



Edel-Smartphones im Test

Wi-Fi 7, superhelle Displays, 1-Zoll-Kamerasensoren, KI-Helfer

TEST

Transkriptions-Apps und -Dienste
Linux: Gnome 46 mit verbesserter Suche
27-Zoll-Monitore mit 4K und USB-C-Eingang
Einhandcontroller für ambitionierte Spieler
Plasticity: Einfaches CAD für 3D-Drucke

Fremdsprachen lernen mit KI

Sprechtrainer im Test • ChatGPT aufrüsten

FOKUS

Browser schlampen bei verschlüsseltem DNS
Im Detail: Windows 11 Version 24H2
Linux: Secure Boot und Nachfolger erklärt
Papierarmes Büro mit paperless-ngx
Alte Macs mit jungem macOS aufbrezeln



Proxmox: Server für virtuelle Maschinen

Kostenlos, einfach, Open Source

Praxis: Starten mit der VMware-Alternative

€ 5,90
AT € 6,50 | LUX, BEL € 6,90
NL € 7,20 | IT, ES € 7,40
CHF 9.90 | DKK 64,00

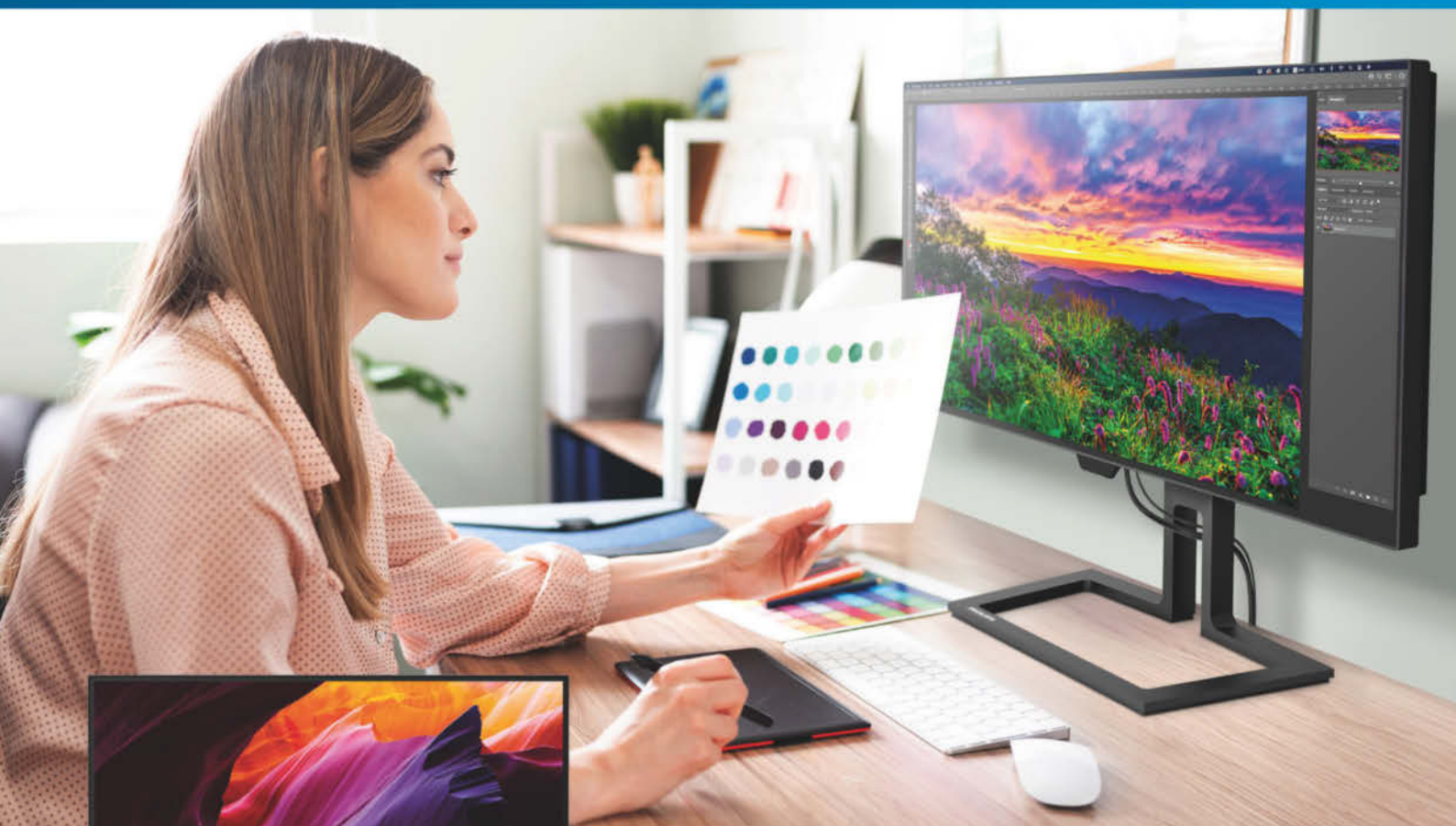


PHILIPS

Monitore

Simply brilliant

Mini-LED mit Thunderbolt 4 & Docking



Brilliance 7000

27" (68,6 cm) | Mini-LED | Thunderbolt 4 | 4K UHD

27B1U7903/00



THUNDERBOLT



MINI LED
Local Dimming

4K

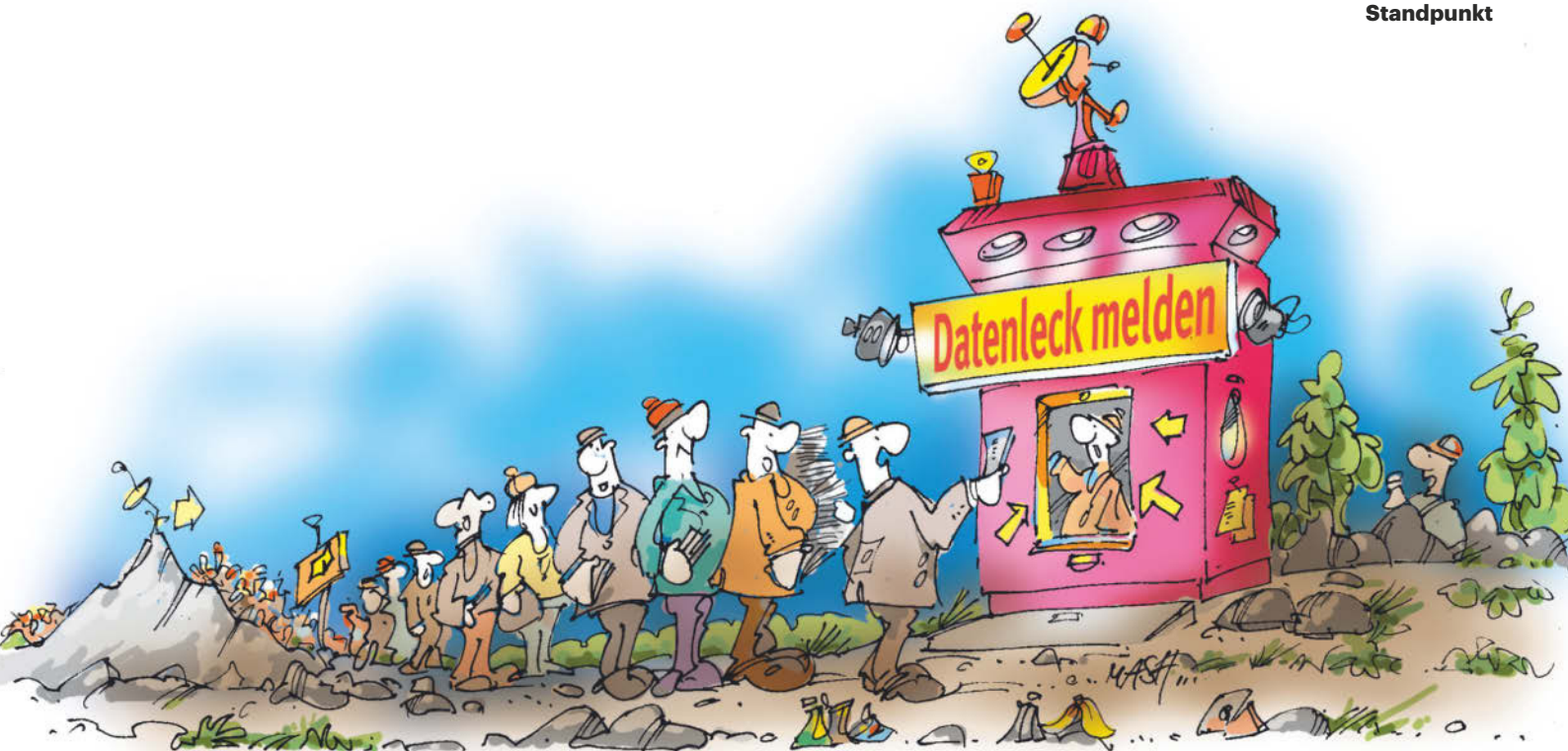
Ultra HD



VESA CERTIFIED
DisplayHDR 1400



innovation  you



Mehr Datenschutz-Skalierung!

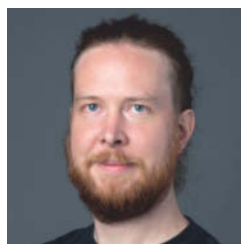
Vor der EU-Datenschutz-Grundverordnung DSGVO sind alle (fast) gleich: Es ist egal, ob ein multinationaler Klinikkonzern oder die kleine Naturheilkunde-Praxis medizinische Daten im Internet leakt.

Riesige Konzerne verfügen mit Heerscharen an Security-Experten und Datenschutzanwälten aber über viel mehr Kompetenz und Ressourcen als IT-ferne Kleinunternehmen. Das sind Unterschiede, denen die DSGVO nicht ausreichend Rechnung trägt, wie man aktuell am Fall von Stay Informed (siehe Seite 32) sehen kann: Dieses Unternehmen verwaltet mit seiner App personenbezogene Daten für mehrere Tausend Kitas, Schulen, Pflegeheime und dergleichen. Formal fungiert es als Auftragsverarbeiter, sodass primär eben die Einrichtungen – beziehungsweise deren Träger – für den Datenschutz in der Stay-Informed-App verantwortlich sind.

Man darf bezweifeln, dass sich all diese Einrichtungen ihrer Verantwortung beim Unterzeichnen des Verarbeitungsvertrags bewusst waren. Stay Informed warb sogar mit Aussagen von glücklichen Kunden, die annahmen, sich nun gar nicht mehr um dieses "heikle Thema" kümmern zu müssen. Selbst schuld, könnte man sagen: Eine Kita kann sich nun mal genauso wenig aus der Verantwortung für den Datenschutz stellen, wie sich ein Restaurant der Verpflichtung zur Nahrungsmittelhygiene entziehen kann.

Das erkennt aber die praktischen Gegebenheiten: Viele, gerade kleinere Einrichtungen haben nicht die Expertise, um Datenschutzrisiken einzuschätzen. Und selbst mit ausreichendem Fachwissen steht und fällt eine Einschätzung damit, ob und wie schnell der Auftragsverarbeiter alle relevanten Informationen zur Verfügung stellt. Vollends absurd ist, dass nun alle betroffenen Kitas und Schulen ein und dasselbe Datenleck an ihre jeweilige Datenschutzaufsicht melden müssen.

Der DSGVO wird viel vorgeworfen, oft zu Unrecht. Aber alle über den gleichen Kamm zu scheren, ist tatsächlich kritikwürdig, egal wie einleuchtend es im Prinzip ist: Es dient dem Datenschutz nicht, wenn verantwortliche Stellen mit ihren Pflichten heillos überfordert sind und Aufsichtsbehörden mit Meldungen überschütten müssen. Der europäische Gesetzgeber sollte den Ansatz "one size fits all" bei der nächsten DSGVO-Evaluierung mindestens hinterfragen.



Sylvester Tremmel

Sylvester Tremmel

TERRA MOBILE 360-13U

TERRA MOBILE 360-13U

- Intel® Core™ i5-1235U Prozessor
(12M Cache, bis zu 4.40 GHz)
- Windows 11 Pro
- Displaygröße 33.8 cm (13.3")
- 1920 x 1080 Display-Auflösung
- Display-Typ IPS Touch-Display
- 16 GB Speicherkapazität
- 512 GB Gesamtspeicherkapazität
- Intel® Iris® XE Graphics

Artikel-Nr.: 1220785

829,-*

Preis zzgl. gesetzl. MwSt.



Schöpfen Sie Ihr Potenzial voll aus mit Windows 11 Pro Geräten

Um neue Wege zu beschreiten, brauchen Sie wegweisende Geräte. Mit Windows 11 Pro Geräten können Sie Workflows und die Zusammenarbeit mithilfe von Lösungen beschleunigen, die alle Mitglieder Ihres Teams zu Höchstleistungen befähigen. Windows 11 unterstützt ein umfangreiches Ökosystem von Apps, Peripheriegeräten und Geräten, sodass Sie für alle Mitarbeitenden

das passende Gerät finden. Dank der rasanten Leistung, der Unterstützung mehrerer 4K-Monitore sowie der Stift-, Freihand-, Toucheingabe- und Sprachfunktionen erzielen Sie bessere Arbeitsergebnisse.¹ Und dank der Akkulaufzeit für den ganzen Tag und der hochwertigen Kameras und Mikrofone können Ihre Teams überall in Verbindung bleiben.^{1,2}

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. 0441/9250095 • 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 • Kortenbreite 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 • Pauly Büromaschinen Vertriebs GmbH, **65555** Limburg, Tel. 06431/500466 • 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 • SCHUCK it GmbH • **78194** Immendingen • Tel. 07462/9474-18 • Resin GmbH & Co.KG, **79589** Binzen, Tel. 07261/6660 • Office Komplett, **79664** Wehr, Tel. 07762 / 708860 • bli computersysteme GmbH & Co. KG • **89077** Ulm, Tel. 0731/18488-0 • Schwarz Computer Systeme GmbH, **92318** Neumarkt, Tel. 09181/48550 • K&L electronics GmbH, **95466** Weidenberg, Tel. 09278/98610-0 •

WORTMANN AG empfiehlt Windows 11 Pro für Unternehmen.

360° klappbares Display



Stift optional erhältlich

 **Windows 11**

* Änderungen und Irrtümer vorbehalten. Preise in € inklusive gesetzlicher Mehrwertsteuer.
Es gelten die AGB der Wortmann AG, zu finden unter www.wortmann.de. Solange der Vorrat reicht. Keine Mitnahmegarantie.

¹ Hardwareabhängig

² Die Akkulaufzeit hängt stark von den Einstellungen, der Nutzung, dem Gerät und anderen Faktoren ab

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.

¹ Windows 11 Survey Report. Techaisle, Februar 2022. Ergebnisse für Windows 11 basieren auf einem Vergleich mit Geräten mit Windows 10.

www.wortmann.de

WORTMANN AG
IT. MADE IN GERMANY.

Titelthemen

Edel-Smartphones im Test

- 16 **Künstliche Intelligenz** auf dem Smartphone
- 20 **Test** Acht High-End-Smartphones

Proxmox: Server für virtuelle Maschinen

- 56 **Virtualisierung** als Universalbetriebssystem
- 60 **Proxmox** Wie die Umgebung funktioniert
- 64 **Praxis** Loslegen mit Proxmox VE

Fremdsprachen lernen mit KI

- 96 **Test** KI-Sprechtrainer
- 104 **ChatGPT** zum Sprechtrainer aufrüsten

Test & Beratung

- 70 **Workstation-CPU** Intel Xeon w7-2495X
- 72 **Workstation mit 96 Kernen**
- 76 **Markdown-Erweiterung** für Word
- 77 **Tower-Kühler** Scythe Mugen 6
- 78 **Saugroboter** Dreame L10s Pro Ultra Heat
- 80 **Maus- und Keyboard-Switch** Synergy 3
- 81 **Lebensmittelscan-App** SOVI
- 82 **Linux: Gnome 46 mit verbesserter Suche**
- 84 **27-Zoll-Monitore mit 4K und USB-C-Eingang**
- 88 **Einhandcontroller für ambitionierte Spieler**
- 92 **Transkriptions-Apps und -Dienste**
- 106 **Prepaidtarife** bis zwölf Monate Laufzeit
- 130 **Plasticity: Einfaches CAD für 3D-Drucke**
- 166 **Bücher** Docker-Praxis, Hackbibel 3

Aktuell

- 14 **Browser schlampen bei verschlüsseltem DNS**
- 32 **Datenleck** hinter Kita-App „Stay Informed“
- 34 **Security** Lücken in Browsern aufspüren
- 36 **Security** Hintertür in der Bibliothek xz
- 37 **Open Source** Redis-Fork Valkey
- 38 **KI** Stimmklone, Regeln für US-Behörden
- 40 **Anwendungen** Evernote Legacy, eM-Client
- 42 **Bit-Rauschen** Windows auf ARM-Chips
- 44 **Netze** Router mit 5G und Wi-Fi 6, Switches
- 45 **Hardware** Mini-PC für KI, KI-Benchmark
- 46 **KI-Beschleuniger** von Nvidia
- 48 **Internet** BDSG schützt Schufa, In-App-Browser
- 49 **Vorsicht, Kunde** jetzt als Podcast von c't
- 50 **Forschung** 3D-Avatar kann Gebärdensprache
- 52 **Web-Tipps** Wortspiel, Raketenstarts, Schriften

16 Edel-Smartphones im Test



Für 1000 Euro darf man eine Menge Smartphone erwarten – und bekommt es auch: schnelle CPUs, knackige Displays und schillernde Fotos, dazu immer mehr KI-Funktionen. iPhone 15 Pro Max und sieben Androiden im Test.

Wissen

- 110 **Zahlen, Daten, Fakten** Reisen
- 112 **Im Detail: Windows 11 Version 24H2**
- 116 **DNS** Verschlüsselung auf Lecks prüfen
- 122 **Corona-Warn-App** Was daraus wurde
- 126 **Thunderbolt** Grundlagen der Schnittstelle
- 128 **3D-gedruckte Augen** Smart und natürlich
- 134 **Windows sudo** Tool für Konsolenfans
- 148 **Linux: Secure Boot und Nachfolger erklärt**
- 158 **Recht** KI-Ghostwriting

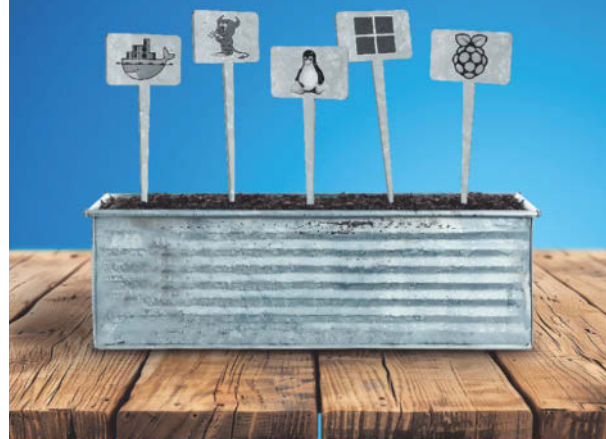
Praxis

- 138 **Alte Macs mit jungem OS aufbrezeln**
- 142 **OpenWrt** Routing über Heimnetzgrenzen
- 152 **Papierarmes Büro mit paperless-ngx**

Immer in c't

- 3 **Standpunkt** Mehr Datenschutz-Skalierung!
- 8 **Leserforum**
- 13 **Schlagseite**
- 54 **Vorsicht, Kunde** MediaMarkt wimmelt ab
- 160 **Tipps & Tricks**
- 162 **FAQ** 3D-Ton für Filme, Musik und Spiele
- 168 **Story** Der ganz besondere Marvin
- 175 **Stellenmarkt**
- 176 **Inserentenverzeichnis**
- 177 **Impressum**
- 178 **Vorschau c't** 10/2024

56 Proxmox: Server für virtuelle Maschinen



Virtualisierung kann zwar heute jedes Betriebssystem, aber es lohnt sich, die kostenlose VMware-Alternative Proxmox kennenzulernen. Wir stellen die Open-Source-Software vor und helfen bei den ersten Schritten.

Frisch aus
c't Nerdistan

134 **sudo** für Windows

c't Hardcore

148 **Secure Boot** Startverbote unter Linux

Leserforum

Nix herausgekommen

Standpunkt zum Solarpaket I, c't 8/2024, S. 3

Sie sprechen mir aus der Seele. Da wurden Unterschriften gesammelt, eine Petition gestartet ... Was ist dabei herausgekommen? Nix. So startet man keine Energiewende! Nach meinem Dafürhalten müssten auch die modernen digitalen Zähler einfach rückwärts zählen, wenn ich Strom einpeise.

Wilfried Sudholz ✓

Das Netz als Speicher

Ich durfte gerade einen Blick nach Schweden werfen. Dort haben Freunde ein Haus gekauft und saniert, mit Wärmepumpe und Solaranlage. Auf die Frage, wieso sie die Solaranlage ohne Speicher bauen, kam die in Deutschland unvorstellbare Antwort: Der eingespeiste Strom wird vom bezogenen Strom grundsätzlich abgezogen. Sprich, das Netz ist der Speicher. In Deutschland unvorstellbar, da werden zu Spitzenzeiten lieber Kohle-/Gaskraftwerke angeworfen und der selbsterzeugte Strom in privaten, teuren Speichern gespeichert.

Paul Göbel ✓

Auf die Finger schauen

Folgen des Brandanschlags auf die Tesla-Produktion in Grünheide, c't 8/2024, S. 12

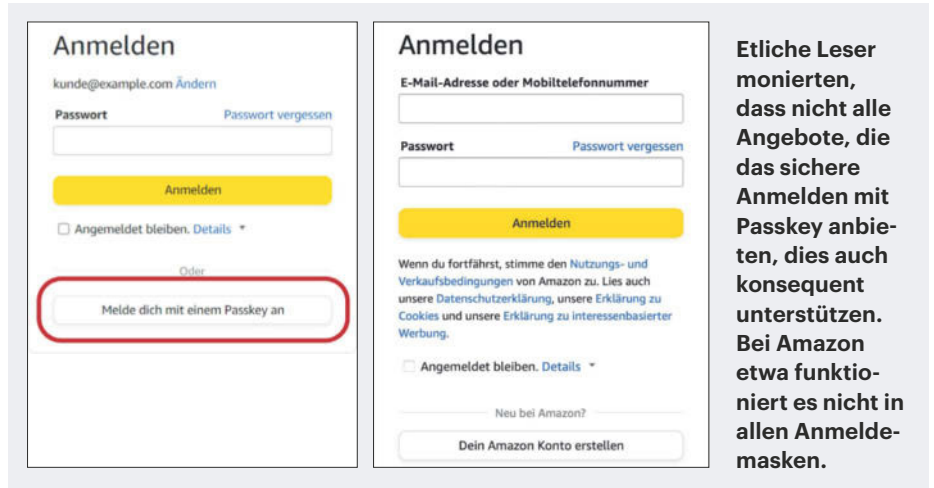
Im Artikel werden die Arbeitsbedingungen im Werk kritisiert. Ich frage mich, ob wir hieraus nicht lernen können und zum Beispiel Intel genauer auf die Finger schauen. Bevor wir einem weiteren US-amerikanischen Börsenunternehmen Steuergelder hinterherwerfen, die letztendlich doch nur wieder bei den Shareholdern jenseits des Atlantiks landen, während die Arbeitskräfte im brandneuen Werk unter Umständen ähnliche Bedingungen wie bei Tesla erdulden müssen.

Patrik Schindler ✓

Unvollständig implementiert

Statt Passwort: Accounts mit Passkeys schützen, c't 8/2024, S. 24

Die auf Seite 26 abgebildete Amazon-Anmeldemaske bekommt man, wenn man den gelben Anmelden-Button anklickt. Falls man direkt seine Bestellungen prüfen



Etliche Leser monierten, dass nicht alle Angebote, die das sichere Anmelden mit Passkey anbieten, dies auch konsequent unterstützen. Bei Amazon etwa funktioniert es nicht in allen Anmelde-masken.

möchte und den Eintrag „Meine Bestellungen“ anklickt, gerät man auf eine Anmeldemaske, bei der die Verwendung des Passkeys nicht vorgesehen ist. Möglicherweise eine unvollständige Umsetzung des Passkey-Designs durch Amazon.

Michael Schwarz ✓

Nicht problemlos

Generell scheint es einen Wildwuchs bei der Implementierung von Passkeys zu geben. Es ist verwirrend, wie viele Optionen es gibt (Windows Hello, andere Geräte, Sicherheitsschlüssel etc.). Und leider funktionieren einigen Dienste nicht so problemlos, wie Sie das in Ihrem Artikel dargestellt haben.

eBay erlaubt bei mir nicht, dass ich selbst weitere Passkeys hinzufüge. In den Einstellungen gibt es keinen entsprechenden Punkt, man kann Passkeys nur deaktivieren. Amazon ist besonders problematisch. Mit keinem Wort haben Sie erwähnt, dass Firefox nicht unterstützt wird. Selbst mit Chrome gab es unter Windows 10 Probleme. Generell scheint die Unterstützung unter Windows 11 besser zu funktionieren als unter Windows 10. PayPal gehört meiner Meinung nach noch nicht in diesen Artikel, dort ist die Passkey-Unterstützung einfach zu rudimentär.

Kay Patzwald ✓

Die Einschränkung bei eBay ist vom Dienst so gewollt. Sie können sich behelfen, indem Sie den Passkey auf einem Smartphone speichern, um ihn mit allen Geräten zu verwenden. Bei Amazon können Sie als Firefox-Nutzer den User Agent von Firefox auf Chrome ändern,

etwa mit der Erweiterung „User-Agent Switcher and Manager“. PayPal arbeitet aktuell noch an der Passkey-Unterstützung. Seit Erscheinen des Artikels hat sich schon etwas getan: Mit der PayPal-App für Android konnten wir erfolgreich einen Passkey erstellen und auch zum Einloggen in die App verwenden.

Immer dabei

Also für Passkeys brauche ich ein Smartphone oder einen Stick. Für Passwörter brauche ich mein Gehirn. Da fällt die Wahl nicht schwer. Das Smartphone habe ich ja immer dabei.

Maniac1000

Genickbruch

Steht Bitcoin vor einer weiteren Runde im Hype-Zyklus?, c't 8/2024, S. 38

Wie an den echten Börsen, sollte man beim Handel nicht nur auf den Kurs schauen, zu denen ein Wert gehandelt wird, sondern auch auf das Handelsvolumen. Wenn nämlich nur wenige Käufer beziehungsweise Verkäufer zum Handel bereit sind, können die Kurse stärker schwanken, ohne dass das repräsentativ sein muss.

Die von Ihnen thematisierte exponentielle Abnahme der Belohnung für die Be-

Fragen zu Artikeln

Bitte senden Sie uns Ihre Fragen per E-Mail an die Adresse des Redakteurs, die am Ende des Artikels steht.

1&1 Glasfaser

Mit 50 bis 1.000 MBit/s zum Surfen, Telefonieren und Fernsehen. Für Mieter und Eigentümer.*

1&1 – Immer wieder besser.

29,99 €/Monat*

DAUERHAFT GÜNSTIG

1&1 Glasfaser 50



**1&1 trägt die
Baukosten!**



1und1.de
0721/960 6060

1&1

*Z. B. 1&1 Glasfaser 50 für 29,99 €/Monat oder 1&1 Glasfaser 1000 für 59,99 €/Monat. Dauerpreis: Kein Preissprung während der gesamten Laufzeit. Internet-Flat: Unbegrenzt surfen bis zu 50 MBit/s (1&1 Glasfaser 50) oder bis zu 1000 MBit/s (1&1 Glasfaser 1000). Glasfaser-Tarife in vielen Regionen möglich. Sofern keine Glasfaserleitung vorhanden: Ausbau und Eigentümergenehmigung erforderlich. Aktion: Baumaßnahmen kostenfrei. Keine Baukosten bis zur Glasfaserdose nach dem Hausübergabepunkt. Je nach Wohnsituation sind ggf. Leitungswege durch Eigentümer im Haus vorzubereiten. Für alle Tarife gilt: Telefon-Flat ins dt. Festnetz. Anrufe in dt. Mobilfunknetze 19,9 ct/Min. Mögliche Hardware: z. B. 1&1 HomeServer Glasfaser für 4,99 €/Monat. Versand: einmalig 9,90 €. Bereitstellungspreis: einmalig 69,95 €. Mindestlaufzeit: 24 Monate. Abbildung ähnlich, Änderungen und Irrtümer vorbehalten. Preise inkl. MwSt. 1&1 Telecom GmbH, 56403 Montabaur. WEEE-Reg.-Nr. DE13470330



rechnung neuer Bitcoin (Halbierung ca. alle vier Jahre) wird dem System meiner Meinung nach langfristig das Genick brechen: Zur Kompensation der Kosten müssten die Transaktionsgebühren exponentiell steigen.

Stephan Schleim ✉

Potenzial verstehen

Dass sich derzeit die ganz Großen auf Bitcoin und Ether stürzen, kann man gerne kritisch sehen, dies ändert jedoch an der ziemlich genialen Technologie nichts. Und es ändert auch nichts an den Eigenschaften wie der Dezentralität des Systems. Es spricht eher dafür, dass die Technologie langsam auch im Mainstream ankommt und das Potenzial verstanden wird. Dass der Markt im großen Stil manipuliert wird, ist ebenfalls nicht spezifisch für Bitcoin, sondern betrifft alle großen Assets.

Frank Herberg ✉

Sehr überschaubar

Licht und Schatten bei der neuen eIDAS-Verordnung, c't 7/2024, S. 14

Lustig, dass Ursula von der Leyen bis 2030 alle wichtigen öffentlichen Dienste online verfügbar machen will. Als deutsche Politikerin sollte sie doch wissen, dass das mit dem deutschen Föderalismus, bei dem jedes Bundesland und möglichst noch jede Gemeinde sein beziehungsweise ihr eigenes Softwaresüppchen kochen will, und mit der Langsamkeit der deutschen Beamten und Bürokratie niemals bis dahin in Deutschland umsetzbar ist.

Wenn ich mich richtig erinnere, wollte damals schon Brigitte Zypries (noch als Staatssekretärin, nicht als Ministerin) die digitale Verwaltung in Deutschland bis 2005 einführen. Jetzt ist es 20 Jahre später und das Angebot an digitaler Verwaltung für den Bürger doch sehr überschaubar.

Carsten Fricke ✉

Systemd-Verweigerer

postmarketOS künftig mit Systemd, c't 7/2024, S. 37

Zwischen den Zeilen liest sich die „lautstarke Minderheit“ der Systemd-Verweigerer fast schon wie eine Beschimpfung. Meines Erachtens sind dies häufig Server-Admins, die gegenüber den augenschein-

Abonnenten lesen Artikel digital und vorab

Das c't-Abo bietet Ihnen viele Vorteile. So können Abonnenten viele c't-Artikel im Webbrowser lesen, meist sogar bevor das Heft im Briefkasten liegt. Dazu genügt ein kostenloser Account bei heise online, den Sie allerdings noch mit Ihrem c't-Abo verknüpfen müssen. Sollten Sie noch keinen heise-online-Account haben, legen Sie diesen unter heise.de/s/6EEjZ an. Unter heise.de/s/lwwY2 verknüpfen Sie Ihren Account mit Ihrem Abo. Danach können Sie die mit „c't Magazin“ gekenn-

zeichneten Artikel auf heise.de/plus lesen, solange Sie mit dem verknüpften Account angemeldet sind.

Um Ihnen das Auffinden der c't-Artikel auf heise+ zu erleichtern, stellen wir sie jeden Dienstag im Club-Newsletter für unsere Abonnenten zusammen. Falls Sie diesen noch nicht erhalten, können Sie ihn unter heise.de/s/WxxOe bestellen.

Accountverwaltung und Newsletteranmeldung: ct.de/ywr5

lich auf Desktopeinsatz fokussierten Gremien der Linux-Distributionen keine Chance haben, mit ihren Argumenten angemessen berücksichtigt zu werden.

Patrik Schindler ✉

Viele der Funktionen, die Systemd anbietet, sind insbesondere für Server sinnvoll.

Wär's doch nur ein Aprilscherz

Titelthema „Windows: Boot-Chaos droht“, c't 7/2024, S. 58 ff.

Als ich den Artikel „Schiffbruch mit An-sage“ las, dachte ich mir: Ist das schon die April-Ausgabe? So hanebüchen kann das doch gar nicht sein ... die vielen „bloß nicht zu Hause nachmachen“ ... aber echt gut ausgedacht. Andererseits: Noch nie war ein April-Scherz ein Titelthema und auf mehrere Beiträge gestreckt. Als ich dann die „Unicode-Neuerungen“ auf Seite 130 las, war klar: Doch, das ist die April-Ausgabe!

Martin Meier ✉

Chaos an Schulen

Nachdem ich Ihre Artikel gelesen hatte, standen mir die Haare zu Berge. Ich habe mir vorgestellt, was es allein für die Schulen bedeutet, wenn demnächst die Rechner von Schülern, Lehrern, Verwaltung und die elektronischen Tafeln reihenweise nicht mehr booten. Die Verteilung der Abituraufgaben an die Schulen kann nicht mehr sichergestellt werden, Abiturienten verlieren ihre Lernunterlagen fürs Abitur, Kollegen können keine Beurteilungen

schreiben, Unterricht und Prüfungen mit elektronischen Boards können nicht mehr sichergestellt werden et cetera.

Thomas Appel ✉

Ergänzungen & Berichtigungen

Dorf statt Heim

Microsoft baut für 3,2 Milliarden Euro Rechenzentren in Deutschland, c't 6/2024, S. 16

Im Bericht über die Pläne von Microsoft hatten wir die Gemeinde Elsheim genannt, gemeint war jedoch Elsdorf.

Wir freuen uns über Post

✉ redaktion@ct.de

💬 c't Forum

f c't Magazin

✂ @ctmagazin

@ ct_magazin

@ ct_Magazin

in c't magazin

Ausgewählte Zuschriften drucken wir ab. Bei Bedarf kürzen wir sinnwährend.
Antworten sind kursiv gesetzt.

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

VOR- SICHT!

Diese Anzeige zerstört sich von selbst,
sobald Du sie gelesen hast!*

Denn was hier steht, geht nur Dich was an!

Cordaware bestzero
Sichere Lösungen
für unsichere Zeiten.

Größtmögliche Sicherheit für Remote Work.
Erhebliche Reduzierung von Cyber-Bedrohungen.
Dedizierter Zugang für einzelne Anwendungen.
Zeitsparend, kosteneffizient, flexibel.

* Inklusive darauf befindliches Genmaterial sowie sämtliche Fingerabdrücke.

Besuchen Sie
uns auf der
Hannover Messe!
Halle 16, Stand D12
22. - 26.04.2024



✓ Verfügbar für Windows, macOS, Linux, iOS und Android

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



IT Made in Germany



WIR TEILEN KEIN HALBWISSEN WIR SCHAFFEN FACHWISSEN



23.05.



Photovoltaik für Einsteiger

Im Webinar lernen Sie die erforderliche Ausstattung einer eigenen Photovoltaik-Anlage zu überschlagen und die technischen Komponenten am Markt einzuschätzen.



28.05.



Einführung ins Threat Modeling

In diesem Workshop lernen Sie Threat Modeling als leichtgewichtige Methode kennen. Sie erfahren, wie Sie zu einem „Positive Threat Mindset“ kommen, sodass Sicherheitslücken proaktiv vermieden werden.



04.06.



Node.js intensiv

Der Workshop bietet einen umfassenden Einstieg in die Entwicklung serverseitiger Anwendungen mit Node.js. Sie lernen die wichtigsten Basics, die Architektur und Best Practices kennen.



05. – 06.06.



Einführung in den Kea DHCP Server

Der Workshop gibt eine vollständige Einführung in die neue Kea-DHCP-Software auf Unix- und Linux-Systemen. Sie lernen, wie man das Kea-DHCP-System installiert, konfiguriert und wartet.



11.06.



Einführung in Power BI

Der Workshop stellt praxisnah die wichtigsten Grundlagen des BI-Konzeptes und die verschiedenen Komponenten vor. Außerdem lernen Sie die Vorteile von Power BI gegenüber dem klassischen Excel kennen.



11. – 12.06.



Dienste mit SELinux absichern

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

Sichern Sie sich Ihren Frühbucher-Rabatt:
heise.de/ct/Events



Falsche Sicherheit

DNS-Leck: Browser ignorieren Windows-Konfiguration

Viele Browser und Anwendungen verschicken kritischen DNS-Verkehr ungeschützt am Betriebssystem vorbei, obwohl Windows diese Daten verschlüsseln soll. Ursache ist eine nicht zu Ende gedachte Automatik.

Von Ronald Eikenberg
und Dušan Živadinović

Wenn Sie möglichst sicher und privat surfen möchten, sollten Sie Ihre DNS-Anfragen verschlüsseln, denn diese sind ein kritischer Bestandteil Ihres Netzwerkverkehrs. Die Anfragen geben einen intimen Einblick in Ihr Surfverhalten, wenn sie ungeschützt sind. Darüber hinaus sind sie ein gefundenes Fressen für Angreifer: Sind DNS-Anfragen unverschlüsselt, können Dritte sie manipulieren, um Verkehr auf beliebige Server umzulenken.

Die meisten Betriebssysteme und Browser können daher den DNS-Verkehr seit einigen Jahren verschlüsseln. Es gibt sogar mehrere Methoden: Zu den verbreiteten gehört DNS-over-HTTPS (DoH), das die DNS-Kommunikation durch einen

TLS-Tunnel zum Resolver schickt. Diesen Schutz können Sie ab Windows 10 in den Netzwerkeinstellungen mit wenigen Klicks einschalten. Doch eine kaum bekannte Automatik in Google Chrome und anderen Chromium-Browsern kann diese Einstellung unbemerkt unterlaufen, sodass der DNS-Verkehr der Browser trotzdem im Klartext durch die Leitung abfließt.

Das Problem fiel uns während detaillierter Analysen des Netzwerkverkehrs eines Testrechners auf. Obwohl in Windows-Einstellungen die DNS-Verschlüsselung eingeschaltet und die Option „Fallback auf Klartext“ ausgeschlossen war, gingen ausgerechnet beim Surfen etliche DNS-Anfragen unverschlüsselt raus.

Um die Ursache für das Leck zu finden, haben wir zunächst verschiedene Browser und DNS-Resolver geprüft. Dabei zeigten sich unerwartete Unterschiede: Während der DNS-Verkehr von Firefox und verwandten Browsern gemäß unserer Konfiguration verschlüsselt wurde, sickerten mit Google Chrome, Edge und anderen Chromium-Browsern auch unverschlüsselte DNS-Pakete durch.

Auch bei den Resolvern zeigten sich Unterschiede: Als wir die DNS-Anfragen zur Auflösung an Google (8.8.8.8), Cloudflare (1.1.1.1) oder Quad9 (9.9.9.9) verschickten, haben Chromium-Browser ihre



DNS-Anfragen bis wenige Sekunden nach dem Start im Klartext versendet und erst dann wie angeordnet verschlüsselt. Doch bei weniger bekannten Resolver-Anbietern wie dem VPN-Anbieter Mullvad oder dem Schweizer Verein „Digitale Gesellschaft“ blieben die DNS-Pakete unverschlüsselt – ausgerechnet bei datenschutzfreundlichen Resolvern, die man einstellt, um die Privatsphäre zu verbessern.

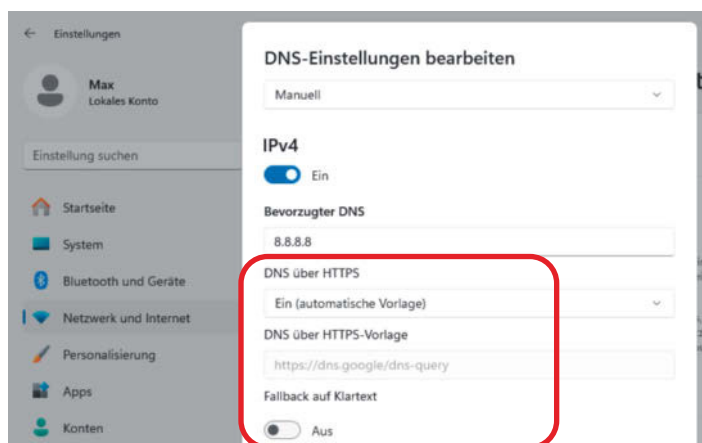
Ursachenforschung

Da nur die Chromium-Browser aus der Reihe tanzten, kontrollierten wir die Browser-Einstellungen von Google Chrome. Dort war unter „Datenschutz und Sicherheit/Sicherheit“ die Option „Namen von Websites, die du besuchst, verschlüsseln“ mit der Voreinstellung „Standardeinstellung des Betriebssystems (falls verfügbar)“ aktiv. Die Verschlüsselung müsste demnach also eigentlich aktiv sein.

Wir fanden mit dem Process Monitor von Sysinternals (siehe Seite 116) heraus, dass Firefox und die meisten anderen Prozesse die Systemkomponente svchost.exe (Service Host) für DNS verwenden. Das geschieht verschlüsselt über HTTPS, wie in Windows konfiguriert. Bei den Chromium-Browsern gehen die DNS-Anfragen hingegen direkt von den Browser-Prozessen aus, etwa bei Google Chrome von chrome.exe. Diese Browser lösen ihre DNS-Anfragen offensichtlich selbst auf, also am Betriebssystem vorbei.

In weiteren Analysen kam heraus, dass Chrome erst seit Version 105 von Ende August 2022 seine DNS-Anfragen selbst verschickt, unabhängig davon, ob im Browser DoH konfiguriert ist oder nicht. Verantwortlich dafür ist die Chromium-Komponente Async DNS, die das Surfen mittels asynchronen DNS-Anfragen beschleunigen soll.

Auffällig ist, dass die Chromium-Browser stets den in Windows eingetragenen DNS-Resolver nutzen, wenngleich nicht verschlüsselnd. Den lesen sie also



Trügerische Sicherheit: Die DNS-Einstellungen von Windows sind hier auf Sicherheit getrimmt – und trotzdem verschicken viele Browser unverschlüsselte DNS-Anfragen.

aus, um ihn dann selbst anzusprechen. Die DoH-Einstellungen von Windows ignorieren sie aber.

Verschlüsselung nach Liste

Zur Erinnerung: Bei den Resolvern von Google, Cloudflare und Quad9 sind die DNS-Übertragungen nur während der ersten Sekunden nach Browserstart unverschlüsselt, bei kleinen und wenig bekannten Resolvern aber dauerhaft. Das spricht dafür, dass Chromium-Browser die Resolver-IP-Adresse aus den Windows-Einstellungen auslesen und dann DoH über einen eigenen Mechanismus zu aktivieren versuchen.

Eine Erklärungen fanden wir im Chromium-Blog: Demnach aktivieren die Browser die DoH-Verschlüsselung automatisch anhand einer statischen Liste (siehe ct.de/ykvn). Steht die ausgelesene Resolver-IP in der Liste, ist DoH fortan aktiv – andernfalls nicht. Die Liste deckt sich mit unseren Beobachtungen: Aufgeführt sind etwa Google, Cloudflare und Quad9, bei denen die automatische Verschlüsselung funktioniert. Mullvad und die Digitale Gesellschaft, bei denen die Browser Klartext plappern, fehlen hingegen.

