung über das USB-Kabel klappt. Für Port und Baudrate schlägt Octoprint die üblichen Werte vor und speichert sie auch für später.**

Zur Kontrolle während des Drucks dient der Reiter „GCode Viewer“. Darin zeigt Octoprint grafisch an, wie die per G-Code versendeten Bewegungsbahnen aussehen. Zuerst erscheinen sie im Browserfenster, gleich darauf sollte der Drucker die Bewegung in der echten Welt genau nachmachen. Da sich hier immer etwas bewegt, ist das der Reiter mit dem größten Unterhaltungswert.

Den Reiter „Zeitraffer“ brauchen Sie nur, wenn eine Kamera angeschlossen ist. Octoprint kann von Haus aus Zeitrafferauf-

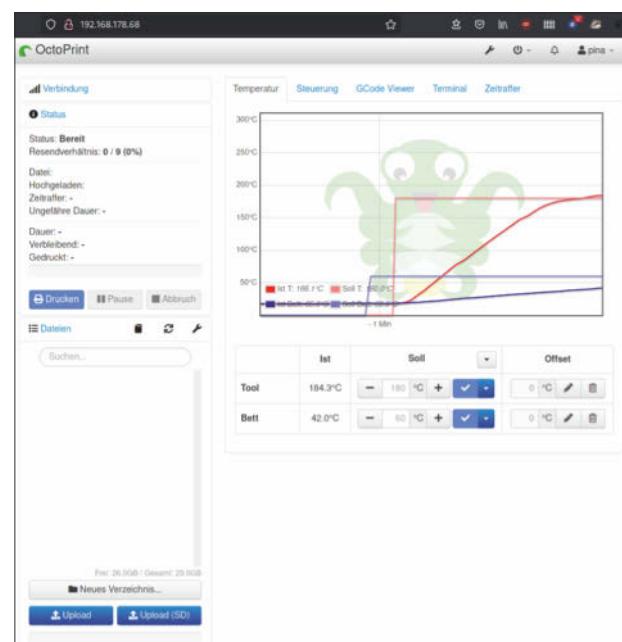
nahmen von den Drucken machen. Wie gut die mit den Bordmitteln von Octoprint aussehen, hängt mit dem Konstruktionsprinzip Ihres Druckers zusammen. Drucker nach dem Ultimaker-Prinzip [3] oder Core-XY fahren die Plattform nach unten weg und bewegen sie nicht in X- oder Y-Richtung. Bei solchen Druckern entstehen direkt hübsche Zeitraffer-Videos. RepRap-artige Maschinen wie der i3 oder Ender 3 bewegen aber das Bett in Y-Richtung, weshalb Zeitraffer-Videos zittrig werden. Für schöne Zeitraffer-Aufnahmen brauchen Sie bei solchen Maschinen ein Plug-in, das Fotozeitpunkt und Bettposition synchronisiert.

## Octolapse

Octolapse durchforstet den G-Code nach geeigneten Stellen, um ein Einzelbild für eine Zeitrafferaufnahme aufzunehmen. Wenn der Druckkopf und vor allem das Druckbett nämlich bei jeder Zeitrafferaufnahme an den gleichen X- und Y-Koordinaten stünden, sähe es im Video so aus, als würde der Druckkopf ohne zittern nach oben wegfahren, während magisch unter ihm ein Plastikteil entsteht.

Octolapse sucht dafür nicht nur die ideale Stelle im G-Code, sondern fügt auch bewusst zusätzliche Bewegungen ein, falls der Druckkopf nicht ohnehin an der gewünschten Fotoposition vorbeikommt. Wo Kopf und Bett stehen, wenn Octolapse knipst, lässt sich in einer Registerkarte einstellen, die rechts neben der Zeitraffer-Karte erscheint, sobald man das Plug-in installiert hat.

**Octoprint zeigt im Browserfenster links Statistiken zum laufenden Druck und darunter die bereit gelegten G-Code-Dateien. Rechts davon zeigen mehrere Reiter die Temperaturen von Düse und Bett, erlauben manuelle Steuerbefehle und zeigen Bilder von einer Webcam, falls angeschlossen.**



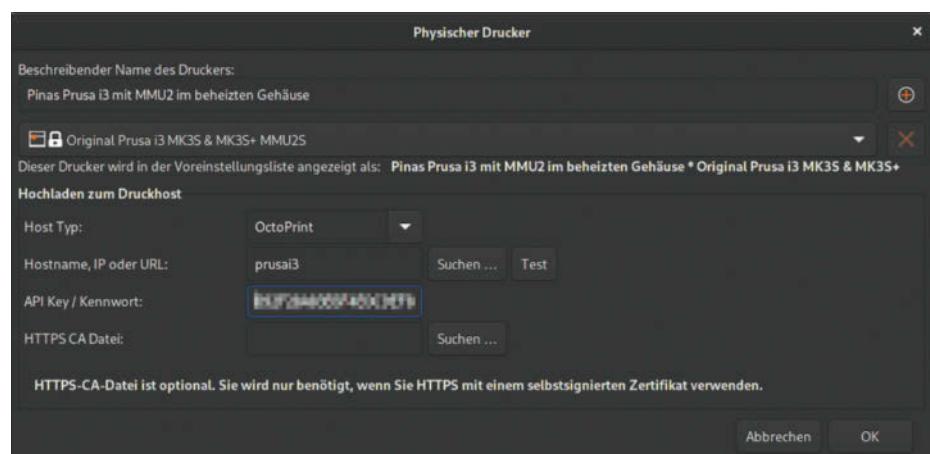
Erfordert die Fotoposition bei jedem Schichtwechsel zusätzliche Bewegungen, dauert der Druck ein wenig länger und die Schichten haben jeweils eine Sekunde oder zwei mehr Zeit, sich abzukühlen. Für PLA spielt das meist keine große Rolle, bei heißer verarbeiteten Kunststoffen kann die Pause aber die Druckqualität beeinflussen (manchmal auch zum Besseren).

In den Einstellungen können Sie auch die Videoqualität und die Bildfrequenz einstellen. HEVC funktioniert auf dem Raspi leider nicht, da er dafür keinen Hardware-Encoder hat. Die Videodateien sind zwar auch mit H.264 angenehm klein, zeigen aber sichtbare Kompressionsartefakte.

## Plug-ins

Neben Octolapse gibt es Dutzende weitere Plug-ins, mit denen Sie Octoprint an Ihre Bedürfnisse anpassen können. Beispielsweise können Sie mit dem Firmware-Updater die Software auf dem Drucker-Mainboard austauschen, ohne das USB-Kabel umstecken zu müssen. Die Plug-ins installieren Sie über den „Pluginmanager“ unter der Überschrift „Octoprint“ in den Einstellungen. Nach der Installation bringen viele Plug-ins eine Konfigurationsseite mit, die in den Einstellungen unter der Überschrift „Plugins“ auftaucht.

Wir haben für unseren Prusa i3 neben dem „Firmware Updater“ noch „Octolapse“ und den „Print Time Genius“ installiert. Letzterer nutzt statt Octoprints eigener Schätzung die Restzeit-Angaben, die der Prusa Slicer im G-Code hinterlassen kann.



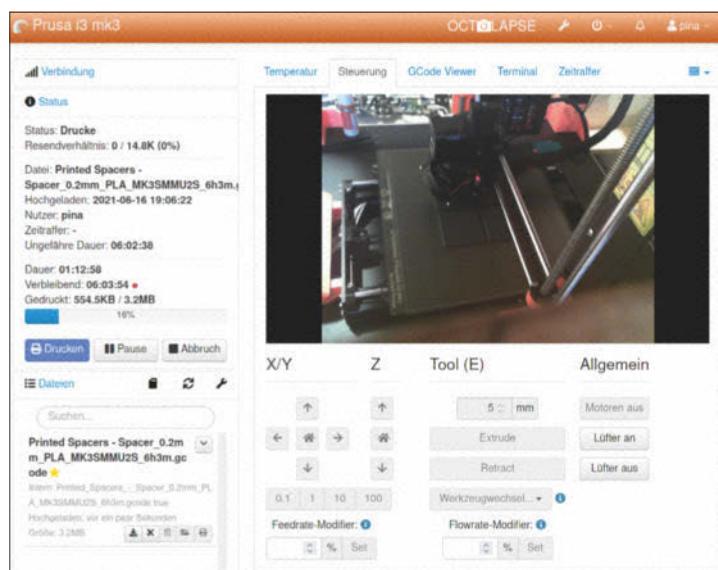
**Prusa Slicer kann die Octoprint-API benutzen, um G-Code direkt in den Druckserver zu laden.**

Damit das klappt, müssen Sie in den Plugin-Einstellungen den Haken bei „Use Slic3r PE M73 time remaining“ setzen und im Prusa Slicer unter „Druckereinstellungen/Allgemein“ im Kasten „Firmware“ den Haken bei „Unterstützt Restzeit“ setzen.

Prusa Slicer kann auch das Octoprint-API benutzen, um Druckaufträge mit einem Knopfdruck an den Drucker zu versenden. Erzeugen Sie dafür zunächst in den Octoprint-Einstellungen unter der Überschrift „Funktionen“ bei „Application Keys“ einen API-Key für den Prusa Slicer. Kopieren Sie die kryptische Zeichenfolge in die Zwischenablage und wechseln Sie in den Slicer. Gehen Sie dort in die Druckereinstellungen und klicken oben in der Leiste auf das Zahnrad-Symbol. Es öffnet sich der Einstellungsdialog zum „Physischen Drucker“.

„wo Sie zunächst einen neuen Namen für Ihren real existierenden 3D-Drucker vergeben müssen. Als „Host Typ“ wählen Sie dann OctoPrint, als Hostnamen den Namen beziehungsweise die IP-Adresse des Druckers im Heimnetz (Angabe ohne „http://“) und im Feld „API Key“ fügen Sie die Zeichenkette aus der Zwischenablage ein. Die „HTTPS CA Datei“ darf leer bleiben, wenn beide Geräte im gleichen Netz stehen. Danach erscheint nach dem Slicen unten rechts ein Knopf, der den G-Code direkt zum Drucker schickt.

Dank solcher Kleinigkeiten kann Octoprint die Arbeit mit dem 3D-Drucker erleichtern und beschleunigen: Wir konnten dank Octoprint mehr als die Hälfte der Laufwege zum Drucker einsparen. Voraussetzung ist allerdings ein 3D-Drucker, der bereits von der SD-Karte ordentliche Drucke abgeliefert hat. Als Bonus macht Octoprint tolle Zeitrafferaufnahmen, mit denen wir ab sofort den Freunde- und Bekanntenkreis per Videonachricht im Messenger beeindrucken. Beispiele finden Sie über ct.de/ypwc. Nur Katzenbesitzer mit Laserpointern kriegen noch mehr Klicks. (pmk@ct.de) ct



**Eine Kamera am Raspi ermöglicht es, den Drucker bei der Arbeit zu überwachen. Neben der Raspi-Kamera funktionieren auch USB-Webcams. Die gleiche Kamera schießt auch die Bilder für Zeitraffer-Videos.**

## Literatur

- [1] Ronald Eikenberg, Raspi-Schnellstart, Raspberry Pi superschnell einrichten durch Vorkonfiguration, c't 11/2021, S. 132
- [2] Pina Merkert, Funkbrücke für Thermostate, Homegear bindet MAX! und HomeMatic-BiCoS zeitgemäß ins Smart Home ein, c't 19/2020, S. 160
- [3] Pina Merkert, Ultimaker gegen seine Klone, 3D-Drucker nach dem Ultimaker-Prinzip schon ab 350 Euro, c't 1/2019, S. 130

**Downloadlinks und Dokumentation: ct.de/ypwc**

# Wolke mit Fenster

## Windows 365: Microsoft vermietet VMs in der Cloud

**Unter dem Namen Windows 365 bekommen Firmenadmins virtuelle Maschinen mit Windows. Anders als die Azure-Desktops für Großkunden lassen sie sich leichter einrichten und sind verständlicher bepreist.**

Von Jan Schüßler

**M**icrosoft hat Windows 365 vorge stellt: Cloud-gehostete virtuelle Maschinen mit Windows 10, die Geschäftskunden ab dem 2. August mieten und über den Microsoft Endpoint Manager verwalten können. Die Bedienung des Systems funktioniert über den Webbrowser.

Der ähnliche Name verleitet dazu, Windows 365 als das Betriebssystem-Pendant zum Office-Mietprodukt Microsoft 365 (ehemals Office 365) zu sehen, doch das trifft es nicht ganz. Erstens ist die Office-Suite auch für Privatkunden zu haben – das ist bei Windows 365 ausgeschlossen. Und zweitens sind die Office-Anwendun-

gen bei vielen Microsoft-365-Abos nicht nur im Webbrowser nutzbar, sondern auch per lokal installierter Software. Windows 365 ist stets eine in Microsofts Azure-Cloud gehostete virtuelle Maschine, die der Nutzer per Browser bedient.

### Nicht ganz neu

Azure-Kunden fällt vielleicht auf, dass ein in der Cloud gehostetes virtuelles Windows so neu nicht ist. Unter dem Namen Azure Virtual Desktop (vormals Windows Virtual Desktop) bietet Microsoft einen ähnlichen Dienst schon seit rund zwei Jahren an. Der Unterschied: Bisher war der Administrationsaufwand höher und das Produkt nur sinnvoll für große Unternehmen implementierbar, in denen sich Admins eigens um die virtuellen Desktops kümmern. Ähnliches gilt für selbst gehostete Windows-VMs, auf die die Mitarbeiter per Remotedesktop-App oder -Webclient zugreifen können.

Mit Windows 365 hingegen zielt Microsoft auch auf kleinere Unternehmen, die möglichst wenig Aufwand in die Administration stecken wollen; alle Voraussetzungen an Lizenzen und Infrastruktur und die Integration ins Active Directory

erklärt Microsoft in einem Beitrag im Windows IT Pro Blog (siehe [ct.de/y751](https://ct.de/y751)). Admins klicken eine Konfiguration aus RAM, CPU-Kernen und Festplattenspeicher zusammen. Dabei sind 1 bis 8 CPU-Kerne möglich, 2 bis 32 GByte RAM und 64 bis 512 GByte Laufwerksspeicher. Microsoft-Partner bieten weitere Vereinfachungen an: Noch am Tag der Windows-365-Ankündigung stellte das Unternehmen ServiceNow eine Möglichkeit vor, mit der man virtuelle PCs per Textnachricht über Microsoft Teams bestellen kann.

Admins sehen bei der Konfiguration einen monatlichen Abopreis für den fertigen virtuellen PC. Auch da sind die Azure Virtual Desktops komplizierter: Zu User- oder Client-Access-Lizenzen (CALs) kommen Kosten für Speicherplatz, Betriebssystem und Profile sowie die Buchung der Azure-Infrastruktur, bei der mitunter auch CPU-Zeit und Netzwerkbандbreite separat abgerechnet werden.

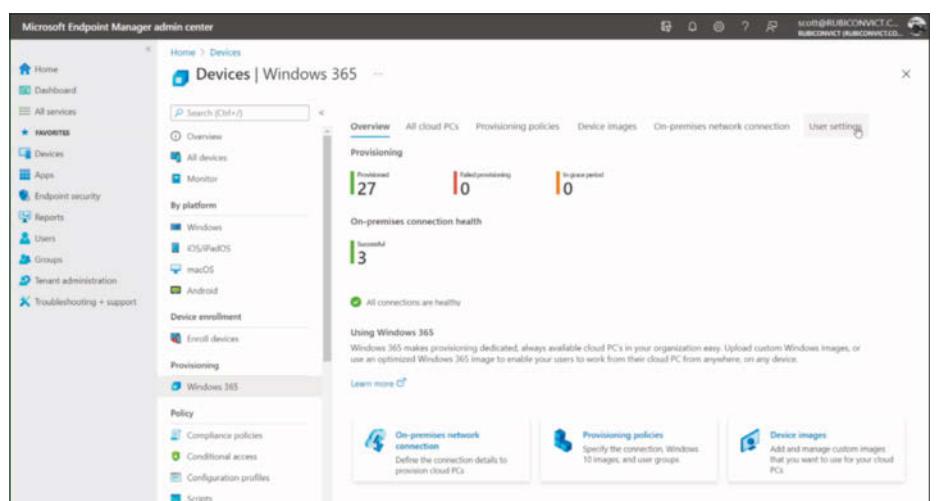
Apropos Preise: In einer Präsentation bei der Partnerkonferenz Inspire zeigte Microsoft ein Preisbeispiel von 31 US-Dollar pro Monat und Person für eine Windows-VM mit 2 CPU-Kernen, 4 GByte RAM und 128 GByte Platten Speicher. Umgerechnet sind das rund 315 Euro im Jahr. Wenngleich es sich nicht um einen offiziellen Preis handelt, wird schnell klar, dass Microsoft hier nicht auf Endkunden zielt. Drei Jahre kämen im Preisbeispiel auf 945 Euro – dafür bekommt man bereits ein ordentliches Notebook inklusive Windows-Lizenz.

### Fazit

Wenn gleich Microsoft mit Windows 365 das Rad nicht neu erfindet, schließt das neue Produkt eine Lücke im Sortiment, die bislang zwischen kompletten Windows-Endgeräten für kleinere Unternehmen einerseits und der Großkundenlösung Azure Virtual Desktop andererseits besteht. Das zu tun, ist aus Sicht des Konzerns naheliegend.

Für welche Einsatzzwecke Windows 365 tatsächlich taugt, wird sich allerdings erst ab dem 2. August zeigen, wenn man es buchen kann und alle Details zu den Preisen bekannt werden. Offen ist auch, ob noch Konfigurationsoptionen für leistungsstarke Grafikkarten hinzukommen – daran hängt, ob sich Windows-365-Maschinen nur als Office-Systeme oder auch etwa als virtuelle Grafikworkstations eignen.

(jss@ct.de) 



The screenshot shows the Microsoft Endpoint Manager admin center with the 'Devices' section selected. Under 'Provisioning', it displays statistics: 27 provisioned devices, 0 failed provisioning, and 0 in progress. It also shows 'On-premises connection health' with 3 successful connections. Below this, there's a section titled 'Using Windows 365' with three cards: 'On-premises network connection' (Define the connection details to provision cloud PCs), 'Provisioning policies' (Specify the connection, Windows 10 images, and user groups), and 'Device images' (Add and manage custom images that you want to use for your cloud PCs).

Windows 365 lässt sich über den Microsoft Endpoint Manager einrichten.

Infos zu Windows 365: [ct.de/y751](https://ct.de/y751)

# Windows 11: runde Optik und Teams-Integration

**Die erste Vorabversion von Windows 11 brachte auf einen Schlag viel Neues, doch fertig ist das System noch lange nicht. Inzwischen hat Microsoft ein paar weitere Neuigkeiten eingebaut.**

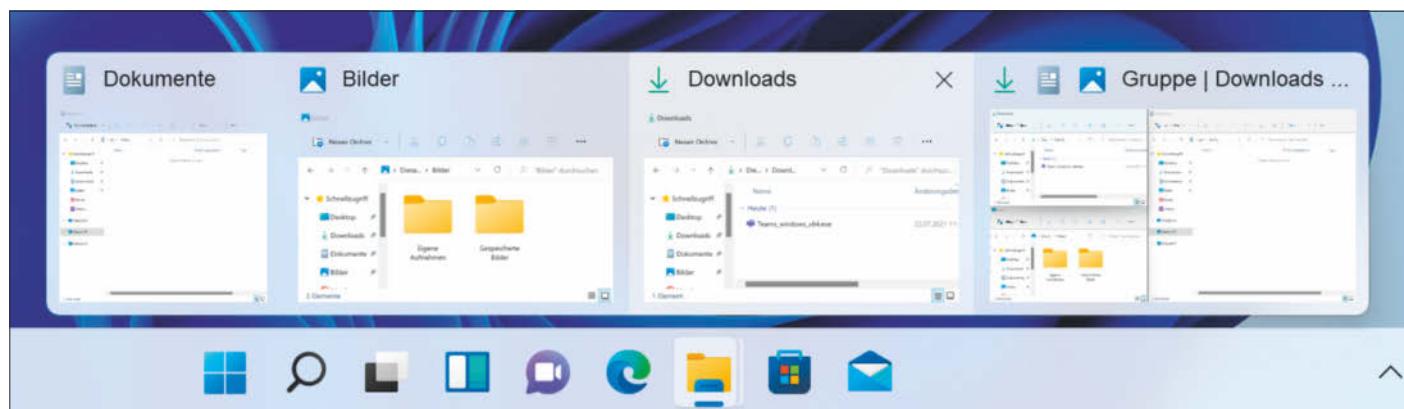
Windows 11 hat ein paar Schritte in Richtung Fertigstellung unternommen. In der aktuellen Insider Preview erscheinen diverse Systemnachrichten und Pop-ups nun im neuen, abgerundeten Design, etwa die Fenstervorschau beim Mouseover auf offene Programme in der Taskleiste. Hinzu

kommt etwas Feinschliff am neu gestalteten Kontextmenü des Datei-Explorers. Das erscheint nun im Milchglas-Look und man kann ohne Umweg über die Schaltfläche „Weitere Optionen“ den Desktop aktualisieren oder PowerShell-Cmdlets mit der Dateiendung .ps1 per PowerShell ausführen.

Auf Monitoren im Hochformat bietet die Snap Layouts genannte Einrastfunktion für Fenster nun dreizeilige statt dreispaltige Layouts an. So lassen sich drei Fenster im Handumdrehen untereinander anzeigen.

Außerdem ist die groß angekündigte Teams-Integration in die Taskleiste nun enthalten. Bislang ist der Funktionsumfang allerdings noch recht beschränkt: Die enthaltene Teams-App funktionierte in einem ersten Test nur mit privaten, nicht aber mit geschäftlichen Microsoft-Konten; zudem unterstützt sie derzeit noch keine Video-Chats und ist komplett englisch.

Wer am Betatestprogramm Windows Insider teilnimmt und eine Windows-11-Installation im Dev-Channel betreibt, bekommt die Änderungen automatisch in Form kumulativer Updates. (jss@ct.de)



**Windows 11 ist an einigen Stellen etwas runder geworden – etwa die Vorschaubildchen offener Fenster beim Mouseover über der Taskleiste.**

## Windows 10: Version 21H2 angekündigt

All die neuen Funktionen und Änderungen von Windows 11 bedeuten nicht, dass Windows 10 keine Funktionsupdates mehr bekommt – Microsoft hatte bereits bei der Vorstellung von Windows 11 klar gestellt: Mindestens **eine neue Windows-10-Ausgabe** wird noch erscheinen. Diese neue Ausgabe hat der Konzern nun angekündigt. Sie heißt Version 21H2, soll also in der zweiten Jahreshälfte 2021 fertig sein. Ein Datum ist zwar noch nicht bekannt, doch erfahrungsgemäß werden die Herbstausgaben von Windows 10 jeweils im Oktober oder November veröffentlicht.

Wie schon beim vorigen Sprung von Version 20H2 auf 21H1 lassen sich auch diesmal die recht speziellen Neuerungen an einer Hand abzählen. Erstens bringt Version 21H2 Unterstützung für die H2E-Erweiterung des WPA3-Verschlüsse-

lungssstandards für Drahtlosnetzwerke und verbessert so den Schutz vor Seitenkanalangriffen. Zweitens soll die Biometriefunktion „Windows Hello for Business“ eine effizientere passwortlose Einrichtungsmethode erlauben, und drittens sollen GPU-gestützte Berechnungen auch im Windows Subsystem für Linux (WSL) und in Azure IoT Edge für Linux auf Windows nutzbar sein.

Als Herbstausgabe wird 21H2 in den Editionen Enterprise und Education 30 Monate lang mit Updates versorgt; in den übrigen Editionen 18 Monate. Zudem wird Version 21H2 auch die Grundlage einer neuen Enterprise-LTSC-Version sein. Bei LTSC (Long Term Servicing Channel) handelt es sich um Langzeit-support-Versionen, die keine Funktionsupdates bekommen, sondern nur mit Sicherheitsupdates versorgt werden. Bei

den bisherigen Langzeitausgaben waren das zehn Jahre. Für das kommende Windows 10 Enterprise LTSC hat Microsoft die Supportdauer auf fünf Jahre reduziert; zehn Jahre gäbe es nur noch für die IoT-Variante des Systems.

Version 21H2 fußt, wie schon zuvor die 21H1 und 20H2, auf der im Frühling des vergangenen Jahres erschienenen Version 2004. Und auch diesmal gilt: Sofern mindestens Version 2004 auf dem PC läuft, kommen die wenigen Änderungen von 21H2 schon ein, zwei Monate zuvor mit den monatlichen kumulativen Updates auf den Rechner. Sobald Version 21H2 veröffentlicht ist und man es per Windows Update installiert, werden die neuen Funktionen nur noch mit Hilfe eines wenige Kilobyte kleinen „Enablement Package“ freigeschaltet.

(jss@ct.de)

# Drei Volltreffer

## Katastrophenfall nach Ransomware und Trojaner

**Drei Beispiele zeigen, wie gefährlich und unterschätzt Angriffe aus dem Internet sind. Ein Klinikum muss auf Papier und Stift umsteigen, zwei Stadtverwaltungen sind lahmgelegt – eine ruft den ersten Cyber-Katastrophenfall aus.**

Von Wilhelm Drehling

Gleich dreimal in zwei Wochen griffen Hacker große öffentliche Institutionen an: das Klinikum in Wolfenbüttel sowie die Stadtverwaltungen in Anhalt-Bitterfeld und Geisenheim. Das Krankenhaus konnte bereits einen Tag nach Befall seine Türen wieder öffnen. Die beiden Stadtverwaltungen hat es schwerer getroffen, nach mehr als zwei Wochen baut Anhalt-Bitterfeld eine neue Notinfrastruktur auf. Damit schneller Hilfe eintrifft, rief die Landkreisverwaltung den Katastrophenfall aus. Geisenheim dagegen sei sicher für „drei Wochen offline“, im schlimmsten Falle dauert es aber zwei bis drei Monate, um den alten Stand zu erreichen.

### Start der Katastrophe

Zuerst traf es am 6. Juli die Landkreisverwaltung Anhalt-Bitterfeld. Die mutmaßlichen Hacker gelangten anscheinend über eine Sicherheitslücke in das System und verschlüsselten die Daten. Der Landrat gehe davon aus, dass es sich um die Microsoft-Drucker-Lücke PrintNightmare handeln könne [1] – sicher ist das aber noch nicht. Zurzeit untersuchen Forensiker des Landeskriminalamtes die betroffenen Windows-Systeme.

Am 9. Juli rief der Landrat den deutschlandweit ersten Cyber-Katastrophenfall aus. Laut eigenen Angaben gebe das dem Landrat die Möglichkeit, schneller zu entscheiden

und Hilfe anzufordern. Durch den Befall der Ransomware seien ab dem Zeitpunkt etwa keine Zahlungen mehr möglich gewesen.

Zwei Wochen nach dem Befall in Anhalt-Bitterfeld stand ab dem 19. Juli die Notinfrastruktur bereit. Landrat Andy Grabner sagte gegenüber dem ZDF, dass es noch bis zu sechs Monate dauern könne, bis sich der Landkreis komplett erholt hat.

Eine Lösegeldforderung lehnte die Verwaltung von Anhalt-Bitterfeld ab. Laut dem Chaos Computer Club (CCC) veröffentlichten die mutmaßlichen Angreifer als Gegenreaktion in einem bekannten Hackerforum 200 MByte an Daten. Der Landkreis bestätigte in einer Pressemitteilung die Authentizität der Daten. Es handele sich um teilweise nicht-öffentliche Sitzungsprotokolle von Ausschuss- und Kreistagssitzungen.

### Zwei an einem Tag

Noch während Beamte in Sachsen-Anhalt an einer Notinfrastruktur feilten, erwischte es unabhängig voneinander am 14. Juli die Stadtverwaltung Geisenheim und das städtische Klinikum Wolfenbüttel. Im Krankenhaus hatte eine Schadsoftware Teile des

IT-Systems lahmgelegt. Auch dort forderten die Hacker laut der Staatsanwaltschaft Göttingen erfolglos ein Lösegeld.

Das Krankenhaus schreibt, es habe gut reagiert und direkt nach Befall die Systeme heruntergefahren sowie die Internetverbindung gekappt. Backups der wichtigsten Daten seien vorhanden. Bereits einen Tag später war die normale Versorgung der Patienten wiederhergestellt. Polizei und Staatsanwaltschaft ermitteln, während das Krankenhaus in der Zwischenzeit zu Papier und Stift wechselt.

In Geisenheim erkannte der Virenschanner den Trojaner, konnte aber dessen Installation nicht verhindern. Laut Pressemitteilung der Stadt Geisenheim dauert es im schlimmsten Fall zwei bis zu drei Monate, bis alle Systeme wieder einwandfrei funktionieren. Die Verwaltung plant, alle EDV-Systeme neu aufzusetzen oder auszutauschen.

### Fazit

Die drei Beispiele zeigen auf, wie wichtig Grundregeln in der IT-Sicherheit sind. Alleine Backups wie in Wolfenbüttel können den Unterschied machen, zwischen einigen Tagen Ausfall und mehreren Monaten. Häufig ist die IT veraltet, nicht auf dem aktuellen Stand oder es fehlen wichtige zeitnahe Patches. Es ist also kein Wunder, dass sich Angriffe in solchen Ausmaßen häufen. Mehr dazu auf Seite 39. (wid@ct.de) **ct**

### Literatur

- [1] Ronald Eikenberg, Windows-Lücke mit Druck, PrintNightmare: Zero-Day-Sicherheitslücke in Windows-Druckerwarteschlange, c't 16/2021, S. 36



**Das Klinikum Wolfenbüttel teilte seinen Patienten über Facebook mit, dass ein Angriff stattgefunden hat. Auf der Website des Krankenhauses dagegen steht nichts zu dem Vorfall.**

## Was wir aus den aktuellen Ransomware-Vorfällen lernen können

Von Jürgen Schmidt  
(Leiter von heise Security)

**O**ft fehlt es bei den Betroffenen von Ransomware-Vorfällen schon an den absoluten Basics – und da sind Ämter, Behörden und Verwaltung ganz vorne mit dabei. Deren IT besteht oft aus einer überalterten Monokultur auf Windows-Basis, bekommt Security-Updates wenn überhaupt dann erst nach Monaten und die IT-Verantwortlichen sind so damit beschäftigt, das alles überhaupt irgendwie am Laufen zu halten, dass für IT-Security keine Zeit bleibt.

Da genügt dann ein falscher Klick, ein gestohlenes Passwort oder ein erfolgreicher Scan auf ein bekanntes Sicherheitsloch und es knallt. Dann fällt wie in Bitterfeld oder Geisenheim die komplette IT auf Wochen oder gar Monate aus. Dabei ließe sich ein Großteil dieser Ransomware-Vorfälle vermeiden, wenn man wenige grundlegende Security-Regeln befolgt: Sicherheits-Updates zügig einspielen, konsequent nur minimale Rechte einzusetzen, für hoch priorisierte Accounts und Remote-Zugänge Zwei-Faktor-Authentifizierung einführen. Und natürlich dürfen gute und funktionierende Backups nicht fehlen. Das wäre dann schon mehr als nur die halbe Miete.

Dass diese Basisanforderungen eine Selbstverständlichkeit werden wie Sicherheitsgurte und funktionierende Bremsen, ist auch Aufgabe der Politik. Die muss Rahmenbedingungen vorgeben, die das nicht nur ermöglichen, sondern konsequent herbeiführen.

Doch wie die Hackerbande REvil mit den aktuellen Attacken eindrucksvoll gezeigt hat, ist es damit noch nicht getan. Denn angesichts von breit gestreuten Zero-Day- und Supply-Chain-Angriffen müssen wir auch unsere Vorstellung von mög-



lichst guter Sicherheit ändern. Bisher ging es da vor allem darum, wirklich alle Angriffe zu verhindern. Das wird aber in Zukunft nicht mehr zu hundert Prozent möglich sein.

Egal wie viel Aufwand wir investieren, es wird erfolgreiche Angriffe geben. Deshalb müssen wir an einen Punkt kommen, an dem auch zunächst erfolgreiche Angriffe nicht mehr sofort „Game Over“ bedeuten, sondern zu ernsten, aber beherrschbaren Vorfällen werden. Dazu müssen wir vor allem für zwei Dinge sorgen: dass wir

- a) eine bessere Chance haben, diese erfolgreichen Angriffe frühzeitig zu erkennen und
- b) solche Angriffe eingrenzen und handhaben können, ohne dass es zu kritischen Verlusten kommt.

Besseres Monitoring und mehr Resilienz sind deshalb die zwei Themen, die meiner Ansicht nach aktuell den Schwerpunkt des konsequenten Ausbaus der IT-Security bilden sollten. Selbstverständlich gilt das erst, nachdem man die Basics im Griff hat, ohne die es weiterhin nicht geht. Wer keine Backups macht, ungepatchte Software einsetzt, schwache Passwörter benutzt und kritische Dienste weitgehend ungeschützt ins Internet exponiert, braucht sich über Zero Days und Lieferkettenangriffe keine Gedanken zu machen. Den wird es treffen – und zwar eher früher als später. (wid@ct.de)

## Unsere Server-Buddies sind #NäherDran – IT-Kompetenz im Doppelpack

Grundsätzlich machen wir es unseren Kunden ja gerne besonders einfach – bei der persönlichen Beratung und Betreuung legen wir aber noch einen drauf. Deshalb kümmern sich Ihre Thomas-Krenn-Buddies immer im Duo um Ihre Anliegen.

Für Sie bedeutet das: Zweifaches Engagement, zweifaches Know-how und zweifache Erfahrung! Gemeinsam sichern Vertriebsberaterin Magdalena und Key Account Manager Andre den Erfolg unserer Kunden in Mitteldeutschland – denn doppelt berät am besten!

### Ihre Buddies in Mitteldeutschland #NäherDran



Magdalena & Andre

Buddy-Beratung unter:  
[thomas-krenn.com/mitte](http://thomas-krenn.com/mitte)

THOMAS  
KRENN®



Bild: Olivier Hoslet/EPA Pool/AP/dpa

mit iMessage-Nachrichten Schadcode einschleusen lässt, über den dann der Angreifer die volle Kontrolle über das Gerät erlangt. Als Schwachpunkt gelten Funktionen zur Anzeige von Bildern.

Innerhalb von Sekunden können Angreifer feststellen, wo sich das Opfer befindet und aus dem Kalender ablesen, wann es sich mit welchen Personen trifft. Aus der Ferne lassen sich Kamera und Mikrofon einschalten, beliebige Login-Informationen und Passwörter auslesen, ebenso Mails und Messages – egal ob verschlüsselt oder nicht.

Um seine Anwesenheit zu verschleiern, blockiert Pegasus den Versand von Crash-Reports an Apple, löscht Einträge aus Log-Dateien, ändert die Namen seiner Programmdateien und Web-Domains. Die Ergebnisse veröffentlichte Amnesty auf GitHub, inklusive eines Analyse-Tools namens MVP (siehe ct.de/yecf).

Laut Amnesty sind Android-Smartphones ebenso betroffen, ließen sich aber schwieriger untersuchen. Die neueste Version von Pegasus soll sich sogar nur flüchtig im Hauptspeicher einnisten und nach einem Reboot verschwinden, was den Nachweis erheblich erschwert.

### Deutsche Beteiligung

Ein technischer Schutz gegen solche Übergriffe ist im Alltag der Betroffenen kaum möglich. Vielmehr ist die Politik gefragt. Laut Amnesty soll Pegasus keine Smartphones innerhalb der USA anzapfen. Ebenso scheinen deutsche Smartphone-User unbehelligt: Auf der Liste fanden sich keine hiesigen Telefonnummern. Offiziell setzen deutsche Geheimdienste Pegasus aus juristischen Gründen bislang nicht ein.

Mussten die Opfer bis vor etwa zwei Jahren noch auf präparierte Links klicken, so können ihre Smartphones seitdem auch ohne ihr Zutun infiziert werden. Im ersten Schritt schicken die Angreifer dem Opfer eine präparierte Mitteilung per iMessage, woraufhin die Nachrichten-App Befehle aus der Ferne ausführt. Wenn das nicht klappt, stellen Angreifer in der Nähe des Opfers einen IMSI-Catcher auf, um seinen Mobilfunk-Datenverkehr abzufangen. Ein IMSI-Catcher tarnt sich dazu als herkömmliche Funkzelle, in die sich Smartphones einwählen.

Offenbar existiert im iPhone-Betriebssystem iOS (nachgewiesen bis Version 14.6) mindestens eine öffentlich un dokumentierte Lücke, über die sich etwa

# Infiziert ohne Klick

## Amnesty International deckt Massenüberwachung durch Pegasus auf

**50.000 Telefonnummern waren Ziel von Pegasus: Die Spähsoftware der NSO Group infizierte Smartphones von Aktivisten, Politikern und Journalisten aus rund 50 Ländern.**

Von Hartmut Gieselmann

Die Analysen von Amnesty International zeichnen ein erschreckendes Bild der Überwachungen von Geheimdiensten: Sie kapern fremde Smartphones mittels spezialisierter Einbruchsprogramme und kehren die Multi-Sensorgeräte zu Spionen gegen ihre Eigner. In Zusammenarbeit mit 17 internationalen Redaktionen (darunter NDR, WDR, Süddeutsche Zeitung und Die Zeit) wertete Amnesty eine ihnen zugespielte Liste mit 50.000 Telefonnummern aus. Sie enthält mutmaßliche Angriffsziele der Abhörsoftware Pegasus, die die israelische NSO Group herstellt.

Amnesty konnte Pegasus etwa auf Smartphones der Angehörigen des getö-

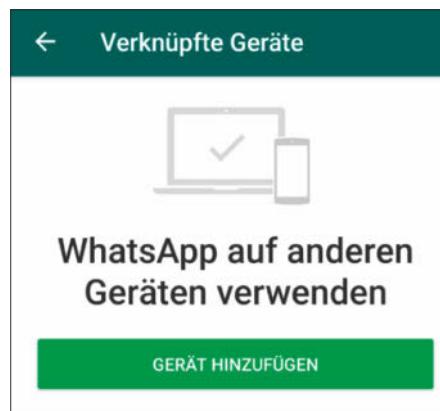
Pegasus-Analyse: [ct.de/yecf](http://ct.de/yecf)

## WhatsApp auf mehreren Geräten

**Der Messengerdienst soll bald auf bis zu vier zusätzlichen Clients laufen können. Ein geschlossener Betatest hat begonnen.**

In zukünftigen WhatsApp-Versionen soll es Nutzern möglich sein, den Messenger auf bis zu vier weiteren Geräten parallel zu verwenden – auch auf Mobilgeräten und in Desktop-Clients. Da Chats und Kontakte nach der Anmeldung eines zusätzlichen Gerätes synchronisiert werden, lassen sich diese außerdem endlich unkompliziert von Android auf iOS und umgekehrt übertragen. Die Ende-zu-Ende-Verschlüsselung will WhatsApp dabei nicht aufgeben. Dafür soll eine neue Architektur sorgen, in der jedes Zusatzgerät einen eigenen Schlüssel erhält.

Die neue Fähigkeit beseitigt eine oft kritisierte Schwäche von WhatsApp: Bislang durften Anwender nur ein einzelnes Smartphone für den Messenger verwenden. Zwar ließ sich der App-Inhalt mithil-



**WhatsApp's Verknüpfungsfunktion wird erweitert: Der Dienst ist bald nicht mehr an ein einzelnes Smartphone gekoppelt.**

fe einer Verknüpfungsfunktion in einen einzelnen Browserzugang spiegeln, die Chats und Kontakte blieben aber auf dem Smartphone. (mon@ct.de)

## Bundesregierung muss Facebook-Seite abschalten

Der **Bundesdatenschutzbeauftragte** Ulrich Kelber verlangt von der Bundesregierung und den obersten Bundesbehörden, bis zum Jahresende ihre Facebook-Präsenzen abzuschalten. Ein DSGVO-konformer Betrieb von Facebook-Seiten sei derzeit nicht möglich, erläuterte Kelber in einem Rundbrief. Dem Bundesdatenschutzbeauftragten obliegt die Aufsicht über Tätigkeiten der Bundesregierung.

Kelbers Ansicht beruht auf einer EuGH-Entscheidung aus dem Jahr 2018. Ihr zufolge sind Betreiber einer Facebook-Fanpage gemeinsam mit Facebook

verantwortlich für die Verarbeitung personenbezogener Daten der Besucher („Joint Controlling“), das heißt, sie hatten nach DSGVO für Datenschutzverstöße von Facebook mit. Der Konzern bot daraufhin eine „Joint-Controller-Vereinbarung“ an, in der Verantwortlichkeiten neu geklärt werden. Es bleibe allerdings weiterhin unklar, was der Konzern mit Nutzerdaten mache, sagte Kelber im Deutschlandfunk. Dies sei ein „unhaltbarer Zustand“, den nicht nur er, sondern auch das EU-Parlament kritisieren. (hob@ct.de)



**Der Bundesdatenschutzbeauftragte Ulrich Kelber nennt Facebooks Umgang mit Nutzerdaten von Seitenbetreibern einen „unhaltbaren Zustand“.**

## Staatstrojaner vor Gericht

Kaum sind die neuen Befugnisse zum Einsatz von Staatstrojanern in Kraft getreten (siehe S. 168), liegt dem **Bundesverfassungsgericht (BVerfG)** die erste Beschwerde dagegen vor: Die FDP-Bundestagsfraktion hat sie am 15. Juli eingereicht. Wenn der Einsatz des Staatstrojaners nun auch den Verfassungsschutzbehörden von Bund und Ländern sowie dem Militärischen Abschirmdienst (MAD) gestattet werde, entstehe eine „Sicherheitslücke für alle Menschen in Deutschland“, sagte der FDP-Abgeordnete Konstantin Kuhle der dpa. Das sei unverhältnismäßig, zumal die Zahl der Überwachungsfälle vermutlich gering sein werde. Der parlamentarische Geschäftsführer der Fraktion, Marco Buschmann, sagte, in einer Gesellschaft, in der jeder jederzeit potenziell damit rechnen müsse, überwacht zu werden, sei es normal, wenn sich Bürger fragten, ob sie überhaupt noch frei reden könnten. Er verglich den Einsatz des „Staatstrojaners“ mit der heimlichen Durchsuchung von Privaträumen. (hob@ct.de)

## Kurz & knapp: Internet

Die Deutsche Bahn stellt für ihre Fernverkehrszüge ab sofort Daten für einen **Echtzeit-Fahrplan im Routenplaner** von Google Maps bereit, samt Verspätungen, Gleiswechseln und Links zum Fahrkartenkauf.

Laut der Finanznachrichtenagentur Bloomberg haben seit Beginn von **Apples neuer Datenschutzpolitik** nur 25 Prozent der iOS-Nutzer dem Tracking in Facebook zugestimmt; andere App-Entwickler sprechen von ähnlichen Entwicklungen.

Die Audio-Diskussions-App **Clubhouse** hat den Betatest beendet; ab sofort ist daher keine Einladung durch Mitglieder mehr erforderlich, um den Dienst nutzen zu können.



erhielt jedes neunte EBR-Mitglied trotz gesetzlicher Vorgaben keine angemessene Ausrüstung für Onlinekonferenzen und knapp ein Drittel bekam keine ausreichende technische Einweisung. Jedes vierte Mitglied musste auf Dolmetscher verzichten, die etwa für die Verständigung einer deutschen mit einer ungarischen Niederlassung dringend notwendig sind.

Eine übergroße Mehrheit sprach sich für eine Rückkehr zu Präsenzsitzungen aus. Diese verbesserten nicht nur die interne Zusammenarbeit der Betriebsräte, sondern auch den Meinungsaustausch mit Managern.

In diesem Punkt stimmten ihnen auch Personalchefs zu, die zusammen mit Betriebsräten von der französischen Denkfabrik Réalités du Dialogue Social (RDS) Anfang Mai für eine Studie interviewt wurden: Vertreter beider Seiten berichteten, dass Online-Meetings mit höherem Tempo ablaufen, bei dem die nicht sichtbare Körpersprache ein gegenseitiges Verständnis beeinträchtige und zu Verzerrungen führe. Betriebsräte hatten zuweilen den Eindruck, dass die Arbeitgeberseite die Distanz nutze, „um Dinge beiseitezuschieben oder durchzusetzen, die ansonsten nicht akzeptabel wären“.

#### Erhöhter Zeitaufwand

Ebenso relativierten sie die angebliche Zeitersparnis virtueller Zusammenkünfte. Denn die Vorbereitungen erforderten deutlich mehr E-Mails und Telefongespräche. Das bestätigt auch eine neue Untersuchung der Nationalen Agentur zur Verbesserung der Arbeitsbedingungen (ANACT) aus Frankreich: Von den 1415 Unternehmer- und Beschäftigtenvertreten sagten 40 Prozent, dass die Vorbereitung von Onlinesitzungen mehr Zeit braucht. Zwei Drittel sahen insgesamt eine erhöhte Arbeitsbelastung zur Aufrechterhaltung des sozialen Dialogs.

Bei den von der Denkfabrik RDS Befragten herrschte Einigkeit darüber, dass der direkte persönliche Kontakt unerlässlich sei, „denn enge menschliche Beziehungen sind das Herzstück des sozialen Dialogs“. Fürsprecher einer Virtualisierung derartiger Verhandlungen könnten am Ende die sozialpartnerschaftliche Zusammenarbeit torpedieren und womöglich ungewollt einen Klassenkampf alter Prägung fördern.

(hag@ct.de) **ct**

**Studien und Umfragen:** [ct.de/yv39](http://ct.de/yv39)

# Digital entfremdet

## Videoschalten erschweren Verhandlungen zwischen Betriebsräten und Managern

**EU-weit klagen Betriebsräte über verschlechterte Verhandlungen mit Arbeitgebern. Die Schuld geben sie dem Umstieg auf Videokonferenzen.**

Von Andreas Schuchardt

**V**irtuelle Meetings sparen oft Zeit und Geld. Doch wenn es um harte Verhandlungen mit konträren Positionen unterschiedlicher Parteien geht, behindern Bildschirme und Mikrofone mitunter eine Verständigung. Das zeigen aktuelle Umfragen und Studien zu den Auswirkungen von Videokonferenzen auf Tarifverhandlungen und die Arbeit von Betriebsräten in Europa. Die Arbeitnehmervertretungen registrieren eine deutliche Verschlechterung der Verhandlungen und eine Verschärfung der Konflikte mit Firmenvorständen.

Seit Mai 2020 sind in Deutschland laut § 129 BetrVG auch Betriebsratsbeschlüsse rechtsgültig, die nicht in Präsenz, sondern am Telefon oder einer Videokonferenz getroffen werden. Mehr als ein Jahr später legte jetzt das zum Europäischen Gewerk-

schaftsbund gehörende Gewerkschaftsinstitut (ETUI) die Ergebnisse einer Befragung von 476 Mitgliedern vor. Sie gehören Europäischen Betriebsräten (EBR) an, von denen rund 1100 in der EU existieren. Voraussetzung für ihre Gründung ist, dass eine Firma mindestens tausend Mitarbeiter hat, von denen mindestens 150 in einem anderen EU-Land arbeiten.

Den Aussagen der Befragten zufolge habe die Unterrichtung und Anhörung durch das jeweilige Management „erheblich gelitten“. Zudem konstatierte ein Drittel der Betriebsräte eine Verschlechterung der internen Funktionsweise ihres EBR.

Vor Ausbruch der Pandemie wurden bei Präsenzsitzungen 78 Prozent der Betriebsräte regelmäßig über die Lage des Unternehmens informiert. Bei der aktuellen Befragung Anfang 2021 waren es nur noch 50 Prozent. Während vor Corona noch in über der Hälfte der Fälle Anhörungen zu Umstrukturierungsplänen der Unternehmensleitung stattfanden, halbierte sich dieser Anteil während der Pandemie auf ein Viertel. Infolgedessen stieg die Zahl „ernsthafter Konflikte“ zwischen Betriebsräten und Vorstandsetagen gegenüber dem Vorjahr von 7 auf 19 Prozent.

Zudem berichteten EBR-Angehörige von Behinderungen ihrer Arbeit. Laut ETUI

# Netzwerk Freie Schulsoftware: Schulen helfen Schulen

**Anfang Juli hat der gemeinnützige Verein Digitalcourage das „Netzwerk Freie Schulsoftware“ gestartet. Das Hilfsprojekt soll den Erfahrungsaustausch zwischen Schulen fördern.**

Akteure an Schulen, die bereits Erfahrungen mit dem Einsatz von freier Software gemacht haben, können über das Netzwerk mit Lehrern, Vertretern der Schulverwaltung und Eltern Kontakt aufnehmen, die noch am Anfang stehen. Mit freier Software sind Programme gemeint, die dem Nutzer die Freiheit einräumen, ein Programm auszuführen, zu modifizieren und unverändert oder verändert weiterzuverbreiten.

Freie Software wird in Schulen für Videokonferenzen und Dateiablage eingesetzt, Messenger und Lernmanagement-Systeme sowie digitale Werkzeuge für einzelne Unterrichtsfächer sind ebenfalls im Einsatz. Wer Know-how und Erfahrungen anzubieten hat, trägt sich auf der Website des Netzwerks ein, um ande-

re zum Austausch einzuladen. Wer Rat sucht, findet in einer alphabetischen Liste mit freier Schulsoftware oder in einer fächerspezifischen Übersicht jeweils den richtigen Ansprechpartner zum favorisierten Programm. Bereits eine Woche nach Projektstart verzeichnete das Netzwerk über 400 Hilfsangebote vom Beratungsgepräch bis zur Unterstützung bei der Einrichtung freier Software.

Das Netzwerk soll dem Einsatz kommerzieller Software wie Microsoft Teams oder Google Classroom in Schulen ent-

gegenwirken, der während der corona-bedingten Schulschließungen stark zugenommen hat. „Dass Schulen sich von den Big Playern des Marktes bezirzen lassen, ohne nachzudenken, was mit den Daten der Lehrer und Schülerinnen passiert, kann man ihnen nicht einmal verbüeln. Es gibt viele Gründe, die unser Bildungssystem an diesen Punkt gebracht haben“, erklärt die Medienpädagogin Jessica Wawrzyniak von Digitalcourage. „Wir müssen aber schleunigst gegensteuern.“

(dwi@ct.de)

**Von A wie Anki bis X wie XMPP/Jabber: Im Netzwerk Freie Schulsoftware findet man erfahrene Ansprechpartner rund um freie Software für den Bildungsbereich.**

## So können Sie mitmachen

### 1. Formular (Biete/Suche)



**Formular ausfüllen:**  
Welche Freie Software nutzen Sie? Wo können Sie helfen? Wo benötigen Sie Hilfe?

### 2. Hilfe finden & anbieten



**Austausch finden & anbieten:**  
Schauen Sie nach, welche Schule in der Nähe Hilfe anbietet und zu welchen Themen noch Expertise gesucht wird.

### 3. Informationen



**Informationen & Aufklärung:**  
Hier finden Sie Informationen zu digitaler Bildung und Datenschutz an Schulen.

# Schul-Konfigurator von der Telekom

Internetanschluss, WLAN, Endgeräte, Präsentationshilfen wie Whiteboards und schließlich die Software – die **Telekom will Schulen mit allem versorgen**, was für die Digitalisierung des Lehrens und Lernens notwendig ist, inklusive Service und Schulungen. Auf seiner Website bietet das Unternehmen neuerdings einen „Schul-Konfigurator“ an, mit dem sich die IT-Verantwortlichen beim Schulträger ihren Wunschzettel zusammenklicken sollen.

Laut Telekom dient der Konfigurator dazu, alle benötigten Module aufeinander abzustimmen. Nach Abschluss der individuellen Konfiguration erstellt die Website eine Zusammenfassung. Die kann laut Telekom als Basis für eine Ausschreibung oder Beauftragung dienen. Auf Wunsch erstellt die Telekom auf dieser Grundlage ein Angebot für Schulen; das Unternehmen wirbt bei Schulträgern damit, die deutschen Datenschutzzvorschriften und den Schutz vor Fremdzugriffen zu gewährleisten.

Tablets, Whiteboards und Software bietet das Telekommunikationsunternehmen gemeinsam mit Partnern an, darunter Apple, Samsung, Microsoft und Lenovo.

(dwi@ct.de)

# Bund und Länder fördern KI

Mit der **Förderinitiative „Künstliche Intelligenz in der Hochschulbildung“** wollen Bund und Länder einerseits die Qualifizierung von akademischen Fachkräften im Bereich der KI verbessern. Andererseits wird damit auch die Gestaltung von KI-gestützten Lern- und Prüfungsumgebungen gefördert.

Die rechtliche Grundlage der Initiative ist eine Bund-Länder-Vereinbarung, die Ende 2020 von der Gemeinsamen Wissenschaftskonferenz (GWK) verabschiedet wurde. Bund und Länder stellen dafür insgesamt rund 133 Millionen Euro zur Verfügung. Die Kosten tragen jeweils im Verhältnis 90:10 der Bund und das Land, in dem die geförderte Einrichtung ihren Sitz hat.

Hochschulen konnten sich einzeln oder im Verbund für die Förderung bewerben. Im Juni 2021 fiel die Entscheidung für 40 Einzelanträge und 14 Verbundprojekte; insgesamt erreicht die Initiative 81 Hochschulen. Sie läuft bis zum 31. Dezember 2025; eine unabhängige Evaluation ist für 2024 geplant.

(dwi@ct.de)

The screenshot shows a step-by-step configuration process. Step 1: Start. Step 2: Internet Anschluss. Step 3: Campus-Vernetzung. Step 4: Tablets. Step 5: Laptops. Step 6: Präsenztechnik. Step 7: Lern- und Konferenzsoftware. Step 8: Schulungen. Step 9: IT Service. Step 10: Zusammenfassung. Below this, a section asks: "Wie möchten Sie den Schulcampus mit Internet versorgen?" It includes icons for a classroom, a building, and a network signal, with text explaining the need for LAN and WLAN coverage. At the bottom, it says: "In zehn Schritten können Schulen mit dem Konfigurator der Telekom geeignete Hard- und Software sowie den passenden Service auswählen."

## Displayfolie zeigt klare Farben auch im Sonnenschein

**Ein reflektierendes E-Paper-Display schwedischer Forscher nutzt das Umgebungslicht und stellt damit farbige Bildschirminhalte auch im Freien gut erkennbar dar. Zudem spart die neue Technik Energie.**

Reflektierende Bildschirme ahmen das optische Verhalten von bedrucktem Papier nach. Während Displays mit Hintergrundbeleuchtung nur in Innenräumen angenehm anzusehen sind und dem Betrachter bei Sonnenlicht Probleme bereiten, nutzen reflektierende Bildschirme das Umgebungslicht für einen natürlichen Seh-eindruck. Damit ist diese Technik energie-sparender und gleichzeitig für die Augen weniger ermüdend.

An der Technischen Universität Chalmers in Göteborg, Schweden, hat ein Team um Professor Andreas Dahlin eine nano-strukturierte elektrochrome Displayfolie entwickelt. Wie das Team gemessen hat, zeigt sie farbige Bilder unter Tageslicht in einem breiteren Farbspektrum und heller an als die jüngste Generation heutiger Farb-E-Reader mit Hintergrundbeleuchtung. Der Energiebedarf liegt bei statischen Anzeigen nahe null, erklärt Dahlin in einer Pressemitteilung. Bisherige reflektive Bild-

schirmtechnik am Markt beschränkt sich auf Schwarz-Weiß-Darstellungen.

Die neue E-Paper-Folie besteht aus einer farbgebenden Schicht Wolframtrioxid, eingerahmt in zwei dünne Schichten aus Gold und Platin. Alle zusätzlichen elektrischen Komponenten liegen hinter der Platin-Spiegelschicht, sodass der Blick auf die Farben davon ungetrübt bleibt. Für die funktionalen Bestandteile der Dis-

playfolie genügt eine Stärke von nur wenigen hundert Nanometern.

Derzeit versuchen die Forscher, vor allem den Platinanteil der Folie noch weiter zu senken. Sie hoffen bereits in naher Zukunft auf einen wirtschaftlichen Einsatz ihrer neuen Displaytechnik, sei es in Smartphones und Tablets oder sogar großflächiger, etwa im Bereich der Außenwerbung.

(agr@ct.de)

**Eine ultradünne elektrochrome Folie zeigt ihr Farbspektrum. Die neue reflektierende Variante nutzt das Umgebungslicht und ließe sich als Display auch im Sonnenschein angenehm betrachten.**



Bild: Mats Tiborn / Chalmers University of Technology

## Autonome Drohne am schnellsten

Ein autonom fliegender Quadrocopter einer Forschungsgruppe der Universität Zürich hat erstmals die Drohnen zweier Weltklasse-Piloten im Wettrennen hinter sich gelassen. Der dabei eingesetzte Algorithmus der Robotics and Perception Group unter Davide Scaramuzza berechnet nicht nur die schnellste Flugbahn, sondern er reizt auch die Leistungsgrenzen der Drohne aus. Bisherige Algorithmen arbeiteten mit vereinfachten Drohnenmodellen.

Die Software verarbeitet externe Kammerbilder, um die Drohnenposition in Echtzeit zu berechnen. Auf dem Parcours, einem Rundkurs mit mehreren festgelegten Wegpunkten, konnten die menschlichen Piloten zuvor trainieren. Parallel errechnete die Drohnensoftware ihre Flugroute. Die autonome Drohne gewann nicht nur ein Rennen, sie **flog alle Runden schneller als die von Piloten gesteuerten Quadrocopter**. Nun wollen die Forscher

ihren Algorithmus weiter beschleunigen, derzeit braucht er zur Planung der optimalen Route bis zu einer Stunde. Zudem wollen sie das System auf Onboard-Kameras umstellen.

(agr@ct.de)



**Ein autonomer Quadrocopter, dessen Aerodynamik sich im Nebel zeigt, hat erstmals Wettrennen gegen von Profis gesteuerte Drohnen gewonnen.**

Bild: Universität Zürich

## KI findet Mittel gegen Covid-19

Ein Team um Professor Friedemann Weber am Institut für Virologie der Justus-Liebig-Universität Gießen hat gemeinsam mit Kollegen aus Cambridge, UK, eine künstliche Intelligenz auf Covid-19 angesetzt. Sie trainierten ihr neuronales Netz mit allen verfügbaren Daten zu zellulären Proteinen und den Signalwegen, die das Virus zur Replikation nutzt. Die **KI entdeckte dann in einer Medikamenten-Datenbank 200 vielversprechende Wirkstoffe**, die bereits im Kampf gegen andere Krankheiten zugelassen sind. Anschließende Laborversuchen bestätigten zwei dieser Wirkstoffe als hochwirksam gegen Covid-19. Das neue „In-silico-Verfahren“ könne laut Weber künftig helfen, Medikamente auch gegen andere Krankheiten schneller zu finden.

(agr@ct.de)

# Kommt der digitale Euro?

**Digital bezahlen ohne Konto oder Karte – und das so sicher, einfach und datenarm wie mit Bargeld? Eine digitale Zentralbankwährung könnte diese Vorstellung wahr machen. Sie wirft aber auch viele Fragen auf.**

Die Europäische Zentralbank (EZB) startet eine auf zwei Jahre veranschlagte Untersuchungsphase zu einem digitalen Euro. Das hat der EZB-Rat nach einer mehrmonatigen „Erprobungsphase“ bekannt gegeben, in der die EZB bereits die technische Machbarkeit erfolgreich geprüft und untersuchungsrelevante Fragen identifiziert habe. Zugleich betonte die EZB ausdrücklich, dass ein digitaler Euro Bargeld ergänzen, nicht aber ersetzen soll.

Zu den Untersuchungsgegenständen zählen laut EZB zunächst die grundsätzliche Architektur und Konzeption eines digitalen Euro und denkbare Anwendungsfälle. Hinzu kommen der rechtliche und politische Rahmen sowie mögliche Folgewirkungen auf Finanzsystem, Wirtschaft und Gesellschaft. In die Untersuchung sollen unter anderem die Ergebnisse der praktischen Erprobung einfließen, die EZB und nationale Zentralbanken im Euroraum bereits gemeinsam mit Akteuren „aus der Wissenschaft und dem privaten Sektor“ gewonnen haben. Dazu gehörten die Bereiche „Kontenbuch“ (Ledger), Datenschutz und Geldwäschebekämpfung, Begrenzung der Umlaufmenge eines digitalen Euro sowie Offline-Zugänge.

ge und Inklusion. Auch die nun folgende Untersuchung solle einer Einführung nicht vorweggreifen, sondern Entscheidungsgrundlagen und Konzepte liefern.

Die Ziele hat die EZB entsprechend offen und abstrakt formuliert. So hat sie beispielsweise nicht vorab festgelegt, ob der Zahlungsverkehr über eine Blockchain oder das vorhandene Echtzeit-Zahlungsabwicklungssystem des Euroraums („TIPS“) abgewickelt werden würde. Beides sei nachweislich dazu in der Lage. Möglich seien zudem „Architekturen, die zentrale und dezentrale Elemente vereinen“.

Die Zentralbank will sich während der Untersuchung mit dem Europäischen Parlament und „anderen europäischen Entscheidungsträgern“ austauschen. Außerdem werde man Privatpersonen, Handel

und Zahlungsverkehrssektor einbeziehen und zusätzlich ein unabhängiges Expertengremium schaffen. Unklar bleibt, inwieweit die endgültige Entscheidung über einen digitalen Euro durch demokratisch legitimierte Institutionen getroffen wird. Für die endgültige Einführung des digitalen Euros veranschlagt EZB-Direktoriumsmitglied Fabio Panetta nach der zweijährigen Untersuchungsphase drei weitere Jahre.

Die Deutsche Kreditwirtschaft (DK), der Spitzenverband der Banken und Sparkassen, begrüßte die Initiative in einer ersten Reaktion. Zugleich forderte die DK, parallel auch tokenisiertes und damit programmierbares Girogeld und Zentralbankguthaben zu entwickeln, damit Banken und Sparkassen ihre angestammte Rolle im Finanzsystem behielten. Die EU-Datenschutzbeauftragten hatten sich zuvor bereits für eine weitreichende Anonymität der Nutzer ausgesprochen.

Beobachter sehen die Eurozone unter Zugzwang. So könnte eine private Kryptowährung wie der von einem Facebook geführten Konsortium geplante „Diem“ dem Euro-Zahlungssystem Konkurrenz machen. Auch staatliche Initiativen wie der „digitale Yuan“ Chinas oder die „e-Krona“ in Schweden üben Druck aus. Bereits im Oktober 2020 hatte die EZB selbst darauf hingewiesen, dass ein digitaler Euro der Innovationskraft, Wettbewerbsfähigkeit und „strategischen Autonomie“ Europas dienen könne. (mon@ct.de)



Bild: dpa / Daniel Karmann

**Die Europäische Zentralbank will die mögliche Einführung eines digitalen Euros vorbereiten.**



Bild: S-Payment GmbH

## Apple Pay: Girocard online nutzbar

Wer mit Apple Pay zahlt und im Wallet eine Girocard („EC-Karte“) einer Sparkasse hinterlegt hat, kann damit zukünftig auch im Internet einkaufen – vorausgesetzt, er nutzt im Onlineshop Apple Pay als Zahlungsart. Bisher war die Girocard auf den Einsatz im stationären Handel beschränkt. Wie der Deutsche Sparkassen- und Giroverband (DSGV) mitteilte, sind zu Beginn allerdings nur eine Handvoll Händler dabei, darunter Flixbus, Media Markt und Lieferando, außerdem mehrere Nahverkehrsunternehmen. Bis Ende 2021 sollen sukzessive weitere Shops folgen, sobald deren Zahlungsabwickler die Funktion

eingerichtet haben. Bereits mit der Integration der Girocard in Apple Pay haben die Sparkassen derzeit ein Alleinstellungsmerkmal in Deutschland.

Nutzern der Girocard in Apple Pay entstehen auch bei Einkäufen im Internet keine Entgelte über jene ihres Kontomodells hinaus; das Sicherheits- und Datenschutzniveau soll unverändert hoch bleiben. Überdies erhalten Nutzer laut DSGV einen Online-Käuferschutz, der „einen vergleichbaren Leistungsumfang wie der anderer gebräuchlicher Online-Zahlverfahren“ aufweise und ebenfalls kostenlos sein soll. (mon@ct.de)

**Die Sparkassen haben die Girocard in Apple Pay internetfähig gemacht.**

# Bit-Rauschen

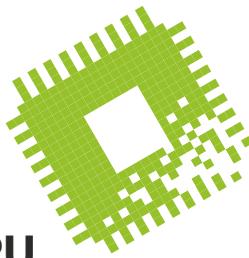
## Intels Fab-Pläne, RISC-V-Neulinge und eine 128-Kern-CPU

**Intel will angeblich 100 Milliarden US-Dollar in Chip-Fabs pumpen. Der Core i-12000 wirft Schatten voraus. RISC-V kommt stärker in Fahrt und AMD plant ein Kernmonster für Server.**

Von Christof Windeck

Bisher sind es nur Spekulationen, allerdings von üblicherweise gut informierten Zeitungen wie Financial Times und Wall Street Journal: Demnach will Intel über mehrere Jahre rund 100 Milliarden US-Dollar in den Ausbau der Chipfertigung stecken. Ein gutes Fünftel davon könnte nach Europa fließen, es laufen Gespräche über Fördermittel und Standorte, darunter der ehemalige Flughafen Penzing bei Landsberg am Lech. Außerdem erwägt Intel angeblich den Kauf des derzeit viertgrößten Chip-Auftragsfertigers Globalfoundries – was dessen Chef Dr. Thomas Caulfield aber dementierte. Er betonte, dass Globalfoundries die eigene Fertigungskapazität deutlich erweitern will. Diese Pläne sind grundsätzlich bekannt, etwa die Investition von jeweils rund einer Milliarde US-Dollar in die Werke in Dresden und in den USA; außerdem soll für vier Milliarden US-Dollar eine neue Fab in Singapur entstehen. Ebenfalls bekannt ist, dass der Staatsfonds Mubadala aus den Vereinigten Arabischen Emiraten, dem Globalfoundries gehört, das Unternehmen an die Börse bringen will – nur wann, ist offen.

Der ehemalige TSMC-Chef Morris Chang warnt unterdessen vor unüberlegter Subventionierung regionaler Chipfertigung, die derzeit die USA, die EU und China auf der Agenda haben. Das könnte dazu führen, dass die Chipfertigung zu teuer wird und die lokalen Hersteller jeweils nicht die ganze Bandbreite der Technologie beherrschen. Das wiederum drohe



den Fortschritt zu bremsen. Die Sicherung lokaler Fertigung für sicherheitskritische Chips – etwa für Rüstungstechnik und kritische Infrastrukturen – nannte er allerdings „umsichtig“.

### RISC-V-Rennen

Einen Schritt in Richtung digitale Souveränität geht auch Russland: Der Staatskonzern Rostec kooperiert mit dem russischen IT-Hersteller Yandro, der wiederum Anteile an der RISC-V-Entwicklerfirma Syntacore hält. Gemeinsam wollen die drei Unternehmen bis 2025 einen RISC-V-Prozessor entwickeln, der genügend Rechenleistung für Notebooks, PCs und Server bereitstellt. Davon sind bisher lieferbare Systems-on-Chip noch weit entfernt, wie der Test des RVBoards Nezha mit Allwinner D1 zeigt (siehe S. 92). Die US-Firma SiFive hat allerdings mit der U8-Baureihe von RISC-V-Kernen deutlich stärkere Out-of-Order-Designs im Angebot. Die Chinesische Akademie der Wissenschaften (CAS) tüftelt am XiangShan, der es in einigen Jahren mit einem ARM Cortex-A76 aufnehmen soll. Das würde dann zumin-

dest für einfache Ansprüche genügen, siehe unsere Tests des Acer Chromebook Spin 513 (S. 74) und des Samsung Galaxy Go (S. 98): In diesen Notebooks rechnet jeweils das ARM-SoC Qualcomm Snapdragon 7c, zu dessen „Kryo 468“-CPU auch zwei Kerne gehören, die einem Cortex-A76 gleichen.

Unter Chrome OS schlägt sich dieser ARM-Chip besser als unter Windows 10. Vielleicht ändert sich das ja mit Windows 11. Das könnte im Oktober starten, weil Intel dann die Prozessorgeneration Core i-12000 „Alder Lake“ mit hybriden Kernen bringen dürfte, die vermutlich erst Windows 11 optimal nutzen kann. Einige chinesische Händler verkaufen bereits Vorserienmuster des Intel Core i9-12900K mit je acht „Performance“-(P-) und „Efficiency“-(E-)Kernen der Typen Golden Cove und Gracemont. Laut ersten Benchmarks – die mit Vorsicht zu genießen sind – takten die P-Kerne auf bis zu 5,3 GHz und im Cinebench R20 zieht der Core i9-12900K mit einigen Prozent Vorsprung am AMD Ryzen 9 5950X vorbei. Die Mobilversionen von Alder Lake erwartet man erst zur CES Anfang Januar 2022.

### 128-Kerner für Server

Als Alder-Lake-Konter hat AMD bekanntlich seinen Ryzen mit Stapel-Cache in Stellung gebracht. Mit einem viel größeren Kaliber zielt AMD dann Ende 2022 auf Server: Dann soll nämlich nicht nur der Zen-4-Epyc 7004 „Genoa“ mit 96 Kernen kommen, sondern angeblich auch der 128-Kerner „Bergamo“. Um die Leistungsaufnahme im Zaum zu halten, verzichtet Bergamo möglicherweise auf Simultaneous Multithreading (SMT). Das verspricht auch Vorteile bei der Sicherheit von Cloudservern, weil dann jede Instanz einen oder mehrere physische Kerne exklusiv nutzt. Bei SMT teilen sich zwei oder mehr Threads die Ressourcen eines CPU-Kerns, also Rechenwerke, Register und Caches, was sich für manche Seitenkanalangriffe ausnutzen lässt. Mit diesem Argument verzichtet beispielsweise ARM bei seinen „Neoverse“-Rechenkernen für Server bisher auf SMT. Und solche ARM-SoCs für Cloudserver dürfte AMD mit dem Bergamo ins Visier nehmen: Möglichst viele Kerne pro Server senken Kosten und Energiebedarf in den riesigen Hyperscale-Rechenzentren von Amazon, Microsoft, Google & Co. (ciw@ct.de) **ct**



Im Core i-12000 „Alder Lake“ kombiniert Intel starke „Golden Cove“-Prozessorkerne mit sparsameren „Gracemont“-Kernen. Je acht davon sollen zusammen den 16-Kerner AMD Ryzen 9 5950X schlagen.

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

# Workstations mit Rocket-Lake-Xeons und leistungsstarken Grafikkarten

**Die CPUs der Serie Intel Xeon W-1300 für Single-Socket-Workstations bringen unter anderem PCI Express 4.0 und die Befehlssatz-erweiterung AVX-512. Fujitsu und Lenovo rüsten erste Systeme damit aus.**

Die Workstations Fujitsu Celsius W5011 und Lenovo ThinkStation P350 eignen sich für CAD-Anwendungen, 3D-Design und Videoschnitt. Sie sind unter anderem für Konstruktionsprogramme wie Autodesk AutoCAD und Dassault Solidworks zertifiziert. Ordern lassen sich die Workstations mit Rocket-Lake-Prozessoren der Serien Core i-11000 oder Xeon W-1300 mit bis zu acht Kernen und 5,3 GHz Maximaltakt. Die Xeon-Varianten unterstützen zusätzlich ECC-RAM. Beide CPU-Serien verwenden

PCI-Express 4.0, um SSDs und Grafikkarten schneller anzubinden.

Die Grafikausgabe übernehmen bei den Workstations von Fujitsu und Lenovo Profikarten bis hinauf zur Nvidia Quadro RTX 5000 mit 16 GByte GDDR6-RAM und vier DisplayPorts. Die Hersteller statthen ihre Systeme mit dem W580-Chipsatz aus, der die Management- und Fernwartungsfunktionen von vPro unterstützt. Die maximale Speichermenge der Celsius W5011 und ThinkStation P350 liegt bei 128 GByte DDR4-RAM. Sie sind optional mit Wi-Fi 6 erhältlich. Lenovo bietet die Thinkstation P350 zudem mit Thunderbolt 4 und einem 80-Plus-Platinum-zertifizierten 750-Watt-Netzteil an. Der Verkauf der Workstations soll im Oktober starten. (chh@ct.de)

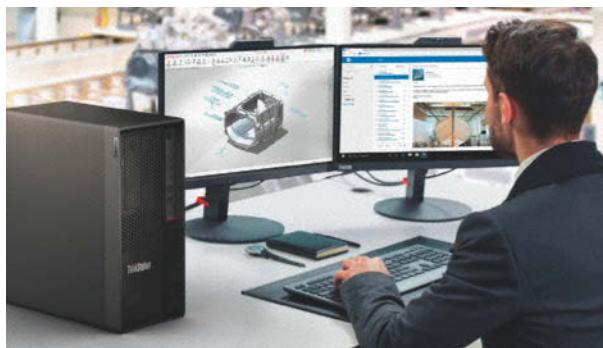


Bild: Lenovo

Die Workstation Lenovo ThinkStation P350 eignet sich dank eingebauter Profigrafikkarten unter anderem für die Konstruktion von Bauteilen.

## Schlanker Prozessorkühler für AMD Ryzen und Intel Core i

Der Tower-Kühler **Shadow Rock Slim 2** von **be quiet!** soll Prozessoren mit bis zu 160 Watt Abwärme kühlen. Diese leiten vier Heatpipes zu den Lamellen. An diesen ist ein PWM-Lüfter mit 13,5 Zentimeter Durchmesser angebracht, der mit maximal 1400 U/min dreht.

Die Lamellen des Shadow Rock Slim 2 sind lediglich 52 Millimeter tief, sodass sich die Speicherriegel auf dem Mainboard auch bei eingebautem Kühler leicht tauschen lassen. Zudem erleichtert das die Montage in kompakten Gehäusen. Der 16 Zentimeter hohe Kühler ist ab sofort für 46 Euro erhältlich. Der Shadow Rock Slim 2 passt auf alle gängigen Prozessoren mit den Fassungen AM4, LGA115X/1200/2066. (chh@ct.de)



Dank großem 13,5-cm-Lüfter soll der Shadow Rock Slim 2 besonders leise arbeiten.

# Hohe PC-Nachfrage

Laut den Marktforschern von Gartner und IDC wuchs die Zahl der neu verkauften Rechner im zweiten Quartal 2021 im Vergleich zum Vorjahreszeitraum um 4,6 beziehungsweise 13,2 Prozent. Je nach Zählweise gingen weltweit zwischen **71,6 und 83,6 Millionen Notebooks und Desktop-PCs** in den Monaten April, Mai und Juni über die Ladentheke. Es besteht also weiterhin eine hohe Nachfrage nach Hardware. Besonders profitiert haben nach Stückzahlen die Hersteller Lenovo, Dell, Apple und Acer.

Zugelegt haben insbesondere Desktop-PCs, weil von der gleichzeitig anhaltenden Komponentenknappe vor allem Notebooks betroffen waren. Dadurch haben sich laut Gartner die Lieferzeiten bei einigen Business-Modellen auf bis zu vier Monaten verlängert. Für die kommenden Monate prognostizieren die Marktforscher weiter steigende Preise bei Komponenten, die die Hersteller bei den fertigen Komplettsystemen aufschlagen werden. Deshalb erwarten Gartner und IDC ein Abflauen des momentanen PC-Booms. (chh@ct.de)

## Kurz & knapp

Der **Nvidia-Grafiktreiber** der Version 471.41 für GeForce-Grafikkarten unterstützt Windows 11 sowie die GPGPU-Schnittstelle CUDA 11.4. Zudem bringt er Optimierungen für die Spiele Chernobylite und Red Dead Redemption 2, die nun auch die KI-Kantenglättungstechnik DLSS nutzen.

Das **Firmware-Update** 613000WD für die PCIe-4.0-SSD WD Black SN850 verbessert die Schreibgeschwindigkeit bei Systemen mit X570-Chipsatz. In den am Chipsatz angebundenen M.2-Slots brach das Übertragungstempo von 5 auf unter 3 GByte/s ein. Das Update hebt die Maximum Payload Size von 128 Bit auf 4 KByte an.

**Download Nvidia-Treiber & WD-SSD-Update:** [ct.de/yfug](http://ct.de/yfug)

## Patriot-SSD VPN100 mit weniger DRAM

**DRAM-Cache soll SSDs auf die Sprünge helfen. Patriot spielt die Bedeutung der Größe solcher Caches jedoch herunter.**

Der SSD-Hersteller Patriot hat in neueren Chargen seiner M.2-PCIe-SSD Viper VPN-100 weniger DRAM eingebaut als in den Spezifikationen angegeben. In den Versionen mit 2 TByte Kapazität soll laut Datenblatt ein DRAM-Cache von 2 GByte verbaut sein, in einigen Fällen aber liegt die Cache-Größe nur bei 512 MByte; die auch hierzulande erhältlichen 1-TByte-Versionen kommen zum Teil mit 256 MByte statt 1 GByte DRAM-Cache. Auch beim Controller gab es unangekündigte Änderungen: Statt des Phison-Controllers E12 sitzt auf den neueren Modellen der E12S.

Die Veränderungen sind auf den ersten Blick nicht ersichtlich, weil die Komponenten unter einem dicken Kühlkörper

verborgen sind. Der Hersteller sieht in den abgespeckten Varianten kein Problem: Der E12S soll trotz weniger Cache die gleiche Leistung bieten wie sein Vorgänger E12, da er nach einem nicht näher benannten neuen Fertigungsprozess hergestellt wurde und zudem mit einer neueren Firmware aufwartet; es handele sich um eine erweiterte Version des E12. Die veränderte VPN100 soll damit beim sequenziellen Lesen und Schreiben die gleichen Werte

erreichen, auch die Zugriffe auf zufällige Adressen und die Ausdauer seien gleich.

Ein Grund für den Komponentenwechsel ist wohl die aktuelle Chipknappheit, die vor allem kleinere Hersteller trifft. Patriot entschuldigt sich für die undokumentierten Veränderungen und verspricht für die Zukunft bessere SSD-Dokumentationen, in denen auch auf etwaige Komponentenwechsel aufmerksam gemacht werden soll. (ll@ct.de)



Der dicke Kühlkörper der Patriot Viper VPN100 verdeckt die SSD-Bauenteile. Ein Komponentenwechsel fällt damit auf den ersten Blick nicht auf.

## Rechenzentrums-Abwärme: Häuser heizen statt in die Luft blasen

Beim Kühlen von Servern in Rechenzentren fällt eine Menge Wärme an, die meistens einfach in die Luft geblasen wird. Durch eine Kooperation des Frankfurter Rechenzentrumsbetreibers Telehouse Deutschland, des Energieversorgers Mainova und des Projektentwicklers Instone Real Estate soll die **Abwärme des Telehouse-Rechenzentrums in Zukunft als Heizwärme dienen**. Mainova will im künftigen Wohnquartier Westville rund 1300 Neubauwohnungen und Gewerbeeinheiten mit der Abwärme des Rechenzentrums versorgen; dort sollen nach den Plänen ab 2023 rund 3000 Menschen leben und arbeiten. Die Abwärme könnte rund 60 Prozent des jährlichen Energiebedarfs von rund 4000 Megawattstunden decken und damit im Vergleich zu konventioneller Wärmeerzeugung rund 400 Tonnen CO<sub>2</sub> im Jahr einsparen.

Das Neubaugebiet ist rund 500 Meter vom Rechenzentrum entfernt und wird zusätzlich an das Fernwärmennetz von Mainova angeschlossen, das vor allem im Winter unterstützen soll. Der Energieversorger zahlt nach eigenen Angaben nichts

für die Abwärme, muss jedoch einen Millionenbetrag für den Bau der Leitungen investieren. Da die Abwärme jedoch nur 30 bis 35 °C beträgt, wird sie ausschließlich zum Beheizen der Wohnungen genutzt. Für die Trinkwasserversorgung und die Duschen wird ein eigenes Netz genutzt, die Temperatur dieses Wassers wird dazu über zwei Großwärmepumpen mit je 320 kW auf 70 °C angehoben.

Nimmt man alle Rechenzentren in Frankfurt zusammen, verbrauchen diese mittlerweile rund eine Milliarde Kilowattstunden Strom pro Jahr und damit mehr als der Frankfurter Flughafen. In den kommenden Jahren soll der Bedarf weiter steigen, rechnerisch könnte bis 2030 der gesamte Wärmebedarf von Haushalten und Büros in der Stadt durch die Abwärme von Rechenzentren gedeckt werden – größtes Problem dabei ist jedoch, Abwärme und potenzielle Verbraucher zusammenzuführen.

Westville gilt deutschlandweit als Pilotprojekt. Zwar gibt es schon ähnliche Projekte, aber keines in dieser Größenordnung. (ll@ct.de)

## Kurz & knapp: Server & Storage

NGD, ein Anbieter von Computational Storage Devices, sieht einen Einsatz seiner rechnenden SSDs auch im Bereich der Kryptowährungen. Das **Berechnen von Chia-Plots** soll durch die Verteilung der Aufgaben deutlich schneller sein als mit einer zentralen CPU.

Der chinesische Halbleiterriese **Tsinghua Unigroup steht vor der Insolvenz**. Eine Zerschlagung des Unternehmens ist jedoch unwahrscheinlich, weil damit Chinas Pläne zum Aufbau einer eigenen NAND-Flash-Fertigung in der Tochterfirma Yangtze Memory Technologies (YMTC) zum Scheitern verurteilt wären.

Acht **PCIe-4.0-SSDs im RAID** nimmt die Adapterkarte AORUS Xtreme Gen4 AIC von Gigabyte auf. Eine mit 4-TByte-SSDs bestückte Karte soll beim Lesen eine Geschwindigkeit von bis zu 28 GByte/s erreichen, beim Schreiben 26 GByte/s.

# Mehr Platz für schnelles WLAN

**Die Bundesnetzagentur hat knapp 500 MHz zusätzliches Spektrum für WLAN und andere Datenfunksysteme freigegeben. Damit können konforme Wi-Fi-6E-fähige Geräte ab sofort in Deutschland betrieben werden.**

24 zusätzliche 20-MHz-Kanäle – entsprechend sechs WLAN-Kanälen der Standardbreite 80 MHz für Wi-Fi 5 und Wi-Fi 6 – passen in das jüngst in Deutschland von der Regulierungsbehörde Bundesnetzagentur für lizenfreie Nutzung freigegebene 6-GHz-Band (5945 bis 6425 MHz).

Die Allgemeinzuteilung „Vfg. 55/2021“ ([ct.de/y5de](http://ct.de/y5de)) sieht wie erwartet

(c't/2021, S. 48) zwei Geräteklassen vor: Low Power Indoor (LPI) und Very Low Power (VLP). Die technischen Rahmenbedingungen für LPI ähneln denen für den unteren 5-GHz-Block (max. 0,2 Watt effektive isotropische Sendeleistung/EIRP, Betrieb nur in Innenräumen, Zügen mit metallbeschichteten Fenstern und Luftfahrzeugen, nicht in Straßenfahrzeugen).

Man darf von Wi-Fi-6E-fähigen LPI-Geräten also eine vergleichbare Performance wie bei 5 GHz erwarten. Die Reichweite wird bei gleicher Datenrate wegen der durch die höhere Frequenz leicht höheren Strecken- und Materialdämpfung (c't 9/2021, S. 138) jedoch etwas geringer sein.

Very-Low-Power-Geräte mit maximal 0,025 Watt EIRP darf man auch in Straßenfahrzeugen und außerhalb nutzen. Sie werden wohl nur für kurze Entfernung auf Sicht taugen.

Österreich muss aufgrund der EU-Harmonisierung ([ct.de/-6111248](http://ct.de/-6111248)) ebenfalls das 6-GHz-Band bis Ende 2021 öffnen. Ein konkreter Termin war bis Redaktionsschluss nicht zu erfahren. Das Bundesamt für Kommunikation der Schweiz (BAKOM) will den Frequenzblock zu gleichen Bedingungen wie in der EU zum 1. Januar 2022 freigeben. (ea@ct.de)

**Allgemeinzuteilung 6 GHz:** [ct.de/y5de](http://ct.de/y5de)

## WLAN-Spektrum in Europa ab 2021

Durch die Öffnung des 6-GHz-Bandes wird das niederfrequente Funkspektrum für WLAN in 48 europäischen Staaten nahezu verdoppelt.



## Sonderheft c't Fritzbox

Viele Büroarbeiten haben sich ins Homeoffice verlagert. Aber den reibungslosen Ablauf müssen viele Router gewährleisten, die man eigentlich für private Zwecke konfiguriert hat. Das Sonderheft schildert, wie man aus den Fritzbox-Routern das Beste herausolt, um geschäftliche Telefonate, Videokonferenzen oder Cloudsynchrosynchronisierungen optimal abzwickeln. Diverse Projekte erweitern den Router an Stellen, die der Hersteller ausgelassen hat, oder erklären, wie sich gebrauchte Fritzboxen zur nützlichen Netzwerkarbeit einspannen lassen.

Im Fokus stehen die Themen Netzwerksicherheit, WLAN-Aufrüstung mit

Blick auf WPA3 und Wi-Fi 6, die Homeoffice- und die Telefonie-Optimierung. Ausgehend von einer gründlichen Konfiguration, die auch spezialisierte Fritzbox-Angreifer abwehrt, kann man sich anhand detaillierter Artikel den Feinheiten der Schwerpunkte widmen, darunter dem Privatsphärenschutz, dem VPN-Aufbau oder der Ankopplung von Business-Telefonen.

Die Print-Ausgabe des Sonderhefts c't Fritzbox ist für 14,90 Euro erhältlich. Die digitale Ausgabe erhalten Sie für 12,99 Euro im heise shop, in unseren Android- und iOS-Apps oder bei Amazon. (dz@ct.de)



## QTS 5.0: Erste Beta verfügbar

Die erste Beta der fünften Version von QNAPs NAS-Betriebssystems QTS steht zum Download bereit: [ct.de/y5de](http://ct.de/y5de)

**Der Linux-Kernel 5.10 bildet den Unterbau der neuen Version.** Damit ist native WireGuard-Unterstützung an Bord. QNAP hat das Protokoll in seine VPN-Verwaltung „QVPN“ integriert, wenige Klicks sollen zum Einrichten genügen.

In puncto KI wurde ebenfalls nachgerüstet: Das System kann per NVMe oder USB angesteckte Edge-TPUs (KI-Beschleuniger) zur flotteren Gesichts- und Objekterkennung in der Netzwerkvideorekordersoftware QVR einspannen. Der „DA Drive Analyzer“ nutzt cloudbasierte KI, um Laufwerksausfälle vorherzusehen und den Administrator zum rechtzeitigen Ersatzteilkauf zu animieren. (amo@ct.de)

# Steam to go

## Steam Deck: Mobile Spielkonsole mit Linux

**Auf der Konsole Steam Deck laufen Linux- und Windows-Spiele aus der Steam-Bibliothek. Dank offenem Konzept lässt sich beliebige Hardware anschließen.**

Von Liane M. Dubowy

Noch im Dezember will Valve die erste Charge seiner mobilen Spielkonsole auf den Markt bringen. Das Steam Deck getaufte Gerät soll ein Linux-Betriebssystem und eine angepasste Steam-Bedienoberfläche mitbringen. Das 7-Zoll-Touchdisplay zeigt eine Auflösung von 1280 × 800 Pixeln. Via USB-C-Port lässt sich das Gerät auch an einen Monitor oder Fernseher anschließen und dann in höherer Auflösung spielen. Eine optionale Dockingstation mit weiteren USB- sowie LAN-, DisplayPort- und HDMI-Schnittstellen soll folgen. Das Steam Deck misst 298 × 117 × 49 Millimeter und wiegt 670 Gramm.

Das Steam Deck wird in drei Varianten erhältlich sein, die sich vor allem in der Größe des Speichers unterscheiden: Das Gerät mit 64 GByte eMMC-Speicherplatz gibt es für 420 Euro, für 256 GByte mit schnellerer NVMe-SSD werden 550 Euro fällig. Die teuerste Ausgabe kostet 680 Euro und bringt eine 512 GByte große NVMe-SSD sowie ein entspiegeltes Display mit. Der Speicherplatz lässt sich bei allen Varianten via MicroSD-Karte erweitern.

### Leistungsfähige Hardware

Im Steam Deck kommt ein angepasster Kombiprozessor von AMD zum Einsatz, der vier Zen-2-CPU-Kerne mit 512 RDNA2-Shader-Kernen kombiniert. Bei der maximalen GPU-Taktfrequenz von 1600 MHz schafft das Steam Deck eine für 3D-Spiele wichtige FP32-Rechenleistung von 1,6 TFlops. Damit lässt es leistungsmäßig die Nintendo Switch beziehungsweise deren angekündigtes



Bild: Valve

OLED-Nachfolgemodell deutlich hinter sich.

Die integrierte RDNA2-Grafik inklusive Raytracing-Unterstützung zusammen mit dem sehr schnellen 16 GByte LPDDR5-Speicher sollte für die derzeit höchste Spieleleistung in diesem Format ausreichen. Allerdings sind speziell durch die Begrenzung der Leistungsaufnahme auf 4 bis 15 Watt keine Wunder zu erwarten.

Steuern lässt sich das Steam Deck mit zwei Thumsticks sowie zwei an den Steam Controller erinnernden Trackpads, die als Mausersatz dienen können. An der Vorderseite sind die vier typischen ABXY-Tasten eingebaut, daneben gibts vier Schultertasten, ein Steuerkreuz und zwei Grifftasten an der Unterseite. Beim präzisen Steuern soll außerdem ein eingebautes Gyroskop helfen. Insgesamt hat das Steam Deck also mehr Eingabemöglichkeiten als viele Spielecontroller. Per Bluetooth oder USB-Klassen sich auch Tastatur und Maus anschließen. Der Speicherplatz ist via MicroSD-Karte erweiterbar. Ein 40-Wattstunden-Akku verspricht mehrere Stunden Spielzeit. Bei weniger anspruchsvoller Verwendung soll der Akku bis zu acht Stunden halten.

### SteamOS 3.0

Valve will das Steam Deck mit dem noch nicht veröffentlichten SteamOS 3.0 ausliefern. Anders als bisherige SteamOS-Versionen soll das System auf Arch Linux basieren. Spiele, die nur für Windows verfügbar sind, sollen darauf mithilfe der Kompatibilitätsschicht Proton laufen [1]. Eine angepasste Steam-Bedienoberfläche stellt neben der Spielebibliothek auch andere Steam-Funktionen wie Chat und Freundesliste bereit. Die Steam-Deck-Oberfläche wird künftig auch auf anderen Geräten den Big-Picture-Modus für die Ansicht an großen Bildschirmen ersetzen.

Cloud-Sync synchronisiert die Spielstände zwischen PC und Steam Deck. Das Steam Deck bringt eine Funktion zum schnellen Pausieren und Fortsetzen mit, sodass ein Druck auf die Powertaste das

System samt Spiel kurzerhand schlafen legt und später an derselben Stelle wieder aufnimmt.

### Rundum offen

Das offene Konzept des Steam Decks bietet viele Möglichkeiten: Statt der ankündigen Dockingstation lässt sich auch eine andere nutzen. Per Bluetooth kann man außerdem Controller und Headsets anbinden. Alle bereits gekauften Spiele aus der eigenen Steam-Bibliothek laufen auch auf der Konsole; exklusive Spiele wie bei der Nintendo Switch soll es nicht geben.

Außerdem ist das Steam Deck ein vollwertiger PC: Man kann es an einen großen Bildschirm anschließen, beliebige Software darauf installieren und das System zum Surfen, Filme schauen oder für anderes benutzen. Sogar andere Spiele-Shops lässt Valve auf dem Gerät zu, man muss sie nur selbst installieren. Dass die meisten Hersteller keine Linux-Version ihrer Software bereitstellen, dürfte halbwegs findige Gamer nicht davon abhalten, ihre Spiele auf dem Steam Deck zu spielen. Open-Source-Tools wie Lutris [2] oder der Heroic Games Launcher erleichtern Installation und Start der Spiele von GOG.com oder Epic Games. Mit Emulatoren können sie das Gerät sogar zur Retrokonsole machen. Via Browser sind auch Cloud-Gaming-Dienste wie Google Stadia oder GeForce Now verfügbar.

Das Interesse der Gamer-Gemeinde ist groß: Zum Start der Reservierungen am 16. Juli 2021 kam es durch den Ansturm auf den Steam-Store immer wieder zu Verbindungsabbrüchen und Fehlermeldungen.

(lmd@ct.de) ct

### Literatur

[1] Liane M. Dubowy, Läuft einfach, Windows-Spiele unter Linux mit Proton, c't 8/2021, S. 164

[2] Liane M. Dubowy, Alles unter einem Hut, Open-Source-Spieleplattform für Linux, c't 17/2016, S. 150

**Steam-Deck-Website & Artikel:**  
[ct.de/yz3m](http://ct.de/yz3m)

# Proxmox eilt Debian voraus

**Die neue Hauptversion des Hypervisor Proxmox baut auf Debian 11 „Bullseye“ auf, das sich noch in der „testing“-Phase befindet. Proxmox 7 wartet mit der Objektspeicherlösung Ceph 16.2 sowie allerlei Annehmlichkeiten in der Weboberfläche auf.**

Während Proxmox 6.x noch auf Debian 10 „Buster“ basierte, vollzieht die Version 7 nun den Wechsel zu Debian 11 „Bullseye“. Allerdings gibt die Proxmox Server Solutions GmbH aus Wien Proxmox VE 7 schon frei, obwohl Debian 11 noch in der „testing“-Phase steckt. Gegenüber c't erklärte das Unternehmen, die relevanten Debian-Pakete seien bereits stabil und die Kernel-pakete von Proxmox wie Kernel, ZFS, Ceph, LXC und QEMU pflege man ohnehin selbst. Thomas Lamprecht, leitender Entwickler bei Proxmox, erläutert zudem in der Pressemitteilung, das Debian-Projekt habe das Release-Datum von Debian 11 aufgrund eines Bugs im Installer verschoben (siehe ct.de/yq3y). Weil Proxmox einen eigenen Installer verwendet, der nicht von dem Fehler betroffen ist, habe man sich entschieden, Proxmox 7 bereits zu veröffentlichen.

Abgesehen vom Debian-11-Unterbau und dem neueren Linux-Kernel 5.11 gibt

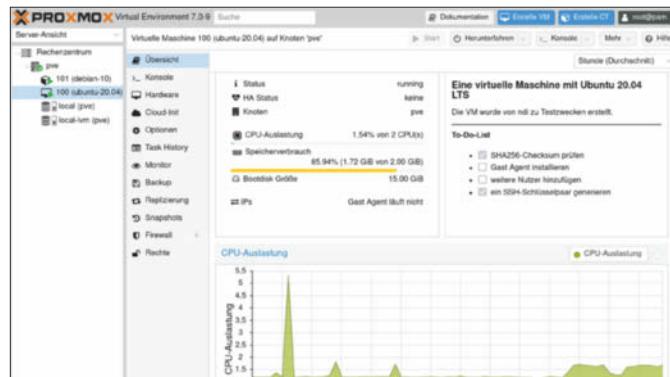
es wichtige Neuerungen im Storage-Bereich. Proxmox 7 liefert die aktuelle Version 16.2 „Pacific“ des Objektspeichersystems Ceph aus. Das Balancer-Modul ist bei neuen Clustern nun standardmäßig aktiviert und soll zu einer gleichmäßigeren Auslastung der Object Storage Devices (OSD) führen. Btrfs ist als „Technology Preview“ mit an Bord.

Paketquellen lassen sich nun direkt im GUI verwalten und müssen nicht mehr mit einem Texteditor im Verzeichnis /etc/apt bearbeitet werden. Proxmox lädt ISO-Dateien jetzt auch über eine Webadresse und verifiziert bei Bedarf direkt die SHA256-Prüfsumme. OpenID Connect

ergänzt die bisherigen Authentifizierungsmethoden wie pam und LDAP. Die Notizen zu VMs und Containern können Administratoren nun in Markdown verfassen.

Zur Vorbereitung des Upgrades von Proxmox 6.4 auf Proxmox 7 stellen die Entwickler das Checklist-Tool „pve6to7“ bereit, das potentielle Fehlerquellen identifiziert (siehe ct.de/yq3y). Zusätzlich zu Proxmox VE 7 gibt die Proxmox Server Solutions GmbH die verwandten Produkte Proxmox Mail Gateway 7.0 und Proxmox Backup Server 2.0 frei. (ndi@ct.de)

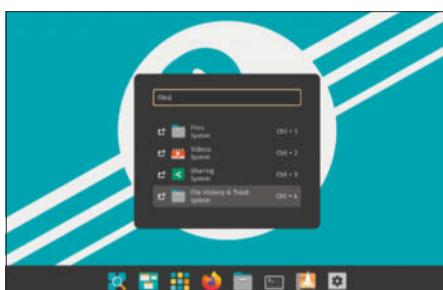
**Pressemitteilung, Upgrade-Anleitung:**  
[ct.de/yq3y](http://ct.de/yq3y)



**Das überarbeitete Notizfeld kann jetzt Markdown interpretieren und als HTML darstellen. So lassen sich Informationen über VMs und Container schnell erfassen.**

# Pop!\_OS 21.04 erstmals mit Cosmic Desktop

Das US-Unternehmen System76 stellt Linux-Notebooks, -Workstations und -Server her. Die Geräte liefert der Hersteller wahlweise mit Ubuntu oder der hauseigenen Distribution Pop!\_OS aus, die auch außerhalb der System76-Kundschaft eine Fangemeinde hat. Das neue Pop!\_OS 21.04 basiert auf Ubuntu 21.04 und verzichtet ebenso auf Gnome 40. Bei der Be-



Mit Cosmic und neuen Features wie dem Launcher geht Pop!\_OS eigene Wege bei der Bedienoberfläche.

dienoberfläche hebt sich Pop!\_OS allerdings mit dem Cosmic Desktop vom Ubuntu-Vorbild ab. Bei Cosmic handelt es sich um ein stark modifiziertes Gnome 3.38, das durch diverse Erweiterungen für eine eigene Nutzererfahrung sorgen soll.

Während Gnome 3.38 das Anwendungsraster und die virtuellen Arbeitsflächen in der Aktivitätenübersicht zusammenfasst, teilt Cosmic diese in zwei getrennte Ansichten auf. Nutzer rufen diese über die Schaltflächen „Workspaces“ und „Anwendungen“ im Panel am oberen Bildschirmrand oder Icons im Dock auf. Die vertikal angeordnete Liste der virtuellen Desktops befindet sich auf der linken Seite. Das Dock platziert Cosmic standardmäßig am unteren Rand der Bedienoberfläche. Ein Mausklick auf das Lupen-Icon im Dock oder die „Super“-Taste („Windows“-Taste) auf der Tastatur öffnet den neuen Anwendungs-launcher. Der startet nicht nur Apps, son-

dern findet auch Dateien und Ordner, löst Rechenaufgaben und dient als Suchmaschine, wenn man ein Präfix vor dem Suchbegriff verwendet (beispielsweise „ddg“ für DuckDuckGo). Wer Tiling-Window-Manager bevorzugt, kann die automatische Anordnung von Fenstern mit der Schaltfläche „Tile Windows“ im Top-Panel aktivieren.

Von Ubuntu 21.04 erbt Pop!\_OS 21.04 die Basispakete und den Linux-Kernel 5.11. Nutzer von Pop!\_OS 20.10 sollten sich mit dem Upgrade nicht zu lange Zeit lassen. Die Version erreicht noch im Juli das Ende ihres Lebenszyklus und wird danach nicht mehr mit (Sicherheits-)Aktualisierungen versorgt. Im Downloadbereich der System76-Webseite steht ein Installationsimage für AMD/Intel-Systeme sowie ein Abbild mit proprietären Nvidia-Treibern zur Verfügung (siehe ct.de/yq3y). (ndi@ct.de)

**Download Pop!\_OS 21.04:** [ct.de/yq3y](http://ct.de/yq3y)

# Wissen(schaft) nicht nur für Journalisten

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

In der Coronapandemie hat die mediale Aufmerksamkeit für wissenschaftliche Themen stark zugenommen. Forscher wie der Virologe Prof. Christian Drosten kritisieren, dass Journalisten zugunsten von schnellen Schlagzeilen Themen nicht durchdringen und mitunter grob verzerrt berichten. Wirklich neu ist dieses Phänomen nicht. Bereits seit 2015 versucht das **Science Media Center** (SMC), mit schneller Expertise gegenzuhalten.