Die Idee hinter dieser Automatik ist offenbar, dass Chrome & Co. automatisch verschlüsseln sollen, auch wenn sich der Nutzer nicht darum kümmert. Das ist begrüßenswert, doch kann diese nicht zu Ende gedachte Automatik auch das Gegenteil bewirken: Der Browser verschlüsselt nicht, obwohl der Nutzer explizit DoH im Betriebssystem aktiviert hat. Das wiegt den Nutzer in falscher Sicherheit.

Downgrade-Angriff auf DoH

Aber selbst wenn in Windows ein Resolver konfiguriert ist, der auf der internen Liste des Browsers steht, kann man sich nicht darauf verlassen, dass die DNS-Verschlüsselung aktiv ist: Die Browser fragen vor dem Wechsel auf DoH eine Domain ab, die zum jeweiligen Resolver passt. Wenn man etwa Googles Resolver einstellt, fragt Chrome im Klartext nach der Domain `dns.google`, einem Bestandteil der DoH-URL `https://dns.google/dns-query`.

Diese Klartext-Anfragen kann ein Angreifer verhindern. Der Browser gibt nach einigen Versuchen auf und kommuniziert daraufhin unverschlüsselt mit dem Resolver. Es kommt also zu einem unerwünschten Fallback auf Klartext-DNS, obwohl das in den Windows-Einstellungen ausgeschaltet ist.

Auch Edge & Co. betroffen

Im Test waren alle gängigen Chromium-Browser für den Downgrade-Angriff anfällig: Chrome (Version 123.0.6312.87), Edge (123.0.2420.65), Vivaldi (6.6.3271.55), Opera One (109.0.5097.38) und Brave (1.64.113). Da die anfällige Automatik im Browser steckt, sind auch andere Betriebssysteme betroffen. Wir konnten das Problem auch unter macOS nachvollziehen, nachdem wir ein Konfigurationsprofil installiert hatten, das eigentlich für verschlüsseltes DNS sorgen soll. Daran hielt sich neben Safari jedoch nur Firefox.

Und schlimmer noch: Die Browser-Engine Chromium steckt auch in Electron-Apps. Deshalb zeigen Apps wie Visual Studio Code, Obsidian, Signal und Slack dasselbe DoH-Problem wie Chrome.

Die Chromium-Browser können Sie absichern, indem Sie direkt in den Browser-Einstellungen einen DoH-Resolver wählen, anstatt sich auf die Automatik zu verlassen. Dann funktioniert die Verschlüsselung so, wie man es erwarten würde: Verhindert ein Angreifer die verschlüsselte DNS-Verbindung, stellt der Browser die Arbeit ein und wirft einen Fehler. Im Issuetracker des

Chromium-Projekts wurde das Downgrade-Problem bereits vor einiger Zeit von einem Nutzer dokumentiert. Laut einem der Entwickler ist es gewollt, dass Chromium im Automatikmodus auf ungeschütztes DNS zurückfällt, wenn die DoH-Verbindung gestört ist. Stellt man von Hand einen DoH-Resolver ein, wird hinter den Kulissen der „SECURE mode“ aktiv, der das Downgrade verhindert. Man bekommt in den Browser-Einstellungen allerdings gar nicht mit, dass der Browser sicherer wird, wenn man einen Resolver wählt.

Fazit

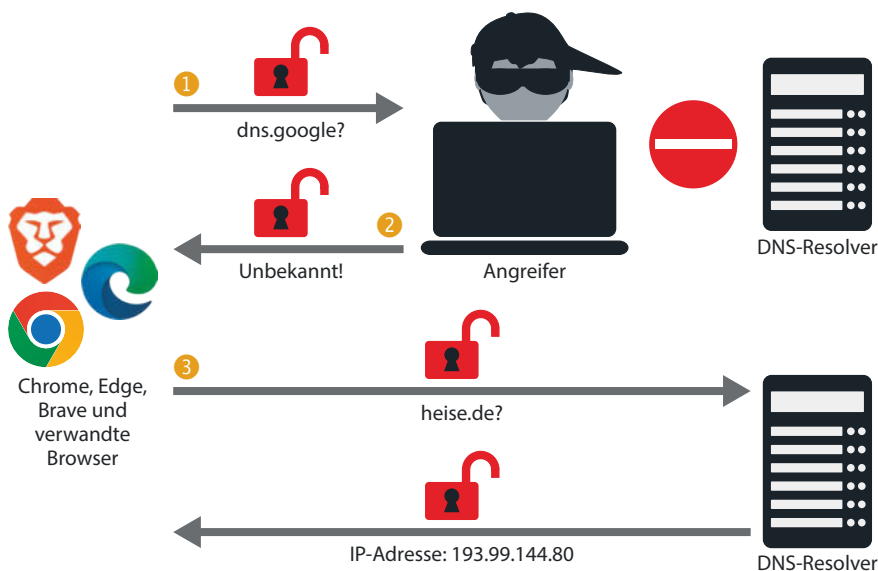
DNS-Anfragen sind ein interessantes und leichtes Ziel für Schnüffler und Angreifer. Es ist daher ratsam, diese Daten zu verschlüsseln. Das klappt jedoch nicht immer fehlerfrei, wie unsere Analyse zeigt. Damit wiegen Browserhersteller die Anwender in trügerischer Sicherheit.

Gehen Sie besser auf Nummer sicher: Auf Seite 116 beschreiben wir ausführlich, wie Sie Lecks im DNS-Verkehr aufspüren und stopfen. *(rei@ct.de) ct*

Hintergrund-Infos: ct.de/ykvn

Downgrade-Angriff auf DNS-over-HTTPS

Standardmäßig ist eine Automatik in Chromium-Browsern aktiv, die dafür sorgen soll, dass DNS-Anfragen mittels DNS-Verschlüsselung (DNS-over-HTTPS, DoH) geschützt werden. Ist ein Angreifer im Spiel, ist dieser Schutz jedoch wirkungslos. Bevor die Verschlüsselung steht, verschickt der Browser ungeschützte DNS-Anfragen, um die IP-Adresse des DoH-Resolvers zu erfahren (1). Fängt ein Angreifer diese Anfragen ab und gibt vor, dass die Domain nicht existiert (2), bleibt der Wechsel auf DoH aus und alle folgenden DNS-Anfragen werden weiterhin im Klartext verschickt (3). Der Angreifer kann diese Klartext-Anfragen dann mitlesen und manipulieren.



Smart wird schlau

Künstliche Intelligenz in Smartphones



Künstliche Intelligenz auf dem Smartphone	Seite 16
Acht High-End-Smartphones im Vergleich	Seite 20

Auf immer mehr Smartphones breitet sich die künstliche Intelligenz aus. Sie verschönert Bilder und Videos, übersetzt in zig Sprachen, schreibt Texte und beantwortet Nachrichten – und steht doch noch ganz am Anfang.

Von Steffen Herget

Bei so vielen Aufgaben, die das Smartphone den Menschen abnimmt, kann es auch gleich selber denken. So oder ähnlich scheint die Maßgabe der Hersteller zu lauten, die durch die Bank immer wilder den KI-Stempel schwingen und alle möglichen neuen Funktionen einbauen, die als künstliche Intelligenz durchgehen sollen. Dazu gehören Spielereien genauso wie richtig Nützliches – und Kleinkram, bei dem man sich fragen muss, ob das wirklich den Begriff KI verdient hat.

Künstliche Intelligenz im Smartphone ist kein ganz neuer Trend mehr. Den Stein losgetreten hat Huawei bereits im Jahr 2017, als das chinesische Unternehmen seinen Prozessor Kirin 970 auf der IFA in Berlin ankündigte. Als erster Mobilprozessor hatte er eine dedizierte NPU an Bord, eine Neural Processing Unit, die speziell für KI-Aufgaben zuständig war. Viel mehr als einige zusätzliche Rechenkerne in einem eigenen Bereich auf dem SoC war das damals nicht, doch der Ton war gesetzt: Smartphones bekamen „künstliche Intelligenz“, die Hardwarebasis als Fundament war da. Mittlerweile haben alle Chips der höheren Leistungsklassen solche eigenen KI-Einheiten. Die des Qualcomm Snapdragon 8 Gen 3 beispielsweise kann mit bis zu 10 Milliarden Parametern rechnen, ganz ohne Hilfe aus großen Serverfarmen.

Doch ganz ohne Cloud, also via Datenverbindung angefunkte Rechenzentren, geht es dann doch nicht. Bei den aktuellen KI-Funktionen auf Smartphones unterscheidet man zwei Spielarten: einerseits die On-device-KI, die rein lokal arbeitet, andererseits die KI in der Cloud, die auf eine möglichst schnelle Internetver-

bindung angewiesen ist. Die dortigen, leistungsfähigeren Rechner sind in der Lage, aufwendigere Aufgaben zu erfüllen, die Reaktionsgeschwindigkeit ist jedoch langsamer als bei lokaler Verarbeitung.

Derzeit ist es vor allem die Smartphone-Oberklasse, die so oft wie möglich mit KI wedelt. Unter den acht Smartphones von Apple, Google, Samsung & Co., die wir auf den kommenden Seiten getestet haben, ist kein einziges, das sich nicht mit künstlicher Intelligenz brüstet. Besonders weit gehen Google und Samsung mit den schlaunen Features, die Koreaner sehen mit dem Galaxy S24 Ultra gar die Ära des „AI Phone“ gekommen, die Zeit des herkömmlichen „Smartphones“ sei abgelaufen. Samsung bündelt all seine KI-Funktionen unter dem Namen Galaxy AI, bei Google heißt das seit Kurzem Gemini, vorher Bard, davor schlicht Assistant.

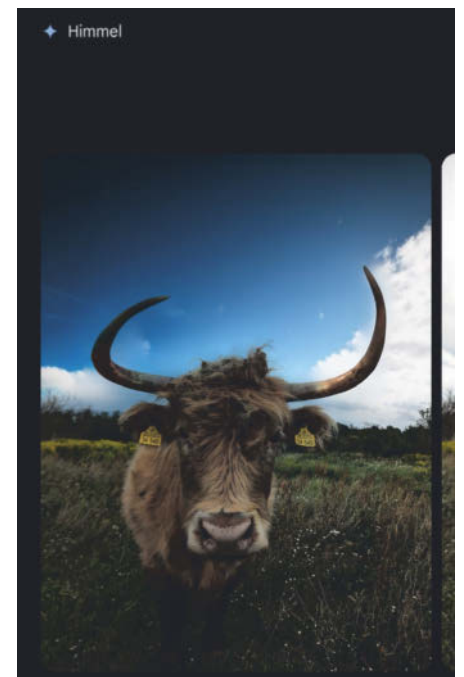
Alle lächeln in die Kamera – immer

Am deutlichsten greift die KI bei allem ein, was mit Fotos und Videos und deren Bearbeitung zu tun hat. Das geht mit der aktuellen Gerätegeneration deutlich über einfache Verschönerungen hinaus. Mit wenigen Fingertipps lassen sich Personen oder Objekte im Foto vergrößern, verkleinern, verschieben oder entfernen, die Lücken im Foto werden automatisch mit passendem Inhalt aufgefüllt. Die neuen Pixel-Smartphones machen es möglich, bei Gruppenfotos die Gesichter jeder einzelnen Person separat auszutauschen, damit alle möglichst schön eingefangen sind. Das Smartphone braucht dazu mehrere Aufnahmen, die Gesichter der Personen erkennt die KI selbständig. Das Landschaftsmotiv ist toll, aber der Himmel grau und eintönig? Zack, einfach markieren und künstlichen Himmel erstellen lassen. Gefallen die vorgeschlagenen Wolken

nicht? Kein Problem, die KI liefert unermüdlich neue Ergebnisse. Liegt das Gesicht bei einer Porträtaufnahme ungünstig im Schatten? Die richtige Bearbeitungsoption lässt die Beleuchtung frei in Richtung und Intensität anpassen, die KI berechnet die korrekten Schattenwürfe der Gesichtszüge.

Wer genau hinschaut und ins Bild zoomt, wird in vielen Fällen zwar deutliche Spuren solcher Nachbearbeitung entdecken. Die Möglichkeiten sind trotzdem beeindruckend, und das ganz ohne Kenntnisse in Bildbearbeitung und mühsamer Pixelschuberei am großen PC.

Gerade bei Fotos stellt sich die Frage: Spiegeln so bearbeitete Bilder überhaupt noch die Realität wider? Wer kann noch auf den ersten Blick ein echtes Foto von einem bearbeiteten Bild unterscheiden? Diese Frage haben vor einiger Zeit bereits Huawei und später Samsung aufgeworfen, als sie bei Super-Zoom-Fotos des Mondes Oberflächenstrukturen oder gleich den ganzen Erdtrabanten einfach ins Bild gerechnet hatten, statt tatsächlich ein Foto zu schießen. Samsung immerhin hat das Problem erkannt: Mit Galaxy AI bearbeitete Fotos bekommen ein kleines Wasserzeichen und eine Anmerkung in den EXIF-Daten, die auf die Bearbeitung hinweisen – wenn man weiß, worauf man achten muss.



Eigentlich war der Himmel flächig hellgrau. Die KI des Pixel 8 Pro macht mehr daraus.



Was die Kamera des Galaxy S24 Ultra einfängt, muss längst nicht das sein, was man am Ende zu sehen bekommt. Immerhin: Ein Wasserzeichen verrät den Einfluss der KI.

Mit Videos haben die KI-Tools nicht ganz so leichtes Spiel, weil die Bewegung im Bild, die vielen einzelnen Frames und die großen Datenmengen höhere Hürden darstellen als bei Fotos. Samsung ergänzt auf Wunsch in normaler Geschwindigkeit aufgenommene Videos um errechnete Zwischenbilder. Damit lässt sich aus einem normalen Video eine flüssige Zeitlupenaufnahme machen, bei der nicht auffällt, dass man nicht von vornherein in Zeitlupe gefilmt hat. Dass die Bilder, die vor dem Auge vorbeiflimmern, zum Teil komplett von der KI erstellt wurden, ist auf Anhieb nicht zu erkennen.

Bei Audio kann die KI ebenfalls helfen. Google nutzt sie, um auf Wunsch in Videoaufnahmen Windgeräusche zu entfernen. Das klappt vor allem bei gleichmäßig pustendem Wind ziemlich zuverlässig, ohne den restlichen Ton zu beeinträchtigen. Viele Hersteller haben in ihren Audiorekorder-Apps eine automatische Sprechererkennung eingebaut, die automatisch Aussagen den jeweiligen Personen zuordnet. Wie gut das funktioniert, hängt neben der Aufnahmequalität und Hintergrundgeräuschen auch von der Anzahl der Personen ab: Je mehr es auseinander zu halten gilt, desto schwieriger.

Simultanübersetzung am Telefon

Eines der KI-Highlights bei Samsung ist die Möglichkeit, in Telefonaten einen

Übersetzungsdienst zuzuschalten. Diese Simultanübersetzung funktioniert derzeit in 13 Sprachen, weitere sollen folgen. Die jeweiligen Sprachen für beide Seiten der Leitung muss man vor dem Gespräch einstellen. Zu Gesprächsbeginn informiert eine Computerstimme darüber, dass man sich in einem übersetzten Gespräch befindet, während dem Telefonat kann man auf dem Handydisplay in Textform sehen, was das Smartphone erkennt und ausgibt. Diese Aufnahmen bleiben jedoch lokal gespeichert, so Samsung auf Nachfrage, und werden nach dem Anruf gelöscht. Für Gespräche von Angesicht zu Angesicht lassen sich Übersetzungs-Apps wie Google Translate im Dialogmodus verwenden, um Sprachbarrieren einzureißen.

Texte sind erst einmal leichter zu verarbeiten als Bilder, Videos und Audiodateien, alleine aufgrund der weitaus geringeren Datenmengen. Kein Wunder also, dass viele KI-Funktionen daran ansetzen. Besonders praktisch ist die Möglichkeit, lange Webseiten im Browser auf ihre wichtigsten Punkte zusammenfassen zu lassen. Gleiches klappt beispielsweise bei Google und Samsung auch mit Texten in den jeweiligen Notiz-Apps. Was man dort als ungeordnete Stichpunkte eintippt, macht die Galaxy AI durch automatische Gliederungen samt Überschriften, Aufzählungen und Zwischentiteln nicht nur optisch schick, sondern fasst auch die – aus ihrer Sicht – wichtigsten Punkte zusammen. Wie Gemini ist auch Galaxy AI für solche inhaltlichen Zusammenfassungen auf eine Internetverbindung angewiesen, das reine Formatieren des Textes wird lokal erledigt.

Social-Media-Posts und Textnachrichten stellen für die KI ebenfalls leichte Beute dar. Gemini und Galaxy AI ändern auf Wunsch im Handumdrehen die Tonart einer Nachricht, aus einem förmlichen „Bitte entschuldigen Sie, ich falle heute wegen Krankheit aus“ wird mit einem Klick „Sorry Bro, liege flach und bin heute raus“. Der LinkedIn-Post fürs „beste Team“ nach der Beförderung schreibt sich samt der passenden Emojis von ganz allein, auch wenn dabei die persönliche Note verloren geht.

Spaß zum Einstieg

Gerade die generative KI, mit der sich alle möglichen Inhalte erstellen oder Lücken füllen lassen, lädt zum Ausprobieren ein. Viele Hersteller erlauben es mittlerweile, auf dem Smartphone Hintergrundbilder nach den eigenen Wünschen zu generie-

ren, und das nicht nur in der Oberklasse. Selbst das unter 400 Euro teure Nothing Phone (2a) hat einen solchen Bildgenerator eingebaut. Dabei handelt es sich nicht um eine Funktion mit großem Nutzwert, einen Zweck hat sie aber doch: Mit solchen Dingen bringt man mehr Menschen niederschwellig in Kontakt mit der KI auf dem Smartphone und macht Lust auf mehr. Nicht zuletzt bei Google genießen deshalb auch solche Spaßfunktionen einen hohen Stellenwert, wie Android-Chef Sameer Samat erst kürzlich im Interview erläuterte (Artikel in c't 7/2024, S. 40).

Dass es bei den KI-Funktionen zu Überschneidungen zwischen den Produkten unterschiedlicher Unternehmen kommt, ist nur logisch. Nicht jedes Unternehmen muss das Rad für sich alleine neu erfinden, es entstehen neue Kooperationen. Samsung etwa hat ausschließlich die On-device-Funktionen seiner Galaxy AI komplett selbst entwickelt. Alles, was in der Cloud läuft, wurde gemeinsam mit Google, Microsoft und anderen Partnern implementiert. Selbst Apple, schon immer



Neues Hintergrundbild gefällig, das sonst niemand hat? Der Bildgenerator erledigt das flott mit einigen Eingaben.

eher Einzelgänger in seinem eigenen Reich, öffnet für KI-Partnerschaften seine Tore und arbeitet für die kommende iOS-Version 18 mit Google zusammen, um Funktionen von Gemini auf das iPhone zu bringen.

Diese Kooperationen sind sinnvoll für die Unternehmen. Die Kehrseite der Medaille: Unter dem Strich machen am Ende alle das Gleiche, die Vielfalt leidet. Schaut man sich etwa die Dokumentation von Asus zum Zenfone 11 Ultra im Hinblick auf künstliche Intelligenz an, findet man dort nahezu die gleichen Funktionen wie bei Samsung. Gerade für kleinere Hersteller wie Asus sind das eher trübe Aussichten, denn ohne einzigartige Funktionen gibt es weniger Gründe für die Kundschaft, zu diesen Geräten zu greifen anstelle zu denen der größeren, etablierten Marken – ein Trend, den beispielsweise gleichförmige Prozessoren, Displays oder Kameraschips schon lange gestartet haben.

Große und kleine Fehler

Eines wird jedoch bei der Benutzung schnell klar: Das Etikett KI führt nicht automatisch dazu, dass plötzlich Dinge wie von Zauberhand gelingen, die zuvor viel Arbeit nötig machten. Längst klappt im Alltag nicht alles, was die Hersteller in schicken Werbevideos und vorbereiteten Demonstrationen zeigen.

Lässt man etwa vom Galaxy S24 Ultra Bildbereiche künstlich auffüllen, liegt der Übergang zwischen fotografierten Inhalten und errechnetem Content in etwa einem Viertel der Fälle daneben. Nach wie vor tun sich KI-Bildgeneratoren mit Merkmalen wie menschlichen Händen schwer und zaubern zu viele oder zu wenige Finger ins Bild. Texte in solchen generierten Bildern bestehen häufig aus erfundenen Buchstaben und Zeichen. Die Rekorder-App des Google Pixel, die Aufnahmen gesprochener Sprache in geschriebenen Text umwandeln soll, verschluckt bei der Transkription immer wieder einzelne Worte oder auch ganze Sätze.

Wer auf korrekten Inhalt angewiesen ist, kommt nicht umhin, das Ergebnis zu kontrollieren. Das gilt für Fotos, Videos, maschinell erstellte oder zusammengefasste Texte, transkribierte Audioaufzeichnungen, für eigentlich alles.

Bei allem, was mit Worten zu tun hat, unterscheidet sich die Qualität zudem massiv in Abhängigkeit von den gewählten Sprachen. Gesprochenes Englisch verstehen die KIs sehr viel besser als Deutsch.



Mit Apps wie Perplexity lässt sich eine gewisse Portion KI auch nachrüsten, allerdings meist kostenpflichtig und nicht so tief ins System integriert.

Doch selbst auf Englisch sollte man sich nicht allzu sicher sein: Ein 25 Minuten lang aufgezeichnetes Gespräch zwischen zwei Personen in ruhiger Umgebung wandelte das Pixel 8 Pro mit seiner KI in einem Fall in ganze zwölf Sätze und Satzbrocken um – ein völlig unbrauchbares Ergebnis. Immerhin: Im Pixel-Rekorder lässt sich mit einem Fingertipp eine erneute Transkription anstoßen, die weitaus besser gelang, aber immer noch zahlreiche Fehler enthielt und Nacharbeit erforderte. Die Übersetzung von Telefonaten bei Samsung war im Test nur leidlich korrekt, zudem fiel die KI-Stimme den menschlichen Gesprächspartnern immer wieder ins Wort.

KI per App nachrüsten

Auch Smartphones ohne eingebaute KI-Funktionen lassen sich mit KI-Apps aufpeppen, wenngleich die meisten weniger können und nicht so tief ins Betriebssystem integriert sind. Im Google Play Store und im Apple App Store finden sich bei-

spielsweise Apps für ChatGPT und Microsoft Copilot sowie zahlreiche Bildgeneratoren, teils kostenpflichtig, teils gratis. Hinzu kommen Apps wie Perplexity, die eben diese KI-Engines verwenden und bündeln, um verschiedene Bereiche abdecken zu können. Perplexity kostet in der Pro-Version rund 200 Euro pro Jahr. Das ist eine ganze Menge Geld, allerdings ist man auch anderswo nicht vor Kosten gefeit. Samsung etwa lässt noch offen, ob alle Features von Galaxy AI künftig kostenlos nutzbar bleiben. Im Kleingedruckten heißt es, diese Regelung gelte zunächst nur bis Ende 2025. TM Roh, bei Samsung für das Mobilgeschäft zuständig, gab erst kürzlich in einem Interview mit der koreanischen ET Telecom zu Protokoll, dass man möglicherweise diejenigen Kunden, die sich mehr KI-Leistung oder spezielle Funktionen wünschen, in Zukunft zur Kasse bitten könne. Eine Entscheidung darüber sei allerdings noch nicht gefallen.

So manche Funktion, die einem heute als revolutionär neues KI-Feature angepriesen wird, hat allerdings mit künstlicher Intelligenz nicht viel zu tun. Populäres Beispiel ist etwa die automatische Verschönerung von Smartphonefotos. Was in neuen Smartphones mit Begriffen wie „KI-basierte Bildverbesserung“ bezeichnet wird, hieß noch vor sechs oder acht Jahren „Bildoptimierung“ oder „Fotoentrauschen“ und macht kaum mehr, als an den Reglern für Farbintensität, Helligkeit und Schatten zu drehen, mit mal mehr, mal weniger guten Ergebnissen.

Bei allen Fehlern, die die KI nach wie vor in unschöner Regelmäßigkeit produziert, und aller Kritik an der Sinnhaftigkeit so mancher Funktion, muss man allerdings konstatieren: Schlechter als jetzt wird das alles in Zukunft nicht funktionieren. Wirft man einen Blick auf die Ergebnisse, die noch vor ein oder zwei Jahren etwa von Bildgeneratoren ausgeworfen werden, ist das ein Unterschied wie Tag und Nacht. Selbst wenn die ersten Pflöcke bereits 2017 mit dem Kirin 970 eingeschlagen wurden, steht die KI auf dem Smartphone nach wie vor am Anfang. Ist das Fundament erst gelegt, werden die Fortschritte schneller und schneller sichtbar. Die acht High-End-Smartphones im folgenden Vergleichstest zeigen, was jetzt schon möglich ist – und was ein teures Luxustelefon abseits von KI so alles kann.

(sht@ct.de) **ct**



Crème de la Crème

Acht High-End-Smartphones inklusive einiger Comeback-Kids im Test

Die Sterneküche der Smartphones kostet knapp unter oder deutlich über tausend Euro. Für so viel Geld darf man viel Power, komplette Ausstattung und edles Design erwarten. Und unsere acht Testkandidaten liefern.

Von Robin Brand und Steffen Herget

Der pure Luxus: Nur die besten Smartphones haben es auf diesen Prüfstand geschafft. Die High-End-Handys setzen die Standards, sie rechnen mit den potentesten Prozessoren, nehmen die schönsten Fotos auf, verste-

hen die schnellsten Funkstandards und erhalten jahrelang Updates. Was es mit den neuen KI-Helferlein auf sich hat, lesen Sie auf Seite 16.

Die Preise der Luxusklasse beginnen bei 900 Euro (Google Pixel 8 Pro und Xiaomi 14) und kratzen in Gestalt des Apple iPhone 15 Pro Max in Volllausstattung an der 2000-Euro-Marke. Gegen das iPhone treten sieben Android-Smartphones an. Sechs davon sind erst dieses Jahr auf den Markt gekommen und mit der frischesten Hardware ausgestattet, außerdem darf aus dem vorigen Herbst das Pixel 8 Pro von Android-Macher Google mit allerlei neu erlernten Fähigkeiten eine Extrarunde drehen. Über unerwartet properen Nachwuchs hat sich erst kürzlich Asus gefreut: Das Zenfone 11 Ultra ist anders als seine Vorgänger kein kompaktes Oberklasse-Smartphone mehr, sondern ein ausgewachsener High-End-Bomber mit 6,8-Zoll-Display. Auch fast alle restlichen Hersteller mögen es eher

groß, nur das Xiaomi 14 bleibt einigermaßen handlich. Das größere 14 Ultra erreichte uns nicht rechtzeitig für den Test.

Die ehemalige Huawei-Tochter Honor schickt das Magic6 Pro mit ungewöhnlicher Kamera und unverkennbaren iPhone-Anleihen ins Rennen. Marktführer Samsung hat beim S24 Ultra mit Stift weiterhin ein Alleinstellungsmerkmal. Und zwei noch vor Kurzem verbotene Früchte sind auch dabei: das OnePlus 12 und das Oppo Find X7 Ultra. Beiden Marken des BBK-Konzerns war fast zwei Jahre lang der Verkauf von Smartphones in Deutschland aufgrund von Patentstreitigkeiten mit Nokia verboten gewesen. Nachdem sich die Konzerne geeinigt haben, hat OnePlus seine Smartphones umgehend wieder in Deutschland verfügbar gemacht. Oppo hat ebenfalls angekündigt, schon bald wieder seine Smartphones in Deutschland verkaufen zu wollen. Erst kurz nach Redaktionsschluss erwarten wir Motorola Edge

50 und Sony Xperia 1 VI, die deshalb außen vor bleiben.

Angesichts der Preise darf man es erwarten: Alle Smartphones sind sauber aus hochwertigen Materialien verarbeitet. Rückseiten aus Glas und Metallrahmen, darunter auch solche aus teurem Titan (Apple und Samsung), sind das Mittel der Wahl. Staub- und wasserdicht gemäß IP68 oder IP65 sind die Gehäuse allesamt, vorbei sind die Zeiten, in denen sich manche Hersteller auch im High End das Label sparten. Sind die Smartphones anhand ihrer Vorderseiten mit den fast gerätegroßen Displays nur schwer zu unterscheiden, ändert sich das, wenn man sie auf die Rückseite dreht. Manch farbiger Rücken sowie kreisrund, balkenförmig, im Viereck oder einzeln angeordnete Kameras verleihen den Smartphones ein unverkennbares Äußeres. War vor zwei, drei Jahren noch der Hochglanzrücken schick, hat 2024 matt Saison.

Qualcomm für alle

So sehr sich die Hersteller um äußerliche Unterscheidbarkeit bemühen, so sehr gleichen sich die inneren Werte der Geräte. Zumindest mit Blick auf die Prozessoren. Vorbei die Zeiten, als sich mal ein MediaTek-, ein Kirin- oder ein Exynos-SoC ins High End verirrt. Der 2024er-Jahrgang der Androiden setzt geschlossen auf Qualcomms Snapdragon 8 Gen3. Im iPhone steckt der A17 Pro und im Pixel der haus-eigene Tensor-Chip der dritten Generation.

Der Apple-Chip wird in 3-Nanometer-Strukturbreite gefertigt. Er besteht aus sechs Kernen, zwei Leistungs- und vier Effizienzkernen. Die schnellen Kerne erreichen eine Taktfrequenz von 3,78 GHz, die Energiesparkerne sind deutlich langsamer getaktet (2,11 GHz). Der in 4-Nanometer-Strukturbreite gefertigte Snapdragon 8 Gen3 besitzt eine 1+5+2-Struktur mit einem starken Prime-Core, fünf Performance-Kernen und zwei schwächeren, stromsparenden Rechenwerken. Der schnelle Cortex-X4 erreicht bis zu 3,3 GHz Taktfrequenz, die fünf Cortex-A720 sind mit 3,2 GHz (drei Kerne) und 3 GHz (derer zwei) kaum langsamer getaktet. Aus ebenfalls drei Clustern, aber neun Kernen besteht der Tensor G3. Das Rechenass der neun ist ein Cortex-X3-Kern mit einer Taktfrequenz von 3 GHz. Ihm zur Seite steht ein Cortex-A715-Cluster mit vier Kernen und einer Taktfrequenz von 2,45 GHz. Die Stromspareinheit bringt vier Kerne (Cortex A510) mit 2,15 GHz mit.

Das Leistungsgefälle zwischen Apple und Qualcomm an der Spitze und Verfolger Google ist recht groß. Im Einkernbetrieb liegt der A17 Pro leicht vor dem Snapdragon und erreicht etwa die anderthalbfachen Werte des Tensor G3. Im Multi-Core-Betrieb hält der Apple-Chip den Vorsprung auf die Google-Konkurrenz, aber muss je nach Benchmark manchmal dem Snapdragon den Vortritt lassen.

Zur Drei-Klassen-Gesellschaft wird das Testfeld, wenn es um die GPU-Leistung geht. In 3DMark Wildlife Extreme, das die Grenzen der Grafikeinheiten im UHD-Rendering auslotet, erzielt der Snapdragon-Chip mehr als die doppelten Werte des Tensor. Der A17 liegt dazwischen, etwas näher am Google- als am Qualcomm-Chip. GFXBench sieht das Feld etwas näher beieinander, aber in der gleichen Reihenfolge.

Fabeldisplays: hell und heller

Noch größere Einigkeit als in Sachen Chipzulieferer herrscht im High End nur mit Blick auf die Displaygröße. 6,7 bis 6,8 Zoll Bildschirmdiagonale haben die Hersteller als Gardemaß ausgemacht. Einzig Xiaomi bleibt mit dem 14 darunter (6,4 Zoll). Allerdings ist das bestausgestattete Xiaomi, das zu spät für den Test gekommene 14 Ultra, ebenfalls ein 6,7-Zöller. Vom um die Gehäusekante gebogenen Display sind die meisten Hersteller abgerückt. Es bringt schlicht keinen praktischen Nutzen, macht das Gerät aber empfindlicher. Nur Honor, OnePlus und Oppo verwenden ein solches, die anderen Hersteller bauen plane Displays in die Geräte.

Alle Hersteller verwenden kontrast- und farbstarke OLED-Displays. Die Bildschirme erreichen maximale Bildwiederholraten von 120 Hertz für eine flüssige Darstellung von Scrollbewegungen oder



Weiter einmalig in der Smartphone-Welt: So nahtlos wie Samsung hat kein anderer Hersteller einen Stift ins Bedienkonzept integriert.



USB-C statt Lightning: Apple rüstet die Ladebuchse der iPhones um.

geschmeidige Animationen in Spielen, die eine solche Bildrate unterstützen. Da längst nicht alle Anwendungen die Vorteile der hohen Bildrate ausnutzen, regelt die Software die Bildrate entsprechend des dargestellten Inhalts. Für den Always-on-Bildschirm kann sie bis auf 1 Hertz herabgesenkt werden, um Akku zu sparen. Über 120 Hertz hinaus hat nur das Zenfone 11 Ultra Reserven: In ausgewählten Spielen – und nur dort – stellt es maximal 144 Hertz dar. Mit dem bloßen Auge erkennt man zwischen 120 und 144 Hertz keinen Unterschied, aber gegenüber den vormals üblichen 60 Hz ist ein Qualitätsgewinn ersichtlich.

Für eine gestochen scharfe Darstellung tummeln sich jede Menge Pixel auf den Smartphone-Displays. Einzig das Zenfone bleibt mit 2400 × 1080 Pixeln unterhalb einer Pixeldichte von 400 dpi. Im direkten Vergleich stellen vor allem OnePlus-, Oppo- und Samsung-Smartphone mit Pixeldichten von mehr als 500 dpi kleine Schriften schärfer dar. Da das Rendern der vielen Pixel sehr akkuhungrig ist – umso mehr in Kombination mit hohen Bildwiederholraten – kann man die berechnete Auflösung in den Einstellungen herunterregeln.

Selbst in der prallen Sonne wird man mit keinem Gerät Probleme haben, den Screen abzulesen. Bei 50 Prozent Weißanteil auf dem Schirm erreichen alle maximale Helligkeiten von weit über 1000 cd/m². Noch heller strahlen OLED-Displays, wenn nur wenige Pixel leuchten müssen. Aus den Bildschirmen des Asus und des Samsung-Smartphones konnten wir bei einem Weißanteil von 10 Prozent Werte über 2000 cd/m² herauskitzeln. Manche Smartphones wie das iPhone und das Magic behalten solch extreme Helligkeiten der Darstellung von HDR-Inhalten vor.

1 Zoll und weniger

In Sachen Sensorgröße und Telebrennweiten stellen die Hersteller 2024 anders als in den Vorjahren keine Rekorde auf. Vor zweieinhalb Jahren waren die ersten Smartphones mit Typ-1-Zoll-Sensor erschienen (das Panasonic Lumix DMC-

CM1 ausgeklammert, das mehr Kamera als Smartphone war). Seitdem haben von den großen Herstellern nur Oppo, Vivo und Xiaomi weitere Smartphones mit dem Sony-Chip vorgestellt. Das Problem des großen Sensors: Um diesen ausleuchten zu können, braucht es verhältnismäßig große Optiken. Sollen diese auch noch lichtstark sein, gilt das umso mehr.

Abgesehen vom Oppo Find X7 Ultra ist im Test kein weiteres Smartphone mit Typ-1-Zoll-Sensor bestückt. Der Rest des Feldes verwendet für die Hauptkamera Sensoren um 1/1,3", sammelt also Photonen auf einer kleineren Sensorfläche. Einige Hersteller, zum Beispiel Honor mit dem Magic6 Pro, gleichen die kleinere Fläche mit lichtstärkeren Optiken aus. Und wie gehabt spielt es eine mindestens genauso große Rolle für ein gelungenes Foto, was das Smartphone mit dem Material, das die Hardware anliefert, letzten Endes anstellt. In Zeiten von KI mehr denn je.

Fast alle Hersteller verwenden für die Hauptkamera 48- oder 50-Megapixel-Sensoren, nur Samsung tanzt mit protzigen 200 Megapixeln aus der Reihe. Standardmäßig geben die Smartphones jedoch 12- oder 24-Megapixel-Fotos aus. Per Pixel-Binning verrechnen die Geräte auf Sensorebene die Signale miteinander, um die Bildqualität zu steigern. Alle Smartphones geben Fotos in voller Auflösung aus, wenn man das möchte. Bei guten Lichtverhältnissen kann man so sichtbar mehr Details aus den Aufnahmen kitzeln.

Die Bildlooks der Smartphones sind recht unterschiedlich. Eher natürliche Farben fangen iPhone, Google und das S24 ein, vorbei die Zeiten, da Samsung-Smartphones für grelle Farben standen. Einen kräftig übersättigten Look zaubern Zenfone, Magic6 und Xiaomi 14 ins Bild, der des Asus ist hell unterkühlt, der der anderen beiden warm. In Details hineingezoomt, gefallen vor allem iPhone, Pixel

und mit Abstrichen Honor Magic und Xiaomi 14 mit plastischen Details und sauber herausgearbeiteten Objektkanten auch kleiner Motive. Diese wirken auf den Fotos des Samsung und vor allem des Zenfone unruhig überschärft mit teils unansehnlichen Treppenartefakten. Oppo und OnePlus schießen scharfe Fotos mit vielen Details, die des Find X7 Ultra zeigen etwas kräftigere Farben.

200 Megapixel in Aktion

Geben die Smartphones Fotos in Sensorauflösung aus, brillieren Apple und Samsung. Die iPhone-Fotos haben vor allem im DNG-Format jede Menge Spielraum für die spätere Bearbeitung. Das S24 Ultra gibt Raw-Bilder nicht in Sensorauflösung aus, sondern nur JPGs. Und auch die sind mit 200 Megapixeln speicherhungrig genug. In höherer Auflösung ist von unruhigen Strukturen wenig zu sehen, stattdessen beeindruckt der Detailreichtum. Geben die Lichtverhältnisse es her, sollte man Landschaftsaufnahmen mit dem S24 also in höherer Auflösung schießen. Ein guter Mittelweg zwischen Qualität und Speicherung ist die 50-Megapixel-Option, die die Kamera-App ebenfalls bereithält.

Neben den hochwertigen Hauptkameras (Brennweiten um 24-mm-KB-Äquivalent) sind es vor allem die zusätzlichen Telebrennweiten, die das High End vom Smartphone-Durchschnitt abheben. Als maximale optische Brennweite für Smartphones hat sich der Bildwinkel etabliert, der grob dem eines 130-mm-Objektivs an einer Vollformatkamera entspricht. Zwar hatte es Samsung mit dem S23 Ultra auch mal mit 230-mm-KB-Äquivalent versucht. Doch um solch lange Teles in einem Smartphone zu realisieren, müssen die Sensoren arg klein sein, zudem sind die Objektive eher lichtschwach, worunter letzten Endes die Bildqualität leidet. Aus dem Testfeld sind das Find X7 Ultra (135

1-Zoll-Sensor

Die Bezeichnung des 1-Zoll-Sensors stammt noch aus der Zeit der Vidiconröhre, deren Größe man anhand des äußeren Glasdurchmessers der lichtempfindlichen Frontfläche angab. Das Vidicon XQ-1030 mit einem äußeren Glasdurchmesser von 1 Zoll zum Beispiel nutzte eine Bildfläche von 13 x 10 Millimetern. Bis heute werden daher Sensoren dieser Ausmaße als 1-Zoll-Sensoren bezeichnet, obwohl weder die Diagonale noch die Kanten des Sensors 1 Zoll (2,54 Zentimeter) erreichen. Deswegen hat sich „Typ-1-Zoll“ als alternative Bezeichnung etabliert.

mm KB), iPhone 15 Pro Max (120 mm KB), Pixel 8 Pro (113 mm KB) und Galaxy S24 Ultra (111 mm KB) mit recht langen Brennweiten bestückt. Oppo und Samsung bauen ihren Smartphones zudem ein etwas kürzeres zweites Tele ein, das sich bestens für Porträts eignet. Einen anderen Trick verwendet Honor: Das Tele ist mit einem 180-Megapixel-Sensor ausgestattet. Das hilft, die fehlende Brennweite durch digitales Zoomen bis zu einem gewissen Grad zu egalisieren. Immerhin bis etwa 10-fach bekommt man noch brauchbare Ergebnisse.

Die dritte Kamera, die alle High-End-Smartphones auf dem Rücken tragen, ist ein Ultraweitwinkel. Was die Weiterentwicklung dieser Kamera angeht, sind die Hersteller eher in Trippelschritten unterwegs. Der steile Winkel der Objektive verursacht Abbildungsfehler, die nur schwer zu korrigieren sind. So recht haben die Hersteller noch kein Mittel dagegen gefunden. Den Detailreichtum der Hauptkameras darf man nicht erwarten. Unschöne Schärfungsartefakte und Farbsäu-

Benchmarks und Akkulaufzeiten

Modell	Geekbench 5 Single-Core [Punkte]	Geekbench 5 Multi-Core [Punkte]	GFXBench Manhattan 3.0 offscreen [fps]	3DMark Wild Life Extreme	Akkulaufzeit YouTube-Stream¹ [h]	Akkulaufzeit Video 720p¹ [h]	Akkulaufzeit Video 4k/ 120 fps¹ [h]	Akkulaufzeit 3D-Spiel¹ [h]
	besser ➤	besser ➤	besser ➤	besser ➤	besser ➤	besser ➤	besser ➤	besser ➤
Apple iPhone 15 Pro Max	2137	5994	221	3512	22,4	28,1	11,9	11
Asus Zenfone 11 Ultra	1670	5550	367	5069	21,1	22,4	17,5	18,5
Google Pixel 8 Pro	1273	3792	210	2409	20,6	17,7	8,3	9,4
Honor Magic6 Pro	1658	6336	358	5195	25,7	28,1	13,8	26,5
Samsung Galaxy S24 Ultra	1705	6458	327	5272	27,5	24,6	13	16,9
OnePlus 12	1617	5959	357	4699	22	24,7	15,2	22,2
Oppo Find X7 Ultra	1654	5842	362	4929	19,8	21,8	13,1	18,6
Xiaomi 14	1635	6160	371	4665	23,8	22,2	11,6	13,8

¹ gemessen bei 200 cd/m² und maximaler Auflösung



Webbaukasten mit KI-Text-Generator!

Künstliche Intelligenz für Ihre Website:
Einfach passende Keywords eingeben und
professionelle Textvorschläge erhalten!

1blu

Homepage Smart

12 .de-Domains inklusive

- > 60 GB Webspace
- > 500 E-Mail-Adressen
- > 50 GB E-Mail-Speicher
- > 50 MySQL-Datenbanken
- > Kostenlose SSL-Zertifikate per Mausklick
- > Viele 1-Klick-Apps inklusive
- > Webbaukasten & Webkonferenzlösung

2,69
€/Monat*



Dauerpreis!
Angebot bis 30.04.2024.

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

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



Apple iPhone 15 Pro Max

Die größten Änderungen sieht man dem iPhone 15 Pro nicht an: Es lässt sich nun von beiden Seiten öffnen und ist damit leichter reparierbar. Andererseits wirft Apple unabhängigen Werkstätten weiter Knüppel zwischen die Beine, indem es Bauteile per Software miteinander koppelt; eine Praxis, der die EU demnächst ein Ende bereiten wird. Die zweite große Änderung ist der Schritt zu USB-C. So kann man sich auf Reisen mehrere Kabel sparen. An der USB-Buchse liegen auch DisplayPort-Signale an.