In der teils stiftungsfinanzierten, gemeinnützigen GmbH sind fast 1000 Wissenschaftler aktiv. Das SMC will nach eigener Aussage „als Intermediär zwischen Wissenschaft und Journalismus, zwischen Forschenden und Medienschaffenden“ fungieren. Und das geht so: Ein Ereignis, eine Studie oder einfach nur Politikaussagen führen dazu, dass ein bestimmtes wissenschaftliches Thema plötzlich in die Schlagzeilen gerät. Die SMC-Redaktion recherchiert dazu und bittet akkreditierte Experten um Einschätzung und Erklärungen, die dann veröffentlicht werden.

Gerade in der Pandemie stützte das SMC Journalisten mit schnellen, profunden und vor allem zitierfähigen Statements. Da geht es mal um eine Einordnung der Delta-Variante des Coronavirus, dann wieder darum, die Änderungen von Empfehlungen der Ständigen Impfkommission zu erläutern. Nicht nur den Medien helfen die vielen Artikel, sondern jedem, der ein wenig hilflos vor der Nachrichtenflut steht und nicht mehr recht weiß, was er glauben soll. Ein wichtiger Baustein gegen die Desinformationsflut, auch in den traditionellen Medien.

(hob@ct.de)

## Google-Friedhof

<https://killedbygoogle.com>

Wenn Google einen Kurznachrichtendienst wie Twitter startet: Würden Sie ihn nutzen? Tja, Chance verpasst, den gabs nämlich tatsächlich unter dem Namen „Jaiku“ – mangels Erfolg 2012 eingestellt. Und falls Google Slack klont und auf den Desktop

bringt? Auch das gabs bereits: „Pie“ wurde 2016 nach drei erfolglosen Lebensjahren von Google beerdigt.

Unter **Killed by Google** listet der Entwickler Cody Osgood all die gescheiterten Experimente auf, die Google seit 2003 gestartet hat – inklusive Grabsteinen und Kurzbeschreibungen. Bis Juni 2021 sind 203 Projekte zusammengekommen. Diese geballte Sammlung zeigt, wie viel Google probiert und wie wenige Dienste es tatsächlich schaffen, sich dauerhaft zu etablieren. Frappierend: Nahezu alle Versuche scheiterten, abseits vom zugekauften YouTube selbst ein soziales Medium ins Leben zu rufen.

Für Google ist die amüsante Sammlung wenig schmeichelhaft, zeigt sie doch, dass man immer wieder Early Adapters vor den Kopf stößt, wenn ein Dienst nicht rentabel ist. Im April 2020 hat Google Osgood dessen Aussage zufolge sogar angeboten, ihn einzustellen, wenn er dafür die Site aufgibt. Er habe dankend abgelehnt. (hob@ct.de)

## Politikeranalyse in Echtzeit

<https://interaktiv.tagesspiegel.de/lab/social-media-dashboard-bundestagswahl-2021/>

Die Berliner Zeitung Tagesspiegel verwandelt zusammen mit der NGO Democracy Reporting International Daten zur Bundestagswahl 2021 in spannende, aufschlussreiche Grafiken: Das **Social Media Dashboard** zeigt nahezu in Echtzeit Aktivitäten der Politiker und Parteien in den sozialen Medien.



Zum Start am 12. Juli haben sich die Machterben zunächst auf die Spitzenkandidaten fokussiert. So erfährt man beispielsweise, dass FDP-Chef Christian Lindner die mit Abstand größte Gefolgschaft auf Twitter hat, SPD-Kandidat Olaf Scholz aber in den letzten Wochen wesentlich aktiver war. Das Dashboard zeigt, welche Postings besonders viel geteilt wurden, und sogar, welche Emojis die Politiker am meisten nutzen.

Nach Angaben des Tagesspiegels werden die Daten zu Postings auf Instagram und Facebook über ein API von Facebooks CrowdTangle abgerufen. Zur Twitter-Analyse nutzt man das Twitter-API, und auch YouTube bietet ein API, das Echtzeit-Daten zu geposteten Videos bereitstellt. Gefördert wird das Projekt von der Stiftung Mercator. Das Dashboard soll in den Wochen vor dem 26. September immer mal wieder um weitere Themensegmente ergänzt werden. (hob@ct.de)

Diese Seite mit klickbaren Links: [ct.de/yjf5](http://ct.de/yjf5)



## USB-C Kracher

Art.Nr. UCH.180.SC

- Adapterkabel UHD 4K@60Hz
- USB Typ-C-Stecker auf HDMI Typ-A-Stecker
- HDCP 2.2 konform



### USB-C AUF HDMI STECKER

\* Gültig für das gezeigte USB-C Adapterkabel innerhalb des Aktionszeitraumes. Nur solange Vorrat reicht.

**WIR.  
VERBINDEN.  
TECHNIK.**



Express bis 14 Uhr bestellt –  
Versand noch am selben Tag\*\*

\*\* Mo - Fr. Warenverfügbarkeit vorausgesetzt



Netzwerk | Multimedia | Installation | Elektro | Werkzeug

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

# Kartentricks

**notebooksbilliger.de verweigert Rücknahme defekter Grafikkarte**



**Wenn eine gelieferte Ware Mängel aufweist, erwartet man vom Verkäufer zu Recht, dass er den Mangel rasch beseitigt oder den Kaufpreis erstattet. Bei notebooksbilliger.de will man das Nachbessern endlos versuchen – zu oft und zu lange für den enttäuschten Kunden.**

**Von Tim Gerber**

**M**itte November 2020 kaufte das Ehepaar Hanna und Jan O. für mehr als 1200 Euro bei ihrem Lieblingsshop notebooksbilliger.de ein. Mit den Komponenten sollte der PC von Hanna O. aufgerüstet

und spieletauglich gemacht werden. Dazu befand sich auch eine Grafikkarte vom Typ Radeon RX 5700 XT für 436 Euro auf ihrer Einkaufsliste.

Doch die Freude nach dem Zusammenbau hielt sich in Grenzen, immer wieder kam es zu Abstürzen mit Fehlermeldungen, die auf Probleme mit der Grafikkarte hindeuteten. Deshalb wandten sich die O.s am 5. Januar an den Verkäufer und schilderten ihm, dass die von ihnen erworbene Grafikkarte absolut willkürlich abstürze, woraufhin die Fehlermeldung „AMD Treiber Timeout“ angezeigt werde. Unterschiedliche Spiele wie „Assassin’s Creed Valhalla“, „Life is Strange“ und andere von verschiedenen Plattformen stürzten bis zu sechsmal hintereinander ab. Der Monitor gehe dann aus und wieder an, die Fehlermeldung erscheine und oftmals bleibe der Desktop

komplett verpixelt, sodass ein Neustart unausweichlich sei.

Ausführlich beschrieben die beiden auch, dass sie zur Behebung des Problems bereits Windows 10 sowie den Grafikkartentreiber neu installiert und auch eine ältere Version der Treiber getestet hätten. Außerdem hätten sie unterschiedliche Monitore angeschlossen, die BIOS-Einstellungen überprüft und verschiedene DisplayPort-Anschlüsse ausprobiert. Doch alles vergeblich.

Auf ihre Reklamation erhielten sie noch am selben Tag einen Retourenschein und sandten die Grafikkarte nebst der gewünschten ausführlichen Fehlerbeschreibung an notebooksbilliger.de. Versuche, sich anschließend telefonisch über den Stand der Bearbeitung zu erkundigen, scheiterten an einer überlasteten Hotline. Nach zwei Wochen vergeblichen Wartens

war die Geduld der O.s erschöpft. Sie kauften ebenfalls bei notebooksbilliger.de eine weitere Grafikkarte, dieses Mal vom Typ MSI Geforce RTX 3060 TI Gaming X Trio für 630 Euro. Diese funktionierte in dem PC von Hanna O. völlig ohne Problem und Abstürze. Alle Spiele, die zuvor Grafikfehler zeigten, lieferten nun ein einwandfreies Bild.

Am 28. Januar, also drei Wochen nach der Einsendung, kam die reklamierte Grafikkarte wieder bei Hanna und Jan O. an. „Ohne Nachbesserung“, hieß es in dem Begleitschreiben der Werkstatt, weil kein Fehler gefunden worden sei. Doch im PC von Hanna O. zeigte die Grafikkarte unverändert dieselben Macken. Deshalb wandte sie sich noch am selben Tag erneut an notebooksbilliger.de und beschrieb erneut den Fehler. Auf Bitten des Kundenservice sandte sie auch mehrere Bilder, einen Screenshot von den Fehlermeldungen bei Abstürzen und mehrere Fotos von den Pixelfehlern in der Spieldrafik. Außerdem teilte sie dem Webshop mit, dass die ersatzweise ebenfalls dort erworbene Grafikkarte ja keinerlei Probleme verursache, mithin ein Defekt der Grafikkarte vorliegen müsse. Sie bat deshalb um Rücknahme und Erstattung des Kaufpreises.

Das lehnte notebooksbilliger.de jedoch mit E-Mail vom 4. Februar ab. Man bedauerte zwar den Ärger, den die Kunden mit dem Gerät hätten, doch: „Bevor wir einen Rücktritt vom Kaufvertrag einleiten, behalten wir uns zwei fehlgeschlagene Nachbesserungen vor. Eine Nachbesserung bezieht sich in solch einem Fall auf einen reinen Hardwaredefekt des Gerätes“, hieß es in dem Schreiben. Wenn Hanna O. einverstanden sei, werde man die Grafikkarte also ein zweites Mal prüfen. Zähnekirschen sendete die Kundin das Bauteil am 9. Februar also erneut an den Verkäufer.

Nach über einem Monat, am 12. März, kam die Grafikkarte wieder bei ihr an. Diesmal sei der Fehler behoben worden, hieß es in der denkbar knappen Anmerkung der Werkstatt. Trotzdem verursachte die Grafikkarte noch immer dieselben Fehler, wie sich nach Einbau der Karte in den PC von Hanna O. schnell herausstellte.

Am 18. März wandte Hanna O. sich deshalb nun ein drittes Mal an den Kundenservice von notebooksbilliger.de und bat nun endgültig um Rücknahme der de-

fekten Grafikkarte und Erstattung des Kaufpreises. Schließlich hatte der Verkäufer nun zwei Chancen gehabt, ihnen eine funktionierende Grafikkarte zu liefern. Umso erstaunter war Hanna O. über die Antwort, die sie wenige Stunden später erhielt: Abermals lehnte notebooksbilliger.de die Rücknahme ab und wies darauf hin, dass man sich zwei Nachbesserungsversuche vorbehalte. „Bisher hat erst eine Reparatur stattgefunden. Während der ersten Einsendung konnte kein Mangel festgestellt werden.“

**VOR  
SICHT  
KUNDE!**

Das wollte Hanna O. nicht akzeptieren und schrieb noch am selben Tag an den Verkäufer, dem sie und ihr Mann seit vielen Jahren treu waren: „Wie kann es sein, dass das defekte Gerät beim ersten Mal ohne Nachbesserung wieder an uns zurückgeschickt wurde, wenn doch beim zweiten Mal ganz offensichtlich eine Reparatur desselben Artikels stattgefunden hat?“, wollte die enttäuschte Kundin wissen. Die von ihr geschilderten Mängel seien offenbar nicht ordentlich seitens der Techniker geprüft worden. „Ich bin seit nunmehr drei Monaten mit der Rückgabe einer defekten Grafikkarte beschäftigt, die wir in drei unterschiedlichen Computern eingebaut haben und die immer wieder die gleichen Mängel zeigt“, beanstandete Hanna O. und bat den Verkäufer, seine Definition von „zweiter Nachbesserung“ zu überprüfen.

### Aus drei mach zwei

Doch das ließ den Händler völlig unbeeindruckt: „Eine Nachbesserung besteht, wenn der Artikel repariert wurde“, schrieb er am 19. März an die verblüffte Kundin. „Kommt das Gerät zurück, weil der Hersteller den Mangel nicht reproduzieren konnte, kann hierbei nicht von einer Nachbesserung gesprochen werden. Bisher sind von Ihnen zwei Einsendungen erfolgt. Bei der Ersten konnte der Hersteller den Mangel nicht reproduzieren. Demnach hat leider auch keine Nachbesserung stattgefunden.“

Von dieser Auffassung ließ sich notebooksbilliger.de auch im weiteren Verlauf nicht abbringen. Am 27. März sandte das Ehepaar O. die defekte Grafikkarte nunmehr zum dritten Mal an den Verkäufer zurück und forderte ihn ultimativ auf, den Kaufpreis zu erstatten, da er bereits zwei

erfolglose Nachbesserungsversuche unternommen hätte. Doch das half nichts. Am 23. April schickte der Händler ihnen eine neue Grafikkarte des gleichen Typs zu. Das Gerät sei im Zuge der Nachbesserung „durch den Servicepartner getauscht“ worden, hieß es im Begleitschreiben. notebooksbilliger.de sah den Fall damit offenbar als erledigt an; auf weitere Schreiben reagierte der Shop nicht.

Jan O. wandte sich am 24. Juni an die c't-Redaktion und schilderte uns die Reklamationsodyssee. Am 28. Juni fragten wir bei der Pressestelle von notebooksbilliger.de an und wollten vor allem wissen, wie man dort zu der Ansicht gekommen sei, dass die erste Einsendung kein Nachbesserungsversuch gewesen sei. Schließlich trägt der Verkäufer in den ersten sechs Monaten die Beweislast dafür, dass er eine mangelfreie Sache geliefert hat. Dass dies nicht der Fall war, zeigt sich schon daran, dass die Grafikkarte beim zweiten Versuch nach Angaben von notebooksbilliger.de repariert und beim dritten Mal ganz ausgetauscht wurde. Demnach war die den O.s im November gelieferte Grafikkarte offenbar von Anfang an mangelhaft. Bei notebooksbilliger.de hatte man also bereits bei der ersten Einsendung alle Chancen, den Fehler zu finden und zu beseitigen. Ob der Versuch an einer falschen Diagnose scheitert oder an einem unauglichen Reparaturversuch, ist rechtlich ohne Belang. Spätestens nach dem zweiten erfolglosen Versuch im Februar waren die Kunden zum Rücktritt berechtigt.

Das hat am Ende auch notebooksbilliger.de einräumen müssen. „Da das bemängelte Symptom hier – offenbar wegen des Mangels – erneut auftrat, müssen wir in diesem Fall einen Fehler eingestehen, der uns aufrichtig leidtut“, antwortete ein Pressesprecher am 29. Juni auf unsere Anfrage. Man habe sich daher „dafür entschieden, der Rücktrittserklärung zu entsprechen, den Kauf rückabzuwickeln und den O.s den vollständigen Kaufpreis zu erstatten. In Zukunft werden wir unsere Mitarbeiter\*innen auf ein kulanteres Vorgehen hin schulen, um deutlich zeitnaher zu diesem Ergebnis zu gelangen.“

Inzwischen haben die O.s tatsächlich den vollen Kaufpreis erstattet bekommen. Vom bisherigen Händler ihres Vertrauens sind sie dennoch enttäuscht. Schließlich kann man nicht jedes Mal erst die Presse einschalten, wenn bei einer Hardwarebestellung nicht alles funktioniert, wie es eigentlich sollte. (tig@ct.de) ct

# Homeoffice to go

**Mobiles Arbeiten wird zum neuen Normalfall – und bringt Angestellten ungeahnte Freiheiten**



- Die neuen Freiheiten für Angestellte ..... Seite 56**
- Wie Konzerne das mobile Arbeiten sehen .... Seite 62**
- FAQ: Die rechtlichen Grundlagen ..... Seite 64**
- Datentarife und mobile Router ..... Seite 66**
- Effizient arbeiten mit mobilen Monitoren .... Seite 70**
- Videokonferenzen unterwegs ..... Seite 72**

# Früher konnte nur wenige Menschen nach Lust und Laune entscheiden, wo sie arbeiten. Seit Corona haben plötzlich viele Angestellte diese Freiheit – und immer mehr nutzen das auch aus.

Von Katja Seidel und Christian Wölbert

**V**or fünf Jahren kündigte Thilo Vogel seine Wohnung und zog in seinen Ford Mondeo Kombi. Seitdem tourt er durch Europa. Er schläft im Dachzelt und arbeitet auf der Rückbank, als Kühlschrank dient ihm die Reserveradmulde. Anfangs verdiente der studierte Ingenieur sein Geld vor allem als Porträtfotograf, mittlerweile führt er aus seinem Auto heraus ein kleines Unternehmen – mit Zoom-Calls, Google Docs und WhatsApp-Sprachnachrichten. „Ich kann ständig auf Reisen sein, Land und Leute kennenlernen, und arbeiten von wo ich möchte“, sagt er im Gespräch mit c’t.

Arbeiten, wo man möchte: Diese Freiheit hatten bis vor kurzem nur wenige Menschen, vor allem Selbstständige wie Vogel. Dann kam Corona und hat dazu geführt, dass nun auch viele Angestellte frei entscheiden können, wo sie ihr Notebook aufklappen. Jeder kann plötzlich ein biss-

chen Digitalnomade sein, auch ohne direkt die Wohnung komplett aufzugeben: Arbeiten geht im Schrebergarten oder bei den Schwiegereltern, im Co-Working-Space oder im Camper.

Während der Lockdowns waren Informationsarbeiter zwar in den eigenen vier Wänden gefangen, abgesehen von gelegentlichen Bürobesuchen. Doch nun, nach dem Auslaufen der Homeoffice-Pflicht Ende Juni, ergeben sich plötzlich ungeahnte Freiheiten. Technisch gesehen ist es schließlich egal, ob man von zu Hause aus an einer Videokonferenz teilnimmt oder aus einer Ferienwohnung.

Auch die formellen Hindernisse bröckeln. Bereits 2019 erlaubten laut einer Umfrage des Instituts der deutschen Wirtschaft (IW) 43 Prozent aller deutschen Unternehmen ihren Beschäftigten „ortsunabhängiges Arbeiten über mobiles Internet“. „Man kann davon ausgehen, dass dieser Anteil nun noch einmal deutlich gestiegen ist“, sagt Oliver Stettes, Leiter des Bereichs Arbeitsmarkt und Arbeitswelt beim IW.

Denn seit Beginn der Coronazeit haben noch mehr Firmen ihre Angestellten mit Notebooks ausgestattet und Meetings durch Videokonferenzen ersetzt. Und Unternehmen, die Unterwegsarbeiten erlauben, schreiben in der Regel keine bestimmten Orte dafür vor. Hauptsache, man ist erreichbar und produktiv. Die Unterschiede liegen eher im Umfang: Manche Firmen gewähren nur einen Tag pro Woche, andere geben gar keine Grenze vor (mehr zu den rechtlichen Rahmenbedingungen lesen Sie in unserer FAQ auf S. 64).

Viele Angestellte kosten diese neuen Möglichkeiten nun erstmals aus. Die Gründe dafür sind so unterschiedlich wie die Menschen selbst. Manche wollen einfach mehr Zeit mit Freunden und Verwandten verbringen, andere direkt nach Feierabend aufs Surfbrett steigen.

## Mit Sitzball, Monitor und Schreibtischaufsatz

Bei Sebastian Raab ist es die Beziehung, die ihn zum MobiArbeiter gemacht hat: Seine Partnerin wechselt berufsbedingt alle drei Monate ihren Arbeitsort innerhalb Deutschlands. Oft erfährt sie nur mit wenigen Tagen Vorlauf, in welche Stadt es als Nächstes geht. Raab zieht von Station zu Station zu Station mit. „So können wir zusammen sein. Und wir finden es spannend, unterschiedliche Regionen kennenzulernen“, sagt der IT-Berater und Ingenieur.

Für Raabs Arbeitgeber, ein international tätiges Beratungsunternehmen, ist



**Frei wie Thilo Vogel:**  
Der Fotograf, Ingenieur und Abenteurer lebt und arbeitet in seinem Ford Mondeo.

# Ein Camper als mobiles Büro

**Die IT-Beraterin, Fotografin und Bloggerin Katja Seidel arbeitet überwiegend in ihrem Ford Nugget. Hier beschreibt sie ganz subjektiv die Vorzüge ihres rollenden Arbeitsplatzes.**

Anfang 2020 hatte ich einen klaren Plan: Mein Camper sollte mein dauerhafter Hotel- und Büroersatz auf Dienstreisen werden. Also richtete ich mir auf der Rückbank und dem kleinen Tisch den für meine Bedürfnisse perfekten PC-Arbeitsplatz ein: mit drei bis vier Monitoren (Notebook plus zwei bis drei portable Bildschirme), iPad, Webcam, Leuchten und Hintergrund für Videokonferenzen, Bluetooth-Konferenztelefon und weiteren Gadgets. Ein Solarpanel, einen mobilen Akku mit Steckdosen für 230-Volt-Geräte (Powerstation) und einen LTE-Router samt externer Antenne hatte ich zuvor schon besorgt [2].

Die Investition schien sich bezahlt zu machen. So konnte ich aus Dienstreisen echte Reisen machen, nach Kundenterminen in inspirierenden Umgebungen weiterarbeiten und nach Feierabend Auszeiten in der Natur genießen.

Durch die Corona-Beschränkungen im Frühjahr 2020 war es dann jedoch vorbei mit der Abwechslung und dem Reisen, und es warteten neue Herausforderungen. In meinem Fall war dies der Mangel an geeigneten Arbeitsplätzen im Haus. Also warum nicht einfach das sogenannte schon eingerichtete mobile Büro

im Camper als stationäres Homeoffice nutzen? Das ging besser als gedacht.

Ein großer Vorteil war die Ruhe in meinem Einzelbüro, die ich für Videokonferenzen und konzentriertes Arbeiten sehr zu schätzen gelernt habe. Und auch wenn es für Außenstehende befremdlich wirken möchte, dass ich jeden Tag in meinem Camper in der Hofeinfahrt arbeite, so hatte ich zumindest einen ergonomischen Heimarbeitsplatz als viele Kollegen. Bei einigen musste der Keller, die Küche oder sogar die Couch als Büro herhalten.

Außerdem hatte ich einen entscheidenden Vorteil: Mein Büro war weiterhin mobil, sodass ich mir bei Bedarf die für mich so wichtige Abwechslung schaffen konnte. Je nach Pandemielage blieb ich nur einige Tage an einem Ort, manchmal einige Wochen.

Genau genommen war ich sogar noch unabhängiger als vorher, da ich mich bis auf wenige Ausnahmen im Sommer 2020 nicht mehr nach Vor-Ort-Kundenterminen richten musste. Natürlich bin ich während der Pandemie nicht so frei gereist wie bisher, aber schon die taegewisse Verlagerung des Arbeitsplatzes an einen inspirierenden Ort in der Natur hat unglaubliche Auswirkungen auf die eigene Psyche und Kreativität. Steht man dabei neben einem See oder Fluss und kann nach Feierabend eine Runde mit dem Standup Paddle Board drehen, macht sich ein Urlaubsgefühl breit.

Für eintägige Fluchten aus dem Alltag eignen sich Wald- und Wanderpark-

plätze, solange der Internetempfang stimmt. Der Strombedarf hält sich für einen Tag in Grenzen, sodass in der Regel die Standardbatterien im Camper ausreichen.

Längere Aufenthalte mit Übernachtungen außerhalb offizieller Stell- und Campingplätze wurden während der Pandemie zur Herausforderung. Ursachen dafür waren der unglaubliche Boom der Campingbranche und die Tatsache, dass manche Camper aufgrund von Beherbergungsverboten auf normale Parkplätze ausgewichen sind.

Überfüllte und vermüllte Plätze hatten dann verschärzte Kontrollen und zahlreiche neue Verbote zur Folge, von denen einige wohl leider auch die Pandemie überdauern werden. Aber auch ein offizieller Stellplatz oder Campingplatz kann ein wunderbarer Arbeitsplatz sein. So habe ich mir – entgegen meiner bisherigen Reisephilosopie – des Öfteren einen schönen Naturstellplatz gesucht, auf dem ich für eine oder zwei Wochen gearbeitet und entspannt habe. Ein weiterer Vorteil neben dem legalen Stehen ist hier die Stromversorgung.

Ein solcher Tapetenwechsel war während der Pandemie wahnsinnig wichtig und wertvoll. Ich verschaffe mir damit Urlaubsfeeling, ohne monatlang auf den wirklichen Urlaub warten zu müssen. Im Hinblick auf die eigene Kreativität, Motivation und Zufriedenheit kann man solch eine Möglichkeit gar nicht hoch genug bewerten.



Bild: Katja Seidel



Bild: Katja Seidel

**Während der Coronazeit noch unabhängiger als zuvor:  
IT-Beraterin Katja Seidel in ihrem mobilen Büro.**

**Kein Kompromiss, sondern ein vollwertiges mobiles Büro:  
Der Arbeitsplatz im Ford Nugget von Katja Seidel.**

dieses ungewöhnliche Lebensmodell kein Problem. Es gewährt Mitarbeitern seit ungefähr einem Dreivierteljahr noch mehr Freiheiten bei der Ortswahl als zuvor schon. Die Berater können innerhalb Deutschlands frei wählen, solange sie die Ansprüche der Kunden sowie Bedingungen wie Datenschutz und Erreichbarkeit erfüllen.

Über die Ausstattung für sein mobiles Homeoffice hat Raab sich viele Gedanken gemacht, denn seine gesamte Ausrüstung muss ins Auto passen und schnell eingepackt sein. „Es geht um den besten Kompromiss aus Mobilität und Arbeitskomfort“, sagt er.

Da es in Airbnb-Wohnungen normalerweise keinen Drehstuhl gibt, hat er sich einen aufblasbaren Sitzball gekauft. Zwei weitere wichtige Anschaffung war ein Aufsatz, der jeden Küchentisch in einen höhenverstellbaren Schreibtisch verwandelt. Der Aufsatz wiegt fast zehn Kilogramm. Raab möchte ihn aber nicht mehr missen. Er absolviert inzwischen alle Videokonferen-

zen, die etwa ein Drittel seiner Arbeitszeit ausmachen, im Stehen. „So wirkt man agil und energiegeladen.“ Obendrein profitiert sein Rücken vom häufigen Wechsel zwischen Stehen und Sitzen [1].

Die meisten Ferienwohnungs-WLANS sind nach Raabs Erfahrung nur eingeschränkt für mobiles Arbeiten zu gebrauchen. Mal gab es häufig Abbrüche, mal reichte die Abdeckung nicht. Er nutzt deshalb häufig sein Smartphone als Hotspot oder surft über das Mobilfunkmodul seines Dienst-Notebooks. Das monatliche Inklusiv-Volumen seiner beiden Mobilfunkverträge liegt insgesamt bei 65 GByte – zumindest bislang reichte das immer aus (unsere Tipps zur Auswahl eines passenden Mobilfunktarifs lesen Sie ab S. 66). Dank seines externen Monitors hat er auch genügend Bildschirmfläche für die Arbeit mit mehreren Anwendungen (einige besonders portable Bildschirme stellen wir ab S. 70 vor).

Als Handicap empfindet Raab sein mobiles Homeoffice nicht: „Ich bin nicht



Foto: Sebastian Raab

**Das mobile Homeoffice von IT-Berater Sebastian Raab: Der verstellbare Tischaufsatz sorgt für Dynamik.**

# Wie führt die Cloud Unternehmen in die Zukunft?



**Gemeinsam mit dir finden wir die Antwort.**

Werde jetzt Teil der Cloud Avengers bei PwC Deutschland! Transformiere mit uns die Welt und begleite Unternehmen ganzheitlich in die Cloud. Egal ob Cloud Consulting oder Cloud Assurance – hier gibt's die Jobs für dich:

[www.karriere.pwc.de/cloud](http://www.karriere.pwc.de/cloud)

weniger produktiv als anderswo. Aber ich kann mein privates Umfeld so gestalten, wie ich möchte, und das steigert meine Zufriedenheit und Motivation.“ Kollegen und Kunden falle zwar in den Videokonferenzen durchaus auf, dass er häufig den Ort wechselt. „Aber das war bisher nie ein Problem, eher ein guter Einstiegspunkt für Small Talk.“

### Städtetrip plus Co-Working

Auch für Tobias Sell haben sich durch Corona und die Umwälzung der Arbeitswelt neue Freiheiten ergeben. Sein Arbeitgeber, ein Braunschweiger IT-Beratungsunternehmen, hat zwar schon immer viel Flexibilität gewährt, aber je nach Projekt sei eine Anwesenheit vor Ort häufig notwendig gewesen, erzählt Sell im Gespräch mit c't. „Seit Corona hat sich einiges geändert. Vorher Undenkbares ist jetzt für viele Kunden einfach selbstverständlich.“

Zurzeit arbeitet Sell vorwiegend im Büro oder im Homeoffice. Doch ein- bis zweimal im Monat entscheidet er sich dazu, einen Arbeitstag in einem Co-Working-Space zu verbringen, zum Beispiel in Braunschweig oder Wolfsburg. Die Kosten für die Tagestickets übernimmt sein Arbeitgeber. „Ich finde es sehr wertvoll, aus meiner gewohnten Umgebung auszubrechen, gerade dann, wenn ich kreativ werden muss“, sagt Sell. Vorstellen kann er sich auch, bald wieder private Städtetrips mit einem Co-Working-Tag zu verbinden.

Früher, in seiner Zeit als Start-up-Gründer, hat er das bereits mehrfach getan, zum Beispiel in Zürich und San Francisco.

Sell schätzt nicht nur den Tapetenwechsel. Wichtig sind ihm auch der Austausch und die Vernetzung mit anderen Besuchern der Spaces. „Ich bin immer wieder auf der Suche nach Tools und Arbeitsmethoden, mit denen ich effektiver arbeiten kann“, sagt er. „Nicht selten komme ich mit einer Buchempfehlung oder einer neuen App nach Hause.“

Was die Technik angeht, ist Sell unterwegs genügsam. Er nimmt nur Notebook, Headset, Notizbuch und Smartphone mit. „Ich wähle meine Arbeitspakete so, dass ich an Tagen im Co-Working Space auf zusätzliche Monitore verzichten kann“, erklärt er.

Die für jedermann zugänglichen Arbeitsflächen gibt es längst nicht mehr nur in Metropolen wie Hamburg und Berlin. Laut der German Coworking Federation existieren aktuell rund 700 solcher Orte in Deutschland. Aufgrund der Pandemie mussten zwar einige Anbieter aufgeben, doch länger als eine halbe Stunde muss trotzdem kaum jemand fahren, um den nächsten Space zu erreichen. Die Kosten für Tagestickets liegen typischerweise bei 10 bis 20 Euro.

### Büro im Wohnmobil oder Kombi

Nicht nur die Co-Working-Spaces verlocken zur Mobilarbeit. Ein weiterer Treiber

ist der Verkaufsboom bei Camping-Fahrzeugen. Laut Marcus Breitfeld geht es vielen Käufern nicht nur um Urlaubsreisen: „Die Zahl der Menschen, die unterwegs leben und arbeiten, ist in den letzten zwei bis drei Jahren stark gestiegen“, meint Breitfeld, Gründer der Community „Camper Nomads“, die unter anderem Co-Working auf Campingplätzen anbietet („Camp & Work“).

Als Gründe sieht er den allgemeinen Drang nach Freiheit und Natur Nähe, aber auch die Corona-Pandemie. Denn durch die Homeoffice-Regeln konnten und durften erstmals auch viele Angestellte aus ihrem Camper heraus arbeiten. Breitfeld lebte und arbeitete selbst jahrelang in einem alten Bulli, mittlerweile hat er zusätzlich ein „Tiny House“ als feste Basis. Was die Technik angeht, tickt er nach wie vor minimalistisch: Ihm reichen sein MacBook mit M1-Chip, ein iPhone, ein LTE-Router und ein paar externe Festplatten.

Auch Thilo Vogel, der eingangs vorgestellte Digitalnomade mit dem Ford Mondeo, schwört auf Minimalismus. Ihm bliebe angesichts der Platzverhältnisse in seinem Auto aber auch nichts anderes übrig. Auch er nutzt ein M1-MacBook. Der Strom kommt aus einer 90-Ah-Batterie, die von einem 150-Watt-Solarpanel auf dem Dach gespeist wird, wenn der Motor nicht läuft. Um auf der Rückbank ergonomisch arbeiten zu können, hat er den Beifahrersitz aus- und eine höhen- und neigungsverstellbare Tischkonstruktion eingebaut.

So weit treiben den Mobilitätsgedanken nach wie vor nur wenige. Aber zumindest gibt es immer mehr, die diesen Lebensstil faszinierend finden: Die von Vogel gegründete Online-Community „Dachzeltnomaden“ zählt bei Facebook, Instagram und TikTok jeweils über 30.000 Follower. Außerdem organisieren die Dachzeltnomaden an verschiedenen Standorten „Dachzelt-Dörfer“. Dort kann jeder ein Dachzelt mieten und darin für ein paar Tage leben – ohne dafür gleich seine Wohnung aufzugeben zu müssen.

(cwo@ct.de) ct



**Tobias Sell im Co-Working-Space „Schiller40“ in Wolfsburg:  
Der IT-Berater schätzt den Austausch mit anderen Besuchern,  
zum Beispiel über Tools und Methoden für effizientes Arbeiten.**

### Literatur

- [1] Ulrike Kuhlmann, Steh mal bitte auf!, Höhenverstellbare Tischaufsätze für ergonomisches Arbeiten, c't 11/2021, S. 100
- [2] Katja Seidel, Digitalnomadin auf vier Rädern, Erfahrungsbericht: ein Campingbus als mobiles Büro, c't 11/2020, S. 136



**Damit die nächste  
Krisensitzung nicht  
im Serverraum  
stattfindet.**

**Mit SINA Gateways werden  
IT-Netzwerke premiumsicher.**

Wo Netzwerke wirksam gegen Cyberangriffe abgeschirmt werden müssen, steht secunet bereit. SINA Gateways von secunet schützen Netz-Infrastrukturen mit BSI-zugelassener Verschlüsselungstechnik und machen sie premiumsicher.

[secunet.com](http://secunet.com) protecting digital infrastructures

© Copyright by Heise Medien.

**secunet**

# Kulturwandel

## Wie Unternehmen das mobile Arbeiten sehen

**Immer mehr Konzerne erlauben ihren Angestellten, sich ihren Arbeitsort selbst auszusuchen. Aus Sicht von Experten überwiegen die Vorteile, sie warnen aber auch vor Risiken.**

Von Christian Wölbert

**E**in Großteil der Angestellten im Homeoffice – das war 2020 für die meisten Unternehmen eine neue Erfahrung. Corona zwang sie dazu, und nun tasten sie sich an neue Regeln und Gewohnheiten heran. Dürfen sich alle künftig aussuchen, wo sie arbeiten? Oder sollte man nach der Pandemie zurück zur Präsenzkultur?

Einige Unternehmen haben sich schon lange vor Corona mit diesen Fragen beschäftigt, und sich für ein hohes Maß an Flexibilität entschieden. Ein Beispiel ist Microsoft Deutschland: Schon seit 2014 gilt dort eine Betriebsvereinbarung zum „Vertrauensarbeitsort“, die allen die Wahl lässt, ob sie im Büro, im Homeoffice oder an einem anderen Ort arbeiten. Diese

Möglichkeiten hätten 90 Prozent der Angestellten auch schon vor Corona genutzt, erklärt Personalchefin Claudia Hartwich im Gespräch mit c't.

Microsoft schreibt nicht einmal eine Mindestzahl an Bürotagen vor. „Solche Regeln passen nicht zu der Grundüberzeugung, dass Mitarbeiterinnen und Mitarbeiter ganz nach ihren individuellen Bedürfnissen darüber entscheiden sollen, wann und wo sie arbeiten möchten“, sagt Hartwich. Lediglich bei bestimmten „Gesprächsformaten“, etwa Personalgesprächen, könne die persönliche Anwesenheit gewünscht sein. Und „je nach Abteilung und Position“ könnte es wichtig sein, bestimmte Standorte kurzfristig erreichen zu können.

Ein Grund, warum Unternehmen Mobilität erlauben, liegt auf der Hand: So locken und halten sie Menschen, die aus individuellen Gründen nicht jeden Tag ins Büro fahren wollen. Aus Hartwicks Sicht steigert die Flexibilität nicht nur die Zufriedenheit, sondern auch die Leistung: „Kreative Ideen, das Nachdenken über Innovationen und die Lösung von Problemen brauchen Freiheit und selbstbestimmte Mitarbeiterinnen und Mitarbeiter.“

Oft spart es auch schlicht teure Arbeitszeit, wenn Angestellte nach einem Kundentermin unterwegs oder zu Hause weiterarbeiten, statt weitere Wege ins Büro zu fahren. Hinzu kommt die Chance, die Büros zu verkleinern und dadurch Miete und Betriebskosten zu senken.

### Egal ob Ferienhaus oder Café

Nun, nach den Pandemie-Erfahrungen, folgen viele Unternehmen dem Beispiel von Vorreitern wie Microsoft. Viele Vorgesetzte waren überrascht, wie die Prozesse weiterschnurrt, obwohl kaum jemand im Büro war.

In den vergangenen Monaten stellte ein Konzern nach dem anderen neue, gelockerte Regeln vor, zum Beispiel TUI, Allianz und Porsche. Der Autobauer erlaubt künftig zwölf Tage mobiles Arbeiten



Bild: Albert Huim

pro Monat. „Im Ferienhäusle in Oberbayern oder im Café, das ist uns letztlich egal“, sagte Personalvorstand Andreas Haffner der Frankfurter Allgemeinen. Der IT-Branchenverband Bitkom schätzt, dass nach der Pandemie etwa 27 Prozent aller Beschäftigten auch außerhalb des Büros arbeiten werden, fast doppelt so viele wie zuvor.

Doch es gibt auch Gegenbeispiele. Netflix-Chef Reed Hastings sieht verteiltes Arbeiten „rein negativ“. Goldman-Sachs-Chef David Solomon nannte Homeoffice im Februar einen „Irrweg“.

Der Arbeitsforscher Oliver Stettes vom arbeitgebernahen Institut der deutschen Wirtschaft (IW) äußert sich über mobiles Arbeiten hingegen positiv: Sowohl die Unternehmen als auch die Angestellten könnten davon profitieren, sagt er.

### Niemals wirklich Feierabend

Doch der Experte sieht auch Risiken. Diverse Umfragen von Wirtschaftsforschern und Gewerkschaften haben gezeigt, dass Menschen, die viel im Homeoffice und unterwegs arbeiten, zwar insgesamt zufriedener sind, aber auch mehr Überstunden machen als ihre Kolleginnen und Kollegen im Büro. Außerdem fällt es ihnen schwerer, abends mental abzuschalten.

„Mit der Freiheit kommt Verantwortung“, sagt deshalb Stettes. Wer viel unterwegs und zu Hause arbeite, müsse auch darauf achten, rechtzeitig Feierabend zu machen. Das liege auch im Interesse der Arbeitgeber: „Diese müssen Sorge tragen, dass das Arbeitszeitgesetz eingehalten wird. Und sie haben nichts davon, wenn Mitarbeiter im Dauerstress sind und dann irgendwann krank ausfallen.“

Auch Microsoft-Personalchefin Claudia Hartwich betont die Verantwortung der Vorgesetzten: „Trotz verteilter Teams und sozialer Distanz sollten Führungskräfte sich stärker um das Wohlbefinden ihrer Mitarbeiter kümmern.“ In diesem Punkt habe auch Microsoft im vergangenen Jahr dazugelernt. (cwo@ct.de) **c't**



Bild: Microsoft

„Mitarbeiter sollen nach ihren individuellen Bedürfnissen entscheiden, wann und wo sie arbeiten möchten“, sagt Claudia Hartwich, Personalchefin von Microsoft Deutschland.



# ALLES AUF ANFANG

Neustart der IT-Weiterbildung

Kennst du schon die neue interaktive Lernplattform für IT-Professionals?

Bei uns findest du das Wissen zu den angesagten IT-Themen - von Experten für Professionals.

**Jetzt testen! Hier geht's zu den ersten Gratis-Videos:**



# FAQ

# Recht: Mobiles Arbeiten

**Corona hat dem mobilen Arbeiten einen Schub verpasst, doch viele Angestellte sind noch unsicher, was sie dürfen und was nicht. Wir geben einen Überblick über die Rechtsgrundlagen.**

Von Christian Wölbert

## Homeoffice vs. Mobilarbeit

Was ist rechtlich gesehen eigentlich der Unterschied zwischen Homeoffice und mobilem Arbeiten?

Gesetzlich ist keiner dieser beiden Begriffe definiert. In der Praxis sprechen die meisten Unternehmen von „mobilem Arbeiten“, wenn Beschäftigte irgendwo außerhalb des Büros arbeiten. Das kann auch zu Hause sein, also im Homeoffice.

Den Begriff Homeoffice vermeiden viele Unternehmen, weil er leicht mit „Telearbeit“ verwechselt werden kann, einer Arbeitsform mit strengen rechtlichen Anforderungen: Vereinbart ein Unternehmen mit einem Angestellten Telearbeit, muss es laut der Arbeitsstättenverordnung die nötigen Möbel und die technische Ausstattung finanzieren und „im Privatbereich des Beschäftigten“ installieren.

## Pflicht ausgelaufen

Gibt es eigentlich einen Rechtsanspruch auf Homeoffice oder mobiles Arbeiten?

In Deutschland, Österreich und der Schweiz haben Arbeitnehmer keinen solchen Rechtsanspruch, abgesehen von temporären Regeln in der Coronazeit. Laut der deutschen Gewerbeordnung darf der Arbeitgeber „Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen“, soweit in Arbeits- oder Tarifverträgen oder Betriebsvereinbarungen nichts Bestimmtes vereinbart ist. Aufgrund der Coronapandemie hatte die Bundesregierung die Arbeitgeber nur vorübergehend verpflichtet, ihren Beschäftigten anzubieten, „in deren Wohnung“ zu arbeiten. Diese Regel lief Ende Juni 2021 aus.

In den Koalitionsverhandlungen nach der Bundestagswahl wird wohl wieder

über das Thema diskutiert werden. Dass dabei ein Rechtsanspruch herauskommt, ist aber unwahrscheinlich. 2020 lehnte die Union bereits einen Vorschlag von Arbeitsminister Hubertus Heil (SPD) ab, einen Anspruch auf mindestens 24 Tage im Jahr zu schaffen. Nun fordert Heil nur noch, dass Arbeitgeber mit ihren Beschäftigten den Wunsch nach mobiler Arbeit erörtern und eine Ablehnung schriftlich begründen müssen.

Doch fehlender Rechtsanspruch hin oder her: In der Praxis erlauben trotzdem immer mehr Firmen mobiles Arbeiten.

## Hauptsache, produktiv

Mein Arbeitgeber erlaubt „mobiles Arbeiten“. Heißt das, ich darf nun überall arbeiten, wo ich möchte?

In vielen Unternehmen regeln Betriebsvereinbarungen die Details des mobilen Arbeitens individuell, in manchen finden sich auch Aussagen zu möglichen Arbeitsorten. Falls der Arbeitgeber mobile Arbeit erlaubt, ohne solche Details vorzugeben, dürfen Beschäftigte nach herrschender Rechtsmeinung grundsätzlich frei wählen, müssen aber Bedingun-

gen beachten: „Man muss bei der Wahl des Arbeitsortes seine Arbeitsfähigkeit und Erreichbarkeit sicherstellen“, fasst Martina Hidalgo, Leiterin des Bereichs Arbeitsrecht bei der Kanzlei CMS, im Gespräch mit c’t zusammen. Außerdem müsste man sonstige Pflichten wie die Wahrung der Vertraulichkeit oder den Datenschutz beachten. „An öffentlichen Orten wie Cafés kann man kaum ausschließen, dass fremde Personen Telefone mithören oder Bildschirminhalte einsehen.“

Ähnlich sieht der Deutsche Gewerkschaftsbund (DGB) die Rechtslage: Die Umstände vor Ort müssten „eine ordnungsgemäße Leistungserbringung ermöglichen“, erklärte eine Sprecherin auf Anfrage. „Unter dieser Voraussetzung geht es aber den Arbeitgeber nichts an, ob Beschäftigte ihr Homeoffice in ihre Stadtwohnung oder im Ferienhaus im Umland einrichten.“

Auch die Entfernung zum Büro kann in der Praxis eine Rolle spielen, denn häufig gestatten Firmen das mobile Arbeiten nur nach Absprache für einzelne Tage. Wird für den nächsten Tag spontan ein Termin im Büro angeordnet, zählt die Ausrede nicht, dass man gerade in einer Ferienwohnung im Allgäu weilt. „Der Arbeit-

The screenshot shows a news article from the TUI Reiseblog. The header reads "Die richtige Wahl des Ziels: Die schönsten Orte weltweit für deine Workation@TUI". Below the header is a section titled "Arbeiten auf den Kanaren" with a large image of a coastal town on a hillside overlooking a blue sea. A caption at the bottom of the image says "Die kanarischen Inseln eignen sich zu jeder Jahreszeit für deine Workation". The TUI logo is visible in the top left corner of the page.

Bei TUI heißt die Mischung aus Urlaub und Homeoffice „Workation“. Wer aus dem Ausland herausarbeiten will, braucht jedoch grünes Licht vom Arbeitgeber.

geber behält im Regelfall das Direktionsrecht, auch wenn er eine gewisse Flexibilität gestattet“, erklärt Hidalgo.

## Spezialfall Ausland

❓ Darf ich auch von meiner Ferienwohnung auf Mallorca aus mobil arbeiten?

❗ Auch wenn der Strand lockt: Im Ausland dürfen Angestellte nur arbeiten, wenn der Arbeitgeber explizit im Einzelfall zustimmt. Denn das Arbeiten vom Ausland aus hat komplexe sozialversicherungsrechtliche und steuerrechtliche Konsequenzen – nicht nur für den Arbeitnehmer, auch für den Arbeitgeber.

## Geld-zurück-Garantie

❓ Kann ich die Kosten für Laptop, Monitor & Co. von der Steuer absetzen?

❗ Im Winter sind neue Steuerregeln fürs Homeoffice in Kraft getreten, diese gelten aber nicht fürs Arbeiten unterwegs: Für jeden Tag, den man „in der häuslichen Wohnung“ arbeitet, kann man bei der Steuererklärung 5 Euro geltend machen. Der Betrag ist auf 600 Euro im Jahr begrenzt, und er wird vom Finanzamt in den allgemeinen Arbeitnehmer-Pauschbetrag von 1000 Euro eingerechnet. Man profitiert also nur, wenn man mehr als 400 Euro an sonstigen Werbungskosten hat. Die Regel gilt zunächst befristet für die Steuererklärungen 2020 und 2021. Arbeitsmittel wie Notebooks, Headsets, Webcams oder Schreibtische kann man ebenfalls als Werbungskosten absetzen, wobei man schätzen muss, zu wie viel Prozent man diese Dinge beruflich nutzt. Computer, Peripherie und Software kann man seit 2021 grundsätzlich auf einen Schlag absetzen. Bei anderen Arbeitsmitteln ist es komplizierter: Übersteigt der Kaufpreis 952 Euro, muss man über mehrere Jahre abschreiben.

## Risikozone Arbeitszimmer

❓ Wer zahlt bei Unfällen?

❗ Bei allen Unfällen im Büro springt die gesetzliche Unfallversicherung ein. Im Homeoffice und unterwegs ist es komplizierter: Versichert sind dort nur Unfälle bei Tätigkeiten, die betrieblichen Interessen dienen, also zum Beispiel der Weg zum Drucker. Stürzt man hingegen auf dem Weg zur Kaffeemaschine in der Küche, ist die Unfallversicherung laut einem Urteil des Bundessozialgerichts nicht zuständig. Auch der Weg zwischen Kindergarten und Homeoffice ist nicht versichert – anders als der Abstecher zum Kindergarten auf dem Weg ins Büro. Arbeitsminister Hubertus Heil hat einen Gesetzentwurf vorgelegt, der diese Ungleichheit beseitigen soll. Über dieses Gesetz wird wegen der Bundestagswahlen aber wohl erst im nächsten Jahr im Bundestag diskutiert werden. (cwo@ct.de)



Die Online-Konferenzen zur secIT by Heise

## IT-Security im Fokus

Vertiefen Sie in einer spannenden Keynote sowie in 3 interaktiven Vorträgen Ihr Wissen rund um IT-Security. Jedes secIT Special präsentiert Ihnen ein exklusives Thema.

### IR, SOC und SIEM

Verteidigungsschinesisch (nicht nur) für Anfänger!  
Im Kombi-Ticket als Aufzeichnung erhältlich

16. September 2021

### Cybersicherheit für KMU

Kaufen, mieten oder selber machen?

9. Dezember 2021

### Hacking for Security

Was Sicherheitstests für Unternehmen bringen!

**JETZT ANMELDEN:** [konferenzen.heise.de/secit-special](http://konferenzen.heise.de/secit-special)

© Copyright by Heise Medien.



Bild: Albert Huim

# Ohne Netz geht nix

## Mobile Router und Datentarife für das Immer-dabei-Office

**Pflicht für jedes tragbare Büro ist ein Mobilfunktarif mit genügend Datenvolumen für Recherchen und Videokonferenzen. Zur Kür gehört ein LTE-Router – gebrauchte Einsteigermodelle gibt es schon für 20 Euro.**

**Von Urs Mansmann, Andrijan Möcker, Katja Seidel und Dušan Živadinović**

**D**as mobile Homeoffice steht und fällt mit einer ordentlichen Verbindung ins Internet. Co-Working-Spaces bieten in der Regel ein flottes

WLAN, doch in Hotels, Cafés oder Ferienwohnungen kann man davon nicht unbedingt ausgehen. Auf Nummer Sicher geht man mit den Mobilfunknetzen: LTE ist locker schnell genug für Videokonferenzen und zumindest in bewohnten Gebieten ordentlich ausgebaut. Wer auch außerhalb von Ortschaften und abseits asphaltierter Straßen arbeiten will, sollte vor der Fahrt die Netzabdeckungskarten der Provider prüfen.

Wenn dann die Wahl auf den oder die Netzbetreiber gefallen ist, sollte man sich Gedanken um das benötigte Datenvolumen machen. Wer werktäglich eine Stunde in einer Konferenz mit 3 MBit/s verbringt, verbraucht allein damit im Monat über 25 GByte. Dabei sind 3 MBit/s ein Mittelwert. Wie hoch das Volumen tatsächlich ausfällt, hängt vom Videokonfe-

renzsystem ab. Manche Programme begnügen sich mit 1 MBit/s, andere kommen auf deutlich mehr.

Oft kann man die Übertragungsmenge senken, indem man die HD-Auflösung abschaltet. Das ist nicht bei allen Programmen vorgesehen, aber Sie können eine niedrigere Auflösung erzwingen, wenn Sie anstatt der im Laptop eingebauten Kamera eine ältere USB-Webcam nehmen. Zur Not schalten Sie Ihr Videosignal ab und bauen nur eine Audiokonferenz auf. Denn neben den Videokonferenzen gilt es auch den Bedarf für Surfen, Messaging, Mails und den Daten austausch mit der Cloud zu berücksichtigen (zahlreiche Möglichkeiten, Mobilfunkvolumen unter diversen Betriebssystemen zu sparen, haben wir in [1] beschrieben).

Wer nur wenig Zeit mit Zoom, Webex & Co. verbringt, kommt vielleicht mit 20

GByte im Monat aus, wofür man je nach Provider und Vertragslaufzeit 25 bis 40 Euro im Monat einplanen muss. Gegen Aufpreis bekommt man bei vielen Anbietern auch 40, 50 oder 60 GByte.

### Ungebremst für einen Tag

Gar nicht aufs Datenvolumen achten muss man mit einer Flatrate, also einem Daten-tarif ohne Volumenbeschränkung. O2 bie-tet seine Flatrate „Free Unlimited Basic“ bei zwei Jahren Vertragslaufzeit für günstige 30 Euro an, dann allerdings nur mit 2 MBit/s im Down- und 1 MBit/s im Upstre-am im LTE-Netz, was nur für Audiokonfe-renzen genügt. Für 40 Euro im Monat gibt es 10/5 MBit/s und 5G obendrauf und für 60 Euro die unlimitierte Variante mit 500/50 MBit/s. Vodafone verlangt für seine Flatrate „Red XL unlimited“ 80 Euro, die Telekom für ihre „Magenta Mobil XL“ 85 Euro – einen detaillierten Vergleich aktueller Mobilfunktarife mit großem Datenvolumen haben wir erst vor Kurzem veröffentlicht [2].

„Ohne Volumenbeschränkung“ gilt für eine SIM-Karte und den zugehörigen Tarif allerdings nur im Inland. Im EU-Aus-land dürfen die hiesigen Anbieter ihre Flatrates gemäß komplizierter EU-Vorga-ben in Tarife mit begrenztem Datenvolu-men verwandeln. Ist das Datenbudget aufgebraucht, zahlt man pro GByte extra. Deshalb kann es sich lohnen, zu einem ört-lichen Provider zu wechseln.

Auch im Inland gilt: Arbeitet man nur ab und an unterwegs, kommt man günsti-ger mit Datenpaketen oder 24-Stunden-Flatrates weg. Bei vielen Anbietern kann man solche Optionen zu jedem Tarif spontan hinzubuchen. Die Telekom zum Bei-spiel verlangt für ihre Tagesflat 6 Euro, bei O2 sind es 5 Euro. Tagestarife gibt es auch in Kombination mit Prepaid-Angeboten. Bei Vodafones CallYa beispielsweise kos-ten 10 Gigabyte für 24 Stunden 5 Euro.

In den meisten Laufzeitverträgen und Prepaid-Tarifen ist eine Telefon-Flatrate in alle deutschen Netze enthalten. In manchen gibt es obendrein eine Festnetz-nummer. Die ist praktisch, weil sie die Kosten für Anrufer und für eigene Ruf-umleitungen von einer Büronummer senkt. An vielen Festnetzanschlüssen werden immer noch überhöhte Gebühren für Verbindungen zu Mobilfunkanschlüs-sen genommen, obwohl die tatsächlichen Minutenkosten, die die Telefongesell-schaften untereinander abrechnen, mas-siv gefallen sind.

Für Mobilrouter, Tablets und Note-books mit eingebautem Modem gibt es Datentarife ohne Telefonie. Flexibel sind Digitalnomaden etwa mit dem „my Inter-net-to-Go“ von O2, denn hier bucht man spontan je nach Bedarf eine Tagesflat (5 Euro), eine Wochenflat (20 Euro) oder eine Monatsflat (50 Euro). Eine Grund-gebühr gibt es nicht, allerdings eine An-schlussgebühr von 50 Euro.

### Hosentaschenrouter

Als Router für das mobile Homeoffice dient im einfachsten Fall das Smartphone. Mit VOLTE klappt das in der Regel auch, während man telefoniert – die allermeis-ten Provider unterstützen diese Technik. Nachteil der Smartphone-Lösung ist der relativ hohe Strombedarf: Das Handy wird warm und sollte am Netzteil hängen, damit der Akku nicht allzu schnell leer-gesaugt wird.

Komfortabler arbeitet man mit einem separaten Mobilfunkrouter. Um unter-wegs ausreichend flott im Netz zu sein, muss man auch nicht eines der neuesten Modelle mit LTE- oder 5G-Modem kaufen. Die Kleinanzeigenportale im Internet sind voll mit ordentlichen LTE-Gebraucht-ge-räten; Finger weg von den älteren, die sich nur für UMTS/3G eignen.

Als günstiges Einstiegsmodell bietet sich der „Magenta Schnellstart“ an. Der von der Telekom so getaufte akkubetrie-bene Mini-Router ist eigentlich ein Hua-wei E5577Cs-321, den manche Kunden als Zwischenlösung bis zur Schaltung des DSL-Anschlusses gratis erhalten. Viele haben danach keine Verwendung für ihn und bieten ihn für weniger als 20 Euro an. Neu verkauft ihn die Telekom inklusive 60 GByte Datenvolumen für 50 Euro. Einen Entsperr-Code für den SIM-Lock kann man auf einer Telekom-Website kos-tenfrei anfordern.

In dem Gerät steckt ein LTE-Modem der Kategorie 4, es liefert also bis zu 150 MBit/s im Downlink und 50 MBit/s im Up-link. Der Router versorgt bis zu 10 Geräte per Wi-Fi 4 auf 2,4 oder 5 GHz (nicht simultan). Der Akku soll laut Telekom bis zu sechs Stunden durchhalten, sofern er nicht abgenutzt ist – der Schnellstart taugt dann also auch fürs Café oder die Park-bank. Aufgeladen wird er über Micro-USB.

### LTE ist nicht gleich LTE

150 beziehungsweise 50 MBit/s klingen zunächst nicht schlecht, aber da sich alle in einer Zelle eingebuchten Mobilfunk-nutzer deren Kapazität teilen müssen, be-kommt man je nach Ort und Tageszeit auch mal nur wenige MBit/s. Beim Mailen, Surfen und Chatten ist das kein Problem, für ein Videokonferenzprogramm kann das aber zu wenig sein. Wenn es gut ge-macht ist, schraubt die Software die Bild-qualität selbst herunter und mit etwas Glück hilft auch die Mobilfunkzelle: Ist die Verbindung gut, also das Signal stark, lässt sich leichter eine hohe Datenrate erzielen, auch wenn die Zelle stark belegt ist. Diese Verkehrsregelung erfolgt aber automati-schisch und dynamisch, sodass man sich darauf nicht verlassen kann.

Abhilfe schaffen moderne Mobilfunk-router ab LTE-Advanced (Cat. 6), die sich für mehr Frequenzbänder und höhere Mo-dulationsstufen eignen sowie mehr Antennen besitzen (MIMO). Eine einfache Dau- menregel lautet: Je mehr Frequenzbänder, Modulationsstufen und Antennen eine Mobilfunkzelle bietet und je mehr davon ein Modem gleichzeitig nutzen kann, desto höher die Gesamtdatenrate und desto höher die Wahrscheinlichkeit, dass das Modem ein Band belegt, das kaum jemand anderes nutzt. Das Angebot an Funkbän-dern der Funkzellen in Ballungszentren ist typischerweise besser als auf dem Land.



**Der LTE-Router „Magenta Schnellstart“ passt in die Hosentasche, spannt ein WLAN für bis zu zehn Geräte auf und ist ge-bräucht schon für 20 Euro zu erwischen.**

Die ersten 5G-Router sind noch relativ teuer – der D-Link DWR-2101 kostet rund 400 Euro.



Mehr Datenrate als der Magenta Schnellstart, für immer noch wenig Geld, bieten zum Beispiel der Vodafone Gigacube (Huawei B528s-23a) und die nahezu baugleiche Telekom Speedbox (B529s-23a). Ihre LTE-Modems der Kategorie 6 erreichen bis zu 300 MBit/s in Downlink- und bis zu 50 MBit/s in Uplink-Richtung; Wi-Fi 5 läuft auf 2,4 und 5 GHz simultan. Gebraucht kosten sie um die 50 Euro, mit etwas Glück auch weniger [3].

Als Würfel mit rund zwölf Zentimetern Kantenlänge beulen die beiden die Laptop-Tasche allerdings aus. Außerdem werden sie nicht über Micro-USB gespeist, sondern über ein 12-Volt-Netzteil. Sie sind also weniger mobil – selbst wenn sie über einen Adapter auch in Fahrzeugen laufen und in der Speedbox sogar ein 3-Ah-Akku steckt, der laut Telekom rund vier Stunden durchhalten soll. Außer über WLAN kommunizieren sie über einen Gigabit-Ethernet-Port per Kabel. Dank TS-9-Anschluss kann man den Empfang mit externen Antennen verbessern.

### Gigabit-Internet unterwegs

Abseits solcher Schnäppchen gibt es eine große Auswahl an aktuellen LTE-Routern. Zu den kompakten, schnellen Modellen

für unterwegs gehört der Netgear AC810 mit Micro-USB und Akku für rund 190 Euro. Er liefert mit seinem Modem der Kategorie 11 bis zu 600 MBit/s und WLAN für maximal 15 Geräte. In der Praxis haben wir mit der optionalen Antenne mit TS9-Anschluss (50 Euro) gute Erfahrungen gemacht, sie hat den Empfang oft signifikant verbessert.

Deutlich schneller sind Router mit Kombi-Modem für LTE und 5G, denn die 5G-Netze bieten nicht nur höhere Kapazität, sie sind auch weniger stark ausgelastet. Dadurch ist Gigabit-Niveau erreichbar, zum Beispiel mit dem leicht tragbaren DW-2101 von D-Link [4]. Mit dem weitgehend baugleichen Zyxel NR2101 5G NR Mobile WiFi bieten sich noch bessere Chancen, denn er hat dem D-Link vier 5G-Bänder voraus. Beide kosten aber rund 400 Euro.

Auch 5G-Router ohne Akku wie der Vodafone Gigacube 5G sind noch teuer beziehungsweise nur dann günstig, wenn man einen fetten Datentarif für zwei Jahre hinzubucht. Deshalb sollte man vor einer solchen Investition dringend abklären, ob man sich überhaupt oft genug in Reichweite von schnellen 5G-Basisstationen aufhält. Die Netzabdeckungskarten von



Der Netgear AC810 für 190 Euro gehört mit seinem LTE-Modem der Kategorie 11 zur Mobilrouter-Mittelklasse.

Telekom, Vodafone und O2 Telefónica finden Sie über [ct.de/ynhd](http://ct.de/ynhd).

### Der richtige SIM-Mix

Bleibt die Frage, welche SIM-Karte man für den mobilen Router auswählt. Hat man einen Smartphone-Tarif mit viel Datenvolumen, bietet es sich an, eine Multi-SIM zu ordern, um das Volumen flexibel aufzuteilen. Bei einigen Anbietern wie 1&1 gibt es das zweite Kärtchen kostenlos, die meisten verlangen rund 5 Euro im Monat extra.

In vielen Fällen ist es aber günstiger, das Handy mit einem kleineren Tarif zu bestücken und für den Router einen speziellen (Prepaid-)Tarif auszusuchen, mit Tages-Flats nach Bedarf. Empfangstechnisch lohnt es sich manchmal, SIM-Karten unterschiedlicher Netzbetreiber im Gepäck zu haben. Steckt der Mobilfunkrouter im Funkloch, hat vielleicht das Smartphone Empfang und kann als Hotspot einspringen. [\(cwo@ct.de\) ct](mailto:(cwo@ct.de) ct)

### Literatur

- [1] Reiko Kaps und Dušan Živadinović, Schonkost, Mobilfunkvolumen für Linux, macOS, Windows, iOS und Android richtig begrenzen, c't 13/2021, S. 70
- [2] Urs Mansmann, Unterwegs ins Netz, Mobilfunktarife für den großen Bedarf, c't 15/2021, S. 114
- [3] Andrijan Möcker, Sparrepertoire, Gebrauchte Netzwerkhardware 2021, c't 9/2021, S. 116
- [4] Dušan Živadinović, Drahtlos-Sprinter, c't 7/2021, S. 74

**Netzabdeckungskarten:** [ct.de/ynhd](http://ct.de/ynhd)

## WLAN-Router für unterwegs

Gibt es im Hotel oder in der Ferienwohnung ein stabiles WLAN, kann man das LTE-Volumen schonen. Eventuell lohnt sich dann ein reisetauglicher WLAN-Router: Hersteller wie GL.iNet und TP-Link bieten per USB mit Strom versorgte Mini-Router wie den AR750s oder den WR902AC im Zigarettenzigarettenformat. Sie verbinden sich mit dem Hotspot und spannen ein eigenes WLAN mit separatem IP-Subnetz und Firewall-schutz auf. So lässt sich die Abdeckung in der Ferienwohnung verbessern, wo von besonders Mobilgeräte mit kleinen Antennen profitieren. Los gehts ab etwa 30 Euro (siehe c't 6/2019, S. 148).

# WebAssembly 2021

Die Heise-Konferenz zu Wasm

31. August 2021 ONLINE



Jetzt  
Tickets  
sichern!

Game Changer auch jenseits des Web

- » Dein Einstieg in das sprach- und plattformübergreifende Ökosystem
- » Lerne den richtungsweisenden W3C-Standard kennen
- » Deep Dives in Blazor, Rust, C#, JavaScript, Container und Flutter
- » Tausche dich aus mit WebAssembly-Insidern

# Pixel für unterwegs

## Portable Monitore für das mobile Office



Bild: Albert Hutm

**Je portabler das Notebook, desto kleiner das Display. Zusätzliche Fläche und Pixel bieten mobile Monitore, die vom Laptop mit Strom versorgt werden. Wir geben einen Überblick über das Produktangebot und Tipps zu Auswahl und Einsatz.**

Von Katja Seidel und Christian Wölbert

**C**hat, Dokumente, Browser und vielleicht noch die eine oder andere fachspezifische Anwendung: Viele Nutzer wollen mehrere Fenster gleichzeitig im Blick haben und arbeiten deshalb mit mehreren Monitoren. Dank portabler Monitore ist das auch unterwegs möglich. Sie sind flach und leicht, weil sie ohne Netzteile und klobige Füße auskom-

men. Aufgestellt werden sie mit einem eingebauten Ständer oder einer magnetisch haftenden Abdeckung, die man zu einer Halterung zusammenfaltet.

Strom und Bildsignal kommen typischerweise über ein einziges USB-C-Kabel vom Laptop. Die Pixelflunden sind deshalb in Sekunden einsatzbereit. Das ist nicht nur im mobilen Büro sehr praktisch, sondern auch in kleineren Meetings, um dem Gegenüber etwas zu präsentieren.

Zumindest die 14- und 15,6-Zöller kosten nicht sonderlich viel: Unter 200 Euro geht es los. Eine große Auswahl bietet Asus, zudem haben wir bei AOC, Lenovo, HP, Acer und Viewsonic einige Modelle entdeckt.

Hinzu kommt eine Flut mobiler Displays kaum bekannter chinesischer Marken, die vor allem über Plattformen wie Amazon erhältlich sind. Unsere Erfahrungen mit solchen Modellen sind allerdings gemischt: Von sechs, die wir in der Praxis genutzt haben, fielen drei nach einiger Zeit

defekt aus. Da die Verkäufer in der Regel ihren Sitz in China haben, ist man für Reparatur oder Umtausch auf den Willen des Verkäufers (oder von Amazon.de) angewiesen. Im Streitfall ist die Durchsetzung von Gewährleistungs- und Garantieansprüchen praktisch unmöglich.

### 14 bis 17 Zoll

Zurück also zu den etablierten Marken. Lenovo verkauft einen 14-Zöller mit matter Oberfläche (ThinkVision M14, 230 Euro) und einen mit glänzender Oberfläche, Multitouch, Digitizer und Stift (M14t, 260 Euro). Letzterer verwandelt jedes Notebook in ein Zeichenbrett, beide lassen sich mit dem fest eingebauten, stufenlos neigbaren Fuß besonders schnell aufstellen.

15,6-Zöller findet man unter anderem bei AOC, Acer und Asus. Ein mattes Exemplar von AOC haben wir bereits getestet (siehe ct.de/yb1t): Der 200 Euro teure I1601FWUX wiegt 800 Gramm, samt mitgeliefertem Hardcover 1 Kilogramm. Einen



Von links nach rechts: Der Asus ROG Strix XG17AHPE misst 17 Zoll, der Asus ZenScreen MB16ACE 15,6 Zoll und der ThinkVision M14t von Lenovo 14 Zoll.

17-Zöller haben wir bei Asus gefunden, den ROG Strix XG17AHPE im noch halbwegs dezenten Gaming-Design. Er hat einen Akku, was sich bei Gewicht (1 Kilo) und Preis (500 Euro) bemerkbar macht.

Egal ob 14, 15,6 oder 17 Zoll: Bei den etablierten Marken haben wir nur Modelle mit Full-HD-Auflösung (1920 × 1080) gefunden. Nur chinesische Newcomer bieten auch mobile Monitore mit 4K-Auflösung. Das Gewicht liegt je nach Größe bei 500 Gramm bis etwa einem Kilogramm.

Bei der Helligkeit muss man im Vergleich zu normalen Monitoren Abstriche machen. Die meisten mobilen Displays leuchten mit maximal 200 bis 300 cd/m<sup>2</sup>, das AOC-Modell schaffte in unserem Test sogar nur maximal 185 cd/m<sup>2</sup>. Gerade unterwegs kann das zum Problem werden, etwa, wenn man im Zugabteil am hellen Fenster oder auf dem Hotelbalkon arbeiten will. Einen Vergleichstest mehrerer Modelle lesen Sie in einer der nächsten Ausgaben von c't.

Im Datenblatt des eigenen Notebooks sollte man vor dem Kauf nachsehen, ob es am USB-C-Port auch DisplayPort-Signale ausgibt – selbst einige aktuelle Modelle tun das nicht. In diesem Fall benötigt man einen portablen Monitor mit HDMI-Eingang, und für die Stromversorgung muss man ein zusätzliches USB-Kabel einstöpseln oder ein Netzteil nutzen.

Will man mehrere portable Monitore gleichzeitig anschließen, muss das Notebook mehrere DisplayPort-fähige USB-C-Buchsen haben, oder man braucht einen Adapter. Größere USB-C-Hubs stellen zwei Monitoranschlüsse bereit – meist einen HDMI-Ausgang und einen DisplayPort. Dafür muss das Notebook an der USB-C-Buchse gleich zwei DisplayPort-Kanäle ausgeben. Alternativ machen USB-auf-HDMI-Adapter aus einem normalen USB-A-Port per DisplayLink einen oder sogar zwei zusätzliche HDMI-Ausgänge. Technisch gesehen sind diese Adapter USB-Grafikkarten mit eher langsamem Chips, daher muss man mit einer leichten Latenz klarkommen, der sich auch als Eingabeverzögerung in den Mausbewegungen bemerkbar macht.

## Tablet als Zweitdisplay

Auch ein Tablet kann als mobiler Monitor dienen. Besonders einfach ist das für Besitzer eines neueren MacBooks und iPads, denn seit der Catalina-Version ist die „Sidecar“-Funktion in macOS eingebaut, die das



Schon für knapp 50 Euro bekommt man zusammenfaltbare, stabile Notebook-Ständer, zum Beispiel von Tounee. Sie bringen die Display-Oberkante auf Augenhöhe.

iPad in ein Zweitdisplay verwandelt. Da der Apple Pencil nutzbar bleibt, kann man das iPad dann auch als Grafiktablett einsetzen.

Windows-Nutzer müssen auf Apps wie Duet Display zurückgreifen, die aus einem per USB oder WLAN verbundenen iPad oder Android-Tablet einen portablen

Monitor machen. Die Latenz ist allerdings erfahrungsgemäß relativ hoch. Diese gewisse Trägheit in Verbindung mit einer vergleichsweise hohen CPU-Last schreckt von dieser Lösung ab. (cwo@ct.de) ct

**Test des AOC-Monitors:** [ct.de/yb1t](http://ct.de/yb1t)

## Ergonomie im mobilen Homeoffice

So komfortabel und ergonomisch wie ein fester Arbeitsplatz kann ein mobiles Büro kaum sein, denn dann müsste man auch Schreibtisch und Drehstuhl mitschleppen. Wer ganze Tage unterwegs arbeitet, sollte zumindest den oberen Rand seines Hauptdisplays auf Augenhöhe bringen. Das ist eines der wichtigsten Kriterien für ergonomisches Arbeiten. Bleibt das Display auf Tischhöhe, muss man zu stark nach unten schauen, und dann belastet das Gewicht des Kopfes die Wirbelsäule enorm.

Man braucht also einen idealerweise höhenverstellbaren Ständer, der das Notebook aufbockt – in Online-Shops findet man stabile Modelle für weniger als 50 Euro. Dann benötigt man nur noch eine Tastatur und eine Maus, um deutlich gesünder arbeiten zu können als ge-

krümmt über dem Notebook. Langfristig danken einem das auch die Sehnen.

Die meisten portablen Monitore lassen sich mit den mitgelieferten Hüllen oder eingebauten Klappen zwar in verschiedenen Winkeln aufstellen, aber nicht auf eine Blickhöhe bringen. Eine Ausnahme ist der 17-Zöller ROG Strix XG17AHPE von Asus: Ihn gibt es für 600 Euro samt einem zusammenklappbaren, höhenverstellbaren Stativ. Andere Modelle kann man mit einem Notebook- oder Tablet-Ständer in die Höhe bringen. Letztere sind typischerweise nur 10 bis 20 Zentimeter hoch, was für große Menschen nicht ausreicht.

Ansonsten gilt auch unterwegs, genau wie im Büro: Je öfter man sich bewegt, die Sitzposition variiert und zwischendurch auch mal im Stehen arbeitet, desto besser.

# Wo bist Du denn schon wieder?

## Tipps für Videokonferenzen unterwegs

**Videokonferenzen sind aus dem Arbeitsalltag nicht mehr wegzudenken. Besonders Mobilarbeiter sollten Bild und Ton mit ein paar Gadgets verbessern.**

Von Katja Seidel und Christian Wölbert

**P**raktisch in jedem Notebook stecken Mikro, Webcam und Lautsprecher. Mobilarbeiter haben also schon alles dabei, was sie für Videokonferenzen brauchen. Doch besonders dann, wenn man an wechselnden Orten arbeitet, sollte man über ein paar zusätzliche Anschaffungen nachdenken.

Erstens ist unterwegs das Risiko höher, dass man auch mal in einer lauten Umgebung landet und das Notebook-Mikro Kinderlärm oder Geschirrgeklapper in die Konferenz bläst. Zweitens hören vielleicht manche Vorgesetzte bei den Mobilarbeitern im Team genauer hin als bei anderen. Kommt der Eindruck auf, dass man unterwegs nicht ungestört arbeiten kann, wird die Reisefreiheit eventuell noch einmal diskutiert.

Digitalnomaden sollten sich also auf jeden Fall ein Headset oder einen Kopfhörer sowie Tischmikro gönnen. Gerade bei Kopfhörern und Headsets, die man stundenlang am Körper trägt, hängt viel von individuellen Vorlieben und Gewohnheiten ab: Der eine nimmt lieber kabellose In-Ears, der andere bevorzugt einen fetten, ohrumschließenden Kopfhörer – die perfekte Lösung für alle gibt es nicht.

### Besser mit Bügel

Grundsätzlich gilt: In-Ears sowie Headsets ohne Mikrofonbügel nehmen relativ viel Umgebungslärm mit auf. An lauten Orten

verwendet man besser ein Modell mit Bügel. Stört man sich nicht am Kabel, bietet sich das leichte, bequeme PDG1a von Audio Technica für 170 Euro an (c't 21/2020, S. 112). Aber auch Einsteigermodelle wie das Poly Blackwire 3325 für 60 Euro lassen die eigene Stimme für die anderen Konferenzteilnehmer viel angenehmer klingen als das Notebook-Mikro (c't 11/2021, S. 68).

Bluetooth-Headsets ersparen das Kabelgefummel. Moderne Exemplare haben obendrein den Vorteil, dass sie sich mit Smartphone und Notebook koppeln lassen und bei Anrufen automatisch umschalten. So telefoniert und videokonferiert man mit demselben Headset und spart Gepäck. Vertreter dieser Gattung sind das Jabra Evolve2 85 und das Poly Voyager Focus 2 UC – siehe auch Seite 84.



Bild: Albert Hilm

Wer schon einen guten Kopfhörer hat, für den bieten sich kleine, leichte USB-Tischmikros an. Für Videokonferenzen genügen zum Beispiel das CAD Audio U29 (35 Euro), oder das Shure MV5C (100 Euro, siehe c't 11/2021, S. 70). Man sollte sie aber nahe am Mund positionieren, also entweder welche mit entsprechend großem Stativ kaufen oder – wenig mobil – einen Mikrofonständner nutzen. Wer gar keinen Kopfhörer tragen will, kann auf USB- oder Bluetooth-Konferenzlautsprecher mit Mikrofon-Arrays ausweichen, zum Beispiel von Jabra oder Beyerdynamic (siehe c't 17/2019, S. 87). Sie nehmen allerdings wieder mehr Umgebungsgeräusche mit auf.

### Schau mir in die Augen

Um auch optisch unterwegs gut rüberzukommen, sollte man die Notebook-Webcam auf Augenhöhe bringen. Dafür braucht man zugegebenermaßen etwas mehr Ausstattung: Einen Ständer, der das Notebook aufbockt, sowie eine externe Tastatur und Maus, was sich aber alles auch ergonomisch lohnt (siehe S. 71).

Reicht die Bildqualität der Notebook-Kamera nicht aus, setzt man eine externe Webcam auf den Bildschirmrand. Für ein rauscharmes Videobild unabhängig vom Tageslicht bieten sich kompakte USB-Leuchten mit Saug- oder Klemmfuß oder Stativ an. Verwendet man ein Ringlicht, klemmt man idealerweise eine externe Webcam in die Mitte.

Wer vor Kollegen und Kunden verborgen will, dass er gerade in der Ferienwohnung arbeitet, kann das mit einem virtuellen Hintergrundbild versuchen. Doch bei Bewegungen blitzt immer mal wieder die Realität durch. Zuverlässig verhindert man ungewollte Einblicke nur mit Low-tech-Hardware, die sich im Gepäck bemerkbar macht: einer Leinwand samt geeignetem Stativ. (cwo@ct.de) **c't**



**Eierlegende Wollmilchsau: Der Jabra Evolve2 85 klingt bassstark und schaltet bei Anrufen automatisch zwischen PC und Handy um.**



**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.**

© Copyright by Heise Medien.





# Silberpfeil

## Chromebook mit Snapdragon 7c

**Ins neue Chromebook Spin 513 baut Acer einen Qualcomm-Prozessor mit ARM-Architektur ein. Es lockt mit guter Leistung zum kleinen Preis.**

Von Stefan Porteck

**D**as Spin 513 von Acer sieht edel aus, das Gehäuse schimmert in mattem Silber. Doch tatsächlich besteht das Chromebook nicht aus Aluminium, sondern aus Kunststoff. Das bedeutet aber nicht, dass es billig verarbeitet wirkt – im Gegenteil: Nichts knirscht oder knarzt.

Anders als bei vielen anderen günstigen Notebooks taugt die Tastatur auch problemlos dazu, lange Texte zu verfassen. Ihre Tasten haben zwar keinen ultrakurzen Hub, sind aber leichtgängig und geben mit einem spürbaren Druckpunkt

ihr Feedback. In dunkler Umgebung schaltet sich automatisch die Tastaturbeleuchtung ein, in der Preisklasse um 400 Euro keine Selbstverständlichkeit.

### Display

Auch die beweglichen Teile machen einen guten Eindruck. Das Flip-Scharnier hält das Display stabil in der eingestellten Position. Etwas störend fanden wir lediglich, dass die Doppelscharniere einen relativ langen Steg haben. Klappt man das Display nach hinten, um das Spin 513 als Tablet zu benutzen, liegen die Geräteunterseite und der Display-Rücken nicht plan aufeinander, sondern es verbleibt ein kleiner Spalt. Wenn man das Gerät nur auf dem Schoß abstellt und es nicht mit beiden Händen hält und dabei leicht zusammendrückt, klappern Display und Gehäuseunterseite bei jeder Touchgeste kurz aneinander.

Mit einer Diagonale von 13,3 Zoll (34 Zentimeter) trifft das Display für Freizeit

und Produktivität einen guten Kompromiss: Auf dem Spin 513 lässt sich problemlos ein Arbeitstag bestreiten, ohne dass einem die Schirmfläche zu mickrig kommt. Es ist zudem Touch-fähig, und Chrome OS unterstützt Stifteingaben, es gehört aber kein Stylus zum Lieferumfang.

Das Display löst mit Full HD (1920 × 1080 Pixel) auf und nutzt blickwinkelstabile IPS-Technik. Der Farbraum entspricht etwa sRGB, verfügt über eine neutrale Abstimmung und stellt Fotos und Videos natürlich dar. Der Kontrast liegt für ein IPS-Panel mit rund 1600:1 auf einem guten Niveau. Aufgrund der maximalen Helligkeit von rund 280 cd/m<sup>2</sup> ist es auch möglich, mit dem Chromebook auf dem Balkon und im Garten zu arbeiten.

### Ausstattung

Der niedrige Preis fordert vor allem bei den Multimedia-Fähigkeiten seinen Tribut. So nimmt die eingebaute Webcam Videos nur mit 720p auf und liegt bei der Bildqualität etwa auf dem Niveau von Frontkameras von Mittelklasse-Smartphones. Zudem ist die Kamera auf relativ viel Licht angewiesen, denn andernfalls wirken die Aufnahmen zu dunkel, etwas flau und zeigen eine leichte Körnung nebst Bildrauschen. Die zwei nach unten gerichteten Lautsprecher sind nicht besonders laut und klingen dumpf und bassarm. Zum Videoschauen oder Spielen ist es deshalb sinnvoll, Kopfhörer anzuschließen.

Das Spin 513 hat auf jeder Seite eine USB-C-Buchse. Das ist vor allem beim Aufladen praktisch, denn man kann das Kabel direkt und ohne lästige Schleifen auf dem Tisch zur Steckdose führen, egal auf welcher Seite sie sich befindet. Zudem steht ein USB-A-Anschluss bereit. Einen HDMI-Ausgang gibt es nicht, stattdessen lässt sich am USB-C-Anschluss ein DisplayPort-Signal abgreifen. Auf einen Speicherkartenleser oder einen Fingerabdrucksensor muss man beim Spin 513 verzichten. Dafür wartet es mir Gorilla Glas am Display und dem Touchpad auf, was beide Komponenten vor Kratzern schützen soll.

Unser Testgerät lief mit der aktuellen Version 91 von Chrome OS inklusive aktiverter Unterstützung von Android-Apps und Linux-Programmen (siehe c't 15/21, S. 28). Über die Kommandozeile der Linux-Umgebung ließen sich die App-Stores KDE Plasma Discover, Gnome Soft-

ware Center sowie Flatpak mitsamt ihren grafischen Oberflächen problemlos installieren. Sofern man nicht unzählige Programme installiert, reichen die 64 GByte interner Speicher des Spin 513 im Alltag aus.

Unter der Haube steckt ein Snapdragon 7c von Qualcomm. Dieses System-on-Chip nutzt als CPU die Kryo 468 mit sechs schwächeren, aber effizienteren Cortex-A55-Kernen und zwei starken Cortex-A76-Cores bei 2,1 GHz. Zusammen mit den 4 GByte RAM ließ sich im Test flott arbeiten. Bei Benchmarks schnitt das Spin 513 im Vergleich mit anderen Chromebooks der Mittelklasse gut ab. Im Geekbench erreicht es ähnliche Werte, wie das auf Seite 98 getestete Windows-Notebook mit Snapdragon 7c. Ein positiver Nebeneffekt: Das System kommt ohne Lüfter aus und ist somit mucks-mäuschenstill.

Sofern man keine Linux-Anwendungen für 3D-Modelling wie Blender oder Programme wie Kdenlive für Videoschnitt nutzen möchte, reicht die Performance völlig aus. Selbst wenn wir etliche Browser-Tabs offen hielten und parallel Android-Apps liefen, stellten wir keine Leistungseinbrüche fest.

Der Akku hat eine Kapazität von 4670 mAh. Damit erreichten wir die von Acer versprochene maximale Laufzeit von rund 14 Stunden nicht – zumindest nicht bei einer Bildschirmhelligkeit von 200 cd/m<sup>2</sup>. Je nach Anwendung hielt das Spin 513 in unseren Tests zwischen rund 7 bis 11 Stunden durch und lag damit im Mittelfeld unserer jüngeren Chromebook-Tests.

## Fazit

Das Spin 513 von Acer bringt Allrounder-Fähigkeiten mit. So hat es genug Leistung und Ausdauer, um damit komfortabel sein Tagwerk zu verrichten und abends bei einem Spiel oder Video zu entspannen, sofern man den dünnen Klang der Lautsprecher akzeptiert. Aufgrund des geringen Gewichts und der kompakten Abmessungen taugt das Spin 513 als Begleiter für unterwegs, macht aber auch als Notebook fürs Homeoffice eine gute Figur. Der Akku hält zwar nicht überragend lang, bringt einen aber locker über den gesamten Tag.

Mit einem Preis von rund 400 Euro zeichnet sich das Chromebook durch ein gutes Preis/Leistungsverhältnis aus. Auf Wunsch bekommt man das Spin 513 auch mit mehr RAM und größerem Speicher. Die maximale Ausbaustufe des Spin 513 kostet rund 650 Euro und bringt 8 GByte RAM sowie 128 GByte internen Speicher und obendrein ein LTE-Modem mit.

(spo@ct.de) ct

## Acer Spin 513

Chromebook	
Hersteller, URL	Acer, acer.de
Display	IPS-LCD, 13,3", 1920 × 1080, 16:9, 1 ... 280 cd/m <sup>2</sup> , 1650:1, spiegelnd, 10-Punkt-Touch
SoC (CPU / GPU)	Qualcomm Snapdragon 7c (Kryo 468: 6 × 1,7 GHz, 2 × 2,1 GHz / Adreno 618)
Speicher	4 GByte / 64 GByte
Schnittstellen	1 × USB-A (5 GBit/s), 2 × USB-C (5 GBit/s, inkl. DisplayPort), Audio (3,5-mm-Klinke), Wi-Fi 5, Bluetooth 5.0
Ausstattung	Webcam (720p), Lautsprecher (Stereo), 360-Grad-Scharnier, Gorilla Glass
Akkukapazität / Laufzeit: Videowiedergabe / -Stream / Spielen / Surfen	4670 mAh / 7,5 h / 9 h / 7 h / 11 h
Abmessungen / Gewicht	31 cm × 21 cm × 1,6 cm / 1,3 kg
Preis / Garantie	420 € / 24 Monate

Es gibt 10 Arten von Menschen.

iX-Leser und die anderen.



3x als Heft



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)

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

49 (0)541 800 09 120



# NÜC de France

## Mini-PC Bleujour Kubb Gen 11 mit Designgehäuse

**Die französische Firma Bleujour verkauft Mini-PCs mit ungewöhnlich gestalteten Gehäusen; in der jüngsten Generation rechnet ein aktueller Intel-Mobilprozessor.**

Von Christof Windeck

**W**enn der Computer schon auf dem Tisch steht, dann soll er wenigstens gut aussehen. Frei nach diesem Motto

schneidert die Firma Bleujour aus Toulouse schicke Gewänder für Minicomputer, unter anderem etwa aus Holz. Konventioneller gekleidet, nämlich in dunkelgraues Metall mit leichtem Glitzereffekt, ist der „Kubb Gen 11 Graphite“. Kubb ist eine Verballhornung des französischen Wortes für Würfel (le cube) und würfelig sieht das Kistchen auch aus.

Im Wesentlichen entspricht die Technik des Kubb Gen 11 dem in c't 7/2021 getesteten Intel NUC11TNKi5 mit Mobilprozessor der elften Core-i-Generation „Tiger Lake“ [1]. Folglich sind Rechenleistung und Schnittstellenausstattung nahezu identisch. Während es sich beim NUC11TNKi5

jedoch um einen Barebone zum Selbstbestücken handelt, liefert Bleujour einen Komplett-PC mit Garantie und Betriebssystem. Die Preise reichen von 640 Euro für die langsamste Version mit dem Doppelkernner Core i3-1115G4 im Verbund mit 8 GByte RAM, 256-GByte-SSD und Linux Mint bis 2000 Euro für das Spitzenmodell mit Core i7-1165G7, 64 GByte RAM, zwei 2-TByte-SSDs und Windows 10 Pro.

Wir erhielten zum Test eine mittlere Version mit Core i5-1135G7, 16 GByte RAM und 512-GByte-SSD, die inklusive Windows 1036 Euro kostet. Der kräftige Vierkernprozessor eignet sich mit genügend Speicher auch für Foto- und Videobearbeitung. Die erste SSD im System ist stets eine NVMe-SSD in M.2-Bauform; Bleujour baut die Seagate FireCuda 520 ein, die zwar flotter ist als eine PCIe-3.0-SSD, aber das Potenzial von PCIe 4.0 nicht ausreicht. Aber für die praktische Nutzung ist das kein Nachteil. Die zweite SSD ist stets eine mit SATA-Anschluss.

### Solides Blech

Das Gehäuse wirkt solide, überzeugt aber nicht auf ganzer Linie: Es fehlen Füßchen, sodass nur der relativ dicke Lack vor Kratzern auf empfindlichen (Design-)Tischplatten schützt. Und unser Testgerät stand nicht absolut plan, sondern wackelte minimal – im Grunde unwesentlich, aber dem Preis nicht angemessen. Bleujour verbietet von Front- und Seitenflächen jegliche Buchsen und Schalter; auch der Einschalttaster sitzt an der Rückseite. Das recht klobige Netzteil muss man unter dem Tisch verstecken. Bleujour denkt aber mit und packt außer einem HDMI-Kabel auch einen brauchbaren USB-Audio-Adapter in den Karton, weil der Kubb Gen 11 keine Klinkenbuchse hat. Gut fürs nachträgliche Aufrüsten, aber ein Nachteil für die Performance ist die Bestückung mit nur einem einzigen Speichermodul. Das optional lieferbare Zweikanal-RAM würde der integrierten Xe-GPU fast 50 Prozent Mehrleistung im Benchmark 3DMark Fire Strike bringen. Für leistungshungrige Spiele taugt der Grafikprozessor allerdings ohnehin nicht.

Während der NUC dank Kunststoffteilen im Gehäuse mit internen WLAN-Antennen auskommt, schraubt Bleujour zwei externe hinten an den Kubb. Die scheinen nicht optimal angepasst zu sein, bei unserer Messung über die 20-Meter-Distanz durch Wände ergaben sich deutlich niedrigere Transferraten als beim NUC. Auf

Kurzdistanz funkts das Wi-Fi-6-Modul aber sehr flott, vor allem im 5-GHz-Band.

## Sparsamer Betrieb

Der Kubb Gen 11 kam mit einer neueren BIOS-Version 0057 als unser NUC-Testgerät (0043); die war vermutlich für die mit 4,6 statt 6,8 Watt deutlich niedrigere Leistungsaufnahme im Leerlauf verantwortlich. Leider jedoch rauscht der Lüfter im Kubb Gen 11 etwas lauter als im NUC, nämlich schon im Leerlauf mit 0,3 (statt 0,1) Sone und unter Volllast mit 1,6 statt 1 Sone. Das ist nicht flüsterleise, aber noch erträglich. Gibt man der Lüfterregelung per BIOS-Setup einen „Minimum Duty Cycle“ von 20 statt 42 Prozent vor, wird der PC leiser.

Leider hat Intel die in [1] erwähnten Probleme mit der Erkennung schneller USB-3.2-Gen-2x2-SSDs an den USB-C-Buchsen noch nicht gelöst. Unsere WD-Black-P50-SSD, die eigentlich über 2 GByte/s schafft, nahm nur per USB-A-Buchse Kontakt auf und lieferte darüber dank USB 3.2 Gen 2 immerhin 1 GByte/s. Deshalb ist es besonders schade, dass am Kubb nur eine einzige USB-A-Buchse mit bis zu 10 GBit/s nutzbar ist; der NUC hat vorne noch zwei weitere. Ein USB-C-Hub funktionierte an den USB-C-Buchsen aber problemlos.

Bleujour hatte die empfehlenswerte und von Microsoft für Computer mit Windows-10-Logo verlangte Secure-Boot-Option im BIOS-Setup nicht aktiviert. Mit der Fastboot-Option im BIOS-Setup lässt sich die Bootdauer von 23 auf 14 Sekunden verkürzen.

## Fazit

Der Kubb Gen 11 Graphite ist ein flotter Büro-PC, der dank starkem Quad-Core-Prozessor auch aufwendigere Rechenaufgaben bewältigt. Anders als viele Tiger-Lake-Notebooks lässt er sich auf bis zu 64 GByte RAM und 4 TByte SSD-Speicherplatz hochrüsten. Für das Würfelgehäuse und die flexible Konfiguration verlangt Bleujour allerdings einen kräftigen Aufpreis. Gemessen daran hätten wir zwar etwas mehr Feinschliff erwartet, dennoch sticht der Kubb aus der Masse heraus.

(ciw@ct.de) ct

## Literatur

[1] Christof Windeck, Tiger-Box, Mini-PC-Barebone Intel NUC11 mit Tiger-Lake-Prozessor Core i5-1135G7, c't 7/2021, S. 100

## Bleujour Kubb Gen 11 „Graphite“

### Mini-PC mit Intel Core i5-1135G7

Hersteller, URL	Bleujour, bleujour.com
Prozessor	Core i5-1135G7 (4 Kerne, 8 Threads, 2,4 – 4,2 GHz, 28 Watt, Tiger Lake)
Grafik	Intel Xe, 80 Execution Units, in CPU integriert (IGP)
RAM (Slots / frei)	16 GByte (2 × SODIMM / 1 <sup>1</sup> ), maximal 64 GByte DDR4-3200
NVMe-SSD	500 GByte / PCIe 4.0 x4 (Seagate FireCuda 520, ZP500GM30002)
Anschlüsse vorn	–
Anschlüsse hinten	2 × HDMI 2.0b, 2 × USB-C (USB 4/Thunderbolt 4), 1 × RJ-45, 1 × USB-A 3.2 Gen 2, 5 × USB-A 2.0, Stromversorgung
Festplattenschächte	1 × M.2-2280 (PCIe 3.0 x4), 1 × 2,5" (SATA)
2,5-Gbit/s-Ethernet / WLAN	Intel I225-LM / Intel AX201 (Wi-Fi 6, 2 × 2)
Soundchip / TPM	– / Firmware-TPM (fTPM 2.0)
Betriebssystem	Windows 10 Pro
Netzteil	Chicony A15-120P1A (19 V/120 W), 7,5 cm × 2,6 cm × 16 cm, Kleeblattstecker, Kabel 1,75 m
Abmessungen Gehäuse	12 cm × 12 cm × 14 cm (Tiefe inklusive WLAN-Antennen)
mitgeliefertes Zubehör	HDMI-Kabel, USB-Audio-Adapter

### Messwerte (Windows 10, FHD-Display, USB-Tastatur - Maus)

BIOS-Version / UEFI Secure Boot	0057 / abgeschaltet
Cinebench R23 Single/Multi	1368 / 5557 Punkte
3DMark Fire Strike	2435 Punkte
PCIe-4.0-SSD (lesen / schreiben)	5,0 / 2,5 GByte/s
USB-C 3.2 Gen 2 (lesen / schreiben)	1,0 / 0,9 GByte/s
WLAN-Durchsatz 2,4 / 5 GHz	nah: 188 / 766 MBit/s, 20 Meter: 22 / 76 MBit/s
Bootdauer	23 Sekunden
Leistungsaufn. Soft-off / Energie sparen	0,9 / 5,9 W
Leerlauf / Vollast CPU / CPU + GPU	4,6 / 48 (67 <sup>2</sup> ) / 48 W
Geräusch im Leerlauf / CPU-Volllast	0,3 (⊕⊕) / 1,6 sone (⊖)
Preis Testgerät / Garantie	1036 € / 3 Jahre Bring-in
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht – fehlt	<sup>1</sup> optional auch 2 × 8 GByte lieferbar <sup>2</sup> für 28 Sekunden (Power Limit 2, PL2)



Anders als Intels NUC hat der Kubb Gen 11 nur hinten Anschlüsse; HDMI- und USB-A-Buchsen sitzen um 180 Grad verdreht im Gehäuse.



# Transport-versicherung

## Externe SSD mit Hardware-Verschlüsselung

**Die robuste externe SSD DataLocker DL4 verschlüsselt die Daten beim Speichern so, dass sie bei Verlust des Geräts geschützt sind. Zum Entsperren tippt man sein Passwort am Touchscreen des Gehäuses ein.**

Von Lutz Labs

Fällt eine externe Festplatte in fremde Hände, erhält der neue Besitzer möglicherweise Daten, die ihn nichts angehen. Um davor zu schützen, verschlüsselt die DataLocker DL4 ihren Inhalt standardmäßig mit AES-256 im XTS-Modus. Mit Preisen ab 360 Euro ist das Laufwerk vornehmlich für den Unternehmenseinsatz zugeschnitten, dazu gesellen sich bei besonderen Anforderungen weitere Kosten in Form einer Jahreslizenz für eine Online-Anwendung.

Schließt man die DL4 an einen PC an, erwartet das Gerät nach einer kurzen

Startphase ein Passwort. Damit andere dies durch die Fingerpositionen beim Eintippen nicht erraten können, vertauscht die Firmware bei jedem Start die Zeichen auf dem Touchdisplay.

### Umständliche Einstellungen

Nach der Eingabe des Passworts hat man ein paar Sekunden Zeit, den Konfigurationsmodus der DL4 aufzurufen. In diesem lassen sich Passwörter vergeben, andere Nutzer einrichten und Anforderungen an die Passwortkomplexität einstellen. In der Standardeinstellung löscht das Laufwerk nach zehnmaliger Passwort-Falscheingabe alle Daten; man kann jedoch auch einstellen, dass es bei zu häufiger Falscheingabe die Firmware löscht – nach dieser Selbstzerstörung kann selbst der Hersteller die DL4 nicht mehr reparieren.

Lässt man nach der Eingabe des Passworts ein paar Sekunden verstrecken, meldet sich die DL4 wie ein gewöhnliches USB-Laufwerk am PC an. Mit rund 230 MByte/s beim Lesen und Schreiben ist sie zwar nicht besonders flott, aber diese Geschwindigkeit behielt unser 1-TByte-SSD-

Modell über die gesamte Kapazität fast bei.

### Komfortabler konfigurieren

Unternehmen, die eine große Anzahl von DL4 im Einsatz haben, greifen zur Konfiguration besser zur Online-Verwaltung via SafeConsole. Dann startet nach der Passworteingabe am Gerät zunächst eine Windows-Anwendung, die Kontakt mit der SafeConsole aufnimmt und sich von dieser die Erlaubnis holt, das Laufwerk freizuschalten. Die Nutzung der SafeConsole kostet zusätzlich: Neben einer Setup-Gebühr von 1189 Euro fallen Lizenzkosten für eine ein- oder dreijährige Nutzung an, die bei 29 beziehungsweise 24 Euro pro Jahr und pro Gerät liegen.

Die Verwaltung über die SafeConsole muss man einmalig direkt im DL4-Konfigurationsmenü einstellen. Anschließend sind Laufwerk und Verwaltungssoftware untrennbar miteinander verbunden. Man kann auch einstellen, dass eine Verbindung zur SafeConsole etwa nur bei jeder zehnten Nutzung notwendig ist, damit Nutzer auch unterwegs ohne Netz auf die Daten zugreifen können. Ebenso lassen sich Länder oder Service-Provider definieren, bei denen eine Nutzung verboten oder erlaubt ist, man kann erlaubte oder verbotene Dateitypen setzen oder eine ausschließlich lesende Nutzung. Geräte lassen sich aus der Ferne sperren oder als verloren definieren sowie mit einem neuen Passwort versehen, falls der Nutzer seines vergessen hat.

Für einen Privatnutzer sind die Kosten für Gerät und Online-Verwaltung zu hoch, das Gerät allein mag für Anwender mit hohem Sicherheitsbedürfnis noch eine Option sein. Unternehmen können die Kombination aus DL4 und SafeConsole hingegen nutzen, um den Verlust von Daten mit hoher Sicherheit zu verhindern.

(ll@ct.de) ct

### Literatur

- [1] Lutz Labs, Sicher transportiert, Robuste externe SSD mit Verschlüsselung, c't 25/2015, S. 60

### DataLocker DL4

USB-SSD mit Hardware-Verschlüsselung	
Modellnummer	DL4-SSD-1TB-FE
Hersteller, URL	DataLocker, <a href="http://datalocker.com">datalocker.com</a>
Anschluss	USB 3.2 Gen 2, USB Typ C
Zertifizierungen	FIPS 140-2 Level 3, IP64
Preise (UVP)	Festplatte: 500 GByte-2 TByte (360 €-580 €), SSD: 1 TByte-15,3 TByte (580 €-5920 €)

# KI mischt mit

## Audiorbeitung mit SpectraLayers 8

**Es grenzt an Zauberei, wenn SpectraLayers von Steinberg aus kompletten Songs den Gesang, das Schlagzeug, den Bass und weitere Instrumente extrahiert. Die neue Version des Audio-Editors hilft darüber hinaus bei schlecht isolierten Mikrofonaufnahmen und weiteren Problemen der Audio-Restoration und Postproduktion.**

Von Hartmut Gieselmann

Steinberg hat seinen Audio-Editor SpectraLayers in Version 8 um zahlreiche Tricks erweitert, die beispielsweise atmosphärische Geräusche und den Frequenzverlauf einer Aufnahme auf eine zweite kopieren. Der Editor stellt Audiodateien in einer Spektralanalyse dar. Die X-Achse gibt die Zeit, die Y-Achse den Frequenzbereich wieder. Mit Retuschierwerkzeugen, die man sonst von Fotobearbeitungen kennt, lassen sich einzelne Töne markieren und anschließend verstärken, löschen, verschieben oder kopieren. Wenn etwa bei einer Aufnahme ein Handy im Hintergrund bimmelt, lassen sich die Störgeräusche mit SpectraLayers 8 meist vollständig entfernen.