Und noch etwas geht auf eine EU-Regelung zurück: Das iPhone-Betriebssystem iOS wird offener. Die EU hat iOS im Digital Markets Act als Gatekeeper eingestuft und zwingt Apple zu grundlegenden Änderungen. Ab iOS 17.4 muss Apple erstmals alternative App-Marktplätze zulassen. Das markiert das Ende des App Store als einzige Bezugsquelle für iPhone-Apps. Unter anderem hat der Spieleentwickler Epic bereits einen eigenen Store angekündigt. Außerdem muss Apple fortan andere Browser-Engines zulassen. Safari-Alternativen wie Chrome und Firefox verwenden bislang Apples WebKit-Engine, alles andere war von Apple verboten. Und auch das kontaktlose Bezahlen muss Apple für andere Anbieter öffnen. Zahlungsdienste und Banken werden eigene Apps mit NFC-Bezahlfunktion auf das iPhone bringen können.

Auch an der Hardware hat Apple geschraubt: Neu und den Pro-Modellen vorbehalten ist der Action Button, der den Schieber zum Stummschalten ablöst. Man wechselt die Modi durch Gedrückthalten und kann den Knopf auch mit Kamera, Taschenlampe, Sprachmemo, Lupe oder Kurzbefehlen belegen.

Die Kamera ist erstmals mit einem Fünffach-Tele bestückt. Die Raw-Fotos des iPhone überzeugen mit einer Fülle an Details für die weitere Bearbeitung. Für Porträts eignet sich die iPhone-Kamera wie keine zweite: So treffsicher wie das iPhone stellt kein anderes Smartphone feine Strukturen frei.

Zwar vom Snapdragon 8 Gen3 als schnellster Smartphone-SoC entthront, wird der A17 dennoch über Jahre für alle Smartphone-Anwendungen ausreichen. Den hohen Apple-Preisen stehen der verhältnismäßig geringe Wertverlust (wer später verkaufen will) und die zuverlässigen Updates entgegen.

- 👆 zuverlässiger Support
- 👆 toller Porträtmodus
- 👇 Ersatzteile an Software gekoppelt

Preis: 1200 bis 1800 Euro



Asus Zenfone 11 Ultra

Moment mal, haben wir dieses Smartphone nicht unter dem Namen ROG Phone 8 Pro bereits getestet (c't 4/2024, S. 70)? Ja, die Frage ist berechtigt. Aber nein, wir haben dem ROG Phone nicht einfach einen Schnurrbart angeklebt und jubeln es Ihnen hier als Zenfone unter. Asus hat sich schlicht dazu entschieden, das (fast) gleiche Smartphone zweimal zu bauen. Schlecht ist das Zenfone deswegen nicht, nur es fällt im Smartphone-High-End eben nicht mehr so recht auf, wie es noch sein kompakter Vorgänger tat.

Denn anders als dieses ist das Zenfone 11 Ultra mit einem 6,8-Zoll-Bildschirm bestückt und nicht mit einem 5,9-Zöller. Von seinem Gaming-Schwestermodell ROG Phone 8 Pro unterscheidet es sich nur in Nuancen: So fehlen dem Zenfone die berührungssensitiven Schultertasten im Gehäuserahmen, eine zweite USB-C-Buchse und maßgeschneidertes Gaming-Zubehör. Dafür ist es 100 Euro günstiger und dennoch fast rundum gut ausgestattet. Das OLED-Display ist extrem hell, wir haben 1830 cd/m² bei 50 Prozent Weißanteil auf dem Bildschirm gemessen, so viel wie bei keinem anderen Smartphone im Prüfstand.

Dank des großen Gehäuses drosselt das Smartphone die unbändige Kraft des Qualcomm Snapdragon 8 Gen3 auch unter Last wenig. Das ROG Phone hat die Abwärme des SoCs aber noch besser im Griff. Für die weitwinklige Hauptkamera verwendet Asus einen 1/1,56" großen 50-Megapixel-Sensor (f/1,9, OIS). Der Ultraweitwinkel schießt 13-Megapixel-Fotos (ca. 13 mm KB), das Tele ist mit einem 32-Megapixel-Sensor ausgestattet (72 mm), gibt aber nur 8-MP-Fotos aus. Die Fotos fallen im Vergleich zum Rest des Testfelds mit etwas zu aggressivem Nachschärfen auf. Der Nachtmodus tut sich vor allem bei bewegten Motiven schwer.

Der 5500-mAh-Akku ist sehr ausdauernd: Im Streaming-dauerlauf hielt das Zenfone 21,1 Stunden durch. Am Kabel lädt das Smartphone mit maximal 65 Watt, kabellos per Qi mit 15 Watt. Ein Ladegerät legt Asus nicht bei. Etwas mager ist das Updateversprechen von Asus: zwei Androidupgrades und vier Jahre Patches soll es geben.

- 👆 lange Laufzeit
- 👆 sehr helles Display
- 👇 nur vier Jahre Updates

Preis: 1100 bis 1200 Euro



Google Pixel 8 Pro

Googles Pixel 8 Pro bekommt man günstiger als die anderen Smartphones des Testfelds. Das ist einigermaßen ungewöhnlich, stellten doch sonst stets die chinesischen Hersteller OnePlus, Xiaomi & Co. den Budgettipp. Als solcher geht das 8 Pro mit Preisen ab etwas unter 900 Euro auch nicht durch, die gibt es im High End schlicht nicht mehr. Und bei den günstigsten Pixel-Pro-Modellen ist Vorsicht geboten: Sie sind mit nur 128 GByte nicht erweiterbarem Speicher bestückt. Die anderen High-End-Modelle fassen in der kleinsten Speichervariante 256 GByte, damit kostet das 8 Pro dann etwa 950 Euro.

Im Pixel steckt eine Besonderheit: der von Google entwickelte Tensor-Chip der dritten Generation. Alle anderen Androiden setzen auf Qualcomms Snapdragon 8 Gen3. Angesichts der überdeutlichen Performance-Vorteile des Snapdragon stellt sich die Frage, wie lange Google noch am eigenen Chip festhalten will. Speziell unter Last laufen die mit Snapdragon bestückten Smartphones deutlich länger als das Pixel.

Zu den Klassenbesten gehört das Pixel-Smartphone, wenn es um die Kamera geht. Das 8 Pro schießt natürlich anmutende Fotos, die sich angenehm vom knalligen Smartphone-Look abheben. Bislang sollte die Kamera-App vor allem intuitiv funktionieren und nicht durch großen Funktionsumfang abschrecken. Beim Pixel 8 Pro versteckt Google daher nun einige Funktionen, mit denen Fotografen mehr Einfluss aufs finale Bild nehmen können: Erst im Pro-Modus der App kann man die Bilder im Raw-Format und in voller 50-Megapixel-Auflösung speichern. Zudem erlaubt die App dann eine manuelle Anpassung von ISO, Belichtungszeit und Weißabgleich. JPGs in Sensorauflösung belegen ungefähr 6 MByte Speicher, DNGs um die 50 MByte.

Google hat das Pixel nach Erscheinen weiter verbessert: Die gemeinsam mit Samsung entwickelte Funktion Circle-to-Search sucht nach Inhalten in Fotos. Dazu umkreist man einfach einen Bildausschnitt auf dem Smartphone-Display, der dann in die Google-Suche fließt. Außerdem ziehen mehr KI-generierte Antworten in die Suche ein. Bei einer Multisearch genannten Funktion kann man Fragen zu den Bildausschnitten stellen. Google antwortet je nach Frage in natürlicher Sprache oder per Linkliste.

- ↑ sieben Jahre Updates
- ↑ natürliche JPG-Aufbereitung
- ↓ schwächster SoC im High End

Preis: 900 Euro bis 1200 Euro



Honor Magic6 Pro

Egal, was Apple tut, irgendein Hersteller wird es schon abkupfern: Für Dynamic Island, das pillenförmige Loch im Display, hat sich jetzt Honor als Kopist gefunden. Wie Apple bringt Honor im Magic6 Pro darin Front- und Tiefenkamera unter und zeigt verkleinerte Benachrichtigungen von im Hintergrund laufenden Apps an. Das ist praktisch, aber leider werden nicht alle Apps unterstützt: Für Google Maps hätte das Konzept besonders nützlich sein können, doch Maps spielt keine Navigationsbefehle über die Pille aus. In einer Hinsicht ist Honor der versammelten Konkurrenz voraus: Es hat gleich zwei vollwertige biometrische Entsperrmethoden. Dank Tiefensensor entsperrt die Gesichtserkennung auch Banking- und Bezahlapps, das können sonst nur das iPhone und das Pixel 8. Anders als bei iPhones steht zudem ein Fingerabdrucksensor dafür bereit.

Das Display regelt die Bildwiederholrate automatisch zwischen 1 und 120 Hertz und ist strahlend hell, der Prozessor rasend schnell und der Akku ausdauernder als der der meisten Konkurrenten. Selbst wenn man ihn mit Spielen fordert, ist er kaum in die Knie zu zwingen.

Honor baut dem Magic6 Pro drei rückseitige Kameras ein: eine weitwinklge 50-Megapixel-Kamera, einen Ultraweitwinkel und ein kurzes Tele. Die Blende der Hauptkamera lässt sich zwischen $f/1,4$ und $f/2$ verstellen, um Lichtausbeute und Hintergrundunschärfe (in Maßen) zu kontrollieren. Die Hauptkamera schießt detailreiche Fotos mit stark gesättigten Farben. Nächtliche Stadtszenarien gelingen auch ohne Nachtmodus.

Das kurze Tele (68 mm gemäß KB) ist mit einem großen $1/1,49$ -Zoll-Sensor bestückt, der von einem recht lichtstarken Objektiv ($f/2,6$) ausgeleuchtet wird. Satte 180 Megapixel drängen sich auf dem Sensor, standardmäßig gibt die Kamera aber 12-Megapixel-Fotos aus. Die vielen Pixel helfen beim digitalen Zoomen. Immerhin bis etwa 10-fach (270-mm-KB) sind brauchbare Ergebnisse möglich.

Bei den Softskills hapert es etwas: Das Betriebssystem ist mit Bloatware vollgekleistert, erinnert noch immer verdächtig an jenes aus Huawei-Zeiten und könnte einen moderneren Anstrich vertragen. Die versprochenen fünf Jahre Updates bleiben hinter Google und Samsung zurück.

- ↑ sehr lange Laufzeit
- ↑ Gesichtserkennung
- ↓ viel Bloatware

Preis: 1100 Euro






OnePlus 12

Anders als Oppo hat OnePlus das Comeback nach Deutschland schon geschafft, sowohl bei freien Händlern als auch über den eigenen Onlineshop sind die Smartphones des Herstellers wieder zu haben. Das OnePlus 12 ist vorne und hinten mit Glas überzogen, die matte Rückseite fasst sich samtig an und lässt Fingerabdrücken kaum eine Chance. Die abgerundeten Kanten geben dem Smartphone eine fließende Form, das 12er liegt so gut in Hand und flutscht schneller in die Tasche als kantiger gestaltete Telefone.

Wenig überraschend läuft das OnePlus 12 schnell und flüssig, doch ähnlich wie das Oppo wird es bei langer Belastung unangenehm warm. OnePlus hat ein neues Kühlsystem mit besonders großer Vapor Chamber eingebaut, das die Wärme vom Prozessor nach außen abführen soll. Das tut es auch, allerdings drosselt das OnePlus 12 etwa im 3DMark-Test bei 20 Durchgängen stärker als die versammelte Konkurrenz – Ziel verfehlt.

Wie beim Oppo Find X7 Ultra ist auch bei OnePlus ein großer Bereich des internen Speichers für das Betriebssystem reserviert. Dieses heißt OxygenOS 14 und überzeugt im Test durch unzählige kleine Helferlein und clevere Funktionen, etwa für genauere App-Berechtigungen oder erweiterte Benachrichtigungen. Menüs und Optionen sind sinnvoll und klar strukturiert, die Optik lässt sich weitreichend anpassen.

Neben dem sehr guten Display – mit dezent abgerundeten Längsseiten – gefällt als technisches Detail der Vibrationsmotor. Er ist besonders groß und liefert exaktes und vielfältiges haptisches Feedback auf unterschiedliche Ereignisse. Der Schiebeschalter an der linken oberen Seite schaltet zwischen laut, Vibration und leise. Das ab 900 Euro teure OnePlus 12 schafft zwei Tage ohne Aufladen, wenn man nicht durchgehend am Smartphone hängt. Geladen wird am Kabel mit bis zu 100 Watt und drahtlos mit bis zu 50 Watt, wenn das passende Ladegerät vorhanden ist. Für das Induktionsladegerät verlangt OnePlus 70 Euro, das 100-Watt-Netzteil wird mitgeliefert.

 relativ günstig
 starker Akku
 Kamera mit Schwächen
Preis: 900 Euro bis 1000 Euro






Oppo Find X7 Ultra

Schaffen wir den Pferdefuß gleich aus dem Weg: Das Oppo Find X7 Ultra ist derzeit nur über Importshops in Deutschland erhältlich, mit allen Risiken, die damit einhergehen, etwa hinsichtlich Garantie und Gewährleistung. Nachdem der juristische Streit zwischen Oppo und Nokia ausgefochten ist, steht einer Rückkehr von Oppo-Smartphones nach Deutschland jedoch nichts mehr im Wege. Für ein importiertes Find X7 Ultra muss man gut 1000 Euro zahlen, bei der Einfuhr werden zudem unter Umständen Steuern fällig, die den Preis weiter nach oben treiben.

Die auffällige Optik macht das X7 zu einem echten Hingucker, die zweifarbige Rückseite mischt Glas mit Kunstleder. Das runde Kameramodul wächst über einen halben Zentimeter aus dem Rücken hervor. Es beherbergt gleich vier 50-Megapixel-Kameras: Hauptkamera, Ultraweitwinkel, Dreifach-Tele und quer eingebautes Fünffach-Zoom-Objektiv. Wie beim OnePlus 12 hat Hasselblad an der Kamerasoftware mitgearbeitet und die Farbgestaltung an den Look der eigenen Kameras angepasst. Die Verwandtschaft zum OnePlus 12 sieht man auch an der Platzierung der Bedienelemente, sogar den charakteristischen Schiebeschalter hat Oppo übernommen.

Im Find X7 Ultra steckt ein Qualcomm Snapdragon 8 Gen 3 mit massig Speicher: 16 GByte RAM und 512 GByte interner Speicher. Von letzterem belegt das Betriebssystem allerdings über 50 GByte, das ist mehr als bei allen anderen Android-Smartphones in diesem Vergleich. Das Smartphone rennt durch Benchmarks, Apps und Spiele, wird bei andauernder Belastung allerdings ziemlich warm. Im Dauertest drosselte es die Leistung wärmebedingt stärker als der Rest.

Unser Testgerät kam mit chinesischer Firmware samt tonnenweise Bloatware, die Google-Dienste mussten wir selbst nachinstallieren. Das gelang zwar ohne größere Schwierigkeiten, den zusätzlichen Aufwand möchte man sich jedoch trotzdem lieber ersparen. Oppos Betriebssystem ColorOS ähnelt in der europäischen Variante OxygenOS von Schwestermarke OnePlus und kommt aufgeräumter daher. Sobald Oppo seine Smartphones wieder offiziell in Deutschland vertreibt, dürfte das Find X7 Ultra eine ernstzunehmende Option werden.

 schicke Two-Tone-Optik
 zweites Tele mit viel Zoom
 schwer erhältlich
Preis: ab 1000 Euro

Drei Wünsche frei? Rack, Tower und Microserver!

Server-Wunsch #1: Das perfekte IT-Einstiegs-Bundle!

Man braucht nicht immer eine Wunderlampe – wenn es um leistungsstarke Hardware-Systeme geht, ist Thomas-Krenn Ihr hilfreicher Flaschengeist! Wir reagieren auf Ihr Feedback und erfüllen Ihre Wünsche. Flexibler Rack-Server, kompakter Tower oder lautloser Microserver? Wir legen Windows Server 2022 Essentials mit ins Bundle und liefern Ihnen Ihr ideales System für Ihre ersten Schritte in der Welt der IT-Infrastruktur! Denn bei Thomas-Krenn werden Ihre Server-Wünsche wahr.



Jetzt gewünschtes
Paket sichern:

thomas-krenn.com/wunsch1

**THOMAS
KRENN®**

IT's people business



Samsung Galaxy S24 Ultra

Alles drin und noch mehr – das ist Samsungs Maßgabe beim Ultra. Seit das Top-Modell der S-Klasse das Galaxy Note verdrängt hat, gehört dazu auch der S Pen. Mit dem schlanken Stift, der im Gehäuse mit Titanrahmen versteckt und geladen wird, lässt sich nicht nur schreiben,ritzeln und malen, sondern auch die Kamera auslösen und vieles mehr. Wasser- und staubdicht nach IP68 ist das S24 Ultra trotz des Lochs im Gehäuse. Dessen spitze Ecken piksen beim längeren Halten unangenehm in den Handballen. Mit einer Hülle schafft man Abhilfe, macht das ohnehin riesige Ultra aber noch ein bisschen größer.

Mit 200 Megapixel räumt Samsung den Auflösungsrekord bei den Kameras ab, doch im Alltag reichen die reduzierten 50 oder 12 Megapixel. Zwei Telekameras und ein Ultraweitwinkel bilden einen großen Brennweitenbereich ab, die Expert-Raw-App bietet zahlreiche manuelle Einstellmöglichkeiten. Auf dem enorm hellen, hochauflösenden Display sehen nicht nur die eigenen Fotos toll aus, der Bildschirm ist einer der besten, den man derzeit bei Smartphones finden kann.

Herausstechen kann Samsung auch bei der Softwareversorgung: Sieben Jahre Sicherheitsupdates und ebenso viele neue Android-Versionen findet man sonst nur bei Googles Pixel-Smartphones. Samsungs One UI lässt sich optisch umfangreich an den eigenen Geschmack anpassen. Dass Samsung den vorgeschriebenen Google-Apps in fast allen Fällen eigene Anwendungen zur Seite stellt, erhöht die Auswahl, kann aber auch verwirren.

Nicht alle diese Hersteller-Apps lassen sich rückstandslos entfernen, manche kann man nur deaktivieren. Wer Samsungs neue KI-Funktionen verwenden möchte, kommt allerdings vielfach ohnehin nicht um sie herum. Unter dem Oberbegriff Galaxy AI fasst Samsung allerhand mal mehr, mal weniger nützliche Funktionen zusammen. So lassen sich beispielsweise Telefongespräche simultan übersetzen, der Inhalt von Webseiten zusammenfassen oder Bildbereiche von Fotos auffüllen. Ein Fragezeichen bleibt hinsichtlich der Kosten, denn Galaxy AI ist zunächst nur bis Ende 2025 kostenfrei nutzbar.

- 👆 Vollausstattung plus S Pen
- 👆 sieben Jahre Updates
- 👇 spitze Kanten

Preis: 1150 Euro bis 1500 Euro



Xiaomi 14

Kompakte Smartphones muss man im High End mit der Lupe suchen. Unter den sieben Riesen geht das Xiaomi 14 mit seinem knapp 6,4 Zoll großen Display schon fast als Zwerg durch, und das ist gut so. Das Smartphone ist angenehm handlich, Erwachsene können es mit einer Hand bedienen. Als einziges Smartphone im Vergleich bleibt es zudem unter 200 Gramm Gewicht, wenn auch nur knapp.

Kleiner und leichter heißt in diesem Zusammenhang allerdings nicht gleichzeitig schwächer. Der Snapdragon 8 Gen 3 leistet auch im Xiaomi 14 ganze Arbeit, in Benchmarks und während der alltäglichen Nutzung ist das Smartphone rasant unterwegs. Der Akku schafft einen Tag ohne Aufladen problemlos, im Testfeld bewegen sich die Laufzeiten im Mittelfeld.

Das OLED-Display schafft die klassenüblichen Standards problemlos: 120 Hertz Bildwiederholrate, Helligkeit deutlich über 1000 cd/m², Pixeldichte weit jenseits der 400 dpi. Der Bildschirm ist komplett flach, Xiaomi verzichtet auf gebogene Displayränder. Bei der Kamera hat Leica vor allem an der Farbgestaltung sowie an der Beschichtung der Linsen mitgewirkt. Rekordverdächtigen Zoom bringt das Xiaomi 14 nicht mit, dafür gleich drei 50-Megapixel-Sensoren in Hauptkamera, Tele und Ultraweitwinkel. Vor allem die primäre Kamera macht ansehnliche Fotos mit hohem Detailreichtum.

Xiaomis Android-Spielart heißt HyperOS. Der neue Name beseitigt ein altes Ärgernis jedoch nicht: Xiaomi installiert selbst bei den teuren High-End-Smartphones zahlreiche Apps vor, ob man will oder nicht. Dazu zählen eigene Anwendungen ebenso wie Social-Media- und Shopping-Apps. Vier große Android-Updates und fünf Jahre Sicherheitspatches hätten vor einiger Zeit noch für ein Sonderlob gereicht, mittlerweile ist das für teure Smartphones Durchschnitt, andere bieten längeren Support.

Im Karton steckt, anders als bei vielen Herstellern, noch das komplette Sortiment: Dem 14er gibt Xiaomi ein Schnellladegerät samt USB-C-Kabel sowie eine Silikonhülle mit auf die Reise. Nur die kleine Speichervariante blieb zum Start bei der UVP den symbolischen Euro unterhalb der Tausend-Euro-Schallmauer, doch mittlerweile gibt es selbst die 512-GB-Byte-Variante für relativ günstige 900 Euro.

- 👆 kompakte Größe
- 👆 Netzteil und Hülle
- 👇 viel Bloatware

Preis: 900 Euro

me entdeckten wir auf allen Fotos, wenn wir in die Details zoomten. Gleichwohl fangen die Objektive Landschaften, Gebäude oder Innenräume ein, wie es mit längeren Brennweiten nicht möglich ist. Die spektakulären Resultate entschädigen für die mangelhaften Details.

Im Nachtmodus kombinieren die Smartphones mehrere Aufnahmen mit teils unterschiedlichen Belichtungszeiten zu einem Foto. Diesen kann man explizit auswählen, das ist aber meist nicht nötig, weil in der Regel eine Art „Nachtmodus light“ automatisch aktiv wird, wenn die Lichtverhältnisse es erfordern. Anfangs hellte der Nachtmodus jede Szenerie auf Teufel komm raus auf. Das sah zwar beeindruckend aus, gab aber die nächtliche Stimmung in keiner Weise wieder. Das können die Smartphones mittlerweile besser. Unschöne Lichthöfe, Rot- oder Gelbstiche und fehlende Details sind aber noch nicht ganz ausgeräumt. Die besten Resultate erzielt einmal mehr das Pixel-Telefon in der Runde. Es zeigt auch noch dort saubere Details, wo andere raten müssen. Auch iPhone und Samsung gefallen. Kurios beim Samsung: Überlässt man der Automatik die Aufnahme, wird sie besser. Der dedizierte Nachtmodus hellt das Foto zwar zusätzlich auf, produziert aber mehr Farbfehler, die Fotos sind insgesamt wärmer und weicher. Unschön ins Rote fallen die Honor-Aufnahmen, ins Gelbe die des Xiaomi. Eine Klasse schlechter als der Rest ist in der Nacht die Asus-Kamera. Die Fotos sind in der Automatik künstlich überschärft und sehen vor allem im Nachtmodus wild aus: so als sei jegliches Rauschen glatt gerechnet und das flache Ergebnis nachträglich mit künstlichen Strukturen versehen worden.

Sind das noch Fotos?

Nicht nur während der Aufnahme, sondern auch davor und danach wenden Smartphones allerlei Tricks an, um das beste Foto aufzunehmen. Das Honor Magic6 Pro erkennt Bewegung im Bild und löst automatisch im passenden Moment aus, wenn man das möchte. Im Test war die Trefferquote erfreulich hoch: Springende oder rennende Motive erwischt man so häufiger mit offenen Augen als händisch ausgelöst. Die Pixel-Telefone verbessern die Fotos per KI nach der Aufnahme: So löscht der magische Radierer ungewollte Bildelemente aus Fotos. Verwackelte Gesichter rettet die KI durch Nachschärfen in vielen Fotos. Bei Gruppenfotos erstellt eine Funk-

tion mehrere Einzelbilder und kombiniert diese so, dass in der fertigen Aufnahme alle Personen lächeln und in die Kamera schauen. Per Editor lassen sich ganze Bildelemente innerhalb der Fotos verschieben oder in der Größe ändern.

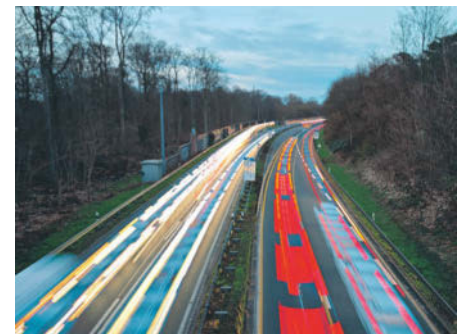
Das iPhone wiederum erkennt die Tiefeninformationen des Motivs und speichert eine Tiefenkarte. So kann man die Aufnahme mit der Fotos-App sofort oder später in ein Porträt mit unscharfem Hintergrund umwandeln oder den Fokus nachträglich von einer Person auf eine andere verschieben. Und die Smartphones sind in der Lage, Langzeitbelichtungen zu imitieren, indem sie mehrere Aufnahmen verrechnen. So sind Lichtspuren von Autos in der Stadt, träumerisch-glatte Flussläufe oder spektakuläre Sternenaufnahmen ganz ohne Stativ möglich, wenngleich gerade bei der Sternenfotografie auch das Smartphone von einem solchen profitiert.

Laufzeitrekorde

Es ist nur wenige Jahre her, da galt ein 4000-mAh-Akku in einem Smartphone als beachtlich. 2024 wagt sich kaum ein Hersteller mehr, sein High-End-Smartphone mit einem Akku mit weniger als 5000 mAh Kapazität auf die Reise zu schicken. Im Prüfstand bleiben nur das iPhone

15 Pro Max und das Xiaomi 14 unterhalb der 5000er-Grenze, aus Gründen. Apple hat mit Soft- und Hardware aus einer Hand das Energiemanagement derart gut im Griff, dass die iPhones schon in der Vergangenheit aus kleinen Akkus große Laufzeiten herauskitzelten. Und im kleinen Xiaomi 14 ist schlicht weniger Platz als im größeren Rest. Dieser beherbergt Akkus mit Kapazitäten zwischen 5000 (Oppo Find X7 Ultra, Samsung Galaxy S24 Ultra) und 5600 mAh (Honor Magic6 Pro).

Damit der Akku nicht nur anfangs lange durchhält, sondern auch nach vielen Ladungen, haben alle Hersteller diverse Möglichkeiten eingebaut, schonend aufzuladen. So kann man das schnelle Laden deaktivieren, die letzten Prozente langsamer füllen, das Laden über Nacht ans Weckerklingeln koppeln oder einfach nur bis 80 Prozent aufladen, um der Batterie den stressigen Zustand des Vollgeladenseins zu ersparen. Besonders viele Optionen hält Asus bereit: Das Zenfone 11 Ultra kann man sogar an den Strom stecken, ohne dass der Akku geladen wird. Dann wird das Smartphone am Akku vorbei mit Strom versorgt. In diesem Modus zog das Smartphone zwischen 0,4 und 13 Watt an der Steckdose, je nachdem wie stark wir es forderten.



Lichtspuren-Fotografie einfach gemacht: Per Software ersetzen die Smartphones Stativ und ND-Filter und errechnen spektakuläre Lichtspuren auch in der Dämmerung, mit sehr unterschiedlichen Ergebnissen. Von oben links im Uhrzeigersinn mit gleichen Lichtverhältnissen im Abstand von zwei Minuten gemachten Fotos von Asus Zenfone 11 Ultra, Honor Magic6 Pro, Xiaomi 14 und Google Pixel 8 Pro.

Auf dem Laufzeitprüfstand ließen die High-End-Smartphones die Rekorde purzeln. Derart hohe Durchschnittswerte über die verschiedenen Szenarien hinweg haben wir in noch keinem größeren Smartphone-Test beobachtet. Waren mehr als 20 Stunden im Video- und Streamingdauerlauf im High-End-Test 2023 noch die Ausnahme, knackte dieses Mal im YouTube-Dauerlauf fast jeder Proband die 20 Stunden. Spielten wir lokal ein Video ab, machte nur das Google Pixel 8 Pro früher schlapp (17,7 Stunden). Diese Fabelzeiten erlaufen die Smartphones nicht nur wegen des großen Tanks, auch die starken Prozessoren spielen eine Rolle. Ein lokal gespeichertes HD-Video oder einen YouTube-Stream spielen sie im Schlaf ab, oder präziser: auf einem der Energiesparkerne.

Es braucht schon Spiele, Benchmarks oder Videomaterial in sehr hoher Qualität, um die SoCs aus der Reserve zu locken. Beim Tensor-Chip im Pixel 8 Pro gelingt das noch recht zuverlässig. Im Spiele- und 4K-Video-Test bricht es auf Werte unter zehn Stunden ein. Das iPhone und die mit

Snapdragon 8 Gen3 bestückten Smartphones schaffen in jedem Testszenario mindestens elf Stunden. Besonders widerstandsfähig erwies sich das Honor Magic6 Pro, das selbst im Spieletest 26,5 Stunden durchhielt, länger als jedes andere Smartphone, das unsere Tests durchlaufen hat. Mit über 22 Stunden landete das OnePlus 12 auf dem zweiten Platz. Verschiedene Stromspareinstellungen können die Laufzeiten der Geräte noch weiter verlängern, doch auch so halten sie bei moderatem Gebrauch meist zwei Tage mit einer Akkufüllung durch.

Mit Ausnahme von OnePlus, Oppo und Xiaomi liefern alle Hersteller ihre Smartphones ohne Netzteil aus. An einem PowerDelivery-Netzteil mit einer maximalen Ladeleistung von 100 Watt haben sie jeweils etwa eine Stunde für eine Ladung von 0 auf 100 Prozent gebraucht. Die maximale Leistung des Netzteils rief dabei kein Smartphone ab. Zumindest die chinesischen Hersteller tanken am eigenen Netzteil schneller, OnePlus- und Xiaomi-Smartphone sind in weniger als 30

Minuten befüllt. Apple, Google und Samsung lassen es traditionell etwas gemüthlicher angehen. Ohne Kabel laden alle mit mindestens 15 Watt, die Qi maximal erreicht. Auf optional erhältlichen, proprietären Ladeschalen laden OnePlus-, Oppo- und Xiaomi-Handy mit 50, das Honor gar mit 66 Watt.

Nachdem sich 5G längst als Mobilfunkstandard etabliert hat, steht 2024 ein Upgrade an, das weniger praktische Auswirkungen für Smartphones hat: Die ersten Geräte funken gemäß Wi-Fi 7. Im Test beherrschen das alle Androiden auch im bei Wi-Fi 7 nicht garantierten 6-GHz-Band, während das iPhone Wi-Fi 6E versteht, also Wi-Fi 6 inklusive 6 GHz. Unter den Androiden wiederum ist das Pixel 8 Pro das einzige, das kein extrabreites 320-MHz-Signal nutzt, das auf kurze Distanzen einen Durchsatz bis knapp unter 3 Gbit/s erlaubt. Kein Beinbruch, denn selbst Wi-Fi 6E ist locker schnell genug, um auch große Dateien vom Smartphone zügig aufs heimische NAS oder in die Cloud zu verschieben.

High-End-Smartphones 2024

Modell	Apple iPhone 15 Pro Max	Asus Zenfone 11 Ultra	Google Pixel 8 Pro	Honor Magic6 Pro
Betriebssystem / Security Level / Updates bis	iOS 17 / 17.1.4 / k.A.	Android 14 / Dezember 2023 / Android 16, Februar 2028	Android 14 / März 2024 / Android 21, Oktober 2030	Android 14 / Februar 2024 / Android 18, Februar 2029
Ausstattung				
Prozessor / Kerne × Takt / GPU	Apple A17 Pro / 2 × 3,78 GHz, 4 × 2,11 GHz / A17 Pro	Qualcomm Snapdragon 8 Gen3 / 1 × 3,3 GHz, 3 × 3,2 GHz, 2 × 3 GHz / Adreno 750	Google Tensor G3 / 1 × 3 GHz, 4 × 2,45 GHz, 4 × 2,15 GHz / Mali-G715	Qualcomm Snapdragon 8 Gen3 / 1 × 3,3 GHz, 3 × 3,2 GHz, 2 × 3 GHz / Adreno 750
RAM / Flash-Speicher / Karten-slot	8 GByte / 1024 GByte (1010 GByte) / –	16 GByte / 512 GByte (490 GByte) / –	12 GByte / 128 GByte (110 GByte) / –	12 GByte / 512 GByte (483 GByte) / –
5G / LTE / physische SIM-Plätze / eSIM / SAR-Wert ²	✓ / ✓ / 1 × Nano-SIM / ✓ / 0,98 W/kg	✓ / ✓ / 2 × Nano-SIM / – / 1,441 W/kg	✓ / ✓ / 1 × Nano-SIM / ✓ / 0,84 W/kg	✓ / ✓ / 2 × Nano-SIM / ✓ / 0,82 W/kg
WLAN (Antennen) ¹ / Bluetooth / NFC / Kompass / Standort	Wi-Fi 6E (2) / 5.3 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo	Wi-Fi 7 (2) / 5.4 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo	Wi-Fi 7 (2) / 5.3 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo	Wi-Fi 7 (2) / 5.3 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo
USB / Kopfhörer / Finger-abdruckscanner	USB-C 3.1, OTG, DP / – / – (Face ID)	USB-C 2.0, OTG, kein DP / ✓ / ✓	USB-C 3.2, OTG, DP / – / ✓	USB-C 3.2, OTG, DP / – / ✓
Akku / Drahtlosladen	4422 mAh / ✓	5500 mAh / ✓	5050 mAh / ✓	5600 mAh / ✓
Abmessungen / Gewicht / Schutzart	16,1 × 7,8 × 0,8 ... 1,06 cm / 222 g / ✓ (IP68)	16,4 × 7,7 × 0,9 ... 1,1 cm / 224 g / ✓ (IP68)	16,3 × 7,7 × 0,9 ... 1,1 cm / 213 g / ✓ (IP68)	16,3 × 7,6 × 0,9 ... 1,1 cm / 235 g / ✓ (IP68)
Display				
Größe / Technik / Auflösung (Punktdichte) / Bildrate	6,7 Zoll / OLED / 2796 × 1290 Pixel (460 dpi) / 1–120 Hz	6,8 Zoll / OLED / 2400 × 1080 Pixel (388 dpi) / 1–120, 144 Hz	6,7 Zoll / OLED / 2992 × 1344 Pixel (487 dpi) / 1–120 Hz	6,8 Zoll / OLED / 2800 × 1280 Pixel (453 dpi) / 1–120 Hz
Helligkeitsregelbereich / Ausleuchtung	1 ... 1658 cd/m ² / 98 % Ausleuchtung	5,56 ... 1830 cd/m ² / 95 % Ausleuchtung	1,8 ... 1576 cd/m ² / 89 % Ausleuchtung	1,84 ... 1495 cd/m ² / 96 % Ausleuchtung
Kamera				
Hauptkamera	48 MP, f/1,78, mit OIS, 24 mm	50 MP, f/1,9, mit OIS, 24 mm	50 MP, f/1,7, mit OIS, 24 mm	50 MP, f/1,4 + 2, mit OIS, 24 mm
Telekamera	12,2 MP, f/2,8, mit OIS, 120 mm	32 MP, f/2,4, mit OIS, 65 mm	48 MP, f/2,8, mit OIS, 113 mm	180 MP, f/2,6, mit OIS, 62 mm
zweite Telekamera	–	–	–	–
Ultraweitwinkelkamera	12,2 MP, f/2,2, ohne OIS, 13 mm	13 MP, f/2,2, ohne OIS, 13 mm	48 MP, f/1,95, ohne OIS, 14 mm	50 MP, f/2, ohne OIS, 13 mm
Frontkamera	12,2 MP, f/1,9, mit OIS, 23 mm	32 MP, f/2,5, ohne OIS, 22 mm	10 MP, f/2,2, ohne OIS, 20 mm	50 MP, f/2, ohne OIS, 21 mm
Bewertungen				
Performance / Akku	⊕⊕ / ⊕	⊕⊕ / ⊕	⊕ / ○	⊕⊕ / ⊕⊕
Display / Kamera	⊕⊕ / ⊕⊕	⊕ / ○	⊕⊕ / ⊕⊕	⊕ / ⊕
Software / Ausstattung	⊕⊕ / ⊕	○ / ⊕	⊕⊕ / ⊕	⊕ / ⊕
Preis	1200 (256 GByte) bis 1800 € (1 TByte)	1100 (256 GByte) bis 1200 € (512 GByte)	900 (128 GByte) bis 1200 € (512 GByte)	1100 €
✓ vorhanden – nicht vorhanden k. A. keine Angabe ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht				

Updatemeister und Schluderer

Wer viel Geld für ein Smartphone ausgibt, will auch lange etwas davon haben. Damit das so ist, braucht es nicht nur beste Hardware-Voraussetzungen, sondern auch lange Updates. Ein gutes Jahr, bevor die Updatevorgaben der EU greifen, üben sich die ersten Hersteller an der Pflichterfüllung. Fünf Jahre ab Verkaufsende eines Smartphones müssen Hersteller nach EU-Vorgaben Updates liefern. Für einen ähnlichen Zeitraum, jeweils sieben Jahren ab Verkaufsstart, versprechen Google und Samsung Updates. Damit erhalten Pixel 8 Pro und das etwas später erschienene S24 Ultra bis Oktober 2030 respektive Januar 2031 Updates. Immerhin fünf Jahre Patches wollen Honor, OnePlus, Oppo und Xiaomi liefern. Nur vier Jahre Patches und zwei Androidversionsupdates heißt es bei Asus – das ist angesichts des Preises und der kommenden Verpflichtung deutlich zu wenig. Google und Samsung halten selbst ihre Mittelklasse-Smartphones länger auf aktuellem Stand. Apple derweil macht

keine Angaben, wie lange es seine Smartphones mit Softwareupdates versorgen will. Ein Blick auf das aktuelle Portfolio gibt eine Orientierung: Die ältesten iPhones, die das aktuelle iOS 17 erhalten haben, sind die 2018 erschienenen XR und XS, die nach unternehmensnahen Quellen auch noch das kommende iOS 18 erhalten werden.

Fazit

Alles, was man braucht und einiges mehr: Den Luxusanspruch erfüllen alle Smartphones im Test. Welches also wählen? Die Frage, ob iOS oder Android lässt sich nicht anhand der Hardware beantworten, zu nah beieinander liegen die Geräte. Man kommt in beiden Welten das Beste vom Besten. Unter den Androiden glänzen Google und Samsung mit dem längsten Support. Der Stift, die längere Akkulaufzeit und der schnellere Prozessor sprechen für das S24 Ultra. Das pure Android, Pixel-exklusive Android-Features und der günstigere Preis sind Argumente für das Pixel 8 Pro. Einloggen per Gesichts- und Finger-

abdruckscan kombiniert das Honor Magic6 Pro mit den längsten Laufzeiten. Das Zenfone 11 Ultra drosselt unter hoher Last am wenigsten und erreicht in Spielen die extrem schnelle Bildwiederholrate von 144 Hertz. Das volle High-End-Programm packt Xiaomi mit dem 14 in das handlichste Gehäuse. Oppo stapelt gleich vier 50-Megapixel-Kameras im Find X7 Ultra, das OnePlus 12 glänzt mit starkem Akku und cleverer Software.

Im iPhone-Universum wiederum unterscheidet sich die 15. Generation vor allem aufgrund von USB-C von den Vorgängern. Den langen Support, über dessen genauen Zeitraum sich Apple wie gehabt ausschweigt, hat sie mit diesen gemein. Erstmals gibt es jetzt die 48-Megapixel-Kamera auch für die Nicht-Pro-Modelle. Das Topmodell Pro Max ist das beste Kamera-iPhone, das es je gab, erstmals mit einem Fünffach-Tele. Wer von iPhone 12 oder älter umsteigt, freut sich über deutlich bessere Kameras, Prozessoren und Displays, ganz gleich, welches 15er-Modell man wählt. (rbr@ct.de) 

OnePlus 12	Oppo Find X7 Ultra	Samsung Galaxy S24 Ultra	Xiaomi 14
Android 14 / Februar 2024 / Android 18, Januar 2029	Android 14 / Februar 2024 / Android 18, Januar 2029	Android 14 / März 2024 / Android 21, Januar 2031	Android 14 / Januar 2024 / Android 18, Februar 2029
Qualcomm Snapdragon 8 Gen3 / 1 × 3,3 GHz, 3 × 3,2 GHz, 2 × 3 GHz / Adreno 750	Qualcomm Snapdragon 8 Gen3 / 1 × 3,3 GHz, 3 × 3,2 GHz, 2 × 3 GHz / Adreno 750	Qualcomm Snapdragon 8 Gen 3 for Galaxy / 1 × 3,4 GHz, 3 × 3,2 GHz, 2 × 3 GHz / Adreno 750	Qualcomm Snapdragon 8 Gen3 / 1 × 3,3 GHz, 3 × 3,2 GHz, 2 × 3 GHz / Adreno 750
16 GByte / 512 GByte (455 GByte) / –	16 GByte / 512 GByte (455 GByte) / –	12 GByte / 256 GByte (229 GByte) / –	12 GByte / 512 GByte (491 GByte) / –
✓ / ✓ / 2 × Nano-SIM / ✓ / 1,18 W/kg	✓ / ✓ / 2 × Nano-SIM / – / k. A.	✓ / ✓ / 2 × Nano-SIM / ✓ / 1,056 W/kg	✓ / ✓ / 2 × Nano-SIM / ✓ / 0,376 W/kg
Wi-Fi 7 (2) / 5.4 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo	Wi-Fi 7 (2) / 5.4 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo	Wi-Fi 7 (2) / 5.3 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo	Wi-Fi 7 (2) / 5.4 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo
USB-C 3.2, OTG, DP / – / ✓	USB-C 3.2, OTG, DP / – / ✓	USB-C 3.2, OTG, DP / – / ✓	USB-C 3.2, OTG, DP / – / ✓
5400 mAh / ✓	5000 mAh / ✓	5000 mAh / ✓	4610 mAh / ✓
16,4 × 7,6 × 0,9 ... 1,2 cm / 220 g / ✓ (IP65)	16,4 × 7,6 × 1 ... 1,5 cm / 221 g / ✓ (IP68)	16,2 × 7,9 × 0,9 ... 1,1 cm / 232 g / ✓ (IP68)	15,3 × 7,2 × 0,8 ... 1 cm / 196 g / ✓ (IP68)
6,8 Zoll / OLED / 3120 × 1440 Pixel (505 dpi) / 1–120 Hz	6,8 Zoll / OLED / 3120 × 1440 Pixel (505 dpi) / 1–120 Hz	6,8 Zoll / OLED / 3120 × 1440 Pixel (505 dpi) / 1–120 Hz	6,4 Zoll / OLED / 2670 × 1200 Pixel (458 dpi) / 1–120 Hz
1,89 ... 1088 cd/m² / 94 % Ausleuchtung	1,97 ... 1557 cd/m² / 93 % Ausleuchtung	0,75 ... 1595 cd/m² / 94 % Ausleuchtung	2,1 ... 1350 cd/m², 98 % Ausleuchtung
50 MP, f/1,6, mit OIS, 23 mm	50 MP, f/1,8, mit OIS, 23 mm	200 MP, f/1,7, mit OIS, 24 mm	50 MP, f/1,6, mit OIS, 23 mm
64 MP, f/2,6, mit OIS, 70 mm	50 MP, f/4,3, mit OIS, 135 mm	50 MP, f/2,4, mit OIS, 111 mm	50 MP, f/2, mit OIS, 75 mm
–	50 MP, f/2,6, mit OIS, 67 mm	12 MP, f/2,4, mit OIS, 67 mm	–
48 MP, f/2,2, ohne OIS, 14 mm	50 MP, f/2, ohne OIS, 14 mm	10 MP, f/2,2, ohne OIS, 13 mm	50 MP, f/2,2, ohne OIS, 14 mm
32 MP, f/2,4, ohne OIS, 21 mm	32 MP, f/2,4, ohne OIS, 21 mm	12 MP, f/2,2, ohne OIS, 25 mm	32 MP, f/2, ohne OIS, 22 mm
⊕⊕ / ⊕	⊕⊕ / ⊕	⊕⊕ / ⊕	⊕⊕ / ⊕
⊕ / ○	⊕ / ⊕	⊕⊕ / ⊕	⊕ / ⊕
⊕⊕ / ⊕	○ / ⊕	⊕⊕ / ⊕⊕	○ / ⊕
900 € (256 GByte) bis 1000 € (512 GByte)	ab 1000 € als Import	1150 (256 GByte) bis 1500 € (1 TByte)	900 €

Fatale Fehlkonfiguration

Datenleck bei Anbieter von Kita-App „Stay Informed“

Wegen der Fehlkonfiguration eines Webserver standen beim Kita- und Schul-App-Betreiber Stay Informed eine Menge schützenswerter Dateien offen im Netz, eventuell über mehrere Jahre. Auf unseren Hinweis reagierte das Unternehmen schnell und transparent, dürfte aber noch lange mit den Folgen des Datenlecks zu tun haben.

Von Holger Bleich
und Sylvester Tremmel

Über die App „Stay Informed“ können Kitas, Schulen und Pflegeeinrichtungen mit Eltern oder Angehörigen kommunizieren. Nach Angaben des Freiburger Herstellers Stay Informed GmbH setzen derzeit mehr als 11.000 Einrichtungen in Deutschland die App ein. Sie geben darin beispielsweise Termine bekannt oder holen Informationen von Erziehungsberechtigten ein. Eltern können ihre Kinder krankmelden und über die integrierte Chatfunktion mit der Einrichtung kommunizieren.

Der Hersteller gibt an, dem Prinzip der Datensparsamkeit zu folgen und wirbt mit einem „Team aus IT-SicherheitsexpertInnen und DatenschützerInnen“, das die Weiterentwicklung der Software begleite. Klingt hervorragend: Eltern und Kitas bekommen eine praktische App und um den Datenschutz kümmern sich Experten. Zitat eines Schulleiters aus einer Werbebroschüre des Unternehmens: „Datenschutz ist ein heikles Thema. Sehr, sehr aufwendig. Ich habe bei Ihrer App damit jedoch gar nichts mehr zu tun. Sie nehmen mir diese ganze Arbeit ab.“

Das war leider eine Fehleinschätzung. Ein anonymer Hinweisgeber informierte c't Mitte März über ein massives Datenleck: Ein Webserver von Stay Informed

war frei zugänglich und erlaubte den Download einer großen Menge an Daten von Nutzern der App. Man musste nicht einmal die Dateinamen kennen oder erraten, denn der Server generierte auch „Directory Listings“, zeigte also alle verfügbaren Dateien übersichtlich an.

Konkret fanden sich auf dem Server vier Arten von Daten, darunter 16.000 Nutzeravatare aus der Chatfunktion der App. Teilweise handelte es sich dabei um Fotos von Kindern oder Eltern. Außerdem hielt der Server PDF-Anhänge von Chatnachrichten vor, die Einrichtungen an Eltern geschickt hatten. (Die Nachrichten an sich offenbarte der Server nicht.) Ob es sich dabei um personenbezogene oder anderweitig schützenswerte Daten handelt, hängt im Einzelfall vom Inhalt des jeweiligen Anhangs ab. Drittens enthielt der Server digitale Unterschriften der Eltern, die immerhin verschlüsselt waren.

Schließlich fanden sich auf dem Server auch noch knapp 1500 CSV-Dateien mit tabellarischen Daten. Nach Angaben von Stay Informed handelte es sich um fehlgeschlagene Importe, mit denen Einrichtungen ihren Nutzerstamm einpflegen wollten; fehlerhafterweise waren diese Daten nicht gelöscht worden. Von diesem Aspekt des Lecks waren etwa 15 Prozent der Einrichtungen, die Stay Informed nutzen, betroffen. Diesen Teil traf es besonders hart: Neben Namen, Geburtsdaten und Anschriften – auch von Minderjähri-

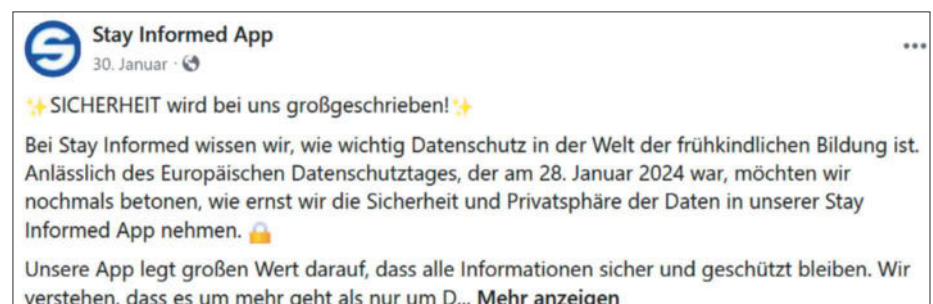
gen – enthielten die Dateien teilweise auch Informationen über Herkunftsländer, Impfungen, Konfessionen, Erziehungsberechtigte, Notfallkontakte, Klassenlehrer und vieles mehr.

Der Server lieferte all die Daten nicht nur ohne Authentifizierung, sondern auch ohne Transportverschlüsselung per HTTP aus, kurioserweise auf Port 443, also genau dem Port, der eigentlich für verschlüsseltes HTTPS vorgesehen ist. Weil auch HTTPS keine Nutzerauthentifizierung erzwingt, hätte eine Transportverschlüsselung das Datenleck aber nicht verkleinert. Laut Hersteller bestand es „frühestens seit dem 20.10.2021 und spätestens seit dem 18.08.2023“. Egal ob verschlüsselt transportiert oder nicht: Dass die Daten so lange für alle Öffentlichkeit auffind- und abrufbar waren, wirft kein gutes Licht auf die „regelmäßigen Pentests“, mit denen Stay Informed wirbt.

Die Zugriffs-Logfiles für den Webserver reichen laut Stay Informed nur 14 Tage in die Vergangenheit zurück, sodass für fast den ganzen Zeitraum offen bleibt, ob außer im Rahmen unserer Recherche und der unseres anonymen Hinweisgebers auch von anderen Personen auf die Daten zugegriffen wurde.

Umgehende Reaktion

Nachdem c't das Unternehmen über die Lücke informiert hatte, reagiert es umgehend: Es behob das Problem binnen zwei



Auf seiner Website und dem Facebook-Auftritt wirbt Stay Informed mit Sicherheit und Schutz der Privatsphäre.

Stunden, meldete den Vorfall beim zuständigen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) in Baden-Württemberg und begann nach zwei Tagen, die betroffenen Einrichtungen und deren Träger zu informieren. Besonders erfreulich: Über ein kontinuierlich wachsendes FAQ-Dokument auf der Website hielt Stay Informed auch die Öffentlichkeit informiert und betonte die eigene Verantwortung für den Vorfall.

Gehemmt wurde diese Transparenz und Hilfsbereitschaft allerdings von der rechtlichen Organisation der App-Infrastruktur: Wie viele andere Software-as-a-Service-Anbieter fungiert Stay Informed als Datenverarbeiter, der im Auftrag seiner Kunden arbeitet. Mit jedem dieser Kunden habe man deshalb einen Auftragsverarbeitungsvertrag geschlossen, erklärte das Unternehmen. Die Kunden sind allerdings nicht die Eltern, Kinder und Pädagogen, deren Daten die App verwaltet, sondern die Kitas und Schulen beziehungsweise deren Träger.

Datenschutzrechtlich betrachtet ist in diesem Konstrukt nicht die Stay Informed GmbH für die Datenverarbeitung verantwortlich. Stattdessen sind es die Einrichtungen oder ihre Träger. Deshalb mussten all diese Kunden das Datenleck separat bei der jeweils zuständigen Landesdatenschutzbehörde melden und entscheiden, welche Eltern und Erzieher sie informieren mussten. Doch nicht nur das: Möchten Eltern oder Erzieher von ihren Betroffenenrechten Gebrauch machen, sind auch hier die Einrichtungen und Träger Ansprechpartner. Sie müssen also beispielsweise Auskunftersuchen fristgerecht bearbeiten und Löschersuchen nachkommen.

In der Praxis können die Einrichtungen selbst bei ausreichender technischer Kompetenz wenig mehr tun, als Anfragen an Stay Informed weiterzugeben und in umgekehrter Richtung die Antworten des Unternehmens weiterzuleiten. Verantwortlich, haftbar und potenziell schadensersatzpflichtig sind sie selbst. Zu Redaktionsschluss rollte die Welle der Meldungen gerade erst los, auf Anfrage von c't berichteten alle Datenschutzbehörden zusammen von gut 650 Eingaben von Stay-Informed-Kunden.

Schwerpunkt Baden-Württemberg

Immerhin dürfen diese darauf hoffen, keinen allzu großen Ärger zu bekommen: Die Landesdatenschutzbehörden gaben



Manche kommunalen Träger (hier die Stadt Balingen) haben als Kunden von Stay Informed umgehend die Betroffenen öffentlich informiert.

uns größtenteils zu verstehen, dass sie erst einmal abwarten wollen, was die Untersuchungen des LfDI Baden-Württembergs gegen Stay Informed ergeben. Gegenüber c't gaben die meisten Landesbeauftragten an, bislang keine Untersuchungen gegen Einrichtungsträger in ihrem Bundesland eingeleitet zu haben. Eventuelle Geldbußen kann eine Aufsichtsbehörde auch gegen Auftragsverarbeiter verhängen, sie muss nicht unbedingt den nach der DSGVO Verantwortlichen angehen. Erwartbar ist, dass sich die Untersuchungen auf die technisch-organisatorischen Maßnahmen sowie das Löschkonzept von Stay Informed konzentrieren (Art. 32 DSGVO).

Einige Behörden betonten allerdings gegenüber c't, dass sie mitunter mindestens Rückfragen an die Einrichtungsträger hätten, auch weil die Ausführlichkeit der Meldungen sowie die Risikobewertungen der Einrichtungsträger sehr unterschiedlich ausfielen. Am deutlichsten wurde ein Sprecher des Bayerischen Landesbeauftragten für den Datenschutz: Es sei stichprobenweise mit vertieften Prüfungen zu rechnen, auch, um gegebenenfalls präventive Handlungsempfehlungen ableiten zu können. Ob diese Maßnahmen ausreichen, sei derzeit noch nicht abschätzbar.

Bei vielen Kunden sind Verunsicherung und wohl auch Frust groß. Erste

Konkurrenten haben Wechselservices für Stay-Informed-Kunden eingerichtet, und Anwaltskanzleien bieten an, Schadenersatzansprüche zu prüfen. Ob man bei einem anderen Anbieter aber wirklich besser aufgehoben ist, steht auf einem anderen Blatt. Stay Informed hat bei der Servereinrichtung deutlich geschlampt, aber auf den Datenschutzvorfall immerhin schnell und transparent reagiert – leider absolut keine Selbstverständlichkeit. (syt@ct.de) **ct**



Viele c't-Investigativ-Recherchen sind nur möglich dank anonymer Informationen von Hinweisgebern.

Wenn Sie Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns Hinweise und Material zukommen lassen. Nutzen Sie dafür bitte unseren anonymen und sicheren Briefkasten.

<https://heise.de/investigativ>

Master of Pwn

Wie findet man Sicherheitslücken in gleich vier Browsern, Manfred Paul?

Beim diesjährigen internationalen Hacker-Wettbewerb Pwn2Own hat Manfred Paul den ersten Platz belegt. Er schaffte es nicht nur, die Webbrowser Safari, Chrome und Edge zu hacken, sondern auch die Sandbox von Mozillas Firefox. Wir haben mit ihm über seine Motivation und sein Vorgehen gesprochen.

Von Marie-Claire Koch

c't: Herr Paul, Sie haben Sicherheitslücken in Edge, Chrome, Safari und Firefox entdeckt und auch gleich Wege gefunden, sie auszunutzen. Wie viel Zeit haben Sie dafür investiert?

Manfred Paul: Schwer zu sagen. Das ist von Target zu Target unterschiedlich. Am meisten Zeit verwende ich darauf, Dinge zu suchen und nichts zu finden. Verschwendet ist die Zeit aber nicht. Man lernt dazu und versteht Dinge, die dabei helfen können, später vielleicht doch etwas zu finden. Es ist aber zu einem gewissen Grad auch Glückssache.



		PRIZE \$	POINTS
1	Manfred Paul	\$202,500	25
2	Synacktiv	\$200,000	20
3	Seunghyun Lee	\$145,000	15
4	Theori	\$135,000	14
5	STAR Labs SG	\$95,000	13

Manfred Paul hat Sicherheitslücken in vier großen Browsern gefunden und beim diesjährigen Pwn2Own-Hacking-Wettbewerb den ersten Platz erreicht.

c't: Was dauert länger, eine Lücke zu finden oder sie auszunutzen?

Paul: Das ist verschieden. Für mich nimmt auf jeden Fall das Bug-Suchen den Großteil der Zeit in Anspruch. Es kommt auf die Methode an. Ich schaue mir oft den Code an und versuche auf diese Weise, Bugs zu finden. Aber das ist nur meine bevorzugte Arbeitsweise. Andere arbeiten mehr mit automatischen Tools. Die zum Laufen zu bringen kostet aber auch Zeit. Natürlich geht es schneller, wenn man schon Erfahrung hat.

c't: Haben Sie ein Rezept, nach dem Sie vorgehen?

Paul: Es ist viel Intuition dabei. Ich schaue mir tendenziell die Teile vom Code an, bei denen ich denke: „Wenn ich da etwas finde, dann ist das schwerwiegend“. Ich achte stark auf den Just-in-Time-Compiler, also auf Code, der zur Laufzeit neuen, optimierten Maschinencode erzeugt.

c't: Wie sieht Ihre Vorarbeit aus?

Paul: Da bin ich eher unorganisiert. Andere gehen strukturierter vor und lesen etwa vergangene Exploits nach. Ich will lieber unbefangener an die Sache herangehen. Wenn ich weiß, was schon alles gefunden wurde, habe ich das Gefühl, „Der Code wird jetzt schon irgendwie seine Richtigkeit haben“. Dann kann ich mich nicht mehr kritisch damit auseinandersetzen.

c't: Gibt es einen Exploit, auf den Sie besonders stolz sind?

Paul: Alle hatten ihre Herausforderungen. Firefox war der einzige Browser, bei dem ich auch die große Sandbox angegriffen habe. Die bietet zusätzlichen Schutz, den mein Exploit ausgehebelt hat, was ihn auch gerade für Endnutzer relevant macht.

c't: Sie haben mit Ihrer Arbeit mal eben Millionen Euro verbrannt. Was ist Ihre Motivation dafür?

Paul: Ich weiß, ich könnte mehr Geld verdienen, wenn ich meine Funde an den Höchstbietenden verkaufen würde. Aber ich will nicht dafür verantwortlich sein, dass Angreifer Schaden anrichten. Daher freut es mich auch wirklich, wenn Lücken anschließend gepatcht werden. Software sollte für alle sicher sein. Zum Beispiel die Firefox-Schwachstelle wurde im Rekordtempo beseitigt und das Update kam schnell heraus.

c't: Wie kamen Sie zur IT-Sicherheit?

Paul: Mein Einstieg in das Thema IT-Security waren sogenannte Capture-the-Flag-Wettbewerbe. Das sind Hacking-Turniere, bei denen man im Code einer Software absichtlich versteckte Bugs finden soll. Dabei habe ich viel gelernt. Ich habe ein Team, mit dem ich immer noch gelegentlich spiele. Nützlich war auch mein Mathematikstudium. Es macht sich vor allem in meiner Methodik bemerkbar: Ich versuche oft, quasi mental einen Beweis zu finden, dass Software korrekt ist.

c't: Obwohl Experten es fordern, wurde der Hackerparagraf bisher nicht abgeschafft. Hatten Sie zu Beginn Ihrer Laufbahn Sorge, mit dem Gesetz in Konflikt zu kommen?

Paul: Da gibt es eine große Schieflage, was die Gesetze angeht. Für die IT-Security-Community ist es eine Schande, zu sehen, dass vor Kurzem wieder jemand verurteilt wurde [1], der eine Sicherheitslücke gemeldet hatte. Ich hoffe, dass sich die Gesetzeslage ändert, damit man rechtssicher Lücken melden kann.

Auch das Thema „Reverse Engineering“ ist in Deutschland rechtlich schwierig. Da kann man als Sicherheitsforscher schon einmal mit dem Urheberrecht in Konflikt kommen. Für mich bestand bisher weniger die Gefahr, weil ich mich primär mit Open-Source-Software beschäftigt habe. Meine ersten Sicherheitslücken habe ich im Linux-Kernel gefunden. Das ist ja keine Infrastruktur, die jemandem gehört. (kst@ct.de) **ct**

Literatur

- [1] Sylvester Tremmel, Unversehens kriminell, „Hackerparagrafen“ und warum sie problematisch sind c't 5/2024, S. 32

Pwn2Own-Website, weitere Berichterstattung: ct.de/y64t

Geballtes Nerd-Wissen!

Spannendes aus Forschung und Technik



Dieses c't-Sonderheft hilft Ihnen, mit nerdigem Fachwissen zu glänzen. Es bietet die perfekte Mischung aus tiefgründigem Wissen und kurzweiliger Unterhaltung. Ein Muss für jeden Technik- und IT-Fan!

- Künstliche Nase analysiert Gasmoleküle
- So erkennt KI Emotionen
- Daten des James-Webb-Teleskops interaktiv auswerten
- Historische Verschlüsselung neu programmiert
- Sicher oder nicht? Security-Mythen im Faktencheck

JETZT
BESTELLEN!



Heft für 14,90 € • PDF für 12,99 € • Heft + PDF 19,90 €



shop.heise.de/ct-knowhow24



Verhagelte Ostern

Perfide Hintertür in der Softwarebibliothek xz

In letzter Sekunde ist eine komplexe Hintertür in der Softwarebibliothek xz Utils aufgefallen, die desaströse Auswirkungen für einen großen Teil aller per SSH erreichbaren Rechner gehabt hätte. Die Suche nach Urhebern und besseren Schutzmaßnahmen läuft auf Hochtouren.

Von Sylvester Tremmel

Am 29. März, Karfreitag, riss der Datenbankentwickler Andres Freund die Open-Source- und IT-Security-Communities jäh aus dem Osterwochenende. Ihm waren ein paar Merkwürdigkeiten an aktuellen Versionen der Bibliothek liblzma aus dem Projekt xz Utils aufgefallen. Seine anschließenden Nachforschungen ergaben, dass in der Bibliothek eine höchst aufwendig verborgene Hintertür lauerte. Wer auch immer die Backdoor kontrollierte, er hätte weltweit unzählige Rechner kompromittieren können, wären diese xz-Versionen in die Paketquellen verbreiteter Linux-Distributionen gelangt und per Update verteilt worden. In zahlreiche Beta-, Unstable- und Rolling-Release-Repositories waren sie bereits eingeflossen, aber noch nicht die Quellen üblicher Server-Linuxe. Die Warnung von Freund kam gerade noch rechtzeitig.

Das ist sehr nahe am Super-GAU: xz findet sich auf den meisten Linux-Systemen und auf macOS-Rechnern, die die Paketverwaltung Homebrew nutzen, weil es zur Komprimierung von Softwarepaketen, Kernelabbildern, Archiven und anderem eingesetzt wird. Schlimmer noch, die Hintertür wurde aktiv, wenn liblzma vom OpenSSH-Daemon sshd geladen wurde, und zwar noch vor der Nutzerauthentifizierung. SSH ist in der Unix-Welt omnipräsent, um aus der Ferne auf Systeme zuzugreifen.

Im Verlauf des Osterwochenendes mutierte die Security-Community zum

laut brummenden Bienenstock, weil gleichzeitig Nachforschungen zum Urheber der Hintertür, der Methode ihrer Platzierung und ihrem eigentlichen Zweck angestellt wurden. Projekte, die xz nutzen, wechselten auf ältere, vermutlich nicht betroffene Versionen der Software; Linux-Distributionen veröffentlichten Sicherheitsupdates und verschoben Releases, um massenhaft Pakete neu zu bauen; das Versagen bestehender Kontrollmechanismen wurde analysiert und neue wurden vorgeschlagen. All dies dauert auch zu Redaktionsschluss noch an (siehe ct.de/ywk4).

Gut versteckt

Grob gesagt modifizierte der Angreifer einen Schritt beim Bau des Softwarepakets xz, um die Hintertür in das Paket zu schmuggeln. Besonders perfide: Der notwendige Code befand sich nicht direkt im Git-Repository des Projekts, wo er interessierten Programmierern leichter aufgefallen wäre. Stattdessen steckte ein erster kleinerer Teil ausschließlich in den Quellcode-Archiven (Tarballs), die das Projekt zur Verfügung stellt, und der zweite größere Teil, mehrfach verschleiert, im binären Datenstrom von zwei Archiven, die zu den Softwaretests des Projekts gehören.

Diverse Prüfungen im Code des Angreifers stellten sicher, dass die Hintertür nur eingebaut wurde, wenn man ein Softwarepaket für DEB- oder RPM-basierte Linux-Distributionen konstruierte. Und auch eine verseuchte xz-Version prüfte allerlei Bedingungen, um sich in aller Regel normal und unauffällig zu verhalten. Vor allem musste sie von sshd geladen

werden, was der OpenSSH-Daemon eigentlich nicht tut. Allerdings lud ein verbreiteter Patch für OpenSSH systemd samt dessen Abhängigkeiten; über diesen Umweg gelangte liblzma samt der Hintertür in den Kontext von sshd. Einen so verseuchten SSH-Daemon hätten Angreifer jederzeit übers Netz kontaktieren und beliebigen Code auf dem betroffenen Server ausführen können.

Jahrelange Planung

Bleibt die Frage, wer der Angreifer war, und wieso er Schreibzugriff auf das xz-Projekt hatte. Er nutzte einen Account namens Jia Tan und hatte sich mit sinnvollen Projektbeiträgen über Jahre das Vertrauen des hauptverantwortlichen Entwicklers Lasse Collin erschlichen. Der kämpfte mit psychischen Gesundheitsproblemen und gab Jia Tan weitreichende Zugriffsrechte, nachdem er von einer Reihe anderer Personen dazu gedrängt worden war. Vermutlich handelte es sich dabei um Fake- oder Zweitaccounts des Angreifers. Nach der Entdeckung der Hintertür hob daher recht schnell auch eine Diskussion darüber an, wie man OSS-Maintainer besser unterstützen kann, nicht nur finanziell. Das sei besonders wichtig, wenn es sich um Einzelpersonen handelt, die in ihrer beschränkten Freizeit kleine, aber fundamentale Bestandteile des Open-Source-Ökosystems pflegen, so wie Lasse Collin und seine xz Utils.

Daneben diskutieren Projekte ihre Build-Gepflogenheiten und stellen ihren Umgang mit Abhängigkeiten von anderen Projekten infrage. Parallel begann die Recherche, wer hinter Jia Tan stecken könnte. Ob der technischen Finesse sowie der Akribie und jahrelangen Vorbereitung, mit der die Hintertür platziert wurde, vermuten viele einen staatlichen Akteur. Dem konnte die Open-Source-Community zumindest in diesem Fall einen Strich durch die Rechnung machen – in letzter Sekunde. (syt@ct.de) **ct**

Weiterführende Analysen: ct.de/ywk4

Eine betroffene xz-Version hatte es auch in die Vorschauversion 40 von Fedora geschafft und wurde per Software-Downgrade wieder entfernt.

Systemaktualisierungen	
wireplumber-libs	0.5.0-2.fc40 → 0.5.1-1.fc40
xdg-desktop-portal	1.18.2-5.fc40 → 1.18.3-1.fc40
yum	4.19.0-1.fc40 → 4.19.2-1.fc40
Herunterstufungen	
xz	5.6.0-3.fc40 → 1:5.4.6-3.fc40
xz-libs	5.6.0-3.fc40 → 1:5.4.6-3.fc40

Linux Foundation adoptiert den Redis-Fork Valkey

Nachdem die Firma Redis Inc. die Abkehr von einer Open-Source-Lizenz verkündet hatte, dauerte es gerade mal eine Woche, bis die Linux Foundation einen offenen Fork der vielseitigen Datenbank Redis präsentierte. Weil es nicht der erste Fork dieser Art ist, wirkt das Prozedere bereits routiniert.

Valkey, das ist eine Wortneuschöpfung, die an Key-Value und Walküren gleichermaßen erinnern soll. An diesen Namen müssen sich jetzt alle gewöhnen, die bisher auf die populäre Schlüssel-Werte-Datenbank Redis gesetzt haben und auch künftig Open-Source-Software im strengen Sinne nutzen wollen. Denn Redis selbst, beliebt in kleinen und großen Umgebungen zum Beispiel für Caches oder zur Verwaltung von Warteschlangen, wird nach Version 7.2.4 nicht mehr unter der „BSD 3-clause license“ erscheinen, sondern unter den Lizenzen „Redis Source Available License 2.0“ (RSALv2) und „Server Side Public License“ (SSPLv1). Das hat das Unternehmen Redis Inc. am 20. März verkündet. Quelloffen bleibt das Projekt weiter, jedoch wird es untersagt, Redis als „managed service“ feilzubieten, also im Rahmen eines Cloudangebots Redis-Instanzen zu vermieten.

Genau das hatten unter anderem Google Cloud und Amazon Web Services (AWS)

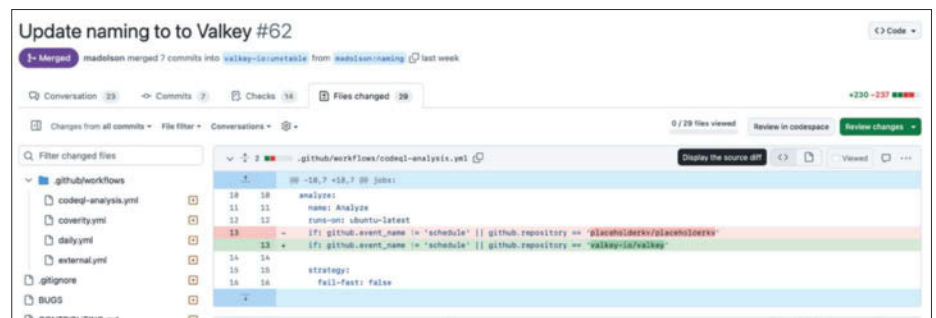
getan und sich im Gegenzug – so der Vorwurf von Redis Inc. – zu wenig an der Entwicklung beteiligt. Bereits am 28. März veröffentlichte die Linux Foundation eine Reaktion auf die Lizenzänderung: Die letzte Open-Source-Version von Redis mit der Versionsnummer 7.2.4 wird die Basis für einen Fork, der unter dem Namen Valkey weitergeführt wird. In der Ankündigung lassen sich AWS, Google Cloud, Oracle, Ericsson und Snap Inc. als künftige Unterstützer nennen. Zitiert wird, wohl auch als Beweis, dass Redis Inc. nicht allein für den Code verantwortlich war, unter anderem die AWS-Mitarbeiterin Madelyn Olson. Sie war bis zuletzt als Redis-Maintainerin aktiv.

Bemerkenswert ist die schnelle Abwicklung des Redis-Forks. Das GitHub-Repository für den Code lag bereits seit

knapp drei Jahren unter dem generischen Namen placeholderkv bereit, enthielt bereits eine Kopie von Redis, und angelegt war bereits eine CI/CD-Pipeline der Software. Per GitHub-Abstimmung einigte man sich dann bis zum 28. März fix auf den Namen Valkey, benannte Organisation und Repository um und bereitete die Pressemitteilung der Linux Foundation vor. Im ersten Schritt besteht die Entwicklungsarbeit vor allem daraus, die Zeichenkette redis aus dem Code zu entfernen.

Das vorbereitete Repository und die schnelle Abwicklung sprechen dafür, dass die Pläne von Redis Inc. nicht überraschend kamen – Redis ist auch nicht das erste große Open-Source-Projekt, bei dem ein Hersteller die Lizenz geändert hat.

(jam@ct.de)



Ein lange vorbereiteter Fork: Unter dem Namen placeholderkv lag das Repository bereits seit Jahren bei GitHub und wartete auf den Tag, an dem Redis Inc. seine Lizenz änderte.

**WIBU
SYSTEMS**

Willkommen in unserer Ideen-Schmiede

**SECURITY
LICENSING**

PERFECTION IN PROTECTION

Arbeiten Sie im Team der Besten an der Zukunft des Produktschutz, um Angreifern einen Schritt voraus zu sein.

Top Bezahlung, TOP100 Arbeitsumfeld Innovation und Technologie.

www.wibu.com



**Top-Innovator
2023**



Starten Sie in unserem Headquarter in Karlsruhe als:

► **Software-Entwickler und -Architekten (m/w/d)**

Weitere Positionen unter jobs.wibu.com

Die Stimmklone kommen

Edmund Stoiber zitiert Lao-Tse in fließendem Mandarin – kein Problem für KI-Modelle, die Stimmen realistisch nachbilden und den Sprechern beliebige Texte in den Mund legen können. OpenAI ist die Technik noch zu brenzlig, das Unternehmen testet seinen Stimmkloner lieber erst mal nur mit handverlesenen Partnern. Andere Betreiber sind da weniger vorsichtig.

OpenAI hat „Voice Engine“ vorgestellt, ein KI-Modell zum Klonen von Stimmen. Stimmproben von nur 15 Sekunden Länge sollen dem Modell ausreichen, um eine Stimme realistisch nachzubilden. In einem Blogbeitrag hat das Unternehmen eine Reihe von Beispielen veröffentlicht, die die Fähigkeiten der Voice Engine belegen sollen.

Derzeit testet OpenAI den Stimmkloner mit ausgewählten Partnern. Anhand der Ergebnisse der Tests werde das Unternehmen eine „fundiertere Entscheidung“



Dieses Video ging viral - auch weil viele Betrachter angezweifelt haben, dass eine KI es angefertigt hat.

darüber treffen, „ob und wie wir diese Technologie im großen Maßstab einsetzen“. Denn trotz vieler sinnvoller Einsatzszenarien, zum Beispiel als Lesehilfe, sieht OpenAI auch ein großes Missbrauchspotenzial – etwa als Fake-News-Generator im Wahljahr.

Dass in naher Zukunft viele gefälschte Zitate in Umlauf kommen dürften, wird aber OpenAIs Zurückhaltung nicht verhindern. Denn andere Betreiber von Stimmklonern sind weniger zurückhaltend – das Forscherteam der University of Texas at Austin und die Firma Rembrand zum Beispiel, das „Voice Craft“ entwickelt hat.

Voice Craft kann natürliche (englische) Sprache bearbeiten, indem es beispielsweise in einen gesprochenen Satz Wörter einfügt oder entfernt und Text in Sprache umwandelt. Es benötigt nach Angaben der Entwickler sogar nur drei Sekunden Ausgangsmaterial, um qualitativ hochwertige Sprachklone zu erzeugen.

Das Forscherteam ist sich der ethischen Probleme bewusst. Es argumentiert aber, dass die Veröffentlichung des Modells der Forschungsgemeinschaft die Möglichkeit gebe, Lösungen für potenzielle Missbrauchsprobleme zu finden.

Andere Anbieter sind noch weiter. Bei HeyGen und arcads.ai können Nutzer digitale Avatare generieren, Videos von Menschen, die lippensynchron in verschiedenen Sprachen sprechen. HeyGen hat kürzlich seine neue Funktion „Avatar in Motion 1.0“ vorgestellt. Damit kann man Menschen in vielen Sprachen lippensynchron synchronisieren – während sie

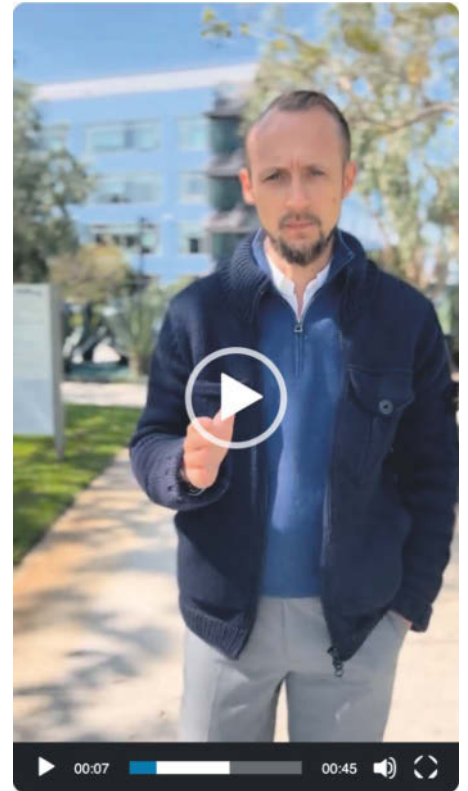


Bild: Screenshot aus HeyGen-Video

Der Mann in der Demo von HeyGen läuft, gestikuliert und spricht dabei beliebige Texte, die man ihm in den Mund legt.

sich bewegen und mit den Händen gestikulieren. Bisher funktionierte das nur mit Personen, die einigermaßen ruhig vor der Kamera saßen.

In einem Beispielvideo läuft ein Sprecher mit der Kamera durch einen Park und gestikuliert intensiv mit den Armen, spricht mal englisch, mal spanisch, man hört die Hintergrundgeräusche. Und arcads.ai lässt eine Frau in einem Video lebhaft und gestikulierend einen vorgegebenen Text sprechen. (jo@ct.de)

Weniger „kassiererlose“ Supermärkte von Amazon

Amazon will künftig weniger Supermärkte mit der „Just Walk Out“-Technik betreiben (siehe c't 1/2022, S. 120). Diese ermöglicht es Kunden einzukaufen, ohne an der Kasse zu bezahlen. Die Kunden benötigten dafür nur eine spezielle App. Die Kosten für den Einkauf werden automatisch abgebucht. Stattdessen will das Unternehmen nun verstärkt auf smarte Einkaufswagen setzen, die mit Kameras ausgestattet sind, um Artikel direkt beim Einkauf zu scannen.

Dieser Richtungswechsel folge der Erkenntnis, dass Kunden beim Einkauf auf größeren Ladenflächen einen Überblick darüber behalten wollen, wie teuer der Einkauf sein wird, so ein Amazon-Manager. Zudem war die Umsetzung von „Just Walk Out“ technisch anspruchsvoll. Das Magazin The Information hat zudem berichtet, dass für das System mehr als 1000 Menschen in Indien tätig waren. Diese Mitarbeiter haben die Bilder von Überwachungskameras aus

den jeweiligen Supermärkten aus der Ferne beobachtet und sichergestellt, dass die Einkäufe korrekt gebucht wurden.

Trotz der Abkehr von „Just Walk Out“ in neuen „Amazon Fresh“-Märkten wird Amazon sie in den kleineren „Amazon Go“-Läden sowie in einigen kleineren „Fresh“-Geschäften in Großbritannien weiterhin verwenden. Das Unternehmen bietet die Technik auch anderen Einzelhändlern an. (jo@ct.de)

KI-Regeln für US-Behörden

Nutzen US-Behörden KI-Werkzeuge, müssen sie künftig eine Reihe neuer Regeln befolgen.

Das gibt ein neues **Dekret der US-Regierung** vor. Ämter und Ministerien werden dazu verpflichtet, regierungseigene KI-Quelltexte, -Modelle und -Daten zu veröffentlichen. Sofern Sicherheitsgründe dagegen sprechen, sollen sie zumindest genutzte Metriken melden. Vor dem Einsatz generativer KI müsse der potenzielle Nutzen bewertet und sichergestellt werden, dass ihr Einsatz kein unangemessenes Risiko darstelle.

Die neue Richtlinie reguliert den Einsatz von KI bei den Strafverfolgungsbehörden, darunter die vorausschauende Polizeiarbeit, die Überwachung sozialer Medien für die Strafverfolgung, das Aufdecken von Plagiaten an Schulen, das Aufspüren oder Messen menschlicher Emotionen und das anlasslose Vorab-Screening bei neuen Arbeitsverhältnissen.

Bis zum 1. Dezember haben die Behörden Zeit, entsprechende Sicherheitsvorkehrungen zu treffen. Tun sie dies nicht, dürfen sie die KI-Tools nicht mehr nutzen – es sei denn, die Verantwortlichen können begründen, dass der Verzicht „nicht vertretbare“ Auswirkungen auf kritische Abläufe hätte.

Gemeinsam mit den Briten wollen die Amerikaner auch kommerzielle KI-Modelle schärfer kontrollieren. Dazu haben die beiden Regierungen eine Absichtserklärung unterzeichnet. Das britische Institut für KI-Sicherheit und sein bislang nur angekündigtes, aber noch nicht in Betrieb befindliches US-amerikanisches Pendant, sollen gemeinsam Testreihen entwickeln, um die Risiken zu bewerten und die Sicherheit der „fortschrittlichsten KI-Modelle“ zu gewährleisten.

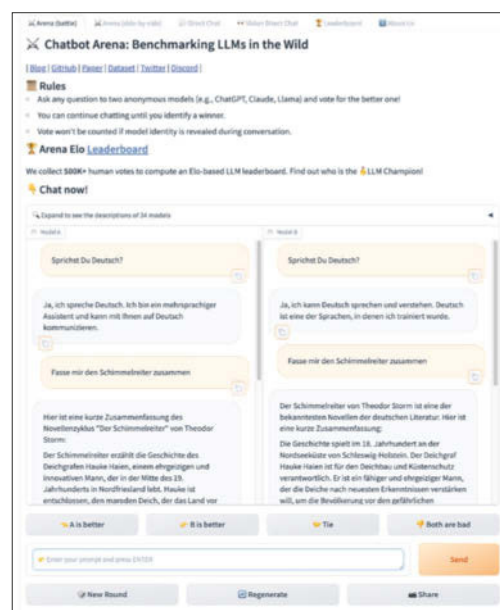
Eine UN-Resolution zum Thema KI-Regulierung mutet dagegen wachschweich an: Sie ermuntert die Staaten zu allerlei wünschenswerten Aktionen, etwa sichere und vertrauenswürdige KI-Systeme zu fördern und „ein Ökosystem auf allen Ebenen“ zu schaffen. Darin fallen viele Stichworte wie „verantwortungsbewusste und inklusive KI-Innovation“, „wirksame, international interoperable Maßnahmen gegen Sicherheitslücken und Risiken schon vor dem Einsatz einer KI“ sowie „internationale Kooperation bei der Erfassung der Auswirkungen von KI auf die Arbeitswelt“. Ein wirksamer Mechanismus, mit dem diese Wünsche umgesetzt werden könnten, fehlt der Resolution allerdings. Und: Die KI-Resolution gilt ausdrücklich nicht für KI im Militärbereich.

(jo@ct.de)

Claude 3 schlägt GPT-4

Der Chatbot Claude 3 Opus führt seit Kurzem das sogenannte **Chatbot Arena Leaderboard** an, vor zwei Versionen von GPT-4 (huggingface.co/spaces/lmsys/chatbot-arena-leaderboard). Die Large Model System Organization (LMSYS) hat die Chatbot Arena ins Leben gerufen, um die Leistungen großer Sprachmodelle miteinander zu vergleichen. Dort treten verschiedene Modelle in anonymen, zufällig ausgewählten Duellen gegeneinander an. Die Nutzer stimmen darüber ab, welches Modell sie für das beste halten. Der Benchmark repräsentiert also das Urteil vieler menschlicher Bewertungen.

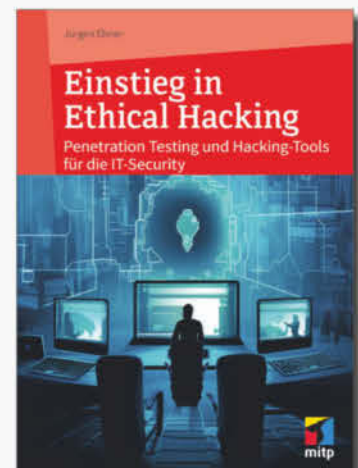
Von einem vielversprechenden neuen offenen Sprachmodell, DBRX vom Unternehmen Databricks, gab es bis Redaktionsschluss nur die Ergebnisse standardisierter Benchmarks. Denen zufolge schneidet DBRX besser ab als Llama 2 von Meta, Mixtral von Anthropic und sogar als das kürzlich veröffentlichte Grok-1-Modell von Elon Musks xAI. Ebenso zeigte DBRX bei den meisten Benchmarks eine bessere Leistung als das GPT 3.5-Modell von OpenAI. (jo@ct.de)



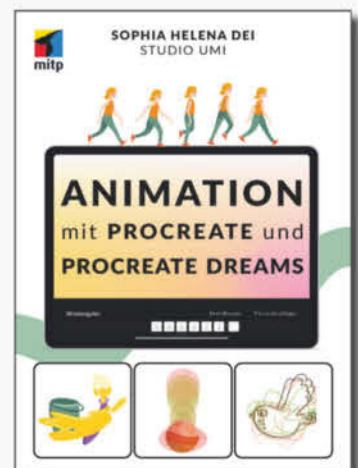
In der Chatbot Arena bewerten die Besucher die Dialoge zweier ihnen unbekannter, zufällig ausgewählter Chatbots.



Auch als E-Book oder Bundle in unserem Shop erhältlich: www.mitp.de/0871



Auch als E-Book oder Bundle in unserem Shop erhältlich: www.mitp.de/0691

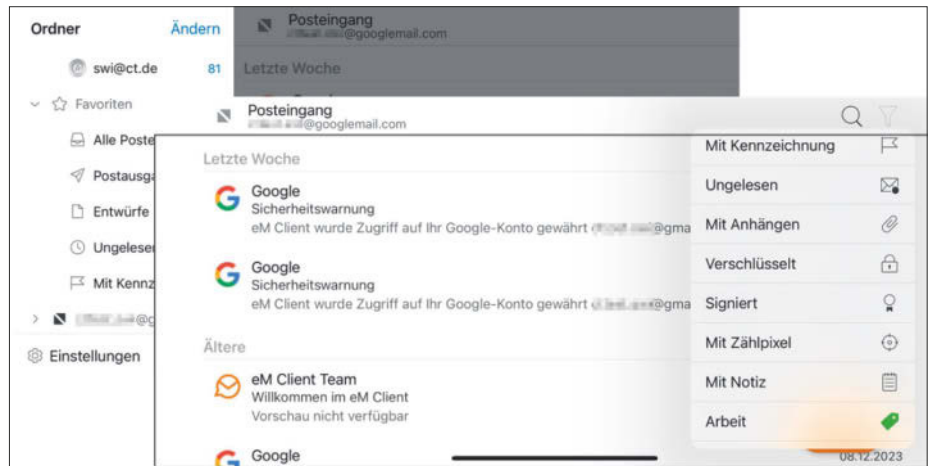


Auch als E-Book oder Bundle in unserem Shop erhältlich: www.mitp.de/0713

Mail-App: mobiler eM Client erschienen

Das E-Mail-Programm eM Client gibt es jetzt auch als kostenlose App für Android und iOS.