Weil solche manuellen Arbeiten zuweilen sehr aufwendig sind, hilft die Soft-

ware mit KI. Spektakulär war die Neuerung im vergangenen Jahr, aus fertigen Songs einzelne Spuren für Schlagzeug, Bass, Gesang, Klavier und übrige Instrumente zu extrahieren – inklusive der zugehörigen Hallfahnen. Die Automatik legt für jede Spur einen eigenen Layer an, der sich anschließend weiter bearbeiten lässt. So genügt etwa ein Mausklick, um den Gesang für eine Karaokeversion komplett zu entfernen.

Zwar hört man immer noch leichte Artefakte, wenn man eine extrahierte Spur einzeln abhört. Wenn jedoch SpectraLayers alle extrahierten Spuren wieder zusammensetzt, konnten wir so gut wie keine Unterschiede zum Original ausmachen. Ebenso hervorragend arbeitet der „Voice-Denoiser“, der eine Stimme aus einem Musikstück oder lauten Störgeräuschen herausfiltert. Die Qualität genügt nicht nur Forensikern, sondern auch Remixern, die um die Stimme herum einen neuen Song stricken wollen.

### Eingedämmte Blutungen

Bei Aufnahmen eines Schlagzeugs oder eines Sängers mit Akustik-Gitarre lassen sich die Mikrofone nicht komplett isolieren. Deshalb landen unvermeidlich fremde Töne auf den einzelnen Spuren. Dieses „Bleeding“ verhindert später eine optimale Einzelbearbeitung der Instrumente im Mix. SpectraLayers 8 konnte diese Übersprechungen beim Test mit zwei Mikrofonen (Gesang, Gitarre) immerhin deutlich verringern – wenn auch nicht ohne

weitere Klangverschlechterungen zu hundert Prozent ausblenden.

Ebenso wie beim De-Clipping, De-Essing, bei der Hall- und Brumm-Reduktion nimmt der Editor die Berechnungen stets offline vor. Der Anwender muss meist einen Schwellwert und eine Effektstärke einstellen und dann je nach Länge des Stücks bis zu 30 Sekunden warten, bevor er eine Vorschau anhören kann. Diese berechnet der Editor bei jeder kleinen Änderung neu. Im Unterschied zu einer typischen Digital Audio Workstation (DAW) wie Cubase klappt das nicht in Echtzeit, während man am Regler dreht.

Deshalb kostet es mitunter viel Zeit, bis man optimale Einstellungen gefunden hat. Gewiss erlaubt SpectraLayers dank der grafischen Darstellung eine viel präzisere Eingrenzung, auf welchen Frequenz- und Zeitabschnitt ein Effekt wirken soll. Wenn die Audioprobleme aber nicht zu groß sind, gelingen manche Reparaturen mit einer Plug-in-Sammlung wie iZotope RX schneller, weil man dort die Auswirkungen einer Einstellung sofort hört.

### Fazit

Aufgrund seiner Algorithmen ist SpectraLayers ein sehr mächtiges Bearbeitungswerkzeug, das als letztes Mittel Probleme beheben kann, wenn einfachere und schnellere Methoden versagen. Dank der ARA-2-Schnittstelle lässt sich das Programm in viele DAWs ebenso einfach einbinden wie die weit verbreitete Tonhöhen-Korrektursoftware Melodyne. DAWs wie Ableton Live oder Logic Pro X rufen SpectraLayers hingegen als externen Editor auf und übergeben ihm die Audiospuren.

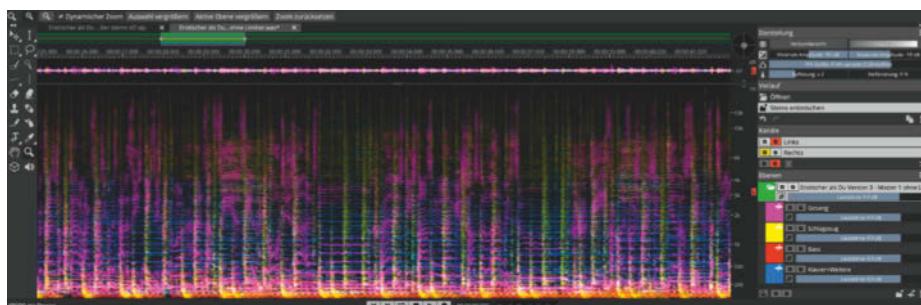
Für Anwender, die nicht in 7.1, sondern nur in Stereo arbeiten und lediglich Gesang, aber keine weiteren Spuren aus kompletten Mixen extrahieren wollen, genügt die günstigere Elements-Version. Einzelheiten zum riesigen Funktionsumfang, den wir hier nur anreißen konnten, listet die Webseite von Steinberg auf. Bei der Einarbeitung helfen umfangreiche YouTube-Tutorials des Herstellers.

(hag@ct.de) ct

### Steinberg SpectraLayers 8

#### Audio-Editor

Hersteller, URL	Steinberg, <a href="http://steinberg.net">steinberg.net</a>
Systemanf.	Windows ab 10, macOS ab 10.14
Kopierschutz	e-Licenser (Software oder USB-Stick)
Preise	Elements: 80 €, Pro: 300 €



Komplette Songs entmischt SpectraLayers auf vier farbig markierten Einzelspuren.



## Keinmucks-monster

**Der CPU-Kühler Noctua NH-P1 bewahrt Prozessoren mit bis zu acht Kernen ohne Lüfter vor dem Überhitzen und arbeitet somit lautlos.**

Geräuschlose Desktop-Rechner von der Stange gibt es meist nur als Mini-PCs mit sparsamen Mobil-CPU. Der Prozessorkühler NH-P1 von Noctua richtet sich hingegen an PC-Bastler, die ein Passivsystem mit leistungsstarken Ryzen- und Core-i-Desktopprozessoren mit bis zu acht Kernen bauen möchten. Damit das klappt, ist beim CPU-Kühler NH-P1 alles eine Nummer größer als normal. Die Abwärme leiten sechs Kupfer-Heatpipes mit jeweils sechs Millimetern Durchmesser zum riesigen Lamellenpaket. Diese aus Aluminium gefertigten Bleche sind deutlich dicker und weiter voneinander entfernt als bei üblichen Prozessorkühlern, weil die natürliche Konvektion so besser funktionieren soll.

Zusammen ergibt das einen rund 1,2 Kilogramm schweren, fast quadratischen Block. Aufgrund seiner Abmessungen findet der NH-P1 nicht in jedem beliebigen PC-Gehäuse genug Platz. Vor dem Kauf sollte man deshalb die umfangreichen Kompatibilitätslisten auf der Hersteller-Website studieren (siehe ct.de/yhwt).

Grundsätzlich passt der Passivkühler mit Ausnahme der Ryzen Threadripper auf alle gängigen AMD- und Intel-Prozessoren mit den Fassungen AM4, LGA1200 und LGA2066. Trotz der gigantischen Abmessungen und der großen Masse ist die Kühlleistung mangels Lüfter limitiert. Statt der Thermal Design Power verwendet Noctua ein eigenes Bewertungssystem. Wir haben uns für den Achtkerner Ryzen 7 3700X und den Kombiprozessor Ryzen 7 4650G mit

sechs Kernen entschieden; für beide ist der Kühler laut Hersteller freigegeben.

Als Testsystem kam unser Bauvorschlag für den Ryzen Allrounder aus dem Herbst vergangenen Jahres mit offenem Gehäusedach zum Einsatz (siehe c't 24/2020, S. 26). Die Montage gelingt dank des mitgelieferten Torx-Schraubendrehers recht flott innerhalb von 10 bis 15 Minuten, unter anderem weil die Konterplatte des Mainboards weiterverwendet wird. Die Gehäuselüfter haben wir alle ausgebaut, der hintere hätte dem NH-P1 im Weg gestanden. Unter längerer Vollast mit dem Render-Programm Blender erreichte der Ryzen 3700X seine Maximaltemperatur von 95 °C. Dadurch schöpft er seinen Turbotakt nicht mehr komplett aus. Mit 4,025 GHz lag die Taktfrequenz dabei aber immer noch deutlich über Nominaltakt (3,6 GHz). Mit dem Monsterkühler statt dem Boxed-Kühler von AMD sank die Rechenleistung um 2,5 Prozent.

Der Kombiprozessor Ryzen 5 4650G rechnete mit dem NH-P1 ebenfalls rund 2,5 Prozent langsamer als mit einem Luftkühler, erreichte mit 87 °C aber noch nicht die Drosselgrenze. Die Spannungswandler des verwendeten Mainboards Gigabyte B550 Aorus Elite erwärmen sich bis auf 62 °C, was unkritisch ist. Allerdings sind auf diesen relativ große Kühlkörper angebracht, bei anderen Mainboards kann eine aktive Kühlung notwendig sein.

Der Noctua NH-P1 eignet sich aus unserer Sicht für den lautlosen Betrieb von Prozessoren der 65-Watt-Klasse, insbesondere für solche mit integrierter Grafik. Bei Systemen mit Grafikkarte ist der recht teure Passivkühler für 110 Euro nicht sinnvoll, weil die Lüfter auf den Karten meist lauter sind als der CPU-Luftkühler. Als Kompromiss für leistungsstarke Prozessoren bietet Noctua für 30 Euro den PWM-Lüfter NF-A12x25 LS-PWM an, der bei null Prozent PWM-Signal stoppt und somit zumindest einen semipassiven Betrieb ermöglicht. (chh@ct.de)

**Kompatibilitätsliste bei Noctua:**  
[ct.de/yhwt](http://ct.de/yhwt)

## Noctua NH-P1

Lüfterloser Prozessorkühler	
Hersteller, URL	Noctua, noctua.at
Abmessungen (H × B × T) / Gewicht	15,8 cm × 15,4 cm × 14,9 cm / 1,2 kg
Lieferumfang	Wärmeleitpaste, Schraubendreher, Reinigungstuch
Preis / Garantie	110 € / 6 Jahre



## Günst-schnüffler

**IKEAs Luftqualitätssensor Vindriktning zählt Partikel in der Luft und warnt per LED.**

Nur 10 Euro verlangt IKEA für den kompakten Partikelsensor Vindriktning, der Schwebeteilchen der Kategorie PM 2.5 zählt. Im Test sprang die eingebaute Ampel zuverlässig um, wenn man im selben Raum warm duschte, kochte oder scharf anbriet. Um vor potenziell (Corona-)virenhaltigen Aerosolen zu warnen, sind Partikel der Größenklasse PM 2.5 allenfalls ein grober Anhaltspunkt.

IKEA bewirbt den kleinen Sensor in Kombination mit einem Luftreiniger: „Mit dem Vindriktning Luftqualitätssensor kannst du die Luftqualität [...] überprüfen und sie bei Bedarf mit dem Föruftig Luftreiniger verbessern.“ Wer gehofft hatte, dass beide per Funk miteinander sprechen, wird enttäuscht. Der Mensch muss selbst den Luftreiniger anknipsen.

Nützlich ist der Sensor mit dem unausprechlichen Namen für alle, die gerne mal vergessen zu lüften. Bastler, die mit Arduino oder ESP selbst eine Smart-Home-Anbindung nachrüsten wollen, bekommen attraktive Hardware im schönen Gehäuse: Die Partikel zählt ein Sensor vom Typ PM1006 des Herstellers Cubic; der allein kostet in China schon 12 US-Dollar. Auf der IKEA-Platine sind die Kontakte für PWM und UART bastelfreundlich herausgeführt und beschriftet. (jam@ct.de)

## IKEA Vindriktning

Luftqualitätssensor	
Hersteller, URL	IKEA, ikea.de
Signalisierung	LEDs in Ampelfarben
Spannungsversorgung	5 Volt, USB-C (Kabel und Netzteil nicht im Lieferumfang)
Preis	9,99 €



## Elegante Gamer-Sitzschale

Für seinen Stuhl Embody Gaming Chair hat sich Möbelhersteller Herman Miller mit Gamingspezialist Logitech zusammengetan. Heraus kam ein schickes ergonomisches Sitzmöbel.

Sowohl der leuchtend blaue Rücken als auch ein dezentes Logo im Lehnengezugs und eine Lasche im Rücken – die sich im Test schnell ablöste – verweisen auf Logitech. Mechanisch entspricht der Stuhl der Bürovariante „Embody“. Er wird aufgebaut in einer großen Kiste geliefert, ist also sofort einsatzbereit. Anstelle einer Bedienungsanleitung verweist der Hersteller auf eine digitale Anleitung im Internet – etwas sparsam für den 1400 Euro teuren Stuhl.

Das Besondere des schicken Möbels sind die vielen einzelnen Stützpunkte in Rücken und Sitzfläche: Statt über eine Lordosenstütze kann man mit Drehknöpfen und Hebeln den Anpressdruck der Stützpunkte und der Rückenlehne gezielt an den eigenen Körper anpassen – das kam bei den meisten unserer Tester sehr gut an. Wie weit man sich mit dem gefederten Stuhlrücken zurücklehnen kann, lässt sich in kleinen Stufen variieren.

Die Sitzhöhe ist über einen Gasdruckzylinder zwischen 46–60 Zentimeter einstellbar; der Stuhl trägt laut Hersteller dauerhaft bis zu 136 Kilogramm. Die Höhe der Armlehen lässt sich in 10 Stufen leichtgängig einstellen. Um ihren Abstand zu verändern, muss man kräftig gegen die Armlehen drücken, doch weil sich der

Abstand nicht fixieren lässt, drückten einige Tester die Lehnen beim Aufstehen dennoch zuweilen auseinander. Die Länge der Sitzfläche kann man über eine interessante Ausrollmechanik an die eigene Beinlänge anpassen – leider hakt diese Hebelmechanik etwas.

Die gummierten Doppelrollen des fünfarmigen Aluminiumfußes schonen Laminat und Parkett, auf Teppich fanden wir sie etwas schwergängig. Unser Hardware-Assistent gab den Stuhl nach kurzem Antesten sofort – und mit Bedauern – zurück: Er hatte bei Messungen an einem Testsystem einen kräftigen elektrostatischen Schlag bekommen, denn die Kunststoffrollen sind nicht leitfähig.

Ein Tester fand den nahtlos gesteppten Polyesterbezug zu plastikmäßig, die anderen kamen auch an heißen Sommertagen gut damit zurecht. Die vom Hersteller versprochene Kühlwirkung des mit Kupfer angereicherten Polyurethanschaums im Sitz können wir zwar nicht bestätigen, man behält aber auch im Sommer einen kühlen Hintern auf dem Embody Chair. Ein Tester bemängelte die schlechte Reinigungsmöglichkeit von Rück- und Unterseite des Stuhls, ein zusätzlicher Staubschutz wäre der schicken Optik indes abträglich. Auch wenn es auf den ersten Blick anders aussieht, fehlt eine Kopfstütze, was für einen Gamingstuhl eher ungewöhnlich, aber laut Hersteller gewollt ist.

Trotz einiger kleinen Schwächen empfiehlt sich der hippe Embody Gaming Chair sowohl für Gamer als auch für Büroarbeiter – zumal die Nicht-Gaming-Variante desselben Stuhls 100 Euro teurer ist. Dank seiner feinen Einstellmöglichkeiten hilft der Stuhl, Arbeitszeiten am Schreibtisch rückenschonend und bequem zu gestalten. Allerdings lässt sich Herman Miller die durchdachte Ergonomie ordentlich bezahlen – gibt aber auch 12 Jahre Garantie auf den Stuhl. Man bekommt die Gaming-Variante ausschließlich direkt bei Herman Miller und darf sie bis zu 14 Tage Probesitzen. (uk@ct.de)

## Embody Gaming Chair

### Ergonomischer Büro- und Gamingstuhl

Hersteller, URL	Herman Miller in Kooperation mit Logitech, degaming.hermannmiller.com
Einstellmöglichkeiten	Sitzhöhe und -tiefe, Armlehnenhöhe und -abstand, Anpressdruck Lenden- und Kreuzbeinstütze, Neigung Rückenlehne
Garantie	12 Jahre
Preis	1400 €



## Mängelware

**Tendas WiFi-6-Router TX3 lockt mit einem niedrigen Preis. Die Performance stimmt, anderes nicht.**

In den Messungen machte der TX3 eine gute Figur: Wi-Fi 6 mit zwei MIMO-Streams lieferte 260 MBit/s netto auf Distanz. Der Router ließ sich mit dem Wizard über ein externes Modem auch am Telekom-VDSL nutzen, nur ohne Multicast-IPTV. An weitere wichtige Einstellungen (IPv6, Zeitzone, WPA3-Verschlüsselung, Gastnetz) muss man selbst denken.

Irritierenderweise funkte das Gerät im 5-GHz-Band immer wieder auf dem für BFWA reservierten Kanal 149, war es doch auf Betrieb in den USA voreingestellt. Man muss es manuell auf Kanal 36 bis 48 setzen, um hierzulande legal zu funken. Andere gehen nicht, denn DFS fehlt. Tenda will die Regionseinstellung per Firmware-Update korrigieren.

Die wichtige Wi-Fi-6-Funktion OFDMA ist ab Werk abgeschaltet, TWT wird laut WLAN-Beacons nicht unterstützt. So gilt: Warten Sie mit dem Kauf, bis die Firmware verbessert ist. (ea@ct.de)

## Tenda TX3

WLAN-Router	
Hersteller, URL	Tenda, tendacn.com/de
WLAN (MIMO-Streams)	2 × Wi-Fi 6 (2) alias IEEE 802.11ax-600/1200, WPA3, kein DFS, WPS
Bedienelemente	Reset, WPS, 1 Statusleuchte
Anschlüsse	4 × RJ45 (Gigabit-Ethernet)
getestete Firmware	16.03.13.11_multi
NAT-Perf. PPPoE (DS / US)	829 / 515 MBit/s
NAT-Perf. IP-zu-IP (DS / US)	950 / 951 MBit/s
WLAN 2,4 GHz nah / 20 m <sup>1</sup>	335 / 202–287 MBit/s
5 GHz nah / 20 m <sup>1</sup>	796 / 261–262 MBit/s
Leistungsaufnahme <sup>2</sup>	4,8 Watt / 8,9 VA
jährliche Stromkosten <sup>2</sup>	13 €
Preis	69 €

<sup>1</sup> gegen Intel AX200

<sup>2</sup> idle, bei Dauerbetrieb und 30 Cent/kWh



# Musikalisches Bild

## Lautsprecher in Bilderrahmen-Optik von IKEA mit Sonos-Technik

**Ein WLAN-Lautsprecher in Form eines Bilderrahmens: Der IKEA Symfonisk mit Sonos-Technik ist für viele Zimmer vielleicht genau die richtige Mischung aus sattem Klang und schöner Optik.**

Von Berti Kolbow-Lehradt

Der neuste Lautsprecher aus Ikeas Reihe Symfonisk, die in Zusammenarbeit mit Sonos entsteht, ist Klang- und Designobjekt in einem. Wie die im Jahr 2019 vorgestellten Symfonisk-Modelle in Form einer Tischleuchte und eines Bücherregals liefert IKEA den Sound-Bilderrahmen in zwei Farbvarianten aus. Eine kombiniert ein weißes Gehäuse mit hellgrau bespannter Stoffvorderseite. Bei der anderen Variante sind Gehäuse und Front schwarz. In beiden Fällen zierte ein abstraktes Muster die ungefähr DIN A2 große

Stofffront. Mit sechs Zentimetern ragt der Sound-Bilderrahmen allerdings unerwartet weit in den Raum hinein.

Das lässt immerhin genügend Platz im Rahmen für von vorne nicht sichtbare Bedien- und Montagehilfen. Mit drei Taschen lässt sich die Musik steuern. Sechs Öffnungen ermöglichen es, mit sanftem Fingerdruck die Stofffront herauszupressen und durch eine andere zu ersetzen. Zwölf Wechselfronten mit abstrakten Mustern und figürlichen Motiven bietet Ikea zum Preis von jeweils 30 Euro an. Eine Möglichkeit, eigene Motive auf die Fronten drucken zu lassen, etwa hochgeladene Fotos, existiert derzeit nicht.

Eine große Aussparung an der Rückseite bietet Platz für Anschlüsse und Kabel. Ist WLAN-Streaming keine Option, lässt sich der Lautsprecher per LAN ansprechen. Strom bezieht er über eine C7-Buchse und das mitgelieferte, 350 Zentimeter lange Netzkabel. Der dritte Steckplatz ist reserviert für ein Verbindungskabel von C8-Stecker auf C7-Buchse, mit dem sich ein zweiter Symfonisk über die gleiche Stromverbindung mitbetreiben lässt.

IKEA bietet die passenden Verbindungs-kabel „Förnimma“ mit 70 und 200 Zenti-metern Länge für 3 und 5 Euro an.

Wie alle stationären Sonos- und Symfonisk-Lautsprecher ist auch dieses Modell immer eingeschaltet. Der Standby-Verbrauch liegt mit gemessenen 2,2 Watt auf normalem Sonos-Niveau, kommt aber an die Energieeffizienz der sparsamsten Smart Speaker nicht heran.

### Fußboden oder Wand

Am schnellsten lässt sich der Symfonisk in Betrieb nehmen, indem man ihn an die Wand lehnt. Dafür liegen zwei Silikon-standfüße im Karton, die den Boden oder die Sideboard-Oberfläche vor Scheuerspu-ren schützen, Rutschpartien vermeiden und das Gehäuse akustisch vom Untergrund abkoppeln. Praktisch: Es gibt Öffnungen an einer kurzen und einer langen Kante, sodass der Rahmen wahlweise horizontal oder vertikal steht. Beim Hochheben fallen die Silikonstöpsel allerdings leicht heraus.

Für die Wandmontage dübelt man eine beiliegende Metallplatte an die Wand; ihr oberes Drittel ist angewinkelt und dient als Haken, an dem das Symfonisk-Gehäuse magnetisch Halt findet, wiederum vertikal oder horizontal. Auf der Rückseite des Lautsprechers verklebte Filzstopper reduzieren Abrieb und Vibration. Zusätzlich kann man das über drei Kilogramm schwere Stück Technik mit einem beiliegenden Stoffband sichern, das an Gehäuse und Wand angeschraubt wird.

### Sonos-typische Bedienung

Technisch ist der IKEA-Lautsprecher ein Teil des Sonos-Systems und lässt sich mit der Sonos-App S2 startklar fürs WLAN-Streaming machen. Die Software findet den Lautsprecher automatisch und lässt ihn im Sonos-System mitspielen.

Wer ein iPhone zur Hand hat, nimmt am besten noch mit Sonos' Trueplay-Verfahren eine Raumklangeinmessung vor – dann tönt der Bilderrahmen präziser. Mit Android-Geräten funktioniert das nicht – dafür kann IKEA nichts, diese Entschei-dung liegt bei Sonos. Immerhin benötigt man das iOS-Gerät nicht permanent, son-dern ein Besucher kann die IKEA-Box ein-malig einmessen. Zudem lässt sich mit den App-Reglern für Treble und Bass auf allen Geräten die Tonausgabe dem eigenen Ge-schmack anpassen.

Mit Musik füttern lässt sich der Symfonisk per WLAN aus der Sonos-App, per

AirPlay 2 aus jeder anderen kompatiblen Musik-App oder via Spotify Connect. Der Lautsprecher ordnet sich auf Wunsch in ein Stereopaar oder in ein Multiroom-Ensemble mit beliebigen Symfonisk- und Sonos-Modellen ein; Spotify-Connect-Nutzer müssen das wie gehabt in der Sonos-App anlegen, können es dann aber aus Spotify heraus direkt nutzen. Bluetooth und Klinken-Eingang fehlen.

Die IKEA-App „Home smart“ bietet sich nur in wenigen Fällen als Steuerzentrale an. Im Wesentlichen ist sie gefragt, wenn beispielsweise die Trådfri-Leuchtmittel im Takt der Symfonisk-Musik aufleuchten sollen. Ansonsten erlaubt die IKEA-App bloß, einen in der Sonos-App gestarteten Titel zu pausieren, die Lautstärke zu ändern und zum nächsten oder vorherigen Titel einer aktiven Playlist zu springen. Diese Steuerbefehle kann man auch über die drei Tasten am Gehäuse oder mit der Symfonisk-Fernbedienung geben. IKEAs Shortcut Button harmonierte im Praxistest ebenfalls mit dem neuen Lautsprecher. Per Knopfdruck kann er zum Beispiel einen zuvor verknüpften Favoriten aus der Sonos-App starten.

Über die Sprachdienste Amazon Alexa, Google Assistant und Siri lässt sich Symfonisk über einen Umweg bedienen: Da er kein Mikrofon enthält, benötigt man ein anderes Gerät als Vermittler, beispielsweise einen Smart Speaker; das Sonos-Konto muss mit dem jeweiligen Sprachdienst verknüpft sein.

## Ton aus Bild

Hinter der Zierfront kümmert sich ein Woofer mit 102 Millimetern Durchmesser



**Ein an die Wand gedübelter Haken hält den Lautsprecher magnetisch fest; das Stoffband sichert, falls der Rahmen vom Haken rutscht.**



**Die zwei Lautsprecher erzeugen einen kraftvollen Klang, bleiben aber hinter dem Sonos One zurück.**

um die Tiefen und Mitten, ein 25,5 Millimeter durchmessender Tweeter um die hohen Frequenzen. Damit steuert Sonos relativ große Treiber bei. Die Gehäusegröße lässt überraschend viel Platz, sodass die ungewöhnliche Bauart das Klangpotenzial der Hardware nicht gravierend einengt. Direkt aus dem Karton spielte IKEAs Streaming-Bild nicht nur sehr klar und detailliert, sondern vor allem beeindruckend kraftvoll auf. Der Klangeindruck wirkte viel räumlicher als bei einem kompakten Regallautsprecher. Ob es den Effekt steigert, wenn zwei der Sound-Bilderrahmen im Stereo-Modus gekoppelt sind, konnten wir mangels zweitem Testgerät nicht prüfen.

Je nach Aufstellort und Song-Arrangement wirkte der Bass sogar etwas zu präsent. Das galt vor allem bei frontalster Hörposition; nach ein paar Schritten zur Seite verlor der Bass an Wirkung. In dieser Hinsicht ist das Klangbrett dann doch bautiefen Boxen unterlegen, die dank Konstruktionstricks den Schall auch seitlich kanalisieren. Außerdem wirkten die Höhen etwas spitz und stellenweise gingen ein paar Nuancen in den Mitten unter. An den Dynamikumfang und die Präzision eines Sonos One kommt der Neuzugang nicht ganz heran.

Die nachträgliche Klangeinmessung per iOS-Trueplay verringerte diesen Unterschied zumindest im heimischen Test-Wohnzimmer etwas. Außerdem zähmte der Eingriff die spitzen Höhen und den wummernden Bass, der Klang wurde natürlicher und ausgewogener.

## Fazit

Der „Symfonisk Rahmen mit WiFi-Speaker“ besticht durch einen originellen Produktansatz, der auch in der Praxis überzeugt und nur wenige Nachteile aufweist: So handelt es sich angesichts der Bautiefe, des Gewichts und des Stromkabels keinesfalls um einen dezenten Einrichtungsgegenstand. Zudem fügt er sich aufgrund der begrenzten Zahl an Wechselfronten womöglich nicht passgenau ins Farbschema der Wohnung ein. Dass er sich nicht mit eigenen Fotos oder Postern dekorieren lässt, ist eine verpasste Chance. Gelungen sind die einfache Montage und Bedienung – nur die Standfüße muss man beim Staubsaugen im Auge behalten.

Der kraftvolle und klare Sound macht nach minimalen Eingriffen in die Klangeinstellungen richtig Spaß, ohne an Sonos’ Bestform heranzureichen. Fürs gesteigerte Musikvergnügen sind daher Sonos One oder besser die größeren Modelle die passenderen Kandidaten. Aber in allen anderen Zimmern legen die dekorativen und günstigen IKEA-Lautsprecher einen starken Auftritt hin. *(jow@ct.de)* ct

## IKEA Symfonisk Rahmen mit WiFi-Speaker

WLAN-Lautsprecher mit Anbindung an Sonos	
Hersteller, URL	IKEA, <a href="http://ikea.de">ikea.de</a>
Größe (B × H × T) / Gewicht	41 cm × 57 cm × 6 cm / 3,5 kg
Lieferumfang	Lautsprecher, Netzkabel (3,5 m), Füße, Wandhalterung
Verbindung	LAN, Wi-Fi 4 (2,4 GHz)
Preis	179 €

# Hört, hört!

## Headset Poly Voyager Focus 2 UC mit drei gleichzeitigen Verbindungen

**Headsets im Homeoffice sollen gut klingen, einen Mikrofonbügel haben und sich per Bluetooth mit PC und Smartphone verbinden. Der Focus 2 kriegt das hervorragend hin, ist aber nicht ganz perfekt.**

Von Jörg Wirtgen

Viele Kopfhörer mit aktiver Geräuschunterdrückung (ANC, Active Noise Cancelling) überzeugen mit tollem Klang, haben aber schlechte Mikrofone. Telefonie-Headsets hingegen punkten mit Mikrofonbügel und niedrigem Gewicht, klingen aber meist nur so lala. Der On-Ear-Kopfhörer Voyager Focus 2 UC mit Mikrofonbügel versucht, das Beste aus beiden Welten zu kombinieren; er kommt von Poly, wie sich der Headset-Hersteller Plantronics seit der Übernahme des Konkurrenten Polycom nennt.

Das Focus 2 koppelt sich per Bluetooth 5.1 an zwei Geräte gleichzeitig. Das Um-schalten funktioniert gut: Kommt beispielsweise am Handy ein Anruf, während man Musik am PC hört, stoppt die Musik beim Annehmen und spielt nach dem Auflegen weiter – auch, wenn der Anruf in einem SIP-Client wie Sipnetic oder Fritz-Fon ankommt. Insgesamt merkt sich der Focus 2 maximal acht gekoppelte Geräte. Der automatische Reconnect lief problemlos; nur wenn gleichzeitig mehr als zwei Geräte von der Merkliste empfangsbereit sind, verbinden sich wie bei Bluetooth-Multipoint üblich nicht immer die beiden gewünschten.

Die Sensorik funktioniert zuverlässig: Legt man das Headset ab, stoppt die Musik; beim Aufnehmen spielt sie weiter. Kommt ein Anruf, während man das Headset nicht trägt, nimmt es auf Wunsch beim Hochnehmen das Gespräch automatisch an.

Für Geräte ohne oder mit zu schlechtem Bluetooth liegt ein USB-Dongle bei. Er rüstet zudem die Teams-Fähigkeiten

nach, der Reconnect gelingt schneller und das Focus 2 ist in Teams automatisch das voreingestellte Gerät.

Alternativ (und zum Laden) schließt man das Focus 2 per Micro-USB an – warum auch immer Poly in 2021 noch diese veraltete Buchse verbaut. Ungewöhnlicherweise bleiben die beiden Bluetooth-Verbindungen dabei aktiv, sodass man drei Geräte gleichzeitig koppeln kann. Ein 1,5 Meter langes USB-A-Kabel liegt bei, das allerdings deutlichen Körperschall produziert. Eine Analogbuchse fehlt.

### Klingt gut

Klanglich spielt das Focus 2 ordentlich auf und liefert für ein On-Ear voluminöse und präzise Bässe, Mitten mit hoher Sprachverständlichkeit und detailreiche Höhen. Bei manchen Bewegungen, vor allem beim Gehen, hört man allerdings ein von der Kopfbügelhalterung kommendes Knarzen.

Die Tonqualität hängt stark vom Sitz der Kopfhörer ab, der nicht so definiert sein kann wie bei Over-Ears. Zusätzlich spielt die Ohrform eine Rolle – beides zusammen führt dazu, dass unser Messdiagramm einen Einbruch zwischen 70 und 500 Hz zeigt, den unsere Hörproben nicht bestätigten. Sitzt er gut, empfanden wir seinen Klang jedenfalls besser als den der meisten On-Ears und durchaus eine Alternative zu dem der ANC-Kopfhörer der 300-Euro-Klasse; die maximale Lautstärke könnte vielleicht etwas höher sein.

Die Geräuschunterdrückung hingegen leidet unter der On-Ear-Bauweise, sie

dämpft Sprache und andere hohe Frequenzen kaum. Lediglich gleichmäßige tiefe Geräusche wie Klimaanlagen filtert das Focus 2 passabel heraus.

### Nimmt gut auf

Das Mikrofon nimmt Sprache klar und voluminös genug für HD-Telefonie und Videokonferenzen auf. Fremdgeräusche wie Hall oder Tastaturgeklapper filtert es hervorragend weg. Frequenzen über 8 kHz schneidet es Bluetooth-üblich ab, auch per USB kamen keine höheren Frequenzen an – zu wenig für Podcasts.

Die eigene Stimme hört man bei Gesprächen deutlicher als bei Over-Ear-Kopfhörern, aber nicht so gut wie bei monauralen oder offenen Headsets. Zwar mischt das Focus 2 die eigene Stimme in per App konfigurierbarer Stärke ein – Sidetone genannt –, aber besonders viel Wirkung hat das nicht. Man wird vermutlich besser damit zuretkommen, bei längeren Gesprächen manchmal eine Muschel vor oder hinter das Ohr zu setzen.

Ob man das Mikrofon rechts oder links trägt, bleibt einem überlassen: Das Focus 2 ist symmetrisch aufgebaut, das Mikrofon lässt sich zu beiden Seiten klappen – und sobald man es herunterklappt, spielt das Focus 2 den rechten und linken Kanal automatisch der richtigen Seite zu und merkt sich die Einstellung.

### Bedienung

Die Muschel mit dem Mikrofonbügel beherbergt den Ein-/Pairing-Schalter und den ANC-Schalter. Zur Lautstärkeregelung lässt sich die Muschel oben und unten



klicken, was zuverlässiger funktioniert als die Touch-Bedienung anderer Kopfhörer. Die Mitte der Muschel kann man mehrfachbelegt drücken: einmal für Start/Stopp oder Auflegen/Annehmen, zweimal für Ablehnen oder den nächsten Song, dreimal für den vorigen Song – falls man sich das merken kann. Koppelt man per mitgeliefertem USB-Stick, entfällt Musik-Start/Stopp, stattdessen startet ein Klick Teams – im Multilinkbetrieb weiß man also gar nicht immer so genau, was ein Klick bewirkt.

Das Mikrofon stellt man stumm, indem man den Bügel nach oben kippt. Auf dem Bügel sitzt ein zusätzlicher Mute-Schalter, der aber nur funktioniert, wenn man mit dem USB-Dongle koppelt.

Dem kompakten Format geschuldet ist ein recht kleiner Akku und damit eine Laufzeit von maximal 20 Stunden. Lange Arbeitstage samt der Feierabendunterhaltung danach übersteht man locker, muss aber alle paar Tage ans Nachladen denken.

Für Android, iOS, Windows und macOS existiert eine App, die für Firmware-Updates und ein paar Einstellungen etwa der Ansagesprache und der Sensorautomatiken zuständig ist. Eine Individualisierung des Klangs ist nicht vorgesehen.

## Fazit

Das Voyager Focus 2 gehört zu den universellsten Homeoffice-Headsets: den ganzen Tag Musik hören, flexibel am PC und am Handy telefonieren, das Mikrofon rechts oder links tragen, wenig Stress mit Reconnects und der USB-Notfallmodus. Für rund 20 Euro Aufpreis gibt es zudem eine Ladestation. Besser wünscht man

## Poly Voyager Focus 2 UC

### On-Ear-Headset mit Mikrofonbügel

Ladenanschluss	Micro-USB
Verbindung / Multilink	Bluetooth 5.1 / ✓
Laufzeit	20 h (mit ANC)
Gewicht	174 g
Muschelgröße (B × H)	70 mm × 70 mm
Lieferumfang	Tragetasche, Micro-USB-Kabel (1,5 m), Bluetooth-Dongle

### Bewertung

Mikrofon	⊕
Klang	⊕
Geräuschunterdrückung	⊖
Tragekomfort	⊕
Straßenpreis	200 € (220 € mit Ladestation)
⊕⊕ sehr gut    ⊕ gut    ⊖ schlecht	○ zufriedenstellend    ⊖ schlecht ✓ vorhanden    — nicht vorhanden

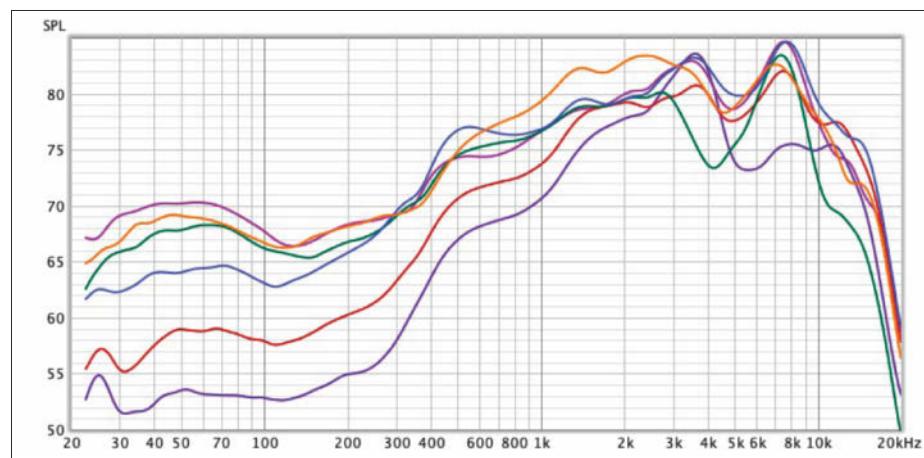
sich vor allem das ANC, die Ein-Knopf-Bedienbarkeit und die Hörbarkeit der eigenen Stimme.

Für den Straßenpreis von etwa 200 Euro bekommt man zwar Kopfhörer mit etwas besserem Klang und ANC, muss dann aber mit den Unzulänglichkeiten der Muschelmikrofone leben, vor allem deren Empfindlichkeit gegenüber Störgeräuschen. Im Vergleich zu anderen On-Ear-Headsets mit Mikrofonbügel wie Jabra Evolve2 65 oder Logitech Zone Wireless [1] platziert sich der Focus 2 dank bestem Klang und hoher Flexibilität an der Spitze. Im Vergleich zum Over-Ear-Headset Jabra Evolve2 85 [1] bietet der Focus 2 einen ähnlich guten Klang, das bessere Mikrofon, aber das schlechtere Noise Cancelling.

(jow@ct.de) 

### Literatur

- [1] Jörg Wirtgen, Ohrschmeichler, Headsets mit guter Musikqualität, c't 11/2021, S. 72



Der Bass des Voyager 2 klingt bei gutem Sitz (die 3 oberen Linien) präsent und präzise, lässt aber je nach Ohrform oder Sitz deutlich nach (die 3 unteren Linien). Das Loch zwischen 70 und 500 Hz haben wir nicht gehört.

## Neue Online-Kurse für IT-Professionals



### Natural Language Processing mit Python

Der große Praxiskurs zur Textanalyse mit Machine Learning

► 86 Videos, 11 Std. Spielzeit, inkl. Jupyter Notebooks



### Azure Active Directory im hybriden Kontext

Der Einstiegskurs für Planung und Betrieb in Azure und On-Premises

► 60 Videos, 6:30 Std. Spielzeit



### Continuous Delivery von A bis Z

Der Kurs für Softwareentwickler mit Gitlab und Jenkins

► 74 Videos, 7 Std. Spielzeit

Gratis-Lektionen aus allen Kursen  
anschauen unter:

**heise-academy.de**

# Uhrzeit-Dino

## Sportuhr Amazfit T-Rex Pro mit 14 Tagen Akkulaufzeit



**Die smarte und robuste Sportuhr gibt es schon für 160 Euro. Da wird man wohl Kompromisse machen müssen.**

Von Michael Link

Die bullig wirkende smarte Sportuhr Amazfit T-Rex Pro erinnert eher an Casios G-Shock-Uhren. Sie misst 47,7 mal 47,7 Millimeter und ist moppelige 13,5 Millimeter dick. Für die Größe fühlt sie sich mit 59 Gramm leicht an. Apps anderer Anbieter lassen sich nicht installieren. Die Pro-Version unterscheidet sich kaum vom Vorgänger ohne Pro, die einem schon für 85 Euro nachgeworfen wird: Sie ist noch widerstandsfähiger gegenüber Staub, Wasser und Erschütterungen und verträgt Temperaturen, bei denen niemand bei Verstand mehr vor die Türe geht. Alltagsnützlicher ist da schon die bessere Wasserdichtigkeit, die nun bis 10 ATM klassifiziert ist. Eine Taucheruhr ist die T-Rex Pro nicht, zum Spülen und Schwimmen reichts.

Das runde Display hat eine Diagonale von 3,3 Zentimetern (1,3 Zoll) und zeigt 360 × 360 Pixel. Eine oleophobische Beschichtung des Gorilla-3-Deckglases mindert durch die Touchscreen-Bedienung entstehende Fingerabdrücke. Das Zifferblatt leuchtet nach Handgelenkdrehung etwas verzögert auf; eine abgedunkelte, dauerhaft sichtbare Uhrzeitanzeige ist möglich, geht aber auf Kosten der Akkulaufzeit. Der Akku (390 mAh) wird über ein USB-Kabel mit Zwei-Kontakte-Anschluss geladen. Die Laufzeit betrug im Test mit täglicher Aktivitätsaufzeichnung inklusive GPS, aber ohne Always-On-Display 14 Tage. Im Stromsparmodus kappt die Uhr die Bluetooth-Verbindung und loggt nur noch Schlaf und Schritte, was die Laufzeit auf 60 Tage bringen soll; getestet haben wir das nicht.

Mit vier Drücken sowie einer nachvollziehbaren Menüstruktur bekommt

man die Uhr schnell in den Griff. Fast alles lässt sich per Drücker erledigen, für das Schnellmenü braucht man aber das Touchdisplay. Huami hat einiges gelernt: Bei der T-Rex Pro klappt der Aufruf der App-Übersicht nun auch per Button, nicht nur durch Wischen von rechts nach links. Und: Jeder Tastendruck weckt jetzt das Display auf, nicht mehr nur ein bestimmter.

Das Display ist AMOLED-typisch farbenfroh und brillant, jedoch in praller Sonne nicht so gut ablesbar wie Transflektiv-Displays. Bis zu acht Zifferblätter sind schaltbar, weitere bekommt man über die Smartphone-App Zepp. Der Name zeigt den Wechsel des Markennamens von Huami auf Zepp an. Ab Herbst soll auch das Betriebssystem so heißen.

Während die Uhr auf übersichtliche Bedienung getrimmt ist, braucht man für die Zepp-App das Orientierungsvermögen von Blauwalen. Sonst verirrt man sich in Untermenüs von Untermenüs. Immer wieder stößt man beim Erforschen ausgedehnter Menü-Irrgärten auf chinesische Schriftzeichen und seltsame Übersetzungen: So kann man sein Gewicht in Steinen oder mit dem Maß Jin eintragen.

### Fast Vollkasko-Ausstattung

Man kann abseits vom Laufen, Schwimmen und Radfahren mehr als 100 verschiedene sportliche Aktivitäten aufzeichnen, beim Vorgänger waren es noch 14. Die Spanne reicht vom Bauchtanz bis zum Parkour, sogar Angeln und das hierzu lande recht exotische Federfußball sind dabei. Aber: Ausgerechnet das verbreitete Triathlon kann die Uhr nicht. Weniger gut auch: Die maximale Sauerstoffsättigung (VO2max) wird zwar mit dem etablierten Algorithmus von Firstbeat ermittelt, allerdings nur für Laufaktivitäten.

Einige Funktionen grenzen die T-Rex Pro von anderen Smartwatches ab: Die automatische Erkennung („Exersense“) von Aktivitäten funktionierte beim Radfahren sehr gut. Schon zwei Minuten nachdem die Uhr eine Aktivität erkennt, zeich-

net sie sogar die Wegstrecke auf – anders als das bei anderen Herstellern üblich ist. Im Test stoppte die Aufzeichnung schon beim kurzen Stopp an der Eisbude. Nützlich ist die DND-Funktion („Do not disturb“). Sie schaltet selbsttätig das Display sowie Benachrichtigungen aus, wenn die Uhr erkennt, dass man schläft.

Für die Wegaufzeichnung verwendet die T-Rex Pro Beidou, Galileo sowie Glonass und GPS. Ein PPG-Sensor misst Puls und Herzratenvariabilität optisch, externe Sensoren sind nicht nutzbar. Im Gehäuse stecken noch ein Barometer und ein dreiachsig gelagerter Kompass. Die Höhenmeteraufzeichnungen waren im Test etwas unpräzise, der GPS-Track genau.

Was fehlt? Da der Dinosaurier kein Mikro und keinen Lautsprecher hat, kann er auch nicht freisprechen. Ohne NFC-Chip fehlt der Uhr eine Bezahlfunktion. Die aufgezeichneten Daten stehen nur Komoot und Strava sowie Relive und im iPhone der Health App, sonst Google Fit zur Verfügung. Auf Android-Geräten klappt die Kopplung auch mit der freien Software Gadgetbridge.

### Fazit

Die Zepp-App braucht eine Entrümpling. Ansonsten: Die T-Rex Pro ist eine reichhaltig ausgestattete robuste Sportuhr. Einiges, das fehlt, ist für viele irrelevant, etwa der Triathlon-Modus und die mangelnde Möglichkeit, externe Sensoren zu koppeln. Wer das nicht braucht, könnte im Funktionsumfang angesichts des geringen Preises einen guten Kaufanreiz sehen.

(mil@ct.de) ct

### Huami Amazfit T-Rex pro

#### Sportuhr mit Aktivitätstracker

Hersteller, URL	Huami, amazfit.com
kompatibel zu	iOS (ab 10.0), Android (ab 5.0)
Display	1,3" (3,3 cm), 360 × 360 Pixel, AMOLED
Sensoren	GNSS (GPS, Glonass, Galileo, Beidou), 3D-Gyroskop, 3D-Beschleunigungssensor, Kompass, Barometer, Licht
Preis	UVP: 169 €, Straßenpreis: 160 €



## Steinchen sortieren

**Der kostenlose App BrickIt genügt ein Foto, um für einen Haufen Lego-Steine Bauvorschläge zu machen.**

BrickIt analysiert im Handumdrehen unsortierte Lego-Steine. Das Video-Tutorial der App zeigt, wie es geht: Lego-Steine ausschütten und alle sperrigen Bauteile wie Reifen, Felswände oder große Platten entfernen. Anschließend muss man die Steine auf einer geraden Oberfläche ausbreiten, sodass sich keine überlappen – und über die App fotografieren. Danach scannt BrickIt das Bild und kleine Kästen wandern von Steinchen zu Steinchen. Ist die Analyse fertig, schlägt die App vor, was sich daraus bauen lässt.

Die Bauvorschläge holt die App aus einer Datenbank, die der App-Hersteller füttert. Sie enthält mehr als 1500 Lego-Sets. Wenn man einen Bauvorschlag auswählt und eins der Bauteile antippt, zeigt BrickIt praktischerweise, wo der Stein auf der Fläche liegt – unabhängig von der Farbe. Bei den Vorschlägen handelt es sich meistens um kleinere Lego-Modelle aus 20–30 Teilen. Die Anzahl der Bauvorschläge hängt stark von Menge und Vielfalt der erfolgreich gescannten Teile ab.

In unseren Tests erhielten wir bei einer Auswahl von knapp 200 Teilen drei Vorschläge, mehr als 600 dagegen erga-

ben 34. In den meisten Fällen erkannte BrickIt die Steine korrekt – zumindest, wenn die Fläche gut ausgeleuchtet war. Vereinzelt gab es Fehler, in der die App Bauteile mit glatten Flächen als schräge Steine erfasste. Bei einem von oben fotografierten 2x2-Stein registrierte die App des Öfteren flache Steine als formgleiche höhere Bauteile.

Die besten Analysen erhalten Sie, wenn Sie die ausgebreiteten Steine mittig und möglichst ohne Schatten fotografieren. Die Foto-Analyse erkennt auch zuverlässig Bauteile von anderen Klemmbausteinfirmen, sofern diese ein Pendant im Lego-Universum haben. Schade ist, dass sich die App gescannte Teile nicht merken kann. Mit jedem Scan von neuen Teilen verwirft die App die bisherigen Ergebnisse.

BrickIt bietet abgesehen vom genannten Steinchen-Scan „Build“ eine „Collect“-Funktion, über die man seine Lego-Set-Sammlung verwaltet. Um eigene Sets einzuspeisen, tippt man entweder die Nummer des Lego-Sets ein oder klickt sich durch die Liste. Unter „what can i build“ gleicht die Applikation die Bausteine der hinterlegten Sets mit der Datenbank ab und spuckt weitere Bauvorschläge aus.

Mit „Collect“ konkurriert die App mit Websites wie Rebrickable oder Bricklink: Auf den Seiten findet man nicht nur alle Anleitungen offizieller Lego-Sets, sondern kann auch Anleitungen sogenannter „My Own Creations“ (MOCs) erwerben und nachbauen – von Fans entworfene Modelle. Rebrickable listet 17.000 Sets und beinahe 50.000 MOCs auf. BrickIts Auswahl ist geringer, dafür aber komplett kostenlos.

BrickIt hat Unterhaltungswert, steht aber noch am Anfang: Die App würde mit Speichern der Scans und mit besseren Vorschlägen große Schritte machen. Zurzeit ist sie nur für Apple-Geräte erhältlich und stürzt gelegentlich mal ab. Die russischen Entwickler haben seit der Veröffentlichung mehrere Performance-Updates nachgeschoben und eine Android-Version für Herbst angekündigt. (wid@ct.de)

## BrickIt

### Lego-Steine sortieren

Hersteller, URL	BrickIt LLC, brickit.app
Systemanf.	ab iOS 13
Sprache	Englisch und Russisch
Preis	kostenlos



## Turbostick

**Von USB-Sticks ist man eine eher gemächliche Gangart gewohnt. Patriots Supersonic Rage Prime aber ist sogar schneller als viele SSDs.**

Bis zu 600 MByte/s, verspricht der Hersteller, schafft der USB-Stick beim Lesen; als Schnittstelle kommt USB 3.2 Gen 2 zum Einsatz. Mit Iometer haben wir beim Lesen und Schreiben fast sogar 1 GByte/s gemessen, auch das Windows-Bewertungstool WinSat bescheinigt dem Stick fast 1 GByte/s beim Schreiben und knapp 900 MByte/s beim Lesen.

In der Praxis aber fällt die Geschwindigkeit dann doch auf das erwartete Maß ab. Das Schreiben eines großen Videos schaffte das Laufwerk mit etwa 520 MByte/s, das Lesen mit knapp 500 MByte/s. Bei sehr kleinen Dateien sind solche Sticks deutlich langsamer. Rund 10 MByte/s erreichte der Supersonic Rage Prime beim Schreiben unkomprimierter Linux-Quelltext-Dateien, doch selbst damit liegt er in der ewigen Bestenliste auch in dieser Disziplin auf Platz 1.

Die Transferrate sinkt mit der Zeit stark ab, auch durch die Erwärmung auf bis zu 76 °C. Für den stolzen Preis von rund 170 Euro bekommt man auch eine flotte USB-SSD; der Stick eignet sich jedoch weit besser zum Datentransport in der Hosentasche. (ll@ct.de)

## Patriot Supersonic Rage Prime

### USB-Stick mit 1 TByte Speicherplatz

Modellnummer	PEF1TBRPMW32U
Hersteller, URL	Patriot, patriotmemory.com
Anschluss	USB 3.2 Gen 2, Typ-A-Stecker
Straßenpreis	circa 170 €

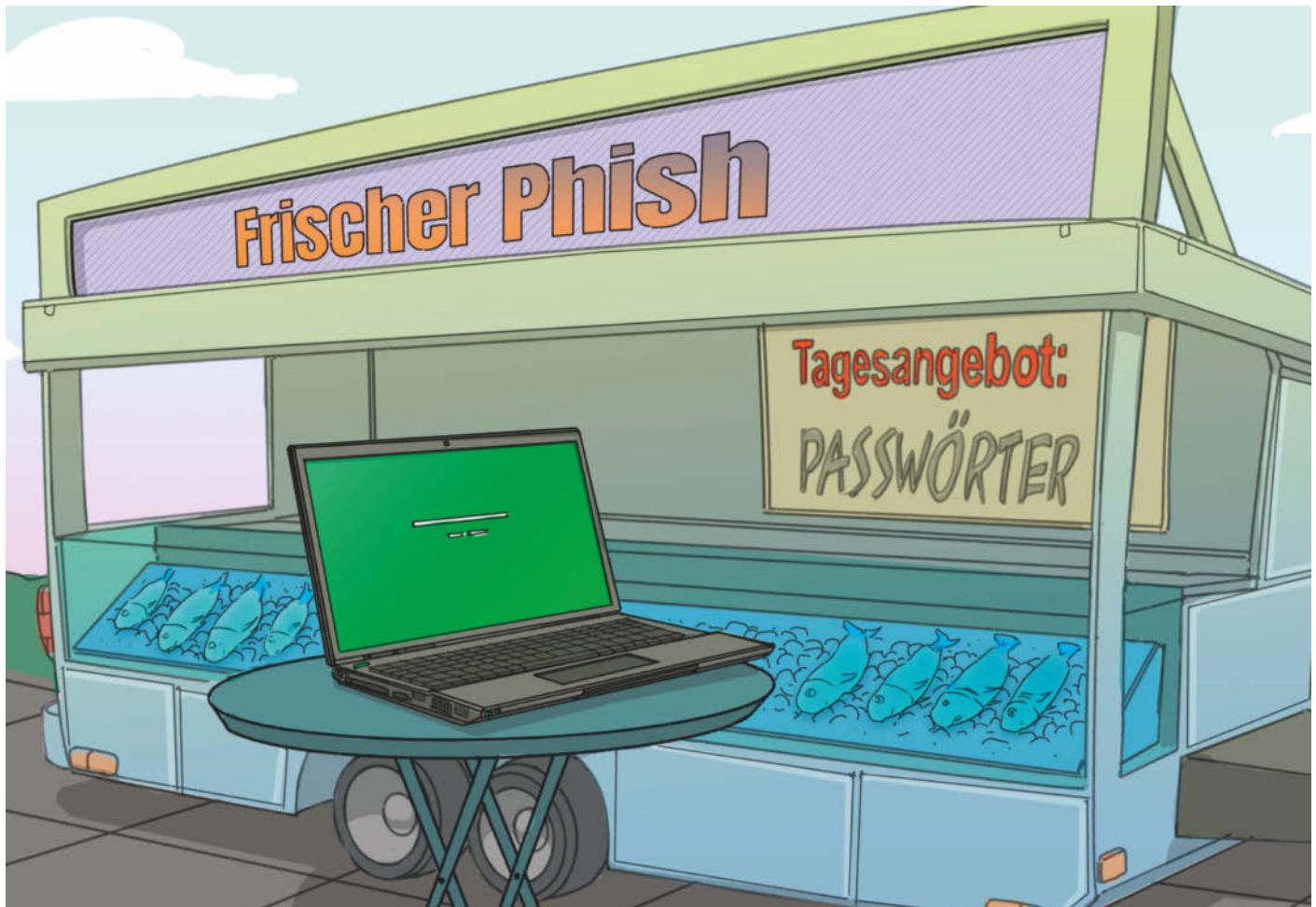


Bild: Thorsten Hübner

# Zurückgephisht

## Wie wir einem unachtsamen Phisher auf die Schliche kamen

**Phishing und Spamming sind eigene kriminelle Industriezweige, die Hand in Hand arbeiten. Weil sich ein Phisher einen dummen Fehler leistete, konnten wir mehr über ihn erfahren, als ihm lieb sein konnte.**

Von Jan Mahn

Eine verdächtige Mail mit einer noch verdächtigeren URL landete in einem Spam-Filter, den einer unserer Leser betreut. Beruflich kümmert er sich um IT-

Sicherheit und so war ihm sofort klar, dass es sich bei der vermeintlichen Aufforderung des Mailanbieters, sich aus Sicherheitsgründen sofort an der Webmail-Oberfläche anzumelden, um einen Phishing-Versuch handeln musste. Der Link in der Mail zeigte zu einer Subdomain von web.core.windows.net und enthielt am Ende als Query-Parameter die Mailadresse. Neugierig schaute sich der Leser die Seite an und fand ein anschauliches Beispiel für eine Phishing-Attacke – und eine Sicherheitslücke zu Ungunsten des Phishers.

In einer virtuellen Maschine probierten wir den Link aus und tauschten die Mailadresse im Link durch eine Beispiel-Adresse beim deutschen Mail-Hoster Web.de aus. In der Mitte erschien vor

grauem Hintergrund ein stark deformiertes Login-Fenster, das nur entfernt an das Original von Web.de erinnerte. Wer dort sein Kennwort eingab, musste schon sehr naiv sein.

Ein Blick in die Entwicklerwerkzeuge des Browsers enthüllte, was sich der Phisher eigentlich überlegt hatte: Per Iframe sollte hinter dem Fenster die echte Web.de-Seite von https://web.de eingebettet werden, darüber sollte das selbstgebaute Login-Fenster schweben. Das hätte die Täuschung zumindest etwas besser gemacht und die Erfolgsquote sicher erhöht. Doch daraus wurde nichts: Weil die Betreiber von Web.de schon länger mit Phishing gegen ihre Nutzer zu tun haben, haben sie ihre Server so konfiguriert, dass sie folgenden Header mitschicken:

```
content-security-policy:   
  frame-ancestors 'none'
```

Moderne Browser weigern sich dann, die Seite im Iframe darzustellen – es bleibt eine unattraktive graue Fläche. Eine kleine Einstellung im Server, die Phishing zumindest etwas erschwert. Wer selbst Login-Seiten betreibt, ist gut beraten, diesen Header zu aktivieren.

Die Phishing-Seite war so programmiert, dass sie dynamisch auf unterschiedliche Mailhoster reagierte: In der URL wurde die Mailadresse des Opfers übergeben, die Phishing-Links müssen also in einer Art Serienbrief personalisiert generiert und verschickt werden. Je nach Mailadresse versucht die Seite, unterschiedliche Mail-Anbieter per Iframe einzubinden und stellt das Favicon der Seite als Logo im Login-Fenster dar. Eine kleine Versuchsreihe zeigte aber, dass die gängigsten Mail-Provider Iframe-Einbindungen per Header unterbunden und die meisten Opfer wohl eine graue Fläche gesehen haben.

## Passwortversand

Neben Iframe und gefälschtem Login-Fenster fanden wir JavaScript auf der Seite. Die Analyse hatten die Entwickler aber deutlich erschwert und den Code mit einem sogenannten Obfuscator etwas unkenntlich gemacht. Ein solches Werkzeug ersetzt möglichst viel aussagekräftigen Klartext (Strings, Funktions- und Variablennamen) durch andere Zeichen, in diesem Fall durch hexadezimale Zeichen. So wird es zwar nicht unmöglich, den Code zu verstehen, aber immerhin mühsam (als Gegenmittel gibt es wiederum De-Obfuscatoren).

Aber auch ohne JavaScript-Code im Klartext konnten wir beobachten, was beim vermeintlichen Anmelden geschah. Die Entwicklerwerkzeuge aller Browser haben einen Reiter „Netzwerk“, der HTTP-Aufrufe mit Anfrage- und Antwortdaten protokolliert und darstellt. Für gewöhnlich wird das Kennwort per HTTP an den Server geschickt und dort gespeichert. Doch dieser Fall war ungewöhnlich – und nicht gerade geschickt:

Sandte man das Formular ab, wurde eine Anfrage an den Endpunkt `sendMessage` von <https://api.telegram.org/> geschickt, in den Formulardaten das Kennwort, das man ins Kennwortfeld getippt hatte:

```
##+nEw+l0g##  
+-----+  
max.muster@web.de+|+geheimes_passwort  
+-----+
```

Im Messenger Telegram kann jeder einen Bot anlegen und mit ihm eine Kommunikation starten. Bots sind klar als solche gekennzeichnet und ganz hilfreich, um sich zum Beispiel Statusmeldungen seiner Server oder des vernetzten Zuhause schi-

cken zu lassen. Dafür reicht ein API-Aufruf, wie wir ihn gefunden haben. Der Phisher nutzte dieses Verfahren, um alle Kennworteingaben von Opfern sofort aufs Handy zu bekommen.

Um das API zu nutzen, generiert Telegram ein Token, auf das man gut aufpassen muss – keinesfalls darf man das API direkt per JavaScript aus einer öffentlichen Seite heraus ansprechen: Die URL zum API enthält nämlich das Token, und wer das kennt, kann den Bot Nachrichten schicken lassen. Eigentlich legt man das Token daher auf einen Server und lässt ausschließlich diesen mit dem API sprechen, niemals den Browser.

Diese grundsätzliche Vorsichtsmaßnahme hatte der Phisher ignoriert und uns so das API-Token für seinen Bot präsentiert. Per API hätten wir ihn jetzt mit Nachrichten überhäufen können, doch damit nicht genug: In der HTTP-Antwort verrät das Telegram-API weitere Details: Vorname, Nachname und Telegram-Benutzername des Benutzers, dem der Bot eine Nachricht geschickt hat. So erfuhren wir, dass der Phisher offenbar Daniel heißt und hatten auch seinen Benutzernamen. Mithilfe des Werkzeugs TgScanRobot, das öffentliche Telegram-Gruppen systematisch durchsucht, fanden wir heraus, in welchen unsympathischen Kreisen er sich herumgetrieben hatte: Über 20 Gesprächs- und Handelsplattformen für Spamming, Hacking-Werkzeuge und Handel mit geklauten Kreditkarten. In einer dieser Gruppen hatte sich Daniel auch mal zu Wort gemeldet und wurde zurechtgewiesen,

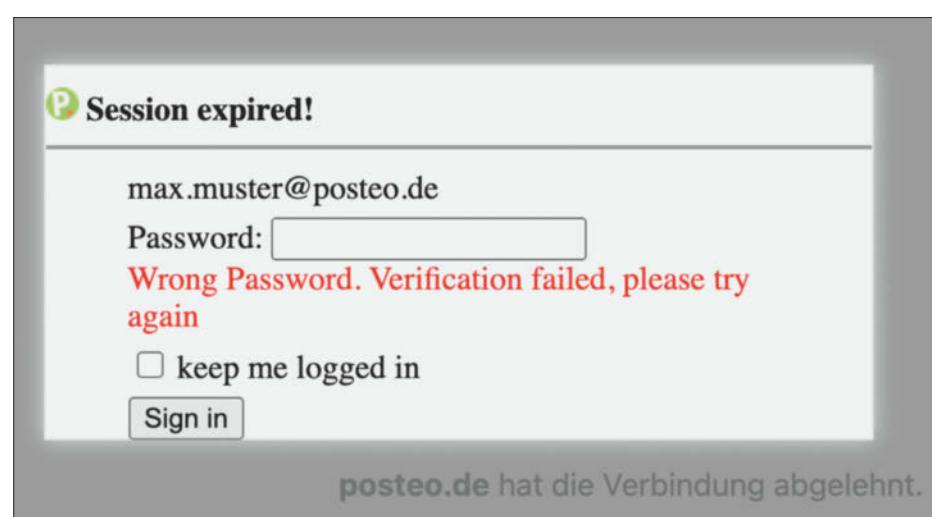
weil er sich nicht an die Regeln der Gruppe gehalten hatte.

Jetzt wollten wir mehr über Daniel wissen – zumindest seine Herkunft interessierte uns. Ein Gruppename mit chinesischen Schriftzeichen deutete schon mal grob auf Asien hin. Um es genauer einzukreisen, stellten wir dem Phisher eine Falle: Mit seinem Token schickten wir ihm über seinen Bot eine Nachricht, dass eben dieser Bot wegen illegaler Aktivitäten gesperrt sei, und er einen Link bei Telegram zur Freischaltung klicken müsse. Statt einem Link zur Telegram-Seite enthielt unsere Nachricht einen Link des Dienstes Grabify – eine Art URL-Kürzer, der dem Ersteller nebenbei zahlreiche Details zu allen Nutzern anzeigt, die ihn angeklickt haben. Ob ein Phisher selbst auf eine solche Phishing-Nachricht hereinfällt?

Nur sechs Stunden später ging er ins Netz und klickte auf den Link: So erfuhren wir, dass Daniel einen aktuellen Firefox nutzt, seinen PC in der Zeitzone „Asia/Shanghai GMT+8“ mit englischer Oberfläche betreibt und über ein Microsoft-VPN im Internet surft, das in den USA endet.

## Gehostet bei Microsoft

Damit Daniel keinen weiteren Schaden anrichten konnte, musste die Phishing-Seite schnell vom Netz. Gehostet wurde sie in Microsofts Azure-Cloud, genauer gesagt handelte es sich um eine statische Seite, wie sie jeder Azure-Kunde anlegen kann. Ungeschickt von Microsoft ist es, dafür Subdomains von windows.net zu vergeben. Phisher könnten damit eine



**Das Phishing-Manöver wirkte etwas verzweifelt. Geplant vom Phisher war, dass im Hintergrund die echte Login-Seite per Iframe eingebunden wird. Das verhindern jedoch die Sicherheitsmaßnahmen moderner Browser.**

-	MMO - Black_swagg_©
-	ins_Crew - H0ligans CREW™
-	rea - Maxic Genius Chat
-	rdersgroup - SHAD〇W CARDERS-█
MARKET GROUP	
-	↳Forums - 🚫 SPAMMERS 🚫 🔑 FORUM 🔑
-	T88 - 银行卡 🔥 个人四件套 🔥 对公账户 USDT 代收
跑分 支付 交流群	
-	Pickups - X-MaxPickup-MONEY/D-Cc
-	shops - Xtools Shop
-	noiszones - ANNOYOUS ZONE
-	orlhdacker - BLACK WORLD
-	jswipeznation - Carding Swipez Nation
-	it_inc - CASHOUT CENTRAL 🎖️ 💰 💰 💰
-	yalty - DARK♥️ ROYALTY 🎉
-	legacy - Escrow Legacy 🌟 Kingtrash family
💡	
-	hamrh - Learn Spammering with REDHAT
-	ang7 - 🏙️ POOR MEN WITH MONEY 💰
-	akvip - @mustleakvip
-	hingforcash - Dread cashgang
-	ngdom - Swift Kingdom
-	usiness - Under Business 🌟 Kingtrash Family
-	nadhackers - MAD-HACKERS ❤️
-	nafia - 🏙️ VIRTUAL MAFIA - PUBLIC 🏙️

13.27

Weil die Phishing-Seite den Telegram-Benutzernamen des Phishers offenbart, konnten wir die Liste der öffentlichen Telegram-Gruppen extrahieren, in denen er Mitglied war. Der Cyber-Klein-kriminelle war gut vernetzt in Spammer- und Kreditkartenbetrügerkreisen.

weitaus wirksamere Phishing-Kampagne für Microsofts eigene Kunden aufsetzen: Wer aufgefordert wird, sein Windows-, Office-365-, oder Outlook.com-Konto einzugeben, wird angesichts einer windows.net-Seite zunächst nicht stutzig. Für die perfekte Täuschung bräuchten die Angreifer aber einen besseren Webdesigner als Daniel, der das originale Microsoft-Design ansehnlich nachbauen kann.

Wir entschieden uns, Microsoft Azure über das Formular im Microsoft Security Response Center über die Phishing-Seite zu informieren (siehe ct.de/y22w). Wenige Tage später war die Seite verschwunden und wir erhielten eine Bestätigung von Microsoft. Dass Strafverfolger über Microsoft eine Chance hätten, den wirklichen Namen von Daniel zu erfahren, ist unwahrscheinlich – wer sich in Foren über geklaute Kreditkarten austauscht, wird sich nicht mit eigenen Daten bei Microsoft anmelden.

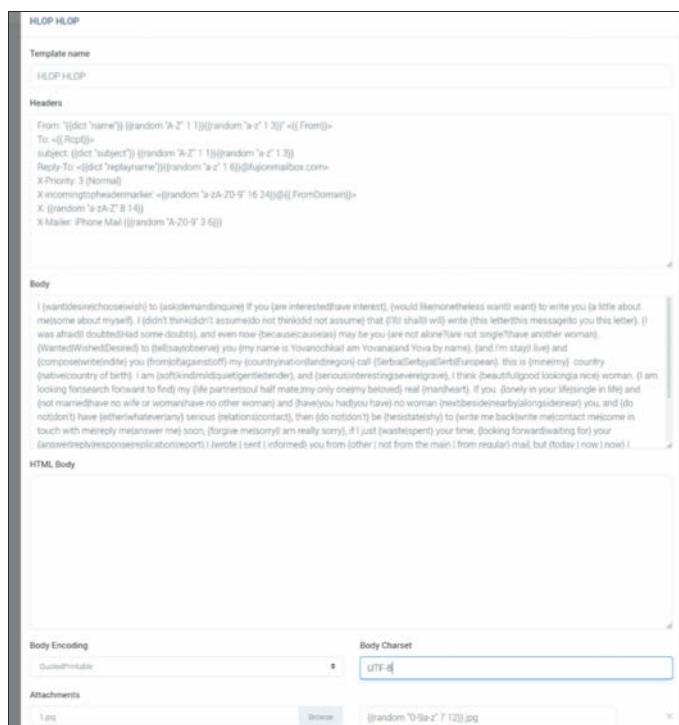
## Professionelle Kampagnen

Wie ein großer Fisch in der Szene wirkt Daniel nicht, mehr wie ein recht unerfahrener Kleinkrimineller, der sich mit dem Verkauf von Mailadresse-Kennwort-Kombinationen verdingen oder über gekaperte Postfächer Kennwörter für Webshops zurücksetzen und in fremdem Namen einkaufen wollte. Unklar ist, ob er die Phi-

shing-Seite selbst gebaut hat, die Expertise in einer der Telegram-Gruppen eingekauft oder dort einen Online-Schnellkurs „Phishing für Einsteiger“ belegt hat.

Doch wer kauft Benutzernamen und Kennwörter, die Kleinkriminelle mühsam sammeln? Diesen Teil der Wertschöpfungskette – sofern man das so bezeichnen möchte – decken professionellere Gruppen ab. Ihre Spuren fand ein Leser zufällig bei einem Port-Scan: Auf Port 80 lag eine umfangreiche Webanwendung, die offenbar zum Verwalten von Spam-Kampagnen gedacht war. Die Beschriftungen deuten auf Betreiber in Osteuropa hin. Da Datenschutz unter kriminellen Spammern ohnehin kein allzu hohes Gut ist, hing die gesamte Anwendung aber ohne Kennwortschutz im Netz. Auf der einen Seite enthielt sie Textdateien mit einigen hundert Megabyte Benutzername-Kennwort-Kombinationen. Außerdem einen ausgeklügelten Manager für Spam-Kampagnen. Der erinnerte vom Aufbau an professionelle Werkzeuge für Newsletter- und Social-Media-Kampagnen – nur eben für Spam. Online konnte man Textvorlagen, Empfänger und Absender kombinieren und so zeitgesteuerte Spam-Wellen planen. Die Vorlagen wurden offenbar von einer Template-Engine verarbeitet, die per Zufall die Platzhalter mit einem der angegebenen Inhalte füllte:

```
I {want|desire|choose|wish} to
{ask|demand|inquire}...
```



Auf diese Weise kann man auch ausgeklügelte Inhaltsfilter an die Grenzen bringen, weil es ausreichend unwahrscheinlich ist, dass zwei identische Mails oder wiedererkennbare Muster entstehen.

Verschickt wurden die Spam-Mails über die legitimen Mailserver von Mail-Hostern – authentifiziert mit einem der Accounts aus der langen Liste von erbeuteten Kennwörtern. In solchen Fällen haben auch Blacklist-Filter und Verfahren wie SPF oder DKIM kaum eine Chance, weil die Mails ja von vertrauenswürdigen Absenderservern verschickt wurden.

Um zumindest diesen einen Sumpfstückweise trocken zu legen, haben wir den Betreiber der Website haveibeenpwned.com auf die öffentlich zugängliche Kennwortsammlung der Spammer hingewiesen. Das Projekt sammelt gefundene Benutzernamen und Kennwörter als Hashes und Anwender können sich informieren, ob ihre Zugangsdaten schon im Internet kursieren.

Wo die Spam-Profis so große Kennwortsammlungen überhaupt finden, kann man nur mutmaßen – ein Teil kommt aus Datenlecks bei Betreibern, die in einschlägigen Foren verkauft werden, ein weiterer Teil sicher über dubiose Marktplätze von Zulieferern wie dem kleinkriminellen Phisher Daniel.

(jam@ct.de) ct

**Microsoft Security Response Center:**  
[ct.de/y22w](https://ct.de/y22w)

**Zur Verwaltung von Spam-Vorlagen, Adressen und Zeitplänen betreiben Spammer umfangreiche Webanwendungen. Per Kennwort geschützt sind die Oberflächen nicht immer.**

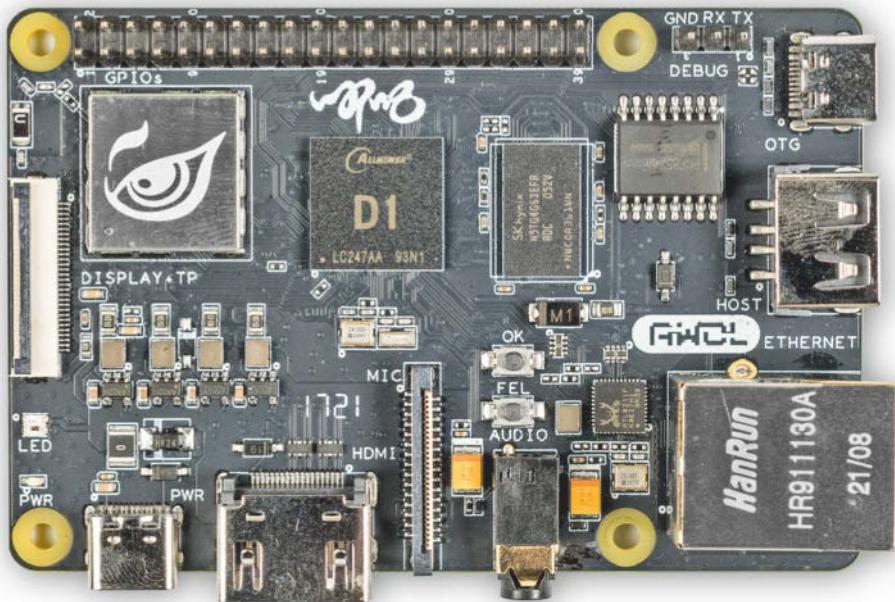
# Ihr Erfolg liegt uns am Herzen

Wir sind Ihr Ansprechpartner, wenn es um erfolgreiches regionales Marketing geht.  
Umfassende Beratung und Full Service sind für uns selbstverständlich.

Mobil, Online oder Print –  
wir übernehmen das für Sie.



Erfolgreiches  
Marketing  
vor Ort.



# Langsam freier

## RISC-V-Einplatinencomputer RVBoards Nezha

**Der Nezha ist der erste bezahlbare und Linux-taugliche Einplatinencomputer, dessen Prozessor die offene Befehlsatzarchitektur RISC-V nutzt. Er ähnelt einem Raspberry Pi und zeigt, welche Hürden RISC-V noch zu nehmen hat.**

Von Christof Windeck

Rund elf Jahre nach der Vorstellung der offengelegten Befehlsatzarchitektur RISC-V kommt ein erstes erschwingliches System damit, auf dem Linux läuft: der Einplatinencomputer Nezha im Raspberry-Pi-Format. Bisher erhältliche RISC-V-Systeme waren entweder mehrere Hundert Euro teuer oder taugten nicht für Linux [1]. Im „D1“-Chip der chinesischen Firma Allwinner, die an der Entwicklung

des Nezha beteiligt war, sitzt ein 64-Bit-RISC-V-Kern gemäß der Spezifikation RV64GC. Für diesen Kerntyp passen viele Linux-Entwickler ihren Code an. Bisher gibt es jedoch erst wenige Linux-Distributionen, die wiederum jeweils nur auf ausgewählten RISC-V-Plattformen laufen; für das Nezha-Board hat der Hersteller ein Linux auf Debian-Basis angepasst, das bisher jedoch nicht für den Produktiveinsatz taugt.

Nezha hat nicht nur dasselbe Platinenformat wie ein Raspberry Pi (4), sondern wie dieser auch eine 40-polige GPIO-Pfostensteckerleiste sowie eine USB-C-Buchse zur Stromversorgung. An die einzige USB-2.0-A-Buchse kann man – gegebenenfalls via USB-Hub – Tastatur und Maus anschließen, für einen Monitor gibt es eine HDMI-Buchse. Im D1-Chip ist auch ein Gigabit-Ethernet-Controller eingebaut, der via RJ45-Buchse nutzbar ist.

Das Nezha-Board bootet ebenso wie ein Raspi von einer MicroSD-Karte; im 99 US-Dollar teuren „Basic Package“, das man

bei der chinesischen Online-Plattform AliExpress bestellen kann, findet sich ein 32-GByte-Kärtchen, auf dem die erwähnte Debian-Variante vorinstalliert ist. Der Systemstart mit der mitgelieferten Micro-SD-Karte dauert auf der schwachbrüstigen Hardware mehrere Minuten: Der Allwinner D1 enthält nur einen einzigen RISC-V-Kern, der auch nur mit 1 GHz taktet, und das Board hat lediglich 1 GByte RAM. Als grafische Oberfläche kommt der ressourcenschonende Linux-Desktop LXDE zum Einsatz. Anders als in der ziemlich chaotischen Online-Dokumentation behauptet, lautet das Passwort für den Nutzer „root“ schlichtweg ebenfalls „root“. Nach dem Anmelden dauert es dann wiederum eine ganze Weile, bis der LXDE-Desktop benutzbar ist.

Nun hat man ein leicht bedienbares Linux-System mit Software-Paketverwaltung vor sich, das allerdings sehr träge reagiert und extrem unsicher konfiguriert ist: Das Debian-Betriebssystem holt Updates über eine ungesicherte Verbindung vom Server der chinesischen Firma Perf-Xlabs. Die Marke RVBoards, die das Nezha-Board vertreibt, gehört zu Perf-Xlabs.

Der vorinstallierte Browser Midori kann viele moderne Webseiten nicht darstellen, lediglich einfachere wie etwa Wikipedia. Wir konnten auf der Kommandozeile mit openssl und dem Komprimierungsprogramm 7-Zip Performance-Messungen durchführen. Demnach ist die Rechenleistung des D1 sehr gering, der ARM-Chip Broadcom BCM2711 des Raspberry Pi 4 mit vier Cortex-A72-Kernen und 1,8 GHz Takt ist rund 15-mal so schnell. Der D1 liegt näher am BCM2835 mit ARMv6-Kern aus der ersten Raspi-Generation von 2012, siehe Tabelle.

Immerhin braucht das Nezha-Board höchstens 1,5 Watt Leistung, also rund 0,8 Watt weniger als ein Raspi 4 im Leerlauf und nur ein Drittel dessen, was er unter Volllast zieht. Der mitgelieferte Kühlkörper mit selbstklebendem Wärmeleitpad ist wegen der geringen Leistungsaufnahme überflüssig; das USB-C-Netzteil passt nur in US-Steckdosen; wir haben stattdessen ein Raspi-Netzteil verwendet.

Außer dem integrierten Ethernet-Controller im D1 hat das Nezha-Board auch ein per SDIO angebundenes WLAN-/Bluetooth-Modul nach dem alten Standard 802.11 b/g/n, das XR829 der chinesischen Firma XRadio Technology. Es wurde zwar erkannt und wir konnten uns über die LXDE-App ConnMan bei einem

Router anmelden, doch per WLAN flossen in unseren Versuchen keine Daten. Es gelang uns zudem nicht, dem Audio-Codec Töne zu entlocken oder gar Videos abzuspielen.

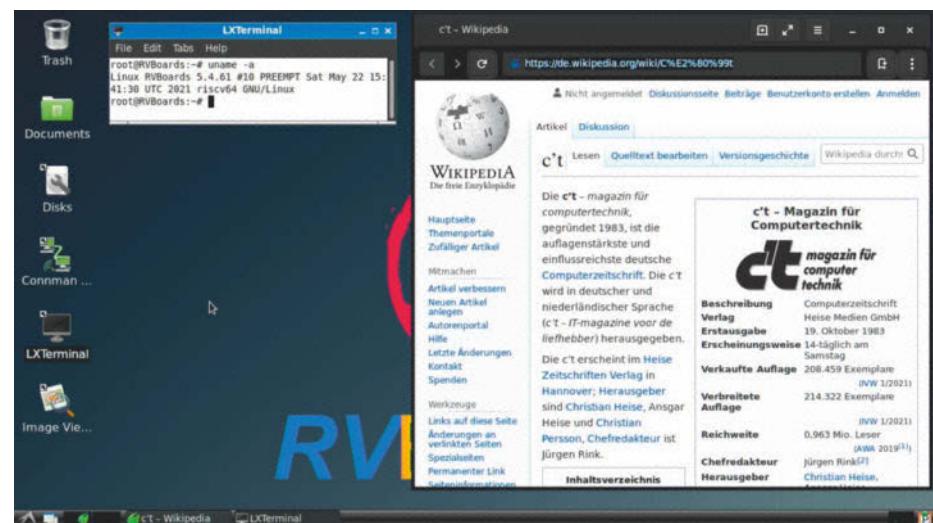
## China First

Das Nezha-Board ist vor allem für Entwickler interessant, die RISC-V-Code unter Linux programmieren. Allwinner hat bei der Entwicklung des Nezha mit den Firmen Sipeed und PerfXlab kooperiert, die auch weiter an der Software feilen. Es gibt einen GitHub-Bereich, in dem PerfXlab Code-Beispiele für Demoprojekte mit dem Nezha bereitstellt (siehe [ct.de/y4cu](https://ct.de/y4cu)). Sie zeigen die Anbindung verschiedener einfacher Sensoren.

Viele Informationen zum D1 und zum Nezha-Board finden sich in der von Allwinner eingerichteten Webseite AW-OL.com (AWOL), aber nur in chinesischer Sprache. Zwar gibt es bei RVBoards auch ein englischsprachiges Forum, das aber kaum genutzt wird; unser Registrierungsversuch dort scheiterte zudem. Im chinesischsprachigen Forum ist mehr los. Wer die chinesische Sprache nicht beherrscht, hat es bisher also schwer, an weitere Informationen zur RISC-V-Hardware von Allwinner und RVBoards heranzukommen.

Auf unserem bei AliExpress gekauften Muster, was rund sieben Wochen nach der Bestellung Anfang Juli in Hannover eintraf, war das Betriebssystem-Image in Version 0.4 installiert. Ein Forumsbeitrag bei RVBoards.org verlinkt auf die Version 0.4.1 und eine der chinesischen Seiten erwähnt eine Version 0.5. Letztere muss man jedoch von einer (chinesischen) Baidu-Website herunterladen und dazu wiederum eine chinesische Windows-Software installieren – das haben wir nicht ausprobiert. Die Version 0.4.1 fand sich wiederum zwar auf dem PerfXlab-Server, aber weder unter Windows (mit der chinesischen Software Allwinner Phoenix-Card 4.2.5), noch unter Linux (mit dem dd-Befehl) gelang es uns, sie so auf eine MicroSD-Karte zu schreiben, dass das Nezha-Board davon bootete.

Laut Allwinner ist eine Nezha-kompatible Version von Fedora in Arbeit; die Ankündigung stammt jedoch aus dem April und wir konnten keine weiteren Hinweise finden. Canonical wiederum stellt Server-Versionen (ohne grafische Desktops) von Ubuntu 20.04.2 LTS und 21.04 für zwei (teurere) RISC-V-Boards von SiFive bereit, aber die booteten in unseren



**Das vorinstallierte Linux auf Debian-Basis verwendet den ressourcen-schonenden grafischen Desktop LXDE, reagiert aber sehr träge.**

Versuchen nicht auf dem Nezha. Folglich haben wir alle Experimente mit der vorinstallierten Version 0.4 des mitgelieferten Betriebssystems ausgeführt.

Steckt keine bootfähige MicroSD-Karte im System, dann lädt das Nezha automatisch Tina Linux, ein abgespecktes Minimalsystem auf Basis von OpenWrt. Der Code liegt in einem SPI-Flash-Chip mit 256 MByte Kapazität auf der Unterseite des Nezha. Tina Linux steuert den HDMI-Ausgang nicht an, sondern ist nur über eine serielle Textkonsole am „Debug“-Port nutzbar. Diese wiederum erreicht man von einem anderen Rechner aus über ein im „Basic Package“ mitgeliefertes „USB2TTL“-Kabel, in dem ein USB-Seriell-Wandlerchip von FTDI steckt. Drei der vier offenen Kontakte des USB2TTL-Kabels (schwarz = Ground, grün = RX, weiß = TX) verbindet man mit dem Debug-Pfostenstecker, das USB-Ende steckt man in den anderen PC. Der FTDI-Wandler wird unter Linux automa-

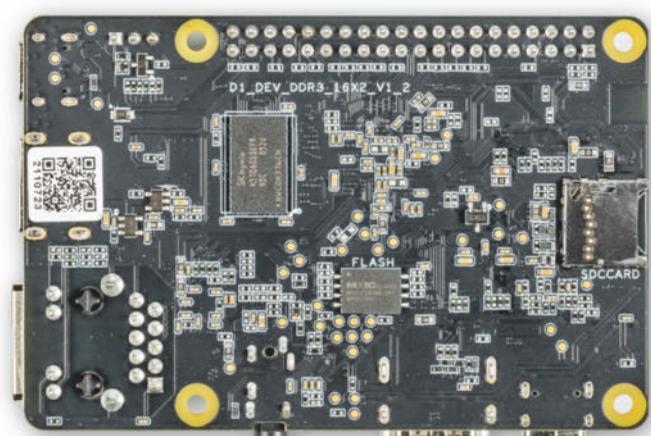
tisch erkannt, für Windows 10 gibt es FTDI-Treiber, sodass man die Konsole beispielsweise mit PuTTY via COM-Port nutzen kann. Unter Linux klappts mit tio und dem Befehl `tio /dev/ttyUSB0`.

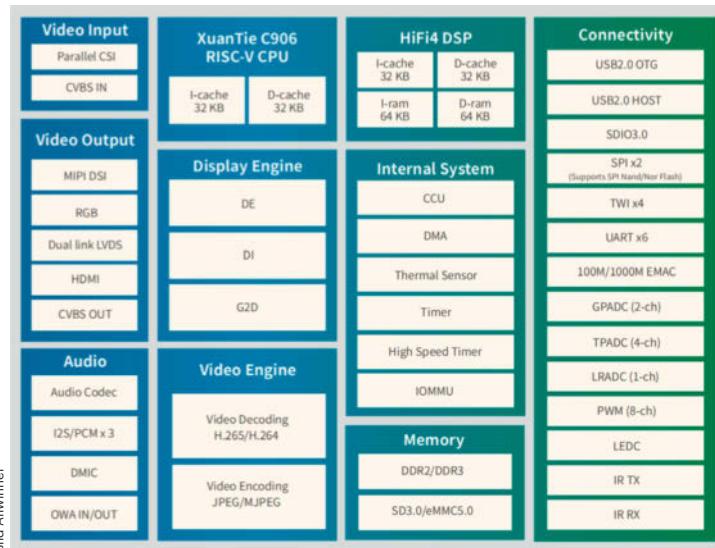
## D1-Kernschau

Den RISC-V-Kern des D1 namens XuanTie C906 hat die Sparte „T-Head“ (alias Pingtouge) des chinesischen Handels- und Cloud-Giganten Alibaba entwickelt. Er steht unter einer gewerblichen Lizenz und ist anscheinend nicht offengelegt. Laut einer Broschüre zum C906 handelt es sich um eine In-Order-Mikroarchitektur ohne L2-Cache, die aber jeweils 32 oder 64 KByte L1-Cache für Daten (L1D) und Befehle (L1I) anbinden kann. Allwinner hat sich beim D1 für nur je 32 KByte L1I/L1D entschieden. Der C906 hat eine Memory Management Unit (MMU) namens Sv39, die den virtuellen Speicher verwaltet.

Linux erkennt den XuanTie C906 als „rv64imafdcv“, was bedeutet, dass er zur

**Die Platine des Nezha von RVBoards ist ebenso groß wie die des Raspberry Pi 4. Auf der Unterseite des Nezha sitzen der zweite DDR3-SDRAM-Chip sowie ein Flash-Chip mit dem Bootloader und Tina Linux.**





**Im Allwinner D1 stecken außer dem RISC-V-Kern XuanTie C906 noch zahlreiche Schnittstellencontroller sowie eine 2D-Grafikseinheit.**

```

Tina Linux (Neptune, SC1C9C53)
processor : 0
hart     : 0
isa      : rv64imafdcv
mmu     : sv39
root@TinaLinux:/# cat /proc/cpuinfo

```

Per USB-Seriell-Wandler bekommt man Zugriff auf die Textkonsole.

Spezifikation RV64GC kompatibel ist. Um das zu verstehen, muss man etwas tiefer in die RISC-V-Spezifikation einsteigen. Die RISC-V-Befehlssatzarchitektur (Instruction Set Architecture/ISA) darf nämlich beliebig erweitert und angepasst werden [2]. Ein 64-Bit-Kern (RV64) muss mindestens lediglich Rechenwerke für ganze Zahlen (Integer, „I“) haben, also „RV64I“ erfüllen. Damit es trotzdem möglichst einfach bleibt, kompatible Linux-Versionen zu entwickeln, hat man dafür eine Basisspezifikation festgelegt, eben RV64GC – doch das ist eine Abkürzung. Das „G“ wurde abgeleitet von „General Purpose“ (Allzweckkern) und steht für die Erweiterungen Multiplikation (M), Atomic Operations (A), Gleitkommazahlen (Floating Point, F) und doppelte Genauigkeit (D), also für „MAFD“. Das nachgestellte

„C“ kennzeichnet die Verarbeitung von komprimierten (compressed) Befehlen, was Speicherplatz und Datentransferrate spart, ähnlich wie bei Arm Thumb. Der XuanTie C906 hat über RV64GC (rv64imafdc) hinaus noch Vektoreinheiten (V) sowie einen User-Mode (U).

Allwinner kombiniert den C906 im D1 mit einem DSP-Kern von Cadence (Tensilica HiFi 4) vor allem für Audiodaten sowie mit zahlreichen Schnittstellencontrollern, 2D-Grafikeinheiten, Video-De- und Encodern sowie einer Display-Engine, die außer HDMI noch beispielsweise LVDS und MIPI DSI ansteuert. Das komplett System-on-Chip (SoC) lässt Allwinner mit 22-Nanometer-Strukturen fertigen.

Auf der seriellen Konsole lässt sich der Bootvorgang des Nezha verfolgen. Den dazu nötigen Code lädt der D1 aus dem

erwähnten SPI-Flash-Speicher. Zunächst startet OpenSBI-Code, der das RISC-V Supervisor Binary Interface (SBI) bereitstellt. Steckt keine bootfähige MicroSD-Karte im Kartenleser, dann bootet automatisch Tina Linux; dort kann man sich auf dem Nezha ohne Passwort mit Root-Rechten auf der Kommandozeile einloggen – praktisch für Entwickler, aber eine klaffende Sicherheitslücke.

Für Tina Linux stellt Allwinner ein Software Development Kit (SDK) bereit, wenn man sich kostenlos als Entwickler registriert.

## Fazit

Die Hardware des RVBoards Nezha funktioniert: RISC-V läuft unter Linux. Doch Dokumentation und Software haben große Lücken und viele rauhe Kanten. Pessimisten würde sagen, dass das lahme und teure Board höchstens für RISC-V-Programmierer interessant ist.

Optimisten sehen es anders: Das Nezha beweist, dass Linux-Systeme mit RISC-V-Chips keine Utopie sind. RV64GC-Designs mit mehreren Kernen und L2-Cache wie der XuanTie C910 (mit Out-of-Order-Technik) und der StarFive JH7100 des BeagleV versprechen deutlich mehr Leistung und stehen in den Startlöchern. Allerdings ist es noch ein weiter Weg bis zum RISC-V-Raspi mit ordentlicher Performance, brauchbarer GPU, guter Linux-Unterstützung und vollständiger Dokumentation. Doch den ersten Schritt hat Allwinner gemacht. (ciw@ct.de) ct

## Literatur

- [1] Christof Windeck, RISC-V mal praktisch, Erste Schritte mit dem RISC-V-Mikrocontroller-Board Sipeed Longan Nano, c't 3/2020, S. 146
- [2] Christof Windeck, Flexiprozessor, Das Potenzial von RISC-V-Prozessoren, c't 19/2019, S. 134

Links zu RVboards Nezha und D1:  
[ct.de/y4cu](http://ct.de/y4cu)

# DIGITAL EVENT **#ISD21**

**16./17.  
September  
2021**

**JETZT  
ANMELDEN!**



**KEYNOTES &  
PANELDISKUSSIONEN  
AUSGEWÄHLTER  
SECURITY-EXPERTEN  
ERWARTEN SIE**

Platin Partner

**DomiNIC**

HUAWEI

Partner

DEUTSCHE GESELLSCHAFT FÜR  
CYBERSICHERHEIT

**heise Events**  
**isd.eco.de**

**eco**  
VERBAND DER  
INTERNETWIRTSCHAFT



# Kombi-Comeback

## Kombiprozessor Ryzen 7 5700G mit Zen-3-Technik (nicht nur) für sparsame Büro-PCs

**Mit den Ryzen-5000-Cpus lassen sich leistungsfähige Ryzen-Systeme mit bis zu acht Kernen bauen, die dank integrierter GPU ohne die derzeit teuren Grafikkarten auskommen. Das spart obendrein Energie.**

Von Christian Hirsch

**A**MD hat PC-Bastler lange auf die modernen Kombiprozessoren Ryzen 5000G „Cezanne“ warten lassen. Weil die Vorgänger Ryzen 4000G mit Zen-2-Architektur Herstellern von Komplett-PCs vorbehalten waren, blieben Endkunden lediglich die beiden Vierkerner Ryzen 3 3200G und 3400G mit betagter Zen+-Technik. Das ändert sich nun mit dem Sechsner Ryzen 5 5600G für 220 Euro und dem Achtner Ryzen 7 5700G für 320 Euro. Letzteren konnten wir vorab eingebaut in einem Komplett-PC kaufen und einzeln testen.

Die zwei Ryzen-Typen mit integrierter Radeon-Grafik sind nicht als separate zweite Serie parallel zu den Ryzen 5000X ohne GPU gedacht, sondern schließen auch einige Lücken im Angebot. Der Achtner Ryzen 7 5700G liegt zwischen dem Ryzen 5 5600X (6 Kerne, 280 Euro) und dem Ryzen 5 5800X (8 Kerne, 380 Euro). Der Sechsner Ryzen 5 5600G runden die Zen-3-Familie nach unten ab. Die neuen Kombi-CPUs laufen auf einem AM4-Mainboard mit A520-, B550-, X570-, B450- oder X470-Chipsatz und haben eine Thermal Design Power von 65 Watt.

Die Ryzen-5000G-Prozessoren für Desktop-PCs sind eng verwandt mit den Mobilprozessoren der Serien Ryzen 5000U und 5000H und verwenden das identische, in 7-Nanometer-Technik gefertigte Halbleiter-Die. Hauptneuerung ist die Zen-3-Architektur der CPU-Kerne, die deshalb bei gleichem Takt 17 Prozent schneller rechnen. Statt zwei getrennter Core Complexes (CCX) mit je vier Kernen gibt es nun nur noch eines mit acht. Dadurch entfallen die Latenzunterschiede bei der Kern-zu-Kern-Kommunikation. Innerhalb eines CCX sind die Antwort-

zeiten zudem deutlich geringer als zu einem Kern in einem anderen CCX.

Des Weiteren hat AMD den Level-3-Cache von 4 MByte pro CCX auf 16 MByte erhöht. Einem Kern steht nun also bis zur vierfachen Menge zur Verfügung, wovon vor allem speicherintensive Programme wie 3D-Spiele profitieren.

Im Vergleich zu den Ryzen 5000X mit 6 bis 16 Kernen ohne GPU gibt es einige Unterschiede beim Prozessoraufbau. Die Ryzen 5000X bestehen aus mehreren Chips: Den CPU Core Dies (CCD) mit acht CPU-Kernen und den Caches sowie einem I/O-Die, in dem Speicher-Controller und I/O-Einheiten sitzen. Die Ryzen 5000G vereinen diese Funktionen und die Radeon-Grafik hingegen zusammen auf einem Halbleiter-Die. Damit die Chipfläche nicht zu groß und damit zu teuer in der Fertigung wird, haben die Kombiprozessoren im Unterschied zu den Ryzen 5000X nur 16 statt 32 MByte L3-Cache pro CCX.

Weil das Halbleiter-Die primär für sparsame Mobilprozessoren entwickelt wurde, beschränkt AMD den PCI Root Complex der Ryzen 5000G auf PCI Express 3.0 statt PCIe 4.0. Er stellt insgesamt 24 Lanes bereit. 16 davon gehen zum PEG-Slot für die Grafikkarte, vier zur M.2-SSD und vier dienen zur Anbindung des Chipsatzes. Der Einsatz von Ryzen-5000G-CPUs auf High-End-Boards mit X570-Chipsatz lohnt sich nicht, weil damit die PCIe-4.0-Fähigkeiten des Chipsatzes entfallen.

Auch thermisch verhalten sich die Kombi-CPUs anders. Während die Ryzen 5000X ihr Package Power Tracking (PPT) von 35 Prozent oberhalb der Thermal Design Power (88 Watt für 65 Watt TDP und 142 Watt für 105 Watt TDP) dauerhaft halten können, gibt es bei den Ryzen 5000G die von den Mobilprozessoren übernommene Funktion Skin Temperature Aware Power Management (STAPM). Dahinter verbirgt sich nichts anderes, als dass die Prozessorleistungsaufnahme die TDP ähnlich wie bei Intels Core-i-CPUs nur für kurze Zeit überschreiten darf und sie im langfristigen Mittel einhalten muss. Deshalb reduzieren die Ryzen 5000G nach einigen Minuten Dauerlast schrittweise ihren Turbotakt, bis das Package Power Tracking die TDP von 65 Watt erreicht hat.

### Effizienzwunder

In der Praxis kann der Ryzen 7 5700G gegenüber seinen Vorgängern deutlich zulegen. So rechnet er in der Multithreading-Wertung des Cinebench R20 14 Prozent

## Ryzen 7 5700G – Performance und Leistungsaufnahme

Prozessor	Kerne / Takt / Turbo	Cinebench R23 1T	Cinebench R23 MT	Leistungsaufnahme Leerlauf / Volllast (Peak) [W]	Preis
		besser ▶	besser ▶	◀ besser	
Ryzen 7 5700G	8+SMT / 3,8 GHz / 4,6 GHz	1510	14000	17/88 (88)	320 €
Ryzen 7 5800X	8+SMT / 3,8 GHz / 4,7 GHz	1604	15572	27/182 (187) <sup>1</sup>	380 €
Ryzen 5 Pro 4650G	6+SMT / 3,7 GHz / 4,2 GHz	1256	9378	16/95 (120)	270 €
Core i7-11700K	8+HT / 3,6 GHz / 5,0 GHz	1578	14905	23/164 (261)	360 €
Core i5-11600K	6+HT / 3,9 GHz / 4,9 GHz	1561	11263	23/163 (296)	230 €

<sup>1</sup> zusätzlich mit GeForce GT 1030 Testsystem: 16 GByte DDR4-3200, SSD

und bei Last auf einem Kern 16 Prozent schneller als der Ryzen 7 4750G mit ebenfalls acht Kernen. Der Performancezuwachs geht teils auf das Konto der höheren Instructions per Cycle als auch der um 200 Megahertz oder 5,5 Prozent höheren Taktfrequenz.

Im Vergleich mit dem Ryzen 7 5800X muss der Kombiprozessor Ryzen 7 5700G zurückstecken, obwohl beide je acht Zen-3-Kerne mit gleichem Nominaltakt verwenden. Der Chiplet-Ryzen arbeitet im Cinebench R23 zwischen 6 und 11 Prozent schneller. Das liegt weniger am 100 MHz höheren Turbotakt und dem größeren L3-Cache, sondern vor allem am thermischen Budget, das beim Ryzen 7 5800X 40 Watt höher ist als bei Ryzen 7 5700G.

Dem ähnlich teuren Intel-Achtkerner Core i7-11700K muss sich der Ryzen 5700G hingegen nur knapp geschlagen geben. Obendrein arbeitet die AMD-CPU dank 7-Nanometer-Technik wesentlich effizienter als der 14-Nanometer-Chip von Intel. Im direkten Vergleich kommt der Ryzen-Kombiprozessor auf 120 Cinebench-Punkte pro Watt, während der Core i7-11700K lediglich 64 Cinebench-Punkte aus einem Watt herauftreibt.

Weil die Kombi-CPU von AMD auch als preiswertere Alternative zum Ryzen 7 5800X für Gaming-PCs beworben wird, haben wir beide Prozessoren mit einer High-End-Grafikkarte vom Typ GeForce RTX 3090 kombiniert. Im synthetischen 3D-Benchmark 3DMark Firestrike lagen die beiden CPUs lediglich 10 Prozent auseinander. Bei realen Spieltiteln wuchs der Unterschied bei Full-HD-Auflösung und hoher Detailstufe auf 16 (Assassin's Creed Odyssey) bis 29 Prozent (Shadow of the Tomb Raider) an. Da Spiele stark von der Speichergeschwindigkeit und kurzen Latzen profitieren, kann der Ryzen 7 5800X mit seinem doppelt so großen Level-3-Cache in dieser Disziplin gegenüber dem Ryzen 7 5700G auftrumpfen.

Zusätzlich haben wir die Latenzen bei der Kern-zu-Kern-Kommunikation gemessen. Im Vergleich zum Ryzen 7 5800X sind diese beim Ryzen 7 5700G mit 23 Nanosekunden sogar 2 Nanosekunden besser. Zum Vorgänger ist der Unterschied aber viel bemerkenswerter: Der Ryzen 7 Pro 4750G hat zu Kernen im gleichen CCX zwar eine Latenz von 22 Nanosekunden, zum anderen CCX beträgt sie jedoch das Dreifache (68 Nanosekunden).

### Schnellere Grafik

An der Radeon-GPU hat AMD bei Cezanne (Ryzen 5000G) zu Renoir (Ryzen 4000G) nichts geändert. Die acht Compute Units (CU) mit jeweils 64 Shader-Kernen verwendet immer noch die fünfte Generation der GCN-Architektur (Graphics Core Next) alias „Vega“, die nun schon rund vier Jahre alt ist. Im 3DMark Firestrike schneidet der Ryzen 7 5700G dennoch rund acht Prozent besser ab und erreicht 3975 Punkte. Der Zuwachs geht wahrscheinlich allein auf das

Konto der kürzeren Kernlatenzen durch den einzelnen Core Complex, der nun alle Kerne umfasst.

Diese Leistung reicht, um recht anspruchslose E-Sport-Titel wie Dota 2 mit sehr hoher Qualität in Full HD flüssig darzustellen (64 fps). Gleches gilt für ältere 3D-Spiele wie Dirt Rally von 2015, wo er eine Bildrate von 67 fps bei hoher Qualität schafft. Zum Vergleich: Die deutlich schwächere UHD-750-Grafik des Core i5-11600K ist nur etwa halb so schnell. Bei modernen Titeln geht der Radeon-GPU des Ryzen 7 5700G allerdings die Puste aus. In der Wirtschaftssimulation Anno 1800 sind selbst mit mittleren Details nur 32 fps drin.

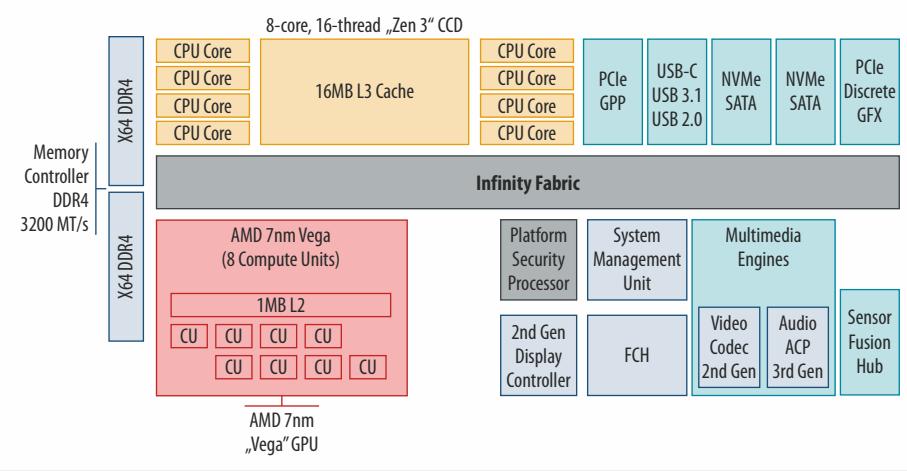
### Fazit

Die Ryzen 5000G sind vor allem dann attraktiv, wenn man relativ viel CPU-Leistung benötigt, aber nur wenig 3D-Performance: fürs Kompilieren, für mehrere virtuelle Maschinen oder für Bild- und Videobearbeitung. Diese Aufgaben erledigt der Achtkerner Ryzen 7 5700G extrem effizient. Gamer, die von vornherein eine leistungsstarke Grafikkarte stecken wollen, sollten beim Bau oder Kauf eines Rechners hingegen lieber zu den Ryzen 5000X mit dem größeren Level-3-Cache greifen. Weil AMD nach längerer Zeit wieder Kombiprozessoren mit aktueller Technik anbietet, die mit aktuellen Chipsätzen zusammen arbeiten, können PC-Bastler ihr AM4-System nun flexibel passend zum Anwendungsprofil mit der optimalen CPU ausrüsten.

(chh@ct.de) ct

## AMD Ryzen 5000G „Cezanne“

Außer den acht CPU-Kernen und den acht Compute-Units der Vega-Grafikeinheit enthält das monolithische Die der Ryzen-5000G-Prozessoren unter anderem eine Videoeinheit und I/O-Controller für PCI Express, USB und SATA. Verbunden sind sie über das Infinity Fabric, das mit der Taktfrequenz des Arbeitsspeichers arbeitet.





# ARM und günstig

## 14-Zoll-Notebook Samsung Galaxy Book Go mit Snapdragon 7c

**Samsungs Galaxy Book Go bietet dank seines ARM-Prozessors Snapdragon 7c ein integriertes LTE-Modem, was bei einem Straßenpreis von 440 Euro eine absolute Besonderheit ist. Doch für den niedrigen Gerätepreis wurde auch an Bildschirm und Speicherausstattung gespart.**

Von Florian Müssig

Qualcomm trommelt seit Ende 2017 für sogenannten Always-Connected-PCs, also Windows-Geräte, die dank integriertem Mobilfunkmodem permanent online sind [1]. Als Antrieb hat Qualcomm seine hauseigenen Snapdragon-Prozessoren ausgerufen: Die SoCs entstammen der Smartphone-Welt und haben deshalb

immer ein LTE-Modem an Bord. Anders als CPUs von AMD und Intel arbeiten sie allerdings ARM- und keine x86-Befehle ab.

Im Gegenzug für die eingeschränkte App-Kompatibilität – dazu später mehr – sollten Snapdragon-befeuerte Notebooks und Tablets günstiger sein als x86-Mobilgeräte, doch dieses Versprechen wurde bislang kaum erfüllt: Geräte mit Snapdragon-SoC wie das Samsung Galaxy Book S oder Microsofts Surface Pro X kosten nämlich trotzdem über 1000 Euro. Erst mit dem jetzt erschienenen Galaxy Book Go rutschen die Preise. Der 14-Zöller geht für 440 Euro über die Ladentheke.

Möglich wird dies unter anderem, weil darin anders als bislang kein High-End-Snapdragon zum Einsatz kommt, sondern das Mittelklassemodell Snapdragon 7c Gen2. Das „Gen2“ bezieht sich auf eine etwas höher getaktete Version des Ende 2019 angekündigten ersten 7c, den man bislang nur in Chromebooks ange-

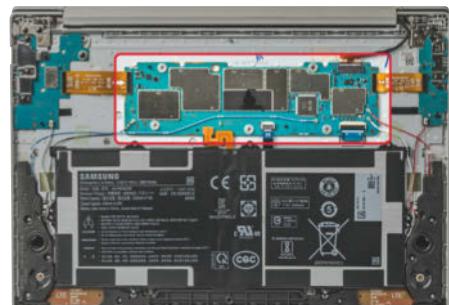
troffen hat (siehe auch S. 74). Bei dem Prozessor handelt es sich wie in der ARM-Welt üblich um einen Verbund unterschiedlich starker CPU-Kerne: Es gibt zwei leistungsstarke und sechs energieeffiziente Kerne. Das SoC kommt mit passiver Kühlung aus, sodass das Notebook durchgängig lautlos arbeitet.

### Performance-Dilemma

Im GeekBench 5 erzielt der 7c Gen2 sowohl bei Single- als auch bei Multithreading-Last in etwa die Werte eines Pentium Silver N6000 oder Celeron N5100 – also von Intels aktuellen Low-End-CPUs, die ausschließlich aus vier kleinen x86-Kernen (ehemals Atom) aufgebaut sind. Von Core-i- oder gar Ryzen-Performance ist der 7c hingegen weit entfernt. Schlimmer noch: Während Windows 10 samt Bordmitteln wie Edge-Browser in einer nativen ARM-Version (WoA, Windows on ARM) vorliegen, sind die meisten Windows-Anwendungen weiterhin ausschließlich als x86-Code verfügbar.

Dann muss eine in Windows enthaltende Emulationsschicht ran, die zusätzlich Leistung frisst; im Cinebench R11.5 liegt der Snapdragon deshalb weit hinter der x86-Konkurrenz. Wer sich angesichts der betagten Versionsnummer wundert: Das ist der letzte Cinebench, den es noch als 32-Bit-Version gab – und die Emulationsschicht kann bisher nur 32 Bit! R15, R20 und R23 bekommt man nur als 64-Bit-App, die deshalb gar nicht im ARM-Windows läuft. Auch viele andere Anwendungen wie etwa Adobes Creative-Cloud-Apps (Photoshop, Premiere, ...) gibt es schon länger nur noch als 64-Bit-Version.

Microsoft hatte Ende 2020 angekündigt, dass die Emulationsschicht künftig auch 64-Bit-x86-Software übersetzen können soll, doch bislang ist davon nichts in Windows 10 angekommen – gut mög-



Alle Komponenten sind auf die kleine Hauptplatine gelötet und zudem mit Blechschilden gekapselt.

lich, dass die Funktion erst künftig mit Windows 11 kommt.

## Speicherknappheit

Letzteres wird nach aktuellem Stand der Dinge auf dem Galaxy Book Go laufen, denn Voraussetzungen wie Secure Boot und fTPM 2.0 sind erfüllt. Beim Arbeitsspeicher kratzt das nagelneue Notebook allerdings schon am absoluten Minimum, weil Samsung dem Gerät nur magere 4 GByte mit auf den Weg gibt.

Weil die LPDDR4x-Chips aufgelötet sind, kann man nicht nachrüsten. Gleicht gilt für die 128 GByte eMMC-Speicher, deren Geschwindigkeit an ältere SATA-SSDs heranreicht. Immerhin kann man befreiend eine MicroSD als Speichererweiterung dazustecken, darf aber keine Geschwindigkeitsrekorde erwarten. Andere Ausstattungsvarianten bietet Samsung hierzulande nicht an. An der Verarbeitung gibt es nichts auszusetzen; preispunktuellisch besteht das Gehäuse aus Kunststoff.

Die Tastatur bietet ein eher weiches, aber brauchbares Tippgefühl; eine Tastenbeleuchtung fehlt. Beide USB-C-Buchsen nehmen Strom entgegen, doch ein Monitor lässt sich nur an der rechten anschließen. Unser mobiles Testdisplay ließ sich jedoch nicht in Betrieb nehmen; vermutlich liefert die Buchse dafür zu wenig Saft. Das mitgelieferte Netzteil stellt magere 25 Watt bereit, weshalb es lange dauert, den Akku zu laden. Die Audioausgabe erfolgt nur mit 16 Bit Tiefe.

Der Bildschirm ist matt, aber mit weniger als 200 cd/m<sup>2</sup> nicht allzu hell und wegen der TN-Bauweise des Panels stark blickwinkeleinabhängig. Damit macht das Galaxy Book Go als Homeoffice- oder -schooling-Notebook, welches tagtäglich mehrere Stunden produktiv benutzt wird, keinen Spaß. Das Gewicht unterscheidet sich mit 1,4 Kilogramm nicht nennenswert von anderen Billig-Notebooks, die Akkulaufzeiten fallen mit bis zu 18,4 Stunden etwas länger aus.

Im Auslieferungszustand fand das Notebook nach der Windows-Ersteinrichtung über Windows Update nicht nur Patches fürs Betriebssystem, sondern auch ein Firmware-Update. Allerdings schaffte es das Gerät nicht, alle gefundenen Updates einzuspielen, sondern hat sich mittendrin aufgehängt. Nach einem harten Reset und ein paar Schweißtropfen auf der Stirn startete es dann aber neu, spielte zuerst die UEFI-Firmware, dann die Windows-Patches ein und zeigte danach keine Auffälligkeiten dieser Art mehr.

## Fazit

Für Akkulaufzeit und Gewicht ist die Prozessorarchitektur eines Notebooks egal, aus Nutzersicht hingegen ganz und gar nicht: Wegen dem weiterhin ungelösten Henne-Ei-Problem der native Apps für Windows-on-ARM-Notebooks hat das Galaxy Book Go einen schweren Stand. Vergleichbare Notebooks mit Low-End-x86-CPUs – also mit voller Windows-Software-Kompatibilität – und ähnlich schlechten TN-Bildschirmen lassen sich bei Speicher-mangel nachträglich aufrüsten [2]. Sie sind zudem mit Preisen unter 300 Euro so viel günstiger, dass man locker einen LTE-

USB-Stick, einen mobilen Router (siehe S. 66) oder ein 100-Euro-Smartphone zum Ankoppeln fürs Immer-Online-Gehen-Können dazukaufen kann und dennoch weniger bezahlt. Damit bleibt als Vorteil nur übrig, dass hier das LTE-Modem tatsächlich vollintegriert ist.

(mue@ct.de) ct

## Literatur

- [1] Christof Windeck, Schlanke Dauerläufer, Always Connected PCs: Windows-10-Mobilrechner mit ARM-Chips angekündigt, c't 1/2018, S. 22
- [2] Carsten Spille, Sparzwang, Billignotebook Acer Aspire 1 (A114-33) mit 14-Zoll-Display und Celetron N5100, c't 16/2021, S. 72

## Samsung Galaxy Book Go: Daten und Testergebnisse

Windows-Notebook mit ARM-Prozessor	
getestete Konfiguration	NP345XLA-KB1DE
Hersteller, URL	Samsung, <a href="http://samsung.de">samsung.de</a>
Lieferumfang	Windows 10 Home 64 Bit, Netzteil
Schnittstellen (V = vorne, H = hinten, L = links, R = rechts, U = unten)	
VGA / DVI / HDMI / DisplayPort / Kamera (Hello)	– / – / – / – / ✓ (–)
USB 2.0 / USB 3.0 / USB 3.1 / LAN	– / 1 × L (1 × Typ C), 1 × R (1 × Typ C) / – / –
Kartenleser / Strom / Docking-Anschluss	L (MicroSD) / – / –
USB-C: Thunderbolt / USB 3.0 / USB 3.1 / DisplayPort / Laden	– / ✓ / – / ✓ / ✓
Ausstattung	
Display	AUO B140HTN02.0: 14" / 35,6 cm, 1920 × 1080, 16:9, 157 dpi, 60 Hz, 4 ... 185 cd/m <sup>2</sup> , matt
SoC	Qualcomm Snapdragon 7c Gen2 (2+6 Kerne), Turbo bis 2,55 GHz, 896 KByte L2-, 1 MByte L3-Cache
Hauptspeicher / Massenspeicher	4 GByte LPDDR4X-4267 / eUFS: Samsung (128 GByte)
Grafikchip (Speicher)	Qualcomm Adreno 618 (vom Hauptspeicher)
Sound	Qualcomm Aqstic
LAN / WLAN	– / Qualcomm (Wi-Fi 5, 2 Streams)
Mobilfunk / Bluetooth (Stack)	Qualcomm Snapdragon X15 (LTE) / Qualcomm (Microsoft)
Touchpad (Gesten) / TPM / Fingerabdruckleser	I2C: HID (max. 4 Finger) / TPM 2.0 / –
Stromversorgung, Maße, Gewicht	
Akku (Ladestopp < 100% einstellbar)	42 Wh Lithium-Ionen (–)
Netzteil	25 W, 95 g, 4 cm × 4 cm × 2,6 cm, Steckernetzteil
Gewicht / Grundfläche / Dicke mit Füßen	1,38 kg / 32,4 cm × 22,6 cm / 1,5 ... 1,7 cm
Tastaturhöhe / Tastenraster	0,9 cm / 19 mm × 18,5 mm
Leistungsaufnahme	
Suspend / ausgeschaltet	0,9 W / 0,7 W
ohne Last: Display aus / 100 cd/m <sup>2</sup> / max.	1,2 W / 3,8 W / 5 W
CPU-Last / Video / 3D-Spiele (max. Helligkeit)	9,3 W / 6,4 W / 7,1 W
max. Leistungsaufnahme / Netzteil-Powerfactor	27 W / 0,57
Laufzeit, Geräusch, Benchmarks	
Laufzeit Idle (100 cd/m <sup>2</sup> ) / Video (200 cd/m <sup>2</sup> ) / 3D (max)	18,4 h / 9,7 h / 8,1 h
Ladestand / Laufzeit nach 1h Laden	41 % / 7,6 h
Geräusch ohne / mit Rechenlast	lautlos
Massenspeicher lesen / schreiben	506 / 192 MByte/s
IOPS (4K) lesen / schreiben	12890 / 7155
Leserate SD-Karte	79 MByte/s
WLAN 5 GHz / 2,4 GHz (20 m) / MU-MIMO-fähig	29,6 / 22,5 MByte/s / ✓
Qualität Audioausgang / Dynamikumfang	⊕ / 91,5 dB/A)
Cinebench R11.5 Rendering (ST / MT)	0,27 / 1,93
Geekbench 5 (ST / MT)	556 / 1623
3DMark: Night Raid	1984
Preis und Garantie	
Straßenpreis Testkonfiguration	440 €
Garantie	2 Jahre
⊕⊕ sehr gut    ⊕ gut    ○ zufriedenstellend    ⊖ schlecht    ⊖⊖ sehr schlecht	✓ vorhanden    – nicht vorhanden    k.A. keine Angabe

# Schwarzmalerei

## OLED vs. LCD: Sony 65A90J und 55X90J im Vergleich

**Durch die partielle Abdunklung der Hintergrundbeleuchtung sollen LCDs mit OLEDs gleichziehen. Wir haben an zwei Sony-TVs untersucht, ob das gelingt.**

Von Ulrike Kuhlmann

Die TV-Hersteller haben in der jüngsten Vergangenheit das Local Dimming ihrer neuesten LCD-TV-Generation sowie ihre verbesserten Bildoptimierungen geprägt. Wir wollten am Beispiel zweier aktueller 4K-Fernseher von Sony prüfen, ob aktuelle LC-Displays dadurch in Sachen Videoqualität nun dem Vergleich mit OLED-Fernsehern standhalten. Dazu haben wir uns den XR-65A90J ins Labor geholt, Sonys aktuelles OLED-Spitzenmodell, das derzeit für 3190 Euro zu haben ist. Als Vergleich diente uns der XR-55X90J, der unter Sonys LCD-TVs die Spitzenspitze darstellt und 1360 Euro kostet. Die 65-Zoll-Version dieses LCD-TVs kostet 1490 Euro, das gleich große OLED-Gerät ist also etwa doppelt so teuer. Preisvergleich unter 55-Zöllern: Die OLED-Variante kostet 2300 Euro und damit 1,7 Mal so viel wie das LCD.

### Licht an

Im Auslieferungszustand erreicht das OLED im HDR-Betrieb eine Maximalleuchtdichte von 790 cd/m<sup>2</sup>, beim LCD-TV waren es 906 cd/m<sup>2</sup>, jeweils gemessen an einem weißen Quadrat auf schwarzem Grund, das 10 Prozent der Gesamtfläche erhellt (10 Prozent Weiß). Das ist ein guter Wert für das OLED. Während das LCD auch bei zunehmendem Weißanteil hell blieb – bei komplett weißem Schirm waren es 625 cd/m<sup>2</sup> –, wurde das OLED schnell dunkler, bei einem komplett weißen Inhalt leuchtete es nur noch mit 190 cd/m<sup>2</sup>. Grund: Die Leistungsaufnahme hängt stark vom Weißanteil ab und damit auch die Belastung des organischen Displays (Stichwort Alterung). Deshalb muss der

Hersteller die Stromstärke durch die organische Schicht begrenzen. Anders als Sony Anfang des Jahres erklärt hat, leuchteten im Test bei punktuellen Spitzlichtern wie Explosionen oder Kerzenflackern nicht etwa alle vier Subpixel (Rot, Grün, Blau, Weiß) auf, sondern allenfalls drei – das blaue Subpixel blieb für Weiß stets dunkel.

Von der höheren Leuchtdichte des LCD-TV profitiert man in sonnendurchfluteten Räumen – gegen ein helles Fenster kann das OLED-TV wenig ausrichten, für draußen taugt es gar nicht. Allerdings ist es im abendlichen Wohnzimmer oder gar Heimkino viel entscheidender, wie schwarz am TV Schwarz dargestellt wird. Hier konnte das Sony-LCD-TV trotz punktueller Dimmung und umfangreicher Bildoptimierung nicht mithalten. Das liegt auch an der überschaubaren Anzahl der Zonen, die Segmente gleicher Helligkeit geraten dadurch zu groß.

Besonders deutlich wird der Unterschied zwischen LCD und OLED beim Abspann von Filmen: Während der schwarze Hintergrund bei Laufschriften am OLED einfach schwarz blieb, geriet er beim LCD-TV grau. Allerdings soffte sehr dunkle Bilddetails am OLED etwas ab, die Darstellung verlor dadurch an Zeichnung. Die Farben

wirkten etwas gedeckter, leuchteten aber gerade in dunkleren Szenen sehr schön. Insbesamt wirkte die Darstellung etwas kühler als am LCD-TV. Sony möchte den mäßigen Schwarzwert des LCDs durch eine besonders intensive Darstellung mit knackigen Farben ausgleichen. XR Triluminos Pro mit Cognitive Processor nennt der Hersteller seine neueste Bildoptimierung. Tatsächlich wirkt die Wiedergabe sehr lebendig, doch sie blieb gerade in dunkleren Szenen hinter der ausdrucksstärkeren Darstellung des OLED-TVs zurück. Der Hersteller nutzt für den 55X90J ein VA-Panel mit zweigeteilten Subpixeln, dessen Farben etwas blickwinkelabhängig sind – das ist im Grunde nicht mehr zeitgemäß für ein Topgerät, wird einen einzelnen Zuschauer im Wohnzimmer aber wenig stören.

### Ausstattung

Beide TVs sind sehr gut ausgestattet mit Doppeltuner nebst Aufnahmefunktion, Sprachsteuerung, Unterstützung der Hochkontrastformate HDR10, Dolby Vision und HLG, dem für Netflix optimierten Netflix Calibrated Modus, der Anbindung von Mobilgeräten via Chromecast oder AirPlay und natürlich einer Vielzahl von Apps aus dem Store des Android-TV.



Das OLED-TV XR-65A90J zeigt etwas gedeckte Farben, liefert aber gerade in dunkleren Szenen ausdrucksstarke Bilder.



**Sony optimiert die Darstellung des LCD-TV XR-55X90J so, dass sie dem menschlichen Auge gefallen soll. Das gelingt gut, hilft aber nicht gegen die Blickwinkel-abhängigkeit.**

Während im OLED-TV ein Raummikrofon eingebaut ist, das sich über einen Schalter im Displayrücken hart abschalten lässt, steckt das Mikro beim LCD-Gerät ausschließlich in der Fernbedienung. Letztere ist beim teureren OLED-Fernseher wertiger und besitzt hinterleuchtete Tasten; das hilft im dunklen Wohnzimmer.

Im OLED steckt eine weitere Besonderheit, nämlich die Acoustic Surface genannte Technik, bei dem die Displayoberfläche als Lautsprecher dient. Dafür stecken im Rücken des OLED zwei Aktuatoren, die Audio-Schwingungen auf das Display übertragen und es so seinerseits in unsichtbare Schwingungen versetzen. Dadurch gelangen beispielsweise die Dialoge der am Schirm gezeigten Personen direkt aus dem Bild zum Zuschauer. Da sich über die kleinen Aktuatoren kein Bass erzielen lässt, hat Sony zusätzlich zwei Tieftöner an den Seiten hinten spendiert. Das ganze System sorgt für eine sehr angenehme Audiokulisse, aber keinen überragenden Heimkino-Sound. Alternativ kann man das OLED-TV als Center-Lautsprecher in eine Mehrpunkt-Anlage einbinden. Das LCD-TV wartet diesbezüglich mit weniger Raffinessen auf, es besitzt aber ordentliche 10-Watt-Lautsprecher.

Die für Gamer interessanten Funktionen wie 4K-Signale mit 120 Hertz Bildwiederholung und der latenzarme ALLM-Modus werden an HDMI 3 und 4 unterstützt; die variable Refreshrate (VRR) muss Sony weiterhin per Firmware-Update nachliefern. Aktuelle TVs von Samsung und LG beherrschen die Gaming-Modi inzwischen an ihren HDMI-Eingängen.

## Android TV

Beide Android-TVs nutzen die aktuelle Version 11, bei der Google auf Video-

vorschläge setzt und die Apps weniger in den Vordergrund stellt. Das kann hilfreich sein, wenn man nur wenige Apps nutzt und brav das Vorschlagssystem mit seinen Vorlieben füttert. Wer das nicht tut, muss den Cursor auf der Suche nach Apps mehr bewegen als bisher.

Die Orientierung ist dank der neuen Sortierung aber etwas einfacher geworden. Außerdem kann man bei Sony mit einem Klick auf das Zahnrädchen die Schnellauswahl-Leiste aufrufen und wichtige Einstellungen darin nach vorn holen. Weil Sony das Bild werksseitig bereits gut eingestellt hat, werden die meisten Zuschauer nicht

mehr allzu viel verändern wollen. Eine weitgehend unverfälschte Darstellung bietet der Anwender-Modus, darin sind nur wenige Bildoptimierungen aktiv und Kameraschwenks werden glatt und ohne starken Soap-Effekt wiedergegeben.

## Fazit

Gegen das satte Schwarz der OLEDs ist bei Sonys LCD-TVs noch kein Bildoptimierungskraut gewachsen. Dazu bräuchte es deutlich mehr einzeln dimmbare Zonen. Vom hohen Kontrast profitieren auch die Farben am OLED-TV, allerdings kann das LCD-Modell hier mithalten und in sehr heller Umgebung sogar ausdrucksstärkere Bilder liefern. Für Heimcineasten bleibt die OLED-Technik indes weiterhin das Maß der Dinge.

Angesichts der ansonsten vergleichbar guten Ausstattung bleibt die Frage, ob das Mehr an Kontrast, der etwas bessere Klang und das schickere Design den doppelten Preis fürs OLED wert ist. Wer häufig im Hellen schaut oder oft am TV spielen will – Achtung: Spielstände und ähnliche statische Inhalte können sich einbrennen –, fährt mit dem LCD-Modell besser. Videoliebhaber und auch abendliche TV-Zuschauer dürften dagegen von der kontraststarken Darstellung am OLED profitieren. (uk@ct.de) ct

## Smart-TVs mit OLED- und LC-Display

Modell	XR-65A90J	XR-55X90J
Hersteller	Sony	Sony
Display Typ	OLED	LCD
Diagonale / Bildgröße	65 Zoll (1,65 m) / 1,43 m × 0,81 m	55 Zoll (1,40 m) / 1,22 m × 0,68 m
Auflösung	3840 × 2169 Pixel (Ultra HD), 68 dpi	3840 × 2169 Pixel (Ultra HD), 80 dpi
Signaleingänge	2 × HDMI 2.0, 1 × USB 2.1, 2 × HDMI 2.1 (eARC, ALLM, VRR nach Update), jeweils inkl. HDCP 2,3	2 × HDMI 2.0, 2 × HDMI 2.1 (eARC, ALLM, VRR nach Update), jeweils inkl. HDCP 2,3
TV-Tuner	2 × DVB-T2/C/S2, 1 × CI+ Slot	2 × DVB-T2/C/S2, 1 × CI+ Slot
weitere Eingänge	2 × USB 2.0, 1 × USB 2.1, Ethernet, WLAN 802.11ac, Bluetooth 5.0 LE, AV (per Adapter), Klinke (Kopfhörer), dig. Audio Out (Toslink)	2 × USB 2.0, 1 × USB 2.1, Ethernet, WLAN 802.11ac, Bluetooth 5.0 LE, AV (per Adapter), Klinke (Kopfhörer), dig. Audio Out (Toslink)
Lautsprecher	2 × 10 W (Acoustic Surface), 2 × 20 W (Bass)	2 × 10 W (Hochtöner + Bass)
Abmessungen	1,50 m × 83,5 cm × 32 cm / 24,6 kg	1,23 m × 78,5 cm × 34 cm / 17,4 kg
Betriebssystem	Android TV, Version 10	Android TV, Version 10
HDR	HDR 10, Dolby Vision, HLG	HDR 10, Dolby Vision, HLG
Audio	Dolby Atmos, DTS	Dolby Atmos, DTS
Ausstattung	HbbTV, USB-Recording, Sprachsteuerung, Google Assistant, Amazon Alexa, Apple Airplay/Home Kit, Chromecast, AutoCal mit Calman, Integr. Mikro (abschaltbar)	HbbTV, USB-Recording, Sprachsteuerung, Google Assistant, Amazon Alexa, Apple Airplay/Home Kit, Chromecast, AutoCal mit Calman
Bewertung		
Bildeindruck	⊕⊕	⊕
Klangeindruck	⊕	○
Ausstattung / Medienfunktionen	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕
Bedienung	○	○
Garantie	2 Jahre	2 Jahre
Preis	3190 € (Stand 19.7.2021)	1360 € (Stand 19.7.2021)

⊕⊕ sehr gut    ⊕ gut    ○ zufriedenstellend    ⊖ schlecht    ⊖⊖ sehr schlecht



# Hochsicherheits-PC

## Mini-PC Nitrokey NitroPC mit quelloffener Firmware

**Dank Open-Source-Firmware und deaktivierter Management Engine ist der flinke NitroPC vertrauenswürdiger als andere Rechner – und damit prinzipiell auch sicherer. Seine SSD ist standardmäßig verschlüsselt.**

Von Ronald Eikenberg  
und Christof Windeck

**D**er kompakte NitroPC des Berliner Herstellers Nitrokey ist nur äußerlich eine Black Box: Innerlich geht es transparent zu, denn nicht nur das vorinstallierte Linux ist Open Source, auch die UEFI-Firmware. Das ist durchaus eine Seltenheit, denn fast alle anderen Rechner sind mit einem proprietären (UEFI-)BIOS aus-

gestattet, über das man keine Kontrolle hat. Auch die Management Engine (ME) der Intel-Chipsätze ist unkontrollierbar, beim NitroPC ist sie deshalb weitgehend abgeschaltet.

Dies soll den NitroPC besonders vertrauenswürdig machen, wodurch er sich sogar als Hochsicherheitsrechner in Unternehmen und Behörden sowie als Arbeitsrechner für investigative Journalisten eignen soll. Wer möchte, kann die Open-Source-Firmware, eine Kombination aus Coreboot und TianoCore, selbst kompilieren und flashen. Der Hauptvorteil ist jedoch, dass ihr Code öffentlich einsehbar ist. Jeder kann ihn auf Sicherheitslücken und Backdoors abklopfen, allerdings mit Ausnahme einiger proprietärer Binärkomponenten von Intel – sogenannte BLOBs –, etwa dem Firmware Support Package (FSP), ohne die auch der NitroPC nicht auskommt.

Bei einem vollständig proprietären BIOS muss man hingegen darauf vertrau-

en, dass der Hersteller alles richtig gemacht hat, denn unabhängige Code-Audits sind selten. Dieser Vertrauensvorschuss kann jedoch gefährlich werden: So musste etwa Dell kürzlich ein Sicherheitsloch stopfen, durch das Angreifer Code im Kontext des UEFI-BIOS ausführen konnten – und das ist nur eines von vielen Beispielen. Das BIOS gilt bei Hackern als heiliger Gral. Wer es schafft, sich darin einzunisten, hat das System weitreichend unter Kontrolle und muss nicht fürchten, dass die Infektion jemals vom Virensucher entdeckt wird.

Das Gleiche gilt für die Management Engine (ME). Es handelt sich um einen Computer im Computer, der chipsatzspezifische Funktionen wie TPM und Hardware-Monitoring übernimmt, aber auch den Fernzugriff aufs System ermöglichen kann. Das öffentliche Wissen über ihre Funktionsweise stammt vor allem von unabhängigen Sicherheitsforschern, die durch Reverse Engineering auch schon diverse kritische Sicherheitslücken darin entdeckt haben. Nitrokey löst dieses Problem, so gut es geht: Wie alle modernen Intel-Systeme ist zwar auch der NitroPC mit der ME ausgestattet, sie ist jedoch so weit wie möglich deaktiviert. Der Hersteller nutzt hierfür das Open-Source-Tool me\_cleaner (siehe ct.de/y3zz).

Diese Besonderheiten schränken die Konfigurierbarkeit ein wenig ein: Wer gerne an den BIOS-Setup-Einstellungen schraubt, macht beim NitroPC ein langes Gesicht. Drückt man beim Einschalten die Esc-Taste, kann man über das rudimentäre BIOS-Setup im Wesentlichen die Boot-Reihenfolge der physischen Datenträger ändern. Netzwerk-Boot beherrscht der Rechner nicht. Etwas mehr geht über die UEFI-Shell. Sie kann unter anderem detaillierte Informationen über Hardware und UEFI-Treiber ausgeben.

Auch die Management Engine ist funktional eingeschränkt: So fehlt das Trusted Platform Module (TPM), das unter Windows etwa für Measured Boot, FIDO2 und BitLocker nützlich ist. Dank der UEFI-Kompatibilität könnte man Windows 10 prinzipiell installieren, aber das wäre widersinnig, weil das Closed-Source-Betriebssystem mehr Risiken birgt, als die Open-Source-Firmware vermeidet. Wer gelegentlich auf ein Windows angewiesen ist, sollte es auf dem NitroPC besser in einer VM nutzen.

Anders als das NitroPad [1], einem durch Nitrokey modifizierten Lenovo

Thinkpad, ist der NitroPC nicht mit der Custom-Firmware Heads ausgestattet. Heads startet dort nach dem Coreboot-BIOS und überprüft, ob das BIOS und wichtige Boot-Dateien manipuliert wurden. Dem NitroPC fehlt mit dem TPM der dafür nötige Vertrauensanker.

Bei der Bestellung im Online-Shop kann man zwischen Ubuntu, Debian und Linux Mint wählen. Gegen 45 Euro Aufpreis installiert Nitrokey auch Qubes OS, das durch seine Virtualisierungsschichten besonders sicher ist. Unser Testgerät war mit Ubuntu 20.04 LTS ausgestattet, dessen LUKS-Festplattenverschlüsselung bereits aktiv war. Ein Beipackzettel wies uns darauf hin, das vorgegebene Standardpasswort „PleaseChangeMe“ zu ändern. Vorinstalliert war lediglich die Nitrokey-App zur Verwaltung der gleichnamigen Krypto-Sticks, die der Hersteller ebenfalls verkauft. Ubuntu lief während unseres Tests flink und zuverlässig auf dem Mini-PC, an der Linux-Kompatibilität der Hardware hatten wir nichts auszusetzen.

## Hardware

Der NitroPC ist weitgehend baugleich mit dem etwas teureren Librem Mini v2 der US-Firma Purism [2]. Die Hardware fertigt ein ungenannter chinesischer OEM-Hersteller; sehr ähnliche Geräte findet man bei AliExpress etwa unter der Marke Hystou, allerdings mit „normalem“ UEFI-BIOS.

Im Mini-PC rechnet der 2019 vorgestellte Intel-Mobilprozessor Core i7-10510U aus der 14-Nanometer-Generation „Comet Lake“. Seine vier Kerne takten kurzzeitig mit bis zu 4,9 GHz, unter Last sind es eher 4,3 GHz. Die Rechenleistung gleicht der eines zwei Jahre alten Notebooks der 1000-Euro-Klasse und genügt auch für anspruchsvollere Aufgaben, zumal Nitrokey für das Gerät bis zu 64 GByte RAM anbietet. Unser Testgerät war mit 16 GByte RAM und einer NVMe-SSD mit 1 TByte bestückt. Gegen Aufpreis bekommt man auch eine 2-TByte-SSD und sogar eine zweite (SATA-)SSD mit ebenfalls bis zu 2 TByte.

Am Betriebsgeräusch gibt es nichts zu meckern: Im Leerlauf hört man den Lüfter praktisch nicht und selbst unter Vollast bleibt der NitroPC sehr leise. Auch die Leistungsaufnahme ist mit knapp 5 Watt im Leerlauf ziemlich niedrig. Kurzzeitig schluckt der Mini – wie viele andere auch – bis zu 40 Watt, was an der Grenze der Belastbarkeit des beigelegten Netzteils liegt; dabei zeigten sich aber keine Probleme.

Gute Noten verdient sich der Mini-PC bei den Datentransferraten. Zwar gibt es noch schnellere PCIe-SSDs und WLAN-Adapter, in der Praxis hat das aber wenig Bedeutung. Die USB-C-Buchse schafft sogar USB 3.2 Gen 2x2, überträgt aber leider keine Displaysignale. Es gibt noch sechs weitere USB-Buchsen, aber keinen Kartenleser.

Der NitroPC startet ohne Speicher bei 599 Euro und liegt damit ungefähr auf dem Preisniveau eines ähnlich ausgestatteten Intel NUC. Betriebsbereit mit 8 GByte RAM und 256-GByte-SSD gibt es ihn für 679 Euro, die Maximalausstattung mit 64 GByte RAM und 2-TByte-SSD kostet über 1400 Euro. Eine zweite SSD und Qubes OS kosten noch mal extra. Auf Wunsch verschickt Nitrokey den Mini-PC für 50 Euro auch mit versiegelten Schrauben in einem ebenfalls versiegelten Beutel. So können Käufer nachvollziehen, ob das Gerät auf dem Transportweg geöffnet und potenziell manipuliert wurde.

## Fazit

Wer einen kompakten Linux-PC sucht und sich nicht um die Installation und etwige Hardware-Inkompatibilitäten kümmern möchte, bekommt mit dem NitroPC ein rundes Gesamtpaket zu einem fairen Einstiegspreis. Obendrauf gibts durch das quelloffene UEFI-BIOS und die reduzierte Management Engine ein Plus an Ver-



**Anschlussfreudig:** Der NitroPC bietet zahlreiche Ports, darunter USB-C mit USB 3.2 Gen 2x2.

trauenswürdigkeit – und damit im Prinzip auch an Sicherheit. Das könnte für manche Zielgruppen Kaufentscheidend sein. Der Mini-PC ist sehr leise und flink genug für die meisten Einsatzzwecke, als Spiele-Computer ist das Linux-System mit seiner Onboard-Grafik jedoch ungeeignet. Der NitroPC ist eine gute Alternative zum Librem Mini v2, der nicht nur etwas teuer ist, sondern auch aus den USA verschickt wird und demzufolge durch den Zoll muss.

(rei@ct.de) ct

## Literatur

- [1] Ronald Eikenberg, Hochsicherheits-Notebook, Linux-Notebook Nitrokey NitroPad X230, c't 7/2020, S. 96
- [2] Johannes Merkert, Freiheits-Notebook, Das Librem 15 mit PureOS und quelloffenem Coreboot, c't 23/2017, S. 114

**Firmwarequellen, Herstellershop:**  
[ct.de/y3zz](http://ct.de/y3zz)

## Nitrokey NitroPC

Sicherer Mini-PC mit Open-Source-Firmware ohne Intel ME	
Hersteller, URL	Nitrokey, <a href="http://nitrokey.com">nitrokey.com</a>
Prozessor	Intel Core i7-10510U (4 Kerne, 8 Threads, 1,8–4,9 GHz, 15 W, Comet Lake (CML))
GPU / RAM	Intel UHD (integriert in CPU) / 16 GByte (2 × 8 GByte DDR4-2666, max. 64 GByte)
SSDs	1 × 1 TByte M.2 (PCIe 3.0 x4), optional 1 × SATA 2,5 Zoll bis 2 TByte
1 GBit/s-Ethernet / WLAN	1 × Realtek RTL8111 / Qualcomm QCA6174A (Wi-Fi 5, 2x2, BT 5.0, M.2)
Anschlüsse vorn	2 × USB-A 3.2 Gen 2 (10 GBit/s), 2 × USB-A 2.0, 1 × Audio-Klinke
Anschlüsse hinten	1 × HDMI 2.0, 1 × DP 1.2, 2 × USB-A 3.2 Gen 2, 1 × USB-C 3.2 Gen 2x2 (20 GBit/s), 1 × Stromversorgung, 2 × WLAN-Antennen
Betriebssystem	Ubuntu 20.04 LTS
Netzteil	Chicony A13-040N3A (19 V/40 W)
Abmessungen Gehäuse	12,8 cm × 3,8 cm × 12,8 cm (ohne Stecker)
mitgeliefertes Zubehör	VESA-Montageadapter
Messwerte (Linux, 4K-Display, USB-Tastatur/-Maus)	
Blender 2.82a, Szene Blender	705 s
7-zip (Ver-/Entschlüsseln)	20.852 / 17627 MIPS
PCIe-3.0-SSD (lesen / schreiben)	2,2 / 1,8 GByte/s
USB-A 3.2 Gen 2 (lesen / schreiben)	1,0 / 1,0 GByte/s
USB-C 3.2 Gen 2x2 (lesen / schreiben)	2,2 / 2,0 GByte/s
WLAN-Durchsatz 2,4 / 5 GHz	nah: 140 / 518 MBit/s, 20 Meter: 13 / 105 MBit/s
Leistungsaufnahme Soft-off	0,7 W
Leerlauf / Volllast CPU	4,9 / 26 W (kurzzeitig 40 W)
Geräusch im Leerlauf / CPU-Volllast	< 0,1 sone / 0,3 sone
Preis Testgerät / Garantie	867 € / Gewährleistung 24 Monate



# Weit gelinst

## High-End-Androide Sony Xperia 1 III

**Das Sony Xperia 1 III ist ein High-End-Smartphone mit Vollausrüstung. Dem scharfem OLED, der Kamera mit verstellbarer Linse und dem wasserdichten Gehäuse steht aber auch die eine oder andere Schwäche gegenüber.**

Von Robin Brand

Um im Smartphone-Markt aufzufallen, reichen manchmal Kleinigkeiten. So sucht man bei Sonys neuem Top-Smartphone Xperia 1 III vergeblich einen Notch oder ein Punchhole – also eine Displayausparung für die Frontkamera. Annehmlichkeiten wie eine Kopfhörerbuchse oder eine Benachrichtigungs-LED, die viele Hersteller für ihre Oberklasse-Smartphones einsparen, gehören dagegen zur

Ausstattung. Das 1300 Euro teure Xperia 1 III wartet zudem mit einer Kameralinse auf, die es in einem Smartphone so noch nicht gegeben hat: ein Tele mit zwei optischen Brennweiten.

Die Verarbeitung des Xperia 1 III mit gläserner Rückseite und kantigem Metallrahmen ist tadellos. Im Metallrahmen sitzen neben Lautstärkewippe und Einschalter mit Fingerabdrucksensor auch eine Taste, die den Google-Assistant weckt, und ein physischer Auslösebutton für die Kamera. Das Smartphone ist gemäß der Schutzarten IP65 und IP68 staub- und wasserdicht. Die Balken ober- und unterhalb des Displays sind für aktuelle Smartphone-Verhältnisse recht groß. Darin hat Sony Lautsprecher, Benachrichtigungs-LED und Frontkamera untergebracht.

### Linse, wechsle dich

Die rückwärtigen Kameras sitzen untereinander angeordnet in einem am Rand platzierten Kameraareal, sodass das Smartphone leicht kippelt, wenn es auf

einer Tischplatte liegt. Alle drei Kameras lösen 12 Megapixel auf. Die weitwinklige Hauptkamera (24 Millimeter Kleinbildäquivalent) und das doppelte Tele (70 und 105 Millimeter) sind optisch stabilisiert. Wechselt man von 70 auf 105 Millimeter, springt eine Linse in der quer ins Gehäuse eingebauten Telekamera von einem definierten Punkt im Objektiv an den anderen. Dabei verkleinert sich die Blende von  $f/2,3$  auf  $f/2,8$ . Schaut man senkrecht auf die Kamera, erkennt man den Wechsel mit bloßem Auge. Hinzu kommt ein Ultraweitwinkel (16 Millimeter) sowie ein Time-of-flight-Sensor für Autofokus und Tiefenschärfe.

Die Hauptkamera schießt auf dem Stativ im Labor aus circa einem Meter Entfernung zum Testchart scharfe, detailreiche Fotos. Sony verzichtet im Unterschied zu Samsung beim S21 Ultra auf allzu heftiges Nachschärfen. So wirken die Fotos auf dem kleinen Smartphone-Bildschirm nicht so knallig; vor allem auf größeren Monitoren gefällt uns der natürlichere und ruhigere Bildlook besser. Für Ultraweitwinkel und die beiden Teles gilt das nur mit Abstrichen. Zwar erzeugen sie einen ähnlichen Bildlook, erreichen aber nicht den Detailgrad der Hauptkamera.

Das Sony-Smartphone hat keinen ausgewiesenen Nachtmodus für die Fotografie im Dunkeln. Wird es schummrig, hellen andere Smartphones wie Apple iPhone 12, die Google Pixels oder vorgenanntes S21 Ultra stärker auf. Auch in diesem Fall entscheidet sich Sony für eine vergleichsweise natürliche JPEG-Bearbeitung. Verlängert man die Belichtung manuell, zaubert das Sony-Smartphone ähnlich viel Licht ins Dunkel wie die Klassenbesten – das funktioniert aber nur auf einem Stativ.

### Schnell im Fokus

In der Praxis fällt der schnelle Autofokus der Hauptkamera positiv auf. Bis zu 20 Fotos pro Sekunde nimmt das Xperia 1 III auf und berechnet dabei nach Sony-Angaben 60-mal den Fokus neu. Fotografiert man zum Beispiel den zappeligen Nachwuchs, will man das nicht mehr missen. Die beiden Teles können da nicht mithalten, immer wieder produzierten wir Ausschuss mit falsch fokussierten Motiven.

Zur Höchstform läuft das Smartphone auf, wenn man den umfangreichen Pro-Modus verwendet. Dieser ist in Aussehen und Bedienung an die Sony-Kameras der Alpha-Reihe angelehnt. Darin lässt sich zum Beispiel in Programmautomatik oder

komplett manuell fotografieren. Die gelungenen aufbereitete Bedienoberfläche animiert auch Laien, sich mit der Fotografie auseinanderzusetzen. Fotografieren kann man im Pro-Modus ausschließlich mit dem physischen Auslösebutton im Gehäuserahmen.

Wie die beiden Vorgänger ist auch die dritte Generation des Xperia 1 mit einem hochauflösenden 6,5-Zoll-OLED-Bildschirm im 21:9-Format ausgestattet. Sony wirbt mit einer 4K-Auflösung, die 3840 × 1644 Pixel entsprechen dem aber nicht ganz. Dennoch ist die Pixeldichte von 644 dpi höher als die aller anderen Smartphone-Displays, die wir bisher im Labor hatten. Das Resultat sind gestochten scharfe Schriften – allein: Der Unterschied zu etwas geringer auflösenden Panels anderer Top-Smartphones (400 bis 500 dpi) ist mit bloßem Auge nicht auszumachen. Eine Möglichkeit, die Auflösung runterzuregeln, um Akku zu sparen, gibt es nicht.

Für scharfe Schrift auch während des Scrollens sorgt die Bildwiederholrate von maximal 120 Hertz, diese lässt sich auch auf 60 Hertz begrenzen. Unterdurchschnittlich für High-End-Verhältnisse ist die maximale Leuchtkraft des Displays, es erreicht maximal 550 cd/m<sup>2</sup>. Maximale Helligkeiten um 1000 cd/m<sup>2</sup> sind für Smartphones dieser Preisklasse eigentlich Standard, selbst Sonys Mittelklasse-Smartphone Xperia 10 III leuchtet heller (618 cd/m<sup>2</sup>). Dramatisch ist das nicht, selbst wenn man in der Sonne steht, kann man das Display des Xperia 1 III ablesen, bei einem zum Vergleich herangezogenen Samsung Galaxy S21 ist das aber entspannter für die Augen.

## Durchschnittlicher Akku

Auch die Akkulaufzeit des Xperia 1 III erreicht kein High-End-Niveau, daran dürfte das hochauflösende Display nicht unschuldig sein. In der Praxis pendelten wir uns auf einen Ladestopp pro Tag ein. Bei genügsamer Nutzung sind auch zwei Tage drin.

Sony stattet das Xperia 1 III mit Qualcomm's Spitzen-Chipsatz Snapdragon 888 samt 12 GByte RAM aus. Damit gehört es zu den schnellsten Android-Smartphones. Weder mehrere parallel geöffnete Anwendungen noch aufwendige 3D-Spiele oder das Abspielen von 4K/120-fps-Videodateien bringen es an seine Leistungsgrenzen. Unter Dauerlast drosselt das Xperia 1 III allerdings recht stark und wird heiß – ein Phänomen, das wir auch bei anderen

Smartphones mit Snapdragon 888 beobachtet haben. Der Snapdragon funkts dank integriertem 5G-Modem zukunftsfähig – für den Nahbereich sind zudem Wi-Fi 6 und Bluetooth 5.2 an Bord. Der 256 GByte fassende Flashspeicher des Sony-Smartphones lässt sich per MicroSDXC-Karte erweitern – mittlerweile eher ungewöhnlich für ein Oberklasse-Smartphone. Ober- und unterhalb des Displays – oder im Querformat gehalten seitlich – sitzen nach vorne abstrahlende Stereo-Lautsprecher, die für Smartphone-Verhältnisse angenehm laut und voll aufspielen. Während Telefonaten profitiert die Verständlichkeit davon, dass die Hörmuschel nicht in die Gehäusekante gequetscht oder unters Display verfrachtet wurde.

Das Betriebssystem belässt Sony relativ nah am Original, hier und da erweitert um praktische Features wie Side Sense: Doppeltippen am Displayrand öffnet eine Übersicht häufig genutzter Apps. Dort lassen sich auch App-Paare hinterlegen, die man gerne gleichzeitig öffnet – Platz genug bietet das langgezogene 21:9-Display. Auf Nachfrage teilte Sony mit, dass das Xperia 1 III zwei Jahre lang alle Sicherheitsupdates und Funktionsupgrades erhalten werde – bei einem Einführungspreis von

1300 Euro hätten wir deutlich mehr erwartet. Samsung beispielsweise beliefert neuerdings auch Einsteiger- und Mittelklasse-Smartphones vier Jahre lang mit Sicherheitspatches. Google und andere Hersteller wie OnePlus liefern diese in der Regel drei Jahre lang.

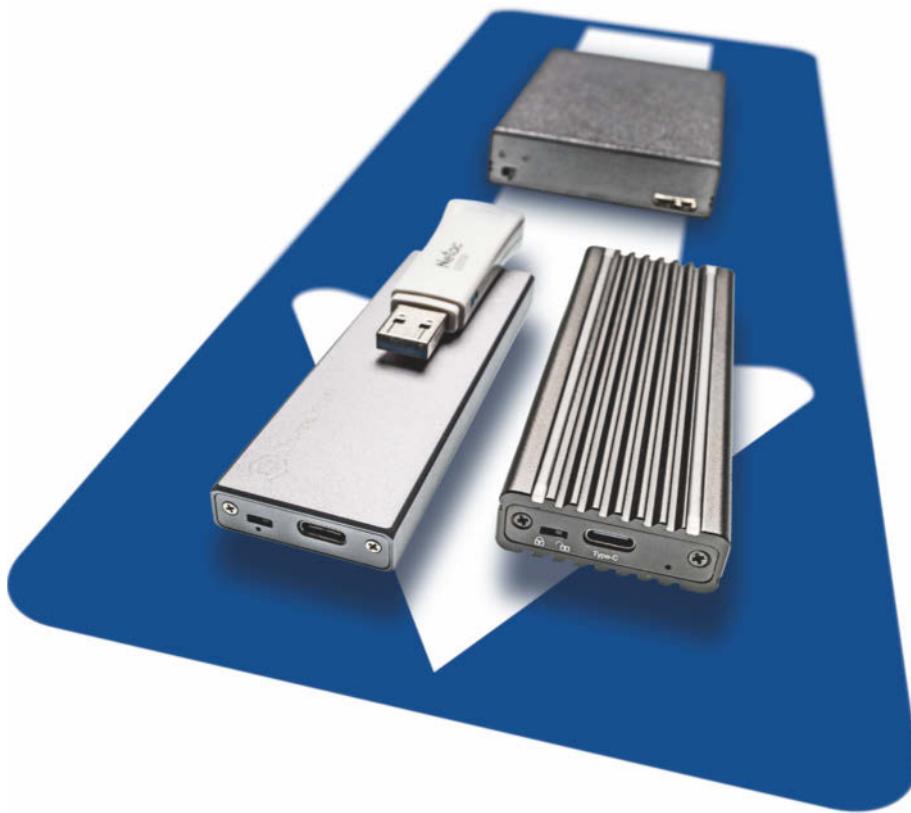
## Fazit

1300 Euro ruft Sony für das Xperia 1 III auf – damit muss es sich an den besten Android-Smartphones und Apples iPhones messen lassen. Das Samsung-Topmodell S21 Ultra ist ähnlich leistungsstark, läuft länger und ist in gleicher Speicherbaustellung mittlerweile günstiger. Muss es ein Snapdragon 888 sein, sind zum Beispiel OnePlus 9 Pro, Oppo Find X3 Pro oder Xiaomi Mi 11 400 bis 600 Euro günstigere Alternativen. Die iPhones glänzen mit dem längsten Software-Support, dem schnellsten Chip und ähnlich guter Kamera. Sony stellt mit dem Xperia 1 III ein Smartphone mit vielen Annehmlichkeiten wie Speicherkartenslot, Kopfhörerbuchse und besonders hochauflösendem OLED-Panel entgegen. Die Kamera setzt zwar keine Maßstäbe – aber dank der professionellen App macht das Fotografieren damit mehr Spaß als mit der Konkurrenz.

(rbr@ct.de) ct

## Sony Xperia 1 III

Android-Smartphone	
Betriebssystem / Security Level	Android 11 / April 2021
<b>Ausstattung</b>	
Prozessor / Kerne × Takt / GPU	Qualcomm Snapdragon 888 / 1 × 2,8 GHz, 3 × 2,4 GHz, 4 × 1,8 GHz / Adreno 660
RAM / Flash-Speicher / Kartenslot	12 GByte / 256 GByte (231 GByte) / ✓
5G (Band 1 / 28 / 77 / 78 / 260 / 261) / LTE / SIMs / SAR-Wert	✓ / ✓ / ✓ / ✓ / ✓ / - / - / ✓ / 2 × nanoSIM / 0,49 W/kg
WLAN (Antennen) / Bluetooth / NFC / Kompass / Standortbestimmung	Wi-Fi 6 (2) / 5.2 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo
USB-Anschluss / Kopfhöreranschluss	USB-C 3.1, OTG, DP / ✓
Akku / Ladezeit / Drahtlosladen	4500 mAh / 50 %: 28 min, 100 %: 114 min mit mitgeliefertem Netzteil / ✓
Abmessungen / Gewicht / Schutzklasse	16,5 cm × 7,1 cm × 0,8 - 1 cm / 186 g / ✓ (IP65/68)
<b>Display</b>	
Größe / Technik	6,5 Zoll (152 mm × 65 mm) / OLED
Auflösung / Helligkeitsregelbereich / Ausleuchtung	3840 × 1644 Pixel (644 dpi) / 2,88 ... 548 cd/m <sup>2</sup> / 97 %
<b>Kamera</b>	
Hauptkamera Auflösung / Blende / OIS / Brennweite (gemäß KB) / Sensorgröße	12 MP (4000 × 3000) / f/1,7 / ✓ / 24 mm / 1/1,7"
Telekamera Auflösung / Blende / OIS / Brennweite (gemäß KB) / Sensorgröße	12 MP (4000 × 3000) / f/2,3 + 2,8 / ✓ / 70 mm + 105 mm / 1/2,9"
Ultranawinkelkamera Auflösung / Blende / OIS / Brennweite (gemäß KB) / Sensorgröße	12 MP (4000 × 3000) / f/2,2 / - / 16 mm / 1/2,5"
Frontkamera Auflösung / Blende / OIS / Brennweite (gemäß KB) / Sensorgröße	8 MP (3264 × 2440) / f/2 / - / ca. 27 mm (78°) / 1/4"
<b>Laufzeiten, Benchmarks</b>	
Laufzeiten bei 200 cd/m <sup>2</sup> Helligkeit	13,7 h HD-Video / 6,9 h 4K/120fps-Video / 10,8 h 3D-Spiel / 12,5 h Stream
Coremark Single / Multi	22743 / 91530
Geekbench V4 Single, Multi / V5 Single, Multi	4878, 14105 / 816, 2804
3DMark Wild Life / Wild Life Extreme	5693 / 1512
Listenpreis	1299€
✓ vorhanden	– nicht vorhanden



# Sicherheitsgewinn

## USB-Sticks und USB-Gehäuse mit Schreibschutz

**Wer einen USB-Stick oder eine USB-SSD an einen fremden PC anschließt, kann sich einen Schädling einfangen. Legt man aber vorab einen Schreibschutzschalter um, braucht man davor keine Angst zu haben.**

Von Lutz Labs

Vor vielen Jahren galt die CD als das Medium der Wahl, um einen virenverseuchten PC zu säubern; schließlich kann kein Schädling den auf der Scheibe gespeicherten Daten etwas anhaben. CDs

und DVDs sind aber für heutige Verhältnisse viel zu langsam, auch gibt es immer weniger Rechner, die ein passendes Laufwerk haben.

Zum Start eines Rettungssystems und vor allem zum schnellen Transport von Daten haben sich USB-Sticks und – bei größerem Platzbedarf – USB-SSDs und -Festplatten etabliert – doch die lassen sich auch von einem Schädling beschreiben. Abhilfe schafft ein Schreibschutz, der auch vor versehentlichem Löschen schützt.

Die USB-SSD-Gehäuse und der USB-Stick, die wir für diesen Test ausgesucht haben, besitzen mechanische Schreibschutzschalter. Der USB-Stick U335 stammt von Netac und ist mit maximal 64 GByte Speicherplatz erhältlich. Bei den USB-Gehäusen bestimmt man die Kapazi-

tät durch den Einbau der passenden SSD selbst. Das gilt auch für Form und Geschwindigkeit der SSD: Von Raidsonic stammen das IB-256WP für 2,5-Zoll-Laufwerke und das IB-1824ML-C31 für eine PCIe-SSD im M.2-Format, von Silverstone haben wir das MS10 getestet, das eine M.2-SATA-SSD aufnimmt.

### Softwareschutz

Linux-Nutzer brauchen eigentlich keine Medien mit Schreibschutz, sie mounten USB-Laufwerke einfach read-only – zumindest, wenn sie einfach nur Dateien davon kopieren wollen. Beim Start eines Betriebssystems von einem Stick oder einer USB-SSD funktioniert das aber nicht.

Auch Windows-Nutzer können Laufwerke in einen Read-only-Modus versetzen. Das klappt mit dem Kommandozeilenprogramm Diskpart [1]. Doch dieser Befehl lässt sich erst ausführen, wenn das Laufwerk bereits angeschlossen ist und ein eventuell vorhandener Schädling damit bereits Zugriff darauf hat.

### Chips von Innostor und JMicron

Der Controller im USB-Stick stammt von Innostor, der IS918M unterstützt laut Datenblatt direkt einen Read-only-Modus. Einen solchen erwähnen die Datenblätter der JMicron-Chips aus den USB-Gehäusen nicht; wir haben in den drei Gehäusen insgesamt drei verschiedene Modelle gefunden: Das älteste Gehäuse für 2,5-Zoll-Laufwerke arbeitet mit dem JMS 578, das M.2-SATA-Modell mit dem JMS 580 und die moderne PCIe-Variante mit dem modernsten Chip, dem JMS 583. Die 58Xer Modelle arbeiten nach USB 3.1 Gen 2 mit 10 GBit/s, der ältere 578er schafft nur USB 3.1 Gen 1, also maximal 5 GBit/s.

In allen JMicron-Datenblättern ist die Rede von GPIO-Pins, die für kundenspezifische Anforderungen genutzt werden können, also etwa einen Schreibschutz. Dieser wird nach Unternehmensangaben auch von JMicron selbst umgesetzt, die Chips liefert JMicron dann bereits mit der angepassten Firmware an die Kunden aus.

Eine solche Firmware in Verbindung mit einem Hardware-Schalter stellt einen höheren Schutz vor Schädlingen dar als eine Software-Lösung. Dennoch: Auch eine Firmware ist eine Software und kann im Prinzip überwunden werden. Dazu müssten bösartige Hacker aber gezielt dieses Gerät attackieren, was sehr unwahrscheinlich ist.

## Test

Zum Test haben wir schnelle SSDs aus unserem Fundus in die Gehäuse eingebaut: eine Samsung 980 Pro ins PCIe-Gehäuse, eine Samsung 860 Evo ins M.2-SATA-Gehäuse und eine Crucial MX500 in das 2,5-Zoll-Gehäuse. Wir haben alle Modelle an den 10-GBit/s-Port unseres Test-Mainboards angeschlossen, einen schnelleren USB-Anschluss benötigt auch das PCIe-Gehäuse nicht.

Der USB-Stick hat den bei diesen Medien immer noch vorherrschenden A-Stecker, die beiden M.2-Gehäuse eine moderne USB-C-Buchse. Das 2,5-Zoll-Gehäuse verrät sein Alter über die mittlerweile unübliche breite USB-B-3.0-Buchse, die als unzuverlässig gilt – es ist seit fast vier Jahren erhältlich.

Die Geschwindigkeitsmessungen ergeben keine Überraschungen: Die PCIe-SSD war am schnellsten, M.2-SATA- und SATA-SSD in etwa gleich schnell, der USB-Stick am langsamsten. Wir haben in diesem Test nur die Spitzenwerte ermittelt, lang laufende Messungen würden Eigenschaften der Laufwerke, nicht aber der Gehäuse wiedergeben.

Laut Datenblatt unterstützen die beiden M.2-Gehäuse TRIM, aber im Test konnten wir dies nur beim IB-1824-C31 verifizieren. Das Utility Trimcheck (siehe ct.de/yakd) meldete auch beim älteren IB-256WP eine TRIM-Unterstützung, beim U335s erwartungsgemäß nicht.

Wer eine Samsung-SSD besitzt, kennt vielleicht das Samsung-Tool „Magician“ – und manche dürften sich schon gewundert haben, warum eine Samsung-SSD in einem externen Adapter mal als solche angezeigt wird, mal gar nicht. Das klappt nur, wenn die Firmware-Programmierer des USB-Adapters den Namen der SSD durchreichen; bei den Gehäusen in diesem Test war das der Fall. Wir haben zudem mit dem Samsung-Tool „Data Migration“ einen Klon des laufenden Windows erzeugt – auch dieses Samsung-Tool arbeitet nur mit einer hauseigenen SSD als Ziel.

## USB-Gehäuse und -Sticks

	seq. Transferraten schreiben/lesen <sup>1</sup> [MByte/s]	IOPS schreiben/schreiben/lesen <sup>2</sup>
	besser ▶	besser ▶
Netac U335S	35/120	750/4131
Icy Box IB-256WP	440/421	46582/52096
Icy Box IB-1824ML-C31	538/566	57866/91600
Silverstone MS10	1032/985	88653/103587

<sup>1</sup> gemessen mit IOMeter, Blockgröße 128 KByte

<sup>2</sup> gemessen mit IOMeter, Blockgröße 4 KByte, Messungen mit 8 GByte großer Datei

Mit den beiden M.2-SSDs im M.2-Slot auf dem Mainboard klappte danach auch der Betriebssystemstart, der Bootversuch mit der 2,5-Zoll-SSD endete in einer Endless-Bootschleife.

## Mal umschalten

Steckt man eine USB-SSD oder den Stick an einen USB-Port, ist er entweder schreibgeschützt oder nicht, je nach Stellung des Schiebeschalters. Ein Umschalten sollte man sich jedoch dann verkneifen, sondern lieber den Stick abziehen, den Modus wechseln und neu anstecken. Denn das Umschalten im eingesteckten Zustand ändert nicht unbedingt den Schreibschutzzustand. Silverstone, der Hersteller des MS10C, weist im Handbuch darauf hin, dass man zur Änderung des Schreibschutzmodus das Gehäuse vom PC abziehen soll.

Alle Gehäuse zeigten ein ähnliches Verhalten. Nachdem wir diese im angeschlossenen Zustand in den schreibgeschützten Zustand umgeschaltet hatten, konnten wir mindestens ein paar Sekunden lang Dateien darauf kopieren, die dann auch im Windows Explorer angezeigt wurden. An einem anderen PC angeschlossen waren auf der M.2-SATA-SSD dann aber nicht alle Dateien vorhanden.

Der umgekehrte Weg klappte, rein sicherheitstechnisch betrachtet, ordentlich: Schaltete man den Schreibschutz im eingesteckten Zustand ab, änderte sich der Zustand nicht; das Medium blieb schreibgeschützt.

Noch wunderlicher verhält sich der USB-Stick, wenn man seinen Schreibschutzschalter im laufenden Betrieb betätigt. Anfangs sieht es gut aus: Schiebt man den Schalter auf „offen“, schließt sich das zugehörige Explorer-Fenster und es öffnet sich ein neues; es scheint, als ob ein neues Laufwerk angesteckt wurde. Nun lassen sich Dateien auf den Stick kopieren – aber weder umbenennen noch löschen. Das klappt erst, nachdem man den Stick ab- und wieder angesteckt hat. Man muss



## Netac USB Flash Drive 3.0 U335S

Auf den ersten Blick ist der Netec U335S ein typischer USB-Stick in einem billig wirkenden Plastikgehäuse. Dieses lässt sich zudem mit den Fingernägeln auseinandernehmen, dabei fällt der Schreibschutzschieber heraus – für den regelmäßigen Einsatz empfehlen wir ein paar Tropfen Sekundenkleber oder Gewebeklebeband, um den Stick zusammenzuhalten.

Beim Lesen erreicht der U335S mit maximal 120 MByte/s noch erträgliche Werte, beim Schreiben größerer Dateien aber schafft er gerade einmal 35 MByte/s. Mit rund 4000 IOPS beim Lesen zufälliger Adressen ist er auch als Bootstick geeignet.

- ⬆ günstig
  - ⬇ fällt schnell auseinander
- Preis: 11 Euro

jedoch schon eine USB-Verlängerung oder einen Hub nutzen, um auf den Gedanken zu kommen, den Schalter im eingesteckten Zustand zu betätigen, denn dieser sitzt sehr dicht am USB-Stecker und lässt sich dort mit dem Fingernagel kaum erreichen.

Ein zufälliges und damit ungewolltes Umschalten ist auch bei den Gehäusen praktisch unmöglich: Der Schalter des 2,5-Zoll-Gehäuses lässt sich zwar mit dem Fingernagel betätigen, doch braucht man dazu schon etwas Konzentration. Für die beiden M.2-Gehäuse braucht man gar einen Kugelschreiber oder einen Schraubendreher, da die Schalter tief im Gehäuse sitzen.

Auf den ersten Blick erkennt man bei keinem Gehäuse, ob der Schreibschutz eingeschaltet ist oder nicht. Die beiden M.2-Gehäuse haben dafür zwar jeweils eine weiß-rote LED, doch die sitzt auf der Platine im Gehäuse und lässt sich durch das jeweils nur etwa 1 Millimeter große Loch nur schlecht erkennen. Beim



### Raidsonic Icy Box USB 3.0 Enclosure for 2.5" HDD/SSD IB-256WP

Das unter der Bezeichnung IB-256WP einfacher aufzufindende externe Gehäuse wirkt mit seiner breiten USB-3.0-Buchse veraltet. Dafür ist es das einzige in diesem Vergleich, das auch eine Festplatte aufnimmt. Die darf sogar bis zu 15 Millimeter hoch sein, damit lassen sich also Festplatten bis 5 TByte einbauen.

Die Übertragungsleistung entspricht dem USB-3.0-Standard: Mehr als 440 MByte/s sind nicht drin, und das auch nur mit einer flotten SATA-SSD; eine Festplatte schafft maximal 120 MByte/s.

günstig  
 alter USB-3.0-Anschluss  
Preis: circa 14 Euro



### Raidsonic Icy Box USB Typ-C Enclosure for M.2 NVMe SSD IB-1824ML-C31

Das schnellste Gehäuse im Test arbeitet mit einer PCIe-SSD, bremst diese jedoch durch die Schnittstelle auf rund 1 GByte/s aus. Zum Starten eines Betriebssystems ist das Gehäuse ausreichend schnell, mit der 980 Pro kamen wir auf mehr als 64.000 IOPS beim Lesen.

Durchsichtige Kunststoffstreifen auf der Oberseite des Gehäuses werden von der Platine in einem RGB-Muster beleuchtet, die Beleuchtung lässt sich jedoch nicht in ein RGB-Setup einbinden.

sehr schnell  
 teuer  
Preis: circa 40 Euro



### Silverstone MS10

M.2-SSDs mit SATA-Interface sind ebenso schnell wie ihre Verwandten im 2,5-Zoll-Gehäuse und mit bis zu 2 TByte erhältlich. Im Silverstone MS10 erreichten wir mit einer Samsung 860 Evo maximal 560 MByte/s und rund 56.000 IOPS, lediglich bei den Zugriffen auf zufällige Adressen schränkt das Gehäuse also die Leistung der SSD ein.

Der Hersteller weist ausdrücklich darauf hin, dass PCIe-SSDs nicht unterstützt werden. Wie beim IB1824ML-C31 passen M.2-SSDs in den Formaten 2242, 2260 und 2280 hinein.

nutzt M.2-SATA-SSD aus  
 klein und handlich  
Preis: circa 24 Euro

PCIe-Gehäuse überstrahlt zudem die RGB-Beleuchtung alles.

### Fazit

Die Schreibschutz-Gehäuse sind teurer als USB-Gehäuse ohne Schreibschutz, auch die Auswahl ist nur klein. Dennoch: Wer

gerade auf der Suche nach einem passenden Gehäuse für eine vorhandene SSD ist, kann mit ein paar Euro Aufpreis eine geschützte Umgebung für seine Daten oder einen Betriebssystemstart schaffen.

Der USB-Stick U335S kostet mit 64 GByte Speicher zwar weniger als die leeren

Gehäuse, ist dafür aber auch am langsamsten. Das mit rund 14 Euro immer noch sehr günstige IB-256WP könnte viele Anwender interessieren, da die meisten ausrangierten SSDs wohl im 2,5-Zoll-Format vorliegen. Schlanker, aber auch teurer, ist das MS10 für M.2-SATA-SSDs. Greift man zum IB-1824ML-C31 und einer PCIe-SSD, hat man nicht nur die teuerste, sondern auch die schnellste Lösung. Man sollte sich jedoch angewöhnen, die Schreibschutzschalter nur im ausgesteckten Zustand zu betätigen, um ungewolltem Verhalten vorzubeugen. Dann aber braucht man vor einem Virenbefall an fremden Rechnern keine Angst mehr zu haben.

(ll@ct.de)

## USB-Speichermedien und -Gehäuse mit Schreibschutz

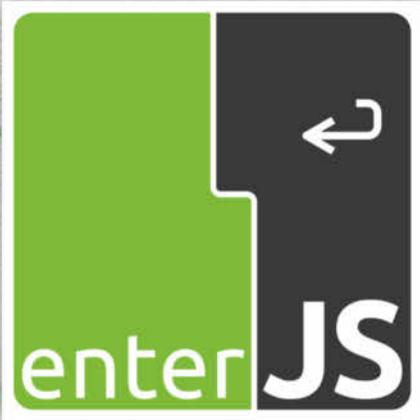
Modell	USB Flash Drive 3.0	USB 3.0 Enclosure for 2.5" HDD/SSD	USB Typ-C Enclosure for M.2 NVMe SSD	MS10
Hersteller, URL	Netac, netac.com	Raidsonic, icybox.de	Raidsonic, icybox.de	Silverstone, silverstonetek.com
Bezeichnung	U335S	IB-256WP	IB-1824ML-C31	SST-MS10C
Typ	USB-Stick	USB-Gehäuse für 2,5"-Medien	USB-Gehäuse für PCIe-SSDs	USB-Gehäuse für M.2-SATA-SSDs
Anschluss	USB-A	USB-B 3.0	USB-C	USB-C
USB-Typ	3.2 Gen 1	3.2 Gen 1	3.2 Gen 2	3.2 Gen 2
Kabel	–	USB-A, 30 cm	USB-A, 30 cm; USB-C, 30 cm	USB-C, 30 cm
Maße	69 mm × 22 mm × 12	113 mm × 77 mm × 21 mm	103 mm × 35 mm × 11 mm	104 mm × 35 mm × 11 mm
Gewicht <sup>1</sup>	8 g	144 g	67 g	103 g
Straßenpreis	11 €	14 €	40 €	24 €

<sup>1</sup> mit SSD

### Literatur

- [1] Lutz Labs, Schreibschutz für Festplatte, c't 6/2019, S. 162
- [2] Kamil Artur Nowak, Schutz per Schalter, c't 15/2016, S. 58

Download Trimcheck: [ct.de/yakd](http://ct.de/yakd)



# Die Konferenz für Enterprise-JavaScript

**29. - 30. September 2021 - Online**

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

Jetzt  
Tickets zum  
**Frühbucher-  
Rabatt**  
sichern!

Veranstalter



MAGAZIN FÜR PROFESSIONELLE  
INFORMATIONSTECHNIK

heise Developer

© Copyright by Heise Medien.

dpunkt.verlag

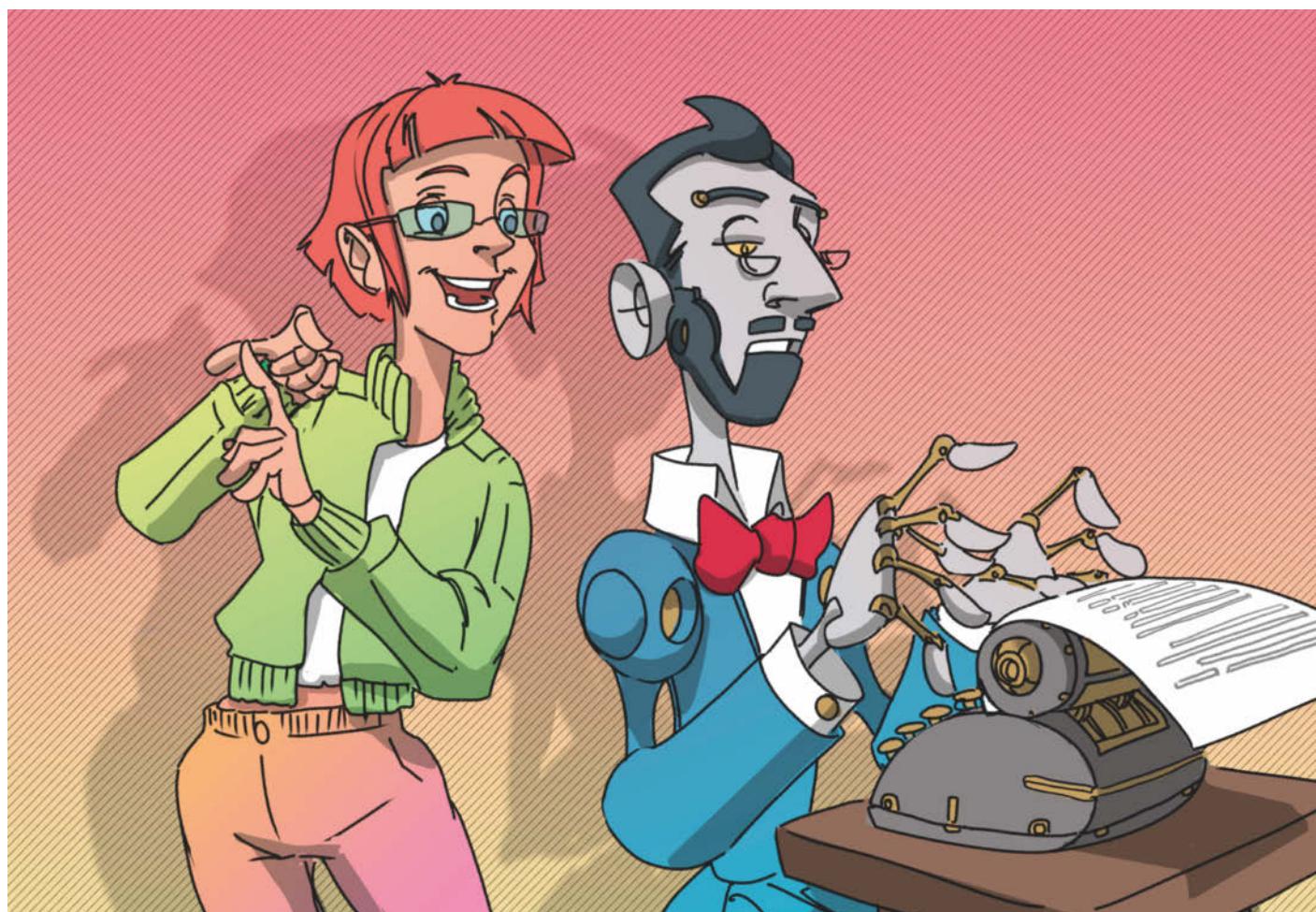


Bild: Thorsten Hübner

# Diktatmaschinen

## Transkriptionsdienste: Audioaufnahmen in Text wandeln

**Webdienste mit künstlicher Intelligenz erkennen deutsche und englische Rede ohne aufwendiges Training. Das erspart, in Vorlesungen, Interviews und ähnlichen Situationen live mitzuschreiben und schafft den Freiraum, sich ganz auf den Vortrag oder das Gespräch zu konzentrieren.**

Von André Kramer

**T**ranskriptionsdienste wandeln gesprochene Alltagssprache in lesbaren Text. Mit Methoden maschinellen Lernens funktioniert das mittlerweile sprecherunabhängig, das heißt ohne vorheriges Training. Das bietet deutlich mehr Freiheit als der frühere Ansatz, bei dem die eingerichtete Software fest an einen Sprecher gebunden war und somit ausschließlich als persönliche Diktatsoftware diente.

Auf YouTube erscheinen bei jedem Video automatisch generierte Untertitel, die zwar gerade in Beiträgen mit vielen exotischen Fachbegriffen nicht immer akkurat sind, aber durchaus gut genug, um den Inhalt wiederzugeben. Sie helfen ge-

hörlosen Zuschauern, aber auch solchen die gerade Kartoffelchips oder eine laute elektrische Zahnbürste im Mund haben.

Webdienste zur Audiotranskription sind für alle hilfreich, die regelmäßig Interviews oder Redebeiträge verschriftlichen. Die Vision der Hersteller: Man hat immer den Audio-Recorder auf dem Smartphone bereit, schickt die Aufnahme im WAV- oder MP3-Format durch die KI auf den Server des Dienstes der Wahl und lädt sich nach kurzer Wartezeit den lupenrein lesbaren Text herunter.

Verglichen mit digitalen Assistenten sollen sie besser mit komplexen Themen zureckkommen. Siri und Alexa geht es da

ehler wie jemandem mit Fremdsprachenkenntnissen aus der Schule: Für Standardsituationen reicht es, aber bei freier Rede ist schnell der Ofen aus.

Sechs Webdienste versprechen deutschsprachige Audioaufnahmen zuverlässig in editierbaren Text zu verarbeiten: Amberscript, Audext, f4x, HappyScribe, Trint und Wreally transcribe.

## Transkriptionsdienste in der Praxis

Dank künstlicher Intelligenz können Neulinge schnell in die Webdienste einsteigen und auch Redebeiträge von weiteren Personen wie Interviewten schnell und unkompliziert verschriftlichen. Auf den Webseiten der Anbieter kann man Audio- oder Video-Dateien direkt von der Festplatte hochladen. Einige unterstützen Dienste wie Google Drive, Dropbox und Microsoft OneDrive oder nehmen YouTube-Links entgegen. Die Anbieter unterstützen Standardformate wie MP3 und WAV beziehungsweise MP4 und MOV. Nach wenigen Minuten stellen sie den Text wahlweise als TXT-, DOCX-, RTF- oder PDF-Dokument zum Download bereit. Amberscript, HappyScribe und Trint, die offenbar dieselbe zugrundeliegende Technik nutzen, bieten auch das Untertitelformat SRT an, eine Textdatei mit Timecodes. HappyScribe und Trint können außerdem automatisch übersetzen. Ins Englische übertragen wirken die Texte passabel übersetzt.

Einige Transkriptionsdienste schreiben nicht nur selbst auf, sondern unterstützen auch beim Niederschreiben und bei der Korrektur, indem sie eine Textverarbeitung mit einem Audioplayer verbinden. So korrigiert man den automatisch ermittelten Text gleich in der Software. Eine Reihe Tastenkürzel vereinfacht den Prozess, indem man pausiert oder einige Sekunden zurückspringt, um eine Passage erneut zu hören. Alternativ kann man USB-Pedale nutzen, um die Hände zum Tippen frei zu haben. Geeignete Fußschalter gibt es für 30 bis 100 Euro. Bei der Korrektur hilft außerdem eine Funktion, die Aufnahme schneller oder langsamer abzuspielen.

Wir haben anhand eines eingesprochenen Beispieltextes mit verschiedenen Passagen die Erkennungsrate der Dienste überprüft und dabei nicht nur die Fehler gezählt, sondern auch die Zeichensetzung in Betracht gezogen. Bei der Korrektur hilft es außerdem, wenn die Dienste Absätze einfügen.

## Akustik, Lexikon und Sprachmodell

Automatische Spracherkennung arbeitet mit statistischen Modellen in drei Stufen: einem akustischen Modell, einem Lexikon und einem Sprachmodell. Im ersten Schritt wird das kontinuierliche Audiosignal in wenige Zehntelsekunden lange Abschnitte segmentiert und in einzelne Laute zerlegt. Akustische Wortgrenzen gibt es nicht. Das akustische Signal enthält keine Pausen, sehr wohl aber unterschiedliche Längen. Das gleichmäßig segmentierte akustische Signal würde direkt übertragen mal wie „Hallo“ und mal wie „Haaaalloooo“ aussehen. Sogenannte Hidden-Markov-Modelle enthalten Wahrscheinlichkeitswerte für den Verbleib bei einem Laut und den Übergang zum folgenden Laut. Sie modellieren das Signal so, dass jeder Laut nur einmal auftritt.

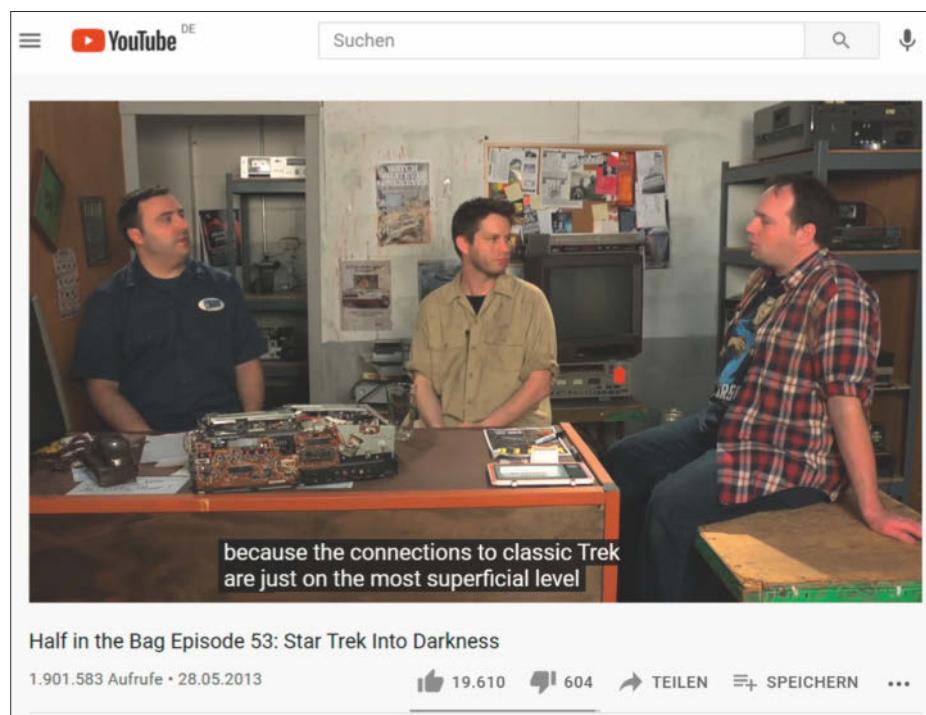
Die deutsche Sprache besteht aus etwa 40 Lauten, den sogenannten Phonemen. Sie lassen sich nicht wie Buchstaben isolieren, denn die jeweils vorherigen und nachfolgenden Laute klingen mit. Entsprechend groß ist das Lautrepertoire. Über die 26 Buchstaben des Alphabets hinaus zählen die Buchstaben ä, ö, ü und Kombinationen wie sch zu den geschriebenen Graphemen. Einem Phonem können unterschiedliche Grapheme zugeordnet sein, wie umgekehrt verschiedene Phoneme

durch dasselbe Graphem abgebildet sind, beispielsweise das lange oder das kurze O, das scharfe oder das weiche S.

Das Lexikonmodell formt aus den identifizierten Lauten Wörter. Sprachverständen hängt nicht nur beim Menschen, sondern auch beim Computer davon ab, ob das Wort bereits bekannt ist. Daher fällt es den Maschinen schwer, beispielsweise Abkürzungen korrekt zu erkennen, wenn diese nicht im Lexikon stehen. Dabei geht es nicht um eine zwanzigjährige Buchsammlung, sondern um ein Verzeichnis, auf das die Software zugreift. Bei einigen Diensten lässt sich das Lexikon manuell ergänzen.

Schließlich baut die Software anhand eines Sprachmodells einen Satz. Dabei nutzt sie Trigrammstatistiken. In strukturierten Texten kann sich die Software anhand von häufig auftretenden Dreiwortfolgen von einem Wort zum anderen hängeln. Auf diese Weise generiert beispielsweise auch ein Smartphone zumindest grammatisch brauchbare Texte, wenn man oberhalb der Tastatur immer den mittleren Wortvorschlag antippt.

Für Diktatprogramme reichen Trigrammstatistiken. Gesprochene Sprache ist jedoch durchsetzt von abgebrochenen Sätzen und Füllseln wie „äh“, „irgendwie“ und „genau“. Das stellt statistisch basierte Software vor Probleme, denn Diktatprogramme



Eine beliebte Anwendung für speicherunabhängige Audiotranskription sind automatische Untertitel wie auf YouTube.



## Amberscript

Das Dashboard von Amberscript zeigt eine große Schaltfläche zum Hochladen von Dateien, darunter eine Liste aller bisher verarbeiteter Aufnahmen und ganz unten das verfügbare Transkriptionsguthaben. Wenn sich letzteres dem Ende nähert, kann man für 20 Euro eine Stunde hinzufügen. Für knapp zwei Euro pro Audiominute kann man den Anbieter auch mit der Transkription durch menschliche Schreibkräfte beauftragen. Alle Rechnungen lassen sich im Dashboard einsehen.

Ein Klick auf ein sogenanntes Amber (deutsch: Bernstein) öffnet einen Editor mit einer Wellenformanzeige der Audiodatei und dem Transkript darunter. Ein Klick auf Play spielt die Aufnahme ab und führt simultan durch den Editor, wo sich der erkannte Text korrigieren lässt. Mit Tastenkürzeln kann man den Player stoppen oder 5 Sekunden zurückspringen. Amberscript bietet eine deutschsprachige Rechtschreibkorrektur und ein Werkzeug, um Textpassagen zu korrigieren. Änderungen speichert das Programm automatisch. Allerdings wirkt der Editor etwas behäbig.

Alltagssprache erkennt Amberscript sehr gut und setzt auch Komposita wie „Transaktionskosten“ weitgehend korrekt zusammen, tut sich aber schwer mit Fachbegriffen, Abkürzungen und Sonderfällen wie Domänenamen. Zahlen schreibt der Dienst als einzelne Wörter aus: 13,5 beispielsweise als „drei und zehn komma fünf“. Der fertige Text glänzt durch tadellose Zeichensetzung, kommt aber in einem einzigen langen Absatz.

- ⬆ gute Texterkennung
- ⬆ einfach zu bedienender Editor
- Preis: 20 Euro pro Stunde



## Audext

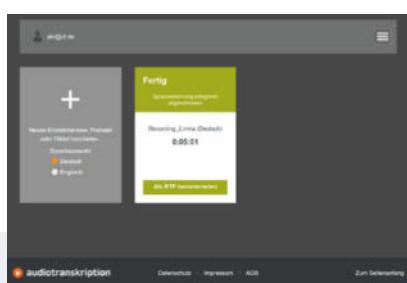
Audext zeigt vorhandene Transkripte, verbleibende Minuten und unterstützte Sprachen in einer übersichtlichen, deutschsprachigen Oberfläche. Mit einem Schieberegler kann man beim Erwerb den Umfang des Guthabens variieren. Er steht bei 60 US-Dollar für insgesamt 5 Stunden und lässt sich erhöhen oder verringern. Je größer das Kontingent, desto höher der Rabatt. Zweites Modell: Mit 30 US-Dollar monatlicher Grundgebühr kostet eine Stunde 5 US-Dollar.

Bei näherem Hinsehen zeigen sich einige Unsauberkeiten bei der Übersetzung der Oberfläche: „Name des Plans: Free“ geht noch als Denglisch durch. „one-time purchase“ und „with subscription“ haben die Entwickler wohl vergessen zu übersetzen.

Der Editor zeigt einen Timecode für jedes Satzfragment. Jede Äußerung kann man einem Sprecher zuordnen. Neben Abspielen und Stoppen, Vor- und Rückspulen um jeweils zehn Sekunden kann man die Wiedergabegeschwindigkeit von 0,25-fach bis zweifach variieren. Wiederkehrende Fehler lassen sich durch Suchen und Ersetzen korrigieren.

Das Ergebnis ist passabel. Audext unterlaufen jedoch die meisten Fehler im Test: Tweed statt Tweet, Elon Mass statt Elon Musk, Derby statt Adobe, All Pet statt iPad, Patrice statt Porträts. Außerdem zerhackt der Dienst Komposita in Einzelwörter (Pinsel Spalten). Auch die Zeichensetzung ist stark fehlerbehaftet. Das Transkript mit Timecodes enthält eine Menge nicht nachvollziehbarer Absätze.

- ⬆ günstiger Preis
- ⬇ hohe Fehlerrate
- Preis: 12 US-Dollar pro Stunde



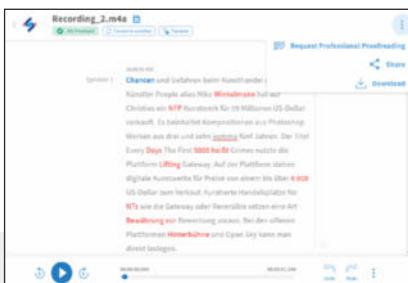
## f4x

Der Hersteller von f4x, dr. dresing & pehl, kooperiert mit dem Fraunhofer IAIS, das auch Videoinhalte für den WDR transkribiert, um diese durchsuchbar zu machen. Der Hersteller wirbt damit, die Inhalte in Deutschland DSGVO-konform zu verarbeiten. Er ist außerdem per Telefon in deutscher Sprache zu erreichen. Die Software gibt es für Windows, macOS und Linux erfrischenderweise als dauerhaft nutzbare Lizenz oder optional im Abo mit 6 Monaten beziehungsweise 2 Jahren Laufzeit.

Der Fokus liegt auf wissenschaftlicher Nutzung. So bietet der Hersteller neben der Spracherkennung in f4transkript auch das statistische Interviewanalysetool f4analyse an. Die in dunklem Grau gehaltene Oberfläche von f4x zeigt ein großes Plus für Hochladen von Dateien und darunter die Sprachauswahl in Deutsch und Englisch. Nach wenigen Minuten kann man das fertige Transkript als RTF-Datei herunterladen. Einen Editor bietet der Dienst nicht, alternative Exportformate auch nicht, was aber nicht weh tut.

Im Großen und Ganzen bietet f4x die beste Erkennungsleistung im Test, kann auch schwierige Begriffe wie „iPad“, „Tweet“ und „Porträt“ korrekt wiedergeben. Die untereinander identischen Ergebnisse von Amberscript, transcribe und Trint weisen auf Wortebene zwar noch etwas weniger Fehler auf, haben aber größere Schwierigkeiten bei der Zeichensetzung. Der Text von f4x kommt nahezu fehlerfrei mit sehr guter Kommasetzung und sinnvoll gesetzten Absätzen.

- ⬆ gute Erkennung incl. Satzzeichen
- ⬆ einfacher Kontakt zum Hersteller
- Preis: 63,65 Euro für 5 Stunden



## Happyscribe

Die Oberfläche von Happyscribe muss sich im Look-and-Feel nicht hinter anderen erfolgreichen Webdiensten verstecken. Statt mit Funktionen zu überfrachten, die man eh erst später in der Textverarbeitung verwendet, zeigt er nur einen Player, Rückgängig und Wiederherstellen sowie Schaltflächen, um vor- und zurückzuspringen. Unklare Begriffe und Dopplungen markiert der Dienst rot. Gegen eine Gebühr kann man professionelle Korrekturleser beauftragen und den Text auf Wunsch über einen Web-Link weitergeben.

Ein Alleinstellungsmerkmal ist der Untertitleditor, der den Text anhand einer Zeitleiste in Untertitel segmentiert und diese in einem Vorschaufenster anzeigt. Die Untertitel exportiert der Dienst unter anderem im gängigen SRT-Format. Außerdem kann man seinen Text automatisch übersetzen lassen – mit passablem Ergebnis.

Die Erkennungsrate ist im Prinzip gut. Die KI neigt dazu, Zahlen in der Form „neun tausend neun hundert neun und neunzig“ auszuschreiben. Außerdem hat sie Schwierigkeiten mit zusammengesetzten Wörtern (Komposita), schreibt beispielsweise „Bilder, Alben“ statt „Bilderablen“, und englischsprachigen Fremdwörtern. Happyscribe gehört mit Amberscript und Trint zu den drei Diensten mit identischem Resultat bei der Audiotranskription, setzt im Unterschied zu diesen aber sinnvolle Absätze und gliedert so den Text. Außerdem ist Happyscribe günstiger als die zuvor genannten.

- ⬆ gute Texterkennung
  - ⬆ günstiger Preis
- Preis: 12 Euro pro Stunde



## Trint

Anders als die übrigen Kandidaten bietet Trint keinen kostenlosen Testzeitraum ohne Haken an: Bevor man den Dienst sieben Tage lang ausprobieren kann, muss man sich mit einer gültigen Kreditkarte anmelden, diese verifizieren und ein Abo abschließen. Das kann man zwar innerhalb der sieben Tage ohne Zahlung kündigen; diese Praxis ist allerdings nahezu einzigartig in der Softwarewelt. Wer den Dienst pausieren möchte, zahlt 5 Euro monatlich. Sonst werden alle Daten gelöscht. Auf Anfragen reagierte der Hersteller nicht. Trint setzt offenbar auf Großkunden. Der Dienst wendet sich an Journalisten und bietet neben Transkription auch automatische Übersetzung an.

Die Oberfläche der Webseite ist ausschließlich in Englisch gehalten, der Dienst selbst erkennt aber auch Aufnahmen in anderen Sprachen. Im Editor kann man Textpassagen markieren, kommentieren, übersetzen lassen, die Aufnahme abspielen und dabei die Geschwindigkeit variieren.

Die Technik ist auch hier offenbar eingekauft: Das Ergebnis ist identisch mit dem von Amberscript und Happyscribe. Die Erkennungsleistung ist recht gut, allerdings tut sich der Dienst schwer mit Zahlen; der Text erscheint ohne Absätze. Neuere Begriffe wie Blockchain, iPad und „Elon Musk“ erkennt er tadellos. Trint eignet sich eher für Unternehmen und Vielnutzer. Das günstigste Abo kostet bei monatlicher Kündigung 55 Euro im Monat und erlaubt die Transkription von maximal sieben Dateien.

- ⬆ gute Texterkennung
  - ⬇ aggressive Abopolitik
- Preis: ab 55 Euro pro Monat



## Wreally transcribe

In einer vergleichsweise spröden und ausschließlich auf Englisch verfügbaren Oberfläche zeigt transcribe von Wreally die verarbeiteten Audioaufnahmen. Oben wählt man, ob man eine automatische Transkription wünscht oder mit dem integrierten Medienplayer des Webdienstes manuell niederschreiben möchte. Als einziger Dienst im Test bietet Wreally transcribe einen Audio-Recorder. Beim Upload kann man die Audiodatei beschneiden, Timecodes einfügen, das Wörterbuch ergänzen und auf Wunsch ein Untertitelformat wählen. Wie die übrigen Dienste auch zeigt transcribe die verfügbaren Restminuten und die Restdauer des Abos an.

Beim Aufruf einer Datei zeigt der Dienst zunächst eine Vorschau des erkannten Textes. Den Editor muss man separat aufrufen. Statt Werkzeugen zum Überprüfen des Transkripts wie einen Schiebereglern für variable Geschwindigkeit bietet er vergleichsweise uninspirierte Formatoptionen wie fett, kursiv und unterstrichen sowie sortierte und unsortierte Listen. Für die Nacharbeit wechselt man besser nach Microsoft Word oder LibreOffice.

Wreally transcribe lieferte die beste Erkennungsrate im Test. Der Dienst kann mit Zahlen wie „18,5 Millionen“ umgehen, gibt auch Wörter wie „Architekturaufnahmen“ und „Desktop-Version“ korrekt wieder und erkennt Eigennamen wie „Elon Musk“. Auch Absätze und Zeichensetzung stellen zufrieden, und das alles zu einem günstigen Preis.

- ⬆ exzellente Erkennungsrate
  - ⬇ uninspirierter Editor
- Preis: 20 US-Dollar pro Jahr und 6 US-Dollar pro Stunde

sind anhand von Tageszeitungen trainiert. Das merkt man wiederum der Worterkennung im Smartphone an, die „Die Zeit“ und „Die Welt“ immer mit großem Artikel schreiben möchte – sie kennt von Haus aus eben vor allem Zeitungsartikel. Jedes aus Unsicherheit eingefügte „genau“ lässt die

Trigrammkette abbrechen und bringt die Software aus dem Konzept.

Neuronale Netze ersetzen mittlerweile die einfachen statistischen Modelle, arbeiten aber mit denselben statistischen Daten. Durch sie lässt sich das akustische Modell viel robuster einsetzen, also für

mehrere Sprecher, bei Akzenten oder bei Hintergrundgeräuschen. Bei Satzabbrüchen und Interjektionen wie „äh“ oder „irgendwie“ kann ein neuronales Sprachmodell über Trigramme hinausweisen und ganze Sätze, Absätze oder gar Artikel bei der Sprachmodellierung berücksichtigen.