Das Mailprogramm eM Client zeichnet sich unter anderem durch die Unterstützung von Exchange-Servern und Funktionen wie einen gemeinsamen Posteingang für alle Konten, eine Filterfunktion für Mails mit Tracking via Zählpixeln und eine flexible Suche aus. Die App ist kostenlos und anders als die Gratis-Version für Windows, Linux und macOS nicht auf zwei Mailkonten beschränkt. Auf Anfrage erklärte der Hersteller, dass das auch so bleiben soll. Aussehen und Bedienung orientieren sich stark an den Desktop-Pendants, jedoch fehlen noch einige Funktionen, die künftig aber nachgereicht werden sollen. Insbesondere müssen Nutzer der App noch auf Kalender, Kontakt- und Aufgabenverwaltung verzichten. Der Hersteller



Mit dem eM Client gibt es eine neue Mail-App für Android und iOS, die sich auch mit Exchange-Servern versteht.

verspricht, auch die neuen Funktionen hinzuzufügen, die in der kommenden Version 10 des Desktop-Clients stecken. Dazu

gehören beispielsweise KI-Anbindung, Klassifizierungskategorien und Quick Actions. (swi@ct.de)

Neue Funktionen in der Microsoft-365-App

Microsoft erweitert die Microsoft-365-App (vormals „Office-App“) für Android und iOS und ergänzt die Schaltzentrale für das mobile Word, Excel, PowerPoint und die PDF-Tools um weitere Dienste.

Buchstäblich im Zentrum (der Symbolleiste) steht der auf ChatGPT basierende KI-Bot Copilot. Je nach Abo führt die Schaltfläche zum kostenlosen Copilot-Chat oder zu Copilot Pro. Hinzugekommen sind die Scanner- und OCR-App Lens

und der auf Dall-E basierende Bildgenerator Designer. Letzterer ist noch als „Preview“ gekennzeichnet und laut Microsoft während dieser Testphase kostenlos nutzbar. Der Designer erreicht zunächst Android-Geräte, in die Microsoft-365-App für iOS soll er in den nächsten Wochen kommen. Auch für den Cloudspeicherdienst OneDrive gibt es eine Schaltfläche. Über die erhält man Zugriff auf alle in der Cloud gespeicherten Dateien mit einer

Übersicht der letzten Zugriffe und einer Suchfunktion.

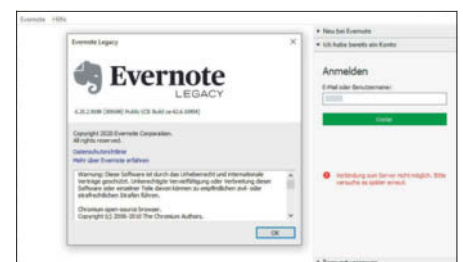
Microsoft will die App offensichtlich vom Launcher für die Office-Apps zu einem **Dashboard für alle Microsoft-Dienste** machen. Sie bleibt bislang aber optional; die Microsoft Apps wie Word, Excel, Copilot, Lens oder OneDrive lassen sich weiterhin auch einzeln mit eigenen Icons auf den Startseiten der Mobilgeräte platzieren und aufrufen. (swi@ct.de)

Evernote: Aus für die Legacy-Version

Vor gut drei Jahren hat der Hersteller des populären Notizprogramms einen Schnitt gemacht und das Programm für alle Mobil- und Desktop-Systeme als Version 10 komplett neu entwickelt. Der fehlten jedoch etliche Funktionen der klassischen Evernote-Clients, weshalb der Hersteller diese unter der Bezeichnung Evernote Legacy weiterhin duldet. Die italienische Firma Bending Spoons, die Evernote zwischenzeitlich gekauft hatte, ließ die Legacy-Version zunächst weiterlaufen, hat nun aber den **klassischen Client endgültig abgeschaltet**. Beim Login-Versuch gibt es seit Ende März nur eine Feh-

lermeldung, dass der Server nicht erreichbar sei. Um an in der Cloud gespeicherte Notizen zu kommen, müssen Nutzer zwingend auf die Version 10 updaten, und sei es nur, um die Daten für den Umzug zu einem anderen Notizdienst zu exportieren.

Im offiziellen Blogpost (heise.de/s/4rrv5) begründet der Evernote-Hersteller diesen Schritt vor allem mit dem Sicherheitsrisiko, das der veraltete und seit 2020 nicht mehr weiterentwickelte Client nebst APIs darstellt. Außerdem würde dadurch alter Code eingespart und die Weiterentwicklung von Evernote vereinfacht. (swi@ct.de)



Der Evernote-Hersteller zieht den klassischen „Legacy“-Clients für Windows und macOS endgültig den Stecker. Ein Login ist damit nicht mehr möglich.

Adobe: Neue KI-Werkzeuge für Kreativ-Workflows

Adobe hat auf seiner Hausmesse Adobe Summit eine Reihe von Lösungen vorgestellt, die Kreative besser unterstützen sollen – mit reichlich KI an Bord.

Adobe flicht in die gesamte Welt seiner Online-Dienste KI ein. In der Experience Platform, Adobes Daten- und Werbedienst, soll ein KI-Chatbot Nutzern unter die Arme greifen, indem er technische Fragen beantwortet, Aufgaben automati-

siert, Ergebnisse simuliert und Zielgruppen und Customer Journeys generiert.

Mit dem GenStudio hat Adobe zudem eine neue, auf die Erzeugung von KI-Inhalten ausgerichtete Plattform vorgestellt. Von der Planung von Workflows über die Erzeugung und Verwaltung von Inhalten bis zur Kampagnenverwaltung und zum Reporting soll sie Kreative unterstützen.

Adobes Bildgenerator Firefly hat eine Reihe neuer Tricks gelernt. Mit der sogenannten Structure Reference soll er die

Struktur eines bestehenden Bildes auf neu generierte Bilder anwenden können. Indem Anwender ein vorhandenes Bild als Referenz angeben, können sie so schnell Dutzende Bildvarianten mit demselben Layout generieren. Wenn sie „Structure Reference“ mit der bereits vorhandenen Funktion „Style Reference“ kombinieren, die den Stil eines Referenzbildes auf die Eingabeaufforderung überträgt, können Anwender nun sowohl die Struktur als auch den Stil eines Bildes weiterverwenden.

Ebenfalls neu sind die benutzerdefinierten Modelle (Customer Models). Damit können Unternehmen den Bildgenerator auf der Grundlage ihrer Stile und Motive trainieren. Das soll die Markenkonsistenz gewährleisten. Sogenannte Stil-Kits sollen es Firmen demnächst erleichtern, Stile, Kampagnen und Text-Prompts zu entwickeln, zu speichern und bereitzustellen.

Obwohl alle Elemente in der Adobe-Welt darauf ausgelegt sind, dass Anwender diese nicht verlassen müssen, stellt Adobe Firefly-Funktionen auch über APIs bereit. Firefly Services sind eine Sammlung von Programmierschnittstellen, mit denen Unternehmen Firefly-Funktionen in ihre Workflows einbetten können. (jo@ct.de)

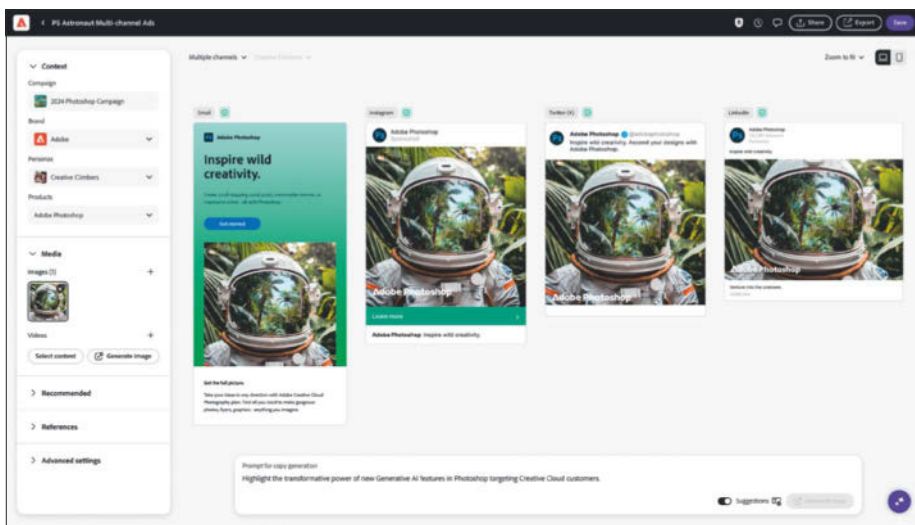


Bild: Adobe

Mit GenStudio sollen Social-Media-Verantwortliche im Handumdrehen Inhalte für verschiedene Kanäle entwerfen können.

Canva übernimmt Affinity-Suite von Serif

Die Grafikdesignplattform Canva hat das britische Entwicklerstudio Serif übernommen, das die **Affinity-Suite von Kreativ-Apps** herausbringt. Affinity Photo, Affinity Designer und Affinity Publisher sind populäre Alternativen zu Adobes Photoshop, Illustrator und InDesign. Canva ist darauf ausgelegt, schnelle Designarbeiten online durchzuführen, gerade auch durch Nutzer, die damit sonst wenig Erfahrung haben.

Für die rund 3 Millionen Nutzer der Affinity-Apps ändert sich zunächst nichts, so Canva. Auch seien „im Moment“ keine Änderungen bei der Preispolitik geplant. Affinity-Benutzer hatten sich besorgt darüber geäußert, dass Canva das Preismodell der Affinity-Anwendungen in ein

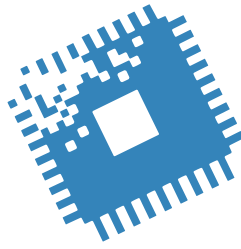
Abomodell umstellen könnte. Bisher werden sie als Einmalverkauf vertrieben. Bestehende Affinity-Käufer sollen ihre Versionen „auf Dauer“ weiter nutzen können, erklärte der Serif-Chef Ashley Hewson in einer FAQ. Zudem seien weitere kostenlose Updates für die Version 2 der Anwendungen in Arbeit.

Perspektivisch sollen Canva und die Affinity-Anwendungen miteinander verknüpft werden. Nutzer sollen dann mit den Profi-Tools Bilder, Logos, Icons und andere Elemente entwerfen, die sich direkt in Canva weiter nutzen lassen. Eine Cloud-Plattform für die Synchronisation von Affinity-Dateien sei dafür denkbar, erklärt der Serif-Chef. (jo@ct.de)

Bilder editieren mit Dall-E

Mit einer neuen Funktion für seinen in den Chatbot ChatGPT integrierten **Bild-generator DALL-E 3** können Nutzer erzeugte Bilder direkt in ChatGPT bearbeiten. Oberhalb generierter Bilder zeigt ChatGPT ein Auswahlwerkzeug an, mit dem Nutzer Bildteile markieren. Die Größe des Auswahlwerkzeugs ist anpassbar und es gibt Schaltflächen zum Rückgängigmachen, Wiederholen und zum Löschen von Auswahlbereichen. Hat ein Anwender einen Bildbereich markiert, kann er im Chatfenster Anweisungen geben, was Dall-E in dem Bereich ändern soll. Die Funktion ist sowohl in der Web- als auch auf der Mobilversion verfügbar. (jo@ct.de)

Bit-Rauschen



Windows on ARM soll es 2024 endlich schaffen

Der ARM-Chip Snapdragon X Elite wirft immer längere Schatten voraus. AMD bekommt NPU-Treiber weiter nicht auf die Kette. CPU-Codenamen geben Hinweise auf Intel-Prozessoren für 2026.

Von Christof Windeck

Bei Windows auf ARM-Chips wird es bald wohl spannend. Jedenfalls verdichten sich die Hinweise, dass es Microsoft und Qualcomm nun endlich hinbekommen wollen. Wie in früheren Ausgaben des Bit-Rauschens bereits gemeldet, tauchten von mehreren unterschiedlichen Notebooks mit Qualcomm-Prozessoren des Typs Snapdragon X Elite Benchmark-Ergebnisse auf. Wie zufällig und versehentlich solche Daten in die Öffentlichkeit geraten, sei dahingestellt – wir vermuten, dass Firmen zumindest einige dieser vermeintlichen Leaks gezielt einsetzen, um Spekulationen über kommende Produkte anzufachen. Im Geekbench 6 übertrifft der Snapdragon X Elite mit zwölf Oryon-Kernen und 4,3 Gigahertz im Turbo jedenfalls alle bisherigen ARM-Chips für Windows-Notebooks. Je nachdem, wie stark die Kühlung ausgelegt ist – also je nach Thermal Design Power (TDP) –, rückt der Qualcomm-Prozessor dicht an aktuelle AMD Ryzen 8040U und Intel Core Ultra heran. Ob er dabei ohne Lüfter auskommt, ist jedoch unklar.

Nach wie vor gibt es wenige Windows-Apps, die für ARM angepassten Code nutzen. Und die Emulation für x86 und x86-64 in Windows 11 frisst viel Leistung. Qualcomm verkündet daher stolz, dass Google eine ARM-Version des Browsers Chrome für Windows fertiggestellt hat. Und KI-Apps soll der Snapdragon X Elite mehr Rechenleistung bereitstellen als bisherige x86-Mobilprozessoren.

Qualcomm verspricht alleine für die Neural Processing Unit (NPU) 45 Tops – mehr, als bei AMD und Intel bisher jeweils NPU, CPU und GPU gemeinsam schaffen. Dank schnellem RAM des Typs LPDDR5X-8533 soll der Snapdragon X Elite mit bis zu 136 GByte/s auf den Arbeitsspeicher zugreifen.

Windows-Notebooks mit Snapdragon X Elite sollen zur Jahresmitte starten, also in wenigen Wochen. Die erwähnten Geekbench-Daten stammen von Lenovo- und Samsung-Geräten, aber höchstwahrscheinlich schickt Microsoft auch eigene Surface-Notebooks mit ARM ins Rennen.

AMD-Treiberk(r)ampf

Unterdessen stellt sich AMD bei Treibern und Firmware weiter ungeschickt an. Im März beschrieb AMD in einem Blog-Beitrag, wie einfach es doch sei, ein KI-Sprachmodell (Large Language Model, LLM) unter Windows 11 auf einem PC oder Notebook mit Ryzen AI oder Radeon 7000-Grafikkarte zu betreiben. Dazu müsse man im Wesentlichen nur die Software LM Studio installieren und darin das gewünschte LLM herunterladen.



Bild: Samsung

Samsung will das Galaxy Book4 – hier eine Version mit Intel-CPU – auch mit dem starken Zwölfkern-ARM Qualcomm Snapdragon X Elite bestücken.

Das klappt tatsächlich einfach, wie sich im c't-Labor zeigte. Doch LM Studio nutzt bisher die in den Ryzen-Prozessoren mit Ryzen AI eingebaute NPU nicht. Stattdessen übernimmt der integrierte Radeon-Grafikprozessor – also die IGP – die KI-Berechnungen. AMD hat zwar nicht gelogen, denn „Ryzen AI“ schließt ausdrücklich auch CPU-Kerne und die GPU/IGP mit ein. Doch offenbar quält sich AMD weiterhin mit der Einbindung der NPU, die viel mehr und vor allem energieeffizientere KI-Rechenleistung liefern soll als die anderen Rechenwerke. Angeblich verlangt Microsoft für einen KI-PC demnächst mindestens 40 Tops, damit der Copilot lokal läuft.

Auch erste Ergebnisse des neuen UL Procyon AI Computer Vision Benchmark (siehe Seite 45) belegen, dass KI unter Windows noch ein Flickenteppich ist. Über das einheitliche Windows-API DirectML lassen sich die NPUs von AMD und Intel immer noch nicht nutzen und Nvidia kocht weiter das eigene CUDA-Süppchen. Der wachsende Druck hat AMD zur Ankündigung bewogen, weitere Teile des GPU-API ROCm offenzulegen. Und bei KI-Servern zieht Nvidia weiter davon, siehe Seite 46.

Neue Codenamen

In von Intel eingereichten Patches für künftige Linux-Kernels tauchen neue CPU-Codenamen auf. Ende 2024 erwartet man nach Meteor Lake (Core Ultra 100) noch Arrow Lake und Lunar Lake, vermutlich beide als Core Ultra 200. 2025 folgen wohl Panther Lake sowie Nova Lake, auch der Name Beast Lake fiel bereits. Nun tauchte Adams Lake auf, ein Kandidat für 2026.

Bei den schnellen Performance-Kernen ist zurzeit Redwood Cove aktuell (im Core Ultra 100), dann folgen angeblich Lion Cove, Cougar Cove, Panther Cove und Douglas Cove. Bei den Efficiency-Cores könnte die Ablösung der aktuellen Crestmont-Mikroarchitektur Skymont heißen, gefolgt von Sheldonmont.

Anscheinend erfinden AMD und Intel absichtlich möglichst verwirrende Codenamen. Denn Intels nächste – und wegen hoffentlich höherer Performance auch dringend nötige – Xeon-Generation Xeon 6 heißt Granite Rapids, während AMD die ebenfalls im Herbst erwarteten Zen-5-Ryzens als Granite Ridge entwickelt. Für letztere kommen schon die ersten BIOS-Updates, damit sie in vorhandenen AM5-Boards laufen – vielleicht als Ryzen 9000.

(ciw@ct.de)

betterCode()

API 2024

Design, Entwicklung und Management von APIs



14. und 16. Mai 2024 • online

In der Softwareentwicklung kommt man nicht um APIs herum: Ob Private oder Public APIs – schwierige Entscheidungen sind zu fällen. Welche **Architekturparadigmen**, welche Verfahren, welche **Protokolle** nutze ich, wann welche besser nicht? Wie gewährleiste ich **Qualität, Kompatibilität** und **Sicherheit**?

Folgende Themen erwarten Sie:

- Fortgeschrittene Entwurfstechniken
- Entwicklungstools
- Versionierung
- Testen
- API Management
- Data Contracts
- API Sprawl und Great Unbundling

Jetzt
Frühbucher-
tickets
sichern!

Workshops am 4. und 6. Juni

api.bettercode.eu

Veranstalter



betterCode()

Spring 2024

Moderne Java-Entwicklung mit Spring



20. Juni 2024 • online

Das **Spring Framework** und **Spring Boot** erfreuen sich wegen ihrer Sicherheit und Stabilität großer Beliebtheit – im praktischen Einsatz sind jedoch einige wichtige Fragen zu klären.

Die betterCode() Spring hilft hier und widmet sich u.a. folgenden Themen:

- Warum sollte ich meine **Spring-Anwendungsarchitektur** mit jMolecules umsetzen?
- Wie ändere ich die **Datenbankzugriffe** schnell und sicher?
- Wie hilft **Chaos Engineering**, die Stabilität der Anwendung auch bei Ausfällen sicherzustellen?
- Ich muss eine **Spring-Legacy-Anwendung** betreuen. Worauf muss ich jetzt achten?

Jetzt
Frühbucher-
tickets
sichern!

Spring-Security-Workshop am 27. Juni

spring.bettercode.eu

Veranstalter



Profi-Router mit 5G und Wi-Fi 6

Der taiwanische Netzwerkhersteller Draytek hat seine Routerreihe Vigor 2927 um zwei Modelle für schnellen Mobilfunk und schnelles WLAN ergänzt. Sie sollen ab Ende April erhältlich sein.

Die Vigor2927-Serie besteht aus kompakten Routern für den Einsatz in kleinen Unternehmen beziehungsweise Außenstellen. Das Gehäuse sieht bei allen Modellen nahezu gleich aus, hat aber Anschlüsse abhängig vom Funktionsumfang. Bislang gab es sechs Modelle mit unterschiedlichen Zusatzfunktionen beziehungsweise Schnittstellen.

Die beiden jüngst von Draytek angekündigten Modelle Vigor2927L-5G und Vigor2927Lax-5G bringen ein 5G-Mobilfunkmodem für bis zu 2,4 Gbit/s Downlink und 900 Mbit/s Uplink mit; das ax-Modell strahlt zusätzlich Wi-Fi 6 mit zwei MIMO-Streams ab. Alle Antennen – zwei für WLAN, vier für 5G – sind bei den Modellen extern und über (RP-)SMA-Anschlüsse aus dem Gehäuse geführt.

Die Internetverbindung über 5G kann an zwei Gigabit-WAN-Ports um weitere Zugänge ergänzt werden; wahlweise als Ausfallsicherheit (Failover) oder als Kapazitätserweiterung mittels Load-Balancing. Welchen Firewalldurchsatz die neuen Geräte schaffen, sagt Draytek nicht. Clients finden an fünf Gigabit-LAN-Ports Anschluss. Genügt das nicht, kann man den zweiten WAN-Port zum LAN-Port umwidmen.

Bis zu acht Subnetze inklusive DHCP-Server können die Router bereitstellen, sodass auch in kleinen Installationen eine sicherheitssteigernde Netztrennung per VLAN möglich ist. Vier davon können Administratoren als Hotspot-Netze mit unterschiedlichen Authentifizierungsverfahren abstellen, darunter etwa RADIUS, Voucher oder SMS-Bestätigungen. Maximal 16 gleichzeitig aktive VLANs (IEEE 802.1q) unterstützt die Routerreihe insgesamt.

Die 2927-Serie baut maximal 25 VPN-Tunnel gleichzeitig auf, unter anderem mit WireGuard, OpenVPN, GRE und mehreren IPSec-Verfahren. Außerdem verwal-



Bild: Draytek

Die neuen Router L-5G und Lax-5G aus der Vigor2927-Reihe bringen ein 5G-Mobilfunkmodem mit, das Multigigabit-Datenraten liefern soll. Dafür besitzen die Router vier Antennenanschlüsse.

tet ein Router bis zu 20 WLAN-APs und 10 Switches.

Das Management erledigt der Administrator wahlweise per Browser, Telnet oder SSH. Der Vigor2927L-5G und der Vigor2927Lax-5G sollen ab dem 24. April im Fachhandel erhältlich sein. Preise nannte Draytek noch nicht. (amo@ct.de)

2,5-Gigabit-Switches mit 10-Gigabit-Uplink

Die NBase-T-Geschwindigkeitsstufe 2,5 Gbit/s etabliert sich immer mehr als preisgünstiger Kompromiss zwischen 1 und 10 Gbit/s; viele neue Mainboards und Netzwerkspeicher haben einen 2G5-Port, bezahlbare USB-Adapter und PCIe-Karten sind verfügbar.

Trendnet hakt mit den Switches TEG-S5061 und TEG-S5091 in diese Entwicklung ein: Die Switches besitzen **fünf beziehungsweise acht 2,5-Gbit/s-Ports** zum Anschließen von Kupfer-Netzwerkhardware und zusätzlich einen SFP+-Slot für Uplinks mit bis zu 10 Gbit/s – beispielsweise per Glasfaser. Die Kupferports sind

rückwärtskompatibel mit 10-, 100- und 1000-Mbit/s-Ethernet.

Beide Modelle besitzen keine Verwaltungsfunktionen wie SSH, VLAN et cetera.

Die Elektronik ist bei beiden Modellen in einem passiv gekühlten Metallgehäuse verpackt. Über ein 12-Volt-Netzteil mit Hohlstecker werden die Switches mit Spannung versorgt; die Leistungsaufnahme der Modelle beziffert Trendnet mit maximal 9,5 Watt.

Der sechsportige TEG-S5061 ist für rund 90 Euro im Handel. Sein 9-Port-Bruder TEG-S5091 liegt bei 130 Euro.

(amo@ct.de)



Die Modelle TEG-S5061 und -S5091 von Trendnet erlauben einen preisgünstigen Einstieg in die Multigigabit-Welt, inklusive SFP+-Uplink für 10-Gbit/s-Verbindungen.

Kurz & knapp

Der Netzkaufrüster Adtran beschleunigt mit der neuen Schnittstellenkarte FSP 3000 M-Flex800 die **WAN-Anbindung seiner Switches und Router auf 800 Gbit/s**. Die Karte nimmt bis zu sechs Optikmodule auf (ZR, ZR+, OpenROADM und andere Typen), die jeweils 100, 400 oder 800 Gbit/s transportieren.

Mit gleich zwei **Prüfgeräten für Optikkontakte** wartet Laser Components auf: Mit dem Tempo FIP100 im Format eines dicken Schraubendrehers sollen Netzwerktechniker schnell erfahren, wie es um die optischen Kontaktflächen von Glasfaserstrecken steht: aufsetzen, Taste drücken, Ergebnis ablesen. Das einer Lötpistole ähnelnde Viavi INX 760 arbeitet ähnlich. Es soll alle Fasern einer 12er-Verbindung in nicht mal 10 Sekunden schaffen. Beide Geräte bringen einen Satz wechselbarer Prüfspitzen für unterschiedliche Steckertypen mit.

KI-taugliche Mini-PCs mit und ohne Lüfter

Zotac bietet fünf kompakte PC-Barebones zum Selbstbestücken an. Darin rechnen Core-Ultra- und Ryzen-7040-CPU's mit KI-Beschleunigern.

Auch die Hersteller von Mini-PCs wollen am KI-Hype mitverdienen. Der chinesische Hardwarespezialist Zotac hat fünf kompakte Barebones mit Prozessoren der Serien AMD Ryzen 7040 und Intel Core Ultra vorgestellt, die sogenannte Neural Processing Units (NPU) enthalten. Diese Recheneinheiten in den CPUs sind für Datentypen geringer Genauigkeit wie INT8 und FP16 optimiert, die bei KI-Anwendungen vorherrschen. Die NPUs entlasten mit kompakter Software die CPU- und GPU-Kerne und schlucken dabei weniger Strom.

Unter den fünf vorgestellten Mini-PCs sind auch zwei lüfterlose. Im ZBox CI671 nano und CI651 nano stecken die Meteor-Lake-Prozessoren Core Ultra 7 155U beziehungsweise

Core Ultra 5 125U mit je zwei Performance-, acht Effizienz- und zwei Low-Power-Effizienz-Kernen (2P+8E+2LP) und 15 Watt Thermal Design Power. Der Core Ultra 5 taktet etwas langsamer (Turbo: 4,3 statt 4,8 GHz). Zur weiteren Ausstattung der Barebones gehören unter anderem Wi-Fi 6, 2 x DisplayPort und 1 x HDMI für drei Monitore und insgesamt sechs USB-Ports.

Mit einer Grundfläche von 15 x 15 Zentimetern und einer Höhe von lediglich 2,9 Zentimetern sind die aktiv gekühlten ZBox edge MI672 und MI652 kompakter. In ihnen rechnen die gleichen Prozessoren wie in den lüfterlosen ZBox-nano-Modellen. Auch die Ausstattung ist bis auf einen DisplayPort-Anschluss weniger identisch.

Ins gleiche Gehäuseformat packt Zotac in der ZBox edge MA762 den Mobilprozessor Ryzen 7 7840HS mit acht Kernen und bis zu 5,1 GHz Takt. Als Besonderheit rüstet der Hersteller den Mini-PC-



Bild: Zotac

Als Extra bringt die Zotac ZBox edge MA762 zwei Ethernet-Ports mit. Die Radeon 780M des eingelöteten Ryzen 7840HS steuert über DisplayPort, HDMI und USB-C (nicht im Bild) drei Monitore an.

Barebone mit zwei Gigabit-Ethernet-Schnittstellen aus. Die ZBox edge MA762 steuert über DisplayPort, HDMI und USB-C drei Displays gleichzeitig an. Zu Preisen und Verfügbarkeit gibt es noch keine Informationen. (chh@ct.de)

Grafikkarten-Benchmark für KI-Bilder

UL Solutions, die Softwareschmiede hinter dem Grafik-Benchmark 3DMark, hat den **KI-Benchmark Procyon AI Image Generation** veröffentlicht. Dieser misst die Geschwindigkeit von GPUs mit dem Bildgenerator Stable Diffusion. Der große Vorteil des kostenpflichtigen Benchmarks ist, dass er sämtliche Softwarekomponenten enthält und einrichtet. Zudem erfordert er keine umfangreichen Parametereinstellungen, sondern startet per Mausklick.

Bei Grafikkarten und integrierten Grafikprozessoren misst er die Zeit, die Stable

Diffusion 1.5 benötigt, um 16 Bilder mit einer Auflösung von 512 x 512 Pixeln zu generieren. Dabei nutzt er abhängig von der Hardware die APIs Nvidia TensorRT, Intel OpenVINO und ONNX mit DirectML. High-End-Karten wie die GeForce RTX 4090 schaffen über 5300 Punkte. Am anderen Ende der Skala liegen integrierte GPUs wie die Intel UHD 770 mit 29 Punkten. Für Grafikkarten mit viel Speicher gibt es eine XL-Wertung mit 1024 x 1024 Pixel großen Bildern. Pro Jahr kostet der Benchmark 5000 US-Dollar. (chh@ct.de)

UL Procyon AI Image Generation

GPU	Stable Diffusion 1.5	Stable Diffusion XL
	besser ►	besser ►
GeForce RTX 4090	5310	4772
GeForce RTX 4070	2027	—
GeForce RTX 4060 Ti	1419	—
Radeon RX 7800 XT	1149	957
Radeon 760M (Ryzen 5 8600G)	137	—
Intel UHD 770 (Core i5-14500)	29	—

E-Books im heise shop

Jetzt viele Titel als ePub, mobi und PDF erhältlich.

Sofort im Zugriff, dauerhaft in Ihrem Account gespeichert.

shop.heise.de/e-books



Blackwell gut, alles gut

Nvidias neue KI-Beschleuniger

Mit neuen Blackwell-Beschleunigern will Nvidia seine Dominanz im KI-Markt ausbauen. Doch die Siliziumoffensive allein ist nur die halbe Miete: Es geht auch um Chip-Kommunikation und Software-Entwicklung.

Von Carsten Spille

Der Auftritt des traditionell schwarz belederkjacketten Nvidia-Chef Jen-Hsun Huang füllte auf Nvidias Entwicklerkonferenz GPU Technology Conference (GTC) locker die mehr als 16.000 Plätze im Eishockeystadion der San Jose Sharks. Auf der Bühne ließ Huang sich von den Besuchern feiern wie ein Rockstar von seinen Fans – Dutzende Milliarden in der KI-Kasse und ein Börsenwert über 1,5 Billionen Euro machen eben sexy. Wenig verwunderlich wollen viele Firmen, Start-

ups und Entwickler mit am Tisch sitzen, wenn der KI-Kuchen aufgeteilt wird und brachten sich auch auf der GTC dafür in Position.

Während sich die versammelte Konkurrenz aus namhaften Firmen wie AMD, Intel oder Google an den vor zwei Jahren angekündigten und weiter heißbegehrten Beschleunigern mit Hopper-Architektur abarbeitet, stellt Nvidia schon die nächste Generation vor. Sie heißt Blackwell und hat außer deutlich mehr Rechenkraft und größerem, für KI-Anwendungen immens wichtigen lokalen Speicher noch ein paar Asse im Ärmel. Und Nvidia wäre nicht Nvidia, wenn man nicht schon genaue Pläne hätte, daraus auch Kapital zu schlagen.

Mit NIMs, Nvidia Inference Microservices, will man speziell Firmen ansprechen, die KI-Modelle auf ihre eigenen Datenbestände trainieren wollen. Diese Pakete bündeln ähnlich einem Docker-Container alle benötigten Laufzeitumgebungen, Bibliotheken und so weiter, um sofort mit den gewünschten Modellen

loslegen zu können. Laut Nvidia sollen sie bald ebenso verbreitet sein wie Nvidias CUDA-Bibliotheken und mit diesen parallel existieren. NIMs kann man nutzen, wenn man sich für eine kostenlose Testperiode von Nvidia Enterprise anmeldet, muss nach deren Ablauf aber eine Abogebühr zahlen.

Backwell-Doppelchips

Obwohl Huang beteuerte, Nvidia sei weder eine Hard- noch Softwarefirma, sondern eine KI-Firma, war die Vorstellung der neuen Blackwell-Architektur für Beschleunigerchips das Kernthema seiner Eröffnungsrede. Die Produkte will man später im Jahr an Partner und Kunden ausliefern; wie viel später, verrät Nvidia indes aber auch auf Nachfrage nicht. Ebenso machte man ein ziemliches Geheimnis um viele weitere Chipdetails, die man früher freimütig preisgegeben, ja sich sogar mit ihnen gebrüstet hatte. Offenbar spüren die Kalifornier langsam den Wind im Gesicht, der ihnen aus Richtung der Konkurrenz entgegenzuwehen beginnt.

Die wenigen Eckdaten, die Nvidia veröffentlicht, lesen sich wie immer beeindruckend: 208 Milliarden Transistoren, in KI-geeigneter FP8-Genauigkeit bei dünn besetzten Matrizen 10 Billionen Rechenoperationen pro Sekunde (TFlops). Das stellt gegenüber dem Vorgänger immerhin Faktor 2,5 dar. Die acht Stapel HBM3-Speicher fassen 192 GByte und übertragen mit 8 Terabyte pro Sekunde zwei Drittel mehr als beim Vorgänger. Wenn HBM3e später auch mit 16 statt nur 12 Lagen verfügbar ist, dürfte eine Version mit noch mehr Speicher folgen.

Für Blackwell nutzt Nvidia wie viele Konkurrenten die Chiplet-Technik. Bei der Variante Blackwell B200 kombiniert man zwei identische, mit rund 800 mm² riesige Siliziumchips mit acht HBM3e-Stapel-Speichermodule. Eine genaue Chipgröße nennt Nvidia für die beiden riesigen Chips nicht und spricht nur von „reticle sized“, also dem per Lithografie belichtbaren Maximum. Dieser Wert liegt knapp über 820 mm².

Die dritte zentrale Komponente der Blackwell-Architektur sind die NVLinks, Nvidias proprietäre Chip-zu-Chip-Verbindungen, über die jede GPU mit ihren Pendants auf anderen Boards kommuniziert. Diese Technik ist so entscheidend, dass sich die KI-Konkurrenten für eine freizunutzbare Vernetzungstechnik im Ultra-Ethernet-Consortium zusammenge-

geschlossen haben und bei jeder Gelegenheit betonen, wie wichtig eine Technik ohne Herstellerbindung, das sogenannte „Vendor Lock-in“, sei.

Die Übertragungsrate hat Nvidia für die nunmehr fünfte NVLink-Generation auf 1,8 Terabyte pro Sekunde verdoppelt. Bis zu 576 GPUs können über die passend dazu erneuerten NVSwitches in einer Domäne hängen und mit voller Geschwindigkeit auf die Speicher der anderen Chips zugreifen. Insgesamt soll die neue NVLink-Generation KI-Supercomputer mit 100.000 GPUs ermöglichen, jede davon über 25.000 Euro teuer.

Micro-Tensors

Diese schnelle Kommunikation ist wichtig für eine weitere Blackwell-Neuerung, die sich in den Tensor-Kernen der vierten Generation versteckt und Micro-Tensors genannt wird. Mittels Optimierungsläufen kann man in den integrierten Transformer-Engines den für verschiedene Szenarien besten Level of Zusammenarbeit ermitteln. Diese offiziell als „Mixture of Experts“ (MoE) bezeichnete Vorgehensweise bestimmt Anzahl der Tensor-Kerne oder GPUs, die über verschiedene Stufen besonders großer Large-Language-Models mit Billionen von Parametern. Verschiedene Kombinationen aus gewünschtem Durchsatz pro GPU (im Endeffekt also der Kosten des KI-Services) und Reaktionsfähigkeit auf User-Eingaben (also die Reaktionsgeschwindigkeit und damit die gefühlte Qualität des Dienstes) führen mit unterschiedlichen Synchronisationsspannen von Tensoren, Pipeline, Experten und Daten zu den besten Resultaten.

Geht es nach Nvidia, lässt sich bei einem GPT-MoE-Modell mit 1800 Milliarden Parametern und passender Optimierung ein Geschwindigkeitsplus von Faktor 30 gegenüber der Hopper-Generation erreichen. Dazu synchronisiert man Tensoren über zwei GPUs, die Experten über 16 GPUs und die Pipelines über zwei GPUs (TP2.EP16.PP2). Ohne MoE sei es immer noch Faktor 7. Doch es gibt noch weitere Optimierungen wie eine selektive Reduzierung der Rechengenauigkeit bis hinab auf FP6 und sogar FP4, die die Blackwell-Rechenwerke verarbeiten. Im theoretischen Idealfall lässt sich mit FP4 im Vergleich zu FP8 ein doppelt so großes KI-Modell in derselben Speichergröße unterbringen und die Berechnungen laufen doppelt so schnell. FP6 spart hingegen nur Speicherplatz und Speichertransferrate.

Die reduzierten Datenformate kommen nur bei ausgewählten Operationen zum Einsatz, sodass das Ergebnis nur minimal unpräziser wird.

Kurios niedrig ist der Blackwell-Durchsatz bei Gleitkommazahlen mit 64 Bit Genauigkeit, die typischerweise abseits von KI speziell in Supercomputern oder beim High-Performance-Computing zum Einsatz kommen. Für einen Blackwell-Doppelchip gibt Nvidia 45 TFlops an, der Vorgänger H100 kam bereits auf 60 und die Matrix-Multiplikatoren von AMDs Instinct MI300X sogar auf 163 TFlops. Es scheint, als habe Nvidia hier der KI den Vorrang gegeben.

Two Chips, one GPU

Aus Softwaresicht sollen die beiden Chips sich wie eine einzige GPU verhalten, ein wichtiges Kriterium, dessen Fehlen Entwickler zum Beispiel bei AMDs Rechenbeschleuniger Instinct MI250X bemängelten, der in Top-Supercomputern wie El Capitan oder Lumi zum Einsatz kommt. Dazu verbindet Nvidia die beiden Chips über eine schlicht High Bandwidth Interface (HBI) genannte Schnittstelle mit einer kombinierten Übertragungsrate von 10 Terabyte pro Sekunde. Genauer wollte man sich nicht zur genutzten Technik äußern. Hinter den Kulissen erfuhr c't aber,

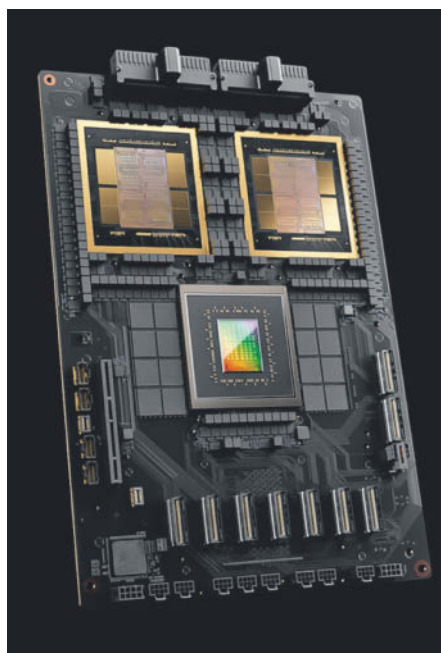


Bild: Nvidia

Die Kombination aus zwei Blackwell-GPUs und einer Grace-CPU bezeichnet Nvidia als GB200-Superchip. Speicher und Verbindung zur CPU müssen sich die Blackwells teilen.

dass es zumindest keine Abwandlung der NVLink-Technik ist, die zum Einsatz kommt, um mehrere Boards miteinander zu verbinden.

Bereits in den Vorgängern A100 und H100 hatte Nvidia zwei Chiphälften intern über zwei Partitionen des gemeinsam genutzten Level-2-Caches gekoppelt, aufgeteilt in Near-L2 und Far-L2. Es wäre naheliegend, wenn diese Erfahrungswerte nun in ähnlicher Form für die Chip-zu-Chip-Verbindung über Siliziumgrenzen hinweg einfließen.

Kilowatt-Klasse

Blackwell soll es wie von Hopper bekannt in verschiedenen Versionen geben: als passiv luftgekühltes Open-Accelerator-Module (OAM) für den Einsatz als HGX-B100-Achtlingsverbund mit 700 Watt oder als DGX-B200 bei bis zu 1000 Watt pro GPU für Flüssigkühlung. Die Drei-Chip-Kombo aus zweimal Blackwell und einem der hauseigenen Grace-ARM-Prozessoren heißt GB200 und schluckt bis zu 2,7 Kilowatt; je 1,2 davon entfallen auf jede Blackwell-GPU.

In die vorgefertigten Serverschränke „GB200 NVL72“ baut Nvidia 18 GB200-Nodes mit je zwei GB200-Boards in einem 1U-Serverschränkeinschub ein, der dann aber Flüssigkeitskühlung erfordert. Dazu kommen neun 1U-Einschübe mit je zwei NVSwitches, die alle GPUs untereinander mit voller Geschwindigkeit über Kupferkabel vernetzen. Für die kurze Distanz sei optische Übertragung nicht vorteilhaft, erläuterte ein Nvidia-Manager. Im Gegenteil würden die nötigen Transceiver weitere 20 Kilowatt schlucken. Bereits ohne diese braucht so ein Schrank insgesamt bis zu 120 kW.

Das klingt enorm viel, geht aber mit einer starken Erhöhung der Rechenleistung einher, sodass Blackwell am Ende um (wohlwollend gerundete) Faktor 4 effizienter als die Vorgänger sein soll. Nvidia-Chef Huang bemühte dazu das oben genannte GPT-MoE-1,8T-Modell als Beispiel: Für einen in 90 Tagen abgeschlossenen Trainingslauf bräuchte man 8000 Hopper-GPUs mit einer Leistungsaufnahme von rund 15 Megawatt. Mit allen Optimierungen käme ein Blackwell-GB200-basierter Supercomputer im selben avisierten Zeitraum mit 2000 GPUs und 4 Megawatt aus. (csp@ct.de) **ct**

Transparenzhinweis: Nvidia bezahlte Anreise und Unterkunft für den Autor.

Datenschutznovelle stärkt die Schufa

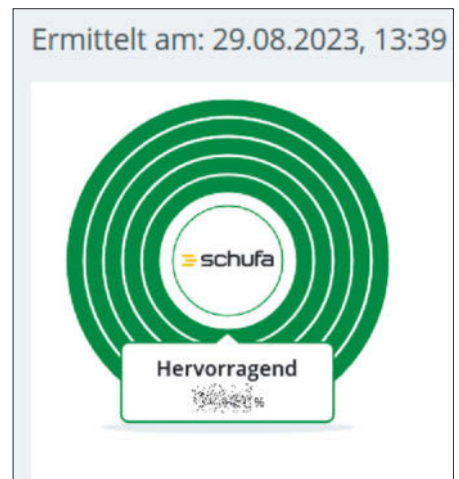
Eigentlich soll die Überarbeitung des Bundesdatenschutzgesetzes die Bürgerrechte bei der Kreditwürdigkeitsprüfung verbessern. Doch das Verbot, die Adressen von Verbrauchern zu nutzen, könnte ausgerechnet der größten deutschen Auskunft in die Hände spielen.