## Audiotranskriptionsdienste

Produkt	Amberscript	Audext	f4x	happyscribe	Trint	Transcribe
Hersteller	Amberscript	Audext	dr. dresing & pehl	Happy Scribe	Trint	Wreally
URL	amberscript.com/de	audext.com/de	audiotranskription.de	happyscribe.com	trint.com	transcribe.wreally.com
Systemanf.	Webbrowser	Webbrowser	Windows ab 7, macOS ab 10.12, Linux oder Webbrowser	Webbrowser	Webbrowser	Webbrowser
Sprache (Bedienoberfläche)	Deutsch	Deutsch	Deutsch	Englisch	Englisch	Englisch
<b>Audiotranskription</b>						
Sprachen (Transkription)	Deutsch, Englisch (39 Sprachen)	Deutsch, Englisch (ca. 60 Sprachen)	Deutsch, Englisch	Deutsch, Englisch (über 120 Sprachen)	Deutsch, Englisch (32 Sprachen)	Deutsch, Englisch (ca. 60 Sprachen)
Sprachauswahl	automatisch	manuell	manuell	manuell	manuell	manuell
Cloud-Upload	–	über Google Drive	–	über Dropbox, Google Drive	über Box, Dropbox, Google Drive, Amazon Cloud und Microsoft OneDrive	–
Formate: Audio	AAC, FLAC, M4A, MP3, OPUS, WAV, WMA	AIF, M4A, MP3, Ogg Vorbis, WAV, WMA u.a.	AIFF, M4A, MP3, WAV	AAC, AIFF, FLAC, M4A, MP3, Ogg Vorbis, WAV, WMA u.a.	AAC, M4A, MP3, WAV, WMA	AAC, AIFF, FLAC, M4A, MP3, Ogg Vorbis, WAV, WMA u.a.
Formate: Video	M4V, MOV, MPEG-2, MP4	AVI, MOV, MP4, WMV	–	3GP, AVI, FLV, M4V, MOV, MP4, MPEG-2, VOB u.a.	AVI, MOV, MP4	3GP, MOV, MP4, WMV
Max. Dateigröße	bis zu 4 GByte	bis zu 200 MByte	k. A.	k. A.	k. A.	k.A.
audiorecorder	–	–	–	–	–	✓ (Live-Diktat im Editor)
Standardexportformate	DOCX, TXT	DOCX, TXT	RTF	DOCX, HTML, JSON, PDF, TXT, XML u.a.	DOCX, TXT, HTML, XML, CSV	DOC
Untertitelformate	SRT	–	–	SRT, STL, VTT	EDL, SRT, STL, VTT	–
weitere Funktionen	Auftrag zu manueller Abschrift (1,90€ pro Minute)	Transkripte über Link teilen	Auftrag zu manueller Abschrift, Sprachanalyse	Auftrag zu manueller Abschrift (2,80€ pro Minute), automatische Übersetzung	automatische Übersetzung	–
<b>Editor</b>						
integrierter Editor	✓	✓	–	✓ (und Untertitel-Tool)	✓	✓
Zeitmarken setzen	✓	–	–	✓	✓	✓
Text farbig markieren	✓	–	–	✓ (und Kommentare)	✓ (und Kommentare)	– (fett, kursiv, unterstrichen)
verlangsamt, beschleunigt abspielen	✓ (Schieberegler)	✓ (0,25x – 2x)	–	✓ (0,2x – 2x)	✓ (0,2x – 2x)	✓ (F1, F2)
Abspielen: Pause / Vor / Zurück	✓ (Strg+Leertaste) / – / ✓ (Strg+R)	✓ (Tabulator) / ✓ / ✓	– / – / –	✓ (Tabulator) / ✓ (Strg+Leertaste) / ✓ (Alt+Tab) / ✓ (Umschalt+Tab)	✓ (Esc) / ✓ (F3) / ✓ (F4)	✓ (Esc) / ✓ (F3) / ✓ (F4)
Suchen und Ersetzen	✓	✓	–	✓	✓	–
Rechtschreibprüfung	✓	–	–	–	–	–
<b>Abrechnung</b>						
kostenloses Testangebot	✓ (bis 30 Min.)	✓ (bis 30 Min.)	✓ (bis 30 Min.)	✓ (bis 30 Min.)	✓ (7 Tage, nur mit Kreditkarte und Abo)	✓ (7 Tage, max. 1 Min.)
Art der Abrechnung	stundenweise oder 5 Std. monatlich im Abo für 56 €	stundenweise oder 2 Stunden monatlich im Abo für 45 US-\$, jede weitere für 5 US-\$	5 Std. für 63,65 €, variable Preise je nach Kontingent sowie für Studierende oder Institutionen	1 Stunde für 12 €, minutengenau ohne Abo (20 Cent pro Minute)	7 Dateien pro Monat für 55 € monatl., unlimitiert für 65 € monatl.	20 US-\$ pro Jahr plus 6 US-\$ pro Stunde, keine autom. Verlängerung
Rechnung zum Download	✓	–	–	–	✓	–
Konto pausieren	kostenfrei	kostenfrei	kostenfrei	kostenfrei	5 € pro Monat	kostenfrei
<b>Erkennungsleistung</b>						
Transkriptionsdauer (5 Min. Audio)	2 Minuten	5 Minuten	3 Minuten	4 Minuten	3 Minuten	2 Minuten
Fehlerquote bei 630 Wörtern	37	69	35	37	37	30
<b>Bewertung</b>						
Funktionsumfang	⊕	○	○	⊕⊕	⊕	⊖
Texteditor	⊕⊕	⊖	⊖⊖	⊕	⊕⊕	⊖
Texterkennung	⊕	⊖	⊕⊕	⊕	⊕	⊕⊕
Textformatierung	○	⊖	⊕	⊕⊕	○	⊖
Preisgestaltung	⊕	⊕⊕	⊕	⊕⊕	⊖⊖	○
Preis	20 € pro Stunde	12 US-\$ pro Stunde	63,65 € für 5 Stunden	12 € pro Stunde	ab 55 € pro Monat	20 US-\$ pro Jahr und 6 US-\$ pro Stunde
⊕⊕ sehr gut	⊕ gut	○ zufriedenstellend	⊖ schlecht	⊖⊖ sehr schlecht	✓ vorhanden	– nicht vorhanden
k. A. keine Angabe						

## Fazit

Bei den Erkennungsraten der Programme kann man eigentlich kaum meckern. Das Schlusslicht bildet Audext. Die übrigen Dienste liegen bei der Anzahl der Fehler mehr oder minder gleichauf. Die Form unterscheidet sich: HappyScribe und Wreally transcribe liefern lesbare und gut strukturierte Texte ab. Auch f4x gliedert den Text in sinnvolle Abschnitte. Bei Amberscript und Trint erscheint ein einzelner langer Absatz, bei Audext ein völlig zerhackter Text.

Die Preisgestaltung ist in der Regel fair und transparent mit stundenweisen Kontingenzen. Aufgrund der hohen Preise eignen sich f4x und Trint eher für Vielnutzer, die übrigen auch für Gelegenheitsanwender. Trint bietet als einziger Dienst keine Testphase ohne Angabe von Kreditkartendaten und Abschluss eines Abos. Die übrigen Dienste kann man sorgenfrei ausprobieren.

Alle Kritik an den Transkriptionsdiensten ist Jammern auf hohem Niveau,

## Spracherkennung in Diktiersoftware

Den Durchbruch erreichte automatische Spracherkennung in den Neunzigerjahren. Damals mussten Programme wie IBM ViaVoice aufwendig eingerichtet werden, indem man der Software etwa eine halbe Stunde lang Texte vorlas, anhand derer sie sich auf Aussprache und Sprachmelodie einstellte. Anschließend ließ sich das Programm nur von der Person einsetzen, die das Training absolviert hatte.

Mittlerweile dominiert das Programm Dragon den Markt der Diktiersysteme. Es arbeitet lokal und ist vor allem in den Berufsfeldern Jura, Medizin und Geschäftsführung verbreitet. Es kostet in

der Erstschaftung mehr als ein Webdienst und eignet sich vor allem für tägliche Diktate durch eine einzelne Person.

Die Erkennung funktioniert mittlerweile ohne aufwendige Einrichtung, wird mit Training aber noch etwas besser. Der Hersteller Nuance empfiehlt, die Software nicht für Interviewsituationen mit mehreren Sprechern zu nutzen, denn sie verunreinigen das Sprecherprofil. Grundsätzlich ließe sich Dragon aber auch für Interviews einsetzen. Nuance wurde vor kurzem von Microsoft übernommen. Dragon dürfte also über kurz oder lang Einzug in Microsoft-Software halten.

vergleichen mit dem Stand der Spracherkennung noch vor wenigen Jahren. Ein gewisses Maß an Nachbearbeitung ist immer nötig, allerdings steht das in kei-

nem Vergleich zum manuellen Mitschreiben. Zum reinen Nachschlagen und fürs Archiv eignet sich der erkannte Text allemal.

(akr@ct.de) ct

# WISSEN SCHÜTZT

Praxiswissen für die  
Security-Achterbahn 2021

**Online-Konferenz**  
9. September 2021

### Auszug aus dem Programm:

- Die IT-Security-Lage – aktuelle Gefahren, neue Trends, darauf sollten Sie sich vorbereiten  
*Jürgen Schmidt*
- Vorbereitung ist alles – der richtige Umgang mit Datenschutzvorfällen  
*Joerg Heidrich, Christoph Wegener*
- Cyber! Versicherung! Will ich das wirklich haben?  
*Linus Neumann*

**Podiumsdiskussion:** Der Emotet-Takedown – was darf der Staat?

# heise Security TOUR

**JETZT TICKET  
SICHERN**



**JETZT ANMELDEN**  
[heisec.de/tour](http://heisec.de/tour)

Unsere Partner



# Zahlen, Daten, Fakten

## Bluetooth

Anfänglich, im Jahre 1994, sollte die Bluetooth-Funktechnik zuerst nur die lästigen Kabelverbindungen zwischen Geräten ersetzen. Daraus entstand bis 1999 ein erster internationaler Standard, der nach und nach durch Profile zum Vehikel für diverse Kommunikationsaufgaben erweitert wurde. Standen der Technik zu

Beginn Sicherheitsprobleme durch mangelhafte Verschlüsselung sowie schlechte Interoperabilität der Geräte im Weg, ist das heute eher die Ausnahme. Auch ein „Akkusauger“ im Smartphone ist Bluetooth längst nicht mehr. Der Low-Energy-Modus hat Bluetooth sogar für Fitnessbänder, andere Wearables und Sensoren

fit gemacht. Seitdem Bluetooth die Versionsnummer 5 trägt, wird die Technik zunehmend für Kleinstnetze sowie für standortbezogene Dienste genutzt. Ganz neu ist das Stromspar-Bluetooth-Profil LE Audio, das mit einem neuen Codec (LC3) eine bessere Audioqualität sowie geringe Latenzen bringen soll. (mil@ct.de) **ct**

## ► Geschichte

Dr. Jaap Haartsen und Sven Mattisson entwickeln Bluetooth zum drahtlosen Verbinden von Geräten auf kurze Distanz.

Gründung der Bluetooth Special Interest Group.

**Erste offizielle Bluetooth Spezifikation** erscheint, max. Datenrate 732,2 kBit/s  
Erste Chipsätze, Mäuse und PCs mit Bluetooth erscheinen

1994

1998

1999

**Version 3 + HS** (Seattle Release) erscheint. Ein Highspeed-Kanal (HS) erhöht die Datenrate auf 3 MBit/s, mit WLAN auf 24 MBit/s (UCD)  
**Version 4.0** kommt. Low Energy im Protokollstapel, 128-Bit-AES-Verschlüsselung

Die **Bluetooth Spezifikation 2.1 + EDR** (Lisbon Release) vereinfacht das Pairing (SSP), Extended Inquiry Response fragt mehr Geräteeigenschaften ab, Sniff Subrating spart Energie im Low-Power-Betrieb

Die **Bluetooth-Spezifikation 2.0 + EDR** erscheint, damit höhere Datenraten möglich (2,1 MBit/s)

2004

Erste Chipsätze mit **Bluetooth 4.0** auf dem Markt

**Bluetooth 4.1** rüstet Client- und Hostmodus für alle Gerätarten nach

**Bluetooth 4.2** erweitert Sicherheitsfunktionen, erhöht Datenrate im Low-Energy-Betrieb auf 650 kBit/s, im Classic-Betrieb auf 26 MBit/s

**Bluetooth 5.** Vierfach größere Reichweite, verdoppelte Datenrate, Standort-Informationen, Ausbau der Energiesparfunktion durch Ankündigung, wann Pakete gesendet werden

2011

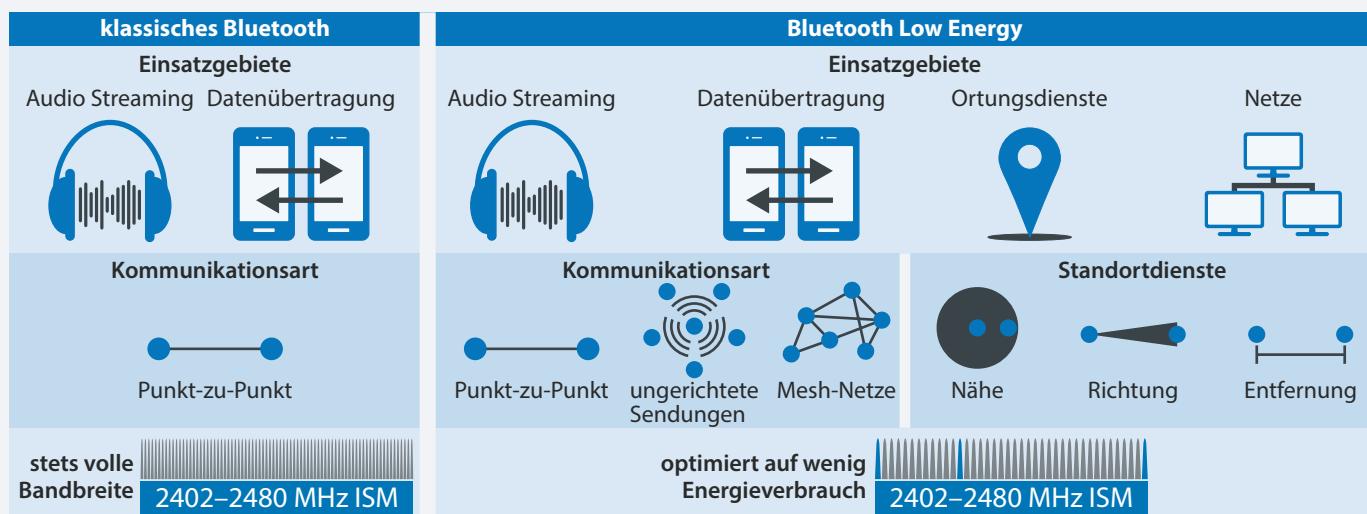
2013

2014

2016

## ► Evolution zu Bluetooth Low Energy

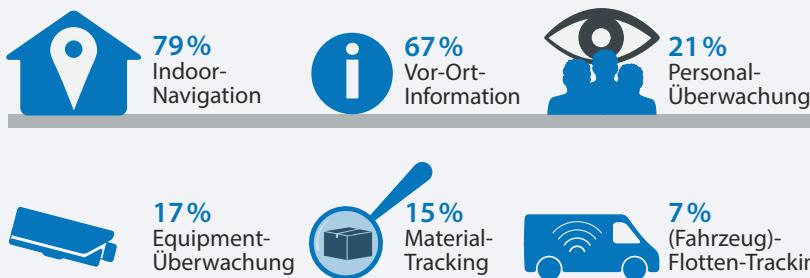
... Bluetooth hat sich von der klassischen Punkt-zu-Punkt-Verbindung zum Netzwerk- und Lokalisierungs-Vehikel entwickelt.<sup>1</sup>



## ► Standortmelder

... die Nutzung von Bluetooth zur Ortsbestimmung soll laut Marktforschern stark wachsen – bis auf 480 Millionen jährlich verkaufter Geräte im Jahre 2025.<sup>2</sup>

### Wofür wird Bluetooth derzeit genutzt?



### In welchen Bereichen wird Bluetooth-Tracking derzeit genutzt?



**Version 1.1 erscheint.** Einführung verschlüsselter Kanäle. Signalstärkemessung (RSSI) für bessere Auslastung von Kanälen. Das Handy Ericsson T39 mit Bluetooth ist kommerziell erfolgreich.

2001

**Version 1.2 erscheint.** Datenrate steigt mit EDR auf 1 MBit/s, Einführung von Energiesparmaßnahmen, bessere Fehlerkorrektur

2003

#### Core-Spezifikation 5.1:

neu Richtungsbestimmung.  
**Version 5.2** führt Stromsparmodus für Audio ein: LE Audio

2020

## ► Bluetooth LE Audio

... Bluetooth LE Audio steht als künftiger Standard-Codec für eine große Erweiterung der Bluetooth-Audio-Fähigkeiten.<sup>3</sup>

-  **Multi-Stream-Fähigkeit:** besseres Handling von mehreren gekoppelten Geräten
-  **Bluetooth LC3 Codec:** auch bei verringerten Bitraten bessere Audioqualität als SBC (= Subband Codec für A2DP), geringere Latenz
-  **Personal Audio Sharing:** Teilen und gemeinsames Hören von Podcasts oder Musik, etwa mit Menschen in direkter Nähe („Social Music“)
-  **Location Based Audio Sharing:** etwa zur Tonübertragung in Kinos, Konferenzen, in Museen oder Fitness-Centren
-  **Hörgeräte:** Verbesserungen für die Ankopplung an Smartphones, mit LC3-Codec bessere Audioqualität

## ► Bluetooth schnelle Fakten

### Frequenzbereich

2402 bis 2480 MHz,  
eingebettet in das ISM-Band  
2400 bis 2483,5 MHz

### Frequenzwechsel

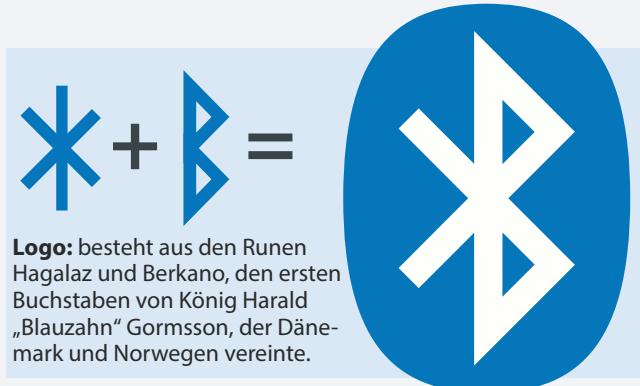
1600 mal pro Sekunde  
(Fast Frequency Hopping)

### 79 Kanäle à 1 MHz

(Ausnahmen: Frankreich, Spanien, Japan, dort nur 23 Kanäle)

### Modulationsverfahren:

Gaussian-Frequency-Shift-Keying (GFSK), Vollduplex



## ► Zahl der Bluetooth-Profile

... beinahe jedes Jahr entstehen neue Profile, mit denen Geräte sich verbinden lassen. Zurzeit sind noch 123 aktiv.<sup>4</sup>

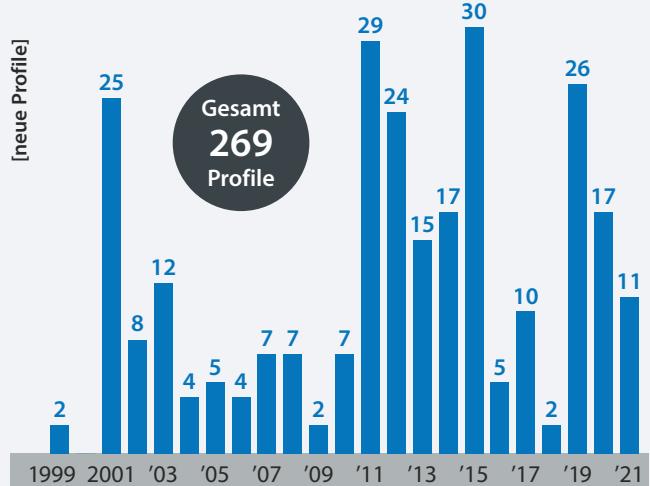




Bild: Thorsten Hübler

# Wähler-Zielvorrichtung

## Personalisierte Online-Wahlwerbung: Transparent ist nur der Wähler

**Das Geschäft mit politischen Anzeigekampagnen auf Facebook und YouTube läuft prächtig – trotz der Skandale um Manipulation und Versuche, bestimmte Gruppen vom Wählen abzuhalten. Auch im Vorfeld der diesjährigen Bundestagswahlen investieren die Parteien kräftig in Online-Wahlkampf und datengestützte Hausbesuche.**

Von Andrea Trinkwalder

**E**ine halbe Milliarde US-Dollar hatten Joe Biden und Donald Trump insgesamt anlässlich der US-Präsidentenwahlen in die Werbenetzwerke von Facebook und Google gepumpt – so viel wie nie zuvor. Denn auf den Social-Media-Plattformen finden Wahlstrategen perfekte Bedingungen, um maßgeschneiderte Botschaften an fein justierte Zielgruppen auszuspielen, die dafür besonders empfänglich sind.

Bürgerrechtler und Wissenschaftler halten solch extreme Formen des Wähler-Targetings für demokratiegefährdend, insbesondere angesichts der undurch-

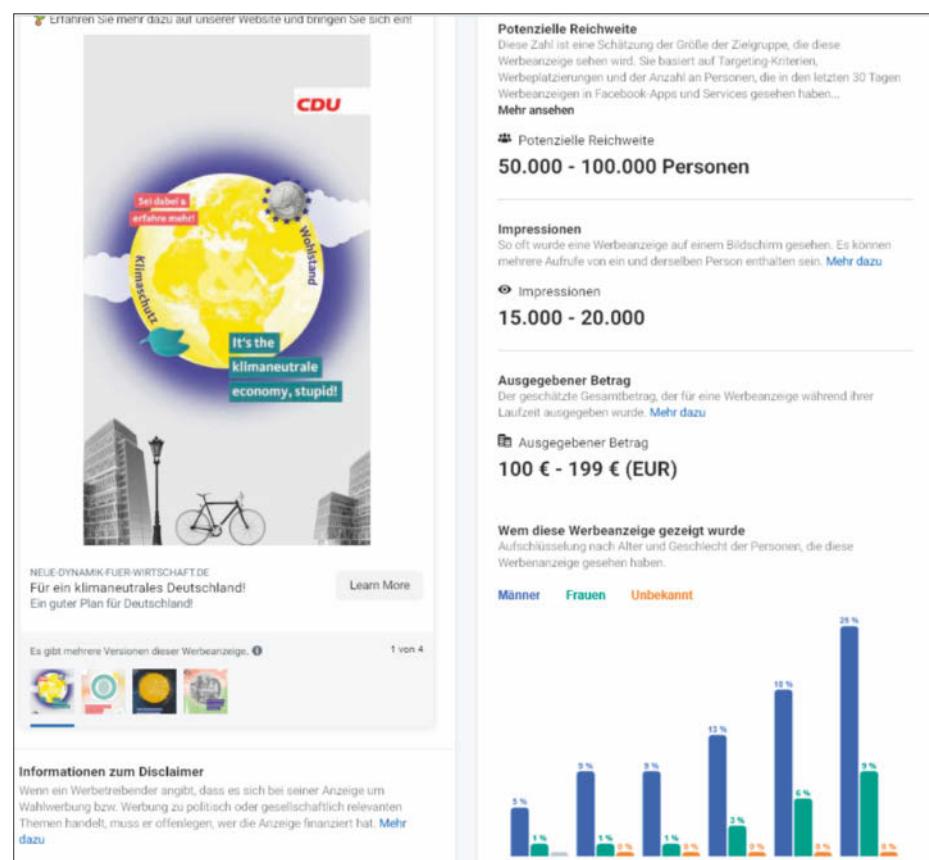
schaubaren Empfehlungsalgorithmen von Facebook, Google & Co., die automatisiert eine Melange aus Nachrichten, privaten Posts und Werbung zusammenröhren und in allzu homogener Form als „Newsfeed“ präsentieren. Skandale um Datenmissbrauch (Cambridge Analytica), Fake News und gezielte Werbekampagnen, die Afroamerikaner und Frauen vom Wählen abhalten sollten, setzten die Konzerne nach den US-Wahlen 2016 und dem Brexit-Votum gehörig unter Druck. Die daraufhin gestarteten Transparenzoffensiven sowie Maßnahmen gegen Hass und Desinformation sind in den

Augen der Kritiker allerdings rein kosmetischer Natur.

Auch deutsche Parteien verlagern die Werbung zunehmend ins Netz und analysieren Daten, um ihre begrenzten personellen und finanziellen Mittel dort einzusetzen, wo es sich lohnt: bei der eigenen Klientel nebst sympathisierenden Wechselwählern. Bereits 2017 experimentierten Kampagnenführer anlässlich der Bundestagswahl mit Micro-targeting und datengestützten Hausbesuchen – allen voran die CDU und SPD, aber auch FDP, CSU und Grüne. Wir haben uns angesehen, welche Möglichkeiten Facebook und Google den politischen Organisationen hierzulande bieten und welche Grenzen ihnen gesetzt sind. Einige Akteure verzichten freiwillig darauf, das theoretisch Machbare voll auszuschöpfen. Bleibt die Frage, wie gut sich deren Verhalten überhaupt kontrollieren lässt.

### Ohnmacht online

Verglichen mit Rundfunk und Presse ist die Online-Werbung ein gesetzlich weitgehend unreguliertes und undurchschaubares Feld. Zwar müssen sich Werbetreibende bei Google und Facebook mittlerweile registrieren, einen Sitz innerhalb der EU nachweisen und politische Anzeigen kennzeichnen, Details dazu siehe ct.de/ymtz. Anders als in Verlagen bekommt deren Inhalt vor der Veröffentlichung jedoch kein Mensch zu Gesicht, sondern nur ein Algorithmus.



**Mit Facebook Dynamic Ads testet die CDU offenbar, wie unterschiedliche Anzeigenmotive bei unterschiedlichen Zielgruppen ankommen.**

Inhaltlich unterzieht Facebook nur normale Accounts einem Faktencheck; Politiker und politische Werbung bleiben davon unbehelligt. Auch Google akzeptiert in Werbung verpackte Lügen, wäh-

rend Twitter keine politische Werbung mehr schaltet, aber den Politikern selbst das Verbreiten von Halb- und Unwahrheiten weiterhin zubilligt. Dies rechtfertigen die Social-Media-Konzerne mit dem Argu-

## Regulierter Rundfunk, Presse mit Kodex

Rundfunk- und TV-Sender sind aufgrund ihrer Reichweite prädestiniert dafür, als Propagandainstrument missbraucht zu werden, weshalb sie in Deutschland den strengsten Regeln bei der Ausstrahlung von Wahlwerbespots unterliegen. Weil der Gesetzgeber sie zu parteipolitischer Neutralität verpflichtet, müssen sowohl die Öffentlich-Rechtlichen als auch die Privaten den Parteien vor den Bundestags- sowie den Landes- und EU-Parlamentswahlen angemessene Sendezeit einräumen. Ein Anrecht darauf haben im Vorfeld der Bundestagswahl diejenigen Parteien, für die mindestens eine Landesliste zugelassen wurde. Auch inhaltlich zieht der Gesetzgeber eine

klare Grenze: Rundfunkanstalten dürfen Wahlwerbespots nur ablehnen, wenn sie gegen das Strafrecht verstößen.

Dagegen muss die Presse keine neutrale Haltung einnehmen. Zeitungs- und Zeitschriftenverlage entscheiden nach eigenen Kriterien, ob sie Anzeigen politischer Parteien annehmen oder ablehnen. In der Regel orientieren sie sich dabei am Pressekodex, legen aber mitunter recht unterschiedliche Maßstäbe an, wie der Faktenfuchs am Beispiel einer AfD-Anzeige dokumentiert (siehe ct.de/ymtz). Die Partei hatte in mehreren Zeitungen Wahlwerbung mit dem Slogan „Freie Wahl statt Impfpflicht“ geschaltet, unter anderem in

der Mittelbayerischen Zeitung sowie im Münchner Merkur.

Als Leser der Mittelbayerischen kritisierten, dass die Anzeige suggeriere, es gebe eine Impfpflicht (was nicht der Fall ist), entschuldigte sich der Verlag und erklärte, dass diese Werbung nach den Kriterien der Verlagsleitung eigentlich nicht hätte veröffentlicht werden dürfen. Der Münchner Merkur zieht die Grenze hingegen erst bei volksverhetzenden und radikalen Inhalten und sah in dem fraglichen Slogan keinen Konflikt. Die Augsburger Allgemeine wiederum veröffentlicht grundsätzlich keine Wahlwerbung der AfD.

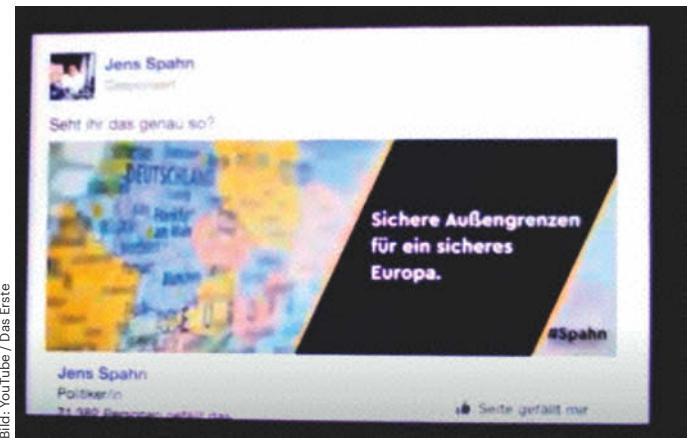


Bild: YouTube / Das Erste



Bild: YouTube / Das Erste

ment, dass sich Bürger selbst eine Meinung über die Parteien und ihre Protagonisten bilden sollen. Die Konzerne wollen sich nicht anmaßen, wie ein Richter über wahr und falsch zu entscheiden.

Kritiker halten die Meinungsfreiheit für ein vorgeschoenes Argument, um das Geschäftsmodell zu retten. Sie geben zu bedenken, dass sich politische Akteure online sehr erfolgreich der öffentlichen Kontrolle entziehen können. Darüber hinaus erlauben die globalen Werbenetzwerke ein Ausmaß an zielgruppenspezifischer Ansprache, wie es via Rundfunk und (Online-)Presse nie denkbar wäre. Bekommen Wähler darüber nur noch maßgeschneiderte Werbebotschaften zu sehen, denen sie zustimmen würden, blieben Beschwerden und Diskussionen über potenziell bedenkliche und demokratiegefährdende Inhalte aus.

### Beobachten, testen, zielen

Große Plattformen wie Google und Facebook können Zielgruppen besonders fein austarieren und mit passender Werbung versorgen. Sowohl der Suchmaschinen- als auch der Social-Media-Konzern haben ausreichend Nutzerdaten gesammelt und auf dieser Basis Machine-Learning-Algorithmen trainiert, um Produkte jedweder

Art – vom Schuh bis hin zur politischen Botschaft – denjenigen anzupreisen, die dafür vermeintlich besonders empfänglich sind. Google hat das Targeting auf die Auswahl von Alter, Geschlecht und Wohnort (Postleitzahl) sowie kontextsensitive Formate beschränkt, während sich Facebook- und Instagram-Kampagnen immer noch nach allen Regeln der Werbekunst optimieren lassen.

Einen direkten Weg zur Zielgruppe bieten Schlagwörter, mit deren Hilfe sich die Zahl der Adressaten etwa auf Männer zwischen 25 und 40 Jahren eingrenzen lässt, die kleine Kinder haben und sich für Umweltthemen interessieren. Oder auf Personen ab 50, die Motorräder mögen. Oder auf Gründerinnen, Handwerkerinnen et cetera. Wer sich mit dem Definieren von Keywords schwertut, kann sich von den Facebook-Algorithmen automatisch Zielgruppen erstellen lassen, nämlich per Custom Audiences, Lookalike Audiences sowie Dynamic Ads.

Für erstere müssen Werbetreibende eine Kundenliste mit Identifikationsmerkmalen wie etwa E-Mail-Adressen, Namen oder Telefonnummern an Facebook übermitteln. Solche Identifikatoren wandelt der Konzern dann in Hash-Werte um und gleicht sie mit der eigenen

**Die ARD-Doku „Infokrieg im Netz“ zeigt, wie Jens Spahn 2017 mit widersprüchlichen Botschaften warb. Gegenüber 22- bis 48-Jährigen, die sich für die AfD interessieren, plädiert er für sichere Grenzen, während er Großstädtern zwischen 20 und 50 Jahren Weltoffenheit vorspielte.**

Datenbank ab, um die zugehörigen Konten zu finden. Diese Werbeform eignet sich, wenn eine Partei etwa die eigenen Mitglieder auf einer der Social-Media-Plattformen ausfindig machen und ansprechen möchte.

Via Lookalike Audience lassen sich auch Personen adressieren, die noch nicht zum Kundenstamm gehören, aber Gemeinsamkeiten mit einem Teil der eigenen Klientel haben. So könnte eine Partei etwa versuchen, ihre Follower und Website-Besucher anhand von Likes und Facebook-Pixel in „Stammwähler“, „Wechselwähler“ und „unbekehrbar“ zu gruppieren. Geht man nun davon aus, dass deutschlandweit viele dieser potenziellen Sympathisanten irgendwie ähnlich ticken (etwa aufgrund von Sozialisierung, bestimmter Interessen oder Meinungen), lässt sich mithilfe dieses kleinen Follower-Grüppchens das gesamte deutsche Facebook-Universum nach potenziellen Sympathisanten durchsuchen – um diese mit motivierenden Botschaften zu umgarren. Die Quell-Audience muss mindestens 100 Personen enthalten; aus ihr leitet der Algorithmus bis zu 500 Lookalike Audiences ab.

### Gläsern, aber anonym

Weil das Direktmarketing über Custom Audiences rechtlich immer heikler wird und die DSGVO flächendeckendes Datensammeln zunehmend erschwert, haben Werbenetzwerke längst einen Plan B in der Hand: Neuere Techniken ermitteln Zielgruppen dynamisch anhand ihres aktuellen (Lese-)Verhaltens und setzen selbstlernende Algorithmen ein, um Anzeigen automatisiert und auf den Kontext abgestimmt zu platzieren. Dafür benötigt man dann deutlich weniger oder gar keine persönlichen Daten der Nutzer mehr.

Vertieft sich beispielsweise jemand – egal wie alt und welchen Geschlechts – gerade in einen Beitrag über den Truppenabzug aus Afghanistan, liest auch die KI des Werbedienstleisters fleißig mit: Mithilfe neuronaler Netze zur Text-, Bild- und Videoerkennung versuchen Plattformen automatisiert einzuschätzen, welche Werbebotschaft zum Thema und der vermuteten Stimmung des Textes passt – und spielen eine passende Anzeige in Echtzeit ein.

Für gesellschaftspolitisch besonders bedenklich halten einige Forscher sogenannte Dynamic Ads – gewissermaßen Anzeigebaukästen und Verhaltensstudien in einem. Damit testen die Algorithmen

mehrere Gestaltungsvarianten automatisiert an verschiedenen Zielgruppen und optimieren die Kampagne anhand der Reaktionen. Der Auftraggeber muss lediglich die Text-, Bild- und Videobausteine liefern – und die Facebook-Algorithmen ermitteln, welche Variante bei welcher Gruppe am besten wirkt.

## Mit Daten und Apps auf Wählerfang

Rein technisch bieten sich also auch deutschen Parteien genügend Möglichkeiten, Facebook-Accounts mit maßgeschneideter Wahlwerbung zu fluten. Dass es nicht so ausartet wie in den USA, liegt an den begrenzten finanziellen Mitteln sowie dem Datenschutz (siehe Kasten auf S. 122) – aber auch an ethischen Grenzen, die die meisten Parteien für sich noch ziehen. SPD und Grüne wollen auf eine allzu feine Segmentierung der Wählerschaft verzichten und haben konkrete Selbstverpflichtungen veröffentlicht. Eine SPD-Sprecherin erklärte gegenüber c't, dass Keywords und kontextsensitive Formate verwendet werden, aber keine Dynamic Ads. Nicht ganz so konkret distanziert sich die FDP in ihren Richtlinien von „Werbe- und Wahlkampfmaßnahmen, die nicht von unserer Rechtsordnung gedeckt sind“. Als Beispiel nennt die Partei explizit das Native Advertising, das Werbung als journalistische Inhalte tarnt. Insbesondere beachte man das hohe Datenschutzniveau der DSGVO; sämtliche Selbstverpflichtungen siehe ct.de/ymtz.

Ganz vorne dran mit dynamischer Facebook- und Instagram-Werbung ist momentan die CDU. Sie hat für den Wahlkampf die Agentur „Serviceplan Reputation“ engagiert, die sich unter anderem auf das (Wieder-)Herstellen der Reputation von Unternehmen spezialisiert hat. Mit Motiven in freundlichen Pastellfarben inszeniert sich die Regierungspartei als Gestalter einer rosigen Zukunft durch technischen Fortschritt – und zwar in allen Bereichen von Wirtschaft über Klimaschutz bis hin zu Gesundheit und Digitalisierung. Dabei machte sie zu Beginn des Wahlkampfs im Juli bereits regen Gebrauch von dynamischen Ads, experimentiert offenbar mit verschiedenen Motiven für verschiedene Zielgruppen. Manche wurden verstärkt an die Zielgruppe ab 35 ausgespielt, die meisten eher an Männer.

Auch die FDP gibt sich auf Facebook tatkräftig, propagiert technische Lösun-

sind falsch! Das geht aus aktuellen Zahlen aus Hamburg hervor, wo der Anteil der falsch-positiven Tests seit Wochen bei mehr als 50 Prozent liegt und nun sogar auf 80 Prozent gestiegen ist. Bei 308.000 Schnelltests wurden in einer Woche 218 positive Ergebnisse gemeldet, von denen sich jedoch nur 44 bestätigt haben.

Wir halten uns vor Augen: Die Sieben-Tage-Inzidenz liegt derzeit bundesweit bei 4,9. Das bedeutet, dass es in den vergangenen sieben Tagen durchschnittlich 4,9 positive Tests pro 100.000 Einwohner gegeben hat. Das entspricht einem Bevölkerungsanteil von rund 0,005 %. Wenn der Anteil der falsch-positiven Tests ähnlich hoch ist wie in Hamburg, dann liegt die Zahl der tatsächlichen Ansteckungen noch deutlich darunter. Von den Infizierten haben wiederum viele Betroffene gar keine oder nur geringfügige Symptome.

Es versteht sich von selbst, dass solche Zahlen noch nicht einmal ansatzweise eine Fortsetzung der derzeitigen Corona-Maßnahmen rechtfertigen!

<https://afdkompakt.de/2021/07/06/80-prozent-der-pcr-positiv-tests-sind-falsch/>

Bitte unterstützen auch Sie unsere Arbeit mit einer Spende:  
<https://www.afd.de/spenden>

Oder platzieren Sie ein AfD-Großplakat. Schon ab 108 €:  
<https://www.afd.de/plakatapendeshop>

Kennen Sie schon unseren Telegram-Kanal? Sofort abonnieren! ❤  
<https://t.me/afdbrennpunkt>



### Informationen zum Disclaimer

Wenn ein Werbetreibender angibt, dass es sich bei seiner Anzeige um Wahlwerbung bzw. Werbung zu politisch oder gesellschaftlich relevanten

Werbeanzeigen sehen wird, sei basiert auf Targeting-Kriterien, Werbeplatzierungen und der Anzahl an Personen, die in den letzten 30 Tagen Werbeanzeigen in Facebook, Apps und Services gesehen haben....

[Mehr ansehen](#)

▪ Potenzielle Reichweite

**>1 Mio. Personen**

### Impressionen

So oft wurde eine Werbeanzeige auf einem Bildschirm gesehen. Es können mehrere Aufrufe von ein und derselben Person enthalten sein. [Mehr dazu](#)

▫ Impressionen

**70.000 - 80.000**

### Ausgegebener Betrag

Der geschätzte Gesamtbetrag, der für eine Werbeanzeige während ihrer Laufzeit ausgegeben wurde. [Mehr dazu](#)

▫ Ausgegebener Betrag

**100 € - 199 € (EUR)**

### Wem diese Werbeanzeige gezeigt wurde

Aufschlüsselung nach Alter und Geschlecht der Personen, die diese Werbeanzeige gesehen haben.

**Männer    Frauen    Unbekannt**



**AfD-Werbung kommt im Stil boulevardjournalistischer Inhalte daher. Die Zahlen und Fakten im Text sind recht kreativ kombiniert, damit der Leser die gewünschten Schlüsse zieht.**

gen für die Probleme der Zeit (von Bildung bis Klima) und inszeniert Christian Lindner als charismatischen Macher. Ähnlich wie die CDU experimentiert auch die FDP mit dynamischen Anzeigen.

Die Grünen werben noch eher zurückhaltend vor allem um Unterstützer im Wahlkampf und thematisch fürs Klima und bezahlbares Wohnen. Dynamische

Anzeigen wurden bislang nicht verwendet, Männer und Frauen eher gleich bedient, der Fokus liegt tendenziell auf der mittleren Altersgruppe. Auch die Linke spart sich das Budget offenbar für die heiße Phase auf, wirbt bislang noch vor allem um Unterstützer.

Die AfD schaltet Werbung mit Skandal-Meldungen im Stil einer Boule-

**Hol dir unsere grünen Apps auf dein Smartphone!**



Bild: Die Grünen

**Momentan werben die Parteien auch massiv um Unterstützer für den wiederentdeckten Haustürwahlkampf. Bei CDU, Grünen und SPD verraten Apps, wo sich Hausbesuche lohnen, oder koordinieren Plakataktionen.**

 Who Targets Me  @WhoTargetsMe · 6. Juli

In Germany, the CDU spent nearly 70% more on Facebook than any other party in the last month.

82 days until the election.

Party	Total spent	Active pages	Total ads	Ads per page	Spend per page	Spend as % of top spender
CDU/CSU	€142,461.00	337	3208	9.52	€422.73	100.00%
SPD	€84,653.00	460	2309	5.02	€184.03	59.42%
Die Linke	€58,138.00	106	567	5.35	€548.47	40.81%
Die Grünen	€48,673.00	198	713	3.60	€245.82	34.17%
AfD	€42,327.00	193	971	5.03	€219.31	29.71%
FDP	€36,913.00	184	1409	7.66	€200.61	25.91%

1 3 7 

**Projekte wie Who Targets Me versuchen, Licht ins Dunkel zu bringen, indem sie die Werbeausgaben aller Parteikanäle zusammentragen und per Reverse Engineering Targeting-Kriterien ermitteln.**

vard-Zeitung, die das Bild eines aus den Fugen geratenen Landes zeichnen und fordert die Rückkehr zu einem „normalen“ Deutschland. Dafür greift sie gern aktuelle Ereignisse oder (vermeintliche) Missstände auf, leitet daraus eine plakative Forderung ab und untermauert die eigene Sichtweise mit geschickt aneinander gereihten Fakten und Zahlen. Die Beweiskette weist allerdings an entscheidender Stelle häufig einen logischen Bruch auf – oder es fehlen wichtige Details.

### Transparente Feigenblättchen

Verglichen mit den immensen Möglichkeiten, die sich Werbetreibenden auf Facebook (und in abgeschwächter Form auch bei Google) bieten, nehmen sich die Kon-

trollwerkzeuge recht bescheiden aus. So wohl Google als auch Facebook haben als Reaktion auf die massiven Vorwürfe der Wahlverfälschung und drohende gesetzliche Regelungen Transparenzoffensiven in Form von Werbebibliotheken gestartet: Dort können sich interessierte Bürger und Journalisten sämtliche Anzeigen von Parteien und anderen Organisationen auflisten lassen. Unter anderem informieren diese Archive auch darüber, wie viel Geld eine Partei für Wahlwerbung ausgegeben hat und an welchen ungefähren Personenkreis eine Anzeige ausgespielt wurde – aber nur bezüglich der Faktoren Geschlecht, Altersgruppe und Bundesland.

Daraus kann man sich im besten Fall erschließen, ob eine Werbebotschaft eher

auf Erst- oder Stammwähler zielt, Bayern anders umworben werden als Küstenbewohner und Frauen/Männer/Diverse mit geschlechtsspezifischen Themen. Welche Targeting-Kriterien der Auftraggeber selbst gewählt oder der Algorithmus ermittelte hat, bleibt hingegen das Geheimnis von Parteien und Plattformen. Damit fehlt auch die öffentliche Kontrolle, ob durch geschicktes Kombinieren von Eigenschaften – etwa Interessen, Postleitzahl et cetera – Menschen anhand von Ethnie, Religion, sexueller Orientierung oder psychischer Verfassung adressiert beziehungsweise ausgeschlossen werden. Die exakten Kriterien kann nur derjenige abrufen, dem eine bestimmte Werbung angezeigt wurde.

Licht ins Dunkel versuchen Wissenschaftler durch Reverse Engineering zu bringen: Facebook-User können sich die Browser-Extension der Initiative Who Targets Me herunterladen, die Informationen über eingebundene Werbeanzeigen zusammenträgt und versucht, auf dieser Grundlage Targeting-Kriterien zu entschlüsseln.

Auch die Universität Viadrina aus Frankfurt an der Oder ruft zu Datenspenden auf: Mithilfe der DataSkop-Plattform von Algorithm Watch möchten die Wissenschaftler den Mechanismen hinter YouTube-Werbeinblendungen auf den Grund gehen. Ebenfalls mit Algorithm Watch arbeitet die Süddeutsche Zeitung, deren #wahlfilter-Projekt bereits 200.000 Instagram-Anzeigen zur Auswertung ge-

## DSGVO-konformes Microtargeting

Sowohl im Haustür- als auch im Online-Wahlkampf setzt die DSGVO den Wahlstrategen deutliche Grenzen – weshalb sich die Parteien faktisch auf Techniken beschränken müssen, die ohne persönliche Daten auskommen. So darf eine Partei zwar Daten kaufen und auswerten, um das Wählerpotenzial in bestimmten Gegenden und Straßenzügen zu erforschen. Diese müssen aber so stark aggregiert sein, dass sie keine Rückschlüsse auf das Individuum zu lassen.

Derart anonymisierte Informationen fallen nämlich nicht in den Anwendungsbereich der DSGVO, weshalb Daten-

händler wie Post Direkt oder die Einwohnermeldeämter sie auch für beliebige Zwecke verkaufen dürfen.

Auch bei den vor Ort erfassten Daten muss die Anonymität gewährleistet bleiben. Die Grünen etwa mussten ihre App nachbessern, weil die mit Standort gespeicherten Notizen erst beim Übertragen an den Server aggregiert wurden. Und eine Sicherheitslücke in der CDU-App erlaubte Zugriff auf die gesamte Datenbank.

Mit Nutzung von Lookalike- und Custom Audiences würde sich eine Partei auf dünnes Eis begeben, wenn sie dafür persönliche Daten wie Mail-Adressen

oder Telefonnummern an Facebook übermittelt. Einem solchen Verwendungszweck hätten die Betroffenen explizit zustimmen müssen, was sie vermutlich bei der Registrierung für einen E-Mail-Newsletter nicht getan haben. Diese Auffassung vertritt beispielsweise das Bayerische Landesamt für Datenschutzaufsicht und untersagt Werbetreibenden, Custom beziehungsweise Lookalike Audiences ohne explizite Genehmigung der Betroffenen zu verwenden. Urteile des Verwaltungsgerichts Bayreuth sowie des Bayerischen Verwaltungsgerichtshofs bestätigten die Sichtweise der Datenschützer.

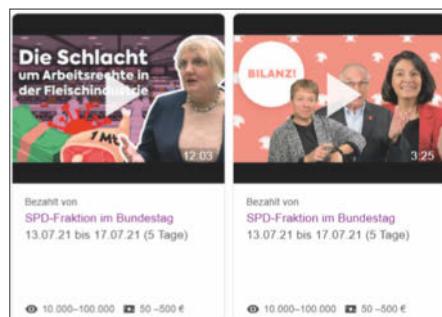
sammelt hat und nun mit Facebook weitermacht, sämtliche Projekte siehe [ct.de/ymtz](http://ct.de/ymtz).

Für die Europawahl 2019 haben die Forscher Simon Hegelich und Juan Carlos Medina Serrano nachträglich untersucht, in welchem Ausmaß und mit welcher Qualität Microtargeting in Deutschland betrieben wurde. Demzufolge verfolgte die CDU damals die professionellste Microtargeting-Strategie und nahm diesbezüglich in Deutschland eine Vorreiterrolle ein – wie schon mit ihrer Haustürwahlkampf-App Connect17 anlässlich der vorangegangenen Bundestagswahl. Auffällig war zudem, dass die AfD zwar die Partei mit der geringsten Werbereichweite war, aber die mit Abstand höchste organische Reichweite auf Facebook erzielt – und zwar während des Beobachtungszeitraums zehnmal so viele Interaktionen wie jede andere Partei.

Bedenklich finden die Wissenschaftler, dass es bei der AfD viele Posts und Werbeanzeigen gibt, die wie News-Meldungen aufgemacht sind. Dieses Verwischen der Grenzen kann man auch im aktuellen Wahlkampf beobachten, wo die AfD dann als Quelle ihr eigenes Presseportal [afdkompakt](http://afdkompakt.de) verlinkt.

### Viel Geld für nichts?

Am Ende bleibt die Frage, wie effektiv politisches Microtargeting wirklich ist, denn anders als bei der klassischen Produktwerbung lässt sich der Erfolg aufgrund des Wahlgeheimnisses nicht direkt messen – und echte Kausalität lässt sich schwer beweisen. Wer auf eine Anzeige klickt oder gar einer Partei folgt, wird nicht zwangsläufig zum Wähler. Wenn etwa Afroamerikaner den US-amerikanischen Wahlen fernbleiben, könnte das auch an den sehr direkten Offline-Maßnahmen



**SPD und Liberale werden auch verstärkt auf YouTube aktiv. Die SPD wendet sich mit eigens produzierten Erklärfilmen offensichtlich an die jüngere Generation.**

**Die Anzeigearchive von Google und Facebook geben einen groben Überblick über die Slogans der Parteien. Ob und in welchem Ausmaß Microtargeting betrieben wird, erschließt sich daraus allerdings nicht.**

liegen: dem Zuschneiden von Wahlbezirken und Entfernen ganzer Bevölkerungsgruppen aus den Wählerverzeichnissen.

Doch auch wenn man den Effekt nicht genau beziffern kann und die teils abenteuerlichen Geschichten von Insidern der Datenfirmen mit Vorsicht zu genießen sind, sollte die Gesellschaft wachsam bleiben. Noch gibt es in Europa eine funktionierende Gewaltenteilung und eine öffentliche Debatte – den wahrscheinlich besten Schutz vor den Gefahren des Microtargeting. Diverse Studien zeigen, dass sich Wähler nicht „umdrehen“ lassen und Lügenbotschaften zwar anklicken, aber nicht unbedingt glauben. Andererseits verdichten sich auch Hinweise darauf, dass das algorithmisch verstärkte und gesteuerte Dauerfeuer aus allen Kanälen langfristig das gesellschaftliche Klima vergiftet und die Gräben vertieft.

Dass Transparenzkosmetik gegen die manipulative Macht der Algorithmen

nicht wirkt und den Konzernen selbst die Kontrolle über die eigene Technik entglitten ist, dafür lieferten die US-Präsidentenwahlen bereits selbst den Beweis: Weil Donald Trump seit Monaten Zweifel an der Legitimität des Wahlprozesses säte, wurde die sonst mit Zähnen und Klauen verteidigte Meinungsfreiheit offenbar sogar Twitter und Facebook zu heikel: Beide sperrten die Konten des amtierenden Präsidenten Donald Trump dauerhaft. Facebook verhängte darüber hinaus eine Woche vor der Wahl eine Sperre für politische Werbung, die bis Anfang März 2021 dauerte.

(atr@ct.de) ct

### Literatur

- [1] Holger Bleich, Manipulationsverstärker, Was Staat und soziale Medien gegen die Fake-News-Flut vor der Wahl unternehmen, c't 16/2021, S. 122

**Studien und Quellen:** [ct.de/ymtz](http://ct.de/ymtz)

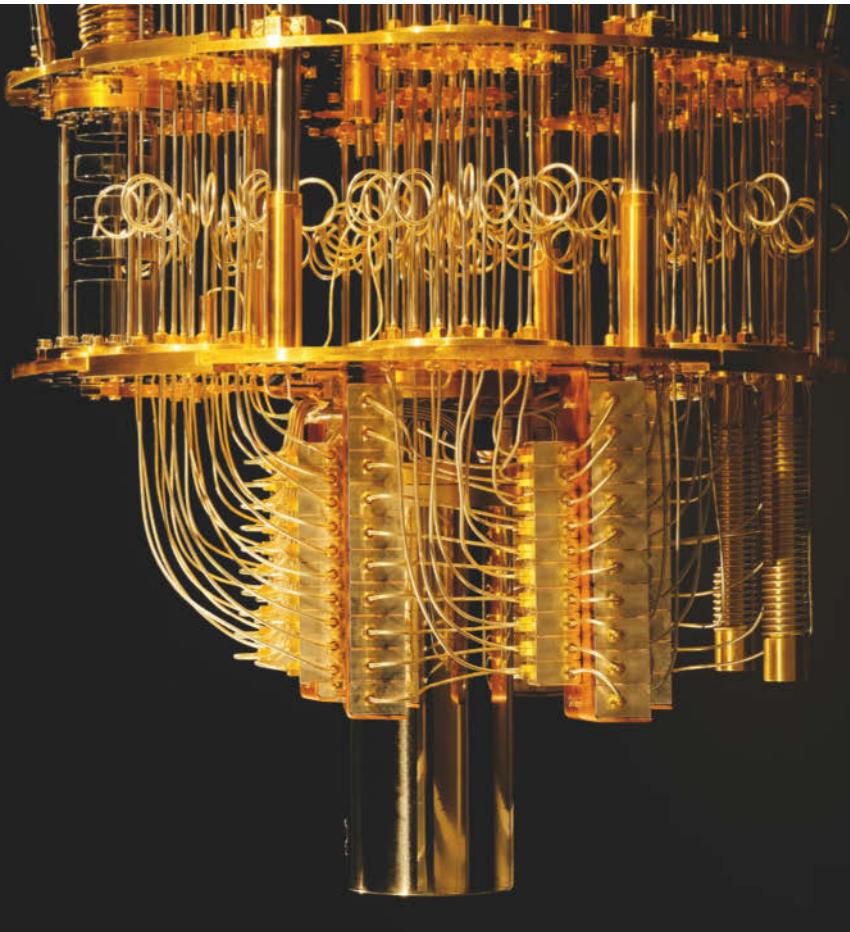


Bild: Graham Carlow / IBM

# Rechnen mit Qubits im Jahr 2021

## Sechs technische Konzepte für Quantencomputer

**Die ersten Quantencomputer müssen sich heute auf ein paar Dutzend fehlerhafte Qubits beschränken, während Anwender Tausende oder Millionen stabile Qubits benötigen. Welche Grundlagentechnik diese Steigerung leisten kann und damit das Rennen um den ersten praktischen Quantencomputer macht, ist noch offen.**

Von Dr. Sabine Hossenfelder

Quantencomputer sind derzeit eines der verheißungsvollsten Entwicklungsfelder; voraussichtlich stehen wir ganz am Anfang einer Phase technischer Durchbrüche und überraschender Anwendungen. So viele verschiedene Unternehmen und Institute arbeiten an der Realisierung des Quantencomputers, dass es schwierig ist, den Überblick zu behalten. Zumal die Marktteilnehmer ganz unterschiedliche technische Ansätze verfolgen.

Die entscheidende Grundlage für das Quantencomputing bilden die Quantenbits oder kurz: Qubits. Dabei handelt es sich um Zweizustandssysteme der Quantenmechanik. Im Gegensatz zu herkömmlichen Bits der klassischen Computertechnik,

die lediglich entweder den Wert 0 oder 1 annehmen, kann ein Qubit beliebige Kombinationen seiner beiden Zustände verkörpern. Doch die wahre Magie des Quantencomputing liegt in der Möglichkeit, Qubits miteinander zu verschränken. Die Verschränkung ist eine quantenmechanische Korrelation, für die es nichts Vergleichbares in der Welt der makroskopischen Dinge gibt. Sie führt dazu, dass sich die verschränkten Qubits einen gemeinsamen Zustand teilen beziehungsweise ein mehrteiliges Quantenobjekt bilden. Wird eines dieser Qubits manipuliert, ändern sich zugleich alle mit ihm verschränkten Qubits, die Beziehungen zwischen ihnen bleiben erhalten.

Es gibt viele Möglichkeiten, wie Qubits miteinander verschränkt sein können. Zum Beispiel lässt sich eine Reihe von Qubits so verschränken, dass sie gemeinsam nur Vielfache von Sechs ausgeben oder ausschließlich Primzahlen. In Verschränkungen liegt der Schlüssel, um spezielle mathematische Probleme zu lösen. So könnten Quantencomputer helfen, die Schrödinger-Gleichung für komplexe Molekülstrukturen zu lösen. Damit wäre es möglich, die Eigenschaften von Materialien und Werkstoffen zu bestimmen, ohne diese erst chemisch synthetisieren zu müssen. Weitere Anwendungsfelder sind Optimierungsprobleme wie etwa das Handlungsreisenden-Problem in der Logistik oder die Optimierung von Finanzportfolios unter Beachtung diverser Unsicherheiten. Bekannte Algorithmen von Lov Grover und Peter Shor zeigen, wie Quantencomputer verbreitete Verschlüsselungsverfahren brechen könnten [1]. Es mangelt also nicht an ganz realen Einsatzfällen.

Aber Quantencomputer eignen sich nicht für alle möglichen Berechnungen, sondern nur für spezielle Aufgaben. Für die Lösung mathematischer Probleme sind sie wie Wurmlöcher für Weltraumreisen: Sie können Reisende nicht überall hinführen. Aber wenn sie eine Verbindung schaffen, dann ist die wirklich schnell.

Aus den besonderen Eigenheiten des Quantencomputers resultieren auch seine größten technischen Herausforderungen. Entscheidend für das Quantencomputing ist es, die Zustände der Qubits und die Verschränkungen zwischen ihnen lang genug aufrechtzuerhalten, um die für einen Algorithmus erforderlichen Rechenschritte ausführen zu können. Schon kleinste Störungen können ein Qubit kollabieren lassen. Zurück bleibt dann ein einfaches Bit, das entweder 0 oder 1 ist, und die quantenmechanische Berechnung schlägt fehl. Ein fehlertoleranter Quantencomputer muss daher nicht nur aufwendigst abgeschirmt werden, er braucht zusätzlich auch mehrere Kopien seiner Eingangsdaten und Zwischenstände sowie eine funktionierende Fehlerkorrektur. Und das bedeutet, dass er mehr Qubits braucht. Aus diesem Grund schätzen Experten, dass Quantencomputer für sinnvolle und zudem zuverlässige Rechenanwendungen nicht 20 Qubits brauchen oder 200, sondern eher eine Million. Zugegeben, ein Daumenwert, der auch stark vom Anwendungsfall, dem verwendeten Algorithmus und der Stabilität der eingesetzten Qubits abhängt.

Solange aber die Zahl verfügbarer Qubits weit darunter liegt, bleiben Quantencomputer lediglich von akademischem Interesse.

Zur Berechnung realer Probleme genügt es nicht, Qubits zu erzeugen, diese müssen auch stabil rechnen und in der Anzahl erheblich skalieren. Ebenso müssen sich die Verschränkungen auf möglichst viele Qubits ausweiten lassen. Das Rennen um die beste Technik für Qubits ist noch längst nicht entschieden.

### Supraleitende Qubits

Die heute mit Abstand am häufigsten verwendeten Qubits basieren auf supraleitenden Schleifen. Das heißt, die Qubits sind feine Ströme in mikrometergroßen Schleifen aus supraleitendem Metall auf einem Siliziumchip. Um die beiden Zustände des Qubits darzustellen, können entweder die Verteilung der Ladung oder die Richtung des Stromflusses in einer Schleife dienen. Der große Vorteil dieser Technik liegt darin, die supraleitenden Qubits massenhaft mit bestehenden Großanlagen der Chipfertigung herstellen zu können, also mittels Verfahren, die die elektronische Industrie in den vergangenen Jahrzehnten perfektioniert hat. Die Sache hat allerdings einen großen Haken: Qubits entstehen in den Schleifen nur unter extrem niedrigen Temperaturen zwischen etwa 10 bis 20 Millikelvin, denn erst in diesen Temperaturbereichen verwandeln sich die Schaltkreise in wider-

standsfreie Supraleiter. Ohne Supraleitung können die Schleifen keine Zweizustands-Quantensysteme bilden und aufrechterhalten.

Trotz der extrem tiefen Temperaturen bestehen die Quantenzustände in supraleitenden Qubits nur kurz. Die Zeitdauer, bis sie zusammenbrechen, wird Dekohärenzzeit genannt und sie kratzt heute von unten an der 100-Mikrosekunden-Grenze. Auf das Konzept der supraleitenden Schleifen setzen Google, IBM und eine Reihe kleinerer Unternehmen. Google demonstrierte mit 53 Qubits 2019 erstmals sogenannte Quantum Supremacy, also einen Quantencomputer, der eine (sinnlose) Aufgabe löste, die kein konventioneller Computer in einer annehmbaren Zeitspanne bewältigen könnte [2].

IBM zweifelte später diesen Überlegenheitsbeweis an: Ein klassischer Supercomputer könnte die gezeigten Berechnungen bei günstiger Programmierung eben doch in vernünftiger Zeit lösen. Damit hätte Google die Quantum Supremacy wohl etwas zu früh verkündet. Vielleicht war das so. Oder IBM war in diesem Moment einfach ein schlechter Verlierer.

IBMs größter Quantencomputer hat zur Zeit 65 Qubits. Allerdings folgt das Unternehmen einer Roadmap, nach der es 2023 einen Chip mit 1000 Qubits vorstellen will. Auf die Rechenleistung kleinerer IBM-Quantencomputer mit 5 bis 16 Qubits können Forscher und Entwickler heute über die Cloud frei zugreifen [3].



Bild: Andrew Lindemann/IBM

**Der Q-System-One-Quantencomputer:** Ohne den ultratiefkühlenden Kryobehälter ist unten der Chip zu erkennen, der 27 supraleitende Qubits beherbergt.

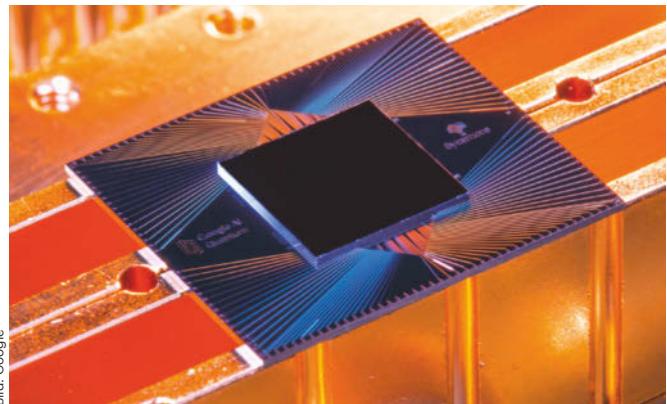


Bild: Google

Trotz der angekündigten Steigerungsraten gibt es ein großes Problem mit supraleitenden Qubits und das ist deren extreme Kühlung. Spätestens, wenn es darum gehen wird, mehrere tausend Qubits in ein Kryosystem zu stecken und zu steuern, könnte dieses Konzept aufgrund der dann erforderlichen Vielzahl an Steuerleitungen an seine Grenzen stoßen.

### Photonen als Qubits

Photonisches Quantencomputing hat diese Probleme nicht. Es nutzt einzelne Photonen als Qubits, deren Quantenzustand darin bestehen kann, dass ein Photon in einem von zwei bestimmten Zeitfenstern vorhanden ist, oder er bezieht sich auf bestimmte variable Eigenschaften eines Photons. Diesen Ansatz verfolgt beispielsweise die Firma Xanadu aus Toronto. Mit dem gleichen Konzept und ebenfalls umstritten demonstrierte Ende 2020 eine Gruppe chinesischer Forscher an der University of

Science and Technology of China die Quantum Supremacy – der zweite Fall nach Googles Demonstration.

Der größte Vorteil photonischer Qubits ist, dass man sie bei Raumtemperatur nutzen kann und sie ihre Quantenzustände wesentlich länger aufrechterhalten als supraleitende Qubits. Ihre Dekohärenzzeit liegt üblicherweise bei einigen Millisekunden, kann unter idealen Bedingungen aber sogar mehrere Stunden erreichen. Damit ist photonisches Quantencomputing wesentlich billiger und einfacher zu handhaben. Diese Systeme haben aber auch einen erheblichen Nachteil: Sie erfordern ganz schnell ganz viel Platz, weil sie je nach der Anzahl der benötigten Qubits und deren Verschränkungen eigens aus Lasern und optischen Einzelkomponenten aufgebaut werden müssen. Der Quantencomputing-Aufbau der chinesischen Forscher belegte eine komplette Tischplatte.

**53 der 54 supraleitenden Qubits auf dem Sycamore-Chip führten in 200 Sekunden Berechnungen aus, für die der stärkste klassische Superrechner Jahre, wenn nicht Jahrtausende benötigt hätte.**

Allerdings behaupten Entwickler des Unternehmens PsiQuantum, sie hätten das Platzproblem photonischer Quantencomputer im Griff und eine Lösung gefunden, mit der sie bis zu einer Million Qubits verknüpfen könnten. Wie genau sie das schaffen wollen, weiß außer ihnen niemand. Trotzdem: ein technisches Konzept für Quantencomputer, das man im Auge behalten sollte.

### Ionenfallen im Vakuum

Qubits in Ionenfallen bestehen aus Einzelatomen, zumeist mit Elektronendefizit. Aufgrund ihrer Ladung lassen sich diese Ionen in elektromagnetischen Feldern im Vakuum festhalten. Per Laserstrahl gelingt es, sie gezielt zu manipulieren und miteinander zu verschränken.

In der Größe sind Ionenfallen vergleichbar zu Mikrochips mit supraleitenden Qubits. Auch Ionenfallen erfordern tiefe Temperaturen, ertragen aber immerhin ein paar Kelvin. Das klingt nicht nach viel, ist aber um Größenordnungen besser als das, was supraleitende Qubits benötigen. Die Kühlung der Ionenfallen erfolgt ebenfalls per Laserstrahl. Der größte Player auf diesem Feld ist der Mischkonzern Honeywell, parallel verfolgt das Startup IonQ denselben Ansatz. Zudem dominiert dieses Konzept für Quantencomputing im akademischen Bereich und wird an zahlreichen Universitäten beforscht – etwa in Innsbruck (siehe den Kasten „Quantencomputer im 19-Zoll-Rack“).

Vorteile hat die Ionenfallentechnik durch ihre lange Dekohärenzzeit, diese kann leicht ein paar Minuten betragen. Zudem lassen sich die Ionen-Qubits gut mit vielen Nachbarn zur Verschränkung bringen. Aber die Arbeit mit Ionenfallen bringt auch Nachteile mit sich. Vor allem reagieren sie langsamer als supraleitende oder photonische Qubits und es ist auch schwieriger, eine große Menge Ionenfallen auf einem Chip zu realisieren. Bisher konnten sie jedoch mit den supraleitenden Qubitsystemen mithalten.

Honeywell behauptete im März dieses Jahres sogar, den leistungsfähigsten Quantencomputer der Welt gebaut zu haben – gemessen am „Quantenvolumen“. Das Quantenvolumen ist eine Metrik, die ursprünglich IBM eingeführt hat, um die Leistungsfähigkeit eines Quantencomputers zu beschreiben. Diese Maßzahl beschränkt sich nicht einfach auf die Anzahl der Qubits, sondern bezieht zusätzlich deren Fehlerrate ein, die Verknüpfungen,

## D-Wave-Annealer nicht frei programmierbar

Bis heute ist D-Wave nach eigener Aussage der einzige Anbieter großer kommerziell nutzbarer Quantencomputer. Bei diesen Großrechnern kommen supraleitende Qubits zum Einsatz und sogar erstaunlich viele: Das 2020er Modell von D-Wave verfügt über mehr als 5000 Qubits.

Aber die D-Wave-Computer sind nicht mit den Konzepten für Quantencomputer zu vergleichen, die Google und IBM verfolgen [4]. Die zahlreichen Qubits in den D-Wave-Maschinen lassen sich nicht einzeln manipulieren und damit auch nicht in der gleichen Weise verschränken wie beim universellen Ansatz

der Konkurrenten. Die großen Qubit-Felder der Kanadier können eine bestimmte Klasse von Optimierungsproblemen lösen, indem sie ein „Annealing“ genanntes Verfahren anwenden, auf das die Rechnerarchitektur ausgerichtet ist. Damit lassen sich im Wesentlichen Fragestellungen der Kombinatorik auflösen, also etwa Routing-Probleme in Netzwerken. Im Gegensatz dazu sind die Qubit-Prozessoren von Google und IBM darauf ausgerichtet, frei programmierbare Algorithmen zu berechnen und völlig unterschiedliche Probleme zu lösen. Beide Ansätze sind interessant, aber im Vergleich sind es eben doch Äpfel und Birnen.



Bild: Tim Herman / Intel

**Ein Intel-Wafer bildet die Infrastruktur für Spin-Qubits, die Wissenschaftler an der TU Delft erforschen.**

die zwischen den Qubits möglich sind, sowie das Maß, wie stark Verschränkungen und auch einzelne Qubits sich gegenseitig stören (Crosstalk). Honeywell hat nach diesem Maßstab für sein Modell H1 mit zehn Qubits ein Quantenvolumen von 512 errechnet. IBM hat bisher erst ein Quantenvolumen von 64 für sich reklamiert – mit einem 27-Qubit-System. Honeywell kündigt inzwischen an, im nächsten Jahr seine Quantencomputing-Ressourcen ebenso wie IBM über die Cloud zugänglich zu machen.

IonQs jüngstes Modell beinhaltet 32 Ionen, die in einer Reihe in einer Ionenfalle stecken. Laut ihrer Roadmap wollen die ehrgeizigen Entwickler 2025 Quantum Supremacy erreichen und 2028 mit ihren Quantencomputern ernsthafte Probleme lösen können.

## Topologische Qubits

Das topologische Quantencomputing ist der Joker. Es gibt zurzeit keinen lauffähigen Computer mit dieser Technik, aber die Idee ist faszinierend: Topologische Quantencomputer speichern Informationen in den Eigenschaften von „Quasiteilchen“, Muster in physikalischen Teilchenstrukturen, die sich wie masselose Elementarteilchen verhalten. Das Tolle an diesen Quasiteilchen ist, dass ihre Eigenschaften physikalisch besonders geschützt sind und damit aufgebaute Qubits dadurch robust gegen Dekohärenz.

Laut Microsoft-Forschern, die an den Grundlagen eines topologischen Quantencomputers arbeiten, sind insbesondere die geringe Fehlerrate der Qubits und ihre Widerstandsfähigkeit gegenüber Umgebungsrauschen überzeugend. Zudem hofft man, die benötigten Strukturen schnell skalieren

zu können. 2018 kündigte Dr. Julie Love, Direktorin für Microsofts Quantencomputer-Geschäft, gegenüber der BBC an, der Konzern werde in nur fünf Jahren einen für wirtschaftliche Anwendungen relevanten Quantencomputer fertigstellen. Allerdings erlitten Microsofts Pläne im Februar dieses Jahres einen Rückschlag, als dessen Forschungsabteilung eine Veröffentlichung zurückziehen musste. Darin hatten die Forscher konkrete Versuche mit Quasiteilchen beschrieben, die sie für den Aufbau eines eigenen Quantencomputers nutzen wollten. Die Ankündigung eines wirtschaftlich nutzbaren Modells für 2023 erscheint damit äußerst fraglich.

## Außenseiter

Abseits der genannten technischen Ansätze, die viel Aufmerksamkeit bekommen, gibt es noch zwei weitere, die man nicht aus den Augen verlieren sollte. Der erste sind Qubits aus Nanostrukturen in Halbleitern. Diese lassen sich ähnlich den supraleitenden Qubits auf Mikrochips realisieren, aber das einzelne Qubit ergibt sich lediglich aus der Ladung eines einzelnen Elektrons oder aus dessen Elektronenspin.

Diesen Ansatz verfolgen derzeit Forscher der TU Delft in den Niederlanden mit Unterstützung des Chipherstellers Intel. Der Vorteil dieser Technik besteht darin, dass auch sie nicht die extrem tiefen Temperaturen der supraleitenden Qubits erfordert, sondern immerhin ein paar Kelvin verträgt.

Die zweite Außenseiter-Technik nutzt Stickstoff-Fehlstellen in Kohlenstoff-Kris-

tallgittern als Qubits, beispielsweise in Diamanten. Diese Qubits umfassen somit nur ein Atom und sie lassen sich bei Raumtemperatur manipulieren und auslesen. Diesen Ansatz verfolgen Entwickler bei Qutech, einer Ausgründung der TU Delft, Forscher am MIT (Massachusetts Institute of Technology) sowie in einem australischen Startup namens Quantum Brilliance.

Zu beiden Außenseitertechniken haben die Forscher bislang noch keine Quantencomputer demonstriert, aber diese technischen Plattformen sind vielversprechend. Und das ist genau die Situation 2021: Das Rennen um die ersten noch eingeschränkten Quantencomputer ist im vollen Gange, aber die Entscheidung, welches technische Grundkonzept den universellen Quantencomputern der Zukunft voraussichtlich zugrunde liegen wird, ist noch völlig offen. (agr@ct.de) ct

## Literatur

- [1] Sylvester Tremmel, Türschloss-Upgrade, Wie Kryptosysteme auf Angriffe von Quantencomputern vorbereitet werden, c't 16/2021, S. 60
- [2] Arne Grävemeyer, Überlegener Qubitrechner, Google sticht mit Sycamore-Chip klassische Computer aus, c't 22/2019, S. 46
- [3] Dr. Florian Neukart, Hallo, Quantenwelt!, Wie man mit Quantengattern programmiert, c't 6/2020, S. 146
- [4] Dr. Alexander Braun, Heißes Eisen?, Quanten-Annealer – Vorbote des Quantencomputers, c't 13/2019, S. 142

**Zu diesem Beitrag finden Sie auch eine Videoversion auf dem YouTube-Channel der Autorin: [ct.de/y4fp](https://www.youtube.com/c/ctde/y4fp)**

## Quantencomputer im 19-Zoll-Rack

Im Juni haben Forscher an der Universität Innsbruck den Prototyp eines Quantencomputers mit 24 Qubits präsentiert. Passend fürs Rechenzentrum findet das autarke Gerät in zwei 19-Zoll-Serverracks Platz. Das Team um Thomas Monz setzt Ionen als Qubits ein. Um die Ionenfallen vor Störungen durch Teilchenkollisionen zu schützen, benötigt der Quantencomputer eine Vakuumkammer, die die Forscher für ihre Serverrack-Variante deutlich verkleinerten. Darüber hinaus weisen die Forscher darauf hin, dass sich alle 24 Qubits miteinander verschränken lassen – eine Rekordzahl. Bis 2022 wollen sie ihre Technik auf bis zu 50 individuell ansteuerbare Qubits erweitern.



Bild: Uni Innsbruck

**Zwei 19-Zoll-Racks – das ist der vollständige Quantencomputer mit 24 Ionenfallen-Qubits.**

# Aneinander vorbei

## Studie zur Interaktion zwischen Passwortmanagern und Webseiten

**So praktisch Passwortmanager sein mögen: Auf manchen Webseiten hakt das automatische Einsetzen von Login-Daten. Ein Forschungsteam der Universität Hannover hat die Ursachen untersucht und gibt Entwicklern von Webseiten und Passwortmanagern Empfehlungen.**

Von Jan Schüßler

Daß Passwortmanager nicht immer einwandfrei mit Login-Seiten zusammenarbeiten, konnten wir auch im jüngsten Test solcher Programme beobachten [1]. Über die technischen Hintergründe war allerdings bis dato nicht allzu viel bekannt: Zwar gibt es bislang reichlich Studien zur Usability und zur Sicherheit von Passwortmanagern, aber kaum welche, die nach den Ursachen der Hakeleien suchen, die zwischen Passwortmanagern und Login-Seiten auftreten können.

Ein wissenschaftliches Team um Nicolas Huaman an der Leibniz Universität Hannover hat sich dieser Probleme angenommen und dafür insgesamt 3319 Problembeschreibungen über Passwortmanager-Add-ons für Chrome gesammelt und nach verwertbaren Problembeschreibungen durchsucht. Nach einem mehrstufigen Prozess des Ausfilterns unnützer Bewertungen („Geht nicht!“), der Problemanalyse und dem Zusammentragen von Codebeispielen verblieben 110 Berichte, die sich auf 59 verschiedene Problemszenarien abbilden ließen. Um die Probleme reproduzierbar testen und nachstellen zu können, hat das Team aus den zusammengetragenen Szenarien 39 vollständige Minimalbeispiele entwickelt („Minimal Working Examples“ oder MWEs; möglichst knappe Codebeispiele,

die ausschließlich dem Reproduzieren eines Problems dienen).

Um den Testaufwand nicht allzu sehr eskalieren zu lassen, hat das Team die 39 MWEs gegen 15 verschiedene Passwortmanager getestet. Das sind die zehn im Chrome Web Store am meisten heruntergeladenen Add-ons, plus KeePassXC und Passbolt sowie zusätzlich noch die integrierten Passwortmanager von Chrome, Edge und Firefox – in der Summe 585 einzelne Tests. Die Ergebnisse hat das Team in einem äußerst detaillierten Bericht zusammengetragen (siehe PDF via [ct.de/yan3](http://ct.de/yan3)).

### Buntes Problemfeld

Das Feld der Problemkonstellationen ist recht bunt gemischt. Im Folgenden einige Beispiele: Unsäuberkeiten auf Webseiten sind etwa Eingabefelder, die im Quelltext falsch oder irreführend ausgezeichnet sind, also etwa Namensfelder, die als Freitextfeld (`<textarea>`) statt als Eingabefeld ausgezeichnet sind (nur drei der untersuchten Passwortmanager funktionierten damit einwandfrei), oder fehlende `<type>`-Attribute bei Eingabefeldern (nur fünf

Kandidaten). Probleme für integrierte Passwortgeneratoren fanden sich im Falle von Passwortfeldern mit begrenzter Zeichenanzahl (nur ein Testkandidat mit ungewöhnlichem Verhalten).

Ebenso lassen sich etliche Passwortmanager durch zusätzliche Elemente auf Login-Seiten verwirren. Das können zum Beispiel Fälle sein, bei denen die Felder für Login und Neuregistrierung auf einer einzelnen Seite liegen (immerhin sieben Passwortmanager mit sauberen Interaktionen), oder wenn eine PIN-Abfrage separate Eingabefelder für jede einzelne Ziffer hat (das konnte keiner der Kandidaten problemlos). Durch JavaScript-Code verursachte Schwierigkeiten finden sich zum Beispiel bei Logins, bei denen das Passwortfeld erst nach Eintippen des Benutzernamens auftaucht oder auf einer nachfolgenden Seite angefragt wird; mit dieser Disziplin kam jeder Testkandidat erst nach einem manuellen Eingriff zurecht. Erstaunlich wenige Add-ons sind in der Lage, mit Pop-up-Fenstern für die altgediente HTTP Basic Authentication umzugehen – nur vier Stück. Skurrilweise verhalten sich diesbezüglich vor allem die in den Browsern serienmäßig enthaltenen Passwortmanager weitgehend problemlos, während die meisten Add-ons gar nicht damit umgehen können.

### Erkenntnisse für Entwickler

Probleme, die vor allem Webseitenbetreiber beheben könnten, sind solche, die durch Multipage-Logins entstehen – wenn also Benutzername und Passwort auf zwei aufeinander folgenden Seiten abgefragt

Melden Sie sich an, um auf diese Website zuzugreifen.

Autorisierung angefordert von <https://web1.ctdb.ct.heise.de>

Benutzername	<input type="text" value="resops.heise.de@gmail.com"/>
Kennwort	<input type="password" value="*****"/>

Anmelden

Abbrechen

Mit den althergebrachten Passwortabfragen für HTTP Basic Authentication können erstaunlich wenige Passwortmanager umgehen.

werden. Um auf solchen Seiten funktionieren zu können, verwenden Passwortmanager oft vordefinierte Listen, um das Verhalten auf beliebten Webseiten anzupassen. Im HTML-Code könnte man das Problem zum Beispiel mit dem `autocomplete`-Attribut entschärfen. Ebenso ist es an Seitenbetreibern, nicht mit JavaScript an Eingabefeldern herumzufummeln, um etwa das Passwort nach dem Eintippen aus dem Feld zu löschen oder zuerst ein Dummy-Feld anzuzeigen, das erst gegen das echte Eingabefeld getauscht wird, wenn der Cursor darin landet. Mit solchen verschleiernden Tricks (Obfuscation) versuchen Betreiber möglicherweise, die Sicherheit zu verbessern – doch wenn es auf Kosten der Usability von Passwortmanagern geht, kann es auch kontraproduktiv sein.

Einige Probleme sind offenkundig nicht einseitig lösbar, etwa das Erkennen und Ausfüllen spezieller Eingabefelder: Während Webseitenbetreiber auch per `autocomplete` alle Login-relevanten Felder

auszeichnen könnten, wäre es ebenso wünschenswert, wenn mehr Passwortmanager individuelle Eingabefelder mit manuellen Eingriffen komfortabel speichern ließen – etwa per Rechtsklick-Aktion.

### Potenziale bei Passwortmanagern

Andere Probleme ließen sich problemlos durch Verbesserungen bei Passwortmanagern beheben, zum Beispiel der mangelhafte Support für HTTP Basic Authentication oder der Umgang integrierter Passwortgeneratoren mit längenbegrenzten Passwortfeldern. Letztere mögen aus Sicherheitsperspektive etwas merkwürdig sein, doch Passwortmanager könnten die Begrenzung (Attribut `max-length`) auch einfach auslesen und ihre Passwortgeneratoren automatisch mit der gewonnenen Info füttern. Fast alle Kandidaten scheiterten daran.

Keine Universallösung existiert zurzeit für Probleme mit Domain-übergreifenden Formularen, wenn also etwa nach

dem Abschicken von Login-Daten Redirects erfolgen und das automatische Speichern fehlschlägt, oder bei der Frage, ob die gleichen Zugangsdaten auch auf anderen Subdomains der gleichen Domain gelten. Letzteres kann ein Komfortgewinn sein, aber auch ein Risiko, wenn Login-Daten eines Dienstes bei einem anderen landen. Ein Patentrezept gibt es dafür bislang nicht; ein Hersteller löst es über eine eingebaute Domainliste. Eine standardisierte Lösung könnte in einem neuen Standard bestehen, der den Mechanismus Cross Origin Resource Sharing (CORS) zum Vorbild nimmt und Passwortmanagern Anweisungen für Domain-übergreifende Interaktion gibt. (jss@ct.de) 

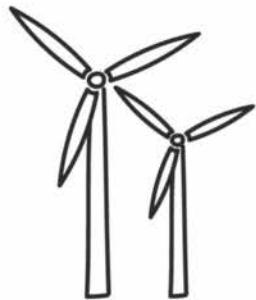
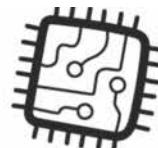
### Literatur

- [1] Jan Schüßler und Marvin Strathmann, Ich kaufe ein \*\*\*\*, 25 Passwortmanager für PC und Smartphone, c't 5/2021, S. 16

Weitere Infos: [ct.de/yan3](http://ct.de/yan3)

## MIT Technology Review

Das Magazin für Innovation von Heise



**Die Welt verstehen,  
wie sie morgen sein wird.**

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

[trvorteil.de/testen](http://trvorteil.de/testen)



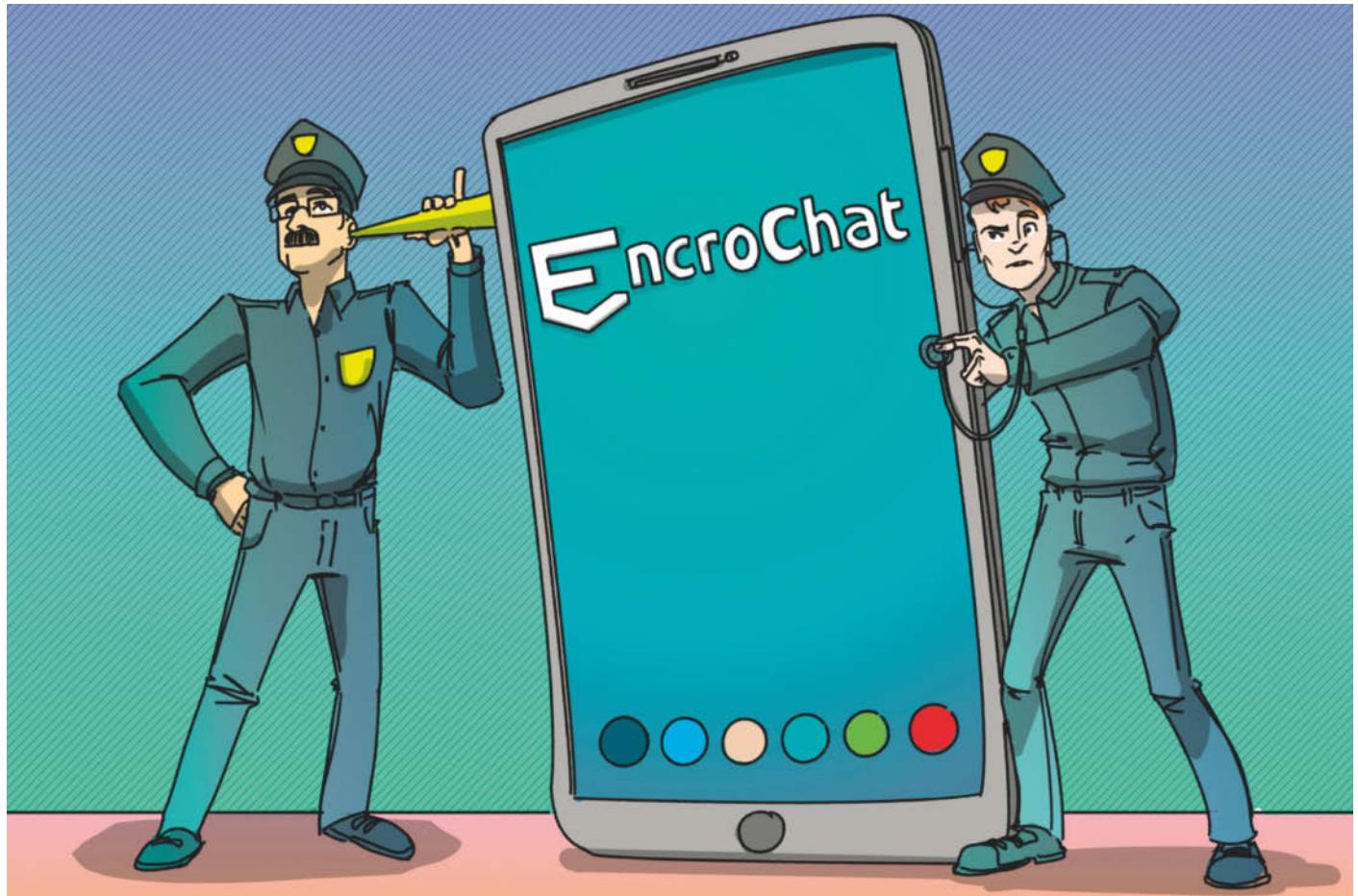


Bild: Thorsten Hübner

# Staatlich abgehörter Messenger

## Der kriminalistische Fallout von EncroChat

**Die Nachwirkungen des staatlichen EncroChat-Hacks beschäftigen Gerichte seit Monaten. Beim Knacken des vermeintlich sicheren Messengers benutzten die Ermittler technisch interessante und juristisch fragwürdige Methoden – zumindest kriminalistisch gesehen war der Erfolg aber durchschlagend.**

Von Detlef Borchers

Vor einem Jahr zapften französische und niederländische Ermittler die IT-Infrastruktur des Unternehmens EncroChat an. Die eigentliche Aktion dauerte genau 40 Minuten: So lange brauchten Spezialisten am 30. März 2020, um einen Server beim großen Hosting-Provider OVH kurz abzuschalten und vor Ort im französischen Roubaix eine neue Software zu installieren. Durch einen höchstrichterlichen Beschluss war OVH zur geheimen Kooperation mit der französischen Generalstaatsanwaltschaft gezwungen und erklärte den kurzzeitigen Ausfall mit einer „Fehlfunktion in einer der Verbindungs-karten eines Backbone-Routers“. EncroChat schöpfte offenbar keinen Verdacht.

Vom 1. April bis zum 26. Juni 2020 konnten die Ermittler dann die Nachrichten mitlesen, die die angeblich rund 60.000 Benutzer des EncroChat-Messengers verschickten. Das gesammelte Material wurde anschließend von Kriminalisten in ganz Europa ausgewertet und bildete die Grundlage für Tausende von Ermittlungen, Verhaftungen und Strafverfahren.

Auch die deutsche Polizei bekam Zugriff auf die Daten. Nach Darstellung des Bundeskriminalamts (BKA) wurden mehr als 2250 Ermittlungsverfahren eingeleitet und mehr als 750 Haftbefehle vollstreckt. In 360 bereits laufenden Ermittlungsverfahren konnten die Chat-Inhalte zur Unterstützung genutzt werden. Zudem führ-

ten sie zur Sicherstellung erheblicher Mengen Drogen und Bargeld. Steve Alter, Pressesprecher des Bundesinnenministeriums, bewertete auf Twitter die Arbeit des BKA als absolute „Weltklasse“. Doch ein Jahr nach der Aktion hat die Debatte darüber begonnen, ob die Chat-Daten als Beweismittel in Strafverfahren zulässig sind.

### Kohlenstoffeinheiten

EncroChat war ein Anbieter von „kryptierten Smartphones“, wie es das BKA ausdrückt. Es handelte sich um modifizierte Geräte – oft auf Basis des Modells Aquaris X2 vom spanischen Hersteller BQ. EncroChat nannte diese Smartphones „Carbon Units“ (Kohlenstoffeinheiten) und statte sie mit SIM-Karten des niederländischen Kommunikationskonzerns KPN aus. Eine Carbon Unit verfügte über zwei Betriebssysteme: ein normales Android und EncroChat OS. Nutzer konnten erstes booten, um ein unauffällig wirkendes Handy vorzeigen zu können.

Nur wenn stattdessen EncroChat OS hochgefahren wurde, stand der – ebenfalls EncroChat genannte und Ende-zu-Ende-verschlüsselnde – Messenger zur Verfügung. GPS, Kamera und Mikrofon waren abgeschaltet, um Überwachung auszuschließen. Außer dem Messenger bot EncroChat OS auch das VoIP-Programm EncroTalk an, über das man per Headset Audiotelefone führen konnte. Im Notfall konnten Nutzer außerdem eine spezielle PIN eingeben, die veranlasste, dass EncroChat OS samt aller Daten auf der Carbon Unit gelöscht wurde. Obwohl die Smartphones selbst schon 1000 Euro kosteten – ein originales Aquaris X2 war für etwa 300 Euro zu haben –, kassierte EncroChat für die genannten Dienstleistungen noch einmal 1500 Euro pro Halbjahr und Nutzer.

Das Unternehmen startete seinen Service 2017, nachdem im Jahre 2016 der Krypto-Provider Ennetcom durch die Polizei vom Netz genommen worden war. Großen Zulauf bekam EncroChat 2018, als aufflog, dass die Polizei auch das System IronChat der Amsterdamer Firma Cryptocom geknackt hatte. Ungefähr zur gleichen Zeit bekamen französische Ermittler einen Hinweis von Kollegen aus Großbritannien, der sie auf den Server in Roubaix aufmerksam machte. Den britischen Kriminalbeamten waren bei der Untersuchung eines Auftragsmordes Carbon Units in die Hände gefallen, deren Daten nicht gelöscht worden waren und die wohl auf den Server und seinen Standort schließen ließen.

Mit diesen Informationen konnten die französischen Spezialisten physischen Zugriff auf den Server nehmen und fertigten im Januar und Juni 2019 jeweils ein Image, also eine Kopie des Serverinhalts an, um das System in Ruhe zu analysieren. IT-Experten bauten dafür einen „EncroChat System Emulator“. Über die dem Server offenbar bekannten IMEI-Nummern rekonstruierten sie, dass mindestens 39.000 Smartphones mithilfe von EncroChat verschlüsselte Chat-Nachrichten austauschten.

Der nächste Schritt erfolgt im März 2020 und bestand wie eingangs beschrieben darin, ein eigens entwickeltes Programm auf dem Server einzuspielen. Nach Recherchen des Magazins Vice Motherboard brach diese staatliche Malware nicht die Chat-Verschlüsselung an sich. Stattdessen spielte sie ein Update an die Carbon Units aus, das die Datenlöschung per PIN lahmlegte, Passwörter abgriff und WLAN-Hotspots im Umkreis protokollierte. Vor allem aber fertigten so aktualisierte EncroChat-Smartphones Kopien der Textnachrichten im Klartext vor dem Verschlüsseln respektive nach dem Entschlüsseln an. So konnten die niederländischen und französischen Ermittler mitlesen, was im Chat verabredet wurde.

### Lauschangriff

Die Behörden bildeten dafür ein internationales „Joint Investigation Team“. Auch Großbritannien war beteiligt, durfte jedoch aus rechtlichen Gründen nicht direkt mitlesen. Insgesamt wurden von April bis Juni 2020 mehr als 100 Millionen Nachrichten der organisierten Kriminalität (OK) mitgeschnitten. „Das war so, als würden wir direkt am Konferenztisch der

Kriminellen sitzen“, erklärte die niederländische Polizeichefin Janine van den Berg im Juli 2020, als die Öffentlichkeit erstmals über die Aktion unterrichtet wurde.

Die Strafverfolger lasen, wie Dealer Drogen in Labors bestellten, wie Waffen und Autos für den Drogenschmuggel gehandelt wurden oder wie jemand einen Auftragsmord bestellte. Sie bekamen mit, wie Rauschgift aus Lateinamerika in den Seehäfen von Antwerpen, Rotterdam oder Bremerhaven und Hamburg gebracht und durch den Zoll geschmuggelt werden sollte. Sie erfuhren von Drogen, die in Schachteln mit Duplo-Bausteinen geschmuggelt wurden (von denen eine irrtümlich auf einem Kindergeburtstag landete), und sie lasen die Mitteilungen, wenn Dealer sich über gelungene Aktionen freuten: „Bro, bald sind wir Millys“ (Millionäre).

Die Ermittler bekamen auch mit, wie ein niederländischer Dealer-Ring in einer Lagerhalle schallisolierte Container als Gefängnisse für Entführungsopfer aufstellte und eine Folterkammer mit einem Zahnräderstuhl für einen Konkurrenten plante: „Wenn ich den einmal auf dem Stuhl habe, werden wir mehr wissen.“ Sie erfuhren außerdem, wer sonst noch ins Räderwerk der OK verstrickt war: In Schweden besaßen laut der Zeitung Expressen zwei Rechtsanwälte EncroChat-Handys und waren im Messenger unter den Pseudonymen „King“ und „Prince“ mit der Werbung „Ihr helft uns und wir helfen euch“ unterwegs. Als Pflichtverteidiger von Drogenhändlern verdienten sie Millionen – mittlerweile wurden sie aus der schwedischen Anwaltskammer ausgeschlossen.



Bild: Metropolitan Police London

Äußerlich waren die „Carbon Units“ von EncroChat normale Smartphones.

Als die EncroChat-Admins bereits argwöhnten, dass das automatische Löschen der Nachrichten nicht mehr richtig funktioniere, gingen die Ermittler zum Gegenschlag über. Die Aktion lief unter Decknamen wie „Venetic“, „Lemont26“ oder „Emma95“ und bestand aus konzentrierten Operationen in verschiedenen Ländern. Insgesamt waren Ermittler in 20 Staaten und überstaatlichen Organisationen beteiligt, etwa das BKA in Deutschland, die National Crime Agency (NCA) im Vereinigten Königreich, die EU-Justizbehörde Eurojust und die europäische Polizei Europol.

In den Niederlanden wurden 926 Personen verhaftet, in Belgien 125, in Großbritannien nahm die Polizei 746 Verdächtige fest. Bis heute ist die Justiz mit der Aufarbeitung dieser Fälle gut beschäftigt, vor allem in den Ländern mit Hafenstädten: In Bremen und Bremerhaven gab es rund 500 pseudonyme Nutzer von EncroChat, denen bislang 37 Verdächtige zugeordnet werden konnten. Von denen wurden wiederum 19 festgenommen. Aktuell laufen dort vier Prozesse gegen Drogendealer. In Hamburg wurden bislang 117 Haftbefehle vollstreckt, weitere 300 Ermittlungsverfahren stehen noch an. Deswegen werden derzeit 28 neue Stellen bei Gerichten und Staatsanwaltschaften eingerichtet, dazu 34 Stellen bei der Polizei. Der größte Erfolg war der Fund von 16

Tonnen Kokain im Hamburger Hafen, zusammen mit einer zweistelligen Millionensumme. Aber auch im Hinterland gibt es viel zu tun: So meldete Baden-Württemberg 146 Ermittlungsverfahren und 125 Haftbefehle gegen Personen, bei denen es gelang, den Pseudonymen der Chat-Teilnehmer realen Personen zuzuordnen.

## (II) legale Beweise

Ziemlich schnell kam mit der Veröffentlichung der Fahndungs- und Ermittlungsereignisse die Frage auf, ob der Mitschnitt von Chats bereits ein ausreichendes Beweismittel für die Verfolgung der so intern ausgeplauderten Straftaten ist. Denn beim EncroChat-Hack wurde pauschal die Kommunikation aller Nutzer eines Dienstes überwacht. In vielen Fällen bestand vor der Analyse der Chats kein Verdacht gegen die betroffenen Nutzer. Auch blieb die Frage offen, ob schon der Besitz eines EncroChat-Handys Ermittlungen rechtfertigt oder ob Carbon Units nicht auch völlig gesetzestreuen – und gut beobachteten – Benutzern gehören können, die für 3000 Euro pro Jahr ihre Privatsphäre schützen wollten. Nach einer Schätzung der französischen Ermittler lag der Anteil der Nutzer ohne kriminelle Ziele bei etwa 10 Prozent.

Im Nachrichtenmagazin Spiegel meinte der Frankfurter Strafverteidiger Oliver Wallasch dazu: „Die Behörden gehen offenkundig davon aus, dass der Zweck die Mittel heiligt. Die Maßnahme in Frankreich war weder zielgerichtet noch auf einzelne Beschuldigte beschränkbar.“ Es seien Geheimdienstmethoden angewendet worden, die in Deutschland nicht zulässig wären. Aber was folgt daraus, wenn die so gewonnenen Beweise in Deutschland genutzt werden? Ebenfalls im Spiegel erklärte ein Strafverfolger die Frage zu einer Bagatelle. Für ihn sei es klar, „dass in einem EU-Land rechtmäßig erhobene Beweismittel über den Weg der Rechtshilfe auch in anderen EU-Ländern genutzt werden dürfen. Es war dort legal, also ist es hier verwendbar.“

Ganz so einfach ist es offenbar nicht: Anfang Juli dieses Jahres verursachte ein Beschluss des Landgerichts (LG) Berlin [1] großes Aufsehen – und Empörung bei den Ermittlern. Eine Richterin am LG ließ, anders als Kollegen an anderen Gerichten in vergleichbaren Fällen, die Verwendung der EncroChat-Protokolle in der Verhandlung gegen einen Drogen-Großdealer nicht zu. In ihrer Begründung schrieb sie,

dass allein der Besitz einer Carbon Unit nicht ausreiche, jemanden unter Verdacht zu stellen, und zog einen Vergleich zu einem Menschen, der einen Bolzenschneider besitzt.

Auch die Aufzeichnung der Chats bewertete die Richterin kritisch; sie sei anlasslos ohne einen konkreten Tatverdacht durchgeführt worden. Eine solche Maßnahme greife schwerwiegend in Persönlichkeitsrechte ein. Mit diesem Beweismittel-Verwertungsverbot platzte das Verfahren in Berlin.

Ob die LG-Entscheidung Bestand hat, steht noch nicht fest. Die Berliner Staatsanwaltschaft will den Beschluss vom Kammergericht (KG) überprüfen lassen. Möglicherweise werden sich auch noch höhere Instanzen mit der Problematik beschäftigen müssen, bis geklärt ist, ob neben den in Masse erhobenen Chatnachrichten noch spezifischere Beweise vorliegen müssen, um vor Gericht eine Verurteilung zu erreichen.

## EncroChat ist tot, lang lebe ...

Das Unternehmen EncroChat verlor mit dem koordinierten Schlag der verschiedenen Ermittlungsbehörden gegen seine Kunden die Geschäftsgrundlage und ging in Konkurs, genau wie der Vorgänger Cryptocom. Doch das nächste Angebot dieser Art ließ nicht lange auf sich warten: Die kanadische Firma Sky Global zog den Dienst Sky ECC mit 70.000 Nutzern auf, der im Februar 2021 von Europol und belgischen Ermittlern geknackt wurde: Allein im Hafen von Antwerpen nutzten 6000 Drogenkuriere das System, um angelandete Ware in ganz Europa zu verteilen.

Eine kriminalistische Erfolgsgeschichte anderer Art war das Verschlüsselungsangebot „Anom“, von dem im Juni 2021 bekannt wurde, dass es von Anfang an ein Honeytrap-System des FBI und der australischen Polizei war (siehe Kasten). Trotzdem – oder deswegen – stehen bereits neue Anbieter in den Startlöchern, um mit einem „WhatsApp für Kriminelle“ einen Reibach zu machen. Möglicherweise sind Ermittlungsbehörden schon damit beschäftigt, auch dort nach Schwachstellen zu suchen.