Der Plan der Bundesregierung, Wirtschaftsauskunfteien wie der Schufa im neuen Bundesdatenschutzgesetz (BDSG) künftig die Nutzung von Verbraucheradressdaten bei der Kreditwürdigkeitsprüfung zu verbieten (c't 5/2024, S. 47), hat offenbar ungewollte Nebenwirkungen. Wie es aus den Verbraucherzentralen heißt, könnte die Regelung die Macht des Marktführers Schufa vergrößern, obwohl das Gesetz eigentlich die Datensammelwut von Auskunftsteien einschränken soll, um einem Urteil des Europäischen Gerichtshofs nachzukommen (c't 1/2024, S. 32).

Der Grund: Die Schufa erhält von nahezu allen Banken und Sparkassen, aber auch von vielen Versandhändlern und Dienstleistern Daten über Verbraucher, etwa zur Existenz von Girokonten, Kreditkarten oder Mobilfunkverträgen. Schufa-

Konkurrenten wie Boniversum, Crif (früher Bürgel) oder Infoscore müssen sich mit einer deutlich geringeren Berechnungsbasis begnügen. Die Schufa kann es sich daher schon jetzt leisten, Adressdaten nur ausnahmsweise in die automatische Berechnung der Kreditwürdigkeit („Scoring“) einzubeziehen. Ihre Wettbewerber sind hingegen häufiger auf die Adressen angewiesen. So verweist etwa Boniversum auf seiner Homepage darauf, dass das Wohnumfeld von Verbrauchern aussagekräftige Hinweise zur Zahlungswahrscheinlichkeit liefere. Das kritisieren Verbraucherschützer seit langem als diskriminierend.

Mit dem Wegfall der Adressdaten würde der Score der Schufa-Konkurrenten eine Hauptkomponente verlieren, während die Situation bei der Schufa unverändert bliebe. Experten befürchten daher, dass sie endgültig zum Monopolisten werden und Marktbedingungen vorschreiben könnte. Zudem hätte eine fehlerhafte Datenbasis der Schufa dann noch stärkere Auswirkungen auf betroffene Verbraucher als bisher. Ein ähnliches Dilemma könnte auch das im BDSG-Entwurf vorgesehene Verbot bringen, die



Die Schufa hat beim Scoring eine bessere Datengrundlage als ihre Konkurrenz. Das neue BDSG könnte diesen Wettbewerbsvorteil weiter vergrößern.

Bonität anhand der Umsatzdaten von Girokonten zu berechnen. Dieser Methode bedienen sich beispielsweise einige Kreditportale, die dafür sogenannte Open-Banking-Dienstleister wie Klarna oder Tink einbinden. Sie kämen künftig wohl ebenfalls nicht mehr an der Schufa vorbei. (mon@ct.de)

Entwickler contra In-App-Browser

In der Non-Profit-Organisation Open Web Advocacy (OWA) organisierte Entwickler fordern, die **EU solle In-App-Browser stärker an die Kandare nehmen**. Solche Browser springen in Smartphone-Apps häufig anstelle des voreingestellten Browsers an, wenn man auf einen Link klickt, und liefern eine eigene Web-Ansicht. Laut OWA können solche In-App-

Browser jedoch die angezeigte Website manipulieren oder die Aktivitäten des Nutzers tracken. So hätten Sicherheitsforscher bereits JavaScript-Injektionen in viel genutzten Apps wie Instagram, Facebook oder TikTok nachgewiesen.

OWA hält aber auch die von iOS und Android für Entwickler bereitgestellten datenschutzkonformen In-App-Browser

für problematisch, da sie letztlich die Browserwahl des Nutzers und damit Vorgaben des Digital Markets Act (DMA) der EU ignorieren. Die Gruppe fordert daher klare Vorgaben für Apple und Google. Insbesondere sollten Apps, die in deren App-Stores angeboten werden, http- und https-Links grundsätzlich nur im Standardbrowser öffnen dürfen. (mon@ct.de)

Yahoo kauft Artifact

Der US-Internetdienst Yahoo hat den angeschlagenen Nachrichtendienst Artifact erworben, der zu einem vom Nutzer gewünschten Thema mittels generativer KI eine Nachrichtenauswahl aus dem Web lieferte. Die einzelnen Meldungen fasste es zusammen, auch der Stil (etwa kindgerechte Sprache) ließ sich dabei vorab festlegen. Unmittelbar nach der Übernahme **nahm Yahoo Artifact vom**

Netz. Das neue Mutterunternehmen ist in erster Linie an der Technik des Dienstes interessiert und will diese nun sukzessive in eigene Angebote einbauen; Artifacts Belegschaft übernahm Yahoo nicht. Auch die Artifact-Gründer Kevin Systrom und Mike Krieger sollen nur übergangsweise als Berater fungieren. Zum Kaufpreis machten weder sie noch Yahoo Angaben.

Bereits im Januar 2024 hatten die Gründer bekannt gegeben, den Dienst aus wirtschaftlichen Gründen einzustellen und ihre Mitarbeiter zu entlassen. Kurz vor der Übernahme hatten sie jedoch verlauten lassen, Kernfunktionen der Nachrichtenauswahl und -zusammenfassung persönlich weiterbetreiben und lediglich die Social-Media-Funktionen streichen zu wollen. (mon@ct.de)



Neu: c't-Verbraucherschutz-Podcast „Vorsicht, Kunde!“

Bereits seit 20 Jahren berichtet c't über Streitigkeiten zwischen Kunden und Händlern, Herstellern oder Servicemitarbeitern. Jetzt gibt es die Fälle auch auf die Ohren.

Im neuen Verbraucherschutz-Podcast „Vorsicht, Kunde!“ diskutieren Ulrike Kuhlmann und ihr c't-Kollege Urs Mansmann skurrile Konflikte, die Kunden ausfechten mussten. Unterstützt werden Urs und Ulrike von Rechtsanwalt Niklas Mühleis. Grundlage der im Podcast besprochenen Streitigkeiten sind reale Konflikte aus der c't-Magazinrubrik „Vorsicht, Kunde!“.

Die Drei knöpfen sich ausgewählte Fälle vor, beleuchten, was dort schiefgelaufen ist, und erklären die rechtlichen Aspekte. Dabei geht es um Tücken bei Vertragsabschlüssen, Garantieleistungen oder Reparaturabwicklungen, denn diese laufen nicht immer problemlos ab. Sie liefern viele Tipps und praktische Ratschläge, was Kunden in solchen und ähnlichen Streitfällen unbedingt vermeiden sollten und wie sie am besten zu ihrem Recht kommen.

Die aktuelle Episode 3 des Podcast dreht sich beispielsweise um die Glasfaser und das Nebenkostenprivileg. Im Podcast klären Ulrike, Urs und Niklas, was der Glasfaseranschluss bringt, wann Vermieter diesen verhindern können und ob Mieter frei über ihren Provider entscheiden dürfen. Letzteres wird auch mit dem Wegfall des Nebenkostenprivilegs interessant. Und sie diskutieren, wer die Kosten für den Anschluss übernimmt.

Den neuen Verbraucherschutzpodcast von c't finden Sie alle 14 Tage freitags überall dort, wo es Podcasts gibt. Sämtliche Episoden gibt es auch auf der Website ct.de/vorsichtkunde oder über den folgenden QR-Code: (uk@ct.de)



Hier gehts zum
Verbraucherschutz-
Podcast
„Vorsicht, Kunde!“

Entdecken Sie die nächste Stufe des KI-Computings:

NVIDIA Blackwell

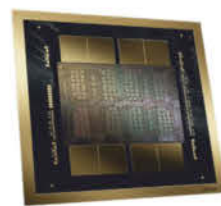


NVIDIA Blackwell: bahnbrechende Leistung, Effizienz und Innovation

Beschleunige dein KI-Training um das Vierfache, erreiche 30-mal mehr Inferenzleistung und senke den Energieverbrauch um das 25-fache. Mit sechs revolutionären Technologien und drei leistungsstarken Systemkonfigurationen steht NVIDIA Blackwell für unübertroffene KI-Leistung. Erlebe die Zukunft heute!

NVIDIA HGX™ B100

NVIDIA GB200-SUPERCHIP



NVIDIA HGX™ B200

Die NVIDIA HGX™ B200 katapultiert das Rechenzentrum in eine neue Ära des beschleunigten Computings und generativer KI, indem er NVIDIA Blackwell GPUs mit Hochgeschwindigkeits-Interconnect integriert, um KI-Leistung im großen Maßstab zu beschleunigen. Als erste beschleunigte Scale-up x86-Plattform mit bis zu 15-mal schnellere Echtzeit-Inferenzleistung bei 12-mal geringeren Kosten und 12-mal weniger Energie, HGX B200 ist für die anspruchsvollsten KI-, Datenanalyse- und Hochleistungs Computing (HPC)-Workloads entwickelt.



sysGen

Ihr NVIDIA Elite Partner für Technologie und Lösungen

Systeme und Informatikanwendungen Nikisch GmbH
Geschäftsführung: Gabriele Nikisch, Sergius Siczek
UST – ID. NUMMER: DE 177360158

Am Hallacker 48, 28327 Bremen
Telefon: 0421 - 40966-0 / E-Mail: info@sysgen.de

Web: www.sysgen.de

Avatar übersetzt simultan in Gebärdensprache

Ein 3D-Avatar aus einem Forschungsprojekt überträgt Texte automatisiert in Gebärdensprache, um zum Beispiel gehörlose Reisende kurzfristig über Fahrplanänderungen zu informieren.

Im Verbundprojekt AVASAG haben sechs Partner einen Gebärdensprache-Avatar entwickelt, der Texte aus dem Themenfeld Reisen automatisiert in Gebärdensprache überträgt. Der Avatar kann gerade bei dynamischen Inhalten wie etwa aktuellen Zugverspätungen eine neue Informationsmöglichkeit für Gehörlose schaffen. Für viele Menschen mit akustischem Handicap sind auch schriftliche Texte wie eine Fremdsprache, da es für sie viel schwerer als für Hörende ist, das Lesen und Schreiben zu erlernen.

Die Projektarbeit beschränkte sich nicht nur darauf, unter der Leitung des Softwareunternehmens Charamel einen 3D-Avatar zu entwickeln. Zugleich kamen menschliche Gebärdensprachler zum Zuge, deren Beispielsätze durch Kameras und Motion Capturing an der Technischen Hochschule Köln aufgenommen und ana-

lysiert wurden. An der Universität Augsburg entstand ein Tool, das hilft, die genauen Bewegungen im zeitlichen Ablauf zu erfassen, und am DFKI trainierten Forscher eine künstliche Intelligenz, die Texte in einen Strom aus Gebärden übersetzt.

Nach dem Projektabschluss haben 68 Gehörlose die Gebärdensprache des Avatars namens Livian mit der des Prototypen Gloria und der menschlichen Gebärdensprecherin Sonja verglichen. Die objektive Verständlichkeit schätzten die Teilnehmer

bei allen drei Beispielen positiv ein, bei Livian und Sonja noch etwas besser als bei Gloria. Bei der subjektiven Akzeptanz lag allerdings der Mensch weiterhin vorn.

Der Avatar ist dafür konzipiert, auf Infoterminals, Websites und in mobilen Apps aktuelle Informationen zu vermitteln. Um das System auch auf andere Themengebiete zu übertragen, bedarf es noch weiterer Forschungsarbeit. (agr@ct.de)

Projektseite: ct.de/yq5r

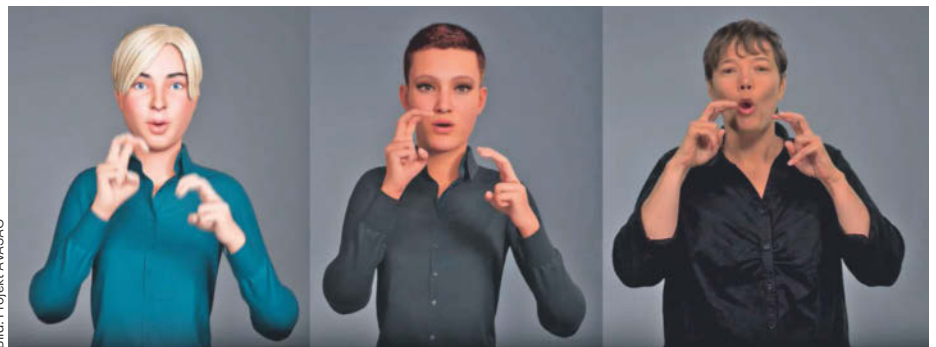


Bild: Projekt AVASAG

Gebärdensprache im Vergleich: Prototyp Gloria (links) wirkt noch etwas cartoonig, Livian daneben stellt die jüngste Entwicklung dar. Sonja (rechts) ist eine Gebärdensprecherin, die am Projekt mitgewirkt hat.

Cubesat für Quantenschlüssel

Ein Forscherteam unter der Leitung des Fraunhofer-Instituts für Optik und Feinmechanik (IOF) hat Technik zur Quantenschlüsselverteilung für Mikrosatelliten komprimiert. Neben einer handteller-großen Photonenquelle, die **eine Million verschränkte Photonenpaare pro Sekunde** erzeugt, gehören dazu zwei Teleskope mit Strahlnachführung und Feinausrichtung. Diese Technik soll die optische Verbindung zu zwei Bodenstationen stabilisieren.

Das System passt in einen Cubesat der Größenklasse 16U mit maximal 20 × 20 × 40 Zentimeter Bauraum. Der soll bei nur einem Überflug einen Quantenschlüssel von 256 Bit zwischen zwei etwa 300 Kilometer entfernten Standorten verteilen können. Gemäß Quantenphysik kann ein Angreifer die Übertragung verschränkter Photonen nicht unbemerkt abhören. Per Glasfaserleitung ist die Quantenschlüsselverteilung auf Strecken bis etwa 200 Kilometer begrenzt. (agr@ct.de)



Bild: Fraunhofer IOF

Kompakte Technik vereinfacht in Zukunft die Quantenschlüsselverteilung: Ein Cubesat im Orbit teilt verschränkte Photonenpaare auf und schickt die beiden Photonenstrahlen an zwei Bodenstationen, die damit gemeinsame Schlüssel generieren.

Radar scannt Fahrerfitness

Mit einem kompakten Radargerät, das sich in den Fahrzeuginnenraum integrieren lässt, hat ein Team um George Shaker an der University of Waterloo ein **medizinisches Überwachungsinstrument für Autofahrer** entwickelt. Das Gerät selbst ist etwa so groß wie ein Zehn-Cent-Stück. Mit seiner Auflösung erfasst es die Brustkorb-bewegungen der Person hinter dem Steuer. Eine integrierte KI bestimmt daraus Atmung und Puls und erkennt veränderte Atemmuster oder Herzrhythmen, durch die sich Herz-Kreislauf-Erkrankungen verraten. So nutzen Reisende die Zeit am Steuer für eine kontinuierliche medizinische Beobachtung. Nach einer Fahrt könnte das Gerät dem Fahrer einen Report zum Verlauf seiner Vitalwerte direkt aufs Smartphone schicken. Dabei achteten die Wissenschaftler auf den Schutz der Bi-daten: Alle Messungen werden nicht in der Cloud, sondern lediglich lokal gespeichert. (agr@ct.de)



S2N

Storage Server Network

Die neue heise-Konferenz für Storage, Server, Network

Die S2N ist der Branchentreff für IT-Administratoren, Systemarchitekten, CTOs und alle IT-Spezialisten. Die zweitägige Konferenz informiert über die neuesten Trends und Technologien in den Bereichen **Netzwerkarchitektur und -management, Serverarchitekturen und moderne Speicherlösungen.**

Die **S2N** ist hervorgegangen aus der storage2day, der heise-Konferenz für Speichernetze und Datenmanagement, und erweitert deren Themenspektrum um Server und Netzwerke.

Call for Proposals läuft bis zum **19. April:**

Haben Sie IT-Know-how, das Sie mit Fachkolleginnen und -kollegen teilen wollen?
Möchten Sie von eigenen Erfahrungen berichten und sie mit einem Fachpublikum diskutieren?
Wir freuen uns über Ihre Themeneinreichungen!



Premiere in Hamburg
am 9. & 10. Oktober

Platinsponsor

INFINIDAT

Goldspensoren

THOMAS
KRENN
IT's people business

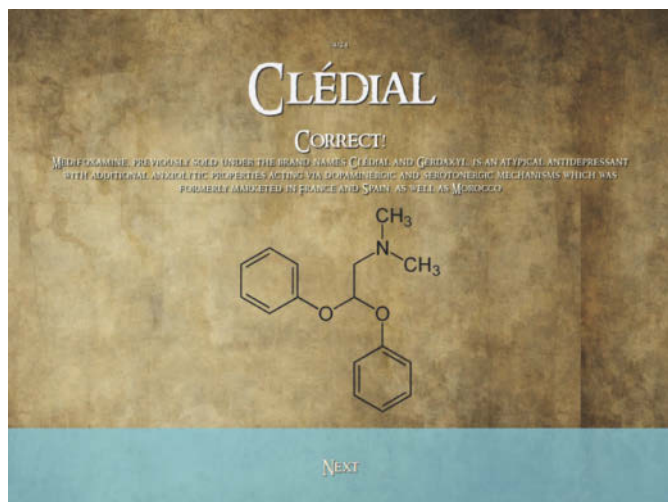


s2n.heise.de

Fantasy gegen Depressionen

<https://antidepressantsortolkien.vercel.app>

Wissen Sie, wer oder was Eronon, Minalcar und Orophin sind? Klingt nach Bekannten von Legolas, Aragorn und anderen Gestalten aus dem Herrn der Ringe. Aber nicht alles, was danach klingt, entstammt auch wirklich dem Legendarium von J. R. R. Tolkien. Zumindest namensschöpferisch scheint ihm nämlich ausgerechnet die Pharmaindustrie das Wasser zu reichen.

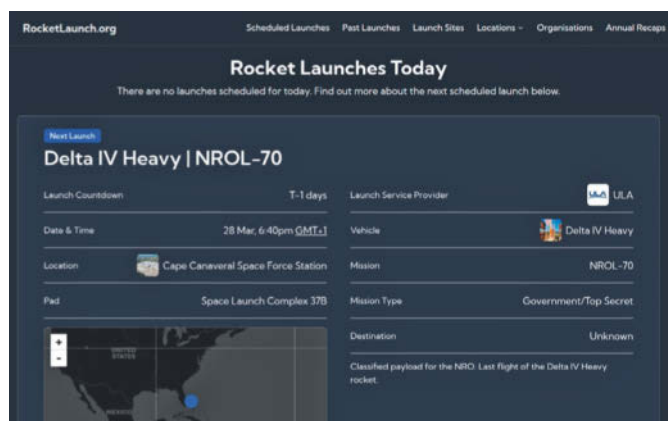


Klingt abstrus, aber die Seite **Antidepressants or Tolkien** stellt es mit einem simplen Spiel unter Beweis: In 24 Fragen muss man entscheiden, ob ein gegebener Name vom Vater der modernen Fantasy-Literatur oder von der PR-Abteilung eines Medikamentenherstellers stammt. Das ist selbst für Fantasy-Fans nicht immer einfach. Und nebenher lernt man Kleinigkeiten über reale Antidepressiva und fantastische Charaktere. (syt@ct.de)

Raketenstartplan

<https://rocketlaunch.org>

Wenn SpaceX eine neue Rakete testet oder Crewmitglieder zur ISS fliegen, mag es noch Medienrummel geben. Ansonsten sind Raketenstarts ein ziemlich alltägliches Ereignis geworden, das medial kaum Beachtung findet.



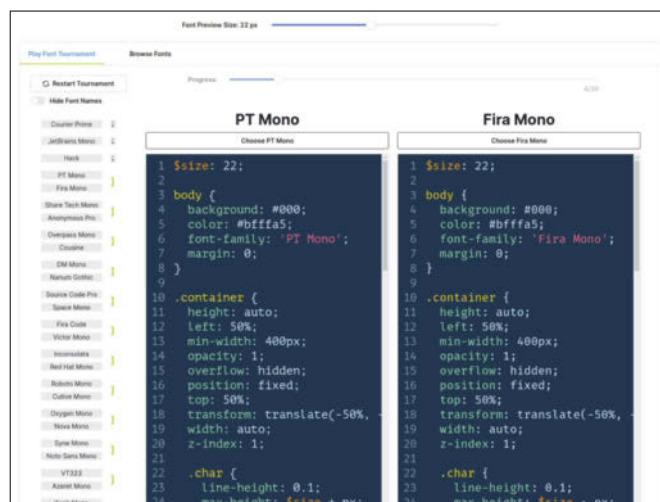
Die Website **RocketLaunch.org** dagegen informiert über jeden einzelnen Start mit Eckdaten zur Mission, Startplattform, dem Unternehmen hinter dem Raketenstart und dem Raketen-typ. Livestreams verlinkt die Seite auch, und zu Unternehmen, Startplattformen und Rakentypen gibt es jeweils eigene Steckbriefe.

Wer will, kann auch in Meldungen zu vergangenen Starts stöbern oder sich unter „Annual Recaps“ ansehen, welche Missionen in welchem Jahr besonders bedeutsam waren. Die Seite entfaltet durchaus einen gewissen Sog und plötzlich liest man über die „Rocket Factory Augsburg“, die im Juni dieses Jahres ihren Jungfernflug vom SaxaVord Spaceport auf den Shetland-inseln plant. (syt@ct.de)

Kampf der Schriftarten

<https://www.codingfont.com>

Es gibt Dutzende Schriftarten speziell für Softwareentwickler: Fonts, die sich besonders gut zum Programmieren eignen sollen, aber auch zur Darstellung von Reintext-E-Mails oder im Texteditor. Merkmale sind besonders leicht erkennbare Buchstabenformen, deutliche Unterschiede zwischen der Eins und dem kleinen L, der Null und dem großen O oder auch spezielle Ligaturen, die beispielsweise häufige Operatoren wie `<=` als `<=` darstellen.



Letztlich sind Schriftarten aber Geschmackssache. Bei der Suche nach dem persönlichen Favoriten hilft die Website **CodingFont** ungemein. Sie listet 30 frei verfügbare Programmierer-Schriftarten auf und bietet gleich eine Vorschau. Vor allem aber treten die Schriftarten auf der Website in einem K.-o.-System gegeneinander an, auf Wunsch auch blind, also ohne Anzeige der Fontnamen. Man wählt einfach aus jeweils zwei als Codebeispiel angezeigten Schriftarten diejenige aus, die einem besser gefällt. Nach 30 Schritten steht der persönliche Sieger fest und man kann ihn direkt herunterladen. (syt@ct.de)

Diese Seite mit klickbaren Links: ct.de/yzwt

NIX VON DER STANGE!

Wunsch-PC selber bauen oder aufrüsten



Günstige Zeiten für PC-Bastler: keine Lieferschwierigkeiten für Hardware mehr, bei den Prozessoren gibt's so viel Rechenleistung wie noch nie und die SSD- und RAM-Preise sind auf niedrigem Niveau. Mit den Bauanleitungen und Aufrüsttipps aus diesem c't-Sonderheft bauen Sie Ihren Wunsch-PC oder schenken Ihrem geliebten alten PC-Schätzchen noch mehr Lebenszeit.

TRAUEN SIE SICH!



- Bauvorschläge für Gaming-PC/ Allrounder
- Nachhaltig und günstig: Alter Rechner länger nutzen
- Praxisanleitung: Windows auf neue SSD umziehen
- Der große CPU-Wegweiser

Heft für 14,90 € • PDF für 12,99 € • Heft + PDF 19,90 €



shop.heise.de/ct-hardwaretipps24



Wie ein Roboter

Mediamarkt wimmelt Gewährleistung ab

Wenn ein gekauftes Gerät einen Mangel zeigt, hat der Kunde die Wahl, ob es repariert oder gegen ein neues ausgetauscht werden soll. Viele Händler umgehen das routiniert wie zum Beispiel MediaMarkt.

Von Tim Gerber

Um sein Reihenendhäuschen in einem kleinen Ort im Allgäu sauber zu halten, erwarb Thomas S. Ende Oktober 2022 über den Webshop von MediaMarkt für 1000 Euro einen Wisch- und Saugroboter vom Typ L10s des chinesischen Herstellers Dreame. Zunächst funktionierte der Haushaltshelfer ganz ordentlich. Nur das

Aufnehmen von Wasser aus seiner Basisstation klappte nicht immer wie vorgesehen. Doch damit konnte Thomas S. einstweilen leben.

Im Frühjahr 2023 nahmen die Probleme mit dem Putzroboter jedoch zu. Zunächst verstopfte die Basisstation immer mehr, dann löste sich die Lenkrolle an der Front allmählich aus ihrer Plastiklagerung. Ende Februar 2023 wandte Thomas S. sich an den Garantieservice des Herstellers. Nach einer Woche hieß es dann, er könne den Roboter zur Reparatur einschicken.

Das wollte Thomas S. eigentlich nicht. Ein neues Gerät ohne Mängel wäre ihm lieber gewesen. Deshalb rief er Anfang März bei MediaMarkt an. Er könne das Gerät einsenden oder in einem Markt abgeben, damit man das prüfen könne, hieß es. Anfang April 2023 hatte sich das Vorderrad des Roboters endgültig aus seiner

Aufhängung gelöst und der Roboter war nicht mehr brauchbar.

Am 10. April sandte Thomas S. das Gerät an den Herstellerservice. Der ließ sich mit der Bearbeitung Zeit. Einen Monat später war noch immer nichts geschehen. Mitte Mai kam dann der Saugroboter wieder bei Familie S. an. Laut mitgesendetem Bericht war jedoch nur die Aufhängung des Vorderrads repariert worden.

Aktenzeichen ungelöst

Die Probleme, dass der Roboter das Wasser zum Reinigen weder ordentlich ansaugte, noch das schmutzige Wasser hinterher ordentlich abpumpte, blieb jedoch bestehen. In den folgenden Wochen und Monaten verrichtete der Roboter seinen Dienst deshalb immer schlechter und verschmutzte trotz vorschriftsmäßigem Betrieb zusehends.

Anfang Januar blockierte die Lenkrolle erneut und kratzte über den Fußboden, woraufhin Thomas S. am 12. Januar ein weiteres Mal reklamierte. Da der L10s permanent Schwierigkeiten machte, schlug er vor, ihn gegen Aufpreis gegen das bessere Modell L20s umzutauschen.

Eine Antwort blieb aus. Also kontaktierte Thomas S. den Mediamarkt am 22. Januar. Sein Fall sei in Bearbeitung, hieß

es, er möge noch etwas Geduld haben. Am 23. Januar kam eine E-Mail: „Eine Rücknahme lehnen wir zu diesem Zeitpunkt ab“, hieß es kurz und bündig. „Rein vorsorglich“ wies der Kundenservice darauf hin, „dass das Recht auf Rücktritt vom Kaufvertrag erst nach zweimaliger erfolgloser Nachbesserung ein und desselben Fehlers möglich ist.“ Seiner Forderung auf Umtausch beziehungsweise Rücktritt vom Kaufvertrag könne man deshalb nicht entsprechen.

Wunschlos unglücklich

Umgehend antwortete Thomas S. dem Händler: Er könne das Gerät gern einsenden, wünsche aber keine Reparatur, sondern einen Umtausch im Rahmen der Gewährleistung. Darauf erhielt er von MediaMarkt ein Retourenlabel.

Am 2. Februar schickte Thomas S. den Roboter zusammen mit einer ausführlichen Fehlerbeschreibung zum zweiten Mal ein. Er gebe MediaMarkt zwar eine zweite Chance der Nachbesserung, schrieb der Kunde, setze hierfür allerdings eine Frist bis zum 23. Februar, um alle Fehler zu beheben. Andernfalls werde er vom Kauf zurücktreten und die Erstattung des Kaufpreises verlangen.

Am 12. Februar erhielt Thomas S. eine Auftragsbestätigung von MediaMarkt. Das Gerät sei nun eingegangen und werde geprüft und repariert, hieß es darin. Es sei verschmutzt, bemängelte der Eingangsbericht, woraufhin Thomas S. entrüstet zurückschrieb, dass es ja Teil der Mangelhaftigkeit sei, da das Gerät nicht ordentlich reinige und das Schmutzwasser von der Station nicht richtig abgesaugt werde.

Nachdem drei Wochen fruchtlos verstrichen waren, erklärte er am 24. Februar per E-Mail den Rücktritt vom Kaufvertrag. Davon gänzlich unbeeindruckt benachrichtigte MediaMarkt ihn am 27. Februar, dass sich die Reparatur beim Hersteller leider verzögere, er möge noch etwas Geduld haben. Die hatte Thomas S. längst nicht mehr und schickte am 28. Februar noch einen eingeschriebenen Brief an MediaMarkt hinterher, mit welchem er seinen Rücktritt vom Vertrag bekräftigte und zur Erstattung des Kaufpreises bis spätestens 8. März aufforderte.

Am 28. Februar hieß es seitens MediaMarkt, dass das Gerät erst am 20. Februar im Servicecenter eingetroffen sei und die Bearbeitung sieben bis acht Tage dauere.

re. Thomas S. war das inzwischen egal, er wollte nur noch sein Geld zurück. Dass MediaMarkt allein für die Erfassung und Weiterleitung an die Werkstatt über zwei Wochen benötigt hatte und dies nun ihm anlasten wollte, trieb seine Verärgerung über den Händler auf die Spitze.

Am 6. März ließ MediaMarkt ihn wissen, dass man seine Frist nicht akzeptieren könne und er ja einen Reparaturauftrag erteilt habe, ohne den das Gerät nicht geprüft werden könne. Wutentbrannt über diese Ignoranz wandte sich Thomas S. an c't.

Uneinsichtig

Wir fragten am 13. März bei MediaMarkt an, warum die Lieferung eines mangelfreien Roboters abgelehnt wurde und warum man sich mit dem Kunden nicht stattdessen auf den Kauf eines teureren Geräts verständigt hatte, was er ja schon im Jahr zuvor aufgrund der zahlreichen Mängel an dem Gerät angeboten hatte.

Am 21. März teilte die Pressestelle von MediaMarkt mit: „Die Überprüfung hat dazu geführt, dass der Hersteller den Defekt innerhalb seiner Garantie anerkannt hat.“ MediaMarkt habe als Händler keinen Einfluss auf die Ausgestaltung und den Umfang der Garantie.

Der Hersteller habe sich für eine Reparatur des Gerätes entschieden und das Gerät wurde in eine zertifizierte Fachwerkstatt übergeben. Die Reparatur sei nun abgeschlossen. „Der Saugroboter wurde komplett überholt und ist wieder voll funktionsfähig. Das Gerät wird nun umgehend an uns zurückgesendet. Wir

kontaktieren den Kunden, sobald wir den Saugroboter an ihn zurückgeben können“, hieß es in der Auskunft weiter.

Wir wiesen MediaMarkt umgehend darauf hin, dass das so nicht zutreffe. Vielmehr hatte Thomas S. den Roboter an MediaMarkt gesandt und um Lieferung eines mangelfreien Ersatzgerätes gebeten. Dass Kunden darauf einen Rechtsanspruch haben, sollten Händler wie MediaMarkt genau wissen.

Am 26. März teilte MediaMarkt uns mit, dass wir recht hätten. In diesem Fall habe der Kunde um die Lieferung eines teureren Geräts gegen Aufpreis gebeten. Diesem Wunsch hätte MediaMarkt nachkommen sollen, hieß es etwas reumütig. „zumal wir das defekte Gerät ohnehin hätten zurücknehmen müssen.“

Doch von der vermeintlichen Reue bekam Thomas S. nichts mit. Weder erstattete ihm MediaMarkt den Kaufpreis noch bot man ihm stattdessen den Erwerb eines anderen Modells an. Stattdessen teilte MediaMarkt ihm am 27. März mit, dass sein Putzroboter aus der Reparatur zurück sei und umgehend an ihn weitergeleitet werde. Thomas S. verweigerte die Annahme und will wegen der Erstattung des Kaufpreises nun einen Anwalt einschalten.

Verbotene Spiele

Der Fall von Thomas S. ist kein einzelner. Systematisch versuchen große Einzelhändler wie MediaMarkt, ihre Kunden im Gewährleistungsfall mit Ausreden hinzuhalten und von der Wahrnehmung ihres Wahlrechts zwischen Reparatur und Ersatzlieferung im Gewährleistungsfall abzuhalten.

Dabei ist man als Kunde lediglich verpflichtet, dem Verkäufer den mangelhaften Artikel zur Prüfung zur Verfügung zu stellen. Ob repariert oder gegen ein mangel freies Produkt ausgetauscht werden soll, bestimmt grundsätzlich der Kunde. Die pauschale Behauptung, dass dies unverhältnismäßig teuer sei, ändert daran nichts.

Auch berechtigt der Umstand, dass ein Austausch unverhältnismäßig teuer sei, nicht etwa automatisch dazu, das Gerät reparieren zu lassen. Vielmehr hätte man dem Kunden unter anderem mitteilen müssen, wie lange die Reparatur voraussichtlich dauern wird, um dies dann auch einzuhalten. Ungeachtet dessen ist das Verhalten von MediaMarkt, trotz eingeräumter Fehler sich nicht mit dem Kunden auf ein neues Ersatzgerät zu einigen, sehr unkulant. (tig@ct.de) **ct**

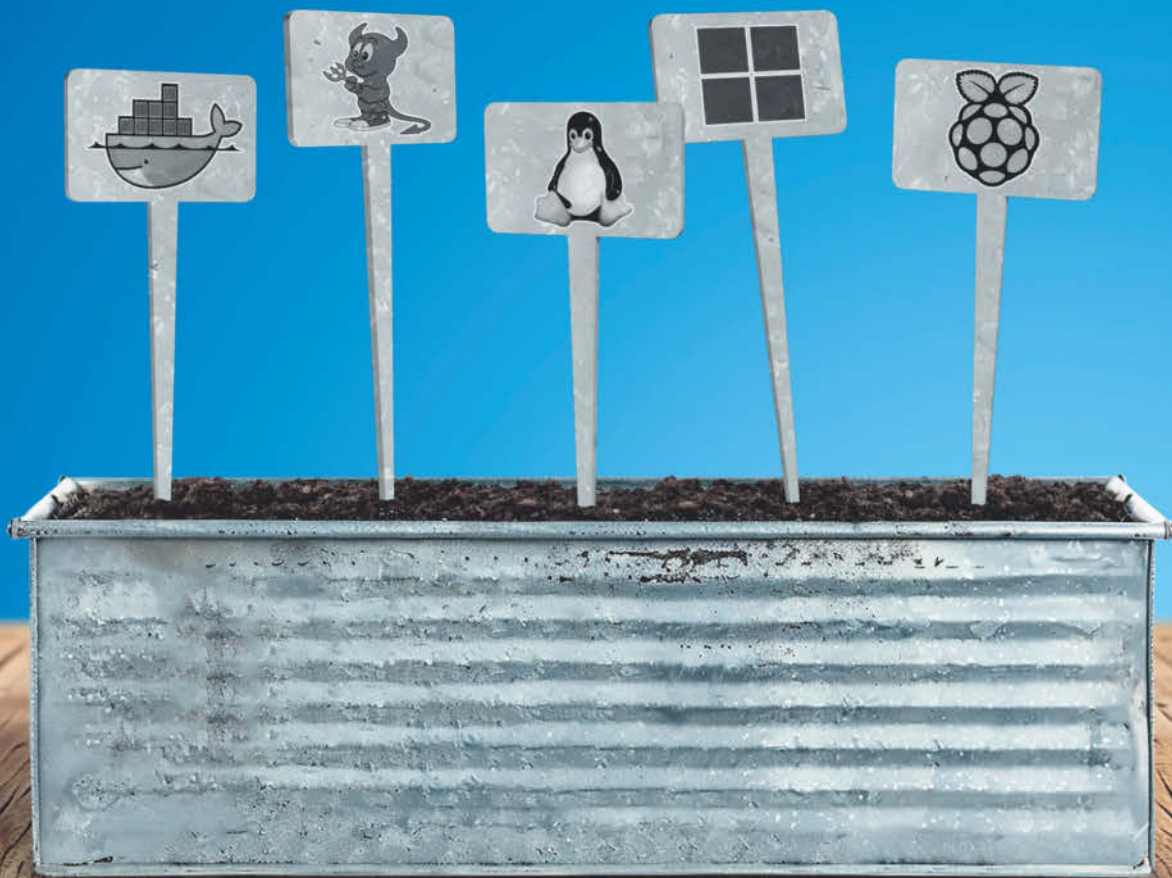
**VOR
SICHT
KUNDE!**



Die schwächliche Halterung des Lenkrades seines Saugroboters machte Thomas S. immer wieder zu schaffen. MediaMarkt wollte ihm dennoch kein Ersatzgerät liefern, auch nicht gegen Aufpreis.

Wahlfreiheiten

Virtualisierung – Universalbetriebssystem für PCs



Universalbetriebssystem für PCs	Seite 56
Proxmox VE vorgestellt	Seite 60
Loslegen mit Proxmox VE	Seite 64

Um VMware herrscht derzeit viel Wirbel, weil der Investor nur noch Abos verkaufen will und Produkte aufgibt. Doch in vielen Bereichen ist die Virtualisierungssoftware ohnehin nicht mehr das Maß der Dinge. Wir blicken auf die spannendsten Alternativen: von der Desktop-Virtualisierung über macOS-Spezialisten bis hin zum vielseitigen Server Proxmox. Vieles davon ist kostenlos oder sogar Open Source.

Von Peter Siering

Seit VMware vor 25 Jahren Virtualisierung in die x86-Welt einführte, laufen auf demselben PC in mehreren virtuellen Maschinen gleich mehrere Betriebssysteme friedlich nebeneinander, und zwar gleichzeitig. Praktisch ist das fürs Testen oder um Auslastung und Effizienz zu steigern. Virtualisierung wird inzwischen auch genutzt, um PCs sicherer zu machen.

Vorher war das in x86-Kreisen allenfalls über meist lahmarschige Emulationen realisiert. Schnell entwickelten sich dann nicht nur die dazu verwendete Software (Hypervisor) und Betriebssysteme weiter, sondern auch die PC-Hardware passte sich an.

Heute läuft Software in einer virtuellen Maschine kaum langsamer als auf realer Hardware. Allenfalls, wenn spezielle Fertigkeiten gefragt sind, etwa superschnelle Datenträgerzugriffe oder Grafikkarten als Coprozessoren oder für 3D-Spiele, lohnt es sich noch, Software nicht in eine VM zu packen, sondern sie auf echter Hardware loszulassen.

Die Vorteile einer virtuellen Maschine (VM) gegenüber einem realen PC überwiegen oft: Eine VM ist leicht auf andere Hardware zu übertragen, einfach vollständig zu sichern, ihr aktueller Zustand lässt sich einfrieren und zu späteren Zeitpunkten wiederherstellen und der Zugriff darauf ist üblicherweise auch aus der Ferne möglich. Auch der Sicherheit ist eine VM dienlich: Potenziell verseuchte Dateien öffnet man

darin ohne Konsequenzen, sofern die virtuelle Maschine abgeschottet ist.

Erklärrückblick

In der Anfangszeit der x86-Virtualisierung rechnete Anwendungssoftware in einer VM nur dann ungebremst, solange sie keine Systemaufrufe tätigte. Sobald Systemaufrufe auftraten, etwa Kontextwechsel ins Betriebssystem, musste die Virtualisierungssoftware diese beobachten und privilegierte Instruktionen emulieren, um die Hardware virtuell zu vervielfachen.

Diese Emulation der privilegierten, dem Betriebssystem vorbehaltenen Instruktionen fraß Ressourcen. Hinzu kam, dass die Software innerhalb einer VM auch die typischen PC-Ressourcen wie Grafik-

karte, Festplatte, Netzwerkkarte und so weiter nachbilden musste. Auch hier half in den Anfangstagen die Emulation gängiger PC-Komponenten, etwa einer S3-Grafikkarte, einer AMD-Netzwerkkarte und eines Buslogic-SCSI-Controllers.

Die in heutigen Prozessoren vorhandenen Funktionen für die Virtualisierung (Intel VT-x, AMD-V) erleichtern und beschleunigen das Ausführen der privilegierten Instruktionen. Die Befehlssätze und die darin geschaffene Softwarearchitektur wurden virtualisiert. Nach und nach bauten Intel und AMD obendrein Funktionen in ihre CPUs, um aus VMs heraus direkt Festplatten, USB-Geräte, Grafik- und Netzwerkkarten anzusprechen, was als I/O-Virtualisierung bekannt ist (I/O steht für Input/Output, also Ein-/Ausgabe).

In heutige Betriebssysteme integrierte spezialisierte Treiber für Festplatten, Netzwerke und Grafikkarten sprechen direkt mit der Virtualisierungssoftware. Sie nehmen eine Abkürzung, sodass aufwendiges Emulieren von PC-Komponenten entfallen kann. Der gängige Name dafür: Paravirtualisierung. Das alles zusammengekommen stellt für aktuelle x86- und auch ARM-Hardware und -Betriebssysteme den gemeinsamen Nenner dar.

Zusammenwirken

Virtualisierungssoftware bindet die Einzelteile zu einem Paket zusammen. Die Daten der virtuellen Festplatte einer VM landen meist als Datei(en) im Dateisystem des realen PCs. Um die VM auf einem anderen PC auszuführen, besteht die wesentliche

Passende Lösung finden

Für den **Desktop-Einsatz von VMware oder VirtualBox** sprechen bei Linux und Windows die vielseitigen Funktionen – sie empfehlen sich aber nur, wenn die betriebssystemeigene Virtualisierung abgeschaltet bleiben kann.

Wer **exotische Betriebssysteme** ausführen will, etwa OS/2, greift am besten zu VirtualBox. Dort sind die Emulationsfunktionen für alte PC-Hardware am weitesten entwickelt und die Wahrscheinlichkeit ist größer, auch alte Schätze ans Laufen zu bringen.

macOS bringt seit Version 12 eine betriebssystemeigene Virtualisierung mit, die nicht abschaltbar ist und für die

eine Oberfläche fehlt. Es gibt aber Software, die hilft, VMs einzurichten, etwa UTM und VirtualBuddy.

Hyper-V ist das Mittel der Wahl für **Windows** auf dem Desktop. Die Verwaltung über den Hyper-V-Manager ist gewöhnungsbedürftig, aber nach der Einarbeitung ist es besonders pflegeleicht.

Für den **Linux-Desktop** bietet sich GNOME Boxes als einfache Oberfläche für KVM an. Wer es technischer mag, nimmt den Virtual Machine Manager (virt-manager) oder gleich die Kommandozeile. Wenn ein Linux-Server gefragt ist, ist Proxmox VE eine Überlegung wert.

Arbeit darin, diese Datei(en) dorthin zu übertragen. Eine trickreiche Verwaltung der Dateiinhalte, die unter anderem Änderungen im laufenden Betrieb der VM separat aufzeichnet, ermöglicht das Anfertigen von Schnappschüssen.

Ins Netzwerk kommt eine virtuelle Maschine, indem der reale PC seine Netzwerkverbindung teilt. Dafür gibt es mehrere Modelle: Eine VM kann sich per Adressübersetzung (NAT) hinter dem PC verstecken. Die VM kann aber auch gleichberechtigt neben dem PC im Netz erscheinen. In der Regel gibt es obendrein die Möglichkeit, mehrere VMs in virtuellen Netzen zu organisieren. So lassen sich komplexe Testszenarien aufbauen, ohne auch nur ein einziges Netzwerkwerkkabel in die Hand zu nehmen.

Die Tastatur, die Maus und der Bildschirm einer VM sind über spezielle Software zugänglich, in deren Fenster die Ausgaben erscheinen. Hat es den Fokus, landen Tastendrucke als Eingaben in der VM. In Grenzen ist es so möglich, per Zwischenablage Informationen in eine VM zu schieben oder auch Informationen herauszuholen. Oft klappt diese Art der Zusammenarbeit aber nur rudimentär.