(syt@ct.de) ct

## Literatur

- [1] LG Berlin, Beschluss vom 1.7.2021, Az. (525 KLS) 254 Js 592/20 (10/21): <https://openjur.de/u/2345547.html>
- [2] S.D. Cal., Application for a search warrant, Case No. '21 MJ01948: <https://heise.de/s/4XEm>



Bild: Metropolitan Police London

**Infolge des EncroChat-Hacks wurden unter anderem große Summen Bargeld – hier britische Pfund – beschlagnahmt.**

# Anom: Wie das FBI zum Krypto-Smartphone-Anbieter wurde

Von Christian Wölbert

Am 7. Juni dieses Jahres nahmen Ermittler aus 16 Staaten in einer koordinierten Aktion rund 800 mutmaßliche Mitglieder krimineller Organisationen fest, 70 davon in Deutschland. Auch diese Festnahmen hingen mit Krypto-Smartphones und verschlüsselten Chats zusammen. Anders als im EncroChat-Fall ein Jahr zuvor mussten die Ermittler dieses Mal allerdings keine Server oder Mobilgeräte hacken. Die US-amerikanische Bundespolizei FBI hatte die von den Verdächtigen verwendeten Telefone selbst konfiguriert und unter dem Markennamen „Anom“ in Umlauf gebracht. Kopien der meisten Nachrichten landeten automatisch auf FBI-Servern.

Wie dieser Coup gelang, beschreibt ein Durchsuchungsantrag des FBI [2]. Laut dem 30-seitigen Dokument rekrutierte das FBI-Büro San Diego im Jahr 2018 einen Krypto-Smartphone-Distributor als Informanten. Der ehemalige Drogenhändler hatte zuvor Geräte anderer Hersteller verkauft und begonnen, an einem eigenen Modell namens „Anom“ zu arbeiten. Nun bot er dem FBI an, dieses Modell zu manipulieren.

Dem Dokument zufolge integrierten das FBI und die australische Bundespolizei AFP einen Generalschlüssel („master key“) in das existierende Verschlüsselungssystem. Eine damit verschlüsselte Kopie jeder Chatnachricht ging fortan an einen Server in einem ungenannten, kooperierenden Land, wurde dort entschlüsselt und ans FBI weitergeleitet.

Die Redaktion von Vice Motherboard hat inzwischen ein Anom-Phone in die Finger bekommen: ein Google Pixel 4a, auf dem eine bislang unbekannte Android-Variante namens „Arcane OS“ läuft. Laut dem Vice-Bericht zeigt der Homescreen zur Tarnung funktionslose App-Icons. Durch Eingabe einer bestimmten PIN auf dem Lockscreen wechselt man in einen Modus, in dem nur die Uhr, die Einstellungen und ein Taschenrechner zu sehen sind. Tippt man auf den Taschenrechner, erscheint ein „Anom“-Login-Screen. Zu den weiteren Besonderheiten gehören Shortcuts zum schnellen Zurücksetzen des Telefons und eine Funktion, die die Ziffern für die PIN-Eingabe immer wieder durcheinanderwürfelt, sodass niemand

durch die Bewegungen beim Tippen auf den Code schließen kann.

Laut dem Gerichtsdokument führten FBI und AFP zunächst einen „Betatest“ durch: Die ersten 15 Geräte lieferte der Informant an Mittelsmänner mit Unterweltkontakte in Australien. Die AFP besorgte sich einen Gerichtsbeschluss und überwachte die Geräte. Dabei habe man festgestellt, dass diese ausschließlich von Kriminellen verwendet wurden.

Nach dem Test heizte das FBI durch Mundpropaganda das Interesse an, sodass mehr Geräte in Umlauf kamen. Im Juli 2020 zog die Nachfrage an, denn kurz zuvor hatte der im Artikel beschriebene EncroChat-Hack stattgefunden. Einen weiteren Schub gab es im März 2021, nachdem der Krypto-Smartphone-Anbieter Sky Global von den Behörden angeklagt worden war: Die Zahl der aktiven Anom-Nutzer sprang von 3000 auf 9000.

Ebenfalls im März 2021 erschien ein Blogeintrag, in dem ein anonymer „Sicherheitsforscher“ vor Anom warnte und zahlreiche Server auflistete, mit denen das Gerät kommunizierte. „Finger weg von Anom, wenn dir Privatsphäre und Sicherheit wichtig sind“, lautete das Fazit.

Die Warnung verhallte: Laut den FBI-Angaben blieb die Nutzerzahl bei rund 9000, bis zum Tag der Razzia. Die Nutzer verteilten sich auf über 90 Länder, mit den höchsten Zahlen in Deutschland, den Niederlanden, Spanien, Australien und Serbien. Über 300 kriminelle Organisationen hätten Anom eingesetzt, vor allem für Drogengeschäfte. Insgesamt liegen dem FBI 20 Millionen Anom-Nachrichten vor. Man kann davon ausgehen, dass die Ermittler zurzeit noch weitere Spuren aus den Chats verfolgen und dass in den nächsten Jahren weitere Festnahmen folgen werden.

Für die Ermittler hat sich der Trick also ausgezahlt, doch rechtlich betrachtet war er durchaus heikel; schließlich wurde die Kommunikation Tausender Nutzer dauerhaft überwacht, ohne dass die Ermittler im Einzelfall einen konkreten Anlass dazu hatten.

Da die amerikanische Verfassung US-Bürger vor solcher Schnüffelei schützt, baute das FBI einen „Geofence“ in Anom ein: Nachrichten von Geräten mit Standort in den USA wurden vom FBI nicht gesammelt und stattdessen automatisch an die AFP weitergeleitet, die darin lediglich nach Hinweisen auf Auftragsmorde und Ähnliches suchen sollte. Die Auswahl der AFP als Partner könnte damit zusammenhängen, dass die Datenschutzstandards in Australien vergleichsweise niedrig sind. Menschen außerhalb der USA waren für das FBI allerdings Freiwild.

In Deutschland dürften Strafvermittler nach herrschender Meinung nicht vorgehen wie das FBI im Anom-Fall, unabhängig vom Standort der Zielpersonen: Die Strafprozessordnung erlaubt Telekommunikationsüberwachung nur unter Richtervorbehalt, gegen konkrete Personen sowie bei Verdacht auf schwere Straftaten. Bei einem allgemein angebotenen Dienst wie Anom wäre aber vorab unklar, wer die Geräte nutzen wird und um welche Straftaten es gehen könnte.

Nach Einschätzung des Strafverteidigers Jens Ferner dürften Ermittler auch nicht einfach zusehen, wie über einen solchen Dienst schwere Straftaten gegen Menschen geplant werden. „Aus meiner Sicht bestehen bei Betreiben solcher Infrastrukturen Garantenpflichten für die Rechtsgüter Dritter“, sagte er gegenüber c't. Ebenso könnten Ermittler in die Lage kommen, dass sie sich des Unterlassens von Hilfeleistung (§ 323c StGB) schuldig machen.

Unabhängig davon zu betrachten ist die Frage, ob deutsche Gerichte die vom FBI zugelieferten Anom-Chats als Beweise anerkennen werden. Ferner vermutet, dass dies der Fall sein wird: „Einige Oberlandesgerichte treten sogar im EncroChat-Fall aggressiv für die Verwertung ein. Im Anom-Fall dürften sie noch weniger Bedenken haben, da es sich weniger um einen staatlichen Hack handelt als vielmehr um eine kriminalistische List der Ermittler.“

**„Finger weg von Anom, wenn dir Privatsphäre und Sicherheit wichtig sind.“**



Bild: Thorsten Hübner

# Geld statt Kohle

## Warum Kryptowährungen auf Proof of Stake umstellen wollen

Viele Kryptowährungen nutzen Blockchains mit „Proof of Work“, aus dem ein enormer Energieverbrauch resultieren kann. „Proof of Stake“ löst dieses Problem, doch das Verfahren hat auch Nachteile. Ganz ohne Proof of Irgendwas lässt sich eine Kryptowährung aber kaum realisieren.

Von Lars Hupel

**B**itcoin ist ob seines Energieverbrauches eine Umweltsau: Abermillionen Miner in aller Welt konkurrieren alle zehn Minuten darum, als erster die richtige Zahl für den nächsten Block zu erwürfeln und dafür eine Belohnung von umgerechnet über 150.000 Euro zu bekommen. Ein gutes Geschäft, bei dem aufgrund des „Proof of Work“-Mechanismus irrsinnige Strommengen wortwörtlich verheizt werden. Nötig ist das, um die Bitcoin-Blockchain vor Manipulationen zu schützen.

Bei staatlichen Währungen passen Geschäfts- und Zentralbanken darauf auf, dass niemand betrügt, etwa indem er fremdes Geld ausgibt oder die Buchführung nachträglich manipuliert. Kryptowährungen wie Bitcoin haben bewusst

keine solche Kontrollinstanz; stattdessen validiert jeder Knoten im Netzwerk eingehende Transaktionen selbst. Aber wie verhindern sie, dass Betrüger Transaktionsprotokolle manipulieren? Dazu dient der „Proof of Work“-Mechanismus.

### Würfeln, bis man Glück hat

Im Grund handelt es sich bei „Proof of Work“ um ein Würfelspiel, bei dem man ein bestimmtes Würfelergebnis erreichen muss. Welches Ergebnis passt, kann man nur durch Ausprobieren herausfinden. Glück spielt also eine große Rolle, aber wer mehr Rechenleistung investiert, also mit mehr Würfeln arbeitet, kann seine Chancen auf den Gewinn verbessern.

Der normale Betrieb läuft so ab: Ein Miner hat anstehende Transaktionen ausgewählt und ein passendes Würfelergebnis vor allen anderen Minern erhalten. Damit kann er einen neuen Block erstellen, an die Kette anfügen und im Netzwerk veröffentlichen. Die im Block enthaltenen Transaktionen gelten dann als verbucht. Für die Würfelei bekommt der Miner eine Belohnung, die vor allem seine Strom- und Hardwarekosten decken soll. Details zum Mining haben wir in [1] beschrieben.

Wollte jemand betrügen, so müsste er von diesem Schema abweichen. Das Würfelspiel selbst ist gegen Betrug kryptografisch gesichert, aber wenn er das Spiel einmal gewonnen hat, könnte ein Miner bestimmte, ihm nachteilige Transaktionen vom neuen Block ausschließen. Oder er könnte gar keine Transaktionen in seinen Block aufnehmen, um das System zu blockieren. Damit das dauerhaft von Erfolg gekrönt ist, müssten die Betrüger aber häufiger beim Proof-of-Work-Würfelspiel gewinnen als alle anderen. Das bedeutet, dass sie mehr Ressourcen aufbieten müssen als alle anderen zusammen. „Proof of Work“ soll verhindern, dass sich eine solche „51%-Attacke“ rechnet. Bei großen Netzwerken ist sie schon technisch kaum zu stemmen.

Prinzipiell könnte ein Betrüger auch versuchen, bereits verbuchte Transaktionen nachträglich zu manipulieren, indem er alternative Blöcke schürft. Aus diesen Blöcken könnte er zum Beispiel Transaktionen entfernen, mit denen er bereits für etwas bezahlt hat, und sich so das Geld illegitim zurückholen. Weil er dieses Geld danach nochmal ausgeben kann, spricht man von einem „double spend“. Die Blöcke einer Blockchain sind aber, wie der Name sagt, verkettet. Es reicht also nicht, wenn der Betrüger nur einen Block austauscht; er muss auch die folgenden Blöcke neu berechnen.

Das führt dazu, dass es zwei Varianten der Kette gibt – ein sogenannter Fork. Die Regeln besagen, dass immer die längste bekannte Kettenvariante gilt (genau genommen die, in die am meisten Rechenzeit investiert wurde). Für einen erfolgreichen Betrug muss die neue Variante also schneller wachsen als die ursprüngliche, an der alle anderen Netzwerkteilnehmer werkeln. Letztlich müsste ein Betrüger auch hier langfristig mehr Rechenleistung investieren als der gesamte Rest des Netzwerkes.

Für die Manipulationssicherheit von „Proof of Work“-Kryptowährungen ist es also entscheidend, dass es für Angreifer unmöglich oder zumindest nicht wirtschaftlich ist, über einen längeren Zeitraum mehr als die Hälfte der Mining-Leistung zu kontrollieren. Weil das Bitcoin-Mining so lukrativ ist, sind die Mining-Kapazitäten und damit die vom „Proof of Work“ erzwungene Ressourcenverschwendungen in den letzten Jahren allerdings rasant gewachsen. Was gut für die Manipulationssicherheit der Blockchain ist, wird

in Zeiten der Klimakatastrophe heftig kritisiert und von Ländern wie China, einst Vorreiter im Kryptoschürfen, auch zunehmend reglementiert.

## Ausgerechnet

Es gibt einige Alternativen zu „Proof of Work“ (siehe Kasten auf S. 136), um Blockchains und Kryptowährungen abzusichern, sie kämpfen aber jeweils mit eigenen Problemen. Eine viel gepriesene Alternative heißt „Proof of Stake“. Statt Rechenleistung zum Würfeln aufzuwenden, sollen Netzwerkteilnehmer nachweisen, in die Kryptowährung investiert zu haben. Daher kommt auch der Begriff „Stake“, der unter anderem „Anteil“ oder „Einsatz“ bedeutet. Die Idee: Wer viel Geld in die Währung investiert hat, hat ein großes Interesse daran, dass alles mit rechten Dingen zugeht. Denn Betrug würde das Vertrauen in die Währung und damit den Wert der eigenen Investition gefährden.

Aktuelle Vorreiterin beim Einsatz von „Proof of Stake“ ist die Cardano-Blockchain mit der Währung Ada. Zu Redaktionsschluss steht Ada auf Platz fünf der populärsten Kryptowährungen. Aber auch die Nummer zwei der Liste, die Ethereum-Blockchain, will mit Ethereum 2.0 auf „Proof of Stake“ umsatteln. Allerdings wurde die schon lange angekündigte Umstellung immer wieder verschoben und der aktuelle Termin „Ende 2021“ scheint alles andere als sicher zu sein.

Das Grundprinzip ist bei allen Proof-of-Stake-Systemen ähnlich: Statt Minern gibt es Validatoren. Um in diese Riege aufgenommen zu werden, hinterlegt man eine bestimmte Menge Geld. Nach einem mehr oder weniger komplizierten Schema darf jeweils ein solcher Validator einen neuen Block bilden. Im Anschluss stimmen die Validatoren per Mehrheitsentscheid darüber ab, ob der Block gültig ist. Bei dieser Abstimmung, von der die Validatoren ihren Namen beziehen, hat jeder Validator ein zur hinterlegten Geldmenge proportionales Stimmrecht, ähnlich einer Aktionärsversammlung. Wer betrügen will und einen ungültigen Block produziert, fällt bei der Abstimmung durch – und verliert seinen Einsatz. Ähnlich wie bei „Proof of Work“ erhalten die ehrlichen Validatoren eine Belohnung pro gebildetem Block.

Um erfolgreich zu betrügen, müsste ein Validator mehr als 50 Prozent des eingesetzten Kapitals und damit mehr als 50 Prozent der Stimmrechte kontrollieren.

Durch die Block-Belohnung kann allerdings ein Zinseszinseffekt entstehen: Erfolgreiche Validatoren erhalten Geld und können dieses reinvestieren, um mehr Stimmengewicht zu erhalten. Wer das nicht tut, verliert relativ gesehen an Stimmengewicht und Einfluss. Skeptiker befürchten, dass das langfristig eine Zentralisierung der Validatoren zur Folge haben könnte.

Befürworter halten dagegen, dass auch Proof-of-Work-Chains wie Bitcoin mit einer Zentralisierung der Miner zu kämpfen haben. Neueinsteiger haben dort kaum eine Chance, erfolgreich in das Streben nach immer mehr Rechenkapazität einzusteigen. „Proof of Stake“ sei hier zumindest weniger anfällig und erlaube durch die Abkehr vom Ressourcenzwang einen leichteren Einstieg.

## Nichts zu verlieren

Ebenfalls noch umstritten ist, wie stabil Blockchains auf Proof-of-Stake-Basis gegenüber Forks sind. Die können nicht nur wie oben erklärt auftreten, wenn jemand betrügen will. Sie entstehen unter anderem auch infolge von Upgrades, wenn die Änderung kontrovers ist: Ein Teil des Netzwerks schließt sich dem Upgrade an, der Rest bleibt beim alten Protokoll. Bitcoin hat in der Vergangenheit schon mehrere solche „Hard Forks“ durchgemacht,



Bild: Bitmain

**Der Energieverbrauch von „Proof-of-Work“ hat enorme Ausmaße erreicht. Das Bild zeigt ein 25-Megawatt-Rechenzentrum zum Bitcoin-Schürfen, das das chinesische Unternehmen Bitmain in Texas betreibt.**

wodurch Abkömmlinge wie „Bitcoin Cash“ und „Bitcoin Gold“ entstanden sind. Da ein Bitcoin-Miner stets nur an einem Block und damit nur an einem Ende des Forks mitwürfeln kann, muss man sich als Betreiber für eine der Varianten entscheiden (oder seine Mining-Ressourcen aufteilen).

Demgegenüber steht Proof of Stake: Sofern sie ihn vor der Spaltung gesetzt haben, halten Validatoren ihren Einsatz bei einem Fork in beiden Kettenvarianten zugleich und können sich daher an beliebigen Ketten parallel beteiligen. Dieses Problem wird auch als „nothing at stake“ („nichts steht auf dem Spiel“) bezeichnet, weil Teilnehmer einen Betrug versuchen könnten und trotzdem keinen Schaden erleiden, wenn letztlich die korrekte Kettenvariante gewinnt. Technische Gegenmaßnahmen beruhen zum Beispiel auf einer erzwungenen Verzögerung zwischen der Einräumung des Rechts, neue Blöcke anzufertigen, und der Möglichkeit, den eigenen Einsatz wieder zurückzuerhalten. Vereinfacht gesagt ist die Idee, dass bösartiges Verhalten so rechtzeitig auffallen und bestraft werden kann.

Daneben wird noch diskutiert, ob „nothing at stake“-Szenarien bei Hard-Forks relevante ökonomische Effekte haben könnten, etwa durch Auswirkungen auf den Währungskurs.

## Effizienz

Einen Vorteil haben Proof-of-Stake-Währungen in jedem Fall: Sie benötigen weniger Rechenleistung und sind viel effizienter. Dass keine exorbitanten Energiemengen für den Mining-Prozess investiert werden müssen, schont die Umwelt und senkt auch den nötigen Ressourcenaufwand pro Transaktion drastisch. Genaue Zahlen aus wissenschaftlichen Erhebungen gibt es dazu allerdings nicht.

Blockchains werden aber auch noch von anderen Performance-Problemen geplagt. Zum Beispiel werden in Bitcoin oder Ethereum sämtliche Transaktionen serialisiert: Alle Miner weltweit arbeiten an derselben Aufgabe, den nächsten Block auszuwürfeln. Ethereum nimmt sich in Version 2.0 daher gleich noch mehr vor und will in Koordination mit der Umstellung auf „Proof of Stake“ die Blockchain in 64 sogenannte „Shards“ aufteilen. Jeder Shard ist nur für einen Teil der gesamten Transaktionen zuständig. Das erhöht den möglichen Gesamtdurchsatz, aber es verkompliziert auch die Umstellung.

WIE MAN SEIN ETH EINSETZT

## Stake deine ETH, um Ethereum-Validator zu werden

Staking ist ein öffentliches Gut für das Ethereum-Ökosystem. Du kannst helfen, das Netzwerk zu sichern und dabei Belohnungen verdienen.

Fang an zu staken

Bild: ethereum.org

**Ethereum erhofft sich viel von der Umstellung auf Proof of Stake. Nachhaltiger und zugänglicher soll Ethereum 2.0 werden und außerdem mehr Transaktionen pro Sekunde ermöglichen.**

## Fazit

„Proof of Stake“ gilt als designierter Nachfolger von „Proof of Work“ und soll dessen ökologische Probleme lösen. Unter anderem Cardano hat bereits vorgelegt, mehrere andere Blockchains wollen folgen. Im Detail versuchen diese Ketten auf unterschiedliche Art und Weise, die Nachteile von Proof of Stake auszugleichen. Welche Implementierungen letztlich das Rennen machen und ob sich Proof of Stake über-

haupt gegen die Masse der anderen Kryptowährungen durchsetzen kann, ist noch nicht abzusehen. (syt@ct.de) ct

## Literatur

- [1] Mirko Dölle und Christof Windeck, Krypto-Hype, Bitcoin, Ethereum & Co: Was Sie über Kryptowährungen wissen müssen, c't 11/2021, S. 18
- [2] Benjamin Kraft, Rückblick: Ein Jahr Team Heise Falter bei Folding@home: <https://heise.de/-/6035027>

## Zoo der Beweisverfahren

Neben „Proof of Stake“ gibt es noch andere Mechanismen, die sich anschicken, das Ressourcenproblem von „Proof of Work“ (PoW) zu lösen. Die simpelste Lösung ist es, das öffentliche Mining schlicht zu unterbinden. Stattdessen dürfen nur bestimmte, extern autorisierte Netzwerkknoten neue Blöcke erzeugen und validieren. Dieses Verfahren heißt „Proof of Authority“ und wird beispielsweise in privaten Ethereum-Netzwerken eingesetzt. Der gravierende Nachteil ist, dass man den Betreibern des Netzwerks vertrauen muss – genau so eine Situation wollen die meisten Kryptowährungen aber vermeiden.

Ein anderer Vorschlag ist, einen „Proof of Work“-Algorithmus zu verwenden, der einen gesellschaftlichen Nutzen hat, etwa über wissenschaftliche Berechnungs-Projekte wie Folding@home [2]. In der Regel benötigen diese Projekte aber eine zentrale Koordinierung, um die Problemstellungen zu selektieren und validieren, was sie für Kryptowährungen wiederum unattraktiv macht.

Eine neuere PoW-Alternative heißt „Proof of Space“. Die derzeit recht bekannte Währung Chia setzt auf das Verfahren, das statt Rechenpower kontinuierlich bereit gehaltenen Massenspeicher erfordert. In der Theorie ist „Proof of Space“ umweltschonender, denn Festplatten oder Flashspeicher benötigen weit weniger Strom für den Betrieb als PoW-Miner. Praktisch kostet aber auch die Produktion von Massenspeichern Ressourcen und wird von Chia massiv befeuert – wiederum ohne, dass diese Massenspeicher irgend etwas Sinnvolles täten.

Eher ein Kuriosum ist „Proof of Elapsed Time“: Dabei handelt es sich um eine Entwicklung von Intel. Spezielle CPU-Befehle erzwingen, dass der Prozessor einfach mal nichts tut. Garantiertes Däumchendrehen, das wortwörtlich Zeit kostet. Intern basiert dieses Verfahren auf sogenannten „Trusted Execution Environments“ und erfordert Vertrauen in den Hardwarehersteller.

NEU

# Router sicher im Griff!

## c't FRITZBOX

Absichern • Erweitern • Tunen

### Komfortabel telefonieren

Gebrauchte Businesstelefone mit Fritzbox verknüpfen  
Abhörsicher mit FritzOS telefonieren  
Funklöcher stopfen mit Fritzbox und Raspi



### WLAN ausreizen

Wie die Verbesserungen von Wi-Fi 6 wirken  
Das bringt AVMs erster Repeater für Wi-Fi 6  
Im Test: Fünf WLAN-Router gegen die Fritzbox  
Mit WPA3 extrasicher funkeln



### Optimal vernetzen

Was für Ihre nächste Fritzbox wichtig ist  
Fritzbox: DynDNS mit IPv6 leicht gemacht  
Internetausfällen vorbeugen



### Fritzbox niet- und nagelfest

Heimnetz absichern • Tracking verhindern • Privatsphäre schützen  
VPN trotz Kabelanschluss einrichten • Malware draußen halten



### c't FRITZBOX 2021

Wie Sie Ihre Fritzbox absichern, optimal vernetzen und Ihr WLAN ausreizen können zeigt Ihnen das neue Sonderheft c't Fritzbox. Auch ein Notfallplan, falls der Internetzugang einmal ausfallen sollte, ist mit dabei. Mit dieser Sonderausgabe holen Sie alles aus Ihrem Fritzbox-Router heraus.

Auch als Set-Angebot inkl. Buch „FRITZ!Box-Bibel“ erhältlich!

[shop.heise.de/ct-fritzbox21](http://shop.heise.de/ct-fritzbox21)

Heft + PDF  
für nur

19,90 € >



heise shop

[shop.heise.de/ct-fritzbox21](http://shop.heise.de/ct-fritzbox21)

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

© Copyright by Heise Medien.

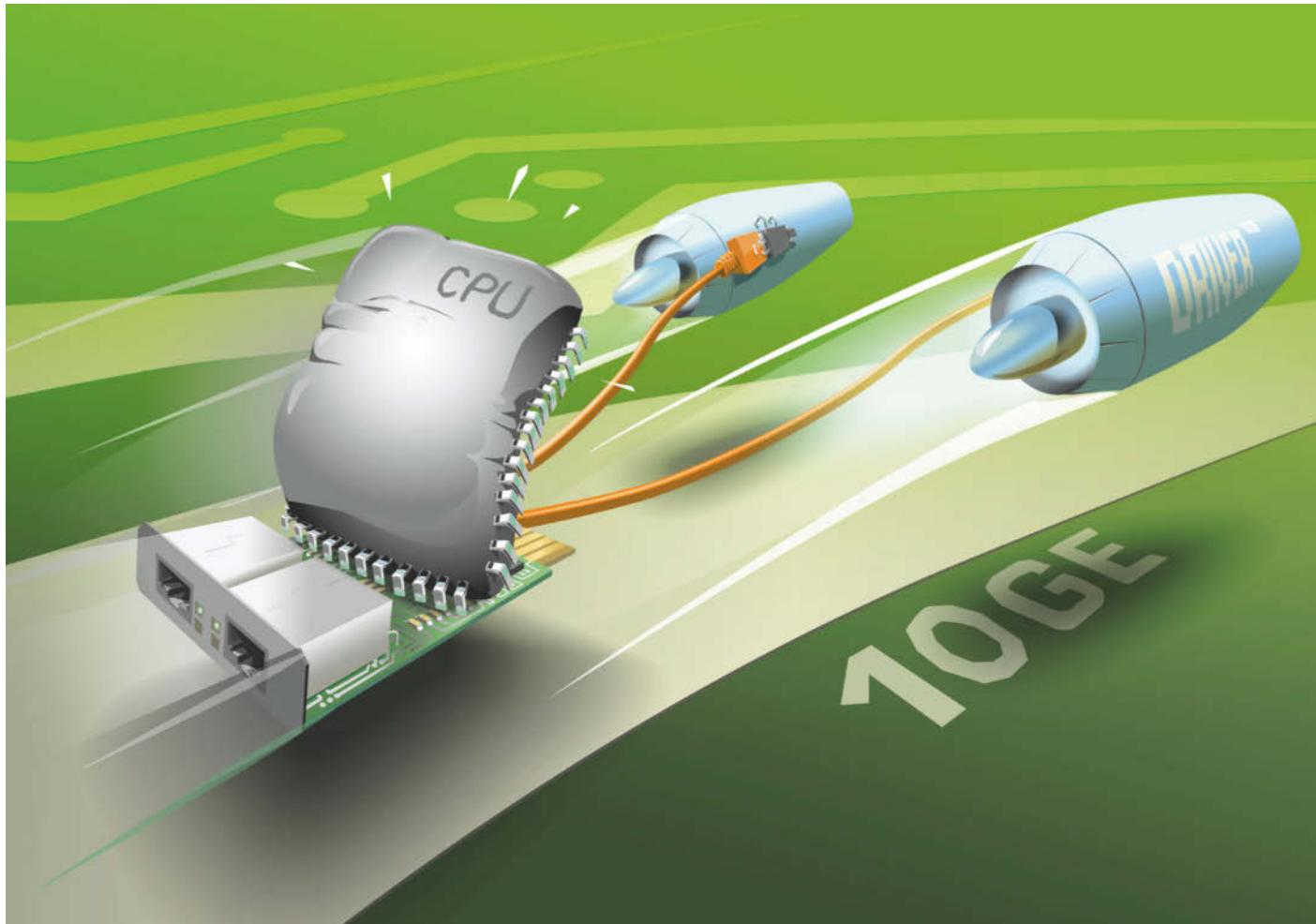


Bild: Rudolf A. Blaha

# Erweckung und Entlastung

## 10-Gigabit-Ethernet: Windows-Treiber optimal programmieren, die besten Netzwerkkarten wählen

**Die Netzwerktechnik 10-Gigabit-Ethernet über Kupferkabel wird langsam erschwinglich und verspricht viel Zeitgewinn bei der Übertragung großer Dateien. Doch mit der verzehnfachen Datenrate sind viele Netzwerkkartentreiber überfordert und bremsen den PC aus. Dagegen helfen einige Programmierertricks und unsere Tipps für die Kartenwahl.**

Von Christoph Lüders und Martin Winkler

Viele Ethernet-Installationen eignen sich nicht nur für Übertragungen mit 1 Gigabit pro Sekunde (GBit/s), sondern auch für 10 GBit/s. Dafür kommen sogar etliche ältere Cat-5e-Verkabelungen in Frage, sofern die Strecken 50 Meter nicht überschreiten [1, 2]. Dann erspart man sich das teure Verlegen neuer Kabel und rüstet lediglich Switch, NAS und PCI-Express-LAN-Karten in den PCs auf. Dank allmählich sinkender Preise erscheint dieser Schritt besonders für kleine und mittlere Unternehmen immer interessanter. Denn wenn große Dateien in einem Zehntel der bisher üblichen Zeit vom NAS zum PC gelangen, schrumpfen

auch die Wartezeiten der Spezialisten, die Daten bearbeiten.

Die Vorfreude kann allerdings schnell in Ernüchterung umschlagen, wenn man alle Netzwerkbausteine aufgerüstet und dann den Durchsatz von gängigen Windows-PCs auf den neuen 10-GE-Strecken misst: Viele liefern nur das Doppelte einer Gigabitstrecke, nicht aber das Zehnfache.

Wenn man die Fehlersuche methodisch angeht und dabei nachinstallierte Software deaktiviert, kommt man schnell darauf, dass fremde Netzwerktreiber den Verkehr bremsen (siehe ct.de/y4ch). Kandidaten dafür sind VPN-Programme, Anti-

**ct Hardcore**

viren- oder Personal Firewalls. Auch Traffic Scheduler, Virtualisierer, Monitoring-Tools oder mit dem Netzwerk-Tool Wireshark installierte Analysetools wie WinPcap können bremsen. Sobald man Windows von solchen Treibern befreit, schöpft es die 10-GE-Leitungen durchaus aus. Dafür eignet sich sogar ein älterer PC mit Core-i3-CPU und einer 90-Euro-Asus-Karte, den wir im Rahmen einer Übersicht zu Multigigabit-Ethernet verwendet haben [1].

Aber den bremsenden Treiber zu kennen hilft nicht, wenn man die Software für die tägliche Arbeit braucht, zu der er gehört. Und schon gar nicht lässt sich so die Ursache beseitigen.

Daher zunächst etwas Licht ins Dunkel: Auf einer 10-GE-Leitung lassen sich mit dem üblichen Transmission Control Protocol (TCP) maximal 1,25 GByte/s übertragen. Dafür lädt die CPU die Nutzlast von der Platte, verpackt sie in Datenpakete und gibt sie für den Versand an die Netzwerkkarte weiter. Umgekehrt entpackt sie die empfangenen Pakete und schreibt sie auf die Platte. Bei einer Paketgröße von 1500 Byte geht so pro Richtung alle 1,2 Mikrosekunden ein Paket auf die Reise. Jumbo Frames mit Größen bis 16.000 Byte klammern wir aus, weil es dafür bisher keine herstellerübergreifende Spezifikation gibt.

Damit bleiben einem modernen PC mit 4 GHz Takt pro Kern nur 5000 Takte, um ein einzelnes Paket zu verarbeiten – das heißt zusammengefasst: empfangene Pakete in Puffer speichern und sie von dort durch die diversen Protokollsichten zur Anwendung durchschleusen.

Ein frisch aufgesetztes Windows kommt damit aus, wenn es keine weiteren Aufgaben hat. Wenn jedoch beispielsweise Mitschneiden oder Filtern des Netzwerkverkehrs oder Ver- und Entschlüsseln von VPN-Paketen hinzukommen, braucht eine übliche CPU länger als 1,2 Mikrosekunden, um Pakete zu versenden oder zu empfangen – so wird sie zum Flaschenhals der 10-GE-Strecke.

## Programmierer-Perspektive

Das Problem können am ehesten die Programmierer der Netzwerktreiber beseitigen. Doch wenn man deren Strategien kennt, kann man davon auch als Anwender profitieren.

Zum Beispiel könnten Programmierer die Arbeit auf mehrere Kerne verteilen. Dagegen spricht aber, dass sich dafür nur

manche Verarbeitungsschritte eignen und dass das Verteilen so viel Synchronisationsaufwand kostet, dass es kaum lohnt. Alternativ könnten die Programmierer die Hände in den Schoß legen und es den Anwendern überlassen, in Systeme mit x-fach schnelleren CPUs zu investieren. Das schmälerst aber die Zielgruppe für ihre Software. Der beste Ausweg besteht daher darin, die Treiber zu modernisieren. Dafür gibt es verschiedene Ansätze. Der einfachste besteht darin, möglichst viele Aufgaben an die Netzwerkkarte auszulagern (Task Offloading).

Da bietet sich zunächst die Berechnung und Verifikation der Prüfsummen an (Checksum Offloading). Wenn der Empfänger ein Paket erhalten hat, rechnet er die Prüfsumme gegen und wenn sein Resultat von der Angabe im Paket abweicht, gilt das Paket als fehlerhaft, sodass er es nicht quittiert und stattdessen auf die Sendewiederholung wartet. Deshalb enthalten alle IPv4-Pakete Prüfsummen für den Header und zusätzlich stehen in allen TCP- und UDP-Paketen Prüfsummen für Header und Nutzdaten.

Das Checksum Offloading kennt man schon von Netzwerkkarten für ältere Ethernet-Spezifikationen. Der Unterschied zu 10-GE-Karten liegt darin, dass sie die Prüfsummen bei voller 10-GE-Geschwindigkeit berechnen müssen (1,25 GByte/s). Allerdings ist Checksum Offloading auch eine Voraussetzung für das Auslagern weiterer Aufgaben an die Netzwerkkarte, denn dann kann sie auch Nutz-

daten und Header zu vollständigen Paketen zusammenfügen (Large Segment Offloading, dazu später mehr).

## Spaghetti gestückelt

Natürlich kann der Treiber der CPU nicht sämtliche Aufgaben ersparen. Zum Beispiel muss sie beim Paketversand für jede Protokollsicht die richtigen Header selbst vor die Nutzdaten schreiben und beim Empfang entfernen. Und genau bei diesen Vorgängen lässt sich durch Neuprogrammierung ebenfalls viel Zeit sparen.

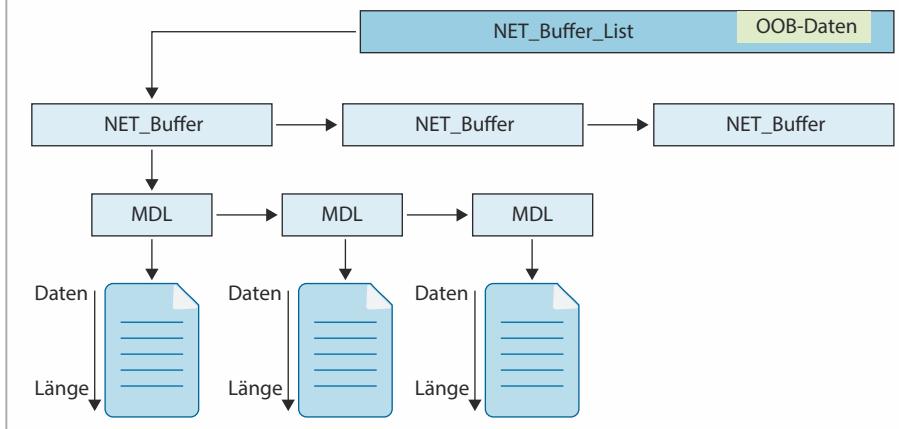
Man kann die Methoden grob in drei Teile aufteilen: Kopiervorgänge im Arbeitsspeicher sparen, individuelle Analysevorgänge reduzieren und Nutzdaten möglichst als große Segmente zusammenfassend bearbeiten und an Netzwerkkarten auslagern.

Alle drei fußen auf Microsofts Network Driver Interface Specification (NDIS). Allerdings hat Microsoft die NDIS-Architektur im Laufe der Jahre an etlichen Stellen verändert und optimiert. Lange Zeit haben Entwickler Treiber gemäß der NDIS-Version 5 programmiert, obwohl NDIS 6 schon seit Windows Vista eingeführt ist. Das erscheint vielleicht unproblematisch, denn NDIS-5-Treiber laufen auch auf Windows 10, das längst für NDIS 6.8x ausgelegt ist.

Doch NDIS 5 setzt stillschweigend voraus, dass Treiber zur Abarbeitung der Netzwerkaufgaben Kopien der Daten im RAM anlegen; das gilt bei NDIS 5 als guter Stil. Und für Entwickler stellt es geringe

## NET\_Buffer

Microsoft hat mit der NDIS-Version 6 im Windows-Netzwerkstack eine indirekte Datenverwaltung eingeführt, die unterm Strich die CPU-Belastung drastisch senkt, allein schon, weil Netzwerktreiber die Paketdaten nicht mehr im Speicher hin- und herschieben müssen.



Anforderungen, da die zu bearbeitenden Daten in einem kontinuierlichen Speicherbereich liegen und so auch leicht zu analysieren sind. Die Analysen erfolgen mittels eigener Routinen, und Treiber bestimmen dabei zum Beispiel, ob sie ein IPv4- oder IPv6-Paket vor sich haben, ob es ins Internet reist oder im lokalen Netzwerk bleibt und dergleichen mehr. Wenn das aber jeder installierte und aktive Treiber aufs Neue macht, vergeudet das Rechenzeit.

Beispielsweise muss das Tuning-Tool cFosSpeed, das die Autoren dieses Beitrags entwickelt haben, bei jedem Paket prüfen, ob es im LAN bleibt oder ins Internet geht, da der Treiber nur den Internetverkehr regelt (Traffic Shaping), nicht aber den lokalen. cFosSpeed liegt seit rund einem Jahr als optimierter NDIS-6-Treiber vor und braucht inzwischen nicht mehr als rund 700 CPU-Takte pro Paket.

Aus der Kopierstrategie erklärt sich, warum ein gemäß NDIS 5 programmiertes Treiber ein Windows-10-System bei 10GE ausbremst – es liegt an der aufwendigen Jonglage der Daten im Speicher, die mit dem eigentlichen Paketversand oder -empfang nur indirekt zusammenhängt. Ein Beispiel dafür ist der alte Wireshark-Treiber WinPcap, der gemäß NDIS 5 programmiert ist.

Eine zweite große Versuchung, Pakete zu kopieren, ergibt sich daraus, dass für alle verwendeten Layer die zugehörigen Header je nach Richtung hinzugefügt oder entfernt werden müssen. Zum Beispiel muss beim Versand vor jedem IP-Paket ein Ethernet-Header angebracht werden. Wie programmiert man das? Ein einfacher Ansatz ist, alle Daten um 14 Bytes zu verschieben, um Platz für den Ethernet-Header zu schaffen und diesen dann zu füllen. Das kostet aber Zeit.



Ab NDIS 6 kann man viele derartige Aufgaben abkürzen und so weniger CPU-Zyklen verbrauchen. Alle drei Strategien – Kopien vermeiden, Analysen reduzieren und große Segmente auslagern – sind freilich schneller aufgezählt als erklärt; insbesondere das Einsparen von Kopiervorgängen setzt gute Kenntnisse der Datenstrukturen von NDIS 6 voraus. Daher gehen wir zunächst darauf ein.

### NDIS-6-Datenstrukturen

NDIS 6 definiert für jedes Paket einen NET\_BUFFER. Mehrere NET\_BUFFER werden zu einer NET\_BUFFER\_LIST zusammengefasst. Letztere enthält einen oder mehrere verkettete NET\_BUFFER mit den Paketdaten und außerdem einen Bereich für Out-of-Band-Daten (OOB). Darin notiert Windows beim Versand oder die Netzwerkkarte beim Empfang Merkmale der Pakete in der NET\_BUFFER\_LIST. Beispielsweise schreibt Windows dort hinein, ob für den Versand die Prüfsumme berechnet werden muss und die Netzwerkkarte vermerkt beim Empfang, ob die Prüfsumme korrekt war.

Auch steht dort das verwendete Layer-3-Protokoll (IPv4 oder IPv6), sodass das nicht jeder Netzwerktreiber selbst ermitteln muss.

Jeder NET\_BUFFER enthält eine verkettete Liste von Memory Descriptor Lists (MDL), die die zugehörigen Speicherbereiche bezeichnen. Das ist cool, denn damit müssen die Daten eines Pakets nicht am Stück im Speicher liegen und auch nicht zur Weiterbearbeitung kopiert werden, zum Beispiel wenn man den Daten einen IP-Header voranstellen will. Stattdessen kann der Netzwerkstack den IP-Header irgendwo im Speicher ablegen und dessen Adresse in eine MDL eintragen. Setzt man diese vor die übrigen MDLs, ist das Paket schon fertig für den nächsten Bearbeitungsschritt.

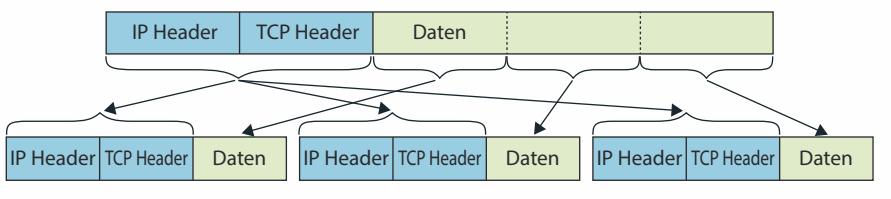
Ohne die MDL-Verwaltung müsste der Protokollstapel einen Speicherblock für den IP- und TCP-Header und die Nutzdaten reservieren, den IP-Header dort hinkopieren und schließlich die TCP-Daten hinter den IP-Header legen. Diese Vorgehensweise ist mit NDIS 5 völlig okay, aber frisst Zeit und Speicher, sodass man mit NDIS 6 einen großen Bogen darum machen will.

Wegen der Referenzierung anhand von MDLs dürfen Treiberprogrammierer natürlich nicht davon ausgehen, dass die Elemente eines Pakets am Stück im Speicher liegen. Daher können sie etwaige eigene, für NDIS 5 ausgelegte Analyseroutinen nicht verwenden. Stattdessen sollten sie auf den NDIS-6-Style der Paketanalyse umsteigen.

Dafür kann man wiederum die NET\_BUFFER\_LIST heranziehen, denn in ihrem Info-Feld stehen bereits die wichtigsten Angaben. Beim Versand schreibt sie der Netzwerkstack hinein, beim Emp-

## LSO

Mit dem Large Segment Offload bearbeitet der Netzwerkstack große Datenmengen am Stück und überlässt die Kleinarbeit der Netzwerkkarte. Das hilft besonders PCs mit älteren CPUs, eine 10-Gigabit-Ethernet-Leitung auszureizen.



# Optimaler Schutz mit Heise-Expertise

Exklusiver  
Frühbucher-  
Rabatt!



Sie wollen Ihre IT absichern? Dann vertrauen Sie unserem Angebot aus Workshops, Webinaren und Konferenzen – in gewohnter Heise-Qualität: unabhängig, praxisnah, kompetent.

## Unser Angebot

### IT-Sicherheit

Notfallplanung und  
Notfallübungen

30. August – 1. September

WORKSHOP

### heise Security

Tour

9. September

KONFERENZ

### Cybersicherheit

Aktuelle Angriffstechniken  
und ihre Abwehr

9. – 10. September

WORKSHOP

### secIT Special – Cybersicherheit für KMU

16. September

KONFERENZ

### KRITIS – Zusätzliche Prüfverfahrens- kompetenz für § 8a BSIG

20. – 21. September

WORKSHOP

### Sicherer Einsatz von Microsoft 365

7. Oktober

WORKSHOP

Mehr Informationen:

[heise-academy.de/security](http://heise-academy.de/security)

© Copyright by Heise Medien.

fang die Netzwerkkarte. Streicht der Programmierer seine selbstgeschriebene Routine aus dem Code und liest die Merkmale einfach aus dem Feld NET\_BUFFER\_LIST\_INFO aus, spart er CPU-Zyklen. Das gilt beispielsweise für Merkmale wie das IP-Protokoll (IPv4 oder IPv6, etc.).

Ein anderes Beispiel ist die Prüfsummenberechnung. Es gibt Fälle, in denen ein Treiber die Prüfsumme tatsächlich selbst mittels einer eigenen Routine berechnen muss, etwa wenn der Benutzer die Funktion in einer Karte abschaltet (nicht empfehlenswert). Daher ist es für Entwickler verlockend, ihre eigene Routine grundsätzlich zu benutzen. Aber dann spannen sie für die Prüfsummenberechnung immer die CPU ein. Stattdessen sollte man immer von Fall zu Fall entscheiden und wann immer möglich die von der Karte berechnete Prüfsumme auslesen.

Und schließlich können ab NDIS 6 verschiedene Schichten des Protokollstapels auf denselben Speicherbereich zugreifen. Das ist nützlich, wenn Nutzdaten im Protokollstapel von Schicht zu Schicht und von Treiber zu Treiber fließen, denn jeder Treiber analysiert die Daten vor der Bearbeitung. Typischerweise untersuchen Treiber den Ethernet-Header, den IP-Header und eventuell den TCP-Header mitsamt aller Optionen. Da zu jedem Zeitpunkt klar ist, welcher Treiber gerade auf eine bestimmte NET\_BUFFER\_LIST zugreifen darf, muss er die Daten gar nicht erst in eigene Bereiche kopieren, um sie zu analysieren.

Die NDIS-5-Architektur fordert aber gerade das und ferner auch die Analyse mittels eigener Routinen. Mit NDIS 6 entfallen der Kopievorgang und die eigenen Routinen, sofern sich der Entwickler die Mühe macht, den zugehörigen Mechanismus

zu verwenden – also einfach in die NET\_BUFFER\_LIST und darin enthaltene NET\_BUFFER reinschauen. So spart er CPU-Zyklen und kann etwa den Durchsatz auf 10GE-Leitungen drastisch beschleunigen. Ein Beispiel dafür ist der Wireshark-Treiber Npcap (NDIS 6), der WinPcap (NDIS 5) ersetzt.

## Segmentierung

Erheblichen Zeitgewinn bringt es auch, wenn der Treiber die Bearbeitung ganzer Segmente an die Netzwerkkarte delegiert, denn so lässt sich die Anzahl der NDIS-Aufrufe und damit die Menge der CPU-Zyklen minimieren.

Mit Large Segment Offloading (LSO) kann Windows Nutzdaten, die normalerweise auf mehrere TCP-Pakete verteilt werden, zu einem Segment zusammenfassen und nur diesem den Header voranstellen. So kann Windows zum Beispiel 64 kByte mit einem einzigen Aufruf des Netzwerktreibers verschicken. Bei herkömmlicher Abarbeitung können dafür leicht 30 bis 40 Aufrufe ablaufen.

Voraussetzung für LSO ist, dass die Daten zu der gleichen TCP-Verbindung gehören, im Speicher in korrekter Reihenfolge referenziert sind und identische Header bekommen sollen. Dann stellt Windows dieser Struktur einen einzigen TCP/IP-Header voran. Dank MDLs gelingt das ohne zu kopieren. Für alle im Stack liegenden Treiber sieht dieser Block wie ein riesiges TCP/IP-Paket aus (oft 30 kByte, maximal 64 kByte). Eine LSO-fähige Netzwerkkarte zerteilt ein solches Segment in viele kleine Pakete, bringt an jedes den Header an, der dem großen Paket voransteht, berechnet und trägt die Prüfsummen ein und versendet sie selbstständig. Die Paketgröße liest sie aus dem NET\_BUFFER aus.

Auch die Netzwerktreiber profitieren von LSO, denn sie müssen nur die Header-Informationen der großen LSO-Pakete analysieren und es sind weniger NDIS-Aufrufe erforderlich. Unterm Strich lässt sich der Aufwand mit LSO mindestens halbieren.

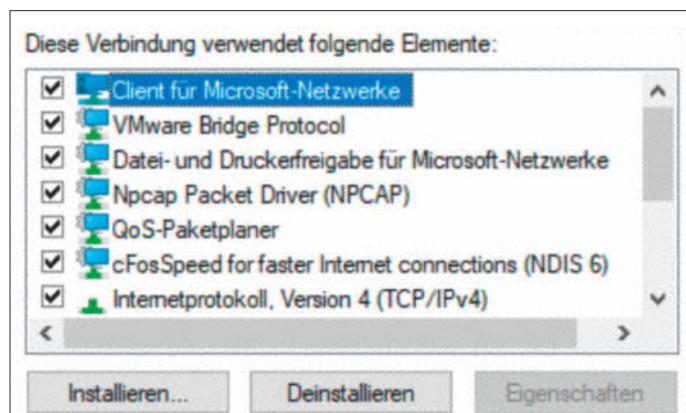
## Receive Segment Coalescing

Das Gegenstück zu LSO beim Versand bildet Receive Segment Coalescing (RSC) beim Empfang. Microsoft hat die Technik mit NDIS 6.4 eingeführt. Mittels der RSC-Funktion fasst eine Netzwerkkarte mehrere TCP/IP-Pakete zusammen und reicht sie als ein Segment weiter. Dabei darf sie nicht beliebig lange auf Pakete warten, weil die Latenz umso länger wird, je später die Karte ein Segment an den Treiber weitergibt.

Allerdings ist die Frist doch etwas länger als man zunächst denken könnte, denn die Netzwerkkarten können sich bei der RSC-Behandlung auf die Funktion Interrupt Moderation stützen. Diese wurde ursprünglich entwickelt, um rechenzeitlich teure Kontextwechsel der CPU zu vermeiden. So muss die Karte den Prozessor nicht mehr für jedes empfangene Paket unterbrechen, sondern nur einmal für mehrere Pakete. Die Länge der Intervalle zwischen den Interrupts legt die Karte fest. Nahezu alle modernen Netzwerkkarten bringen die Funktion Interrupt Moderation mit. Bei manchen lässt sich die Funktion abschalten, bei anderen ist sie grundsätzlich eingeschaltet.

Jedenfalls: Wenn die Karte ohnehin die Interrupt Moderation nutzt, dann kann sie zwischen zwei Interrupts eingegangene Pakete zu einem Segment zusammenfassen und in NET\_BUFFER schreiben. Wie bei LSO müssen dafür die aufeinanderfolgenden Pakete zu einer TCP-Verbindung gehören und die Header müssen gleich sein. In die OOB-Daten der NET\_BUFFER\_LIST trägt die Karte ein, wie viele Pakete sie zusammengefasst hat und ob die Prüfsummen korrekt waren. RSC impliziert also Checksum Offloading in Empfangsrichtung. In unseren Tests wurden bei Volllast durchschnittlich rund 20 Pakete zusammengefasst.

RSC reduziert so wie LSO die Anzahl der NDIS-Aufrufe und erspart den Treibern und dem Netzwerkstack das Kopieren der Daten vor den Analyseschritten; stattdessen können sie dafür einfach die von der Karte angegebenen Header-Informationen verwenden.



**Treiber, die gemäß älteren NDIS-Spezifikationen geschrieben sind, können erhebliche CPU-Last verursachen. Hat man sie identifiziert, kann man sie in den Adaptereinstellungen leicht deaktivieren.**

Beide Funktionen, sowohl LSO als auch RSC, stellen höhere Anforderung an die Hardware und den Treiber der Netzwerkkarte. Sie braucht eine schlauere CPU, etwas RAM oder DMA-Zugriff auf den Hauptspeicher und Funktionen zum selbstständigen Zusammenführen und Zerteilen von Paketen.

## Treibertricks und Kartenwahl

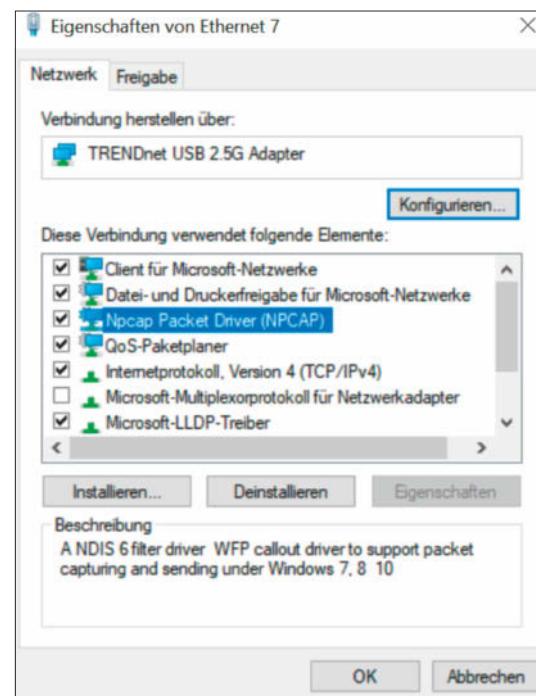
Wer 10-Gigabit-Ethernet ausschöpfen will, sollte nach Netzwerkkarten Ausschau halten, die viel Hardware-Unterstützung bieten, also neben dem obligatorischen Checksum Offloading zumindest LSO. LSO findet man auch bei preisgünstigen NBase-T/10G-Karten wie Aquantia AQC107 auf besagter 90-Euro-Asuskarte aus unserem Test-PC. RSC bringen derzeit nur Karten der Oberklasse mit, aber das könnte sich mit zunehmender 10GE-Verbreitung ändern. Wir haben für Messungen und NDIS-6-Optimierungen zwei Exemplare der Broadcom-Karte NetXtreme II BCM957810A1008G verwendet. Ein weiteres Beispiel mit LSO und RSC ist die Lenovo-Karte ThinkSystem QL41134 (ab 400 Euro).

Ist die Karte installiert, sollte man die Treibereinstellungen öffnen und sicherstellen, dass Checksum Offloading und andere Hardware-Beschleunigungen aktiviert sind („Netzwerk- und Freigabecenter/Adapter-Einstellungen ändern/Adapter/Eigenschaften“, dann Konfigurieren und Erweitert öffnen).

Wenn Sie Software verwenden, die eigene Netzwerktreiber installiert, prüfen Sie, für welche NDIS-Version diese ausgelegt sind. Der Rechner und die Netzwerkkarte sind am schnellsten, wenn alle Treiber mindestens gemäß NDIS 6.3 arbeiten. Daher empfiehlt es sich, nach der Installation neuer Netzwerk-Software zu prüfen, ob das Offloading aktiviert ist.

Auch installieren manche Antiviren-Programme ihre Netzwerktreiber stillschweigend. Man sieht aber in „Netzwerk- und Freigabecenter/Adapter-Einstellungen ändern/Adapter/Eigenschaften“, welche Treiber in den Netzwerkstack eingehängt sind. Wenn möglich, sollte man NDIS-5-Treiber deaktivieren. Windows kann sie zwar im NDIS-5-Kompatibilitätsmodus nutzen, aber sie bremsen das System aus, selbst wenn sie gerade keine Aufgaben haben. Ein Indiz für bremsende Treiber ist eine hohe CPU-Last auf einem Kern während des Transfers großer Dateien; sie kann leicht auf 100 Prozent klettern.

**Vorbildlich: Manche Programmierer notieren im Info-Feld, dass sie ihren Netzwerktreiber für das moderne NDIS 6 ausgelegt haben.**



Die RSC-Funktion kann Windows nur dann verwenden, wenn sich die installierten und aktiven Treiber mindestens für NDIS 6.3 eignen. Um die NDIS-Versionen abzufragen, kann man in PowerShell das folgende Kommando eingeben:

```
Get-NetAdapter | Select Name, NdisVersion
```

RSC wird normalerweise erst nach dem Neustart aktiv.

Es gibt diverse ältere Treiber, die das Task-Offloading deaktivieren. Dazu gehört der Packet-Capture-Treiber WinPcap von Wireshark, der virtuelle Bridge-Adapter von VMWare und ältere cFosSpeed-Versionen. Solche Treiber sollte man für volle 10GE-Kapazität deaktivieren, damit Windows das Task Offloading einschalten kann. Ob Offloading aktiv ist, zeigen folgende PowerShell-Kommandos:

```
Get-NetAdapterChecksumOffload  
Get-NetOffloadGlobalSetting
```

Um Treiber zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Netzwerksymbol im Tray, öffnen die „Netzwerk- und Interneteinstellungen“, klicken auf „Ethernet“ und dann auf „Adapteroptionen ändern“. Öffnen Sie mit der rechten Maustaste die „Eigenschaften“ der LAN-Schnittstelle. Eine Windows-10-Installation enthält ab Werk neun Elemente: Client für Microsoft-Netzwerke, Datei-

und Druckerfreigabe, QoS-Paketplaner, Internetprotokoll Version 4 (TCP/IPv4), Microsoft-Multiplexorprotokoll, Microsoft-LLDP-Treiber, Internetprotokoll Version 6 (TCP/IPv6), Antwort für Verbindungsschicht-Topologie und E/A-Treiber für Verbindungsschicht-Topologie.

Wenn in der Liste weitere Treiber aufgeführt sind und einer davon das System bremst, nehmen Sie das Häkchen daneben weg, um ihn zu deaktivieren und booten Sie den Rechner neu. Anschließend sollte der Rechner eine 10GE-Leitung zumindest im lokalen Netzwerk auslasten können, zum Beispiel im Zusammenspiel mit einem 10GE-fähigen Netzwerkspeicher (NAS). Windows merkt sich den Zustand bis zum nächsten Neustart.

Wenn man die Software wieder benötigt, die auf den veralteten Treiber setzt, aktiviert man ihn wiederum in den Adaptereinstellungen und bootet den Rechner. Auf Dauer nervt das natürlich. In solchen Fällen kann es nicht schaden, dem Entwickler der Software eine Überarbeitung seines Treibers vorzuschlagen. (dz@ct.de) ct

## Literatur

- [1] Ernst Ahlers, LAN extraflott, Multigigabit-Ethernet für mehr Netzwerkdurchsatz, ct 16/2020, S. 52
- [2] Ernst Ahlers, Presto-NAS, Schnelle Netzwerkspeicher: Vier NAS für 10-Gigabit-Ethernet, ct 25/2020, S. 124

**NDIS-Infos, schnelle 10-GE-Netzwerkkarte:** ct.de/y4ch



kommen sei nur etwas für absolute Profis, und jeder unbedachte Klick führe unweigerlich zum Systemabsturz. Zugegeben: Sehr benutzerfreundlich kommt sie wirklich nicht daher und ja, es gibt Aktionen, die Sie besser unterlassen sollten, wenn Ihnen Ihr Windows lieb ist. Mit ein bisschen Grundlagenwissen stellt der Einstieg aber auch keine unüberwindliche Hürde dar.

### Einsteigen

Ähnlich wie ein Dateisystem auf einem Massenspeicher ist die Registry hierarchisch aufgebaut: Die Rolle von Ordnern übernehmen sogenannte Schlüssel, die einerseits weitere Schlüssel enthalten und andererseits Werte speichern können. Werte sind sozusagen die Atome der Registry: Sie werden immer am Stück gelesen oder geschrieben.

Einem Wert ist immer ein Typ zugeordnet. Zu den verbreitetsten Typen gehören Zeichenfolgen (REG\_SZ) und Ganzahlen (REG\_DWORD, eine 32-Bit-Ganzzahl zwischen 0 und 4.294.967.295). In Binärwerten (REG\_BINARY) können Anwendungen beliebige Byte-Folgen speichern, die sie dann selbst interpretieren müssen. Der Vollständigkeit halber sei noch der Datentyp REG\_QWORD für 64-Bit-Ganzzahlen erwähnt sowie die etwas unglücklich übersetzten „Werte der mehrteiligen Zeichenfolge“ (REG\_MULTI\_SZ), die mehrere Zeichenfolgen auf einmal speichern können, und die „Werte der erweiterbaren Zeichenfolge“ (REG\_EXPAND\_SZ): Eingebettete Umgebungsvariablen werden darin beim Auslesen durch ihren Wert ersetzt, also etwa „%SYSTEMROOT%\System32“ als „C:\Windows\System32“ zurückgeliefert.

Schlüssel und Werte tragen Namen, die innerhalb des jeweiligen Schlüssels eindeutig sein müssen; Klein- und Großbuchstaben werden dabei nicht unterschieden. Jeder Schlüssel enthält zudem einen Standard-Wert ohne Namen und vom Typ Zeichenfolge; er kann leer sein.

Ähnlich wie Ordner und Dateien in NTFS-Dateisystemen sind Registry-Schlüssel durch Zugriffsrechte geschützt. Die Rechte eines Schlüssels gelten automatisch auch für alle enthaltenen Werte.

### Regedit

Als Werkzeug, mit dem man die Registry erkunden und ihre Inhalte ändern kann, bringt Windows den Registrierungs-Editor mit. Im Startmenü findet er sich links in der Liste aller Programme im Ordner „Windows-Verwaltungsprogramme“. Wer

# Registratur

## Was Sie über die Windows-Registry wissen müssen

**Auf Webseiten und in Computermagazinen – auch in c't – liest man immer mal wieder, dieses oder jenes Windows-Problem sei dadurch zu lösen, dass man einen Eintrag in der Registry ändere. Doch was ist die Registry überhaupt und wie kommt man an sie heran? Hier stehts.**

Von Hajo Schulz

**A**ußerhalb der Computerei steht das englische Wort „Registry“ für eine Registratur oder eine Meldebehörde – und damit ist auch schon die Aufgabe der Registry in Windows ganz gut umrisSEN: Sie ist die zentrale Datenbank, die den Zustand und die Konfiguration des Systems und der installierten Software verwaltet. Microsoft nennt sie in der deutschen Dokumentation häufig „Registrierung“ oder „Registrierdatenbank“, aber im allgemeinen Sprachgebrauch haben sich diese Übersetzungen kaum durchgesetzt. Deshalb bleiben auch wir im Folgenden bei der englischen Bezeichnung.

Um die Windows-Registry ranken sich allerlei Mythen: Ihr überhaupt nahe zu

ihn häufig benutzt, kann ihn wie jedes andere Windows-Programm ans Startmenü oder die Taskleiste anheften. Alternativ lässt er sich mit der Eingabe von `regedit` in den Dialog hinter dem Tastenkürzel Windows+R starten.

Startet man den Registrierungs-Editor unter einem Benutzerkonto, das Mitglied der Gruppe der Administratoren ist, beschafft er sich über die Benutzerkontensteuerung volle Admin-Rechte. Er funktioniert aber auch unter einem eingeschränkten Konto, kann dann aber bestimmte Schlüssel und Werte nicht ändern.

Der Registrierungs-Editor präsentiert sich ähnlich dem Datei-Explorer in einer zweigeteilten Ansicht: Links gibt es die Struktur von Schlüsseln und Unterschlüsseln in einer Baumansicht. Wählt man einen Schlüssel aus, erscheint rechts eine Liste aller Werte in diesem Schlüssel. Schlüssel und Werte lassen sich – so es denn die Zugriffsrechte erlauben – mit F2 umbenennen und mit Entflöschen. Werte öffnet man mit einem Doppelklick auf den Namen zum Bearbeiten. Die Befehle zum Erstellen neuer Schlüssel und Werte stecken in dem Kontextmenü, das sich per Rechtsklick auf einen Schlüssel oder auf eine freie Stelle in der Werte-Ansicht öffnet. All diese Befehle finden sich auch noch einmal im „Bearbeiten“-Menü. Anders als der Datei-Explorer beherrscht Regedit keine Operationen, um Schlüssel oder Werte zu kopieren oder zu verschieben.

Wenn Sie eine direkte Manipulation in der Registry ausprobieren möchten, die Sie auf einer vertrauenswürdigen Webseite gelesen haben, ist die Eingabezeile direkt unter der Menüleiste recht praktisch: Hier können Sie einen woanders kopierten Schlüsselnamen einfügen und mit Enter direkt zu diesem Schlüssel springen. Darauf, dass der Name wie beim Navigieren per Mausklick mit „Computer\“ beginnt, besteht Regedit dabei nicht und verdaut sowohl die ausgeschriebenen Namen der Wurzel-Schlüssel als auch die kurzen, von denen gleich die Rede sein wird.

## Was ist wo?

Öffnet man den Registrierungs-Editor zum ersten Mal, präsentiert er unter dem Wurzel-Eintrag „Computer“ fünf Schlüssel der ersten Ebene: Unter `HKEY_CLASSES_ROOT` (wir werden diesen Schlüssel im Folgenden wie häufig in der Literatur mit `HKCR` abkürzen) finden sich die Einträge, die

bekannten Dateitypen und -endungen die zuständigen Anwendungen zuweisen, sowie im System registrierte COM-Klassen (Component Object Model, ein Mechanismus zur Interprozesskommunikation). Der Schlüssel `HKEY_CURRENT_USER` (kurz `HKCU`) gehört dem Benutzer, unter dessen Konto Regedit gerade läuft; darunter können das System und Anwendungen benutzerspezifische Einstellungen und sonstige Daten ablegen.

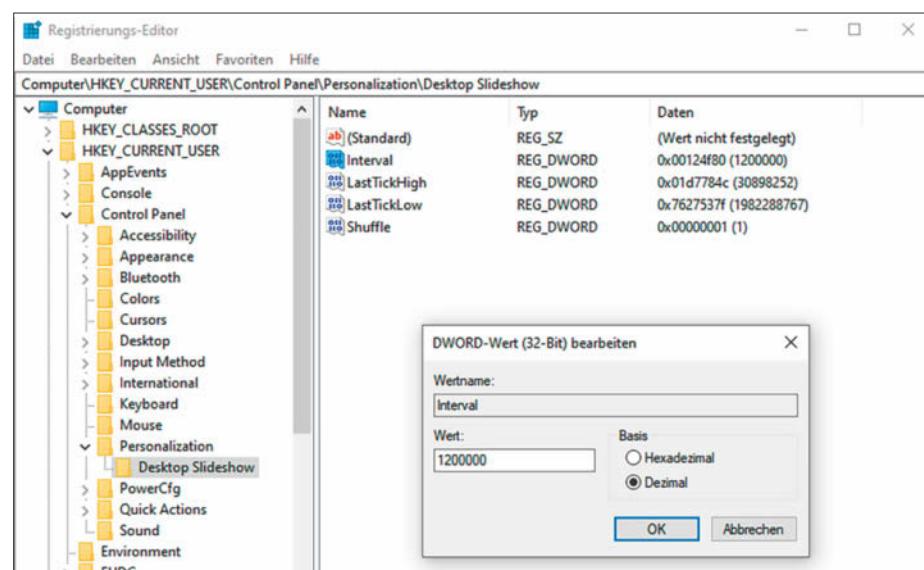
Globale Anwendungs- und Systemeinstellungen sowie die Konfiguration von Treibern und Systemdiensten stecken in den Unterschlüsseln von `HKEY_LOCAL_MACHINE` (abgekürzt `HKLM`). In `HKEY_USERS` (`HKU`) finden sich die Current-User-Schlüssel aller gerade angemeldeten Benutzerkonten sowie die der Systemkonten „System“ (S-1-5-18), „Lokaler Dienst“ (S-1-5-19) und „Netzwerkdienst“ (S-1-5-20). Schließlich speichert der Zweig unter `HKEY_CURRENT_CONFIG` (`HKCC`) Informationen zur aktuellen Hardware-Konfiguration.

Interessanterweise sind drei dieser Wurzeleinträge gar keine echten Registry-Schlüssel, sondern nur Verweise auf andere Orte innerhalb der Registrierung: `HKCC` residiert eigentlich unter `HKLM\System\CurrentControlSet\Hardware Profiles\Current`. `HKCU` ist eine Abkürzung zu jenem Schlüssel unter `HKU`, dessen Name der SID des aktuellen Benutzers entspricht – SID steht für „Security Identifier“ und identifiziert Benutzerkonten überall dort im System, wo es um Zugriffsrechte geht. Ein ganz besonderes Pflänzchen ist der Schlüs-

sel `HKCR`: Er setzt sich zusammen aus dem Inhalt von `HKLM\Software\Classes` und `HKCU\Software\Classes`. Bei Einträgen, die in beiden Zweigen existieren, hat `HKCU` Vorrang, neue Schlüssel oder Werte landen aber in `HKLM`.

Den Inhalt aller Schlüssel und Unterschlüssel zu beschreiben, die die Registry kennt, verbietet sich schon aus Platzgründen. Außerdem hängt der Umfang der gespeicherten Daten von der genauen Windows-Version, den aktivierten Systemfunktionen und installierter Nicht-Microsoft-Software ab. Einige prominente Ecken der Registry verdienen aber ein paar Bemerkungen.

Da wäre zum Beispiel der Aufbau der Unterschlüssel von `HKCR`: Alle Schlüssel, deren Namen mit einem Punkt beginnen, beschreiben einen Dateityp, allerdings meist nicht direkt. Vielmehr verweisen sie in der Regel auf einen weiteren Schlüssel, der dann beschreibt, wie Windows mit diesem Dateityp umgeht – ein Beispiel verdeutlicht das: Im Auslieferungszustand steht etwa im (Standard)-Wert des Schlüssels `HKCR\.txt`, also in dem für Dateien mit der Endung .txt zuständigen Eintrag, der Wert `txtfile`. Dieser verweist auf den Schlüssel `HKCR\txtfile`, der dann in weiteren Unterschlüsseln etwa das zu diesem Dateityp gehörende Explorer-Icon definiert (`DefaultIcon`) und bestimmt, welche Anwendung sich bei einem Doppelklick auf so eine Datei öffnet (`shell\open\command`). Woher der Explorer weitere Angaben zu diesem Dateityp nimmt, etwa



**Der Registrierungs-Editor – oder kurz Regedit – ist das Standard-Werkzeug zum Erkunden und Bearbeiten der Registry. Links stellt er die Hierarchie der Schlüssel dar, rechts die Werte.**

den Inhalt des Kontextmenüs oder die Einträge in der „Öffnen mit“-Liste, haben wir ausführlich in [1] beschrieben.

Die meisten Einstellungen speichern sowohl Windows als auch mitgelieferte und zusätzliche Programme in den Zweigen `HKCU\Software` und `HKLM\Software`. Deren Unterschlüssel sind per Konvention nach dem Schema `Hersteller\Programmname` benannt; bei der weiteren Strukturierung kocht jeder Hersteller sein eigenes Süppchen. Microsoft verwendet etwa für die Konfiguration von Windows die Schlüssel unter `...\\Software\\Microsoft\\Windows\\CurrentVersion`, einige Einträge stehen auch – wohl eher aus Tradition als aus technischen Gründen – in `...\\Software\\Microsoft\\Windows NT\\CurrentVersion`.

Wie oben schon kurz erwähnt, stecken die systemweit gültigen Daten in `HKLM`. Schreibrechte besitzen in diesem Ast aus gutem Grund nur Administratoren: Mit einer unbedachten Änderung in diesem Zweig ist eine Anwendung oder gar Windows selbst schnell unbrauchbar gemacht. Einige besonders sicherheitskritische Einstellungen behält Windows sogar dem Systemkonto oder dem Benutzerkonto „`TrustedInstaller`“ vor, das etwa auch als einzige Instanz Systemdateien im Rahmen von Updates überschreiben darf.

Der Zweig `HKCU` gehört dagegen dem aktuellen Benutzer; er darf alles lesen, ändern oder löschen. Auch dabei ist allerdings ein bisschen Vorsicht geboten, denn manche Software reagiert ziemlich allergisch auf unvorhergesehene oder fehlende Einträge. In jedem Fall bleiben die Auswirkungen aber auf das aktuelle Benutzer-

konto beschränkt: Meldet sich jemand unter einem anderen Konto an, bekommt er eine eigene Version des Zweiges `HKCU`.

### Ex- und Import

Ein probates Mittel, um sich vor unerwünschten Nebenwirkungen von Eingriffen in die Registry zu schützen, sind Sicherungskopien der Schlüssel, in denen Sie Änderungen vornehmen wollen. Dazu bietet der Registrierungs-Editor den Befehl „Datei/Exportieren“ an. Er fragt nach einem Dateinamen und schreibt dann den Inhalt des gerade ausgewählten und aller Unterschlüssel in eine Datei mit der Endung `.reg`. Sollte sich bei anschließenden Experimenten an Registry-Einträgen herausstellen, dass sie nicht die gewünschte Wirkung haben oder gar schädlich sind, können Sie die REG-Datei mit dem Regedit-Menübefehl „Datei/Importieren“ oder einem einfachen Doppelklick auf die Datei im Explorer wieder importieren und so Ihre Änderungen rückgängig machen.

Ein paar Kleinigkeiten gibt es dabei allerdings zu beachten: REG-Dateien werden ziemlich groß, wenn Sie Ihren Export weit oben im Schlüsselbaum beginnen. Sie sollten auf diese Weise also nur Äste speichern, von denen Sie wirklich eine Sicherheitskopie brauchen – wenn Sie einen Schlüssel löschen wollen, setzen Sie das Backup aber besser eine Etage höher in der Hierarchie an. Etwa den kompletten `HKCU`-Zweig zu sichern ist auch noch aus einem anderen Grund nicht empfehlenswert: Etliche Registry-Einträge werden von Windows sehr oft neu geschrieben, etwa um Vorgänge im System zu protokol-

lieren. Wenn Sie die beim Re-Import zurücksetzen, bringen Sie möglicherweise eine Systemfunktion aus dem Tritt. Schließlich stellt der Import einer REG-Datei zwar gelöschte und geänderte Einträge wieder her, löscht aber keine Schlüssel und Werte, die seit der Sicherung hinzugekommen sind.

Dem kann man aber mit einem Trick abhelfen: REG-Dateien bestehen aus reinem Text, lassen sich also mit jedem einigermaßen modernen Texteditor bearbeiten. Unicode sollte er aber beherrschen, denn die Dateien sind UTF-16-kodiert – auf das Windows-eigene Notepad trifft das zu. Ein exportierter Schlüssel sieht als Text beispielsweise wie folgt aus:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_CURRENT_USER\Software\Test]
```

```
"TheAnswer"=dword:0000002a
```

```
[HKEY_CURRENT_USER\Software\Test\V1]
```

```
"LastCheck"="2021-07-12"
```

Auf die Kopfzeile, anhand derer der Registrierungs-Editor die Datei als gültig erkennt, folgen, beginnend beim obersten Schlüssel der exportierten Hierarchie, die Schlüssel in eckigen Klammern und jeweils direkt darunter die Werte in diesem Schlüssel. Beim Import arbeitet der Registrierungs-Editor die Zeilen auch in diese Reihenfolge ab. Sie können den Anfang der Datei nun folgendermaßen ändern:

```
Windows Registry Editor Version 5.00
```

```
[-HKEY_CURRENT_USER\Software\Test]
```

```
[HKEY_CURRENT_USER\Software\Test]
```

```
"TheAnswer"=dword:0000002a
```

```
...
```

Sie kopieren also den ersten Schlüsselnamen, fügen ihn gleich darüber, getrennt durch eine Leerzeile, noch einmal ein und schreiben hinter die öffnende eckige Klammer ein Minus-Zeichen. Das weist den Registrierungs-Editor an, den Schlüssel mit diesem Namen zu löschen und mit ihm auch alle enthaltenen Werte und Unterschlüssel. Danach folgt dann der ursprüngliche Inhalt, der die exportierte Struktur nun von Grund auf neu aufbaut.

In REG-Dateien können auch Zeilen enthalten sein, die Werte löschen. Sie sind nach dem Muster `"Löschein"=-` aufgebaut; dem Wert wird einfach ein Minus-Zeichen

## Regedit-Alternativen

Außer dem grafischen Registrierungs-Editor bringt Windows noch zwei textbasierte Werkzeuge mit, die Sie zum Bearbeiten der Registry verwenden können: Fans der Eingabeaufforderung benutzen das Programm `reg`. Mit seinen Unterbefehlen wie `reg query`, `reg add` oder `reg delete` können Sie Schlüssel und Werte auslesen, hinzufügen oder löschen. Mit einigen seiner Kommandos ist `reg` sogar dem Registrierungs-Editor überlegen: So kann man mit `reg copy` ganze Registry-Äste kopieren und mit `reg compare` Unterschiede zwischen Schlüsseln aufspüren. Details zu den einzelnen Befehlen verrät `reg /?`.

Die PowerShell behandelt Registry-Schlüssel wie Ordner in einem Dateisystem: Sie definiert standardmäßig die beiden „Laufwerke“ `HKCU:` und `HKLM:`, in denen man unter anderem mit `Set-Location` oder `cd` navigieren kann, sich mit `Get-ChildItem` oder `dir` Schlüssel anzeigen lassen oder mit `New-Item` und `Remove-Item` Schlüssel erstellen und löschen kann. Werte sind in diesem Bild aber keine Dateien, sondern Eigenschaften der Schlüssel, denen man mit Befehlen wie `Get-ItemProperty` und `Set-ItemProperty` zu Leibe rückt. Einige Links zu relevanten Online-Dokumenten haben wir unter [ct.de/ydxz](http://ct.de/ydxz) zusammengestellt.

zugewiesen, aber ohne umschließende Anführungszeichen.

REG-Dateien sind nicht nur als Backup vor riskanten Experimenten zu gebrauchen, sondern etwa auch zur Dokumentation oder zur Fehlersuche: Exportieren Sie einen Schlüssel, in dem Sie eine Fehlkonfiguration vermuten, einmal aus einer einwandfrei laufenden Windows-Installation und einmal aus einer fehlerhaften, dann können Sie die beiden Versionen in einem Programm für Textvergleiche wie Win-Merge (Download via ct.de/ydxz) nebeneinanderlegen und spüren Unterschiede schnell auf. Dieselbe Vorgehensweise funktioniert, um etwa den Machenschaften problematischer Installationsprogramme auf die Schliche zu kommen: Dazu exportieren Sie zentrale Bereiche wie die oben beschriebenen CurrentVersion-Schlüssel einmal vor und einmal nach der verdächtigen Installation. Dabei ist dann aber ein bisschen Instinkt gefragt: Meist finden sich auch Unterschiede, die mit dem eigentlich untersuchten Vorgang gar nichts zu tun haben.

Deshalb bietet sich für solche Fälle auch noch eine andere Vorgehensweise an: Besorgen Sie sich das kostenlose Microsoft-Tool Process Monitor und stellen Sie seine Filter so ein, dass Sie nur noch Zugriffe auf die Registry sehen, die von dem Programm stammen, um das es Ihnen geht. Der Arbeit mit dem Process Monitor haben wir vor einiger Zeit eine dreiteilige Artikelserie gewidmet [2, 3, 4].

## Dateien

Beim Thema Sicherheitskopie könnte man auch auf die Idee kommen, einfach die Dateien zu sichern, in denen die Registry physisch auf der Festplatte residiert. Das ist aus mehreren Gründen nicht praktikabel: Zum einen besteht die Registry nicht nur aus einer oder fünf Dateien, sondern aus etlichen mehr – siehe die Tabelle auf dieser Seite. Zum anderen liegen die meisten Dateien im Ordner C:\Windows\System32\config, auf den man ohne Admin-Rechte gar keinen Zugriff hat, nicht mal zum Lesen. Selbst wenn man sich die erforderlichen Rechte besorgt, scheitert das Kopieren bei einigen der Dateien daran, dass Windows sie im laufenden Betrieb ständig exklusiv geöffnet hält – lesen, geschweige denn überschreiben verboten.

Selbst wenn man all diese Klippen etwa mit einem parallel installierten Zweit-Windows oder dem c't-Notfall-Windows umschiffen würde, stellt sich die

## Dateien der Registry

Registry-Schlüssel	Datei	Zweck
HKCU	C:\Users\<Kontoname>\ntuser.dat	Benutzerspezifische Daten und Einstellungen
HKCU\Software\Classes	C:\Users\<Kontoname>\AppData\Local\Microsoft\Windows\usrClass.dat	Benutzerspezifische Dateitypen und COM-Klassen
HKLM\BCD00000000	[UEFI-Partition]\EFI\Microsoft\Boot\BCD <sup>1</sup>	Boot-Konfiguration
HKLM\HARDWARE	– (Wird zur Laufzeit dynamisch erzeugt)	Informationen zu angeschlossener Hardware
HKLM\SAM	C:\Windows\System32\config\SAM	„Security Accounts Manager“: Anmeldenamen, Kennwort-Hashes etc.
HKLM\SECURITY	C:\Windows\System32\config\SECURITY	Sicherheitsrichtlinien und Benutzerrechte
HKLM\SOFTWARE	C:\Windows\System32\config\SOFTWARE	Systemweit geltende Daten und Einstellungen
HKLM\SYSTEM	C:\Windows\System32\config\SYSTEM	Konfiguration von Treibern und Diensten
HKU\.\DEFAULT	C:\Windows\System32\config\DEFAULT	Daten und Einstellungen des Kontos „Lokales System“
HKU\\$1-5-18	C:\Windows\System32\config\DEFAULT	Daten und Einstellungen des Kontos „Lokales System“
HKU\\$1-5-19	C:\Windows\ServiceProfiles\LocalService\ntuser.dat	Daten und Einstellungen des Kontos „Lokaler Dienst“
HKU\\$1-5-20	C:\Windows\ServiceProfiles\NetworkService\ntuser.dat	Daten und Einstellungen des Kontos „Netzwerkdienst“

<sup>1</sup> mit Legacy-BIOS: [Boot-Partition]\Boot\BCD

Frage nach dem Sinn: Die in der Registry gespeicherten Informationen sind derart eng mit dem Zustand des Systems, installierten Anwendungen, Updates und Patches verwoben, dass eine Wiederherstellung allein der Registry mehr Probleme schafft als löst. Wer regelmäßig ein Komplett-Backup der Registry haben möchte, sollte Nägel mit Köpfen machen und das Systemlaufwerk per System-Image sichern, beispielsweise mit unserem Tool c't-WIMage [5]. Ein Image schützt selbst dann, wenn man die Registry so weit kaputt gespielt hat, dass Windows gar nicht mehr startet – eine REG-Datei hilft dann nicht, weil ohne Windows ja auch der Registratur-Editor nicht läuft, den man zum Importieren braucht.

Zu wissen, in welchen Dateien – Microsoft nennt sie Hive-Dateien – die Registry auf der Festplatte gespeichert ist, schadet trotzdem nicht: Um etwa einen Trojaner oder einen marodierenden Treiber loszuwerden, kann es nützlich sein, die Registry zu bearbeiten, während das dazugehörige Windows gerade nicht läuft. Dazu startet man ein parallel installiertes Zweit-Windows oder das c't-Notfall-Windows, öffnet dort den Registry-Editor und markiert einen der Schlüssel HKLM oder HKU. Mit dem Menübefehl „Datei/Struktur laden“ öffnet man die gewünschte Datei. Regedit fragt nach einem Schlüsselnamen – den können Sie beliebig wählen; unter diesem Namen hängt Regedit die Datei daraufhin in die bestehende Registry ein und Sie können ihren Inhalt bearbeiten. Wenn Sie fertig sind, bitte nicht vergessen, den eingehängten Ast über „Datei/Struktur entfernen“ wieder zu entladen. Damit stellen Sie sicher, dass alle Änderungen wirklich auf dem Datenträger landen und

dass der fremde Ast in diesem Windows keine Nebenwirkungen mehr entfalten kann.

## Fazit

Auch wenn die Bedienoberfläche des Registratur-Editors auf den ersten Blick nicht besonders einladend aussieht: Angst muss man beim Umgang mit ihm nicht haben. Vor allzu unbedachtem Herumfricken an der Registry sei aber gewarnt: Schnell hat man sich sein System so kaputt konfiguriert, dass nichts mehr geht. Wohl dem, der vor Experimenten Sicherheitskopien der betroffenen Registry-Äste, besser noch eine Komplettsicherung per Image angelegt hat.

Genauso bedenklich wie eigene Experimente aufs Geratewohl sind übrigens angebliche Registry-Säuberer und ähnliche Tools, die versprechen, in der Registry aufzuräumen und dadurch das System um Faktor X zu beschleunigen: Ungenutzte Registry-Einträge bremsen kein Windows mess- oder gar spürbar aus – was das System nicht liest, verschwendet auch keine Zeit.

(hos@ct.de) **ct**

## Literatur

- [1] Hajo Schulz, Wunschgemäß verbunden, Dateitypen verwalten unter Windows, c't 26/2017, S. 164
- [2] Axel Vahldiek, Unter dem Mikroskop, Windows analysieren mit dem Process Monitor – Teil 1, c't 16/2017, S. 148
- [3] Axel Vahldiek, Schärfer stellen, Windows analysieren mit dem Process Monitor – Teil 2, c't 17/2017, S. 154
- [4] Hajo Schulz, Noch mehr Durchblick, Windows analysieren mit dem Process Monitor – Teil 3, c't 18/2017, S. 162
- [5] Axel Vahldiek, Ersatzrad, c't-WIMage erstellt Windows-Backups, c't 10/2021, S. 18

**Tool-Downloads, Online-Doku:**  
[ct.de/ydxz](http://ct.de/ydxz)

# 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 € >



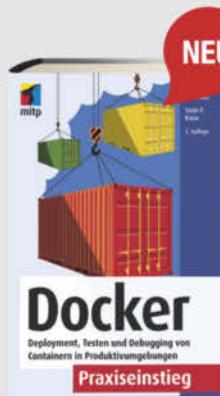
### Jörg Frochte **Maschinelles Lernen (2. Aufl.)**

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 € >



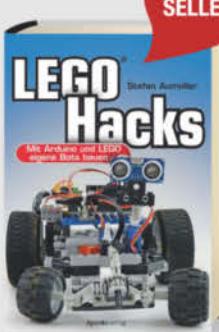
### Karl Matthias, Sean P. Kane **Docker Praxiseinstieg (2. Aufl.)**

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 € >



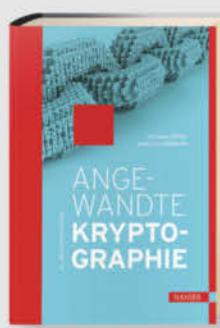
### Stefan Aumüller **LEGO® Hacks**

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 € >



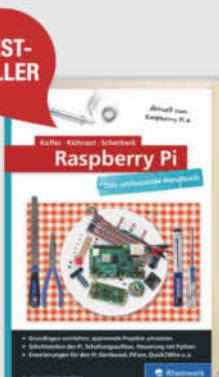
### Wolfgang Ertel, Ekkehard Löhmann **Angewandte Kryptographie (6. Aufl.)**

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 durchstarten 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 € >

**PORTOFREI  
AB 20 €  
BESTELLWERT**

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

© Copyright by Heise Medien.

# 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.



### Komplettset Argon ONE Case mit Raspberry Pi 4

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 € >

NEUER PREIS!



### ArduiTouch-Set

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 Fallschirmsenseide 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 € >



### 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-Lötbausatz mit LEDs und Batterie.

-27,70 €

[shop.heise.de/makey-paket](http://shop.heise.de/makey-paket)

19,90 € >





heißt CloudReady. Die Home-Ausgabe für den Privatgebrauch ist kostenlos. Bildungseinrichtungen und Firmen müssen hingegen die Verwendung für rund 20 beziehungsweise 49 Euro pro Gerät und Jahr lizenziieren, bekommen dafür aber auch erweiterten Support und Integration in die Google Admin Console.

Ausprobiert haben wir CloudReady Home auf drei alten Rechnern. Auf einem Notebook Lenovo G780 von 2012 mit Intel i3-2328M-Prozessor fiel auf, dass der Rechner beim Herunterfahren sporadisch nicht abschaltete; es half dann, die Power-taste vier Sekunden gedrückt zu halten. Ein Microsoft Surface Pro der ersten Generation (ebenfalls von 2012) läuft völlig unproblematisch; der Lagesensor des Tablets wird allerdings nicht ausgewertet. Außerdem haben wir noch ein Windows-Tablet Acer Iconia W500 ausprobiert. Zu sagen, dass es läuft, wäre übertrieben – es kriecht vielmehr; der Stromspar-Dual-Core AMD C-50 ist deutlich zu schlapp, um CloudReady halbwegs flüssig laufen zu lassen. Immerhin hat das System sämtliche Hardware anstandslos erkannt.

#### Unterschiede

Bedienung und Aussehen von Chrome OS und CloudReady gleichen sich wie ein Ei dem anderen. Auch die Linux-Umgebung lässt sich in den Einstellungen im Menü „Entwickler“ nachinstallieren. Und als Online-Betriebssystem setzt auch CloudReady einen Login mit einem Google-Konto voraus, um es nutzen zu können.

Doch obwohl die beiden Betriebssysteme die gleiche Basis verwenden, gibt es Unterschiede. Vor allem fehlen CloudReady proprietäre Bestandteile, die Google zusätzlich in Chrome OS eingebaut hat. Das betrifft zum Beispiel die Google Play Services und damit Apps aus dem Play Store. Auch die Indizierung für Google-Drive-Inhalte, die schnellere Ergebnisse bei Suchvorgängen in cloudgelagerten Dateien liefert, ist nicht enthalten, und auch Googles erweiterte Rechtschreibprüfung fehlt. Updates fürs Betriebssystem kommen ein paar Wochen später an als auf Chromebooks.

Die sonstigen Unterschiede sind eher spezieller Natur: Die Virtualisierungslösung Parallels wird auf CloudReady nicht unterstützt, ebenso wenig der „Power-washing“-Mechanismus, der auf Chromebooks zum Zurücksetzen auf die Werkseinstellungen dient. Die Lösung für Letzteres ist recht trivial: Wer CloudReady

# Altmetall verchromen

## Alte PCs mit dem Chrome-OS-Klon CloudReady aufmöbeln

**Um Chrome OS zu nutzen, muss man ein Gerät kaufen, auf dem das Betriebssystem vorinstalliert ist – eigentlich, denn der Hersteller Neverware bietet den Klon CloudReady an, der auf dem freien Chromium-OS-Projekt aufbaut und für die private Nutzung gratis ist.**

Von Jan Schüßler

Wir haben in Ausgabe 15/2021 eine Menge dazu geschrieben, welche Vorteile Chrome OS hat [1]. Doch so praktisch es sein mag: Wie macOS ist es ausschließlich mit neuer Hardware erhältlich. Um das Betriebssystem von Google zu nutzen, muss man ein Chromebook kaufen. Doch es gibt eine Möglichkeit, ein sehr ähnliches System auf vorhandener Hardware zu installieren. Chrome OS fußt auf dem quelloffenen Projekt Chromium OS, weshalb sich damit Alternativen bauen lassen, die dem Google-System sehr ähnlich sind.

Die zurzeit wohl bekannteste davon kommt vom Hersteller Neverware und

zurücksetzen will, installiert es einfach erneut. Anders als Chrome OS ist CloudReady in der Lage, ohne kompatibles Trusted Platform Module (TPM) zu funktionieren.

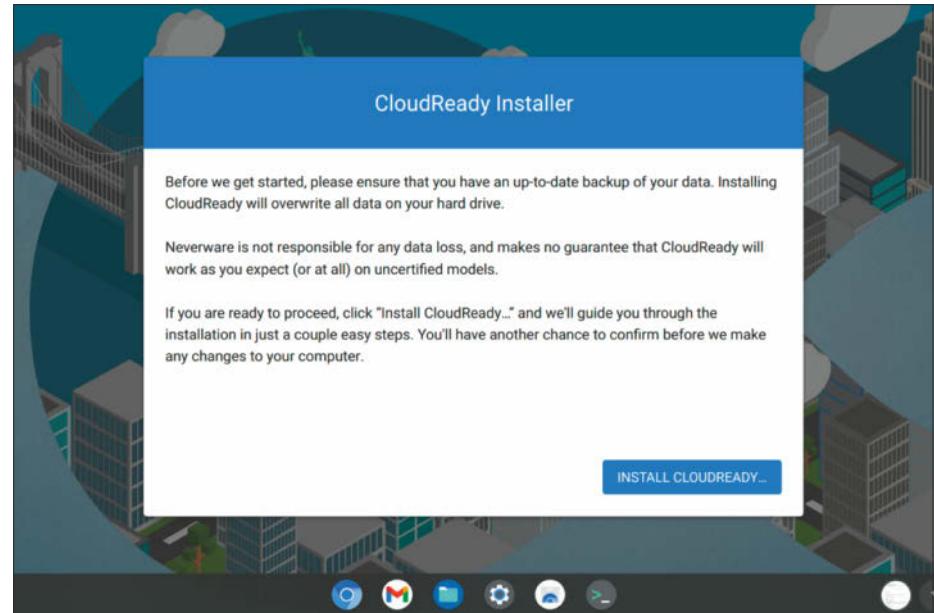
## Setup-Stick

Um CloudReady zu installieren, brauchen Sie zunächst einen bootfähigen Setup-USB-Stick, wie er auch für die Installation von Windows und Linux-Distributionen üblich ist. Auf Windows-Systemen gibt es dafür einen „USB Maker“, ein Tool, das CloudReady herunterlädt und fix und fertig auf einen USB-Stick schreibt (siehe ct.de/ynp9). Die Bedienung ist denkbar einfach: Stick anstecken, USB Maker starten, zweimal auf „Next“ klicken, unter „Select Drive“ den USB-Stick auswählen und wieder auf „Next“ klicken. Eventuell zuvor vorhandene Inhalte des USB-Sticks werden dabei gelöscht. Nach ein paar Minuten Wartezeit – oder auch mehr, je nach Performance des Internetanschlusses und des USB-Sticks – ist der Stick fertig. Achtung: Während der USB Maker den Stick partitioniert und formatiert, findet Windows mitunter neue Partitionen, und bietet sie zum Formatieren an. Ignorieren Sie diese Meldungen einfach.

Unter Chrome OS, macOS und Windows lässt sich ein CloudReady-Stick alternativ auch mit einem heruntergeladenen Setup-Abbild und der Chrome-Erweiterung „Programm zur Chromebook-Wiederherstellung“ anfertigen (siehe ct.de/ynp9). Mit Linux funktioniert die Erweiterung nicht. Klicken Sie in der Erweiterung auf das Zahnrad-Icon oben rechts und auf „Lokales Bild verwenden“. Geben Sie im Auswahldialog das heruntergeladene Image an, wählen Sie den angeschlossenen USB-Stick aus und bestätigen Sie die Dialoge mit „Weiter“ und „Jetzt erstellen“.

## Installieren

Starten Sie nun den Rechner vom USB-Stick. Wie das geht, kann sich von PC zu PC unterscheiden. Im Regelfall gibt es eine Taste, mit der Sie direkt nach dem Einschalten des Rechners, noch bevor das Betriebssystem startet, ein Bootmenü des BIOS aufrufen können. Meist ist es eine der Tasten F8, F11, F12 oder Esc, oder die Eingabetaste – ein Blick ins Handbuch des Rechners oder des Mainboards hilft weiter. Wählen Sie im BIOS-Bootmenü den USB-Stick aus. Bootet der Rechner vom Stick, erkennen Sie das nach ein paar Se-



**Die CloudReady-Installation ist die wohl einfachste, die wir je erlebt haben: drei Klicks, keine Fragen.**

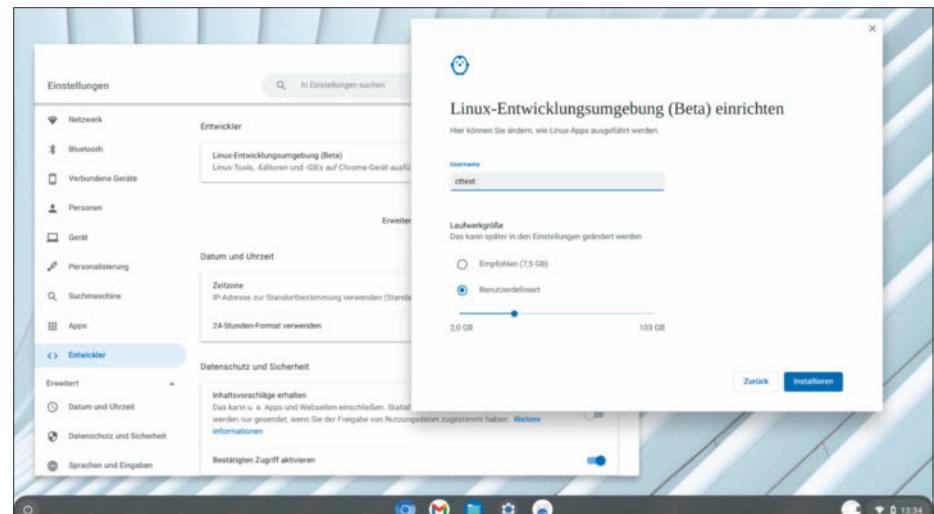
kunden an einem weißen Ladebildschirm mit CloudReady-Logo. Auf manchen älteren PCs mit sehr alter Firmware kann es zudem nötig sein, im BIOS-Setup die Funktion UEFI Secure Boot abzuschalten, damit CloudReady vom USB-Stick bootet.

Der Installationsvorgang ist bei CloudReady einer der simpelsten, die wir je erlebt haben. Klicken Sie unten rechts auf die Uhrzeit, dann auf „Install OS“, auf „Install CloudReady“ und dann auf „Erase Hard Drive And Install CloudReady“. Die Installation dauert nach unserer Erfahrung selten länger als fünf Minuten. Eine

Möglichkeit zur Partitionierung der Festplatte oder gar für Dual-Boot-Konfigurationen bietet der CloudReady-Installer nicht; das Setup ist auf maximale Einfachheit ausgelegt. Nach der Installation schaltet sich der Rechner automatisch aus. Entfernen Sie den Stick und schalten Sie den PC wieder ein.

## Einrichten

Die Einrichtung gleicht der eines Chromebooks weitgehend: Sprache und Tastaturlayout einstellen, Netzwerkverbindung herstellen, Nutzungsbedingungen bestätigen. Achtung: Bei letzterem ist ein Häk-



**Wie Chrome OS bietet auch CloudReady eine einfach nachinstallierbare Linux-Umgebung.**

chen für die Übermittlung von Diagnosedaten an Google werkseitig gesetzt und auf manchen Rechnern erst nach dem Herunterscrollen sichtbar. Dann folgen noch der Login mit einem Google-Konto und das Abnicken der Synchronisierung – fertig.

Im Unterschied zum Chromebook fällt vor allem ein Unterschied auf: Die Bestimmungen für die Google Play Services fehlen – logisch, denn das ist eins der Features, die den echten Chromebooks vorbehalten bleibt, ebenso die Verbindung mit einem Android-Smartphone, die es erlaubt, SMS vom Chromebook zu versenden, das Notebook per Smartphone zu entsperren und ähnliches.

### Lieber erst einmal ausprobieren?

Möglicherweise möchten Sie CloudReady ausprobieren, bevor Sie es auf einen PC installieren. Neverware bietet dafür zwei Möglichkeiten an, die sich auch eignen, vor dem Kauf eines Chromebooks das Look-and-feel von Chrome OS kennenzulernen.

Die erste Möglichkeit kennen Sie vielleicht schon von Linux-Distributionen. Sie können das System, das vom Setup-USB-Stick startet, auch ohne weitere Installation als Live-System verwenden. So lässt

sich auch am einfachsten herausfinden, ob die Hardware des Rechners von CloudReady unterstützt wird. Auch eine Einrichtung des Systems mit Google-Konto und weitere Personalisierungen sind möglich; die Einstellungen bleiben nach einem Neustart erhalten.

Zur längerfristigen Nutzung ist das Live-System vom USB-Stick aber kaum geeignet, da USB-Sticks als Systemlaufwerk weniger zuverlässig sind und meist auch keine gute Performance liefern. Wenn gleich sich die Datenübertragungsrate moderner USB-Sticks sehen lassen kann, ist die Leistung beim Lesen und Schreiben vieler kleiner Dateien oft unterirdisch. Und zur portablen Nutzung eignet sich ein CloudReady-Stick ebenfalls nicht, weil das System eine erneute Ersteinrichtung durchlaufen will, sobald es an einem anderen PC gestartet wird.

### Probieren per VM

Die zweite Testmöglichkeit ist eine virtuelle Maschine (VM). Für diesen Zweck bietet Neverware einen vorgefertigten virtuellen Rechner in Form einer OVA-Datei (Open Virtual Appliance) an. Die Desktop-Virtualisierer Oracle VirtualBox und VMware Workstation können das Format importieren, allerdings funktioniert die

CloudReady-VM nicht mit VirtualBox – laut Neverware ist der CloudReady-Grafiktreiber inkompatibel mit dem Virtualisierer.

Der Hersteller empfiehlt die inzwischen recht alte VMware-Version 14. In unseren Tests mit dem aktuellen VMware Workstation 16 Player, der für die private Nutzung gratis ist, lief es aber anstandslos. Auch mit den älteren Ausgaben VMware Workstation 15.5 Player und Pro konnten wir keine Probleme feststellen.

Um CloudReady mit VMware auszuprobieren, brauchen Sie das OVA-Paket von Neverware und, falls noch nicht vorhanden, das Setup-Paket für VMware Workstation Player (siehe ct.de/ynp9). Installieren und starten Sie den Virtualisierer; klicken Sie dann auf „Open a Virtual Machine“ und verfütern Sie die OVA-Datei. Ein Klick auf „Import“ schließt den Vorgang ab – je nach Hardware kann das ein paar Minuten dauern. Die Schaltfläche „Play virtual machine“ startet die VM. Das System lässt sich einrichten und aktualisieren wie eine CloudReady-Installation auf echter Hardware, allerdings steht die Linux-Umgebung in der VM nicht zur Verfügung. Zudem war die Bildschirmauflösung in manchen unserer Tests auf 1024 × 768 Pixel festgelegt.

### Aussichten

Interessant könnte die langfristige Entwicklung von CloudReady werden, denn Google hat die Herstellerfirma Neverware im Dezember 2020 gekauft. Erste Befürchtungen, die Firma sei nur erworben worden, um sie kleinzuhacken, haben sich zum Glück nicht bewahrheitet.

Spannend bleibt daher die Frage, ob Google Neverwares Techniken später einmal nutzen wird, um auch Chrome OS mit einem universellen Installer zu versehen, damit es sich auf vorhandener Hardware installieren lässt. Bislang hat Google allerdings keine derartigen Pläne angedeutet – bis auf Weiteres bleibt CloudReady also ein Chrome-OS-Lookalike, zwar ohne Play Store, aber mit der gleichen einfachen Bedienung.

(jss@ct.de) 

### Literatur

[1] Stefan Porteck, Auf Chromeglanz poliert, Chromebooks: Vom Nischenprodukt zum vollwertigen Notebook, c't 15/2021, S. 16

**CloudReady-Downloads:** [ct.de/ynp9](http://ct.de/ynp9)

Mit der Linux-Umgebung lässt sich auch Software nachinstallieren, die es im Chrome Web Store nicht gibt – zum Beispiel der P2P-Synchronisierer Syncthing.

# Halten Sie Ihre Prozesse im Takt



Exklusiver  
Frühbucher-  
Rabatt!

 heise Academy

DevOps, Continuous Delivery und Container-Orchestrierung sind der Schlüssel für eine effizientere Softwareentwicklung. Werden Sie mit unseren Workshops zum Meister Ihrer Softwareentwicklung.

## Unser Angebot

**Terraform –  
Infrastructure as  
Code**

10. – 11. August

WORKSHOP

**DevSecOps –  
Sec gehört dazu**

31. August – 1. September

WORKSHOP

**Container managen  
mit Kubernetes &  
Rancher**

9. – 10. September

WORKSHOP

**Container-  
Orchestrierung  
mit Kubernetes**

20. – 23. September

WORKSHOP

**Elastic Stack  
Fundamentals**

5. – 7. Oktober

WORKSHOP

**Continuous  
Integration  
mit Jenkins**

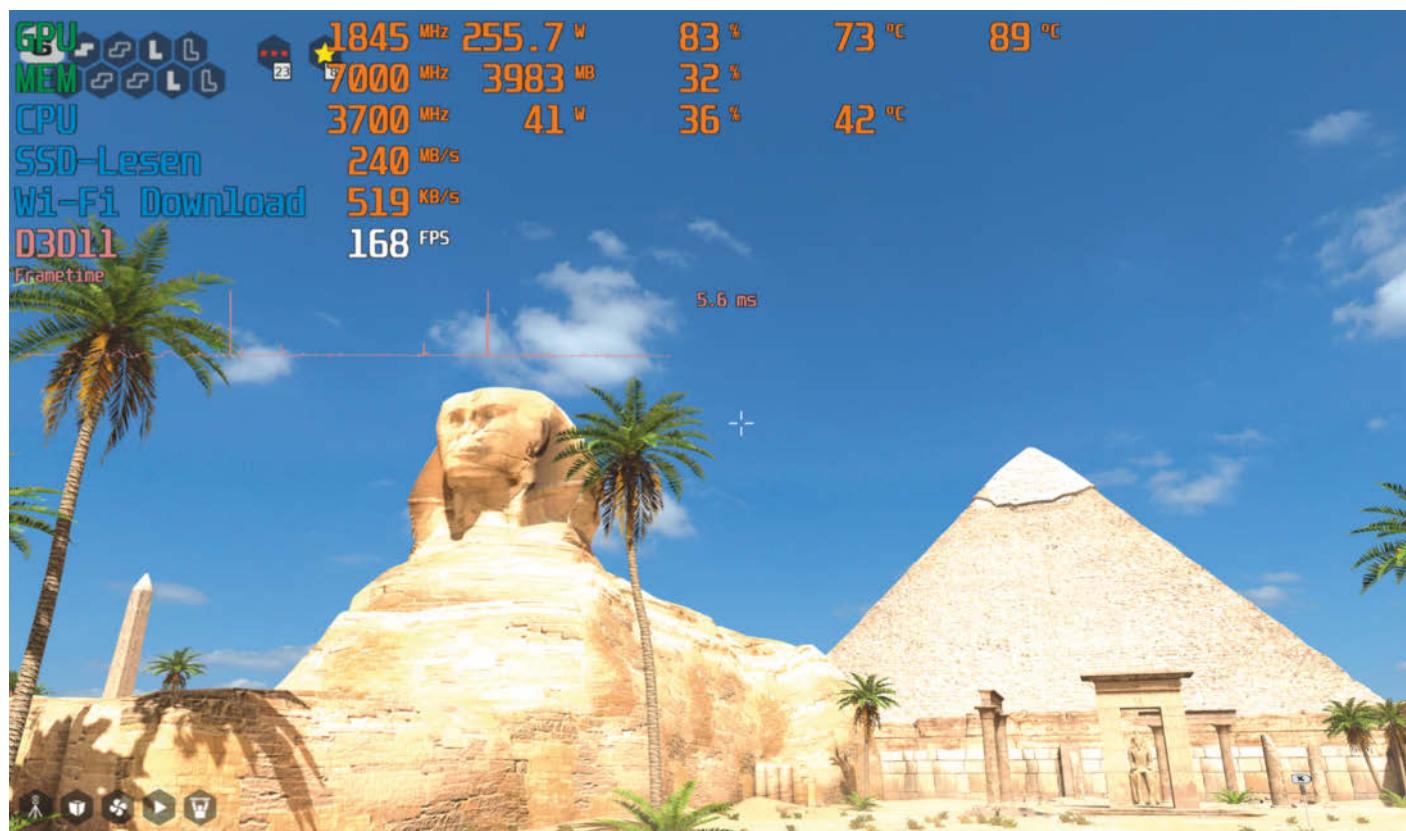
12. – 13. Oktober

WORKSHOP

Mehr Informationen:

[heise-academy.de/devops](http://heise-academy.de/devops)

© Copyright by Heise Medien.



# Mächtig überlagert

**Hardware-Diagnose per OSD: Temperaturen, Takte und mehr immer im Blick**

**Wer Probleme mit PC-Abstürzen hat, kennt das: Wie finde ich die Ursache? Kostenlose Windows-Programme überwachen die Hardware auch während des Spieletreibs und helfen, dem Übeltäter leichter auf die Schliche zu kommen.**

Von Carsten Spille

**M**it einem gut konfigurierten On-Screen-Display, kurz OSD, behalten Sie eine Reihe wichtiger Parameter immer im Blick und spüren mögliche Störungen schnell auf: Taktet der Prozessor wirklich

hoch oder verweilt er im Leerlaufmodus? Ist der Grafikspeicher rappelvoll? Taktet der Grafikchip herunter, weil er zu heiß wird oder weil er an der Grenze der erlaubten Leistungsaufnahme arbeitet?

Die Fehlersuche am häufig abstürzenden PC kann einer Sisyphosarbeit gleichen. Um zumindest die Hardware-Komponenten auch während fordernder Vollbildanwendungen wie 3D-Spielen im Auge zu behalten, eignen sich Overlays. Sie überlagern einen Teil des Bildes halbtransparent mit Echtzeitinformationen aus den verschiedensten Sensoren des PCs wie etwa Taktfrequenzen, Temperatur und Leistungsaufnahme von Prozessor und Grafikkarte sowie Transferraten von Massenspeicher und Internetzugang. Dadurch erlauben sie zum Beispiel, ein kurzes Stocken im Bildfluss mit einer Temperaturspitze oder

dem Nachladen von der Festplatte in Verbindung zu bringen oder eine Verzögerung im Online-Spiel durch Netzwerkverkehr. Das funktioniert mit einfachen Messmethoden, wie sie der Windows-Taskmanager mitbringt, nur unzureichend. Denn wenn man aus Vollbildanwendungen zurück auf den Desktop schaltet, sinken Temperaturen und Leistungsaufnahme in Sekundenbruchteilen. So hat man keine Chance, die Übeltäter zu erwischen.

Um gleich loszulegen, benötigen Sie eigentlich nur einen PC mit einem halbwegs aktuellen Windows, Administratorrechte sowie zwei kostenlose Tools. Zunächst wäre da der MSI Afterburner. Trotz seines Namens funktioniert er auch problemlos mit den Grafikkarten anderer Hersteller und installiert automatisch den Riva Tuner Statistics Server für das Over-

lay mit. Als weiteren Datenlieferanten benötigen Sie das ebenfalls kostenlose HWInfo in der Freeware-Version. Links zu den Tools und ein Video der gesamten Einrichtung finden Sie via ct.de/yan1.

## Bordmittel, Treiber und Tools

Sofern Sie Ihren PC bei der Ausführung einer im Fenster laufenden Anwendung überwachen wollen, genügt meist schon ein Blick in den Task-Manager. Das geht am schnellsten über Win+Umschalt+Esc und spätestens nach einem Klick auf „Mehr Details“ verrät er im Tab „Leistung“ bereits viele Details.

Vielen Spielern ebenfalls bekannt sein dürfte das Steam-Overlay, welches zum Beispiel die derzeitige Bildrate in einer Bildschirmecke einblenden kann.

Einen Schritt weiter gehen die aktuellen Treiber von AMD-Radeon- und Nvidia-GeForce-Grafikkarten. Sie heißen Radeon Software Adrenalin für Karten mit AMD-Grafikchip und schlicht GeForce Game Ready Driver für Nvidia-Karten und werden von den meisten Spielern sowieso installiert.

In ihnen sind bereits Overlay-Funktionen enthalten, die man – einmal aktiviert – während eines Spiels mit Alt+R aufruft. Bei Nvidia muss man dafür die sogenannte GeForce Experience (GFE) während der Treiberinstallation mit ausgewählt haben und zudem in einem immerhin kostenlosen Konto bei Nvidia eingeloggt sein. AMD koppelt sein In-Game-Overlay nicht an solche Voraussetzungen.

Die Anzeigen von Radeon und GeForce sind vom Umfang her recht ähnlich und konzentrieren sich verständlicherweise auf die Funktionen des Grafikchips, auch wenn zum Beispiel auf Wunsch die CPU-Auslastung ebenfalls dargestellt wird. Nvidia gibt in der erweiterten Version des GFE-Overlays auch die Minimal-Fps (Perzentil P99) und die Latenz des Bildes aus [1].

Was beide nicht können, sind auch andere Sensoren in die Überwachung einzubinden oder grafische Verläufe anzusehen. Letzteres kann zwar das verbreitete Tool GPU-Z, welches ohne Installation auskommt. Diese Informationen sind aber nicht live während des Spielens im Vollbild zu sehen – außer, man hat noch ein zweites Display angeschlossen.

## Mächtig überlager

Hier kommt das kostenlose Tool MSI Afterburner ins Spiel. Es funktioniert so-

wohl mit GeForce- als auch mit Radeon-Karten. Beim Afterburner handelt es sich um die am häufigsten gepflegte Variante des früheren RivaTuners; prinzipiell sind die hier beschriebenen Schritte aber auch mit anderen RivaTuner-Varianten wie EVGAs Precision-X möglich.

Der Afterburner bringt im Rahmen seiner Installationsroutine standardmäßig den RivaTuner Statistics Server mit, den Sie aber noch separat abnicken müssen. Der RTSS hat auch sein eigenes Tray-Icon. Die nötigen DirectX-Komponenten für Afterburner und RTSS werden ebenfalls installiert und über dxwebsetup bei Bedarf automatisch nachgeladen.

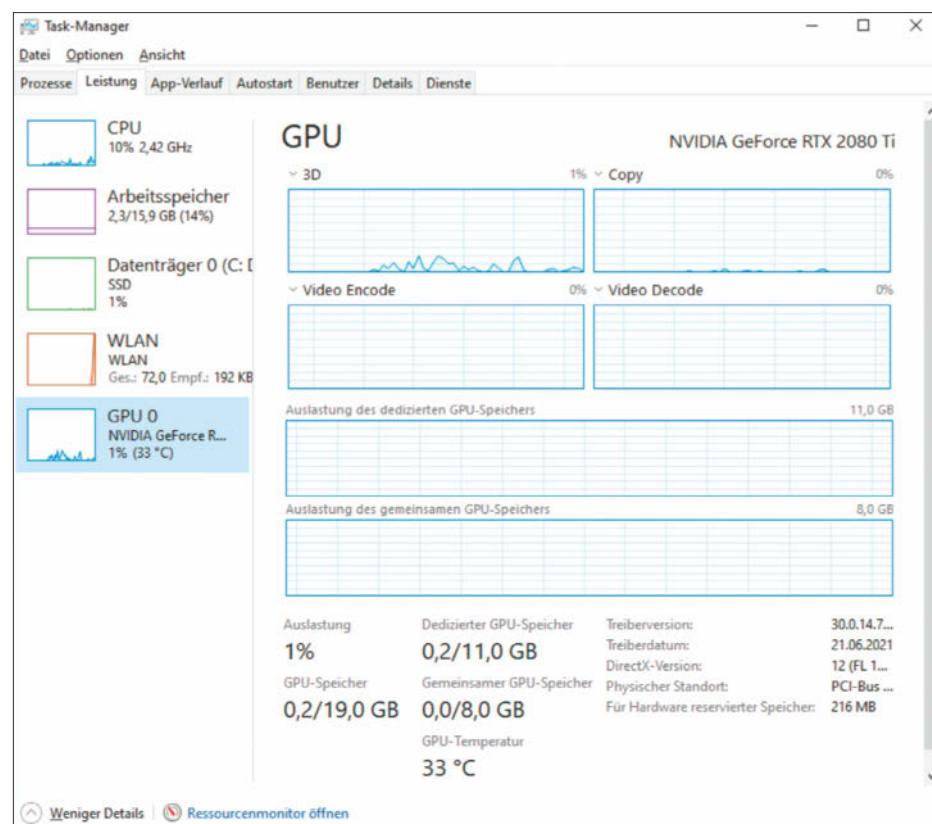
Der Afterburner ist für die Konfiguration des Overlay zuständig und liest bereits eine Menge Daten aus. Damit auch Transferraten von SSD und Netzwerk, die Temperatur mancher Mainboardsensoren oder neuere Spezialitäten wie die Speichertemperatur angezeigt werden, braucht es zusätzliche Datenquellen. Das Programm der Wahl dafür heißt HWInfo und kommt auch in der c't-Redaktion häufig zum Einsatz, zum Beispiel bei Mainboard- oder Grafikkartentests. Der Entwickler aktualisiert es häufig, sodass auch

neue Hardware meist kurz nach Bekanntwerden korrekt ausgelesen wird. Es ist wahlweise in einer portablen Version erhältlich, kommt also ohne Installation aus. Im Prinzip funktioniert das Overlay mit den 3D-Schnittstellen Direct3D 9 bis 12, Vulkan und OpenGL. Nutzt ein Programm zu exotische Rendertricks oder schlägt eine Anti-Cheat-Software im Multiplayer Alarm, können Sie versuchen, den Rendering-Mode über das Tray-Icon des RTSS umzuschalten und den Application Detection Level zu variieren.

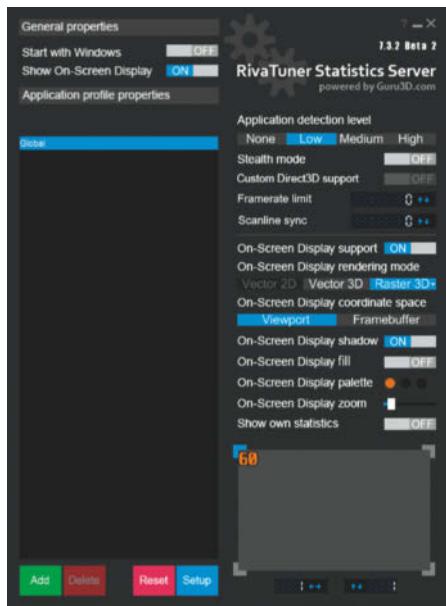
Im Dropdown von Raster3D wählen Sie die Schriftart der Anzeige, im „On-Screen Display zoom“ die Größe der Buchstaben und mit der Palette eine gut sichtbare Farbe. Mit den Koordinaten unterhalb der Overlay-Position platzieren Sie das OSD nahezu frei auf dem Bildschirm. Bei Bedarf legen Sie in diesem Fenster auch verschiedene Profile an, um optimale Sichtbarkeit in verschiedenen Spielen zu gewährleisten.

## Vorbereitungen

Zunächst müssen Sie das Overlay des Afterburners konfigurieren. Das gelingt durch einen Klick auf das Zahnradsymbol,



**Die Informationen im Task-Manager sind für manche Zwecke bereits ausreichend, etwa um einen vollen Arbeitsspeicher oder mangelnde Auslastung der Grafikkarte zu diagnostizieren**



Im RTSS-Einstellungsfenster passen Sie das Erscheinungsbild des Overlays an.

woraufhin sich die Eigenschaften des Tools in einem Standardfenster öffnen.

Zuerst sollte man dem Overlay im Reiter „On Screen Display (OSD)“ einen Umschalter zuweisen – vor allem, damit man es nach der Konfiguration nicht vergisst. Auf Standardtastaturen mit Ziffernblock haben sich dafür die NUM- oder /-Taste bewährt, die in sehr vielen Spielen mit nichts Wichtigem belegt sind. Bei der Gelegenheit kann man auch gleich die Taste fürs Bildschirmfoto im gleichnamigen Reiter auf die +-Taste im Ziffernblock legen. Dort kann man sie gut erreichen und nahezu jederzeit einen Snapshot sowohl des Spiels als auch des Overlays festhalten.

Die Hauptaufgabe wartet im Reiter Überwachung. Hier sollten Sie zuerst den Hardware-Abfragezeitraum auf 333 oder 250 Millisekunden festlegen, also drei respektive vier Mal pro Sekunde. Beim Standard-Intervall von einer ganzen Sekunde entgehen einem sonst manchmal kleine Ausschläge.

Direkt darunter sind die vom Afterburner standardmäßig auslesbaren Datenquellen aufgelistet. Diejenigen mit einem Haken davor werden ausgewertet, aber nicht standardmäßig angezeigt. Dafür braucht es im unteren Abschnitt einen Haken im Kästchen vor „Zeige On-Screen-Einblendung (OSD)“, woraufhin in der Liste unter Eigenschaften ein „in OSD“ erscheint. Wählen Sie also alle für Sie interessanten Werte an. Wir empfehlen den Prozessortakt (hier ist der Grafikprozessor

gemeint), die Speichergeschwindigkeit und die jeweiligen Temperaturen und Auslastungen. Bei der CPU-Temperatur lohnt es, für eine Problemdiagnose die Temperaturen und Takte jedes Kerns im Blick zu behalten, zur allgemeinen Kontrolle genügt die zusammenfassende Anzeige.

## Ein erster Blick

Wenn Sie sich das OSD nun am lebenden Objekt ansehen, sind die Angaben recht wild gestreut, aber in drei Gruppen zusammengefasst: GPU, MEM und CPU. Die Reihenfolge der Angaben innerhalb einer Zeile richtet sich nach der Position im Überwachungs-Reiter – sie ist per Drag & Drop änderbar. Für eine gute Übersicht sollten die Sensordaten für Taktraten, Temperaturen und Auslastung in den jeweiligen Zeilen für CPU, GPU und Speicher immer untereinander stehen.

Die Gruppenzugehörigkeit lässt sich im zugehörigen Feld bei den meisten Sensoren überschreiben, um so später externe Sensoren aus HWInfo in die Reihe der CPU-Anzeige zu platzieren oder die Speichersensoren in die GPU-Zeile zu integrieren. Letzteres gelingt, indem sie einfach ein Häkchen vor „Gruppennamen ändern“ setzen und GPU in das Feld schreiben. Nun wird der Speichertakt in der GPU-Zeile angezeigt. Wählen Sie zur Anzeige von kurzen Rucklern auch die Sensoren für Framerate und Frametime aus und ändern Sie bei letzterer noch die Anzeigeform im Dropdown-Menü von Text auf Diagramm. Auch das wird in der Liste oben angezeigt, sobald Sie auf Übernehmen geklickt haben.

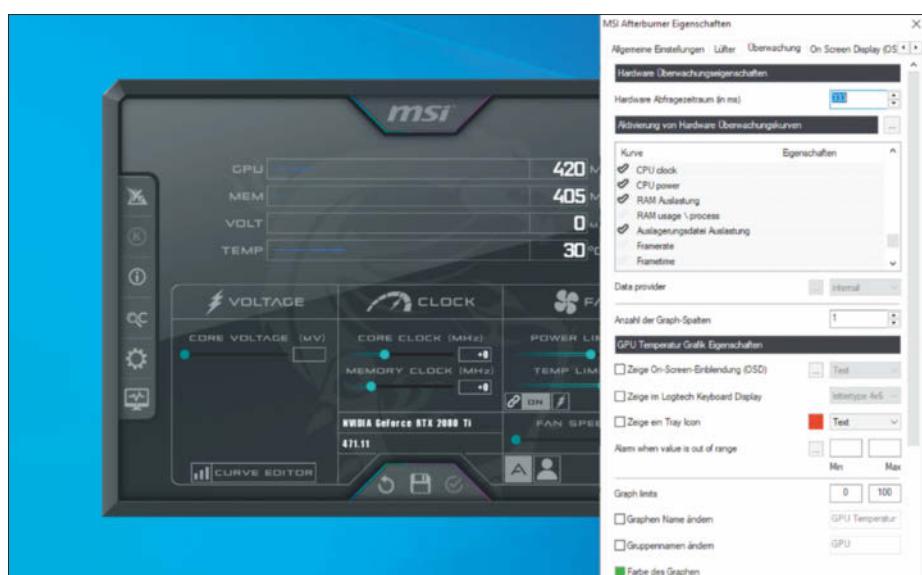
Im Reiter Überwachung haben Sie auch die Möglichkeit, Tray-Icons und Alarme für überwachte Sensoren anzulegen. Für die spätere Analyse können Sie auch einen Hotkey definieren, um eine Protokolldatei mit den Werten der ausgewählten Sensoren schreiben zu lassen.

## Die Extra-Sauce

Das bisher Beschriebene bringt nur kleine Vorteile gegenüber den Treiber-Overlays. Nützlicher wird es, wenn Sie externe Sensoren einbinden. Wir zeigen am Beispiel von HWInfo, wie das geht.

Dazu starten Sie das Programm und aktivieren im Dialog oder im Menü Settings die Option „Shared Memory Support [12-HOUR-LIMIT]“. Dies müssen Sie – vielleicht haben Sie es erahnt – alle 12 Stunden wiederholen. Zeitlich unbegrenzt funktioniert das Feature nur in der Pro-Version von HWInfo. Ältere Versionen der 6er-Generation hatten diese Einschränkung noch nicht; falls die Ihre Hardware bereits zufriedenstellend unterstützt, können Sie Version 6.42 aus dem Archiv der HWInfo-Homepage nutzen.

Mit aktivem Shared-Memory-Support ist HWInfo bereit, seine Sensorwerte mit anderen Programmen wie eben dem Afterburner zu teilen. Es muss dazu allerdings im Hintergrund laufen, die reine Sensorenansicht genügt aber. HWInfo hat sein eigenes Abfrageintervall, welches ab Werk auf viel zu langen 2 Sekunden steht. Synchronisieren Sie es am besten mit dem des Afterburners auf 250 oder 333 Millisekunden durch einen Klick auf das Zahnn-



Im Einstellungsmenü des Afterburners gilt es, im Reiter Überwachung die Anzeige der gewünschten Sensordaten für die Darstellung zu aktivieren.

rad-Symbol in der Sensorenansicht von HWInfo und dort im Feld „Global“ der Sektion „Polling Period“ im Reiter „General“ – vergessen Sie nicht, die Änderungen durch einen Klick auf „Set“ zu übernehmen.

Wechseln Sie nun zurück in den Reiter Überwachung der Afterburner-Eigenschaften. Ein Klick auf die drei Pünktchen neben „Aktivierung von Hardware Überwachungskurven“ führt zur Auswahl möglicher Plug-ins, darunter HWInfo. Markieren Sie die Zeile, setzen Sie den Haken davor und klicken auf Setup.

Im sich nun öffnenden Fenster sind ein paar Sensoren von HWInfo vorausgewählt. Klicken Sie hier auf „Add“, um zur vollständigen Liste zu gelangen.

Wir wählen im Beispiel Sensoren für den GPU-Hotspot oder die Memory Junction Temperature, die einige moderne Grafikkarten mit GDDR6-Speicher ausgeben. Dazu lassen wir die Package Power des Prozessors und die Download-, also Leseraten von SSD und der genutzten Internet-Verbindung anzeigen. Im Fenster mit den Hardware-Sensoren sollten Sie nun die zusätzlichen Werte sehen. Bestätigen Sie die offenen Fenster mit OK, bis Sie wieder in den Afterburner-Eigenschaften angekommen sind. In der Liste der Sensoren sollten die frisch ausgewählten Datenlieferanten nun ganz unten zu finden und bereits angehakt sein. Fügen Sie jedem noch ein Häkchen für die OSD-Anzeige hinzu und probieren Sie nach dem allfälligen Klick auf „Übernehmen“ das OSD dann in einem Spiel aus.

Je nach Wunsch können Sie auch Schreibraten (respektive Uploads) und die Antwortzeiten der Datenträger anzeigen lassen oder verschiedene Mainboard-Sensoren auslesen. Schieben Sie sie dann an einen Listenplatz Ihrer Wahl. Praktisch ist es, den neu hinzugefügten Werten noch Gruppennamen wie „SSD Lesen“ zu verpassen, um die Anzeigen besser auseinanderhalten zu können. Auch die GPU-Hot-Spot-Temperatur und die CPU Package Power wollen wir in den entsprechenden Zeilen haben.

Auch wenn Sie dort im Gruppennamen korrekt GPU respektive CPU einge tragen haben, macht das OSD jeweils eine neue Zeile auf. Um das zu beheben, weisen Sie der GPU-Hot-Spot-Temperatur einen neuen Typ zu: Klicken Sie im Reiter Überwachung unterhalb der Liste der Überwachungskurven auf die drei Pünktchen neben „Data Provider“ – im ausgegrauten

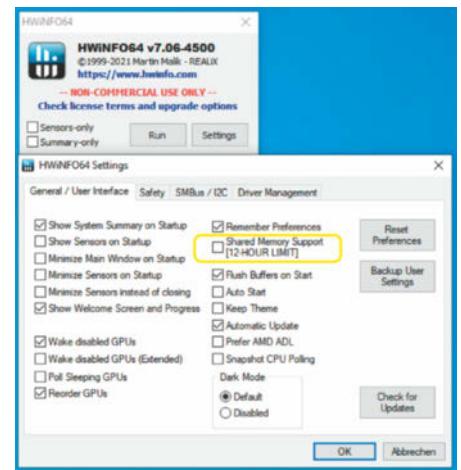
Feld sollte dort bei ausgewähltem Listen eintrag bereits HWInfo.dll und eine Zahl stehen. Im sich öffnenden Fenster wählen Sie unter „Plugin data source properties“ nun zum Beispiel den „Type“ GPU Temperature 2 und bestätigen mit OK, bevor Sie die Änderungen übernehmen.

Wer möchte, schiebt die Frame rate-Anzeige noch unter die Transferraten von SSD und Wi-Fi – das funktioniert übrigens zur Laufzeit und sollte beim Wechsel zurück zum noch laufenden Spiel direkt übernommen werden. Nun sollte die Anzeige schon in etwa so aussehen wie in unserem Aufmacherbild.

Ein paar Hinweise noch: Taktraten von CPU und Grafikkarte sind bei modernen Rechnern sehr dynamisch, sie werden üblicherweise nur so weit hinauf geschraubt wie nötig, um ein Leistungs niveau zu erreichen. Meist ist das die Refreshrate des Monitors. Spielen Sie mit 60 Hertz und vertikaler Synchronisation, berechnet der PC nicht mehr als maximal diese 60 Bilder, sodass hier auch die Taktraten häufig niedrig sind. HWInfo bietet zudem die Möglichkeit, die Lüfter zu überwachen. Wird Ihr PC zu heiß oder zu laut, behalten Sie deren Drehzahl während des Spielens nach oben beschriebenem Muster im Auge.

## Ausblick

Mit dem Afterburner, RTSS und HWInfo sind Sie gut aufgestellt, was die Hardware-Diagnose am PC angeht: Zu heiße Komponenten, Betrieb an der Leistungsgrenze oder Nachladeruckler durch zu



Damit das Overlay des Afterburners auf die HWInfo-Daten zugreifen kann, muss man alle 12 Stunden den „Shared Memory Support“ aktivieren.

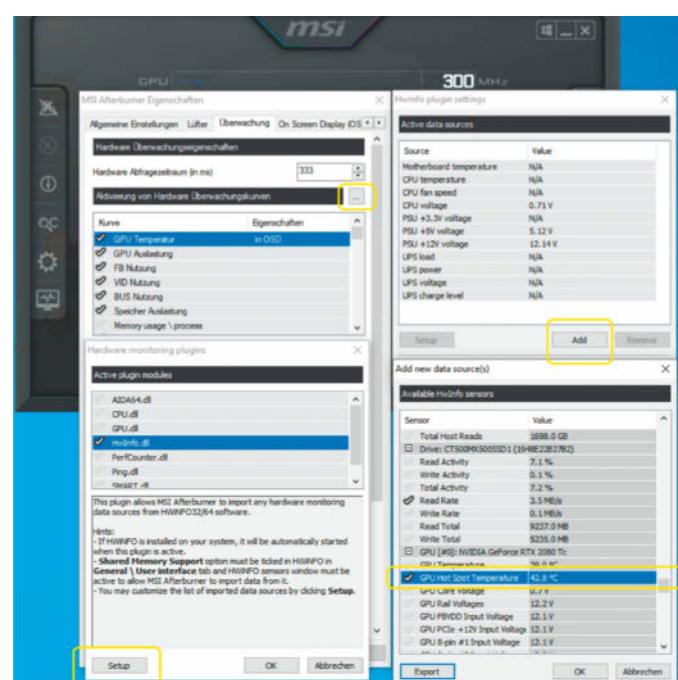
lahme Datenübertragungen sind so problemlos erkennbar. Läuft (wieder) alles rund, schalten Sie das Overlay ab, denn in Einzelfällen kann es etwas Leistung kosten.

In Verbindung mit weiteren Tools ergeben sich noch andere interessante Optionen wie Darstellung der Latenz, die wir in einem späteren Artikel separat vorstellen.  
(csp@ct.de) ct

## Literatur

- [1] Carsten Spille, Mehrwerte-Benchmark, Zu aussagekräftigen Benchmark-Ergebnissen mit ein bisschen Mathematik, c't 16/2019, S. 116

## Tools und Video: ct.de/yan1



Externe Sensoren binden Sie zur Anzeige im Overlay über das Setup des HWInfo-Plug-ins ein.



# Mit auf der Liste

## Microsoft Lists im Team verwenden

Aus den sperrigen SharePoint-Listen ist ein alltagstaugliches Werkzeug geworden: Mit Microsoft Lists lassen sich Events planen, Fehlermeldungen nachverfolgen und Kundendaten verwalten. Seitdem die App in die Teams-Umgebung eingebunden ist, gelingt das auch Personen ohne umfangreiches SharePoint-Wissen.

Von Sigrid Hess

Ob es darum geht, eine Software-Einführung zu planen, Messdaten auszuwerten oder auch nur eine Inventarliste zu nutzen und zu pflegen – in der Regel sind daran mehrere Kollegen beteiligt. Dann spielt die Microsoft-365-App Lists einen Vorteil gegenüber Excel aus: Informationen lassen sich damit datensatzweise freigeben, zuweisen und versionieren. Während Excels Speichereinheit immer die gesamte Arbeitsmappe ist, verwaltet Lists für jede Zeile einer Liste separat deren Versionsstände und die dafür geltenden Zugriffsrechte. Außerdem ist die App eng mit Teams verknüpft und kann über Power Automate mit anderen Anwendungen interagieren. Mit Regeln und Flows lassen sich komplexe Wenn-dann-Abläufe festlegen.

Wer lediglich an einfache Checklisten zum Abhaken denkt, unterschätzt das praktische Werkzeug. Viele Aufgaben, für die Excel-Nutzer gewohnheitsmäßig zum Tabellen-Klassiker greifen, lassen sich mit Lists flexibler und eleganter erledigen.

### Einrichten und loslegen

Weil Lists ein Teil von SharePoint ist, enthalten lediglich die Enterprise- und Hochschul-Lizenzen von Microsoft 365 die App; privaten Nutzern steht sie nicht zur Verfügung. Wer über ein Microsoft-365-Abo verfügt, das SharePoint umfasst, findet sie nach der Anmeldung auf [www.office.com](http://www.office.com) unter „Alle Apps“. Falls Sie den kurzen Weg über die Taskleiste schätzen: Öffnen Sie die App einmal in Edge, klicken Sie auf die drei Punkte ganz rechts oben und wählen Sie „Apps/Diese Site als eine App installieren“. Anschließend können Sie das gelb-rot-violett gestreifte Lists-Icon an der Taskleiste anheften.

Seit einiger Zeit gibt es auch Lists-Apps für Mobilgeräte. Auf einem kleinen Smartphone-Bildschirm kann man umfangreiche Listen zwar nur mühsam betrachten und bearbeiten, aber die Mobil-

Apps erweisen sich in bestimmten Situationen doch als praktisch, etwa um schnell ein Bild einzufügen oder einen Barcode zu scannen und die ausgelesene Information in eine vorhandene Liste zu übernehmen. Die Mobil-Apps befinden sich noch in einem frühen Stadium; aktuell entspricht ihr Funktionsumfang noch nicht dem der Web-Anwendung.

Legen Sie eine Liste in Lists an, gilt es mehr zu bedenken als bei einer Excel-Tabelle. Grundsätzlich gibt es drei Wege, um zu starten: Sie können eine der mitgelieferten Vorlagen verwenden und anpassen, eine vorhandene Excel-Tabelle in Lists importieren oder die geplante Liste ganz frei erstellen. So oder so zahlt sich gute Planung zu Anfang aus: Einmal mit der passenden Struktur eingerichtet, nehmen die Listen Ihnen und den Anwendern später viel Arbeit ab. Die reine Dateneingabe erlernen auch weniger versierte PC-Nutzer rasch.

### Inventarliste aus einer Vorlage

Eine Übersicht aller Vorlagen erreichen Sie nach einem Klick auf die Schaltfläche „+ Neue Liste“ oben. Aktuell gibt es acht von Microsoft bereitgestellte Vorlagen. Deren Namen vermitteln eine erste Idee von typischen Anwendungsszenarien: Problemverfolgung, Mitarbeiter-Onboarding, Ereignisablaufplan, Ressourcenverwalter, Personalbeschaffungsstracker, Reiseanfragen, Arbeitsstatus-Tracker und Inhaltsplaner. Die großen Icons deuten Struktur und Zweck der vorgefertigten Listen an. Mit einem Klick darauf öffnen Sie eine Vorlage und können prüfen, ob sie für Ihre Aufgaben die richtige ist. Falls ja, legen Sie über die Schaltfläche „Vorlage verwenden“ eine Kopie dieser Liste an. Wenn Sie beispielsweise eine Inventarliste anlegen möchten, eignet sich die Vorlage „Ressourcenverwalter“ besonders gut.

Auf die Auswahl der Vorlage folgt ein Dialog, in dem Sie Name, Beschreibung, Symbol, Farbmarkierung und Speicherort Ihrer neuen Liste anpassen. Wichtig: Wenn Sie als Speicherort die Voreinstellung „Meine Listen“ übernehmen, bleibt die Liste in Ihrem Bereich und ist auch nur für Sie verfügbar. Falls die Datei später innerhalb von Teams bearbeitet werden soll, wählen Sie stattdessen die Teams-Website Ihrer Arbeitsgruppe als Speicherort aus.

Die Struktur der Vorlage wird nur selten genau für den eigenen Zweck passen. Sie können sie kinderleicht modifizieren,

indem Sie überflüssige Spalten löschen und weitere hinzufügen. Die Reihenfolge der Spalten ändern Sie einfach per Drag & Drop im Spaltenkopf. Um Änderungen an einer Spalte vorzunehmen, klicken Sie auf den Spaltenkopf und wählen „Spalteneinstellungen/Bearbeiten“. Die Schaltfläche „+ Spalte hinzufügen“ finden Sie ganz am Ende hinter der aktuell letzten Spalte. Falls Sie eine für Standardmetadaten wie das Erstelltdatum des Eintrages oder den Namen des Erstellers ergänzen möchten, prüfen Sie zuerst den untersten Menüpunkt „Spalten ein-/ausblenden“ – möglicherweise ist die gewünschte Spalte bereits vorhanden und lediglich ausgeblendet.

Möchten Sie dagegen eine Spalte für spezifische Inhalte hinzufügen, etwa eine Dropdown-Auswahl für die Standorte der Niederlassungen Ihres Unternehmens, geht es weiter mit einem Klick auf „Mehr...“. Vergeben Sie nun einen Namen für die Spalte und wählen Sie den Inhaltstyp „Auswahl“. Tippen Sie eine kurze Beschreibung als Hilfe ein und entscheiden Sie, ob es sich um ein Pflichtfeld handeln soll. Dann geben Sie die Antwortvorgaben ein. Weiter unten können Sie noch zwischen Dropdown-Menü, Optionsfeldern oder Kontrollkästchen als Darstellungsform wählen.

Häufig ist es sinnvoll, eine Standardauswahl festzulegen: Falls sich der Hauptsitz Ihrer Firma beispielsweise in Hannover befindet und daneben kleinere Niederlassungen in München und Frankfurt existieren, legen Sie die Standardauswahl auf

„Hannover“ fest und ergänzen die beiden anderen Städte als weitere Optionen.

Wollen Sie eine Spalte löschen, wählen Sie nach einem Klick auf den Spaltenkopf ebenfalls „Spalteneinstellungen/Bearbeiten“. Ganz unten im „Spalten bearbeiten“-Dialog finden Sie die Schaltfläche zum Löschen.

### Spalten formatieren

Sobald die Struktur der Liste passt, geht es an die Feinarbeit. Je nach Art der darin enthaltenen Daten können Sie Spalten unterschiedlich formatieren. Auch dafür gibt es vorbereitete Vorlagen. Zu diesen gelangen Sie nach einem Klick auf den Spaltenkopf über „Spalteneinstellungen/Diese Spalte formatieren“. Lustig: Im Formatierungsdialog bietet Lists mitunter „Pillen der Wahl“ an – ein Beispiel dafür, was bei automatischer Übersetzung herauskommen kann. Gemeint sind unterschiedliche Darstellungsoptionen für Listeninhalte in Form von runden, bunten Labeln.

Damit die fertige Liste von allen im Team genutzt und gepflegt werden kann, erstellen Sie im Teams-Kanal Ihrer Arbeitsgruppe eine neue Registerkarte und wählen „Vorhandene Liste des Teams“ aus. Kollegen können die Liste dann später direkt in Microsoft Teams mit neuen Daten bestücken, filtern oder sortieren. Ein positiver Nebeneffekt: Pflege und Nutzung der Daten sind vom Bearbeiten der Struktur einer Liste klar getrennt. Wer die Liste in Teams öffnet, kann lediglich deren

**Lists verwaltet Daten in Form von Tabellen. Sie lassen sich flexibel sortieren, gruppieren und filtern.**

**Legen Sie eine Liste an, fragt Lists nach Namen, Beschreibung, Farbcodierung und Icon. Als Speicherort sollten Sie die Teams-Website wählen.**

## Einstellungen › Spalte erstellen

Name und Typ  
Geben Sie einen neuen Namen für diese Spalte ein, und wählen Sie den Typ der Informationen aus, die Sie in dieser Spalte speichern möchten.

Spaltenname: Standort

Der Informationstyp in dieser Spalte ist:  
 Eine Textzeile  
 Mehrere Textzeilen  
 Auswahl (Menü)  
 Zahl (1 / 1,0 / 100)  
 Währung (\$, Y, €)  
 Datum und Uhrzeit  
 Nachschlagen (in Informationen, die...  
 Ja/Nein (Kontrollkästchen)  
 Person oder Gruppe  
 Link oder Bild  
 Berechnet (Berechnung basiert auf a...  
 Bild  
 Ergebnis der Aufgabe

Zusätzliche Spalteneinstellungen  
Bitte geben Sie die detaillierten Optionen für den von Ihnen ausgewählten Informationstyp an.

Beschreibung: Welchem Standort ist das Gerät zugeordnet?

Diese Spalte muss Informationen enthalten:  
 Ja  Nein  
Eindeutige Werte erzwingen:

**Wenn bei den Standardspalten einer Vorlage nichts Passendes dabei ist, können Sie Spalten nach Bedarf maßschneidern.**



Inhalt bearbeiten, jedoch keine Änderungen am Aufbau der Liste vornehmen. Die Bearbeitungsoptionen erreicht man über „..../In SharePoint öffnen“.

### Import aus Excel

Als zweites Beispiel dient eine sogenannte LOP (Liste offener Punkte), die mehrere Kollegen gemeinsam nutzen. Falls diese die LOP-Liste bisher in Excel gepflegt haben, kam es vielleicht auch vor, dass Teammitglieder in der Zeile verrutscht sind und vernehmlich eine noch offene Aufgabe als „erledigt“ markiert haben. Solche Schnitzer passieren in Lists nicht so leicht.

Für den Import einer Tabelle aus einer Excel-Datei als Liste in Lists müssen die Daten in Excel als „Formatierte Tabelle“ vorliegen. Ist dies noch nicht der Fall, stellen Sie in Excel den Cursor irgendwo in die Tabelle und drücken Sie dann Strg+T. In Lists erhalten Sie bei der Datenübernahme Vorschläge für den Spaltentyp aller Spalten. Korrigieren Sie alle falsch vorgeschlagenen Typen; durch Wahl der Option „Nicht importieren“ lassen sich Spalten

Spalte bearbeiten

Weitere Informationen zu Spaltentypen und -optionen.

Name \*  
Standort

Beschreibung  
Welchem Standort ist das Gerät zugeordnet?

Typ  
Auswahl

Auswahlmöglichkeiten \*  
Hannover  
Frankfurt a. M.  
München

+ Auswahl hinzufügen

Kann Werte manuell hinzufügen ⓘ

Standardwert  
Hannover

**Für jede Spalte der Datentabelle können Sie – in Abhängigkeit vom Spaltentyp – eine ganze Reihe von Eigenschaften festlegen.**

**Den Inhalt von Listen kann man direkt in Teams bearbeiten; um die Struktur einer Liste zu verändern, muss man sie in SharePoint öffnen.**

vor Anlage der Liste von der Übernahme ausnehmen. Wenn alles passt, gelangen Sie durch Klick auf „Weiter“ zu einem Dialog, mit dem Sie die Liste anlegen.

In der Teams-Ansicht füllt die Eingabemaske, die Sie mit „+ Neues Element“ oder „Bearbeiten“ erreichen, das komplette Fenster aus. Wer also nur Daten erfasst, filtert und abliest, kann alles direkt auf der Registerkarte erledigen. Dabei ist nur der aktuelle Datensatz aktiv – Verrutschen ausgeschlossen. Eingefleischte Excel-Nutzer, die das nervt, wählen stattdessen „In Rasteransicht bearbeiten“. In dieser Ansicht können Sie Daten direkt in der Tabellenansicht eingeben und Felder auch – wie von Excel gewohnt – füllen, indem Sie am Kreuz ziehen.

Für die tägliche Arbeit mit Listen bietet Lists viele weitere Komfortfunktionen. Beispielsweise lassen sich Daten flexibel filtern und gruppieren. Die dabei erstellten Ansichten lassen sich mit einem Namen versehen, speichern und später jederzeit mit zwei Klicks aktivieren. Sie finden gespeicherte Ansichten unter dem Eintrag

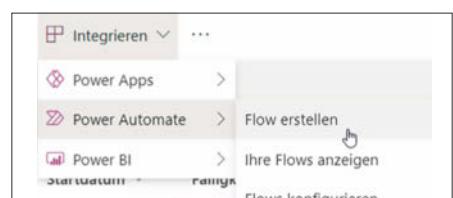
„Alle Elemente“ oben rechts in der Menüzeile. Für eine Aufgabe zuständige Personen können sich vor dem Fälligkeitsdatum benachrichtigen lassen.

### Unterschrift oder Genehmigung einholen

Ist die Liste auf der Website Ihrer Arbeitsgruppe gespeichert, können Sie über Power Automate [1] einen Workflow einrichten, um eine Unterschrift anzufordern oder eine Genehmigung einzuholen. Dass dieselbe Funktion bei Lists „Unterschrift“, bei Teams aber „Genehmigung“ heißt, gehört zu den Ungereimtheiten der Microsoft-365-Welt.

Um einen Genehmigungslauf zu starten, markieren Sie das genehmigungspflichtige Element beziehungsweise den Datensatz, für den eine Genehmigung eingeholt werden soll. Nach Klick auf „Automatisieren/Unterschrift anfordern“ öffnet sich rechts der Bereich „Flow erstellen“. Eventuell müssen Sie einmalig den Zugriff auf SharePoint, Genehmigungen und Benachrichtigungen erlauben; falls hinter den drei Icons dieser Apps ein grünes Häkchen erscheint, sind Sie startklar. Mit „Weiter“ geht es zur Auswahl der genehmigungsberechtigten Personen und zur Eingabe einer obligatorischen Notiz an die Adressaten. Danach starten Sie den Flow. Die Anfragen kommen sowohl im Feed in Teams als auch per E-Mail bei den Adressaten an und können auf demselben Weg beantwortet werden. Als anfragende Person erhalten Sie ebenso Nachricht über eine Genehmigung oder Ablehnung.

Die Liste erhält mit diesem Lauf automatisch eine weitere Spalte: „Status Unterschrift“. So lässt sich jederzeit ablesen, in welchem Genehmigungsstatus sich ein Vorgang befindet. Beide Ansichten – in der Liste alles, was die zugehörigen Vorgänge betrifft, und in der Teams-App alles, was einzelne Personen betrifft – helfen, den Überblick zu behalten: Man muss nicht mehr nach einer E-Mail suchen, in welcher ein OK gegeben wurde, sondern findet alle Informationen dazu übersichtlich an einer Stelle.



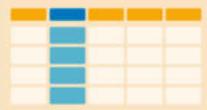
**Über das Integrieren-Menü besteht aus Lists heraus Zugriff auf Power Automate.**

**Alle Ihre gesendeten und erhaltenen Genehmigungen haben Sie jederzeit in Teams im Bereich „Genehmigungen“ im Blick – egal woher sie kamen.**

### Regel erstellen

Erstellen Sie Regeln für Aktionen, die bei Änderungen an Daten in dieser Liste ausgeführt werden sollen. Wählen Sie eine Bedingung aus, die die Regel ausgelöst werden soll. Weitere Informationen

Jemanden benachrichtigen, wenn



Eine Spalte ändert sich



Ein Spaltenwert verändert sich



Ein neues Element wurde erstellt

**Mit Regeln lassen sich Aktionen festlegen, die automatisch ausgeführt werden, sobald jemand ein Listen-Element oder eine ganze Spalte verändert.**

Interessant sind auch die weiteren Regeln, die sich unter „Automatisieren/Eine Regel erstellen“ anlegen lassen. Hier können Sie beispielsweise Benachrichtigungen an Personen veranlassen, die in einer Liste in der Verantwortlich-Spalte geführt werden. Der Trigger kann möglicherweise sein, dass jemand einen Eintrag ändert, einen neuen Datensatz anlegt, eine Spalte ändert oder einen Datensatz löscht. So könnten aus der LOP-Liste heraus alle für eine Aufgabe verantwortlichen Personen automatisch eine Nachricht erhalten, sobald der Wert in der Priorität-Spalte auf „kritisch“ wechselt.

Automatische Benachrichtigungen lassen sich auch in Abhängigkeit von einem Datum einrichten, zum Beispiel immer zwei Tage vor dem Fälligkeitsdatum einer Aufgabe. Dazu wählen Sie „Automatisieren/Erinnerung festlegen/Fälligkeitsdatum“. Der gewünschte Flow wird daraufhin vorbereitet, Sie vergeben lediglich einen Namen und tragen die Anzahl der Tage ein. Um einen bestehenden Flow anzupassen, wählen Sie „Integrieren/Power Automate/Ihre Flows anzeigen“.

Falls Sie über Genehmigungen und Benachrichtigungen hinaus weitere Workflows automatisieren möchten, beispielsweise ein Posting in einem Teams-Kanal, sobald ein neuer Listen-Eintrag erstellt wurde, lässt sich auch das ohne Programmierkenntnisse machen („Integrieren/Power Automate/Flow erstellen“). Auf der rechten Seite erscheinen Vorlagen für Flows; nach Klick auf „Mehr anzeigen“ sehen Sie auch eine Vorlage für ein Posting in Teams. Diese Vorlage können Sie im Bereich der Flow-Konfiguration bei Bedarf anpassen. So wählen Sie im unteren Fen-

ter beispielsweise aus, ob das Posting vom Flow-Bot oder vom User kommen und wo genau es gepostet werden soll.

### Versionierung und Berechtigungen

Da Lists jeden Datensatz als eine Speicher-Einheit verwaltet, lässt sich in der Browseransicht der Verlauf jedes einzelnen Datensatzes abrufen. Mit einem Klick auf das kleine „i“ in der oberen rechten Ecke öffnen Sie den Detailbereich. Scrollen Sie darin nach unten bis zum Bereich „Aktuelle Aktivitäten“, um diese Informationen einzusehen.

Aktuell archiviert Lists standardmäßig 50 Versionen jedes Datensatzes. Wenn

**Im Abschnitt „Aktuelle Aktivitäten“ innerhalb des sogenannten Detailbereichs lassen sich die Bearbeitungsschritte jedes einzelnen Datensatzes abrufen.**

Sie das für Ihre Liste ändern möchten, wechseln Sie in die SharePoint-Ansicht und dort über das Zahnrad oben rechts zu den Listeneinstellungen. Unter dem Menüpunkt „Versionsverwaltungseinstellungen“ können Sie Änderungen vornehmen.

Eine Liste, die einem Team zugeordnet ist, erbt die Berechtigungen dieses Teams. Welche Personen Mitglieder des Teams sind, können Sie auf der SharePoint-Seite über die Schaltfläche „Mitglieder“ ersehen. Es ist möglich, Berechtigungen darüber hinaus differenzierter zu vergeben oder Berechtigungen an Personen außerhalb des Teams hinzuzufügen – sowohl für die gesamte Liste als auch für einzelne Listen-Elemente. Klicken Sie dazu im Detailbereich auf „Zugriff verwalten“. Doch Vorsicht: Machen Sie, wenn überhaupt, klare zusätzliche Vorgaben – zu groß ist sonst die Gefahr eines Zugriffs-Wirrwars.

### Einen Blick wert

Wenn Listen im Spiel sind, greifen Excel-Kenner am ehesten zur vertrauten Tabellenkalkulation mit ihren flexiblen Tabellenstrukturen und vielfältigen Sortier- und Filtermöglichkeiten. Je nach Anwendungsfall lohnt es jedoch, sich die Zeit zur Einarbeitung in Lists zu nehmen. Insbesondere wenn Ablaufpläne, Status-Tracker oder Materiallisten im Team bearbeitet werden sollen, bietet sich die App mit Versionierung und detaillierten Freigaben als geeignete Alternative an. (dwi@ct.de) ct

### Literatur

- [1] Dorothee Wiegand, Power to the People, Routine-aufgaben mit Power Automate automatisieren, c't 8/2021, S. 58



Tastatur und Display anzuschließen, oder sich mit WebVNC-Konsolen eines Hosters herumzuschlagen, geht es auch ganz bequem per SSH, egal ob vom Linux-Rechner, dem Windows-PC oder vom Mac aus.

Das Prinzip ist schnell erklärt: Während des Bootvorgangs startet ein Linux-System aus dem Initramfs-Image, das Hilfsprogramme und Treiber enthält. Steckt darin ein minimaler SSH-Server, kann man sich mit diesem verbinden und in der SSH-Sitzung die verschlüsselte Systempartition entsperren. Nach erfolgreicher Passwort-Eingabe beendet der SSH-Server die Verbindung, und das System setzt den Start wie gewohnt fort.

Da die Nutzer- und Passwortdaten auf der verschlüsselten Systempartition beim Booten noch nicht zugänglich sind, authentifiziert der SSH-Server die Nutzer stattdessen anhand eines Public-Key-Verfahrens mit vorher im Initramfs hinterlegten SSH-Keys. Durch die verschlüsselte SSH-Verbindung wird das LUKS-Kennwort sicher übertragen.

Die folgende Anleitung erklärt die notwendigen Befehle Schritt für Schritt beispielhaft unter Linux. Mit Server ist der Computer gemeint, der entschlüsselt werden soll, der PC ist der persönliche Computer oder Laptop, von dem aus man sich zum Entsperrn einloggt.

### Server Installation

Debian, Ubuntu und davon abgeleitete Linux-Systeme bringen in ihren Repositories das Paket „dropbear-initramfs“ mit, das die notwendigen Bestandteile enthält. Anderen Distributionen fehlt so ein vorkonfiguriertes Paket leider.

Installieren Sie zunächst auf dem Server das Paket dropbear-initramfs:

```
sudo apt install dropbear-initramfs
```

Während der Installation erzeugt Dropbear die benötigten Schlüssel (Host-Keys) und gibt für jeden Schlüssel je einen Fingerprint und eine wirre ASCII-Grafik aus. Mit den ausgegebenen Fingerprints kann man beim Aufbau der SSH-Verbindung den Host-Key des Servers verifizieren. Die ASCII-Grafik ist als visuelle Hilfe gedacht, aber wird für diese Anleitung nicht weiter benötigt. Die Installation endet mit einer Warnung, dass es wegen einer fehlerhaften authorized\_keys-Datei nicht möglich sei, die Systempartition aus der Ferne zu entsperren. Ignorieren Sie die Warnung vorerst.

# Aufsperrren aus der Ferne

## Verschlüsselte Linux-Systeme über SSH entsperren

**Eine verschlüsselte Linux-Systempartition schützt die gespeicherten Daten, aber nach einem Neustart verlangt das System in der Regel ein Passwort zum Entsperren. Das geht bequem und trotzdem sicher über das Netzwerk. Bei Debian, Ubuntu & Co. hilft dabei ein speziell vorbereitetes Paket.**

Von Keywan Tonekaboni

**D**as gesamte System zu verschlüsseln, ist grundsätzlich empfehlenswert. Und sei es nur, damit Unbefugte auf ent-sorgten Datenträgern keine persönlichen Dateien finden. Unter den meisten Linux-Distributionen lässt sich die Verschlüsse-lung mit LUKS komfortabel direkt bei der Installation einrichten, auch für die Systempartition. Was auf dem PC oder Laptop eine Lappalie ist, rangiert auf dem Server zwischen nervig und anspruchs-voll: die Eingabe des LUKS-Passworts während des Bootvorgangs. Statt hinter den heimischen Server zu krabbeln, um

Notieren Sie sich den Fingerprint des ECDSA- oder RSA-Schlüssels. Die Unterschiede zwischen den Schlüsselverfahren haben wir in [1] erläutert. Der Fingerprint wird jeweils über der ASCII-Grafik angezeigt. Er beginnt mit der Schlüssellänge und dem Hash-Verfahren, gefolgt von einem Buchstabensalat (zum Beispiel „2048 SHA256:sqPNOB/CgTSCdK6...“) und endet mit den Daten des Servers und dem verwendeten Algorithmus („root@laborserver (RSA)“).

Als Nächstes müssen Sie den öffentlichen Teil Ihres SSH-Schlüsselpaares in der Dropbear-Konfiguration hinterlegen. Diesen Public-Key finden Sie auf dem PC in Ihrem Benutzerverzeichnis im Unterordner .ssh, also unter Linux sowie macOS ~/ssh oder %HOMEPATH%\ssh\ bei Windows. Der Public-Key hat einen Dateinamen wie id\_rsa.pub, id\_ecdsa.pub oder ähnlich.

Wenn Sie noch kein persönliches SSH-Schlüsselpaar haben, dann generieren Sie dieses auf der Kommandozeile mit ssh-keygen. Dropbear unterstützt nur Schlüssel vom Typ DSA, RSA und ECDSA. DSA gilt zwar noch als sicher, ist aber veraltet. Üblicherweise erzeugt ssh-keygen ein RSA-Schlüsselpaar. Bevorzugen Sie lieber einen schlanken ECDSA-Schlüssel, geben Sie dies mit der Option -t an:

```
ssh-keygen -t ecdsa
```

Zunächst fragt der Befehl den gewünschten Speicherort ab, wobei Sie die Vorgabe /home/USER/.ssh/id\_ecdsa unverändert mit Enter bestätigen können. Daraufhin fragt ssh-keygen nach einem Kennwort (Passphrase), mit dem der Schlüssel vor unerlaubter Verwendung geschützt wird. Diese Passphrase sollten Sie festlegen. Mehr zu SSH und ssh-keygen steht in [2,3].

## Öffentlichen Schlüssel hinterlegen

Haben Sie bei der Schlüsselgenerierung als Speicherort .ssh/id\_ecdsa angegeben, finden Sie den öffentlichen Schlüssel in der Datei .ssh/id\_ecdsa.pub. Kopieren Sie nun den Inhalt dieser Datei. Wechseln Sie wieder auf den Server und führen Sie die folgenden Schritte per sudo oder als root mit Superuser-Rechten aus. Öffnen Sie mit einem Editor Ihrer Wahl die Datei /etc/dropbear-initramfs/authorized\_keys beziehungsweise legen Sie diese neu an. Fügen Sie dort dann den kopierten Schlüssel ein, aber in einer einzigen Zeile

```
Generating Dropbear ECDSA host key. Please wait.
Generating 256 bit ecdsa key, this may take a while...
256 SHA256:WB22e4KGR+fEY4UMoss5qdtVUriaH+uLGrJ27a2U0Q root@laborserver (ECDSA)
[ECDSA 256]-----+
| . .00..
| . 0E+0+
| . .+ 0
| . + B- o
| * =S +
| o =-
| . * +..
| o B+B
| . ++X+
[SHA256]-----+
update-initramfs: deferring update (trigger activated)
Dropbear has been added to the initramfs. Don't forget to check
your "ip=" kernel bootparameter to match your desired initramfs
ip configuration.

Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for initramfs-tools (0.136ubuntu6.3) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-77-generic
dropbear: WARNING: Invalid authorized_keys file, remote unlocking of cryptroot via
SSH won't work!
[Progress: 94% [#####
#].....]
```

und ohne Umbrüche. Für jeden weiteren Schlüssel legen Sie eine neue Zeile an. Die authorized\_keys-Datei sieht dann grob so aus:

```
ssh-rsa AAAAB3NzaC1... cttest@laborratte
ecdsa-sha2-nistp256 AAAA... ct@labormaus
```

Die Nutzerkennung am Ende dient nur menschlichen Betrachtern zur Orientierung und wird bei Aufbau der SSH-Verbindung nicht abgeglichen oder anderweitig überprüft.

Als Nächstes legen Sie fest, dass nach einer erfolgreichen Verbindung mit dem Dropbear-SSH-Server dieser direkt den Befehl zum Entsperrnen der Systempartition aufruft (cryptroot-unlock). Öffnen Sie dazu die Datei /etc/dropbear-initramfs/config und passen Sie die Zeile mit DROPBEAR\_OPTIONS entsprechend an:

```
DROPBEAR_OPTIONS="-c cryptroot-unlock"
```

Wer sich gut mit SSH auskennt, könnte auf die Idee kommen, den Aufruf von cryptroot-unlock über die authorized\_keys zu erzwingen. Das klappt zunächst auch, aber wenn man sich beim LUKS-Passwort

**Während der Installation zeigt Dropbear die Fingerprints der SSH-Host-Keys an, mit denen man später die Verbindung verifizieren kann.**

vertippt, ist man über SSH ausgesperrt. Mit der empfohlenen Methode erfragt das Skript erneut das LUKS-Passwort.

Wenn auf Ihrem Server auch ein regulärer SSH-Server läuft, sollten Sie auf Ihrem PC die SSH-Konfiguration anpassen, damit der SSH-Client dort den Dropbear-Server zum Entsperrnen und den regulären SSH-Server auseinanderhalten kann. Beide haben unterschiedliche Host-Keys und das würde stets für Warnungen sorgen.

Für beide SSH-Server den gleichen Host-Key zu verwenden, ist eine schlechte Idee, da der Host-Key des Dropbear-Servers unverschlüsselt im Initramfs-Archiv liegt. Außerdem speichern Dropbear und OpenSSH den Host-Key in unterschiedlichen Formaten. Sortieren können Sie dies, indem Sie den Dropbear-Server auf einem anderen Port lauschen lassen. Dafür ergänzen Sie bei DROPBEAR\_OPTIONS die Angabe -p 2222, wobei 2222 für den von Ihnen frei gewählten Port steht.

## IP-Adresse festlegen

Mit Dropbear an Bord versucht das Initramfs-System, eine IP-Adresse per DHCP zu beziehen. Eine feste IP-Adresse können

```
3.1868901 raid6: using algorithm avx512x4 gen(0) 19161 MB/s
3.1064421 raid6: .... xor() 10225 MB/s, rmw enabled
3.1079271 raid6: using avx512x2 recovery algorithm
3.1155831 xor: automatically using best checksumming function avx
3.1257491 async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... Volume
Cannot process volume group ubuntu-vg
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Listening on LPF/ep1s8/52:54:00:41:e1:2b
Sending on LPF/ep1s8/52:54:00:41:e1:2b
Sending on Socket/fallback
DHCPDISCOVER on ep1s8 to 255.255.255.255 port 67 interval 3 (xid=0xc69a367f)
DHCPOFFER from 192.168.122.98 to 192.168.122.1
DHCPREQUEST for 192.168.122.98 on ep1s8 to 255.255.255.255 port 67 (xid=0x7f369ac6)
DHCPACK from 192.168.122.98 to 192.168.122.1 (xid=0xc69a367f)
Please unlock disk dm_crypt-0: bound to 192.168.122.98 -- renewal in 1377 seconds.
Begin: Starting dropbear ...
```

**Mit Dropbear-Initramfs wird recht früh im Bootprozess eine IP-Adresse per DHCP geholt. Das System akzeptiert das LUKS-Kennwort anschließend per SSH oder über die lokale Konsole.**

Sie dem Startprozess über eine Kernel-Option verpassen. Diese IP-Adresse ist unabhängig von der Netzwerkkonfiguration des Servers selbst. Fügen Sie für eine statische IP-Adresse in der Datei /etc/initramfs-tools/initramfs.conf die Variable `IP=` hinzu, deren Inhalt nach dem Schema `IP=IP-Adresse:NFS-Server:Gateway:Netzmaske:Hostname:Device:` aufgebaut ist. Nicht benötigte Felder wie das des NFS-Servers lassen Sie leer. Für die statische IP-Adresse 192.168.122.90 sieht die minimal notwendige Konfiguration so aus:

```
IP=192.168.122.90::192.168.122.1:  
      255.255.255.0:
```

Wichtig sind die zwei Doppelpunkte zwischen IP- und Gateway-Adresse, da das Feld für den NFS-Server leer bleibt. Übrigens bleibt die IP-Adresse dem Server

dauerhaft zugewiesen, auch nachdem das System komplett gebootet ist und seine eigene Netzwerkkonfiguration angewendet hat. Verwenden Sie daher in beiden Setups dieselbe IP-Adresse, um Probleme zu vermeiden.

Wenn Sie die SSH-Keys hinterlegt und die Konfiguration angepasst haben, müssen Sie noch das Initramfs-Image neu erzeugen:

```
update-initramfs -u
```

Diesen Aufruf müssen Sie immer dann wiederholen, wenn Sie etwas an der Dropbear-Konfiguration ändern, die SSH-Keys austauschen oder neue hinzufügen. Hat alles geklappt, sollte auch keine Warnung mehr über eine ungültige `authorized_keys`-Datei kommen, wie noch nach der Installation. Der Server ist

nun bereit, per SSH die Systempartition zu entsperren.

## Sesam, öffne dich

Starten Sie den Server neu und prüfen auf dem PC mit `ping IP-ADRESSE`, wann der Server wieder erreichbar ist. Sobald `ping` ein Lebenszeichen liefert, bauen Sie mit dem SSH-Client die Verbindung auf:

```
ssh -p 2222 root@192.168.122.90
```

Passen Sie die IP-Adresse entsprechend Ihrer Konfiguration an und lassen Sie die Option `-p 2222` weg, wenn Sie keinen alternativen Port festgelegt haben. Der Dropbear-Server erwartet eine Verbindung für den User.

Bei der ersten Verbindung fordert der SSH-Client auf, den Fingerprint zu bestätigen. Sie sollten die angezeigte Prüfsumme mit dem bei der Installation von Dropbear ausgegebenen Fingerprint vergleichen. Bestätigen Sie, indem Sie im Terminal „yes“ eintippen. Sie können stattdessen den am Anfang kopierten Fingerprint einfügen, dann vergleicht der SSH-Client die Fingerprints für Sie miteinander. Dabei fügen Sie nur den Mittelteil („SHA256:AbC...dEf“) ohne Schlüssellänge und Nutzerkennung ein. Passt der Fingerprint nicht, dann haben Sie vielleicht nur den Fingerprint des falschen Schlüssels verglichen, zum Beispiel jenen des RSA- statt des ECDSA-Keys. Akzeptierten Sie den angezeigten Fingerprint, hinterlegt der SSH-Client diesen in der Datei `~/.ssh/known_host`.

Kommt die SSH-Verbindung zustande, sollten Sie die Aufforderung „Please unlock disk dm\_crypt-0:“ sehen. Geben Sie das LUKS-Kennwort ein. Sobald Cryptsetup die Systempartition erfolgreich entschlüsselt hat, beendet Dropbear die SSH-Verbindung. Wenn das System erfolgreich gestartet ist, können Sie sich über den OpenSSH-Server wie gewohnt anmelden. Wer nicht jedes Mal den sperriegen SSH-Befehl eingeben will, nutzt stattdessen ein Alias für den Zielhost. Wie das geht, erklärt der Kasten „SSH Abkürzungen“. Das spart Tipparbeit und schont die grauen Zellen. (ktn@ct.de) **ct**

## SSH-Abkürzungen

Statt bei jeder Verbindung Angaben wie User, Port und IP-Adresse lästig einzutippen, kann man für einzelne Hosts oder ganze Rechnergruppen Vorgaben für den SSH-Client festlegen. Diese Profile definieren Sie in der Datei `~/.ssh/config`. Die Einstellungen schreibt man hinter den Namen der jeweiligen Option. Welche es gibt und wie die heißen, zeigt `man ssh_config` an. Das Schlüsselwort `Host` markiert einen neuen Eintrag und verpasst dem im Folgenden beschriebenen System einen frei wählbaren Namen. Alle weiteren Zeilen bis zur nächsten Host-Zeile gehören zusammen. Das Beispiel definiert den Alias „`laborserver`“ und legt IP-Adresse, Port und Username fest:

```
Host laborserver  
HostName 192.168.122.90  
Port 2222  
User root
```

In diesem Beispiel ist für `HostName` die IP-Adresse angegeben, die der Server erhält. Stattdessen kann man auch einen Domainnamen wie „`homeserver.local`“ oder „`mycloud.example.com`“ angeben. Wenn Sie nun `ssh labortuer` aufrufen, baut der SSH-Client eine Verbindung zu „`root@192.168.122.90`“ über Port 2222 auf.

Wenn Sie wollen, können Sie die `~/.ssh/config` um einen weiteren Eintrag für die SSH-Verbindung zum eigentlichen System ergänzen.

```
Host laborserver  
HostName 192.168.122.90  
User cctest
```

Mit diesen beiden Einträgen können Sie sich mit `ssh labortuer` zum Entsperren des Passworts verbinden und mit `ssh laborserver` im vollständig gestarteten System anmelden.

The screenshot shows a terminal window titled "cttest@laborserver:~". It displays the following sequence of commands and output:

```
keywan@river:~$ ssh labortuer
Please unlock disk dm_crypt-0:
cryptsetup: dm_crypt-0 set up successfully
Connection to 192.168.122.90 closed.
keywan@river:~$ keywan@river:~$ ssh laborserver
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)
Last login: Wed Jun 30 07:10:27 2021 from 192.168.122.1
cttest@laborserver:~$
```

**Mit der ersten SSH-Verbindung entsperrt man die verschlüsselte System-Partition. Mit der zweiten meldet man sich am System an.**

## Literatur

- [1] Dr. Jan Kopia, Sicherer Kanal, Symmetrische und asymmetrische Verschlüsselung, c't 7/2021, S. 56
- [2] Heike Jurzik, Sicher unterwegs, Verbindungen mit SSH verschlüsseln, c't 14/2018, S. 144
- [3] Peter Siering, FAQ SSH – Secure Shell, c't 3/2018, S. 158

# Herbstcampus

Wissen, Inspiration und Praxisrelevanz

**15. September 2021 – Online**

**Die gewohnt kommunikative Konferenz  
für Unternehmensentwickler mit:**

- ✓ mehr als 20 Vorträgen
- ✓ Themenclustern aus drei Vorträgen und interaktiven Diskussionen
- ✓ Themen: Softwarearchitektur, Containerisierung, Java, APIs, Infrastructure as Code, Teamwork & Weiterentwicklung
- ✓ Diskussionsrunden per Chat und Video
- ✓ virtuellem Get-together am Abend

Bis  
13. August  
für nur 49 €  
buchen!

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

Veranstalter



heise Developer



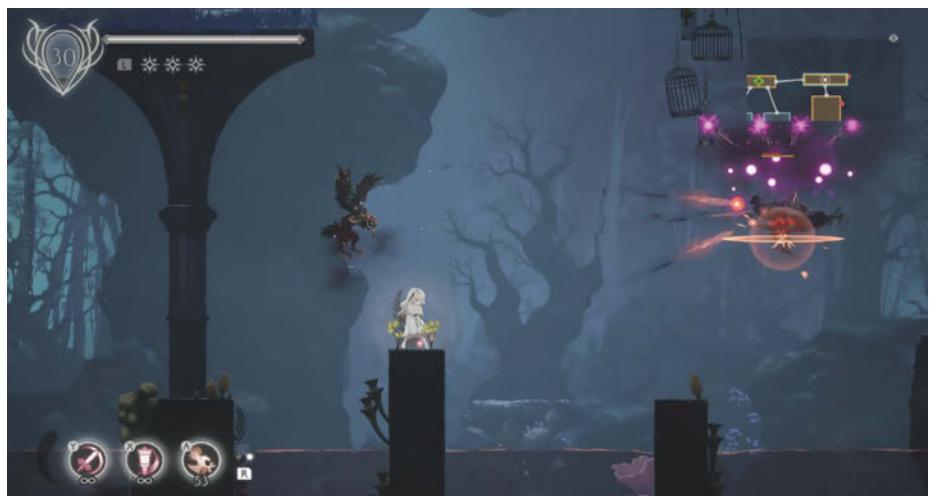
dpunkt.verlag

© Copyright by Heise Medien.

Silber-Sponsor



**infoteam**  
software



# Todesmutig

## Ender Lilies – Quietus of the Knights: Die Geister, die ich rief

**In Ender Lilies stürzt sich ein Mädchen mit ihren untoten Begleitern in ein labyrinthartiges Abenteuer, um ihre Welt vor dem Untergang zu bewahren.**

Von Andreas Müller

Die düstere Story führt ins Endland: Ein sogenannter Todesregen hat hier fast alle Lebewesen in tödliche Monster verwandelt. Die einzige Rettung für diese Welt scheint das Mädchen Lily zu sein, das allein in einem verfallenen Gemäuer aufwacht. Woher sie kommt, erfährt man nicht. Nur, dass eine schier unlösbare Aufgabe sie immer tiefer in eine traurige Geschichte voller Tod und Verderben hineinzieht. Aber Lily hat Glück im Unglück: Schon bald gesellen sich die Geister verstorbener Helden an ihre Seite und helfen ihr, sich gegen die zahlreichen Feinde zu wehren.

### Tiefste Tiefen

Bei Lilies Abenteuer stand der Nintendo-Klassiker Metroid Pate, dessen geistige

Nachfolger Fans als Metroidvanias bezeichnen. Ähnlich wie in Spielen wie „Ori and the Will of the Wisps“ oder „Hollow Knight“ müssen Lily und ihre untoten Helfer neue Fähigkeiten erlernen, um ein komplexes Labyrinth zu erkunden. Dabei kehren sie bei diesem Spielprinzip immer wieder in bekannte Gebiete zurück, um neue Wege freizuschalten. Einfach ist das nicht: Geht einmal die Konzentration verloren, können selbst kleine Gegner den Bildschirmtod bringen. Butterweiche Animationen und eine präzise Gamepad-Steuerung sorgen auf dem PC und den Konsolen fürfordernde, aber nie unfaire Kämpfe. Rätsel muss Lily dagegen nicht lösen.

Stattdessen kämpft und springt Lily in der seitlichen 2D-Ansicht durch Gemäuer, tiefe Gewässer und sumpfige Wälder. Trifft sie auf Feinde, aktiviert sie die Waffen ihrer Geister, um sich mit Schwert, Axt oder magischen Geschossen zu wehren. Anfangs ist Lilies Arsenal noch begrenzt, aber wenn es ihr gelingt, besonders hartnäckige Gegner zu besiegen, dann schließen sich deren Geister dem mutigen Mädchen an. An Rastpunkten muss sie sich entscheiden, welche Geister sie begleiten

sollen, denn die Ausrüstungsplätze sind begrenzt und nicht jedes Monster hat die gleichen Schwachpunkte.

### Cleveres Leveldesign

Mit jedem Sieg sammelt Lily Erfahrungspunkte. Steigt sie dann einen Level auf, wird sie stärker und widerstandsfähiger. An versteckten Stellen findet sie Relikte, die ihr besseren Schutz oder einen weiteren Ausrüstungsplatz spendieren. Wenn Lily dazu noch genügend sogenannte Seelen sammelt, kann sie damit ihre Waffen dauerhaft verstärken. Ein komfortables Schnellreisesystem lässt sie schnell von einem Ort zum anderen wechseln. Allerdings werden dann die bereits besiegteten Monster wiederbelebt.

Viele bunte Effekte hat Ender Lilies nicht zu bieten; der Anime-Look wirkt nur auf den ersten Blick verspielt. Schnell dominieren dunkle, kontrastarme Farben, bei denen kein Platz für Popcorn-Effekte ist. Was zählt, ist das clevere Leveldesign, das viele Geheimnisse und Abkürzungen bereithält. Ein bisschen Spektakel gibt es nur bei den zahlreichen Boss-Kämpfen, die Lily und ihre untoten Helfer mit mehreren Angriffswellen malträtierten. Bis der Abspann läuft, vergehen rund 15 Spielstunden.

### Fazit

Ender Lilies: Quietus of the Knights ist ein düsteres Action-Abenteuer, bei dem Konzentration und Neugier gefragt sind. Vom scheinbar hilflosen Anime-Look der Hauptfigur sollte man sich nicht täuschen lassen, denn dahinter verbirgt sich eine dunkle Vergangenheit. Statt auf bunte Effekte und das große Spektakel konzentrieren sich die japanischen Entwickler deshalb auf das Wesentliche: cleveres Leveldesign und präzise Steuerung. Deshalb dürften sich vor allem Metroidvania-Fans angesprochen fühlen. Sie bekommen einen würdigen Nachfolger, in dem sie sich stundenlang verlieren dürfen, bis sie am Ende triumphierend das Sonnenlicht erblicken.

(lmd@ct.de) ct

### Ender Lilies

Action-Abenteuer	
Vertrieb	Binary Haze Interactive, LiveWire, Adglobe, <a href="http://enderlilies.com">enderlilies.com</a>
Systeme	Windows, Xbox One, Nintendo Switch
USK	ab 12 Jahren
Preis	25 €



# SO SPANNEND KANN WISSEN SEIN!

Das Magazin,  
das Wissen schafft.



**TESTEN SIE WISSEN  
MIT 30 % RABATT!**

2 Ausgaben für nur 11,20 €\*  
statt 15,80 €\* im Handel

**Jetzt bestellen:**

[www.emedia.de/wissen-mini](http://www.emedia.de/wissen-mini)

\*Preis in Deutschland.



**Mit Geschenk**

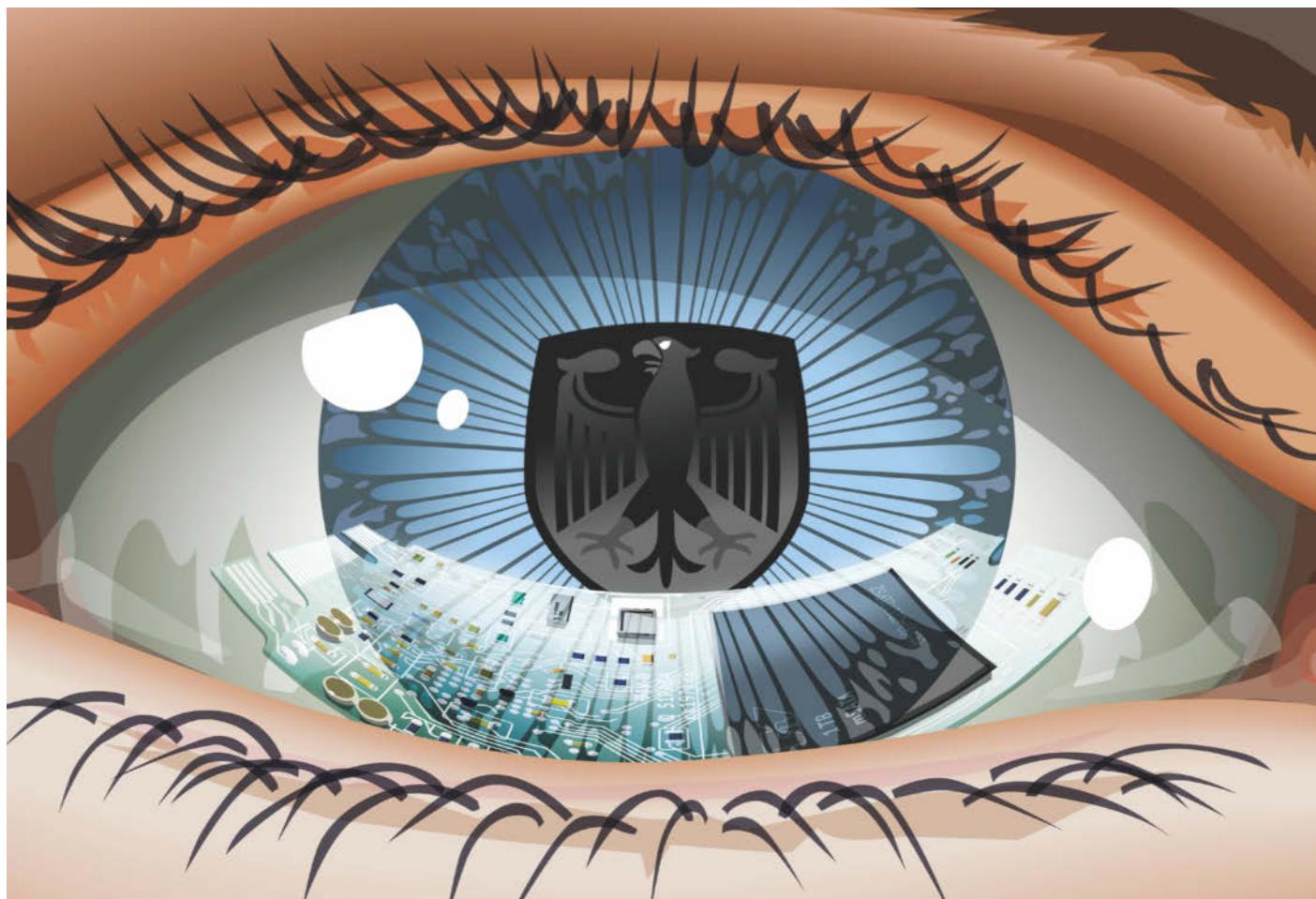


Bild: Rudolf A. Blaha

# Sicherheitsgewinn oder Überwachungs Albtraum?

## Verfassungsschützer erhalten neue Befugnisse

**Der deutsche Gesetzgeber hat es heimischen Geheimdiensten leichter gemacht, auf Daten und Kommunikationsinhalte von verdächtigen Personen zu zugreifen. Bedenken gegen die ausgeweitete Überwachung rechnergestützter Kommunikation im Rahmen der sogenannten Quellen-TKÜ kommen von kompetenter Seite.**

Von Harald Büring

Vor Kurzem noch haben Spaltenpolitiker das gesamte Internet als eine Art ratselhaftes Neuland empfunden. Mittlerweile bemüht sich die Legislative mit ungewohntem Tempo, Gesetze aus dem prä-digitalen Zeitalter wirksam an gegenwärtige Verhältnisse anzupassen. Das betrifft in jüngster Zeit ganz besonders das rechtliche Instrumentarium von Behörden bei Strafvermittlung und Gefahrenabwehr.

Ein Ergebnis jüngster Gesetzesänderungen besteht darin, dass ausgerechnet ein hochumstrittenes Instrument wie die sogenannte Quellen-Telekommunikationsüberwachung jetzt für mehr behörd-

liche Akteure als je zuvor bereitsteht [1]. Es geht dabei um den gezielten Einsatz manipulativer Software auf PCs und Smartphones verdächtiger Personen mit dem Ziel, vermeintlich geschützte Kommunikation unbemerkt abzufangen respektive auszulesen und für die Ermittler transparent zu machen. Die sogenannten Staatstrojaner greifen die Inhalte laufender Telekommunikation auf den Geräten beim Versand noch vor dem Verschlüsseln beziehungsweise beim Empfang direkt nach dem Entschlüsseln ab. Die „Quellen-TKÜ Plus“ umfasst zudem den Zugriff auf entschlüsselte Kommunikation, die ab

dem Zeitpunkt des Maßnahmenstarts auf den infiltrierten Geräten gespeichert werden ist. Die Maßnahmen sollen aber nicht etwa beliebige gespeicherte Informationen auswerten – was einer Online-Durchsuchung gleichkäme. Dass diese strenge Trennung sich in der Praxis technisch konsequent umsetzen lässt, bezweifeln Kritiker der erweiterten Quellen-TKÜ.

Die umstrittene Befugnis war ursprünglich dem Bundeskriminalamt (BKA) für die Terrorismusabwehr vorbehalten. Seit 2017 gibt die Strafprozessordnung in § 100a auch Strafverfolgungsbehörden bei Ermittlungen zu bestimmten schweren Straftaten das Instrument der „Quellen-TKÜ Plus“ in die Hand. Der Katalog dieser Straftaten, der sich in Absatz 2 des Paragrafen findet, umfasst unter anderem bandenmäßige Steuerhinterziehung, Hochverrat, Mandatsträgerbestechung, Geldfälschung und Mord.

Mittlerweile findet sich die Befugnis zur „Quellen-TKÜ Plus“ in mehreren Polizeigesetzen der Bundesländer, etwa in NRW [2]. Jetzt ist der Kreis der berechtigten behördlichen Akteure zudem auf die Bundes- und Landesbehörden für Verfassungsschutz sowie den in deren Informationsverbund einbezogenen Militärischen Abschirmsdienst (MAD) ausgeweitet worden; die möglichen Anlässe umfassen dort verschiedene Bedarfssätze der Gefahrenabwehr und sind auf keinen konkreten Straftatenkatalog beschränkt.

Bei all dem geht es wohlgerne nicht um anlasslose Massenüberwachung. Die Polizeibehörden brauchen für jede TKÜ-Maßnahme einen richterlichen Beschluss, der wiederum einen konkreten Verdacht voraussetzt.

## Anpassung an die Gegenwart

In diesem Zusammenhang hat der Bundestag am 10. Juni 2021 zwei Gesetze verabschiedet, die viel Kritik auf sich gezogen haben. Zunächst nahm er den zuvor noch vom Innenausschuss modifizierten Gesetzentwurf der Koalitionsfraktionen „zur Modernisierung der Rechtsgrundlagen der Bundespolizei“ an [3], der Änderungen am Bundespolizeigesetz (BPoG) vornehmen sollte. Jenes Gesetz stammt in weiten Teilen aus dem Jahr 1994 und regelt die Arbeit der Bundespolizei, also des ehemaligen Bundesgrenzschutzes.

Der Gesetzentwurf sah in § 27d Abs. 1 vor, dass die Beamten dieser Behörde eine Befugnis zur präventiven Telekommunikationsüberwachung erhalten soll-

ten. Anders als für die Regelung in §100a Abs. 1 Satz 1 StPO sollte diese nicht an Ermittlungen zu einer bereits verübten Straftat gebunden sein. Nicht einmal eine dringende Gefahr für die in § 27d Abs. 1 Nr. 1 genannten Rechtsgüter hätte zwingend vorliegen müssen, um den Einsatz der Überwachung zu rechtfertigen. Dies betrifft die Sicherheit des Bundes beziehungsweise eines Bundeslandes respektive von Leib, Leben oder Freiheit einer Person. Vielmehr sollte die Überwachung bereits zulässig sein, wenn „bestimmte Tatsachen die Annahme rechtfertigen, dass die abgehörte Person innerhalb eines übersehbaren Zeitraums eine zumindest ihrer Art nach konkretisierte Straftat begangen wird, die eine nicht unerhebliche Schädigung der ... Rechtsgüter erwarten lässt.“

Zudem räumte § 27d Abs.2 des Entwurfs der Bundespolizei die Befugnis ein, eine „Quellen-TKÜ Plus“ durchzuführen, um Schleusungen effektiv zu bekämpfen und gefährliche Eingriffe in den See-, Luft- oder Bahnverkehr zu verhindern.

Die Bundespolizei hätte die vorgenommenen Veränderungen an den überwachten IT-Systemen nach Abschluss der Maßnahme rückgängig machen sollen, sofern dies „technisch möglich“ gewesen wäre – was großen Spielraum für Interpretationen lässt.

## Bundesrat erteilt Dämpfer

Allerdings hätte der vom Bundestag angenommene Gesetzentwurf, um in Kraft

treten zu können, die Zustimmung des Bundesrats gebraucht. In der Länderkammer fand sich am 25.6.2021 jedoch keine Mehrheit dafür. Der Bundesregierung wie dem Bundestag steht es dann offen, den Vermittlungsausschuss anzurufen.

Ein Sprecher des Bundesinnenministeriums (BMI) teilte dazu am 2.7. mit, dass die Regierung darauf verzichtet. Eine Sprecherin des Bundestags erklärte am 20.7., dass auch das Parlament noch nicht den Vermittlungsausschuss angerufen habe. Es sei jedoch offen, ob der Bundestag dies noch tun werde.

Die geplante Befugniserweiterung für die Bundespolizei ist also vorerst am Bundesrat gescheitert, allerdings nicht aus der Welt. Bis zum Ende der laufenden Legislaturperiode kann das Gesetzesvorhaben theoretisch noch im Vermittlungsausschuss landen. Zudem ist denkbar, dass eine neue Bundesregierung das Anliegen später wieder aufgreift.

## Geheimdienste dürfen entschlüsseln

Das zweite Gesetz hatte mehr Erfolg: Der Gesetzentwurf der Bundesregierung „zur Anpassung des Verfassungsschutzrechts“ wurde in einer vom Innenausschuss geringfügig modifizierten Fassung am 10.6.2021 verabschiedet [4]. Der Bundesrat hätte die Möglichkeit gehabt, nach Art. 77 Abs. 2 GG Einspruch einzulegen. Die Länderkammer beschloss jedoch, dies nicht zu tun [5]. Nach seiner Unterzeich-

The screenshot shows the official website of the Federal Ministry of the Interior (BMI). At the top, there's a navigation bar with links for 'Ministerium', 'Themen', 'Presse', 'Service', and 'EU-Ratspräsidentschaft 2020'. A search icon is also present. Below the navigation, a banner reads 'HÄUFIG NACHGEFRAGT' (Frequently Asked Questions) and 'Fragen und Antworten zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts'. It includes a link: 'Weitere Informationen zum Gesetzgebungsverfahren finden Sie [hier](#)'. The main content area contains several questions and their answers, such as: 'Was ist der zentrale Inhalt des Gesetzentwurfs?', 'Was ist eine "Quellen-TKÜ"?' (What is a "Quellen-TKÜ"?), 'Wozu brauchen die Nachrichtendienste diese Befugnisse?', 'Sind "Berufsgeheimnisträger" – also z.B. – Journalisten geschützt?', 'Warum wird die Beobachtungsaufgabe bei Einzelpersonen erweitert?', and 'Wozu ist der Einbezug des MAD in den Informationsverbund des Verfassungsschutzes nötig?'. At the bottom, there are links for 'Seite teilen', 'Seite drucken', 'Suche', 'BESUCHEN SIE UNS AUF', and social media icons for Twitter and YouTube.



Bild: Mario Sixtus, CC-BY-SA de 3.0

**padeluun von Digitalcourage e.V.:**  
„Das ist eine totalitäre Maßnahme.“

nung durch den Bundespräsidenten und Veröffentlichung im Bundesgesetzblatt (BGBl) ist es am 9.7.2021 in Kraft getreten.

Für die Bundesrepublik Deutschland arbeiten drei Geheimdienste: Der Bundesnachrichtendienst (BND) gewinnt auslandsbezogene Informationen. Der Militärische Abschirmdienst (MAD) arbeitet fürs Verteidigungsministerium (BMVg) und widmet sich Aufgaben der Informationssammlung, Spionage- und Sabotageabwehr im Bereich der Bundeswehr. Das Bundesamt für Verfassungsschutz (BfV) wiederum untersteht dem BMI; es beobachtet und analysiert Bestrebungen gegen die freiheitliche demokratische Grundordnung. Ihm zur Seite stehen die 16 Verfassungsschutzbehörden der Bundesländer (LfV).

Bereits vor der genannten Gesetzesänderung durften diese Akteure eine präventive Telekommunikationsüberwachung durchführen. Das erlaubte und erlaubt ihnen das sogenannte Artikel-10-Gesetz (G 10), das behördliche Eingriffe in die Grundrechte aus Artikel 10 des Grundgesetzes (GG) regelt – also Eingriffe ins Brief-, Post- und Fernmeldegeheimnis [6]. Voraussetzung: Es müssen „tatsächliche Anhaltspunkte“ für den Verdacht bestehen, dass jemand eine in dem Katalog von § 3 Abs. 1 G 10 aufgeführte Straftat „plant, begeht oder begangen hat“. Kontrollinstanz ist die G-10-Kommission, die in jedem Einzelfall über anstehende Überwachungsmaßnahmen entscheidet. Dieser Mechanismus entspricht bei den Ge-

heimdiensten praktisch dem, was der Richtervorbehalt für polizeiliche Maßnahmen bedeutet.

Das Gesetz zur Änderung des Verfassungsschutzrechts nimmt eine Reihe von Änderungen am G 10 vor. So verankert es im neu eingefügten Abs. 1a von § 11 G 10 die Möglichkeit der Quellen-TKÜ durch Eingriff „in ein von dem Betroffenen genutztes informationstechnisches System“. Im Rahmen der „Quellen-TKÜ Plus“ dürfen die Verfassungsschützer von Bund und Ländern auch auf Spuren vergangener Kommunikation eines betroffenen Nutzers zugreifen, die auf seinem infiltrierten Gerät gespeichert sind. Laut dem Gesetzeswortlaut darf dies aber nur Material betreffen, das nach der Anordnung der Quellen-TKÜ gespeichert worden ist und das theoretisch auch in Echtzeit verschlüsselt hätte abgefangen werden können. Bereits die wissenschaftlichen Dienste des Bundestags haben sich im Vorfeld zu den Schwierigkeiten, die damit zusammenhängen, kritisch geäußert [7].

Einen weiteren Aufreger liefert das Gesetz dadurch, dass es die Nachrichtendienste berechtigt, die Mitwirkung der Provider bei der Quellen-TKÜ einzufordern. § 2 Abs. 1a G 10 verpflichtet diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu weitgehender Unterstützung: Auf Anordnung müssen sie nicht nur Zutritt zu ihren Einrichtungen gewähren und den Anschluss von Geräten der Behörden dulden, sondern auch Inhalte „ausleiten“, die ihnen zur Übermittlung anvertraut sind.

Was genau unter „Ausleiten“ zu verstehen ist, definiert die Vorschrift nicht. In

der Gesetzesbegründung heißt es lediglich, dass es dabei um die Übermittlung von Inhalten der Telekommunikation gehen soll [8].

### Landesbehörden mit im Boot

Das G 10 bezieht die LfV mit ein – es bedürfte also keiner eigenen Umsetzung der dort verankerten Befugnisse in Gesetzen der Bundesländer mehr. Unabhängig davon haben einige bereits in ihren Landesgesetzen ihren LfV erlaubt, eine Quellen-TKÜ durchzuführen. Das betrifft etwa Baden-Württemberg [9], Bayern [10] und Hamburg [11].

Der Trend zur Erleichterung von Datenzugriffen für Verfassungsschutzbehörden betrifft nicht nur die Quellen-TKÜ, sondern auch andere in Datenschutzhinsicht sensible Informationen. So hat der niedersächsische Landtag am 7.7.2021 beschlossen, dass das zuständige LfV unter festgelegten Voraussetzungen bei Geldinstituten und Finanzdienstleistern Kontostammdaten Verdächtiger abfragen darf. Der niedersächsische Verfassungsschutzpräsident Bernhard Witthaut hat dafür im Vorfeld mit dem Argument geworben: „So würde es künftig auch in Niedersachsen einfacher, die finanzielle Ausstattung extremistischer Organisationen zu ermitteln und einzuschätzen“ [12].

Das geänderte niedersächsische Verfassungsschutzgesetz (NVerfSchG) ist nach Ausfertigung durch den Landtagspräsidenten und Verkündung im niedersächsischen Gesetzblatt am 14.7.2021 in Kraft getreten [13]. Auf Instagram (@verfassungsschutz.nds) und Twitter (@LfV\_NI) feierte das LfV diese Gesetzesänderung mit einem Meme [14].

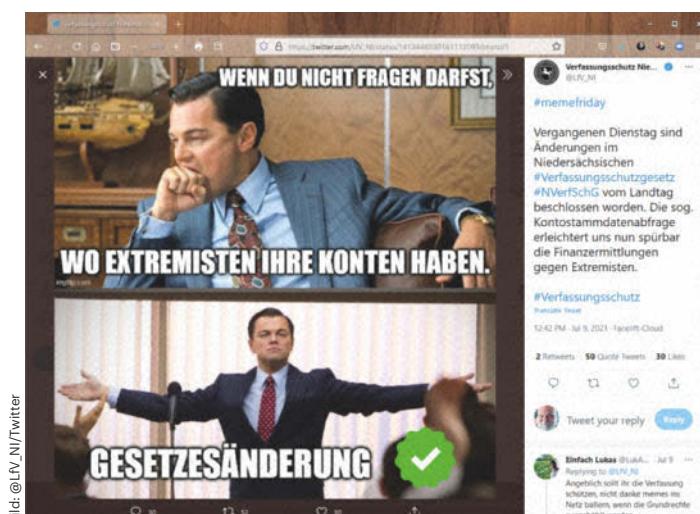


Bild: @LfV\_NI/Twitter

**Das niedersächsische Landesamt für Verfassungsschutz kleidet seine Freude über die neuerdings bestehende Befugnis zur Abfrage von Kontostammdaten in ein Meme, hier auf Twitter.**

Die Voraussetzungen, unter denen die Behörde die neue Befugnis nutzen kann, ähneln denen für den TKÜ-Bereich [15]: Insbesondere setzt eine Kontostammdatenabfrage voraus, dass „tatsächliche Anhaltspunkte“ dafür vorliegen, dass eines der in § 3 Abs. 1 NVerfSchG genannten Rechtsgüter bedroht ist. Dazu gehören die freiheitliche demokratische Grundordnung, der Bestand beziehungsweise die Sicherheit des Bundes oder eines Landes. Darüber hinaus muss die Maßnahme „erforderlich“ sein. Die Begriffe in der Begründung zum Entwurf des zugrunde liegenden niedersächsischen „Gesetzes zur Änderung nachrichtendienstlicher Bestimmungen“ sind ziemlich weit auslegbar. Sie wecken Zweifel daran, dass der Gesetzgeber die Beschränkung einer Kontostammdatenabfrage auf Extremisten damit wirksam sichergestellt hat.

Eine vergleichbare Befugnis besitzt auf Bundesebene bereits das Bundesamt für Verfassungsschutz (BfV, § 8a Abs. 1 Satz 1 Nr. 2 des Bundesverfassungsschutzgesetzes – BVerfSchG). Gleches gilt für die Verfassungsschutzbehörden in Nordrhein-Westfalen (§ 7c Abs. 1 VSG NRW) sowie Baden-Württemberg (§ 5b Abs. 1 LVSG). Es handelt sich also nicht etwa um eine niedersächsische Spezialität.

### Massive Expertenkritik

Bereits im Entwurfsstadium zeichnete sich ab, dass das Gesetz zur Anpassung des Verfassungsschutzrechts auf schwerwiegende Bedenken in der Wirtschaft, bei Medien und bei zivilgesellschaftlichen Akteuren treffen würde. Zu denjenigen Stellen, die das BMI aufforderte, bereits bis 30.6.2020 Stellung zu nehmen, gehörten der Branchenverband Bitkom und ein breites „Bündnis der Medien“, dessen Spektrum von ARD und ZDF über den Presserat und den Verlegerverband VDZ bis zu zwei Journalistengewerkschaften reicht [16].

Das Bitkom-Statement spendet zunächst etwas Lob für das Gesetzesanliegen, wird dann aber sehr deutlich, was die „dringend korrekturbedürftigen“ neuen Bestimmungen zur Quellen-TKÜ betrifft: „Netzbetreiber [werden] ... in einen unerwünschten Rollenwechsel gedrängt.“ Der Einsatz von Staatstrojanern mit Unterstützung der Provider könne „nicht losgelöst von der Tatsache betrachtet werden, dass (unbekannte) Schadsoftware über die Netze der Dienstanbieter in das entsprechende System eingeschleust werden

muss, um eine solche intendierte Wirkung zu erreichen. Als Konsequenz verkennt der Gesetzesentwurf die hohen Risiken und negativen Auswirkungen auf die gesamte Netzintegrität.“

Das „Bündnis der Medien“ weist auf Gefahren für die Pressefreiheit hin und nennt bereits eine entscheidende Schwachstelle der „Quellen-TKÜ Plus“: „Wenn Spionage-Software auf einem informationstechnischen System unbemerkt installiert wird, besteht theoretisch immer der volle Zugriff auf alle dort gespeicherten Daten. Dadurch entstehen Abgrenzungsschwierigkeiten zur sog. ‚Online-Durchsuchung‘.“

Das BMI als federführendes Ministerium für das Gesetz zur Anpassung des Verfassungsschutzrechts bleibt auf die Bitte hin, zu den massiven technischen und rechtlichen Bedenken Stellung zu beziehen, sehr allgemein. In einer E-Mail an c't vom 21.6.2021 sagte BMI-Sprecher Marek Wede insbesondere zu den nun nicht wirksam gewordenen Befugniserweiterungen für die Bundespolizei: „Mit Blick auf technische Entwicklungen und geänderte Nutzungsgewohnheiten ist eine Modernisierung der rechtlichen Grundlagen des Bundespolizeigesetzes und des Verfassungsschutzrechtes notwendig. Verbesserte Befugnisse etwa zur Überwachung von Telekommunikation oder zum Einsatz gegen Drohnen stellen eine erhebliche Verbesserung der Sicherheit in Deutschland dar. Die Bundespolizei ist die größte deutsche Sicherheitsbehörde, die einen wesentlichen Beitrag zur Gewährleistung der inneren Sicherheit in der Bundesrepublik Deutschland leistet. Sie nimmt umfangreiche polizeiliche Aufgaben insbesondere in den Bereichen Grenzschutz, Bahnpolizei und Luftsicherheit wahr. Der Bundespolizei obliegen darüber hinaus der Schutz für Objekte des Bundes, Aufgaben auf See, internationale Aufgaben, polizeiliche Unterstützung der Länder sowie die Kriminalitätsbekämpfung.“

Auch zur Ausweitung der Quellen-TKÜ-Befugnisse für die Verfassungsschutzbehörden äußert sich Wede. Er verweist vorrangig darauf, dass es um die Anpassung des Verfassungsschutzrechts an die digitale Welt gehe. Zudem müsse sich die Überwachung weiterhin in einem „engen gesetzlichen Rahmen“ bewegen. Das Ministerium weist auch darauf hin, dass das veränderte G 10 eine erweiterte Kontrolle von TKÜ-Maßnahmen durch die G-10-Kommission erfordert.



Bild: Karlsruher Institut für Technologie (KIT)

**Matthias Bäcker, Experte für Datenschutzrecht, weist darauf hin, dass der Einsatz von Quellen-TKÜ für Nutzer infiltrierter Systeme ein hohes Sicherheitsrisiko bedeutet – die entstehenden Sicherheitslücken können Hackerangriffe begünstigen.**

Wede zitiert ferner Bundesinnenminister Seehofer, der zu dem kontroversen Thema sehr grundsätzliche Töne anschlägt: „Ein starker Rechtsstaat braucht starke Sicherheitsbehörden. Mit dem neuen Bundesverfassungsschutzgesetz bekommt das Bundesamt für Verfassungsschutz ein längst überfälliges Update für den Kampf gegen die Feinde unserer Verfassung“ [17].

### Datenschutz- und Sicherheitsprobleme

Erhebliche Bedenken kommen von prominenten BürgerrechtlerInnen. So schreibt der Datenschutzaktivist padeluun von Digitalcourage e.V.: „Wir halten die Verletzung der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für unzulässig. Das ist eine totalitäre Maßnahme, die in einer rechtsstaatlichen Demokratie keinen Platz hat. Wir haben da sogar noch eine Verfassungsbeschwerde auf Vorrat: <https://aktion.digitalcourage.de/kein-staatstrojaner>. Natürlich ist dann auch eine Mitwirkungspflicht von Providern hinfällig. Diese Mitwirkungspflicht ist besonders perfide, weil sie Provider zu Hilfsbeamten der Staatsanwaltschaften macht. Das ist aber nicht deren Aufgabe – im Gegenteil. Meiner Providerin muss ich vertrauen können.“

Das Denken hinter solchen Forderungen und Gesetzen ist totalitär.“

## Einfallstor für Hacker

Datenschutzexperte Matthias Bäcker, Professor am Fachbereich Rechts- und Wirtschaftswissenschaften der Johannes-Gutenberg-Universität Mainz, hebt in einem Statement zur Quellen-TKÜ vor allem die Folgen für Nutzer hervor. Das damit verbundene heimliche Implementieren eines Staatstrojaners auf dem Endgerät eines Nutzers, so Bäcker, ist für diesen mit einem hohen Sicherheitsrisiko verbunden: Eine entstehende Sicherheitslücke könne kriminellen Hackern als Eintrittspforte dienen. Darauf hatte er auch bereits in einer Stellungnahme [18] zum Gesetzentwurf zur Anpassung des Verfassungsschutzrechts hingewiesen, die er bei einer Anhörung des Bundestagsausschusses präsentierte [19]. Dort forderte er, die Ermächtigung der Nachrichtendienste zur Durchführung der Quellen-TKÜ müsse mit Schutzvorkehrungen versehen werden, um zu verhindern, dass Hacker durch unbekannte Sicherheitslücken beim Einsatz von Staatstrojanern in infiltrierte Systeme eindringen könnten.

Was die Mitwirkungsverpflichtungen der Provider gegenüber den Geheimdiensten betrifft, so betont Bäcker, dass diese Grenzen habe. Das geänderte G 10 zwingt Diensteanbieter nicht dazu, selbst einen Trojaner in ein Zielsystem einzubringen. Sie seien nur zur Duldung und Unterstützung verpflichtet, also etwa zum Anschlie-

ßen einer bereitgestellten Black Box. Auf dem Klageweg dagegen angehen können sie nicht – es fehlt ihnen an einer Klagebefugnis.

## Wie klagt man gegen heimliche Aktionen?

Wer von Quellen-TKÜ betroffen ist, hat aus anderen Gründen nur wenig Chancen, sich dagegen zu wehren. Gegen Maßnahmen von Verfassungsschutzbehörden ist zwar eine Klage vor dem zuständigen Verwaltungsgericht möglich. Wenn es etwa um Aktivitäten des BKA geht, wäre in erster Instanz das Bundesverwaltungsgericht (BVerwG) in Leipzig zuständig. Das Problem besteht allerdings darin, dass die Behörden die betroffenen Nutzer erst nachträglich über die bereits abgeschlossenen Überwachungsmaßnahmen informieren – das liegt in der Natur der Sache.

Beobachter, die mit der behördlichen Praxis vertraut sind, weisen immer wieder darauf hin, dass auch mit den neuen Befugnissen von einem massenhaften Trojanereinsatz durch Verfassungsschutzbehörden keine Rede sein könne. Sogenannte G-10-Fälle, also aufs G 10 gestützte Überwachungsvorgänge, seien mit enormem technischem und personellem Aufwand verbunden und kämen insgesamt nur selten vor. Zudem muss jeder Einzelfall im Hinblick darauf geprüft werden, ob die Maßnahme auf einem hinreichenden Verdacht aufbauen kann und ob sie verhältnismäßig ist. Diese Einzelfallprüfung obliegt bei Quellen-TKÜ-Maßnahmen

durch Verfassungsschutzbehörden der G-10-Kommission, deren Mitglieder vom parlamentarischen Kontrollgremium des Bundestags (PKGr) berufen werden. Ihr Vorsitzender muss Volljurist sein. Nach der bisherigen Erfahrung verfährt die G-10-Kommission mit Freigaben nicht unbedingt großzügig.

Auf jeden Fall ist auch nach der nunmehr geltenden Rechtslage keine anlasslose Serienüberwachung mit Staatstrojanern zulässig. Das Gesetz liefert keine Handabe, um etwa Spionagesoftware auf breiter Basis zu streuen und dabei auch Unbeteiligte zu erfassen. (psz@ct.de) **ct**

## Literatur

- [1] Stefan Krempel, Gesattelte Staatstrojaner, Neue Schnüffelwerkzeuge für Geheimdienste, c't 16/2021, S. 12
- [2] Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW), § 20c Abs. 2: heise.de/s/4XWd
- [3] Gesetzentwurf des Bundestags zur Modernisierung der Rechtsgrundlagen der Bundespolizei, BT-Drucksache 19/26541: heise.de/s/dDn4
- [4] Bundestag ändert das Recht des Verfassungsschutzes, BT-Drucksachen 19/24785, 19/24900 und 19/30477: heise.de/s/oOd4
- [5] Bundesrat, 1006. Sitzung vom 25.6.2021, Bundesrats-Drucksache 512/21: heise.de/s/3jWA
- [6] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses: heise.de/s/BDKN
- [7] Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste, Ausarbeitung der wissenschaftlichen Dienste des Deutschen Bundestags vom 19.2.2021, Az. WD 3-3000 -293/20, Seite 7: heise.de/s/gPrl
- [8] Begründung im Gesetzentwurf der Bundesregierung, BT-Drucksache 19/24785, Seite 21: heise.de/s/VX56
- [9] Baden-württembergisches LVSG, § 5d: heise.de/s/57Wv
- [10] Art. 13 BayVSG: heise.de/s/EPnn
- [11] § 8 Abs. 12 HmbVerfSchG: heise.de/s/qn3d
- [12] Presseinformation der Niedersächsischen Staatskanzlei vom 1.9.2020: heise.de/s/vZEEx
- [13] NVerfSchG, Nds. GVBI. Nr. 27/2021 vom 13.7.2021: heise.de/s/D808
- [14] Meme auf der Instagram-Präsenz des niedersächsischen Landesamts für Verfassungsschutz (@verfassungsschutz.nds) vom 9.7.2021: heise.de/s/Qxod
- [15] Begründung der niedersächsischen Landesregierung zum „Entwurf des Gesetzes zur Änderung nachrichtendienstlicher Bestimmungen“, Landtags-Drucksache 8/7315, Seite 10: heise.de/s/8dWJ
- [16] Alle sechs Stellungnahmen der vom Ministerium angefragten Stellen sind über die Informationsseite des BMI zum Gesetzgebungsverfahren abrufbar: heise.de/s/P2dk
- [17] BMI, Meldung vom 25.6.2021: heise.de/s/LWXI
- [18] Matthias Bäcker, Stellungnahme bei der öffentlichen Anhörung zum Gesetzentwurf zur Anpassung des Verfassungsschutzrechts, Ausschussdrucksache 19 (4) 844 A: heise.de/s/bq6A
- [19] Öffentliche Anhörung vor dem Bundestagsausschuss, 17.5.2021: heise.de/s/p0ow
- [20] Verfassungsbeschwerden gegen polizeiliche Quellen-TKÜ-Befugnisse, Az. 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18: heise.de/s/Y4ve
- [21] Verfassungsbeschwerde von 64 FDP-Bundestagsabgeordneten, 14.7.2021: https://heise.de/s/6GW1

## Futter für Verfassungsrichter

Gegen den Einsatz der Quellen-TKÜ liegen bereits mehrere Verfassungsbeschwerden vor. So wird der zweite Senat des Bundesverfassungsgerichts (BVerfG) sich mit der Frage befassen müssen, ob bereits die polizeilichen Möglichkeiten des Trojanereinsatzes, die durch das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ vom 17. August 2017 in die StPO hineingekommen sind, verfassungsgemäß sind. Unter anderem haben Rechtsanwälte, Künstler und Journalisten dazu Verfassungsbeschwerde erhoben. Zu den Beschwerdeführern gehören auch einige Bundestagsabgeordnete [20].

Die jüngste und wohl spektakulärste Verfassungsbeschwerde zum Thema Quellen-TKÜ erhoben 64 der 80 FDP-Bundestagsabgeordneten am 14.7.2021. Ihr Vorstoß richtet sich gegen insgesamt zehn Normen des durchs „Gesetz zur Anpassung des Verfassungsschutzrechts“ vom 5. Juli 2021 neugeregelten G 10. Der 108-seitige Schriftsatz, den Rechtsanwalt Nikolaus Gazeas ausgearbeitet hat, geht ausführlich auf die Problematik der Sicherheitslücken ein und legt den Finger genau auf wichtige wunde Stellen der neuen Bestimmungen [21]. Eine lohnende Lektüre – auch für Leute, die das Anliegen der Beschwerdeführer nicht teilen.

# Digitalisierung leicht gemacht!

Wenn Ihre Bücherregale gerade überquellen, bieten wir Ihnen die ideale Lösung. Das gesammelte Know-how Ihrer Fachmagazine kompakt auf Archiv-Discs und -Sticks gespeichert jederzeit zum Abruf bereit. Ideal auch für jene, die an den kompletten Fachinformationen aus den Zeitschriften-Jahrgängen interessiert sind.



## Bessere Aussichten mit dem Blick zurück:

Fakten, Meinungen, Tests und Hintergrundwissen – das Jahresarchiv 2020 mit allen Beiträgen aus 26 c't-Heften

auf DVD **24,90 €**  
auf 32 GByte USB 3.0-Stick **34,90 €**

## c't-Know-how XXL:

Alle Artikel von 1983 bis 2020

auf Blu-ray Disc **99,90 €**  
auf 64 GByte USB 3.0-Stick **139,90 €**

[shop.heise.de/ct-archiv20](http://shop.heise.de/ct-archiv20)



## iX-Know-how für IT-Experten:

Nachlesen, vergleichen, absichern – alle iX-Inhalte kompakt.

auf DVD **24,90 €**  
auf 32 GByte USB 3.0-Stick **34,90 €**

## iX-Know-how XXL:

Alle Beiträge von 1988 bis 2020

auf 64 GByte USB 3.0-Stick **109,90 €**

[shop.heise.de/ix-archiv20](http://shop.heise.de/ix-archiv20)



## Neues baut auf Altem auf:

Ihr Blick in wichtige Fakten und Hintergrundinfos des Archives 2020 von Deutschlands einzigem Innovationsmagazin.

auf DVD **24,90 €**

## Technology Review-Know-how XL:

Alle Artikel von 2003 bis 2020

auf DVD **59,90 €**

[shop.heise.de/tr-archiv20](http://shop.heise.de/tr-archiv20)

**heise shop**

[shop.heise.de/archive20](http://shop.heise.de/archive20)

Bestellen Sie ganz einfach online im heise shop oder per E-Mail: [service@shop.heise.de](mailto:service@shop.heise.de)

© Copyright by Heise Medien.

# Tipps & Tricks

# Sie fragen – wir antworten!

## Öffentlichen Windows-PC vernageln

**?** Auf einem öffentlich aufgestellten PC in einem Museum sollen die Besucher ein interaktives (Windows-)Programm benutzen können, das per Touchscreen bedient wird. Das Programm belegt den ganzen Bildschirm, es soll kein Zugriff auf Windows möglich sein. Selbst ohne Maus oder Tastatur können Besucher aber derzeit mit einem Fingerwisch vom linken Bildschirmrand nach rechts die Task-Ansicht einblenden; ein Wischen vom rechten Bildschirmrand nach links öffnet das Benachrichtigungsfenster. Über beide Wege kann der Museumsbesucher Zugriff auf die Taskleiste und das Startmenü bekommen und allerlei Unfug treiben. Kennen Sie einen Weg, wie man die Wischmöglichkeiten verhindert und die Touch-Funktion ausschließlich aufs Tippen innerhalb des Programms reduziert?

**!** Welches die für Ihren Anwendungsfall passende Lösung ist, hängt vor allem davon ab, um was für ein Programm es sich bei der Anwendung handelt, die die Be-

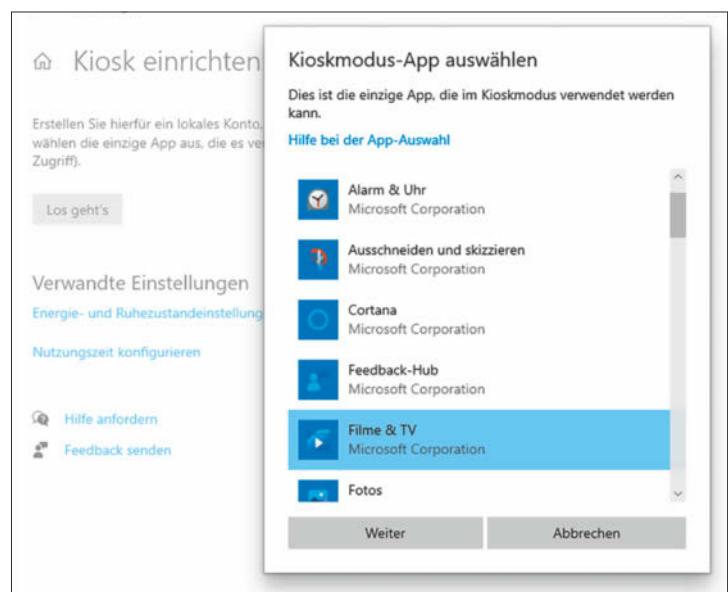
sucher benutzen sollen: Wenn es eine normale (Win32-)Anwendung ist, sollten Sie zunächst ein gesondertes Benutzerkonto einrichten, unter dem die Anwendung künftig läuft. Mit diesem Konto melden Sie sich einmal normal an, starten das Programm regedit und navigieren in der Registry zum Schlüssel `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\Current Version\Winlogon`. Erstellen Sie per Rechtsklick oder über das Bearbeiten-Menü eine neue Zeichenfolge und nennen Sie sie `Shell`. Als Wert tragen Sie den kompletten Pfad zum Besucherprogramm ein, also zum Beispiel "`C:\Program Files\Museum\Steinzeit.exe`"; wenn der Pfad wie im Beispiel Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen sein.

Wenn Sie sich nun abmelden und (mit oder ohne Windows-Neustart) unter demselben Konto neu anmelden, sollte sich direkt die Besucheranwendung öffnen, ohne dass zuvor der Explorer startet und einen Desktop lädt. Und ohne Desktop gibt es auch kein Action Center mit Benachrichtigungen und keine Task-Ansicht mehr. Allerdings auch kein Startmenü, über das sich der Rechner herunterfahren

oder die Einstellung rückgängig machen ließen. Dafür müssten Sie – auf einer kurzfristig angeschlossenen oder im Normalbetrieb vor den Besuchern versteckten Tastatur – die Tastenkombination `Strg+Alt+Entf` drücken und aus dem erscheinenden Menü den Befehl „Task-Manager“ wählen. Um dessen Menü anzuzeigen, müssen Sie gegebenenfalls unten auf „Mehr Details“ klicken. Anschließend können Sie per „Datei/Neuen Task ausführen“ nebst der Eingabe `explorer` einen Desktop starten und kommen so wieder an den Registry-Editor oder die Befehle zum Herunterfahren des Rechners.

Sollte es sich bei der Besucheranwendung um eine UWP-App aus dem Microsoft-Store handeln, öffnen Sie stattdessen die Einstellungen von Windows 10, wechseln auf die Seite „Konten/Familie und andere Benutzer“ und klicken unter „Kiosk einrichten“ auf „Zugewiesener Zugriff“. Ein weiterer Klick auf „Los geht's“ startet den Kiosk-Assistenten, der als Erstes einen Namen für ein neues Konto wissen will – lassen Sie das Feld leer, heißt es „Kiosk“. Im zweiten Schritt wählen Sie die Kiosk-Anwendung aus (wenn Ihre Besucher-App in der Liste fehlt, handelt es sich um eine normale Anwendung und die oben geschilderte Anleitung gilt). Wie oben müssen Sie sich nur noch unter dem neuen Konto anmelden, um die Besucher-App zu starten.

(hos@ct.de)



**Im Kiosk-Modus führt Windows nur eine einzige App aus und verwehrt den Zugang zu allen Systemfunktionen.**

## Unbound vs. Hyperlocal-Root

**?** Seit Ihrem Artikel „Selbstauskunft“ (Namensauflösung inklusive Datenschutz für Heimnetz, c't 12/2017, S. 130) betreibe ich einen eigenen DNS-Server mit Unbound unter Debian. Meine Frage: Welche Vor- oder Nachteile – vor allem in Bezug auf die Sicherheit – hat ein Betrieb von Unbound mit Hyperlocal-Root gegenüber der bestehenden Konfiguration mit DNS over TLS und Quad9 als Forwarder?

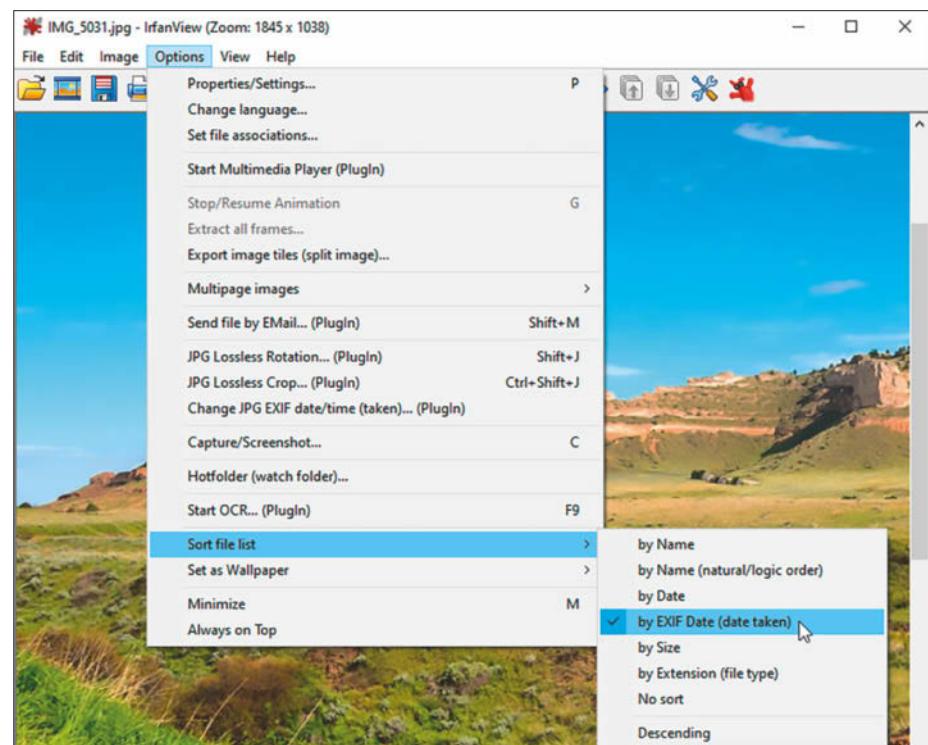
**!** Der Hauptunterschied besteht darin, dass man mit DoT und Quad9 einen externen Resolver befragt. Die Anfragen, die Sie an Quad9 schicken, sind zwar per TLS (also technisch) gegen Manipulation und Mitlesen gesichert, nicht aber dagegen, dass der Resolver-Betreiber Ihre Anfragen protokolliert und auswertet. Quad9 sichert zwar zu, das nicht zu tun, in der Praxis lässt sich das aber nur schwer überprüfen, sodass Sie dem Resolver-Betreiber vertrauen müssen. Wenn Sie hingegen Ihren Resolver selbst betreiben (Unbound mit Hyperlocal-Root), dann entfällt dieser Punkt.

Der zweite und nicht unwesentliche Unterschied besteht darin, dass ein externer Resolver-Betreiber selbst für den Betrieb seines Resolvers verantwortlich ist. Wenn etwas schiefgeht, repariert er es in der Regel auch selbst. Wenn man einen DoT-Client wie Stubby verwendet, kann man diesen so konfigurieren, dass er mehr als einen Resolver befragt. Das verbessert zumindest die Ausfallsicherheit des DNS-Dienstes. Je nach Befragungsprofil kann das sogar den Privatsphärenschutz verbessern: Stubby kann ja seine Anfragen an mehrere Resolver streuen, sodass keiner davon ein komplettes Abbild Ihrer Bewegungen im Netz mitbekommt.

Wenn Sie Unbound mit einer eigenen Hyperlocal-Root betreiben, liegt auch die Administrationsarbeit inklusive der Caching-Optimierungen komplett bei Ihnen und die Ausfallsicherheit ist mit einem einzigen Resolver natürlich geringer. Aber Sie könnten ja auch mehr als eine Unbound-Instanz betreiben – alles eine Frage des Aufwands.  
(dz@ct.de)

## Reihenfolge beim Blättern in Bildern

**?** Ich sammle in einem Ordner auf der Festplatte Fotos aus verschiedenen Kameras und sortiere die Liste im Explorer üblicherweise nach Aufnahmedatum. Doppelklicke ich auf ein Foto, um es in voller Größe zu betrachten, öffnet sich die Windows-Fotoanzeige – so weit, so gut. Wenn ich aber jetzt mit den Tasten Bild-auf oder Bild-ab zum vorherigen oder nächsten Foto wechseln will, springt die Fotoanzeige scheinbar willkürlich von Bild zu Bild, ich kann die Reihenfolge jedenfalls nicht nachvollziehen. Was kann ich tun, um der Fotoanzeige eine sinnvolle Reihenfolge beim Blättern beizubringen?



Manche Bildbetrachter wie das hier gezeigte IrfanView erlauben es, die Sortierreihenfolge beim Durchblättern von Fotosammlungen zu ändern.

**!** Leider nicht viel: Die Fotoanzeige von Windows 10 sortiert die Bilder offenbar nicht, sondern zeigt sie beim Blättern einfach in der Reihenfolge an, in der sie auf dem Datenträger gelandet sind – das entspricht im Zweifelsfall weder dem im Explorer angezeigten Datum noch dem Änderungsdatum und schon gar nicht dem im Bild selbst gespeicherten Aufnahmedatum.

Wenn Sie auf die Anzeigereihenfolge Wert legen, sollten Sie sich vielleicht einen alternativen Bildbetrachter zulegen und Windows so konfigurieren, dass sich JPG-Dateien bei einem Doppelklick in diesem öffnen. Zu den beliebtesten Programmen dieser Kategorie gehören IrfanView und XnView (Download via [ct.de/ynjc](http://ct.de/ynjc)). Bei beiden lässt sich konfigurieren, in welcher Reihenfolge sie durch Ordner blättern.  
(hos@ct.de)

**Alternative Bildbetrachter:** [ct.de/ynjc](http://ct.de/ynjc)

## PC als Access-Point

**?** Kann man eigentlich einen WLAN-fähigen Rechner, der über ein LAN mit dem Router verbunden ist, als Access-Point für den Router betreiben? Das würde mir die Anschaffung eines Repeaters ersparen.

**!** Im Prinzip ja. Im Microsoft-Store gibt es dafür sogar mehr oder weniger einfache Lösungen wie MyPublicWifi, Connectify, Virtual Wi-Fi oder WiFi HotSpot (Soft AP).

Beim Betrieb solcher Apps müssen Sie aber einige Nachteile in Kauf nehmen. So spielen sie Mesh-mäßig nicht mit dem restlichen WLAN-System zusammen. Dadurch wandern zentrale Änderungen etwa des Passworts nicht automatisch weiter und das Gastnetz ist nicht verfügbar. Auch fehlen den Apps typischerweise Funktionen zur Unterstützung des Client-Roamings (IEEE 802.11k, 11v).

Ein dauerlaufender PC braucht wesentlich mehr elektrische Energie als ein Repeater oder Access-Point. Zudem funktionieren übliche WLAN-Module in PCs nur in

Fragen richten Sie bitte an

**ct** [hotline@ct.de](mailto:hotline@ct.de)

**f** [c't Magazin](#)

**t** [@ctmagazin](#)

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter [www.ct.de/hotline](http://www.ct.de/hotline).

einem Frequenzband (2,4 oder 5 GHz, auf 5 GHz meistens mangels DFS auch nur im Kanalblock 36 bis 48). Für den Dauerbetrieb ist ein separates Gerät unserer Erfahrung nach stets sinnvoller als ein umfunktionierter PC. (ea@ct.de)

## WhatsApp-Konto löschen

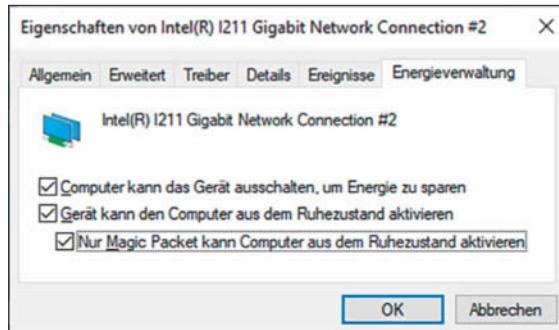
**?** Ich lehne die neuen Nutzungsbedingungen von WhatsApp ab und möchte mein Konto löschen. Inzwischen erscheint beim Aufruf der iOS-App aber ein vorgesetzter Dialog zur Zustimmung, ohne den man nicht mehr in die App kommt. Ein Löschen aus der App heraus ist damit ohne Zustimmung nicht mehr möglich. Auf eine Anfrage an WhatsApp mit der Bitte, mein Konto zu löschen, bekam ich als Antwort nur einen Textbaustein mit dem Hinweis, dass ich mein Konto in der App selbst löschen kann.

**!** An sich sollte man die aktualisierten Nutzungsbedingungen auch ablehnen können und damit den Account löschen, ohne den Bedingungen zustimmen zu müssen. Bei einem Redaktions-iPhone funktioniert das auch: Das Pop-up lässt sich per Kreuzchen schließen (und kommt dann irgendwann wieder).

Sie sind allerdings nicht der erste Leser, bei dem das offenbar nicht klappt. Eine Rückfrage bei WhatsApp ergab, dass es „eine kleine Anzahl an Nutzern“ gebe, die eine Weile inaktiv gewesen seien und daher ein WhatsApp-Update – das offenbar den Dialog abwählbar macht – nicht erhalten hätten. WhatsApp empfiehlt, dass davon betroffene Nutzer sich an support@whatsapp.com wenden, um das Problem zu lösen.

Prinzipiell haben Sie noch zwei weitere Optionen. Zum einen können Sie versuchen, eine Löschung über die Datenschutzkontakte bei WhatsApp zu veranlassen. Laut WhatsApps Datenschutzrichtlinie (Linkszudengenannten Dokumenten unter ct.de/ynjc) erreichen Sie den Datenschutzbeauftragten unter DPO-inquiries@support.whatsapp.com. Speziell für den Widerspruch der (weiteren) Datenverarbeitung ist laut Datenschutz-FAQ die Adresse Objection.eu@support.whatsapp.com zuständig.

Am besten richten Sie Ihr Anliegen an beide Adressen, falls Sie diesen Weg beschreiten wollen. WhatsApp verlangt allerdings, dass Sie eine ganze Latte an In-



In den Einstellungen von Netzwerkkarten lässt sich üblicherweise einstellen, dass sie den PC nicht bei jedem Broadcast-Paket aus dem Netz wecken, sondern nur beim Ein-treffen eines „Magic Packet“.

formationen beilegen (siehe „Wie kann ich Widerspruch einlegen?“ in den FAQ).

Die andere Möglichkeit ist, dass Sie WhatsApp deinstallieren und einfach warten. WhatsApp behauptet, dass inaktive Accounts nach 120 Tagen „normalerweise“ gelöscht werden. Das wäre wohl der geringste Aufwand für Sie, allerdings bekommen Sie so keine Bestätigung, dass die Daten tatsächlich weg sind. (syt@ct.de)

**WhatsApp-Dokumente:** [ct.de/ynjc](http://ct.de/ynjc)

## Rechner wacht von selbst auf

**?** Wenn ich meinen Rechner herunterfahre, schaltet er sich nach unbestimmter Zeit, manchmal nach Minuten, manchmal nach Stunden von selbst wieder an. Ich habe den Verdacht, dass meine Fritzbox 7490 mit diesem Phänomen zu tun hat, denn wenn ich das Netzwerkabel abziehe, ist dauerhaft Ruhe. Im BIOS-Setup ist Wake-on-LAN (WoL) eingeschaltet und das soll möglichst auch so bleiben. In der Fritzbox ist unter „Heimnetz/Netzwerk“ die Option „Diesen Computer automatisch starten, sobald aus dem Internet darauf zugegriffen wird“ für den betroffenen PC ausgeschaltet. Was kann ich noch tun?

**!** Schauen Sie mal, auf welchen Wake-on-LAN-Modus die Schnittstelle des PCs konfiguriert ist. Manche Betriebssysteme haben eine Voreinstellung, bei der auch Broadcast-Pakete einen Wake-on-LAN auslösen. Eventuell gibt es in den erweiterten Einstellungen des LAN-Ports eine Wahlmöglichkeit. Dort stellen Sie dann „Nur Magic Packet“ oder ähnlich ein, siehe Beispiel im Screenshot.

Broadcasts gehen ständig durchs Netz, wenn auch nur ein Gerät mit (W)LAN-Schnittstelle aktiv ist, beispielsweise beim Einschalten zur IPv4-Adressabfrage und zur Kollisionserkennung per DHCP.

Daran ist nichts ungewöhnlich oder besorgnisregend. (ea@ct.de)

## BIOS-Einstellungen für „optimalen PC“

**?** 2012 habe ich den „optimalen PC“ nach Ihrer Anleitung gebaut und bis vor wenigen Tagen hat er prima funktioniert. Dann war aber die Knopfzelle am Motherboard leer. Deshalb hat das BIOS alle Einstellungen verloren und es gibt bei jedem Start Probleme. Nach dem Tausch der Batterie möchte ich nun die Einstellungen wieder so setzen, wie sie damals auf der Projektseite dokumentiert waren. Leider ist die Seite mit den BIOS-Einstellungen nicht mehr erreichbar. Deshalb meine Bitte: Sind die BIOS-Einstellungen für das Motherboard Asus P8Z77-M in Ihrem Archiv noch auffindbar und könnten Sie mir diese zukommen lassen?

**!** Sie haben recht, die Webseite gibt die BIOS-Einstellungen tatsächlich nicht mehr her. Zusammen mit unserem technischen Assistenten Denis Fröhlich habe ich unser Archiv durchstöbert und dort konnten wir die Einstellungen finden. Sie entnehmen sie der untenstehenden Tabelle. (csp@ct.de)

## BIOS-Optionen für den optimalen PC 2012

Option	Wert	Menü
EPU Power Saving Mode	Enabled	Ai Tweaker
Intel Virtualization Technology	Enabled	Advanced/CPU Configuration
Intel xHCI Mode	Enabled	Advanced/USB Configuration
ErP Ready	Enabled	Advanced/APM
CPU Fan Speed Low Limit	200 RPM	Monitor
CPU Fan Profile	Silent	Monitor
Chassis 1 Fan Speed Low Limit	300 RPM	Monitor
Chassis 1 Fan Profile	Silent	Monitor
Boot Option #1	Samsung SSD 830 Series	Boot/Hard Drive BBS Priorities



# DIE Jobbörse für IT-Experten\*

## unter dem Dach von heise online

Qualität  
statt  
Quantität

**Im neuen Look:** Frisch • Jung • Modern.

### Und neuen Features:

- Die besten Jobs in der IT – mit über 3.000 Jobangeboten.
- Jobmailer: passende Jobs zu Ihrer Suche finden
- Stellenanzeigen mobil-optimiert – egal wo und wann.  
Immer gut lesbar.
- Verknüpfung mit den redaktionellen Rubriken: IT, Mobiles, Entertainment und Wissen.
- Die perfekte Bewerbung mit bewerbung2go erstellen.

\* viele Stellenangebote für Fach- und Führungskräfte

**Finden Sie bei uns Ihren Spitzen-Job in der IT!**

Schauen Sie vorbei: [www.heisejobs.de](http://www.heisejobs.de)

# FAQ

# Multigigabit-Ethernet

**Gigabit-Ethernet ist Alltag, Multigigabit-Ethernet alias NBase-T lockt mit vielfach höherer Datenrate. Die wichtigsten Fakten zur nächsten Technik-generation fürs LAN erörtern wir anhand häufiger Fragen und Antworten.**

Von Ernst Ahlers

## Kabel statt Funk

❓ Wozu braucht man noch Ethernet, es gibt doch WLAN?

❗ Das Netzwerkkabel hat einen schlagernden Vorteil: Die Geräte an seinen Enden nutzen es exklusiv, anders als das Funkspektrum bei WLAN, wo einem immer Nachbarn reingrätschen können. Man erhält per Kabel jederzeit die maximal mögliche Nettodatenrate, bei Gigabit-Ethernet rund 950 MBit/s (circa 115 MByte/s), bei 2,5-, 5- und 10-GBit/s-Ethernet entsprechend mehr. Stationäre Geräte sollte man möglichst immer per Kabel anschließen. Das entlastet das eigene WLAN, besonders wenn Dauerverkehr darüber läuft, beispielsweise Videostreaming. Schließlich kann ein Ethernet-Kabel anders als WLAN auch Energie transportieren (Power-over-Ethernet, PoE). Damit lassen sich Überwachungskameras, WLAN-Basen oder VoIP-Telefone über eine einzige Leitung anschließen.

## Mehr Speed

❓ Wer braucht 2,5 GBit/s oder mehr im LAN?

❗ Alle, die ständig sehr große Dateien – Videoaufnahmen oder VM-Images – im LAN hin und her kopieren, profitieren direkt durch kürzere Wartezeiten von den höheren Datentransferraten. Indirekt nutzen extraschnelle Verbindungen zwischen Abteilungsswitches in Firmen. Für den Heimeinsatz genügt hingegen Gigabit-Ethernet – zumindest solange noch, bis sich Internetanschlüsse ausbreiten, die mehr als 1000 MBit/s liefern.

## Mehr Strom

❓ Welche Nachteile hat Multigigabit-Ethernet?

❗ Für Netze mit Multigigabit-Ethernet braucht man neue Verteiler (Switches) sowie Netzwerkadapter in PCs und Notebooks, es wird also eine Investition in Hardware fällig. Viele High-End-Mainboards bringen schon einen immerhin 2,5 GBit/s schnellen Netzwerkanschluss mit. Je schneller der Ethernet-Link ist, desto höher wird auch sein Leistungsbedarf: Während ein Gigabit-Ethernet-Port mit rund 0,3 Watt auskommt, werden für 10 GBit/s über Kupfer schon 2–3 Watt fällig. Damit steigen die Stromkosten und Desk-

top-Switches fürs Büro – zumindest jene der im Sommer 2021 aktuellen Generation – sind wegen ihrer Lüfter nicht unhörbar.

## Mehr Kosten

❓ Warum ist 10-Gigabit-Ethernet über Kabel noch so teuer?

❗ Zwar gibt es 10GBase-T, 10 GBit/s über Kupferkabel, schon seit 2006. Aber es hat sich bisher sehr langsam verbreitet, weil es für die maximale Ethernet-Segmentlänge von 100 Metern eine CAT6a-Verkabelung voraussetzt. Langsam löst NBase-T mit den Zwischenstufen 2,5 und 5 GBit/s das etablierte Gigabit-Ethernet ab, denn es funktioniert auch auf älteren CAT5e-Kabelsystemen – bei 10 GBit/s aber nur bis ungefähr 50 Meter Leitungslänge. Wer nun seine Hardware aufrüstet, sollte aber nicht aufs Marketing hereinfallen und sich mit 2,5 GBit/s zufriedengeben, sondern gleich für die Zukunft planen und mindestens 5 GBit/s vorsehen. Sonst wird vielleicht in ein paar Jahren schon wieder ein Hardware-Tausch nötig.

## Teilschritte

❓ Was bringen die Zwischenstufen 2,5 und 5 GBit/s?

❗ Wenn der Sender – beispielsweise ein Netzwerkspeicher oder Server – seine Daten flott genug liefern kann, schaffen die NBase-T-Zwischenstufen praktisch den zweieinhalb- beziehungsweise fünf-fachen Durchsatz von Gigabit-Ethernet. Die 2,4 GBit/s netto bei einem 2,5-GBit/s-Link rechnen sich um zu rund 300 MByte/s, entsprechend rund 550 MByte/s bei einem 5-GBit/s-Link. Um eine 10-GBit/s-Verbindung mit 1100 MByte/s auszuschöpfen, muss ein NAS aber mit einer passend angebundenen RAID-5-



Multigigabit-Switches wie der Zyxel XGS1250-12 schaffen auf mehreren Ports bis zu 10 GBit/s, ziehen aber deutlich mehr Energie als ihre Gigabit-Ethernet-Pendants und müssen deswegen aktiv gekühlt werden – ein kleiner Lüfter sirrt leise.

Konstellation aus SATA-SSDs oder gleich mit NVMe-SSDs bestückt sein.

## Multigigabit per USB

**?** Warum gibt es keine USB-Adapter für 10 GBit/s?

**!** USB 3.2 Gen 2 erreicht zwar 10 GBit/s auf der USB-Leitung, aber durch den Protokoll-Overhead wird man diesen Durchsatz auf der Ethernet-Seite nicht erreichen. Schon bei Adapters mit USB 3.2 Gen 1 alias SuperSpeed (5 GBit/s) für NBase-T mit maximal 5 GBit/s stellten wir fest, dass sie bestenfalls rund 3,5 GBit/s übers Netz schicken (c't 6/2020, S. 78). Vielleicht wird es mit dem kommenden USB 4.0 dann Ethernet-Adapter geben, die bis zu 10 GBit/s im LAN schaffen.



**USB-Adapter für Multigigabit-Ethernet wie Trendnets TUC-ET5G mit USB 3.2 Gen 1 alias SuperSpeed (5 GBit/s) erreichen auf dem LAN-Kabel ebenfalls schon 5 GBit/s Linkrate. Wegen Beschränkungen im USB-Protokoll transportieren sie auf Anwendungsebene aber höchstens 3,5 GBit/s – immerhin fast das Vierfache von Gigabit-Ethernet.**

## Licht statt Elektrik

**?** Ist Glasfaser im Haus sinnvoller?

**!** Ethernet über Glasfaser erreicht zwar viel höhere Datenraten als über Kupfer, aktuell ist es bis 800 GBit/s standardisiert. Aber die Leitungen sind empfindlicher und es gibt nur sehr wenige Router, die fürs LAN SFP+-beziehungsweise SFP+Slots enthalten (Einsätze für 1- und 10-GBit/s-Optikmodule). Auch PCs mit SFP/SFP+-Fassungen sind rar, sodass man

## Gebräuchliche Ethernet-Varianten

Bezeichnung	Medium <sup>1</sup>	max. Distanz <sup>2</sup>	Bruttodatenrate
100Base-TX	Kupfer (2 Adernpaare)	100 m	100 MBit/s
1000Base-T	Kupfer (4 Adernpaare)	100 m	1000 MBit/s
1000Base-SX	Glas (2 Fasern, MMF)	220–550 m	1000 MBit/s
1000Base-LX	Glas (2 Fasern, SMF)	5 km	1000 MBit/s
1000Base-BX10	Glas (1 Faser, SMF)	5 km	1000 MBit/s
2500Base-T	Kupfer (4 Adernpaare)	100 m	2500 MBit/s
5000Base-T	Kupfer (4 Adernpaare)	100 m	5000 MBit/s
10GBase-T	Kupfer (4 Adernpaare)	100 m	10.000 MBit/s
10GBase-SR	Glas (2 Fasern, MMF)	25–400 m	10.000 MBit/s
10GBase-LR	Glas (2 Fasern, SMF)	10 km	10.000 MBit/s

<sup>1</sup> MMF = Multi-Mode Fiber, SMF = Single-Mode Fiber

<sup>2</sup> Kupfer: auf CAT5e-Leitungen, bei 10GBase-T CAT6a, das mit CAT5e max. ca. 50 m

eine PCI-Express-Karte plus Optikmodul nachbestücken muss.

Sinnvoll ist eine Glasfaserverbindung wegen der elektrischen Potenzialtrennung (Blitzschutz, keine PEN-Ausgleichsströme) beispielsweise, wenn man ein Nebengebäude ans LAN des Haupthauses anschließen möchte. Ferner braucht ein 10-GBit/s-Optikmodul mit rund 1 Watt auch nur ein Drittel der Leistung eines vergleichbaren 10-GBit/s-Moduls für Kupferkabel. Ob diese Energieersparnis den Umrüstungsaufwand wert ist, muss jeder selbst entscheiden.

## Schnellerer Ping

**?** Sinkt mit Multigigabit-Ethernet nicht auch die Pingzeit?

**!** Ja, die Latenz (Round Trip Time, RTT) sinkt mit steigender Datenrate tatsächlich etwas. Aber der Unterschied zwischen Gigabit-Ethernet (1000 MBit/s) und 10-Gigabit-Ethernet (10.000 MBit/s) im LAN ist nach unseren Messungen so klein (0,50 Millisekunden zu 0,40 Millisekunden), dass er für Gamer bedeutungslos ist. Wenn es nur um den Ping geht, können Sie sich die Ausgabe für Multigigabit-Ethernet sparen.

## Jumbo-Frames bleiben proprietär

**?** Bei 10-Gigabit-Ethernet konnte man früher mit Jumbo-Frames den Durchsatz erhöhen beziehungsweise die CPU-Last senken. Ist diese Technik inzwischen standardisiert?

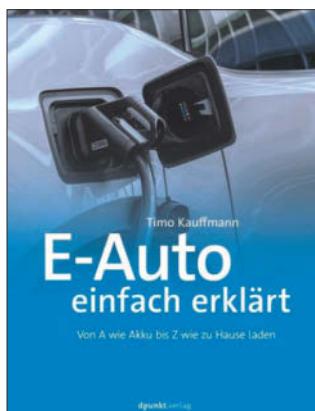
**!** Jumbo-Frames sind tatsächlich schon sehr lange in Gebrauch, aber auch mit

der Erweiterung NBase-T (IEEE 802.3bz) immer noch nicht in den Ethernet-Standards IEEE 802.3 eingeflossen. Nach wie vor kann es also in seltenen Fällen wegen Inkompatibilitäten zu Durchsatzeinbrüchen kommen, wenn man sie auf Hardware unterschiedlicher Hersteller aktiviert. Unseren Versuchen nach klettert der maximale TCP-Durchsatz auf einer 10-GBit/s-Verbindung mit 9000-Byte-Frames von 9,4 auf 9,9 GBit/s. Diese fünf Prozent kann man zwar messen, wird sie in der Praxis aber nur selten spüren. Immerhin bleibt der Vorteil der niedrigeren CPU-Last erhalten: Bei einem Core-i3-6300-Prozessor sank sie von rund 15 auf 5 bis 10 Prozent (je nach Übertragungsrichtung). Auch das dürfte in der Praxis vernachlässigbar sein.

## Stop-and-Go am Switch

**?** Ich habe einen 10-GE-fähigen PC über einen Switch mit dem WLAN-Router verbunden, der 2,5 GBit/s kann. Der WLAN-Durchsatz zu meinem Notebook ist aber niedriger als bei einer 1-GBit/s-Verbindung. Was ist da los?

**!** Einen ähnlichen Effekt haben wir bei WLAN-Messungen an Routern festgestellt: Mit 10 GBit/s zwischen Test-PC und Switch sowie 2,5 GBit/s zwischen Switch und Router gingen nur rund 0,9 GBit/s über WLAN. Begrenzt wurde die PC/Switch-Verbindung per Konfiguration am Switch auf 2,5 GBit/s, dann kletterte der gemessene WLAN-Durchsatz deutlich auf 1,4 GBit/s. Vermutlich kam es durch die stark unterschiedlichen Linkraten zu einem Stau mit Stop-and-Go durch volllaufende Puffer in Switch und Router. Manchmal kann es also helfen, die Linkraten zu senken. (ea@ct.de)



Timo Kauffmann

### E-Auto einfach erklärt

Von A wie Akku bis Z wie zu Hause laden

dpunkt, Heidelberg 2021

(der Buchverlag gehört  
wie c't zu Heise Medien)

ISBN 978-3864908255

254 Seiten, 25 €

(PDF-/Epub-/Kindle-E-Book: 20 €)

## Smartphones auf Rädern

**Die EU-Kommission hat das Jahr 2035 zum Schlusspunkt für die Zulassung neuer Autos mit Verbrennungsmotor erklärt. Der Umstieg auf E-Mobile bedeutet für Autofahrer in vielerlei Hinsicht eine Neuorientierung. Kauffmanns Erklärbuch zeigt, worum es in der Praxis geht.**

Timo Kauffmann fährt seit Jahren einen Tesla und ist es von daher gewohnt, dass seine Mobilität von deutlich mehr digitaler Intelligenz bestimmt und überwacht wird als die des gegenwärtigen Durchschnittsautomobilisten. Aus seiner eigenen Erfahrung vermittelt er in seinem Buch E-Auto-Neulingen, welche Überlegungen, Einschränkungen und anderen Parameter für ihren Fahralltag wichtig sind.

Dabei kommt auch Grundsätzliches zur Sprache – so vergleicht Kauffmann den sogenannten CO<sub>2</sub>-Fußabdruck des Elektroantriebs mit dem anderer Technologien, wobei er die Herkunft des Stroms mit einbezieht.

Intensiv widmet er sich Aspekten der Reichweite. Er gibt Tipps zur Verringerung der Leistungsaufnahme und zur optimalen Reiseplanung. Seine Argumente untermauert er mit konkreten Zahlen.

Ein weiterer Themenschwerpunkt betrifft Akku und Lade-technik. Ausführlich behandelt der Autor alle gegenwärtig verfügbaren Optionen. Bei den verschiedenen Spielarten öffentlicher Ladesäulen berücksichtigt er auch Bezahlmöglichkeiten einschließlich Ladekarten und Apps.

Technisch orientierte Kapitel geben Interessierten Einblick in Konstruktionsdetails von E-Autos. Dort geht es etwa um Motor-, Akku- und Steckertypen. Auch Liebhaber von Technologiegeschichte kommen nicht zu kurz.

Die Abschnitte, die sich um das eigentliche Fahren drehen, zeigen Autofahrern, dass ein Umstieg auf elektrische Antriebstechnik eine größere Umgewöhnung bedeutet, als man annehmen möchte, und viel Lernbereitschaft verlangt. Das betrifft etwa die typische Praxis des One-Pedal-Driving, also das rekuperative Fahren vornehmlich mit dem „Gaspedal“ und mit minimalem Bremseinsatz.

Auch sonst gibt es mancherlei zu beachten; so zwingen Witterungsbedingungen und zusätzliche Stromverbraucher im Wagen zu ungewohntem Haushalten mit Wattstunden. Gegen Schluss klären mehrere kurze Kapitel über Besonderheiten etwa bei der Fahrzeugwartung, zusätzliche Versicherungen oder die Bedeutung des E-Kennzeichens auf.

Kauffmanns Text liest sich locker, ist allerdings streckenweise deutlich subjektiv gefärbt und zudem Tesla-lastig. Viele seiner Ratschläge können dennoch für anstehende Kaufentscheidungen hilfreich sein.

(psz@ct.de)

## Erziehung mit Augenmaß

**Gerade dachten Eltern, sie seien mit ihren Facebook- und WhatsApp-Kenntnissen ganz gut gerüstet für die Medien-erziehung, da sind ihre Kinder schon weitergezogen zu TikTok und Snapchat. Bückleins Ratgeber erklärt den Reiz und die Fallstricke der neuen Plattformen und hilft Eltern, eine Haltung dazu zu finden.**

In seinem ebenso klug wie unterhaltsam geschriebenen Buch liefert Tobias Bücklein alles, was Eltern aktuell über soziale Netzwerke wissen sollten. Er erklärt die Funktionen von TikTok, Snapchat und Insta, kurz und knapp auch die von WhatsApp, Facebook, Twitter und so weiter. Außerdem liefert er rechtliche Hinweise und Informationen zu Datenschutz und Vermarktingsstrategien und gibt schließlich immer wieder wunderbare Erziehungstipps. „Sie dürfen streng sein“, steht da etwa in einem Merktext, aber auch so wichtige Sätze wie „Das Warum muss klar sein“ oder „Kritisieren Sie das Handeln, nicht das Kind“.

Bücklein – selbst Vater – weiß, wovon er schreibt; sein Sohn ist als YouTuber aktiv. Die Reihenfolge der Kapitel macht klar, welche Priorität die Themen für den Autor haben: Erst geht es um die richtige Haltung dem Thema gegenüber, dann generell um die dunklen Seiten der sozialen Medien. Danach folgen einzelne Abschnitte zu den derzeit angesagtesten Plattformen und erst ganz zum Schluss gibt ein knappes Kapitel handfesten Rat zu technischen Hilfsmitteln wie Kinderschutz-Apps und beschränkenden Einstellungen in iOS und Android.

Wenn es an diesem gelungenen Ratgeber etwas zu kritisieren gibt, dann sind dies leichte Schwächen in der grafischen Gestaltung. Bei den reichlich vorhandenen, aber zu klein geratenen Bildern ist der Bezug zum Text oft unklar. Schwerer wiegt das Farbkonzept des Buchs: Jedes Kapitel hat seine Signalfarbe, Zusammenfassungen und Tipps sind in diesen Farben gestaltet. So steht ausgerechnet das Wichtigste in Himmelblau auf Weiß oder in Grau auf Zartlila und ist nur schwer zu lesen.

Ansonsten ist Bückleins Buch eine klare Empfehlung wert. Wer Kindern einen kritischen, selbstbewussten Umgang mit sozialen Medien vermitteln möchte, bewegt sich auf einem schmalen Grat: Alles prima finden ist keine Lösung – alles mit erhobenem Zeigefinger madig machen aber auch nicht. Dieser Ratgeber nimmt Eltern keine Erziehungsentscheidungen ab, hilft ihnen aber zuverlässig, sie irgendwo zwischen diesen Extremen richtig zu treffen.

(dwi@ct.de)



Tobias Bücklein

### TikTok, Snapchat und Instagram

Der Elternratgeber

**TikTok, Snapchat und Instagram**

Stiftung Warentest, Berlin 2021

ISBN 978-3747104200

192 Seiten, 17 €

(PDF-/Epub-/Kindle-E-Book: 14 €)

# TECHNIKUNTERRICHT MACHT ENDLICH SPÄß!



Spannende  
Unterrichts-  
materialien  
**GRATIS**

## Make: Education

Mit **Make Education** erhalten Sie jeden Monat kostenlose Bauberichte und Schritt-für-Schritt-Anleitungen für einen praxisorientierten Unterricht:



Für alle weiterführenden  
Schulen



Digital zum Downloaden



Fächerübergreifend



Monatlicher Newsletter

Jetzt kostenlos downloaden: [make-magazin.de/education](http://make-magazin.de/education)



# CYBERCRIME FÜR ANFÄNGER

## von Barbara Schwarz

**D**ie Dame mir gegenüber hinter dem Schreibtisch warf einen kurzen Blick auf ihren Fragebogen. „Wie haben Sie von unserem Unternehmen erfahren?“, leierte sie herunter. „Print-Inserate, Onlinewerbung, Mundpropaganda oder Sponsoring? Bitte nur eine Antwort.“

„Äh, Mundpropaganda.“ Ich rutschte voll Unbehagen auf meinem Stuhl hin und her und hoffte, sie würde nicht fragen, welcher meiner alten Knastkumpels mir den Tipp gegeben hatte.

Sie machte auf dem Bogen ein Häkchen, griff dann mit spitzen Fingern nach dem obersten Blatt des Papierstapels, der vor ihr lag. Für einen Moment erstarrte ihre Miene. „Und hier ist Ihr Lebenslauf. Ein – ich muss schon sagen – ungewöhnliches Format.“

„Finden Sie?“ Ich hatte mir große Mühe gegeben, eine ordentliche Schere und den guten, teuren Klebstoff verwendet. Die knallig pinkfarbenen, geschwungenen Buchstaben mochten vielleicht etwas feminin wirken, aber in der Notunterkunft am Bahnhof gab es eben bloß eine begrenzte Auswahl an Zeitschriften. „Warum?“

Sie seufzte. „Herr Paulsen –“

„Paule, bitte. Alle meine Kumpels nennen mich so.“

„Herr Paule.“ Bevor ich widersprechen konnte, redete sie weiter: „Üblicherweise verfasst man seine Bewerbungsunterlagen am Computer. Man klebt nicht ausgeschnittene Buchstaben auf Papier.“

„Tschuldigung.“ Beschämmt zog ich den Kopf ein. „Die Macht der Gewohnheit.“

„Gewohnheit“, wiederholte sie bedeutsam und überflog den Lebenslauf. „Ach ja, ich sehe: Sie waren gleich nach der Schule das erste Mal ...“ Sie ließ den Satz in der Luft hängen.

„Im Knast“, gestand ich und versuchte entwaffnend zu lächeln. „Nur wegen eines Dummejungenstreichs! Man hat kein Geld, will aber dazugehören und Zigaretten sind teuer ...“

„Das war erst der Anfang. Nötigung, Bedrohung, Erpressung, versuchte Erpressung“, unterbrach sie mich scharf. Sie tippte etwas in ihren PC. Der Bildschirm stand so, dass ich nicht sehen konnte, was. „Tatsächlich. Das sollte ...“ Mit neuem Elan klickte sie sich durch ein Menü, musterte mich dann eindringlich. „Sie erfüllen zwar nur einen Teil der Voraussetzungen, aber – sind Sie lernwillig, Herr Paule?“

Eifrig nickte ich. „Da können Sie jeden in der Gefängnisstante fragen. Hat mir einer mal gesagt: ,Paule, ich will nur einen Löffel Gemüse zum Fleisch!‘, habe ich ihm nie wieder einen zweiten auf den Teller geklatscht.“

**Die Digitalisierung lässt allerorten neue Chancen und Geschäftsmodelle entstehen. Gleichzeitig bekommt mancher, der im konventionellen Business daheim ist, Orientierungsschwierigkeiten. Der Wandel, der fast alle Bereiche von Handwerk, Industrie, Medien und Verwaltungswesen durchzieht, macht auch vor der Unterwelt nicht halt.**

Das schien ihr zu genügen. „Sie können in drei Tagen anfangen. Wir haben mehrere freie Stellen in den Abteilungen Media Marketing und Data Governance zu besetzen, aber bei Ihrem Profil denke ich am ehesten an Human Resources.“

Verstohlen kniff ich mich in den Schenkel. Nach unzähligen erfolglosen Bewerbungen gab es tatsächlich noch so was wie Wunder. Oder ich hatte mich verhört. „Human Re-

sources? Heißt das nicht Personalabteilung?“, erkundigte ich mich vorsichtig. „Ich meine ... so etwas wie Lohnverrechnung habe ich nie gelernt und wie das mit den Kassen funktioniert, weiß ich auch nicht so genau.“

„Bei uns bedeutet ‚Human Resources‘ schlicht und einfach ‚menschliche Ressourcen‘“, informierte sie mich. „Soll heißen: Wir bueten Menschen aus.“ Unvermittelt lehnte sie sich über den Tisch und schüttelte meine Hand. „Und Sie, Herr Paule, werden uns dabei helfen.“

\* \* \*

Drei Tage später stand ich in meinem besten Anzug, dem mit den nur leicht ausgebeulten Knien, im Empfangsbereich der Firma. Ein gutes Omen: Drei war meine Glückszahl. Na ja, meistens. Das dritte Mal vor dem Richter hatte mir ganze zehn Jahre hinter schwedischen Gardinen eingebracht – und das ausgerechnet nachdem Lydia mir gestanden hatte, dass ihre Tage bereits seit drei Wochen überfällig waren. Lassen wir das. Ich zog, so gut es ging, den Bauch ein und hoffte, niemand würde genau genug hingucken, um den Streifen behaarter Haut zwischen dem ausgeleierten Gummi meiner Socken und den zu kurzen Hosenbeinen zu bemerken.

Pünktlich um neun schlenderte ein Mitarbeiter der Firma in Jeans und einem roten Pulli herbei. Und diese Frisse über dem Kragen kannte ich doch. „Babybrei-Kalle!“, entfuhr es mir. „Ich dachte, du sitzt noch ein.“

„Nee, gute Führung. Wurde vorzeitig entlassen“, erwiderte Kalle launig und hieb mir auf die Schulter, dass es klatschte. „Flinkfinger-Philipp arbeitet auch hier“, verriet er mir im nächsten Atemzug. „Der macht jetzt Data Governance. Und der schöne Ludo – du erinnerst dich an Ludo?“

Und ob! Ludo war ein Heiratsschwindler. Mehr als das: Er war der beste Heiratsschwindler, den unser Knast je erlebt hatte. Jeden Tag hatte er Besuch von Frau und Kind gehabt. Montags war es die Rothaarige mit dem Baby gewesen, dienstags eine hochschwangere Blondine, mittwochs dann die Zwillingsmami mit den schwarzen Locken – und immer

so weiter bis zu der Brünetten mit ihrer Mutti und den drei halbwüchsigen Jungs, die bei uns alle zusammen nur „die Sonntags“ geheißen hatten.

Während wir über alte Zeiten quatschten, führte mich Kalle rauf. Verdutzt blieb ich am Eingang zum Großraumbüro stehen. Der große, helle Raum erschien mir völlig anders als die Büros, die ich kannte. Nicht dass ich je in einem gearbeitet hätte, aber man wusste doch aus dem Knastfernsehen, wie so was aussah: jede Menge Schreibtische zwischen diesen tristen grauen Raumteilern, die mich immer an meine heimelige Zelle erinnert hatten. Das hier ähnelte eher dem Gemeinschaftsraum im Knast, bloß mit Lederosas, einer Bar und nicht den zugespachtelten Löchern überall dort, wo Gorilla Bruno die Faust ausgerutscht war.

## „FLINKFINGER-PHILIPP MACHT JETZT DATA GOVERNANCE.“

„Da drüben sind wir: Human Resources“, erklärte Kalle. „Und dort Media Marketing“, er ruckte mit dem Kinn in die Richtung einer Gruppe junger Frauen und Männer, die auf Laptops herumtippten. Ich folgte ihm zu einer Ledercouch. Dabei mussten wir an drei großen Terrarien in der Mitte des Raumes vorbei – schalldichten Quadern, rund zwei Meter zwanzig hoch und vielleicht acht Quadratmeter Grundfläche. Im ersten saß der schöne Ludo mit seinen schulterlangen, ge gelten Locken und seinem Megawatt-Lächeln und telefonierte.

Kaum angekommen, reichte mir Kalle ein Smartphone. „Hier, für die Arbeit.“

Eine Werkbank mit Leim oder Kleister wäre mir lieber gewesen. „Und was genau ist die Arbeit?“

„Pass auf: Du gehst mit einem unserer Fake-Profile auf Social Media. Die Leute vom Media Marketing erstellen die für uns, kannst dir ja mal angucken wie, ist aber erst mal nicht so wichtig. Dann suchst du dir Profile von Frauen zwischen vierzig und hundert raus. Die schreibst du an. Und zwar immer: ‚hey alles okay bei dir‘. Und wenn eine antwortet, egal was, schreibst du zurück: ‚du siehst süß aus‘.“

„Und dann?“

„Wenn sie darauf noch mal reagiert, hast du sie an der Angel. Dann geht es nur noch darum zu entscheiden, wann man sie einholt oder ob man sie noch zappeln lässt. Aber darum brauchst du dich nicht zu kümmern, das übernehmen ich und später dann Ludo, Nils oder Matteo.“

Der Job erschien mir nicht schwierig – allemal leichter als den Bahnhofskiosk nach Zeitschriften zu durchforsten, in deren Schlagzeilen „Q“, „Z“ oder „Y“ vorkamen. Kalle hockte neben mir, er hatte die Beine auf dem Couchtisch und machte das, was er die Stufe zwei des Jobs nannte.

„... schi-cke mir geld für das be-grä-bnis meiner o-mi“, murmelte er beim Tippen vor sich hin.

Moment mal. „War das beim letzten Mal nicht das Be- gräbnis deiner Schwester?“

Er grinste verlegen. „Manchmal improvisiere ich. Das merkt keiner. Du verpfeifst mich doch nicht?“  
„Natürlich nicht! Ehrensache.“

\* \* \*

Ich lernte schnell. Schon nach ein paar Tagen Einweisung durfte auch ich auf Stufe zwei arbeiten und zehntausend Mal am Tag fremden Frauen schreiben: „bin so verzweifelt, mein sohn braucht eine teure op. baby kannst du mir helfen mein engel??“ Das war schon härtere Kost; ich wurde beim Schreiben selbst ganz verzweifelt und meine Gedanken schweiften ab. Zu dem Besuchstag, an dem Lydia mich mit dem Ultraschallbild überrascht hatte. Und zu Muttis verheultem Gesicht hinter der Glaswand. Ich war ja daran gewöhnt gewesen, dass sie meinetwegen geheult hatte, aber meistens nicht vor Freude. „Versprecht mir, dass ihr den Jungen, wenn es einer wird, nach seinem Opa benennt“, hatte sie geschnieft. Keine Ahnung, ob Lydia das getan hatte.

Ein lauter Schrei und Türenknallen rissen mich aus den Gedanken. Aus einem der Terrarien stürmte ein junger Mann mit tränenerüberströmtem Gesicht. Die Tür der Raucherterrasse fiel hinter ihm ins Schloss.

Ich wandte mich an Kalle. „Sollten wir fragen, was mit dem armen Kerl los ist?“

„Iwo“, wehrte der Bayer von der Couch gegenüber ab. „Des is bloß der Nils, der drückt mal wieda auf die Tränendrüse.“

Hilfe suchend guckte ich Kalle an. „Schauspielschüler“, erklärte dieser knapp. „Verdient sich hier sein Studium.“ Er musste merken, dass ich nicht überzeugt war, denn er schüttelte leicht den Kopf. „Komm mit.“

Wir gingen raus und Kalle deutete auf den jungen Schauspieler, der mit zwei Frauen nahe dem Terrassengeländer stand und unbekümmert lachte und scherzte. Der Bayer war uns gefolgt. „Paule, Erpressung und Nötigung“, stellte Kalle uns einander vor. „Sepp, Safeknacker.“

„Mei Mama wollt immer, dass ich in einer Bank arbeite“, witzelte Sepp, der Safeknacker. „Nur eben net mit Gummihandschuhen, sondern mit Ärmelschonern.“ Er wies auf die inzwischen bereits drei hübschen jungen Frauen, die Nils umringten. „Wo kommen die her?“

„Data Governance“, verriet Kalle uns beiden. Und seufzte. „Glaub mir, das ist wie Zauberei. Ich durfte mal zugucken.“

### Über die Autorin

Die Österreicherin Barbara Schwarz ist mit ihren mal humorigen, mal anrührenden, mal schockierenden Geschichten ein gern gesehener Stammgast bei den c't-Stories. Mit dem in c't 16/2019 abgedruckten „Score!“ war sie 2020 für den renommierten Kurd-Laßwitz-Preis (KLP) nominiert. Die Autorin begegnet dem technischen Fortschritt mit Neugier und einer gehörigen Portion Skepsis. Insbesondere fasziniert sie, wie viel Macht wir den Maschinen im Alltag einräumen.

betterCode()

# JAVA 17

Die Heise-Konferenz zur  
neuen LTS-Version

Online am 14. September 2021

Jetzt  
**Frühbucher-  
Rabatt  
sichern!**

Die betterCode() Java 17 gibt  
Ihnen Antworten auf wichtige Fragen:

- ✓ Was sind die zentralen Neuerungen seit Java 11?
- ✓ Was ändert sich mit Java 17?
- ✓ Wie können Sie von Records, Pattern Matching und Switch Expressions profitieren?
- ✓ Was sind die relevanten API-Änderungen?
- ✓ Was macht ein LTS-Release genau aus?
- ✓ Warum jetzt wechseln?
- ✓ Was gilt es bei der Migration zu beachten?

heise Developer



dpunkt.verlag

[java.bettercode.eu](http://java.bettercode.eu)

© Copyright by Heise Medien.

Die tippen“, er streckte beide Hände vor sich aus und bewegte alle zehn Finger rasend schnell wie ein Klaviervirtuose, „und – zack! – erscheint auf dem Bildschirm: „Wir haben alle deine Daten, ha ha! Und geben sie dir erst zurück, wenn du uns ein bisschen Geld schickst.“

„Ein bisschen Geld?“, echte ich.

„Englisch“, erklärte mir Sepp, der Safeknacker, weise. „Heißt ‚Bisschen-Münzen‘.“ Kalle nickte.

Ich musterte ihn von der Seite her. „Denkst du ans Wechseln? Hauptberuflich Briefe schreiben so wie früher?“

Er seufzte wieder. „Manchmal juckt es mich schon in den Fingern“, gab er zu und senkte die Stimme, bevor er uns beschämte gestand: „Dann setze ich mich zu Hause hin, ganz professionell mit Gummihandschuhen, schneide Buchstaben aus der Fernsehzeitschrift und klebe sie auf ein schönes weißes Blatt Papier. „ALARM! RATTENGIFT IM BABYBREI!“, zitierte er. „EINE – MILLION – IN – BAR – ODER – TOTE – BABYS.“ Er strich sich über die schüttler werdenden Haare und sah plötzlich alt aus. Dabei waren wir derselbe Jahrgang, oder?

## „WENN SIE DARAUF NOCH MAL REAGIERT, HAST DU SIE AN DER ANGEL.“

„Ich schicke das natürlich nicht mehr ab“, beeilte Kalle sich zu versichern. „Da drüben“, er wedelte in Richtung der Data-Governance-Frauen, „steht die Zukunft. Keine Auslagen mehr für Zeitungen, Klebstoff und Papier, kein Problem mit Fingerabdrücken und vor allem keine Geldübergaben zwischen stinkenden Mülltonnen. Keine Angst, dabei fotografiert zu werden. Und nicht die ewige Frage nach dem richtigen Outfit: Hut oder kein Hut? Trenchcoat und Schal auch im Sommer? Einfach nur vor dem Bildschirm sitzen und reich werden“, schloss er schwärmerisch.

Sepp nickte begeistert. „I war zuletzt Türsteher in so einer Mafia-Bude“, erzählte er uns. „Aber des da is besser. Weniger Besoffene und man kriegt keine aufn Deckel.“

„Und die Sozialleistungen!“ Kalle wischte sich rasch ein Tränchen aus dem Auge. „Gratisgetränke, zu jedem Geburtstag gibt's für alle Döner, und Weihnachten und Jubiläen lässt sich die Firma auch was kosten.“

„Zum Fünfjährigen gibts Handschellen mit echten Diamanten“, wusste Sepp.

„Und wer bezahlt das alles?“

„Na, die Kunden!“ Kalle grinste mich an.

Ich schüttelte den Kopf. „Ich meine, wem gehört die Firma?“

„Namen sind Schall und Rauch. Der CEO ist ein junges Genie ...“ Kalle wurde unterbrochen, als sein Handy kurz vibrierte. Er überflog die Nachricht und riss triumphierend die Faust hoch. „Ja! Anke-Einsames-Herz hat angebissen! Ich wusste, sie ist scharf auf mich.“

„Zeig moi.“ Sepp lehnte sich näher. Ankes Profilbild, sahen wir, war ein Chihuahua in einem bunt gemusterten

Mäntelchen. Kalles zeigte einen Schäferhund. „Sie glaubt, wir sind Seelenverwandte.“

\* \* \*

Der geheimnisvolle CEO war erst mal vergessen, bis ich ihn ein paar Tage später dann selbst zu sehen kriegte. Wir saßen gerade auf der Couch und ich bat Sabine-Gibt-Es-Noch-Traummänner um eine dringende Geldüberweisung für meine lebensrettende OP, als jemand lässig ins Büro schlenderte. Ich erhaschte bloß einen Blick auf blonde Haare und eine Brille, bevor sich die Media-Marketing-Crew um ihn drängte.

„Chef!“, hörte ich eine nervöse junge Frau rufen. „Ich weiß nicht, was ich tun soll!“

Ohne groß nachzudenken stand ich auf und ging nach vorn, um besser zu sehen. Kalle folgte mir. Die nervöse Frau reichte dem blonden Mann ihren Laptop, er stellte ihn auf die Bartheke und fing mit rasender Geschwindigkeit an zu tippen.

„Gucken wir mal“, murmelte er vor sich hin. Erwartungsvolle Stille senkte sich über das Büro. Alle hingen an seinen Lippen. „Linda G., 35, führt über ihre Tage mit einer Menstruations-App Buch. Diese ist mit ihren Social-Media-Profilen synchronisiert, was sie nicht weiß. Seit zwei Wochen erhält sie verstärkt personalisierte Werbung für Windeln und Babybrei.“ Kalle neben mir riss bei diesem Stichwort den Kopf hoch.

„Soll heißen, sie ist schwanger“, fuhr unser CEO fort und schenkte den Versammelten ein dünnes Lächeln. „Und jetzt ... ihr Verlobter ...“, er tippte etwas ein und kräuselte die Stirn. „Nein, ihr Ehemann – ts, ts, Linda, warum hast du deinen Beziehungsstatus nicht gleich upgedatet? Sehr nachlässig von dir! – war zum Empfängniszeitpunkt in Hamburg, was durch den GPS-Status seines Handys bestätigt wird. Linda wohnt aber in München.“

Er tippte weiter und murmelte dabei: „... Baby nicht von ihm ... habe Beweise ... wenn du nicht willst, dass dein Mann ... für den kleinen Preis von 5 Coins kann dieses Problem schnell verschwinden ...“, betätigte dann eine abschließende Taste und sah auf. Sein Gesichtsausdruck war triumphierend.

Die gesamte Media-Marketing-Crew, Männer wie Frauen, starrte ihn schwärmerisch-verzückt an. Auch ich war zutiefst beeindruckt. Zwar hatte ich nur jedes zweite Wort kapiert, trotzdem kam ich mir dämlich vor. All die Nächte, während derer ich mir in dem Hauseingang gegenüber dem Parkplatz der Herzblatt-Bar die Beine in den Bauch gestanden hatte, um Fremdgänger beim Seitensprung zu fotografieren ... Allein die Kamera hatte damals wie viel gekostet? Dazu das Ausarbeiten der Bilder und dann noch jedes Mal die Gebühr, damit mir mein Kumpel bei der Zulassungsstelle zu den Autokennzeichen die Namen besorgt hatte ...

Und unser Chef erledigte die gleiche Arbeit ganz lässig mit ein paar Klicks.

„Chef, das war klasse!“, hauchte eine Frau. „Könnten Sie uns noch ein Beispiel geben?“

Das blonde Büschchen wedelte abfällig mit einer Hand. Genau wie es Lydia getan hatte, wenn ich sie zu überzeugen versucht hatte, ein Date mit Bockwurst beim Imbiss wäre doch fast genauso nett wie eines mit Krebs-oder-wie-die-

Pfannkuchen-beim-Franzosen-hießen. „Nicht so hastig. Wir sind mit Linda noch nicht fertig. – Daten, Leute“, wandte er sich an alle, „sind das neue Gold. Erpressung ist ein netter Zuverdienst, aber es gibt jede Menge weitere Möglichkeiten abzuzuschalten. Einige davon sind sogar legal.“ Er machte eine kunstvolle Pause, bevor er weitersprach: „Linda G. ist schwanger und weiß es selbst noch nicht. Wen könnte diese Info interessieren?“

## „CHEF!“, HÖRTE ICH EINE NERVÖSE JUNGE FRAU RUFEN. „ICH WEISS NICHT, WAS ICH TUN SOLL!“

„Den Kindesvater?“, rutschte mir heraus. Ich hatte wohl lauter gesprochen als gedacht, denn alle guckten zu mir rüber. Beschämmt sah ich zu Boden und ich musste plötzlich an das Foto denken, das mein alter Zellenkollege an der Wand gehabt hatte. Es hatte ihn selbst gezeigt, mit einem Arm um einen blonden, ungefähr sechsjährigen Jungen. Oft, wenn ich nachts nicht schlafen konnte, hatte ich mir das Bild angeguckt und mir vorgestellt, das wäre meine Familie. Wenn sie nicht kurz vor der Geburt des Babys endgültig abgehauen wäre, hätte sie die Kamera halten können, während ich und Klein-Xav...

„Netter Versuch, aber viel zu oldschool“, wischte der Blonde meinen Einwurf zur Seite. „Denk größer.“ Wieder wandte er sich an alle: „Denkt an zahlungskräftige Konzerne. Banken. Versicherungen. Lindas Arbeitgeber. Und natürlich die gesamte Marketingindustrie. Das größte Gesundheitsrisiko für werdende Mütter ist heutzutage, von der Flut an Prospekten erschlagen zu werden.“ Die gesamte Media-Marketing-Crew machte sich eifrig Notizen.

Später, als die Übrigen zu ihren Arbeitsplätzen zurückgekehrt waren, kam unser CEO auf uns zu. Kalle neben mir stand plötzlich so kerzengerade und aufrecht wie bei der Bundeswehr. Das Einzige, was durch die jähre Stille drang, war Nils' überlautes Schluchzen aus einem der Telefonterrarien.

Dann stand er vor uns. Unser Chef. Ein strohblondes Bürschchen, das Jeans und ein schwarzes Polohemd trug und noch nicht mal alt genug aussah, um unters Erwachsenenstrafrecht zu fallen.

„Aha, der neue Mitarbeiter“, begrüßte er mich. Seine grünen Augen hinter der Brille fixierten mich wie eine Stecknadel einen Schmetterling im Album.

Erst Kalles Ellbogenstoß riss mich aus der Starre. „P-paule. Sehr ... sehr erfreut“, stammelte ich. „Abgefahrene Laden, den du hier hast. Den Sie hier haben“, verbesserte ich mich hastig.

„Findest du?“ Er lächelte spöttisch. „Freut mich, dass es dir gefällt. Ich sehe schon, du bist ein echter Experte für Cybercrime.“ Bevor mir darauf etwas zu sagen einfiel, redete er weiter. „Wir bauen nächste Woche noch mal aus, eine neue Abteilung kommt dazu. Phishing. Mal davon gehört?“

„Äh, ja. Man geht mit der Angel zum Fluss, tut einen Wurm dran und ...“

„Alter!“, entfuhr ihm. Sichtlich frustriert gaffte er mich an, als könnte er nicht glauben, dass jemand so dumm sein konnte. „Phi-shing, nicht Fischen“, erklärte er mir langsam und überdeutlich. „Das heißt, man bringt die Leute mit gefälschten Nachrichten dazu, einem Infos zu geben. Und damit klaut man ihnen das Geld von den Bankkonten.“

Kalle, der seine berufliche Karriere als Taschendieb begonnen hatte, lehnte sich vor. „So wie Portemonnaies ziehen?“

„Ja, fast genau so.“ Der Blonde rollte die Augen. „Bloß sind auf den Konten Tausende Euros und das Portemonnaie enthält bestenfalls einen Fünfziger.“ Er warf einen langen, abschätzigen Blick auf mich, als versuchte er den Inhalt meines Portemonnaies zu erraten. „Oder auch bloß einen Zwanziger oder einen Zehner?“

Beschämmt senkte ich den Kopf.

„Oder totale Ebbe bis auf, sagen wir mal, Omas Glücks pfennig?“, ätzte er weiter. „Und ...“ Unwillkürlich sah ich auf. Seine grünen Augen hinter der Brille belauerten mich plötzlich, als wäre er ein hungriger Wolf und ich ein Hase. „... ein Foto. Von einer Frau. Mit langen schwarzen Haaren und einem dicken Bauch.“

Ich erstarrte. Woher wusste er ...?

Diese Augen. Ich kannte diese Augen.

Lydias Augen.

## „NETTER VERSUCH, ABER VIEL ZU OLDSCHOOL. DENK GRÖSSER.“

Der CEO schenkte mir sein dünnes Lächeln. „Ja, ich weiß eine Menge über dich. Soll ich auch gleich raten, wie dein Passwort für die Mitgliedschaft bei ‚Knacki heute‘ lautet, Paps?“

„Xaver“, flüsterte ich tonlos. „Xaver Paulsen.“ Und mit dieser Erkenntnis machten sich unbändiger Stolz und Erleichterung in mir breit. Verkorkstes Leben hin oder her: Das Einzige, was ich je wirklich bereut hatte, war, dass ich meinem Jungen keine Zukunft schenken können. Aber als ich nun in die kühlen Augen des CEO blickte, zweifelte ich nicht mehr daran: Mein und Lydias Klein-Xaver hatte es auch ohne seinen Paps zu was gebracht. (psz@ct.de) ct

### Die c't-Stories als Hörversion

Unter [heise.de/-4491527](http://heise.de/-4491527) können Sie einige c't-Stories als Audiofassung kostenlos herunterladen oder streamen. Die c't-Stories zum Zuhören gibt es auch als RSS-Feed und auf den bekannten Plattformen wie Spotify, Player FM und Apple podcasts ([ct.de/yz13](http://ct.de/yz13)).

# GOVERLAN REACH



## Remote IT Support

### Goverlan Reach

- verwaltet neben PCs Tablets und Smartphones ebenfalls Geldautomaten, Kassenterminals und Digitale Anzeigen
- Heilt DSS Ausfälle ohne den System Desktop nach außen zu zeigen
- Administratoren können mehrere visuelle Prüfungen und Jobs gleichzeitig durchführen. Es können Funktionsgruppen definiert werden, auf denen gleichzeitig Änderungen laufen.

Client Verbindungen können aufgebaut werden mit dem Goverlan Reach Protokoll oder mit: RDP, VNC, AMT, Telnet oder SSH.

Voller Support für VDI, RDP & Citrix Sitzungen unterstützte Betriebssysteme: Windows, MAC und Linux dazu IoT (Internet of Things).

#### Die 3 Versionen von Goverlan Reach

- ✓ **Standard**  
Umfangreicher Remote Control Support
- ✓ **Professional**  
zusätzlich Active Directory Integration
- ✓ **Enterprise**  
zusätzlich Prozess Automation, IT Compliance Integration mit dem Incident Management von: JIRA Service Desk, ManageEngine Service Desk, Solarwinds

#### Alle Preise pro Administrator/Techniker

- Es zählen nur die aktiven Nutzer
- Keine Bindung an Namen
- Keine Node Begrenzung
- Die Lizenzen laufen jeweils 1 Jahr

Weitere sehr ausführliche Infos in englisch und eine 30 Tage Testversion gibt es unter:  
<https://www.goverlan.com/tools/remote-control>

SienerSoft GmbH  
Schoßbergstraße 11  
65201 Wiesbaden  
Telefon 0611-89077621  
infos@sienersoft.de

Viele weitere Software finden Sie bei uns unter:  
[www.sienersoft.de](http://www.sienersoft.de)

Angebote anfordern bei → [order@sienersoft.de](mailto:order@sienersoft.de)

**SienerSoft**

**NEU**

# iX Special Quantencomputer



Auch als PDF  
sofort zum  
Download!



### iX Special Quantencomputer

Wie funktionieren Quantencomputer und wie ist der Stand der Technik? Für welche Anwendungen eignen sie sich und wie lassen sie sich programmieren? Diese und noch mehr Fragen beantwortet Ihnen das iX Special 2021 Quantencomputer.

[shop.heise.de/ix-quantencomputer](http://shop.heise.de/ix-quantencomputer)

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



**heise shop**

[shop.heise.de/ix-quantencomputer](http://shop.heise.de/ix-quantencomputer)

# Ihre Windows-Werkzeugbox

## c't Windows 2021

Dieses c't-Sonderheft enthält wie immer das Beste zum Thema Windows. Die c't-Redaktion gibt Ihnen Werkzeuge an die Hand, um Ihren Alltag mit Windows zu erleichtern und bei der Konfiguration und Fehler suche zu helfen. Außerdem bietet das Heft Hilfestellungen für einen verlässlichen Betrieb und das neueste c't-Notfall-Windows.

Auch als einzelnes Heft erhältlich.

[shop.heise.de/ct-windows21](http://shop.heise.de/ct-windows21)

Heft + PDF  
für nur

19,90 € >

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



### Tools für den Alltag

100 Gratis-Programme von Microsoft PowerToys, Konsolen-Tipps, Sysinternals Wissenswertes zum Windows-Kauf

### Wenn Windows streikt

Windows-Probleme lösen per Mausklick Robuste System-Backups mit c't-WIMage Kaputte Updates rückgängig machen

### Know-how für Profis

Windows-Installationen für Testzwecke Eingabeaufforderung effizienter nutzen Welches Dateisystem wofür?

### Das c't-Notfall-Windows

Das Rettungssystem zum Selbst-Schädlingsuche - Datenrettung

Heft + PDF  
mit 29%  
Rabatt



[shop.heise.de/ct-windows21](http://shop.heise.de/ct-windows21)



27" / 68,58 cm  
16:9

LC-POWER™  
[www.lc-power.com](http://www.lc-power.com)

4K  
ULTRA HD

27"

HDR ready

144Hz

90°

Pivot-Funktion

Sehe ULTRA scharf dank LC-Power!

LC-M27-4K-UHD-144





## Redakteur (m/w/d) heise online mit dem Schwerpunkt Fintech



### Redakteur (m/w/d) heise online mit dem Schwerpunkt Fintech, zunächst befristet für 2 Jahre

Du kennst den Unterschied zwischen Bitcoin und Ethereum, die Vor- und Nachteile wichtiger Apps zum Aktien-Trading und weißt, welche Themen die internationale Finanzbranche bewegen? Dann suchen wir Dich für heise online, dem Leitmedium für deutschsprachige Hightech-Nachrichten!

#### Deine Aufgaben

- Du recherchierst und schreibst Analysen, Ratgeber sowie Tests zu aktuellen Entwicklungen rund um Finanztechnologie – von Online-Banking über Mobile Payment bis hin zu Kryptowährungen und Trading.
- Zusammen mit dem Redaktionsteam tauschst Du Dich zu den Themen aus und arbeitest auch mit externen Fintech-Experten zusammen.
- Dazu gehört auch das Redigieren von Manuskripten.

#### Deine Talente

- Du verfügst über einschlägige Berufserfahrung im Bereich Fintech und Banking.
- Ein technischer Studienabschluss ist wünschenswert, aber kein Muss.
- Du kannst IT-Finanzthemen verständlich erklären und journalistisch auf den Punkt bringen.
- Verständnis für technische Zusammenhänge sowie ein ausgeprägtes Interesse an Fintech zeichnen Dich aus.
- Kommunikationsstärke, eine organisierte Arbeitsweise sowie Neugier und Spaß daran, sich stetig in neue Themen einzuarbeiten, bringst Du außerdem mit.
- Englisch beherrschst Du sicher in Wort und Schrift.

#### Deine Benefits

- Flache Hierarchien und eine familiäre Arbeitsatmosphäre zeichnen das Arbeiten bei uns aus.
- Du erhältst einen kostenlosen Zugang zu unseren Heise-Produkten inklusive der heise Academy.
- Einen Platz in unserem engagierten und qualifizierten Team – die Entwicklung jedes Einzelnen ist uns dabei sehr wichtig.
- Flexible Arbeitszeiten, die Möglichkeit, mobil zu arbeiten, tolle Mitarbeiter-Events, eine Kantine, ein Mitarbeiter-Fitnessprogramm und vieles mehr.

Bitte bewirb Dich online:  
[www.heise-gruppe.de/karriere](http://www.heise-gruppe.de/karriere)

Bei uns ist jede Person, unabhängig des Geschlechts, der Nationalität oder der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters sowie der sexuellen Identität willkommen.

**Wir freuen uns auf Ihre Bewerbung!**

#### Dein Ansprechpartner

Dr. Volker Zota, Chefredakteur heise online  
Tel.: 0511 5352 608

Wir suchen

INSPIRIERENDE  
ZUKUNFTSGESTALTER

HOCHSCHULE  
ANSBACH



## Professur (W2)

für Simulation für Energieeffizienz und nachhaltige Produktionsprozesse

Start zum 01.03.2022 Kennziffer: 2021-33-NIW1

Nachhaltigkeit, Künstliche Intelligenz, Virtual Reality Technologie und mehr. An der jungen, bestens etablierten Hochschule Ansbach beschäftigen wir uns in Forschung und Lehre mit zukunftsweisenden Themen in den Bereichen Wirtschaft, Medien und Technik. Dabei stehen Studierende, Lehrende und Beschäftigte der Hochschule stets im Mittelpunkt. Mit 3.500 Studierenden in 31 Studiengängen bieten wir ein exzellentes Angebot als moderner Arbeitgeber.

Bitte bewerben Sie sich bis spätestens 06.09.2021 über unser Online-Portal.

Informationen unter  
[www.hs-ansbach.de/service/hochschule-als-arbeitgeber](http://www.hs-ansbach.de/service/hochschule-als-arbeitgeber)



Landeshauptstadt  
Düsseldorf



Wir stellen zum nächstmöglichen Zeitpunkt ein:  
mehrere Bachelor of Science Fachrichtung Informatik oder vergleichbarer Studienabschluss, mindestens abgeschlossene Berufsausbildung als Fachinformatiker\*in oder gleichwertige Berufsausbildung mit Berufserfahrung (EG 10 TVöD) - Kennziffer 37/03/03/21/270

für das Amt 37 - Feuerwehr, Rettungsdienst und Bevölkerungsschutz in der Abteilung Technik

Alle Einstellungen erfolgen im Arbeitsverhältnis zu den Bedingungen des Tarifvertrages für den öffentlichen Dienst (TVöD).

Beschäftigungsdauer, Aufgaben, Anforderungsprofile, Bewerbungsfristen und Ansprechpartner\*innen entnehmenn Sie bitte unserer Homepage [www.duesseldorf.de/stellen](http://www.duesseldorf.de/stellen).

# Inserenten\*

1blu AG, Berlin .....	23	<b>Stellenanzeigen</b>
B1 Systems GmbH, Vohburg .....	196	Heise Gruppe GmbH & Co. KG, Hannover .....
bluechip Computer AG, Meuselwitz .....	2	Hochschule für angewandte Wissenschaften, Ansbach .....
Cisco Systems GmbH, Garching b. München .....	31	Landeshauptstadt Düsseldorf, Düsseldorf .....
CRONON GmbH, Berlin .....	11	
EXTRA Computer GmbH, Giengen-Sachsenhausen .....	27	<b>Veranstaltungen</b>
KabelScheune.de, Burgbernheim .....	53	heise Academy .....
PricewaterhouseCoopers GmbH, Düsseldorf .....	59	secIT Specials .....
secunet Security Networks AG, Essen .....	61	betterCode WebAssembly .....
Siemens AG, Nürnberg .....	9	heise Academy Videokurse .....
SienerSoft AG, Wiesbaden .....	188	Internet Security Days .....
Silent Power Electronics GmbH, Willich .....	189	enterJS .....
Thomas Krenn.com, Freyung .....	39	heise Security Tour .....
WORTMANN AG, Hüllhorst .....	4, 5	Cluster Security .....
		DevOps .....
		Herbstcampus .....
		heise jobs .....
		betterCode .....

heise Academy .....	63
heise Events .....	65
heise developer, dpunkt.verlag .....	69
heise Academy .....	85
eco Verband, heise Events .....	95
iX, heise developer, dpunkt.verlag .....	109
heise Events .....	115
heise Academy .....	141
heise Academy .....	153
iX, heise developer, dpunkt.verlag .....	165
heise jobs .....	177
iX, heise developer, dpunkt.verlag .....	185

## Veranstaltungen

heise Academy .....	63
secIT Specials .....	65
betterCode WebAssembly .....	69
heise Academy Videokurse .....	85
Internet Security Days .....	95
enterJS .....	109
heise Security Tour .....	115
Cluster Security .....	141
DevOps .....	153
Herbstcampus .....	165
heise jobs .....	177
betterCode .....	185

Teile dieser Ausgabe enthalten Beilagen der DIMABAY GmbH, Berlin und EXTRA Computer GmbH, Giengen-Sachsenhausen.

\* Die hier abgedruckten Seitenzahlen sind nicht verbindlich.  
Redaktionelle Gründe können Änderungen erforderlich machen.

## IMMER AUF AUGENHÖHE

2x Mac & i mit 35 % Rabatt  
testen und Geschenk sichern!

### Mac & i – Das Magazin rund um Apple

- Tipps & Workshops
- Apps und Zubehör
- Hard- & Softwaretipps
- inkl. Club-Mitgliedschaft

Für nur 14,40 € statt 21,80 €

NEU: Mit Mac & i Club-Mitgliedschaft  
exklusive Vorteile genießen



Jetzt bestellen:

[www.mac-and-i.de/minabo](http://www.mac-and-i.de/minabo)

✉ leserservice@heise.de



0541 80 009 120

Mac & i. Das Apple-Magazin von c't.

# 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, E-Mail: ct@ct.de

**Titelthemenkoordination in dieser Ausgabe:** „Upcycling mit dem Raspi“:  
Peter Siering ([ps@ct.de](mailto:ps@ct.de)), „Homeoffice überall“: Christian Wölbert ([cwo@ct.de](mailto:cwo@ct.de))  
**Chefredakteur:** Dr. Jürgen Rink ([jr@ct.de](mailto:jr@ct.de)) (verantwortlich für den Textteil)  
**Stellv. Chefredakteur:** Axel Kossel ([ad@ct.de](mailto:ad@ct.de))  
**Chef vom Dienst:** Georg Schnurer ([gs@ct.de](mailto:gs@ct.de))

### Leser & Qualität

**Leitung:** Achim Barczok ([acb@ct.de](mailto:acb@ct.de))

**Textredaktion & Qualitätssicherung:** Oliver Lau ([ola@ct.de](mailto:ola@ct.de))

**Koordination Leserkommunikation:** Martin Triadan ([mat@ct.de](mailto:mat@ct.de))

**Ressort Internet, Datenschutz & Anwendungen**

**Leitende Redakteure:** Hartmut Gieselmann ([hag@ct.de](mailto:hag@ct.de)), Jo Bager ([jo@ct.de](mailto:jo@ct.de))

**Redaktion:** Holger Bleich ([hob@ct.de](mailto:hob@ct.de)), Anke Brandt ([abr@ct.de](mailto:abr@ct.de)), Arne Grävemeyer ([agr@ct.de](mailto:agr@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)), Jan Mahn ([jam@ct.de](mailto:jam@ct.de))

**Redaktion:** Niklas Dierking ([ndi@ct.de](mailto:ndi@ct.de)), Mirko Dölle ([mid@ct.de](mailto:mid@ct.de)),

Wilhelm Drehling ([wid@ct.de](mailto:wid@ct.de)), Liane M. Dubowy ([ldm@ct.de](mailto:ldm@ct.de)), Ronald Eikenberg ([rei@ct.de](mailto:rei@ct.de)), Alexander Königstein ([ako@ct.de](mailto:ako@ct.de)), Pina Merken ([pmk@ct.de](mailto:pmk@ct.de)), Dennis Schirrmacher ([des@ct.de](mailto:des@ct.de)), Hajo Schulz ([hos@ct.de](mailto:hos@ct.de)), Jan Schüßler ([jss@ct.de](mailto:jss@ct.de)), Ingo T. Storm ([it@ct.de](mailto:it@ct.de)), Keywan Tonekaboni ([ktn@ct.de](mailto:ktn@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)), André Kramer ([akr@ct.de](mailto:akr@ct.de)), Michael Link ([ml@ct.de](mailto:ml@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\\_uk@ct.de](mailto:ltg_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))

**Redaktionsassistent:** Susanne Cölle ([suc@ct.de](mailto:suc@ct.de)), Christopher Tränkmann ([cht@ct.de](mailto:cht@ct.de))

**Software-Entwicklung:** Kai Wasserbäch ([kaw@ct.de](mailto:kaw@ct.de))

**Technische Assistenz:** Ralf Schneider ([ltg\\_rs@ct.de](mailto:ltg_rs@ct.de)), Hans-Jürgen Berndt ([hjb@ct.de](mailto:hjb@ct.de)), Denis Fröhlich ([dfr@ct.de](mailto:dfr@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 ([jnoh@ct.de](mailto:jnoh@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)), Jürgen Gonnermann, Birgit Graff, Angela Hilberg, Martin Kreft, 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, Kevin Harte, Martin Kreft, Pascal Wissner

**Illustrationen:**

Jan Bintakies, Hannover, Rudolf A. Blaha, Frankfurt am Main, Thorsten Hübner, Berlin, Albert Hulm, Berlin, Sven Hauth, Schülp, Thomas Kuhlenbeck, Münster, Andreas Martini, Wettn, Henning Rathjen, Oberursel

**Editorial:** Hans-Jürgen „Mash“ Marhenke, Hannover, **Schlagseite:** Ritsch & Renn, Wien, **c't-Logo:** Gerold Kalter, Rheine

**c't-Krypto-Kampagne:** Infos zur Krypto-Kampagne unter <https://ct.de/pgp>. Die Authentizität unserer Zertifizierungsschlüssel lässt sich mit den nachstehenden Fingerprints überprüfen:

Key-ID: 5C1C1DC5BEEDD33A

ct magazine CERTIFICATE <[pgpCA@heise.de](mailto:pgpCA@heise.de)>

D337 FCC6 7EB9 09EA D1FC 8065 5C1C 1DC5 BEED D33A

Key-ID: 2BAE3CF6DAFFB000

ct magazine CERTIFICATE <[pgpCA@ct.heise.de](mailto:pgpCA@ct.heise.de)>

A3B5 24C2 01A0 D0F2 355E 5D1F 2BAE 3CF6 DAFF B000

Key-ID: DBD245FCB3B2A12C

ct magazine CERTIFICATE <[pgpCA@ct.heise.de](mailto:pgpCA@ct.heise.de)>

19ED 6E14 58EB A451 C5E8 0871 DBD2 45FC B3B2 A12C

**heise Investigativ:** Über diesen sicheren Briefkasten können Sie uns anonym informieren.

Anonymer Briefkasten: <https://heise.de/investigativ>

via Tor: [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. 38 vom 1. Januar 2021.

**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: POFICHBX, 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 5,50 €; Österreich 6,10 €; Schweiz 8.10 CHF; Dänemark 60,00 DKK;  
Belgien, Luxemburg, Niederlande 6,50 €; Italien, Spanien 6,90 €

**Abonnement-Preise:** Das Jahresabonnement kostet inkl. Versandkosten: Inland 130,95 €, Österreich 140,40 €, Europa 149,85 €, restl. Ausland 176,85 € (Schweiz 186,30 CHF); ermäßiges Abonnement für Schüler, Studenten, Auszubildende (nur gegen Vorlage einer entsprechenden Bescheinigung): Inland 94,50 €, Österreich 95,85 €, Europa 113,40 €, restl. Ausland 140,40 € (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. Ermäßiges 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 98,55 €, Österreich 98,55 €, Europa 117,45 €, restl. Ausland 144,45 € (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 Verfügungsberecht 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 2021 by Heise Medien GmbH & Co. KG

ISSN 0724-8679 AWA ACTA 

# Vorschau 18/2021

Ab 14. August im Handel und auf ct.de



## Gaming-Notebooks, Grafikkarten & Gamescom

Die digitale Spielemesse Gamescom wartet im August mit vielen Highlights auf. Große Namen sind ebenso vertreten wie zahlreiche Indie-Studios. Wir blicken im Vorfeld auf die Trends der Spielewelt, testen Gaming-Notebooks und beraten beim Kauf von Grafikkarten, Gaming-Tastaturen und vielem mehr.



## Schicke E-Bikes

Obwohl Pedelecs immer leistungsfähiger werden, bleiben die Preise stabil oder sinken sogar. Obendrein wächst das Angebot und die Räder sind zusehends schlanker, leichter und schicker. Mit dem richtigen Wissen über E-Bike-Technik findet jeder das passende Rad.

## Mehr Speed mit PCIe-SSDs

Schnelle PCIe-SSDs haben sich dank gutem Preis/Leistungsverhältnis als Standard-Massenspeicher etabliert. Wann reicht eine günstige mit PCIe 3.0, wann muss es ein Topmodell mit dem neueren und doppelt so schnellen PCIe 4.0 sein? Sechs aktuelle Geräte im Test.

## Was Sie über VPN wissen müssen

Auch abseits mobilem Arbeiten und professioneller Vernetzung haben Zugänge per Virtual Private Network ihren Nutzen: Sie schützen Surfer in offenen WLANs und verbergen den Aufenthaltsort ihrer Nutzer. Mancher Anbieter verspricht obendrein Anonymität beim Surfen – wie sehr kann man sich darauf verlassen?

## Clever lernen mit Karteikarten-Apps

Ob Vokabeln, Daten oder Formeln – Karteikarten-Apps taugen als nützliche Lernhilfen für beinahe jedes Fach und Thema. Wir zeigen, wie Sie die digitalen Kärtchen optimal einsetzen und vergleichen den Funktionsumfang der Anwendungen.

Noch mehr  
Heise-Know-how

The booklet cover for 'c't FRITZBOX' features the 'c't' logo and the word 'FRITZBOX' in large red letters. Below it says 'Absichern • Erweitern • Tunen'. It includes several small icons representing different functions like security, networking, and tuning. The price '€ 14,90' is at the bottom right.

c't Fritzbox 2021  
jetzt im Handel und  
auf heise-shop.de

The magazine cover for 'iX 8/2021' features a green and yellow design with the number '8' and the date 'August 2021'. It has several headlines: 'KI-Hilfen für IDEs • Software schreibt Code • Effiziente Unit-Tests', 'Besserer Code mit KI', 'Homeserver und funktionale Verschlüsselung', 'Verteilt genutzte Daten schützen', 'Digitale B2B-Marktplätze', 'Texte analysieren mit Python', 'DB2 defragmentieren', 'Autoscan-Shadsoftware finden', and 'Angriffe auf Windows erkennen'. It also features a large image of a laptop screen displaying code.

iX 8/2021 jetzt im Handel  
und auf heise-shop.de

The booklet cover for 'c't Make: MICROPYTHON SPECIAL' features the 'c't' logo and the word 'MICROPYTHON' in large red letters. It has sections for 'Grundlagen' (with sub-points like 'Python – verständlich erklärt', 'Installation & Editorien', etc.), 'Einstieg' (with sub-points like 'Wichtige Sprachelemente', 'Objekte, Listen, Fehlerbehandlung', etc.), and 'Projekte' (with sub-points like 'CO₂-Ampel bauen', 'Display ansteuern', etc.). It includes an image of a microcontroller board. The price '€ 14,90' is at the bottom right.

Make Special: Micro-  
python jetzt im Handel  
und auf heise-shop.de

# **NUR WER SEINE INFORMATIONS- QUELLEN WÄHLEN KANN, KANN WIRKLICH WÄHLEN.**



**Zeitschriftenverleger  
gemeinsam für Pressefreiheit**

VDZ

Verband Deutscher  
Zeitschriftenverleger



## B1 Consulting Managed Service & Support

individuell – umfassend – kundenorientiert

Neue oder bestehende Systemlandschaften stellen hohe Anforderungen an Ihr IT-Personal. Mit einem individuellen Support- und Betriebsvertrag von B1 Systems ergänzen Sie Ihr Team um die Erfahrung und das Wissen unserer über 140 festangestellten Linux- und Open-Source-Experten.

Unsere Kernthemen:

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

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



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

ROCKOLDING · KÖLN · BERLIN · DRESDEN

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

© Copyright by Heise Medien.