Um den Austausch zwischen ausführendem System (Wirt/Host) und der VM (Gast) zu fördern, bedient sich Virtualisierung gern der Dienste von Helfersoftware in der VM: Die verbessert die Steuerung von Tastatur und Bildschirm, indem sie dafür optimierte Fernsteuertechniken einspannt. Sie erleichtert den Austausch von Dateien, indem sie entweder einen Ordner zu Übergabe schafft oder sogar Drag & Drop von Dateien erlaubt.

Die Helfer übernehmen oft noch weitere Aufgaben: Sie erlauben der Virtualisierungssoftware, von außen Signale in eine VM zu schicken, etwa zum geordneten Herunterfahren des Gastes. Sie vermitteln Informationen aus der VM heraus an den Wirt, um zum Beispiel dort deren IP-Adresse anzuzeigen. In einigen Fällen übernehmen sie auch eine aktive Rolle und helfen, CPU-Takt und Speichernutzung von VMs zu optimieren.

Produktarten

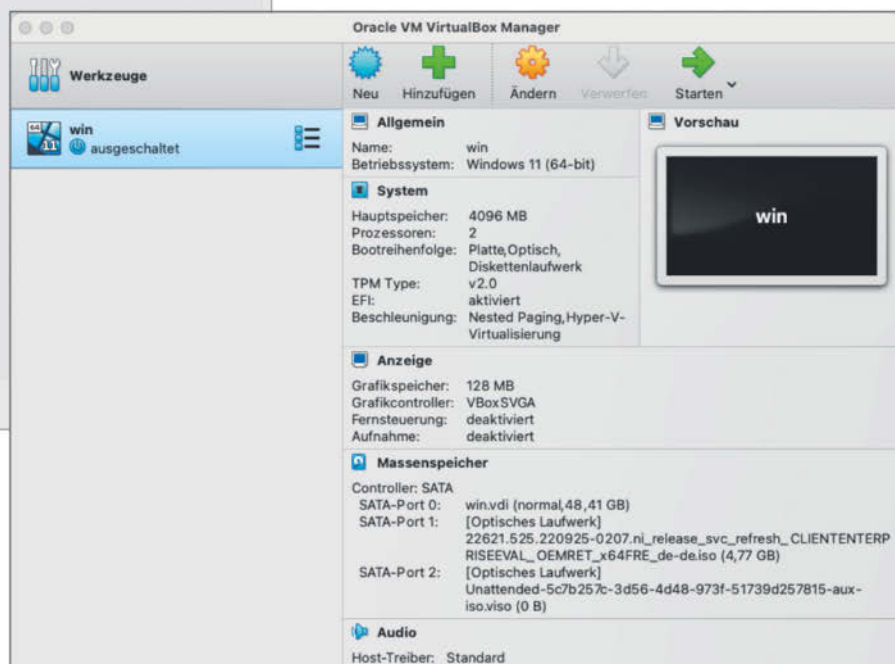
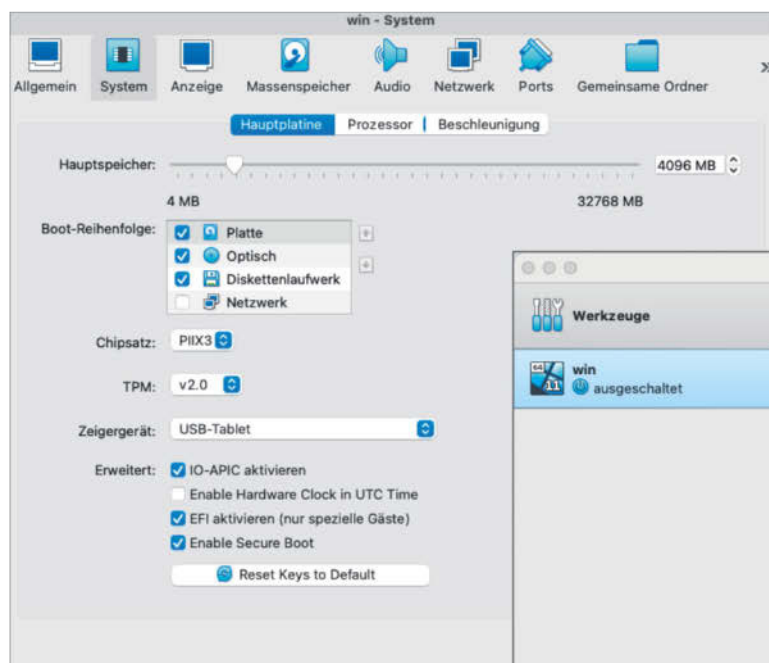
So, wie sich die Bedingungen für Virtualisierung geändert haben, hat sich auch die Software entwickelt. Der Klassiker, den heute viele PC-Anwender kennen dürften, sind Desktop-Produkte: Sie installieren

sich als Anwendung und erweitern allenfalls das vorhandene Betriebssystem um systemnahe, als Treiber eingerichtete Module. VMware Workstation und Player funktionieren noch heute so. Auch Virtual-Box arbeitet auf diese Weise.

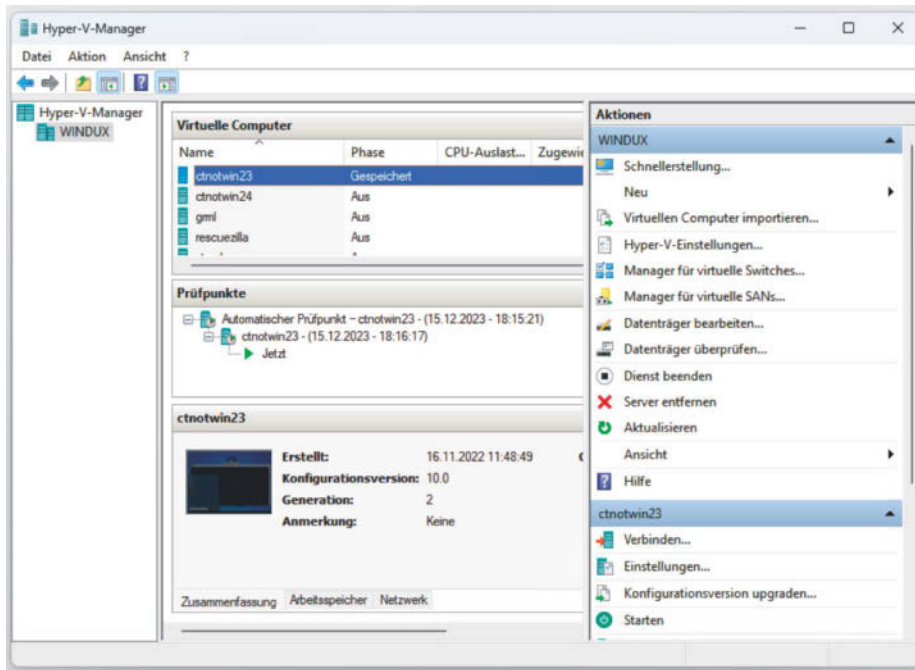
Parallel hat aber Software zum Ausführen von virtuellen Maschinen in viele gängige Betriebssysteme Einzug gehalten: Windows bringt Hyper-V mit. Seit macOS Version 12 (Monterey) steckt auch im Apple-Betriebssystem Virtualisierung. Die Linux-Entwickler haben eine eigene Virtualisierungstechnik namens KVM entwickelt und im Kernel eingebaut. Auch die BSD-Welt kennt eigene Hypervisor. Oftmals sind diese die beste und kostengünstigste Methode. Als Bestandteil des Betriebssystems erschließt sich Virtualisierung auch neue Aufgaben, etwa für höhere Sicherheit: In Windows sperrt Microsoft auf Wunsch kritische Anmeldedaten in einer separaten VM weg.

Mit der Integration eines Hypervisors in Betriebssysteme haben sich auch zwei Standards für paravirtualisierte Treiber und daran anschließende Dienste verbreitet: In der Linux-Welt und neuerdings auch bei macOS ist das VirtIO. In der Windows-Welt sind es die von Microsoft sogar in den Linux-Kernel eingebrachten Integrationsdienste für Hyper-V (eine ähnliche Entwicklung gibt es auch für BSDs).

Die zweite Art von Virtualisierungsprodukten sind die für Server. Sie sind darauf ausgerichtet, viele VMs zuverlässig auszuführen. Sie teilen die bis hierher auf-



Auf dem Desktop ausgeführte Virtualisierungssoftware wie VirtualBox bietet zahlreiche Feineinstellungen. Manches funktioniert nicht, weil sich in Betriebssysteme integrierte Virtualisierung dazwischen drängelt.



Der Umgang mit Hyper-V ist etwas gewöhnungsbedürftig, was auch am spröden Charme der in die Jahre gekommenen Windows-Management-Console liegt.

geschlüsselten Eigenschaften, ergänzen aber ausgefeilte Funktionen, etwa um VMs im laufenden Betrieb von Server zu Server zu migrieren. Ein Spezialfall sind x86-NAS-Geräte oder einige Server-Betriebssysteme wie Unraid oder OVM. Die können je nach Ausstattung auch VMs beherbergen, halten aber featuremäßig nicht mit ausschließlich auf Virtualisierung ausgerichteten Ansätzen mit.

Typisch für Server-basierte Virtualisierung ist, dass die virtuellen Festplatten der VMs nicht mehr in Dateien landen. Sie nutzen stattdessen blockbasierten Speicher, etwa solchen, den ein Logical Volume Manager verwaltet. Für Snapshots können sie dann auf dessen Funktionen zurückgreifen. Manches Produkt verwendet Dateisysteme mit entsprechender Technik wie ZFS oder BTRFS. Lediglich Hyper-V nutzt vornehmlich Dateien.

Von dem Ansatz, mehrere Server ein gemeinsames Speichersystem nutzen zu lassen, auf dem die VMs dann liegen und so leicht von Server zu Server migrierbar sind, kommen die Serverprodukte zunehmend ab. Der Trend geht zu Hyperkonvergenz; dabei sorgt die Software dafür, dass alle Server ihren Speicherplatz redundant teilen und eine gemeinsame Sicht aufs Netzwerk haben.

Die Auswahl an Software für den Serverbetrieb wird leider zunehmend dünn: Microsoft hat die bisher kostenlos nutz-

bare Fassung Windows Hyper-V-Server mit der 2019er-Ausgabe aufgegeben (bis 2029 gibt es aber Support); für die regulären Server fallen Lizenzgebühren in saftiger Höhe an. VMware-Investor Broadcom hat den kostenlos nutzbaren ESXi-Server eingestampft und verkauft nur noch hochpreisige Abos.

Aus dem Angebot ragt Proxmox VE heraus: Es baut auf Linux und KVM auf, bietet eine übersichtliche Weboberfläche und gilt gerade als die heiße Alternative für frustrierte VMware-Nutzer. Andererseits ist es aber so einfach zu nutzen, dass es für manchen Anwender eine Alternative zu den für den Desktop gedachten Lösungen ist – für Betreiber eines Homelabs ist es das ohnehin. Auf Seite 60 stellen wir es vor und ab Seite 64 lesen Sie, wie Sie mit Proxmox loslegen.

Verstrickungen

In der Praxis ist Virtualisierung kein Selbstläufer, wenn die Ansprüche wachsen: Durchgriff auf die Hardware, der Betrieb trotz aktiver betriebssystemeigener Virtualisierung und die Verfügbarkeit einzelner Funktionen hängen nicht nur davon ab, welches Produkt läuft, sondern auch davon, auf welchem Betriebssystem es aktiv ist und was innerhalb der VMs geschehen soll.

Beispiele gefällig? Wenn in Windows die zweite Auflage des Subsystem für

Linux (WSL2) aktiviert ist, greift das auf die betriebssystemeigene Virtualisierung zurück. VirtualBox und VMware laufen dann nur noch mit geringerem Funktionsumfang und reduzierter Leistung. Unter macOS ist es noch extremer: Die Virtualisierung ist immer an, VirtualBox läuft seit macOS 12 stets mit angezogener Handbremse.

Das im Linux-Virtualisierungsumfeld gebräuchliche Spice soll nicht nur die Konsole einer VM komfortabel zugänglich machen, sondern auch USB-Geräte am Wirt. Das klappt auch prima, solange auf beiden Seiten Linux im Spiel ist. Sobald Windows oder macOS als Client dienen, verweigert der virt-viewer (alias remote-viewer) den Zugriff auf die Geräte.

Ein tückisches Feature stellt der Durchgriff auf reale Hardware aus VMs dar: Kann klappen, muss es aber nicht. So prüften Nvidia-Treiber zeitweise, ob sie in einer VM liefen und verweigerten dann die Arbeit. Oft stecken aber hinter Fehlfunktionen beim direkten Hardwarezugriff keine bösen Absichten.

Vieler Einschränkungen und Auflagen kann man sich bequem entledigen, indem man die Virtualisierung auf ein eigenes Gerät verlagert, das sich ausschließlich dieser Aufgabe widmet. Das muss kein fetter PC sein, sondern schon ein Mini-PC oder umgewidmeter Thin Client kann genügen. Was Sie im Fall von Proxmox VE dann erwarten dürfen, klärt der folgende Artikel. (ps@ct.de) **ct**

Erwähnte Produkte: ct.de/yam9



Angesichts der Vielfalt von PC-Betriebssystemen kann man nicht darauf bauen, dass jedes Feature in jeder Umgebung funktioniert. Beispielsweise verbindet Spice lokal angeschlossene USB-Geräte nur dann mit einer entfernt ausgeführten VM, wenn auf beiden Seiten Linux läuft.



Bild: Collage ct

Aufzuchthelfer

Ein genauerer Blick auf Proxmox VE

Proxmox VE ist nicht nur eine auf Virtualisierung spezialisierte Linux-Distribution für Server, sondern auch interessant für Menschen, die virtuelle Maschinen auf dem Desktop verwenden wollen, aber keine Lust auf einen fetten, lärmenden Rechner unter dem Schreibtisch haben – oder als Ersatz für beliebige viele Raspis.

Von Peter Siering

Was Linux-Distributionen gern zugeschrieben wird, nämlich kryptisch zu sein, gilt für Proxmox VE nicht: Nach der Installation eröffnet dem Nutzer eine komfortable Web-Oberfläche die gesamte Welt der Virtualisierung: virtuelle Maschinen einrichten, starten, stoppen, klonen, Snapshots anfertigen, Netzwerkdetails konfigurieren, Platten vergrößern, Backups ziehen, Proxmox-Updates installieren und vieles mehr.

Ebenfalls im Browser erhält man Zugriff auf die Konsolen der virtuellen Maschinen, etwa um eine darin ablaufende Betriebssysteminstallation zu bedienen. Dieser Tastatur-, Maus- und Bildschirmersatz genügt zum Bedienen. An den Komfort der Desktop-Virtualisierung mit VMware, VirtualBox und Co. reicht es aber nicht ganz heran, weil es standardmäßig auf dem simplen VNC-Protokoll aufbaut.

Wie es geht

Beim Einrichten einer VM oder auch später lässt sich allerdings ein alternatives Verbindungsprotokoll der Konsole aktivieren: Spice. Mit einem Spice-Client und etwas vermittelnder Software kann man sich so komfortabel direkt auf die virtuelle Konsole einer VM aufschalten, ohne dafür auch nur die Proxmox-Web-Oberfläche aufrufen zu müssen; die dabei hilfreiche Software PVE VDI Client, die nicht von Proxmox selbst stammt, finden Sie via ct.de/ycnh.

Bei der Art und Weise, wie Proxmox die virtuellen Festplatten der VMs verwaltet, weicht es von Desktop-Lösungen ab: Statt Dateien benutzt es standardmäßig logische Volumes, also Teilbereiche vorhandener Partitionen, die ein spezialisiertes Volume-Management verwaltet. Man muss sich darüber keine Gedanken machen, sollte das aber wissen.

Welche Art von Volume-Management Proxmox nutzt, lässt sich schon bei der Installation bestimmen: Die Proxmox-Entwickler haben als Alternative zum bewährten Logical Volume Management (LVM) auch ZFS eingebaut. Natürlich ist es möglich, auch später noch Speicher zu ergänzen. Man ist dabei nicht auf das bei der Installation ausgewählte Verfahren festgelegt; es ist im Vorfeld aber sinnvoll, sich mit der Auswahl zu befassen.

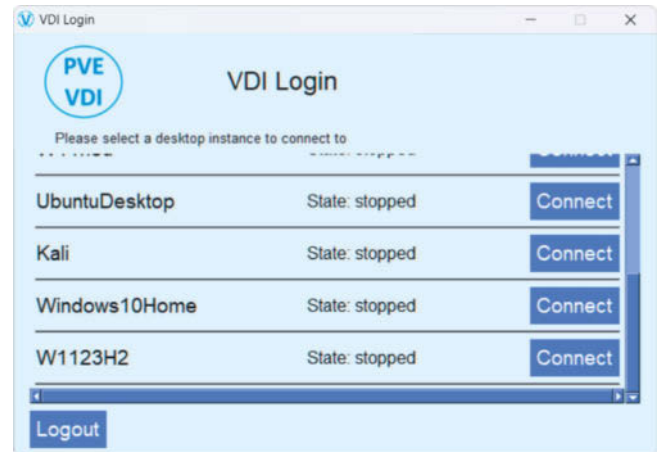
Für ZFS spricht: Es kennt inkrementelle Snapshots. Die verwendet Proxmox geschickt, um Änderungen an virtuellen Platten von einem Proxmox-Knoten auf einen anderen zu replizieren. Da nur geänderte Daten durch die Leitung wandern, ist das schnell und für alle interessant, die mehrere Proxmox-Rechner als Cluster-Knoten betreiben und VMs hin und herschieben wollen.

Proxmox baut auf der Virtualisierung im Linux-Kernel (KVM) auf. In diesem Kontext liest man auch immer wieder den Namen QEMU. Dieses ursprünglich als Systememulator gestartete Projekt hilft Virtualisierungssoftware häufig dabei, die nötige PC-Umgebung auf die Beine zu stellen, so auch Proxmox.

Was drin ist

Die Minimalausstattung für einen Proxmox-Knoten ist ein x86-PC mit nutzbaren Virtualisierungsfunktionen im Prozessor

Etwas zusätzliche Software hilft, vom Desktop-PC oder Notebook die VMs fernzubedienen, ohne die Proxmox-Web-Oberfläche überhaupt aufrufen zu müssen.



und eine SSD als Datenspeicher für Betriebssystem und die VMs; Magnetplatten taugen für Virtualisierung nicht, sie sind zu langsam. Ein Mini-PC oder mancher Thin Client genügt also vollkommen, je nach Arbeitslast und Inhalt der VMs natürlich.

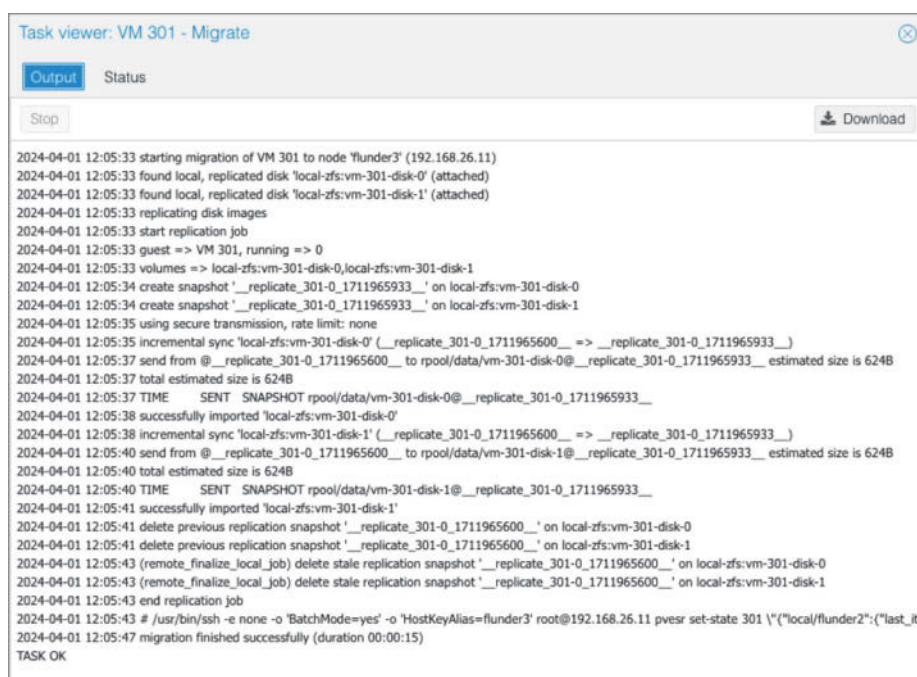
Unter der Haube von Proxmox steckt ein aufgebohrtes Debian. Der Hersteller erweitert es mit eigenem Kernel, unter anderem für den ZFS-Support, Erweiterungen zur Verwaltung der virtuellen Maschinen (qemu-Server genannt) und viele Zutaten, die erst im professionellen Einsatz interessant werden, wenn mehrere Proxmox-Knoten im Verbund auf ein gemeinsames Speichersystem zugreifen sollen oder gemeinsam ein solches bilden.

Grundsätzlich ist eine Installation auch aus einem bereits laufenden, aktuellen Debian-System heraus möglich. Das kann hilfreich sein, wenn Proxmox auf einen Mietserver gelangen soll, dort keine passenden Vorinstallationen angeboten werden und auch ein Anstöpseln eines USB-Sticks oder ISOs aus der Ferne nicht vorgesehen ist.

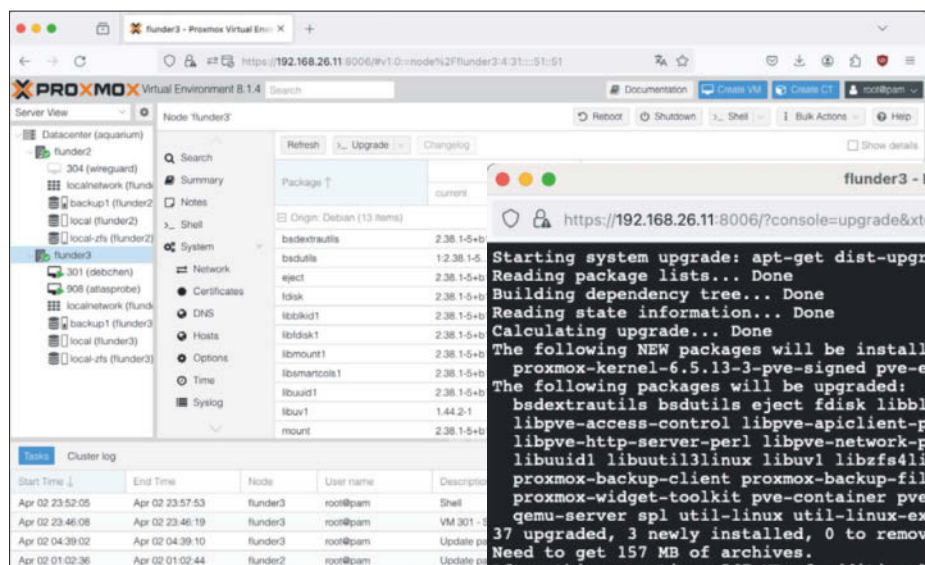
Dass Debian die Basis bildet, ist auch aus einem weiteren Grund wichtig zu erwähnen: Für Updates nutzt Proxmox die Debian-Paketverwaltung (APT). Deren Ausgaben und eventuelle Rückfragen bei der Paketinstallation versteckt es nicht hinter der Weboberfläche, sondern öffnet ein weiteres Browserfenster mit einer Textkonsole dafür. Hier muss der Nutzer eventuell Fragen beantworten und sieht den Fortschritt.

Die Update-Installation und Upgrades auf die nächste Proxmox-Version sind die einzigen Stellen, an dem auch Proxmox-Nutzer ohne Linux-Ambitionen eine Kommandozeile verwenden müssen. APT stellt dort Rückfragen, die mit der vorgegebenen Standardantwort meist passend beantwortet werden können. Die Proxmox-Entwickler helfen bei Upgrades zur nächsten Version vorbildlich: Es gibt ein Programm, das überprüft, ob alle Voraussetzungen überhaupt erfüllt sind, und mit Hinweisen dient, wie die gegebenenfalls herzustellen sind.

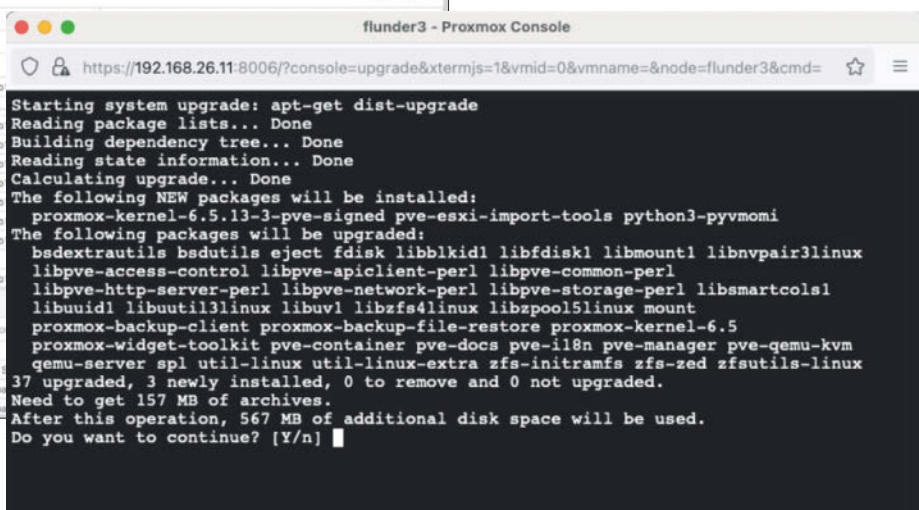
Mit jeder Proxmox-Version wachsen die Fähigkeiten des Produkts. Sämtliche Funktionen werden nur die wenigsten Nutzer brauchen. Ein paar Highlights: Die integrierte Nutzerverwaltung kennt Zweifaktorauthentifizierung und Rollen. Die ohnehin komfortable Netzwerkverwaltung, die mit VLANs und Bridges umgehen kann, ist zum vollwertigen SDN-Stack angewachsen (Software-defined Networking).



Mit ZFS als Aufbewahrungsort und eingerichteter regelmäßiger Replikation schiebt Proxmox VMs binnen Sekunden von einem Cluster-Knoten auf einen anderen.



Für Updates und Upgrades spannt Proxmox die Debian-Paketverwaltung APT ein. Das geht nicht ganz ohne den Charme der Kommandozeile.



Schon immer kennt Proxmox nicht nur gekapselte virtuelle Maschinen, sondern erlaubt es auch, Container-Technik zu nutzen. Die Entwickler setzen dabei allerdings nicht auf Docker, sondern Linux Container (LXC), die technisch anders funktionieren (siehe nachfolgender Artikel).

Was entsteht

Proxmox macht bereits auf einem Minimal-PC eine gute Figur. Es kann dort VMs beherbergen, die zum Beispiel die im Haus verstreuten, fürs Smarthome zuständigen Raspis ersetzen. Über die Funktionen zum Hineinreichen von USB-Geräten des Wirts-PCs in die VMs kommen Docker-Container in einer VM bequem auch an Zigbee-Sticks heran. In der Proxmox-Oberfläche trägt man dazu nur die USB-IDs ein und die VM sieht das Gerät.

So bündelt Proxmox Dienste, die aus taktischen Gründen als separate Hosts eingerichtet sind, platz- und energiesparend in VMs: VPN-Server, Backup-Server, virtualisierte Ripe Atlas Probe, Freifunk-Offloader sowie Software-Firewall haben keine großen Ansprüche an Hauptspeicher. Denen genügen oft ein paar GByte oder sogar nur wenige 100 MByte RAM und etwas Plattenplatz.

Ebenso gut befeuert Proxmox fett ausgestattete Systeme, um darauf mehrere Windows-VMs zu betreiben, beispielsweise eine Testumgebung inklusive Active Directory. Egal, ob Linux oder Windows: Groupware, Mailsdienste, Software für die private Cloud, all das lässt sich in VMs auftrennen, sodass unterschiedliche Systemanforderungen, etwa für die Basisdistribution, nicht den Einsatz weiterer Rechner erfordern. Weitere VMs genügen.

Mit wachsenden Ansprüchen bietet Proxmox die Möglichkeit, mehrere Server zu Clustern zusammenzufassen. Es überträgt VMs, die man unter den Schutz des High-Availability-Modus stellt, automatisiert auf andere Knoten im Cluster. Live-Migration von VMs von einem auf einen anderen Knoten brauchen dann nicht zwangsläufig ein gemeinsam genutztes Speichersystem. Aber auch das kann Proxmox: Mit dem verteilten Speichersystem Ceph lässt es mehrere Knoten auf einen gemeinsamen Speicher blicken.

Was davon man wirklich braucht, hängt von den Ansprüchen ab. Wer nur sicherstellen will, keine VMs und darin enthaltene Daten zu verlieren, sollte sich in jedem Fall den Proxmox Backup Server ansehen. Der ist auch dann sehr nützlich, wenn man VMs nur gelegentlich bequem per Mausklick von einem auf einen anderen Server schieben möchte.

Wer dahintersteckt

Fast unglaublich ist, wie entspannt die Proxmox-Schöpfer ihr unter AGPLv3 gestelltes Produkt anbieten. Jeder darf die Virtualisierungsumgebung gratis nutzen. Wer die stärker qualitätsgesicherten Enterprise-Pakete verwenden möchte, die der Hersteller für produktiven Einsatz empfiehlt, kann dafür ein Abo für 110 Euro pro Jahr abschließen. Supportleistungen sind ab 340 Euro pro Jahr inbegriffen.

Laut Auskunft der Firmeninhaber haben nicht einmal ein Zehntel der Be-

treiber der derzeit über eine Million aktiven Installationen ein solches Abo abgeschlossen. Trotzdem, so sagt Martin Maurer, einer der Gründer, im Gespräch mit c't: „Unser Businessmodell funktioniert auch, wenn weit über 90 Prozent der Nutzer nichts bezahlen.“

Proxmox gehört den Firmengründern und das soll auch so bleiben. Maurer dazu: „Wer verkauft, hat den Glauben an die Zukunft seines Unternehmens verloren, und/oder es ist ein Eingeständnis des Scheiterns, oder er braucht dringend Geld oder eine Mischung aus allem. Alle diese Punkte treffen auf uns nicht zu.“

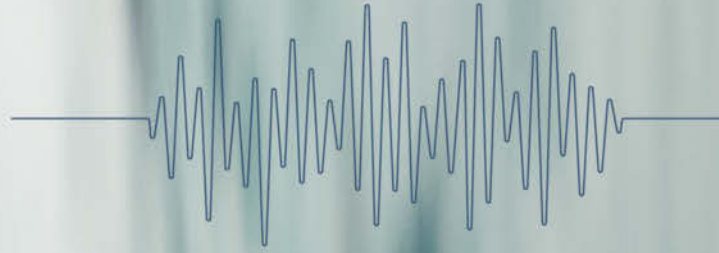
Das lässt hoffen, dass das seit Gründung 2005 wachsende Unternehmen mit derzeit Umsätzen im zweistelligen Millionenbereich eben anders tickt als das durch Investorenhande kreisende VMware. Deren Treiben lobt Maurer als „sehr gute ‚Vertriebstätigkeit‘ von Broadcom“ und spielt damit auf die Umstellung der VMware-Produkte durch Broadcom auf ein für Kunden teures Abomodell an.

Der folgende Artikel taucht tiefer in die Welt von Proxmox ein und zeigt Wege auf, wie VMware-ESXi-Verstoßene ihre VMs recht bequem in die entspannte Proxmox-Welt retten können. Sollten Sie nur nach einer Alternative zur bisher verwendeten Desktop-Virtualisierung suchen: Sie werden längst nicht alles brauchen, was der Artikel zeigt. Aber das schadet auch nicht.

(ps@ct.de)

Erwähnte Downloads: [ct.de/ynch](https://www.proxmox.com/en/downloads)

Multitalent Audio-Werbung



Schalten Sie Audio-Spots und erreichen Sie Ihre Zielgruppe auf beliebten Sendern im Webradio und in Podcasts!

Ihre Vorteile:

- regionale oder nationale Ausspielung
- exakte Zielgruppenansprache
- effizienter Budgeteinsatz
- hohes Interesse & Werbeakzeptanz
- starke Aufmerksamkeit
- Messbarkeit Ihrer Werbemittelkontakte

Setzen Sie auf hörbaren Erfolg mit unseren heise Audio Ads!

Neue
Kunden und
Mitarbeitende
gewinnen!

Mehr über heise Audio Ads erfahren Sie auf heise-regioconcept.de oder rufen Sie uns an 0511 80 90 89 43.





Bild: Collage c't

Multitalent

Loslegen mit Proxmox Virtual Environment

Proxmox Virtual Environment ist eine funktionsreiche und vielseitige Virtualisierungsumgebung, die man komfortabel über eine Weboberfläche administriert. Wir zeigen, wie Sie Proxmox aufsetzen, virtuelle Maschinen erstellen oder bestehende importieren und was man beachten muss, um es produktiv zu nutzen.

Von Niklas Dierking

Wie lege ich mit Proxmox los? „Passt das zu unseren Anforderungen?“, „Wie ziehe ich die VMs um?“ dürften Fragen sein, die sich in jüngster Vergangenheit vom Familienadmin über den Homelabber bis zum technischen Leiter eines IT-Teams viele Nutzer gestellt haben dürften. Die Open-Source-Virtualisierungsplattform Proxmox ist unter Interessierten schon lange kein Geheimtipp mehr, steht aber spätestens im Rampenlicht, seitdem Broadcom, der neue Eigner von VMware, die kostenlose Variante des vSphere Hypervisor (VMware ESXi) abgekündigt hat. Auch abseits von Heim- und Testumgebungen fühlen sich Kunden

von der Umstrukturierung der Lizenz- und Produktlandschaft gegängelt und sehen sich nach Alternativen um.

Der Wechsel zu Proxmox liegt nahe, denn die Virtualisierungsplattform ist etabliert und lässt, wenn es um Brot-und-Butter-Virtualisierung geht, wenig Wünsche offen. Einsatzgebiete und die dafür nötigen Hardwarekonfigurationen reichen von einer Handvoll VMs auf einem Mini-PC, um mal eine Linux-Distribution Probe zu fahren, bis zu VM-Flotten auf einem hyperkonvergenten Cluster im Rechenzentrum, der Hunderte Produkktivsysteme ausführt.

c't-Redakteure nutzen die Virtualisierungsumgebung beispielsweise, um Malware in einer isolierten Windows-VM auf die Finger zu schauen oder betreiben einen Kubernetes-Cluster auf einem Verbund schlanker Linux-VMs. Proxmox schultert auch einen Teil der Heise-Infrastruktur, wie man unter ct.de/ya81 nachlesen kann. Wer beruflich mit Virtualisierungsumgebungen arbeitet, könnte bei Proxmox eine automatische Verteilung von VMs im Cluster, abhängig von der Last der einzelnen Knoten,

und Support für Enterprise-Backups wie Veeam vermissen. Die meisten Nutzer dürften sich aber für Proxmox interessieren, um aus einem Computer mehrere zu machen und das in der Regel auf einer dafür abgestellten Maschine, die über das Netz administriert werden kann.

In diesem Artikel konzentrieren wir uns deswegen zunächst auf die Installation auf einem einzelnen Rechner. Wir führen durch die Weboberfläche und zeigen, wie Sie VMs erstellen, importieren und sichern. Das reicht, um sich mit der Virtualisierungsplattform vertraut zu machen. Wer Größeres vorhat, verdrahtet mehrere Proxmox-Knoten zu einem Cluster.

Proxmox installieren

Zunächst laden Sie ein Installationsmedium aus dem Downloadbereich der Proxmox-Website herunter und schreiben das mit einer Anwendung wie Etcher auf einen USB-Stick (alle Tools und Downloads finden Sie über ct.de/ya81). Alternativ installieren Sie auf einem Debian-System Proxmox und dessen Kernel aus dem Proxmox-Repository. Das bietet sich beispielsweise an, wenn Sie Proxmox bei einem Cloudprovider aufsetzen wollen, der es nicht im Angebot hat.

Grundsätzlich hat Proxmox keine hohen Systemvoraussetzungen. Für Testzwecke reicht eine 64-Bit-CPU mit Intel-VT- oder AMD-V-Features, die auch im UEFI-BIOS aktiviert sein müssen, und 1 GByte Arbeitsspeicher. Wer mehrere VMs betreiben will, braucht mehr Arbeitsspeicher. Um Geräte wie eine Grafikkarte in eine VM zu reichen (PCIe-Passthrough), müssen CPU und Motherboard IOMMU-Remapping (I/O Memory Management Unit) beherrschen. VMs und Proxmox selbst profitieren von schnellem SSD-Massenspeicher. Für die Sicherung virtueller Maschinen empfiehlt sich ein zweiter Rechner, auf dem Sie Proxmox Backup Server installieren, aber dazu später mehr.

Schließen Sie Monitor, Maus und Tastatur an den Proxmox-Host an und verbinden Sie ihn mit einem Netzwerk, auf das Sie von einer weiteren Maschine Zugriff haben. Nach dem Start vom USB-Stick begrüßt Sie der grafische Installationsassistent. Akzeptieren Sie die Lizenzvereinbarungen und wählen dann ein Laufwerk für die Installation. Wenn Sie nur ein Laufwerk haben, das sowohl Proxmox selbst als auch VM- und Container-Images beherbergt, müssen Sie jetzt eine wegweisende Entscheidung treffen.

Der Installer beansprucht standardmäßig das gesamte Laufwerk und richtet es für den Linux-eigenen Logical Volume Manager (LVM) als physisches Volume ein. Das gliedert sich in die logischen Volumes root, swap und data. Die Root-Partition wird mit ext4 formatiert. Das data-Volume nutzt LVM-thin, um platzsparende Snapshots zu ermöglichen.

Diesen Weg empfehlen wir den meisten Nutzern, die Proxmox im Heimbetrieb einsetzen. Wer aus mehreren Proxmox-Knoten einen Cluster machen will, greift stattdessen zu ZFS. Das ist Voraussetzung für die sogenannte Storage Replication zwischen Proxmox-Knoten. Dabei werden Schnappschüsse der Gastsysteme auf weiteren Knoten vorgehalten. Das verkürzt die Migration einer VM von mehreren Minuten auf wenige Sekunden. Natürlich können Sie später auch weiteren Speicher hinzufügen und für ZFS einrichten. Beachten Sie, dass ZFS gern mehr RAM beansprucht. Die Proxmox-Entwickler raten mindestens zu 8 GByte.

Im nächsten Schritt müssen Sie Land, Zeitzone und Tastaturlayout angeben, wenn der Installer das nicht selbst ermitteln konnte. Anschließend vergeben Sie eine Mail-Adresse und ein Passwort für den Nutzer root, mit dem Sie sich standardmäßig in der Weboberfläche und via SSH anmelden. Der Installer sollte Proxmox eine IP-Adresse mittels DHCP besorgen. Falls nicht, dann passen Sie jetzt die Netzwerkkonfiguration an. Sie sollten dem Proxmox-Host in Ihrem Router eine feste IP-Adresse zuweisen oder reservieren. In dieser Anleitung gehen wir

ct kompakt

- Proxmox Virtual Environment läuft nicht auf dem Desktop, sondern ist eine quelloffene Virtualisierungssoftware für Server.
- Der Funktionsumfang reicht vom Virtualisierungsspielplatz im Home-lab bis zum Cluster-Betrieb im Rechenzentrum.
- Proxmox ist eine Virtualisierungsalternative für gestrandete Nutzer von VMware ESXi. Wir zeigen, wie Sie Ihre VMs umziehen.

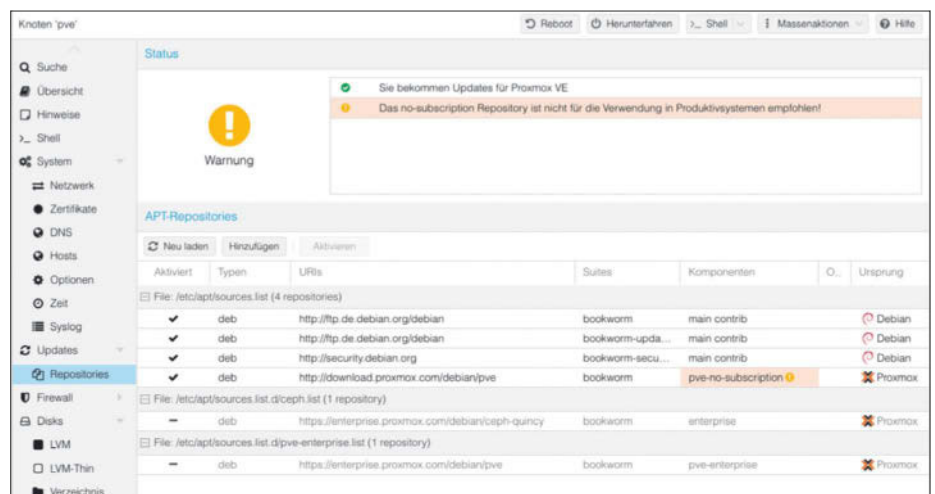
davon aus, dass der Hostname Ihres Proxmox-Knoten „pve“ lautet.

Kontrollieren Sie im letzten Schritt die Zusammenfassung und starten dann die Installation. Nach einem Neustart zeigt Proxmox die URL seiner Weboberfläche an, beispielsweise <https://192.168.1.90:8006>.

Rufen Sie die Adresse im Browser von einem anderen Gerät im Netz auf, bestätigen Sie die Ausnahme für das selbst signierte Zertifikat und melden Sie sich dann als root an. Wenn die Seite nicht erreichbar ist, gibt es wahrscheinlich ein Problem mit Ihrer Netzwerkkonfiguration. Bei der Fehlersuche hilft ein Blick in `/etc/network/interfaces` und die Proxmox-Dokumentation (siehe ct.de/ya81).

Weboberfläche

Die Weboberfläche von Proxmox setzt sich aus vier Bereichen zusammen. Über den



Proxmox ist erst mal kostenlos für Jedermann. Wer nicht für Enterprise-Repositories bezahlen will, die intensiver getestete Pakete enthalten, muss mit den Community-Repositories vorliebnehmen.



In der Mitte der Weboberfläche befindet sich ein dynamischer Bereich, der Informationen über die ausgewählten Objekte anzeigt. Das Log Panel am unteren Rand des Fensters listet laufende und abgeschlossene Tasks. Ein Task kann beispielsweise ein Backup oder der Neustart einer VM sein.

Wenn Sie Proxmox ohne Support-Abonnement nutzen, müssen Sie die Enterprise- gegen die Community-Repositories tauschen, damit Sie Updates bekommen. Navigieren Sie auf der Ebene des Knotens in das Menü „Repositories“ unterhalb von „Updates“

Aktualisierungen für Proxmox VE spielen Sie über das Menü „Updates“ ein. Alle Funktionen, die in diesem Artikel anhand der Proxmox-Weboberfläche erklärt werden, haben eine Entsprechung auf der Kommandozeile (ct.de/va81).

Der Ressource Tree listet unterhalb des Knoten pve mindestens zwei lokale Storage-Pools, die unterschiedliche Aufgaben erfüllen. Wenn Sie sich bei der Installation für LVM entschieden haben, heißen sie „local“ und „local-lvm“. Proxmox verfügt über eine ganze Reihe von Storage-Plug-ins und unterscheidet Storage nach Datei- oder Blockebene (siehe ct.de/va81).

Über das Menü „Storage“ können Sie jederzeit weitere Datenspeicher, beispiels-

Befördern Sie eine ISO-Datei in den Storage local, um sie als Installationsmedium für eine virtuelle Maschine zu nutzen. Die können Sie von Ihrem lokalen Rechner hochladen, von einer URL herunterladen oder mit `scp` in das Verzeichnis `/var/lib/vz/template/iso` schieben. Für erste Gehversuche bietet sich beispielsweise das schlanke Ubuntu Server 22.04 als Gast-system an (siehe ct.de/ya81).

Sie sollten nach Möglichkeit immer den Haken für den QEMU-Gastagenten setzen und den Helfer später auf dem Gastsystem installieren. Wie üppig Sie die VM mit CPU, Speicherplatz und Arbeitsspeicher versorgen, hängt von Ihrer Hardware und geplanten Workloads ab. Bei der Option CPU-Typ müssen Sie gewünschte Performance und Kompatibilität abwägen. Die Einstellung „host“, auch CPU-Pass-through genannt, ist performanter als eine generische CPU wie „x86-64-v2-AES“, kann aber zu Problemen führen, wenn Sie VMs in einem Cluster zwischen Knoten mit unterschiedlichen Prozessoren migrieren wollen. Im Reiter „Speicher“ legen Sie über die erweiterten Optionen zusätzlich zum maximalen Speicher auch eine minimale Speichermenge fest. Zum Schluss fasst der Assistent die Konfiguration der VM nochmal zusammen.

c't 2024. Heft 9

Nach der Installation von Gastsystemen sollten Sie den QEMU-Gastagenten nachrüsten. In Ubuntu installieren Sie dazu das Paket `qemu-guest-agent`:

```
sudo apt update
sudo apt install qemu-guest-agent
```

Je nach Distribution müssen Sie danach noch dafür sorgen, dass der Agent beim Systemstart anläuft:

```
sudo systemctl enable qemu-guest-agent
sudo systemctl start qemu-guest-agent
```

Bei einem Debian-Gastsystem können Sie sich diesen Schritt sparen. Danach zeigt Proxmox die IP-Adresse(n) der VM im Menü „Übersicht“. Außerdem fährt es VMs mit dem Gastagenten geordnet herunter und bereitet sie auf Backups und Snapshots vor.

Um nicht immer wieder den Installationsprozess, beispielsweise von Ubuntu Server, zu durchlaufen, können Sie VMs klonen oder Sie in Templates umwandeln, also Vorlagen. Proxmox unterscheidet zwischen vollständigen und verknüpften Klonen. Letztere sparen Speicherplatz, sind aber nicht Knoten-übergreifend möglich, weil sie Zugriff auf den lokalen Storage mit der virtuellen Festplatte brauchen. Die Proxmox-Dokumentation rät dazu, VM-Templates frei von Nutzerdaten und Geheimnissen zu halten (siehe ct.de/

[ya81](https://ct.de/ya81)). Wie Sie Gastsysteme mit `cloud-init` vorkonfigurieren und verhindern, dass virtuelle Maschinen aus Templates die gleiche IP-Adresse wie die Vorlage bekommen, haben wir in [1] aufgeschrieben.

Windows-VMs

Im Assistenten zur Erstellung virtueller Maschinen müssen Sie im Reiter „OS“ für Windows-VMs den Typ „Microsoft Windows“ auswählen. Im Unterschied zu den meisten Linux-Distributionen, die Treiber für paravirtualisierte Geräte (VirtIO) mitbringen und automatisch laden, müssen Sie die bei Windows-VMs nachinstallieren.

Das Fedora-Projekt stellt ein ISO-Image mit quelloffenen, signierten VirtIO-Treibern und dem QEMU-Gastagenten zur Verfügung (siehe ct.de/ya81). Laden Sie die ISO-Datei in den local-Storage und reichen Sie sie an die virtuelle Maschine durch. Das können Sie beim Erstellen der VM direkt im Reiter „OS“ erledigen, indem Sie den Haken bei „Zusätzliches Laufwerk für VirtIO-Treiber hinzufügen“ setzen oder Sie holen das später im Menü „Hardware“ nach. Die Treiber- und Werkzeugsammlung installieren Sie dann in Windows.

Für Windows-11-VMs müssen Sie außerdem OVMF (UEFI) statt SeaBIOS auswählen sowie ein TPM (Trusted Platform Module) und ein EFI-Laufwerk hinzufügen. Achten Sie beim ersten Start darauf, dass die Installations-ISO die

höchste Priorität in der Bootreihenfolge bekommt. Das erledigen Sie im Menü „Optionen“ unter „Bootreihenfolge“.

VMs von ESXi importieren

Um virtuelle Maschinen von einem VMware-ESXi-Host zu Proxmox zu migrieren, gibt es mehrere Methoden. Ihnen ist gemein, dass Sie vor dem Transfer Umzugskartons packen müssen, indem Sie eingehängte ISO-Dateien auswerfen, VMware-Gästetools deinstallieren und die VMs herunterfahren.

VMware stellt für Umzüge das Kommandozeilenwerkzeug `ovftool` zum Download bereit (siehe ct.de/ya81), das man auch direkt auf dem Proxmox-Knoten ausführen kann. Dadurch spart man sich beispielsweise den Umweg über eine Netzwerkfreigabe. Für den Download mussten wir einen kostenlosen VMware-Account einrichten. Befördern Sie den Installer via `scp` auf den Proxmox-Knoten. Dort machen Sie ihn ausführbar und installieren `ovftool`:

```
chmod +x ./VMware-ovftool-\  
4.6.2-22220919-lin.x86_64.bundle  
  
./VMware-ovftool-\  
4.6.2-22220919-lin.x86_64.bundle
```

Mit dem folgenden Befehl fischen Sie virtuelle Maschinen als OVF-Paket aus dem ESXi-Datastore:

Virtualisierung light: Container

Neben VMs verfügt Proxmox mit Linux Containern (LXC) noch über eine zweite Methode der Virtualisierung. Anders als bei „ausgewachsenen“ virtuellen Maschinen, wo jedes Betriebssystem einen eigenen Kernel ausführt und je nach Konfiguration auch Geräte emuliert werden müssen, teilen sich Container den Kernel mit dem Host. Das reduziert den Overhead und ermöglicht schnellere Startzeiten. Verwechseln Sie Linux Container aber nicht mit Docker- oder anderen OCI-Containern (Open Container Initiative).

In seiner Anfangszeit hat Docker auf LXC aufgebaut und beide nutzen auch heute die gleichen Kernel-Funktionen zur Containerisierung, erfüllen aber verschiedene Anwendungszwecke. Docker-Images sind bewusst schlank gehalten

und darauf gestützt, nur eine Anwendung im Container auszuführen, während Linux Container als Ersatz für ein komplettes System dienen. Deswegen unterscheidet man sie auch als Anwendungs- und Systemcontainer. In Linux Containern finden Sie alle Dienste und Anwendungen, die man von einem Linux-System erwartet.

Praktisch: Proxmox bringt eine große Vorauswahl an Container-Templates mit, die Sie über das Menü „Container-Templates“ in den local-Storage laden können. Darunter sind viele populäre Linux-Distributionen und Images von turnkeylinux.org, in denen, ähnlich wie bei Docker-Containern, bereits eine Anwendung wie WordPress oder eine Datenbank wie PostgreSQL steckt.

Container erstellen Sie über die Schaltfläche „Erstelle CT“ im Header. Durch den gemeinsam genutzten Kernel sind Container weniger isoliert vom Wirt als eine virtuelle Maschine. Damit ein kompromittierter Prozess keinen Schaden auf dem Host anrichten kann, sollten Sie nach Möglichkeit auf unprivilegierte Container setzen. Die biegen die User-ID 0 des root-Nutzers im Container auf die User-ID eines unprivilegierten Nutzers außerhalb des Containers um. Container profitieren ebenso wie virtuelle Maschinen von Proxmox-Features wie Replizierung, Migration oder High Availability und greifen auf die gleichen Ressourcen zu, beispielsweise die Netzwerkkonfiguration. Docker sollten Sie nie direkt in Proxmox installieren, sondern eine virtuelle Maschine als Dockerhost einrichten.

```
ovftool vi://root@192.168.1.10/vm \
/var/lib/vz/template/iso
```

Ersetzen Sie im obigen Befehl die IP-Adresse durch die Ihrer ESXi-Instanz und den Platzhalter „vm“ durch den Namen Ihrer virtuellen Maschine. Das Import-Verzeichnis können Sie frei wählen, unser Beispielauftrag nimmt das Standardverzeichnis für ISO-Dateien.

Navigieren Sie in das Importverzeichnis und importieren Sie die VM in Proxmox:

```
qm importovf 301 vm.ovf local-lvm
```

Ersetzen Sie die VM-ID 301 durch eine eigene VM ID und passen den Namen der OVF-Datei an. Außerdem müssen Sie einen Storage für die virtuelle Festplatte der VM festlegen, beispielsweise local-lvm. Die importierte Maschine taucht anschließend im Ressource Tree auf. Die OVF-Datei können Sie jetzt löschen.

Bevor Sie die VM das erste Mal starten, müssen Sie sie in Proxmox vorbereiten. Welche Arbeitsschritte anstehen, hängt davon ab, wie Sie die VM in ESXi konfiguriert hatten. Nach einem Transfer von Ubuntu Server 22.04 mussten wir die Firmware von SeaBIOS auf OVMF umstellen, eine EFI-Disk ergänzen, eine Netzwerkkarte (VirtIO) hinzufügen und den SCSI Controller auf VirtIO SCSI single umstellen.

Eine IP-Adresse via DHCP bekam die VM erst, nachdem wir in Ubuntu in der Datei /etc/netplan/00-installer-config.

yaml das neue Netzwerkinterface namens enp0s19 eingetragen hatten. Sie sollten außerdem stets den QEMU-Gastagenten nachinstallieren und in der VM-Konfiguration das entsprechende Häkchen setzen.

Kurz vor Redaktionsschluss haben die Proxmox-Entwickler noch einen experimentellen Assistenten für die VM-Migration von ESXi in die Weboberfläche von Proxmox integriert. Für den müssen Sie im Menü „Storage“ Ihren ESXi-Datastore einbinden, den Proxmox über das ESXi-API anzapft.

Danach markieren Sie die zu importierenden VMs in einer Liste. Sie sollten deren Konfiguration gründlich prüfen und eventuelle Fehler ausbügeln, bevor Sie den Transfer starten. Bei unserem Testlauf hat der Assistent einer Windows-11-VM beispielsweise vier CPU-Sockel angedichtet, obwohl es vier CPU-Kerne hätten sein müssen. Einige Nutzer berichten im Proxmox-Forum auch von Problemen mit Rate Limiting bei Massenimporten. In den erweiterten Hosteinstellungen von ESXi können Sie das Limit der gleichzeitigen Verbindungen erhöhen, indem Sie den Wert bei Config.HostAgent.vmacore.soap.maxSessionCount erhöhen oder eine 0 setzen, um Rate Limiting zu deaktivieren.

Für die Nachsorge gelten die gleichen Tipps wie beim herkömmlichen Import von VMs mit ovftool. Mehr Informationen dazu finden Sie in der Proxmox-Dokumentation und im Community-Forum (siehe ct.de/ya81).

Proxmox-Cluster

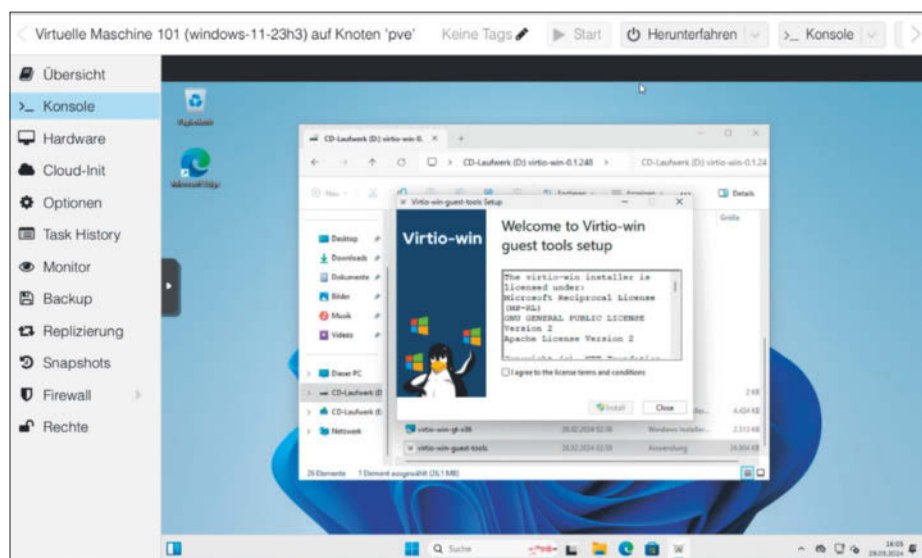
In einer Produktivumgebung ist es sinnvoll, mehrere Proxmox-Knoten zu einem Cluster zusammenzufassen, um VMs herumzureichen. Die Konfigurationen der VMs speichert Proxmox dann im Cluster-Dateisystem pmxcfs und synchronisiert die Daten über das Cluster-Protokoll corosync. Damit das klappt, müssen die Knoten sich gegenseitig über die UDP-Ports 5405 bis 5412 für corosync und Port 22 für SSH erreichen können.

Für High Availability (HA), also den automatischen Transfer einer VM, wenn ein Knoten ausfällt, braucht es mindestens drei Knoten im Cluster, damit die sich auf ein gemeinsames Vorgehen einigen können. Es besteht aber die Möglichkeit, ein externes QDevice (Quorum Device) einzubinden, beispielsweise einen stimmberechtigten Raspberry Pi (siehe ct.de/ya81). Weil corosync allergisch auf hohe Latenzen reagiert, sollten Sie den Cluster-Traffic im Idealfall über eine zweite Netzwerkkarte in einem separaten Netzwerk leiten.

In unserem Testlauf haben wir drei Proxmox-Knoten mit ZFS-Storage zu einem Cluster verdrahtet. Sie erstellen den Cluster über die Weboberfläche im gleichnamigen Menü auf der Ebene des Rechenzentrums. Prüfen Sie vorher, ob die IP-Adressen und Hostnamen aller Knoten passen, denn nach dem Beitritt zum Cluster können die nicht mehr geändert werden. Proxmox zeigt nach dem Erstellen des Clusters Informationen an, die Sie an die anderen Beitrittskandidaten im Menü „Cluster beitreten“ verfüttern.

Um einen verteilten Storage mit Ceph einzurichten, wird Netzwerkhardware aufwärts von Gigabit-Ethernet empfohlen. Um auch ohne Ceph Redundanz im Cluster zu gewährleisten, können Sie Schnappschüsse von VMs auf anderen Knoten vorhalten (ZFS-Replikation). Das verkürzt die Dauer der Migration zwischen zwei Knoten von mehreren Minuten auf wenige Sekunden. Navigieren Sie dazu in das Menü „Replizierung“. Hier legen Sie einen oder mehrere Zielknoten fest und konfigurieren ein Intervall, in dem Proxmox das Volume der VM synchronisiert. Nach der ersten vollständigen Synchronisation werden beim nächsten Mal nur die Änderungen am Datenstand, auch Delta genannt, übertragen.

Nur weil Ihr Cluster alle Voraussetzungen für den High-Availability-Modus erfüllt (siehe ct.de/ya81), heißt das noch



Für Windows 11 in Proxmox braucht es ein paar zusätzliche Handgriffe. Treiber für VirtIO bringt man über eine ISO-Datei in die virtuelle Maschine.

nicht, dass der Cluster Ressourcen automatisch migriert, sobald ein Knoten offline ist. Dafür müssen Sie die VMs oder Container unter den Schutz des High-Availability-Managers (ha-manager) stellen. Das geht über die Weboberfläche im Menü „HA“ auf der Ebene des Rechenzentrums, wo Sie auch einsehen können, ob ein funktionierendes Quorum besteht, der Cluster also beschlussfähig ist. Aktivieren Sie den HA-Modus über die Schaltfläche „Hinzufügen“ für alle Ressourcen, die Sie gegen Ausfall schützen wollen.

Je nach Workload und Zweck der VM kann es sinnvoll sein, den angestrebten Zustand, beispielsweise „started“ oder „stopped“, sowie die maximalen Versuche der Wiederbelebungen und Migrationen anzupassen.

Wer Proxmox professionell einsetzt, sollte bedenken, dass echte High-Availability auch entsprechende Hardware und Infrastruktur wie redundante Stromversorgung oder Failover-Netze braucht. Die meisten Heimanwender dürften mit einem Proxmox-Host und einer Backuplösung auskommen, aus der man VMs wiederherstellen kann.

Backups

Proxmox VE hat mit `vzdump` ein simples und solides Backup-Werkzeug an Bord, das Sie über die Weboberfläche oder die Kommandozeile konfigurieren können. Es funktioniert gut, erfasst aber alle Daten einer VM, erstellt also jedes Mal ein vollständiges Backup. Das mag für Setups mit wenigen oder kleineren virtuellen Maschinen gut funktionieren. Wenn man aber viele VMs betreibt oder gleichzeitig mehrere Backups vorhalten will, dürfte Speicherplatz irgendwann rar werden.

Ein beliebtes Ziel für `vzdump`-Backups sind SMB-/CIFS- oder NFS-Freigaben, zum Beispiel auf einem NAS. Binden Sie dafür die Netzwerkfreigabe im „Storage“-Menü als Ziel ein, indem Sie auf „Hinzufügen“ klicken. Bei einem NFS-Share müssen Sie einen Namen (ID) vergeben, die IP-Adresse des Servers und die exportierte Freigabe eintragen, beispielsweise `/mnt/backups`. Über das Dropdown-Menü „Inhalt“ markieren Sie die Freigabe als Ziel für „VZDump Backup Dateien“. Backup-Jobs, also wann von welcher Maschine Backups gezogen werden und wie lange sie vorgehalten werden, konfigurieren Sie im Menü „Backups“ in der Weboberfläche von Proxmox VE.

Nach der Installation bekommen Sie vom Proxmox Backup Storage nicht mehr viel mit. Er verhält sich wie ein weiterer Storage, den Sie als Ziel für Backups konfigurieren können, bietet aber viel mehr Funktionen.

Proxmox unterscheidet für virtuelle Maschinen die Backup-Modi `snapshot`, `suspend` und `stop`: Letzterer vermeidet inkonsistente Daten, verursacht aber Downtime, weil die Maschine heruntergefahren und nach dem Backup neu gestartet werden muss. Der Modus `snapshot` funktioniert im laufenden Betrieb. Wenn der QEMU-Gastagent läuft, reduziert er das Risiko inkonsistenter Daten. Vom `suspend`-Modus raten die Entwickler ab. Er ist aus Kompatibilitätsgründen vorhanden.

Ein eigenständiger Proxmox Backup Server, den Sie auf einem weiteren Rechner installieren, bietet mehr Funktionen als lokale oder NAS-Backups mit `vzdump`, beispielsweise platzsparende Deduplizierung, inkrementelle Backups oder die Wiederherstellung einzelner Dateien. Die ISO-Datei laden Sie kostenlos von der Proxmox-Website herunter.

Die Installation funktioniert so, wie Sie es bereits von Proxmox VE kennen, und auch der Backup Server bringt eine eigene Weboberfläche zur Administration mit. Als ersten Schritt können Sie wie bei Proxmox VE auf die Community-Repositories umsatteln.

Wenn sie nicht auf Profi-Features wie Tape-Archivierung angewiesen sind, müssen Sie in der Weboberfläche des Backup Servers nicht viel Zeit verbringen. Am einfachsten legen Sie mit Backups los, indem Sie den Datastore namens `backup-data` als Storage wie im Screenshot auf dieser Seite einbinden. Neben IP-Adresse, Benutzername und Passwort brauchen Sie dafür auch den Fingerprint des selbstsignierten TLS-Zertifikats. Den Fingerprint zeigt der Backup Server Ihnen im Dashboard an. Optional können Sie die Backups Clientseitig verschlüsseln lassen.

Backup Server verhalten sich passiv zu Ihrem Proxmox-Cluster: Sicherungen konfigurieren Sie pro VM im Menü „Backups“ in der Weboberfläche von Proxmox VE, das die Snapshots an den Backup Ser-

ver schickt (Push-Betrieb). Die Funktion zur Wiederherstellung einzelner Dateien einer VM haben die Entwickler im Menü „Backup“ auf VM-Ebene versteckt. Die Schaltfläche für die Dateiwiederherstellung erscheint dort erst, nachdem Sie den Backup Server als Storage ausgewählt haben. Über den Dateibrowser können Sie auch Dateien auf Ihre lokale Maschine herunterladen.

Wer die Möglichkeiten des Proxmox Backup Server ausschöpfen will, sollte sich mit der umfangreichen Dokumentation vertraut machen.

Das günstigste Support-Abo für den Proxmox Backup Server ist mit 540 Euro deutlich teurer als Proxmox VE. Professionellen Support gibt es für ihn ab 1040 Euro im Jahr.

Fazit

Sie haben die wichtigsten Funktionen von Proxmox VE kennengelernt und können jetzt mit dem Virtualisieren loslegen. Wir ermutigen dazu, nach Herzenslust zu experimentieren, denn – das ist ja das Schöne an virtuellen Maschinen – Fehler lassen sich meistens schnell ungeschehen machen. Wenn Sie Fragen haben, die in Richtung „und wie mache ich XY bei meinem exotischen Anwendungsfall“ tendieren, dann sei Ihnen ein Besuch im Proxmox-Forum empfohlen. Dort tummeln sich eine sehr hilfsbereite Community und viele Proxmox-Entwickler, die Fragen beantworten. Wahrscheinlich hatte jemand anders das Problem schon vor Ihnen und Sie können von der Lösung profitieren.

(ndi@ct.de) 

Literatur

- [1] Niklas Dierking, Alles nach Plan, Infrastructure as Code mit Terraform und Proxmox, c't 16/2023, S. 136

Proxmox-Dokumentation, ISO mit VirtIO-Treibern und mehr: [ct.de/ya81](https://www.proxmox.com/en/documentation)



24 mal P

Workstation-CPU Intel Xeon w7-2495X für LGA4677

Für einen Workstation-Prozessor ist Intels 24-kerniger Xeon w7-2495X noch halbwegs günstig, hat schnelle AVX512-Einheiten und integrierte KI-Beschleuniger AMX. Im Test muss sich der Xeon gegen AMDs Threadripper 7970X und Intels eigenen Core i9-14900K mit ebenfalls 24 Kernen beweisen.

Von Carsten Spille

Wer braucht schon einen Workstation-Prozessor, der nicht mehr Kerne als das Desktop-Spitzenmodell – nämlich 24 – hat? Diese Sinnfrage beantworten die erweiterten Ausstattungsmöglichkeiten der Plattform und tatsächlich auch die Rechenleistung, denn Kern ist nicht gleich Kern.

Das gilt für Intel-Prozessoren mehr noch als für solche von AMD. Nur eins vorweg: Für Spieler hat Intel mit dem Achtkern-Desktop-Prozessor Core i9-14900K eine gute Balance gefunden. Der Xeon w7-2495X kann sich aber für Hardcore-Anwendungen lohnen, selbst wenn diese nicht von den vielen zusätzlichen PCI-Express-Leitungen für Beschleuniger, M.2-Speicher, schnellen Netzwerk- oder 3D-Grafikkarten profitieren.

Blender-Renderer, Audio- oder KI-Workstations sind sinnvolle Einsatzbereiche für den Xeon w7-2495X, auch wenn die Plattform teuer ist. Die günstigsten Boards und das günstigste 64-GB-Speicherkit kosten schon etwa 700 Euro mehr als eine vergleichbare Kombi für die Desktop-Plattform LGA1700. Dazu kommt der CPU-Preis von rund 2400 Euro. Der liegt zwar circa 1800 Euro über dem Core i9-14900K, aber immerhin 4300 Euro unter dem Xeon w9-3495X mit stattlichen 56 Kernen [1].

Wer aber mit Rechenleistung Geld verdient, für den kann sich der Griff zu einem Workstation-Prozessor lohnen. Ein paar Budget-Stufen höher liegen außer dem Xeon w9 auch AMDs Threadripper Pro 7000X und 7000WX (siehe [1] und S. 72).

Xeon-Technik

Der Xeon w7-2495X stammt aus der Sapphire-Rapids-Generation und passt auf Workstation-Boards mit W790-Chipsatz und der Fassung LGA4677. Er teilt sich damit sein Innenleben mit den just abgelösten Xeon-Scalable-Prozessoren der vierten Generation. Im Gegensatz zu den Server-CPUs und auch anders als beim größeren Xeon-w9-Geschwister mit bis zu 56 Kernen in vier Chip-Kacheln setzt Intel im Xeon w7-2000 keinen Chipverbund, sondern ein einzelnes Die ein, die sogenannte MCC-Ausbaustufe (Mid Core Count). Dadurch sind keine Chip-zu-Chip-Verbindungen nötig, die im großen Xeon bremsend wirken können. Ein weiterer Unterschied zu den Xeon w9 ist die Speicherschnittstelle. Anstelle von satten acht hat der w7 nur vier Speichercontroller für DDR5-4800-RDIMMs.

24 Kerne: P vs. P+E

Als monolithischer 24-Kerner bietet sich der Vergleich zu Intels anderem monolithischem 24-Kerner an, der zudem in einem ähnlichen TDP-Rahmen läuft: Der Core i9-14900K für die Desktop-Fassung LGA1700. Dessen acht P-Kerne können mit bis zu 6 GHz deutlich schneller takten als die maximal 4,8 GHz schnellen Kerne des 2495X.

Dafür gehören alle 24 Kerne des Xeon w7-2495X zur P-Gattung, die nicht nur mehr Leistung pro Takt und einen größeren Cache haben als die E-Varianten. Im Gegensatz zu den P-Kernen in Intels aktuellen Desktop-Prozessoren führen sie auch AVX512-Instruktionen aus und haben die Matrix-Multiplikatoren „AMX“, die speziell KI-Anwendungen beschleunigen. Pro Kern und Takt verdoppelt sich nominell also die Rechenleistung, was synthetische Tests wie MAXFLOPS im Test auch bestätigten: Statt 1232 GFLOPS in 64-Bit-Gleitkommagenauigkeit beim 14900K erreichte der 2495X 2266 GFLOPS.

Ab Werk muss der Xeon mit 225 Watt auskommen und darf im sehr kurzen Turbofenster bis 270 Watt aufdrehen, der Core i9-14900K muss sich nur nominell auf 125 Watt beschränken. Im Turbo darf

er aber 253 Watt schlucken und Intel erlaubt den Boardherstellern, dieses Fenster beliebig lang anzusetzen, sodass er de facto durchweg mit 253 Watt läuft [2]. Durch die im Vergleich zum Desktop-Prozessor rund dreimal so große Chipfläche ist auch der Wärmeübergang zum Kühler für den Xeon w7 deutlich einfacher; selbst unter Dauervolllast hält ihn ein Noctua NGH-U14S DX-4677, also ein Single-Tower-Luftkühler, locker unter 70 Grad Celcius. Für den i9-14900K brauchten wir eine Flüssigkühlung, um unter der Drosselgrenze von 95 Grad Celsius zu bleiben.

Der Xeon tat sich in Spielen schwer, mit dem Desktop-Prozessor mitzuhalten. Das galt auch für CPU-lastige Titel wie die erste Szene des Benchmarks von Avatar: Frontier of Pandora oder den Microsoft Flugsimulator 2020 mit voller Detailstufe im Tiefflug über Manhattan. Im Gegenteil war die Bildrate dort meist geringer.

Auch viele Anwendungen profitierten nicht oder nur wenig von den vielen P-Kernen, wie etwa Handbrake zur Videokodierung. Andere wiederum konnten die Rechenleistung durchaus in Mehrperformance umsetzen. Dazu zählen hochoptimierte Spezialsoftware die wie y-cruncher mathematische Konstanten oder PI berechnen, aber auch KI-Anwendungen, wie sie der AI-Computer-Vision-Teil des UL-Procyon-Benchmarks anhand von sieben verschiedenen KI-Modellen simuliert.

Bei letzterem kam auch der AMX-Vorteil zum Tragen, denn die Matrix-Multiplizierer wurden unter Intels OpenVINO automatisch mit angesprochen. Schaffte der Core i9-14900K hier in FP32 und FP16-Genauigkeit nur 186 respektive 184 Punkte, schaufelte der Xeon w7-2495X mit 662 respektive 668 Punkten das 3,6-Fache durch – in grob vergleichbarem



Nicht nur das Package, wie im Bild zu sehen, sondern auch der Chip des Xeon w7-2495X (links) ist im Vergleich zum Core i9-14900K größer.

TDP-Rahmen wohlgemerkt. Mit Festzahl-Genauigkeit (Integer) lag zwischen beiden immer noch Faktor 2: 523 zu 1018 Punkten.

Übertaktbar!

Intel wirbt trotz gedachten Workstation-Einsatzes beim Xeon w7-2495X auch mit RAM-Übertaktung und lieferte zum Test ein Kit mit DDR5-6000 Extreme Memory Profile (XMP) mit. Die normalen Messungen haben wir selbstverständlich ohne OC-Einstellungen mit DDR5-4800 durchgeführt.

Mit dem auf DDR5-6400 beschleunigten, also 33 Prozent schnelleren Speicher stieg die Bildrate in der ersten, CPU-lastigen Szene des Avatar-Benchmarks nur um rund 4 Prozent von 106 auf 111 Bilder pro Sekunde. Im Rendering-Programm Blender legte der Xeon mit der Szene „Lone Monk“ ebenfalls nur wenig zu: von 16:13 Minuten ging es herunter auf 16:08 Minuten, die die CPU dauerhaft an ihrer 225-Watt-Lastgrenze verbracht. Lösten wir auch diese Bremse und aktivierten die Auto-OC-Funktion des Asus-Mainboards Pro WX W790E-SAGE-SE, stieg die Leis-

tungsaufnahme auf 259 Watt und der anliegende Takt von 3,1 auf 3,3 Gigahertz, die Renderzeit sank um knapp sieben Prozent auf 15:11 Minuten.

Das Maximum, was wir mit vertretbaren Temperaturen knapp unter der Drosselgrenze erreichten, waren 4,3 GHz auf allen Kernen und 2,6 GHz für das interne Mesh, also die Verbindung der Prozessorkerne und den L3-Cache, sowie XMP mit DDR5-6400. Die Bildrate in Pandora stieg damit zwar nur auf 118 fps, die Rechenzeit der Lone-Monk-Szene sank aber auf knapp 12 Minuten und war damit 25 Prozent kürzer als im Werkszustand. Die CPU schluckte dann 424 Watt.

Fazit

Keine CPU für jedermann. Das macht allein der Preis des Prozessors und der gesamten Plattform deutlich. Wer jedoch mehr als 256 GByte Arbeitsspeicher nutzen oder mehrere Beschleuniger mit voller Transferrate parallel an die CPU anbinden will, der kommt um einen Workstation-Prozessor nicht herum. Von AMDs preislich grob vergleichbaren Threadrippern setzt sich der Intel Xeon w7-2495X allerdings nur bei spezialisierten KI-Berechnungen unter AMX-Einsatz. Ansonsten arbeitet der Threadripper 7970X deutlich schneller. Hier gilt es, den geplanten Verwendungszweck vor einem Kauf möglichst genau einzugrenzen und danach seine Entscheidung zu treffen. (csp@ct.de)

Literatur

[1] Carsten Spille, Hochgezüchtet, Intel Xeon w9-3495X gegen AMD Threadripper 7970X und 7980X, c't 1/2024, S. 90
[2] Christian Hirsch, Ehrenrunde, Core i9-14900K, i7-14700K und Core i5-14600K im Test, c't 24/2023, S. 40

Leistungsvergleich Workstation- und Serverprozessoren

Prozessoren	Kerne pro CPU [phys./virt.]	7-Zip 23.01 Kompression [MByte/s]	MaxFlops Double-Precision [GFlops]	Kbench 0.9.6 Kernel kompilieren¹[s]	Handbrake 1.5.1 4K Production Max. [fps]	MLC 3.10 Bandwidth² [GByte/s]	Blender 3.6.1 classroom [s]	Blender 3.6.1 Lone Monk [s]	y-Cruncher 0.8.2.9522 Pi, 10 Mrd. Stellen [s]
	besser ▶	besser ▶	besser ▶	◀ besser	besser ▶	besser ▶	◀ besser	◀ besser	◀ besser
Intel Xeon w7-2495X	24/48	191	2266	576	64	100	124	1032	205
Intel Core i9-14900K	24/32	175	1232	569	67	72	132	1162	331
Intel Xeon w9-3495X	56/112	336	4385	335	75	200	69	582	101
AMD Threadripper 7980X	64/128	416	4491	219	124	126	38	369	109
AMD Threadripper 7970X	32/64	332	2458	323	112	128	64	609	113
Zum Vergleich									
2 × Xeon Platinum 8280	28/56	245	8552	417	57	193	84	708	190
2 × AMD Epyc 7601	32/64	191	1350	490	44	250	89	945	288
Alle Messungen unter Ubuntu Server 22.04.3 LTS ¹ Kernel 6.4.11 mit gcc 12.3.0, inklusive Kernelmodulen ² max. Transferrate im Test „Stream Triad-like“									

Wenn viel nicht genug ist

High-End-Workstation mit 96-Kern-Prozessor und zwei Profigrafikkarten

Dell rüstet die Precision 7875 mit der stärksten Workstation-CPU Ryzen Threadripper Pro 7995WX und zwei Nvidia RTX 6000 Ada aus. Wir hatten Mühe Software zu finden, welche die enorme Performance ausreizt.

Von Christian Hirsch

Auf Arbeit gilt das Motto: Zeit ist Geld. Ingenieure, 3D-Grafiker und Programmierer sollen möglichst wenig untätig herumsitzen, während der PC Strömungen simuliert, einen Animationsfilm rendert oder ein Softwareprojekt kompiliert. Wenn die Rechenarbeit gut parallelisierbar ist, kommen daher leistungsstarke Workstations mit vielen CPU-Kernen und mehreren schnellen Grafikkarten zum Einsatz.

Dieser kleinen, aber finanzstarken Zielgruppe bietet Dell die Precision 7875 Tower an. Wir erhielten eine Konfiguration nahe dem Maximum, die auch für uns Hardware-Tester der c't nicht alltäglich ist: Als Herz der Workstation schlägt der derzeit stärkste Desktop-Prozessor AMD Ryzen Threadripper Pro 7995WX mit 96 Zen-4-Kernen. Ihm stehen 128 GByte DDR5-RAM zur Seite, aufgeteilt auf acht Kanäle mit je einem 16-GByte-DIMM. Für KI, Rendering und CAD packt Dell gleich zwei der leistungsstärksten Profigrafikkarten RTX 6000 Ada von Nvidia mit jeweils 18.176 Shader-Kernen und 48 GByte GDDR6-RAM dazu. Das Betriebssystem Windows 11 Pro liegt auf einem RAID-0-Verbund aus zwei PCIe-4.0-SSDs.

Die ganze High-End-Technik hat ihren Preis: Allein der Prozessor schlägt

mit rund 12.000 Euro zu Buche. Die derzeit für KI heiß begehrten Grafikkarten kosten jeweils 10K. Unter dem Strich stehen dann knapp 40.000 Euro für die von uns getestete Ausführung der Dell Precision 7875 auf der Rechnung.

CPU-Kerne im Überfluss

Äußerlich wirkt das Gehäuse der Workstation recht unscheinbar, hier traut sich Lenovo bei den ThinkStations P/PX etwas mehr Design und Farbe [1]. Im Inneren offenbart sich der Unterschied zu normalen PCs. In der Workstation steckt wesentlich mehr Ingenieurskunst. So lassen sich nahezu alle Komponenten ohne Schraubendreher durch Schnellverschlüsse leicht austauschen. Die Lüfter für den CPU-Kühler sind in einem großen, herausnehmbaren Ansaugkanal eingebettet. Das hat den Vorteil, dass Netzteil, Prozessor und die Grafikkarten jeweils in eigenen thermischen Zonen sitzen. Seine zahlreichen Abwärmequellen überwacht das System pedantisch: Inklusive der Messdioden in den 96 CPU-Kernen haben wir 146 Temperatursensoren mit der Windows-Software HWInfo auslesen können [2].

Nach dem Einschalten führt die Precision 7875 zusätzlich zur Initialisierung der umfangreichen Hardware einen Preboot-Check durch und benötigt deshalb satte 53 Sekunden bis zum Windows-Desktop. Gängige Desktop-PCs schaffen das in einem Drittel der Zeit. Parallel zum BIOS-Setup gibt es auch ein grafisches Diagnoseprogramm in der Firmware, das PCIe-Ports, Kabel, Lüfter, Laufwerke, Prozessor und Arbeitsspeicher auf Fehler prüft.

Das Topmodell der Prozessorserie Ryzen Threadripper Pro 7000WX „Storm Peak“ mit 96 Kernen hatten wir bisher noch nicht im c't-Labor. Die 96 Zen-4-Kerne verteilen sich auf zwölf Core Complex Dies



(CCD), wo sie jeweils zu acht mit 32 MByte Level-3-Cache sitzen. Insgesamt ergibt das 384 MByte L3-Cache. In der Spitze takten die Kerne mit 5,1 GHz, doch wenn alle unter Volldampf stehen, begrenzt das Power-Limit von 350 Watt die Taktfrequenz auf den Nominaltakt von 2,5 GHz.

Im mittig unter dem Heatspreader untergebrachten IO-Die sitzt der Speichercontroller mit acht DDR5-Kanälen für bis zu 2 TByte Speicher (Registered ECC). Theoretisch erlaubt das bei Einsatz von DDR5-5200-RAM einen Durchsatz von 333 GByte/s. In der Praxis haben wir mit den von Dell eingebauten, etwas langsameren DDR5-4800-Modulen 272 GByte/s erreicht. Zum Vergleich: Aktuelle Desktop-PCs mit zwei Kanälen schaffen 50 bis 80 GByte/s.

Weiterhin enthält das IO-Die des Threadripper-Prozessors einen PCIe Root Hub mit 128 PCIe-5.0-Lanes. Daran hängen in der Precision 7875 unter anderem die sechs Steckplätze für Erweiterungskarten im x16- und x8-Format, wovon Dell aber nur drei im PCI-Express-5.0-Modus betreibt. In zwei davon stecken die beiden Grafikkarten vom Typ RTX 6000 Ada. Für SSDs gibt es intern zwei M.2-Slots sowie an der Front einen aktiv gekühlten Wechselschacht für ein Modul, das eine M.2-SSD aufnimmt. In der uns zur Verfügung gestellten Variante verteilen sich die beiden 1-TByte-SSDs von SK Hynix auf einen der internen sowie den extern zugänglichen Einschub.

Beide SSDs fasst Dell in einem RAID-0-Verbund mit 2 TByte Kapazität zusammen. Das bedeutet, die Daten werden gleichmäßig auf sie verteilt, was den

Durchsatz auf 12 GByte/s nahezu verdoppelt. Für eine Workstation, bei der es auf geringe Ausfallzeiten ankommt, verwundert uns das jedoch. Denn fällt eine SSD aus, sind alle Daten des Verbunds inklusive der Systempartition unwiederbringlich verloren. Da der Datenträger im Wechselrahmen leicht herausnehmbar ist, besteht ein gewisses Risiko, das RAID zu beschädigen.

Für klassische SATA-Laufwerke im 2,5- und 3,5-Zoll-Format bietet die Workstation mehrere freie Einschübe. Einer davon ist in der Front untergebracht und von außen zugänglich. Direkt darunter, wir konnten wir unseren Augen zunächst kaum trauen, bringt Dell einen DVD-Brenner unter. Deutlich moderner ist das Lesegerät für SD-Kärtchen in der Front, das von einer Lexar Professional 2000x Daten mit bis zu 278 MByte/s transferiert.

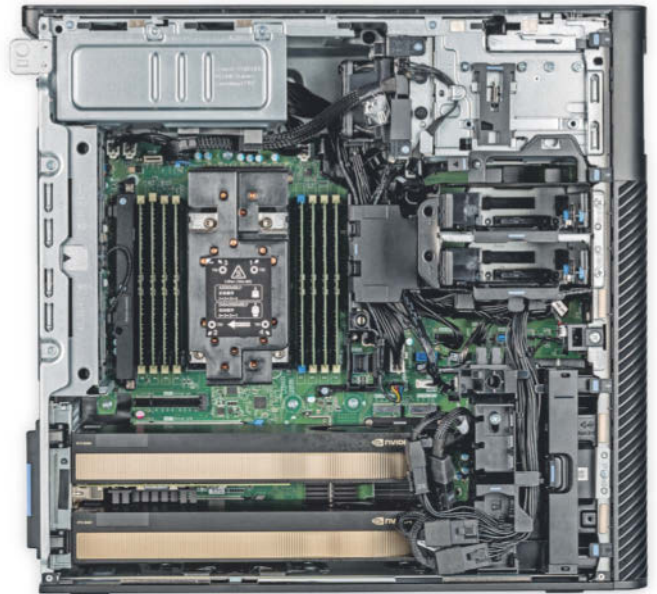
Satte Performance

Im Rendering-Benchmark Cinebench R23 knackt der Threadripper Pro 7995WX die 100.000-Punkte-Marke. In der aktuellen 2024er-Version kommt er auf 5882 Punkte. Die Dual-Socket-Workstation Levono Thinkstation PX mit zwei 60-Kern-Xeons [1] hat mit 4542 Punkten und 29 Prozent Rückstand keine Chance gegen den einzelnen 96-Kerner der Precision 7875. Im



Zwischen dem DVD-Brenner und der M.2-SSD im Wechselrahmen liegen 30 Jahre Technikfortschritt. Fürs Foto haben wir den Deckel des SSD-Einschubs entfernt.

Dell rüstet die Precision 7875 mit zwei RTX-6000-Ada-Grafikkarten (unten) mit je 48 GByte Speicher aus. Die CPU-Lüfter sind hier nicht im Bild, weil wir für das Foto den großen Luftkanal in der Mitte herausgenommen haben.



Vergleich zum 64-Kerner Threadripper 7980X rechnet der Threadripper Pro 7995WX jedoch nur um sieben Prozent schneller. Viel mehr als 70 Kerne kann der Cinebench wohl nicht sinnvoll nutzen.

Noch stärker zeigt sich das Problem beim Videotranskodierer Handbrake. Diese Software profitiert nur von rund 30 Threads, sodass der 96-Kerner der Dell-Workstation mit 115 fps gleichauf mit der 16-Kern-Desktop-CPU Ryzen 97950X liegt. Besser klappt es beim Komprimieren von Daten mit 7-Zip. Dort rennt der Threadripper Pro 7995WX allen anderen CPUs davon. Er erreicht in dieser Disziplin 441 MByte/s.

Auch im 3D-Renderprogramm Blender schneidet der Prozessor der Precision 7875 sehr gut ab: Die Szene „Lone Monk“ absolviert er mit 290 Sekunden um 37 Prozent schneller als der 64-Kerner Threadripper 7980X. Gegen das Doppelpaket aus zwei Xeon Platinum 8490H gewinnt er mit 13 Sekunden beziehungsweise vier Prozent Vorsprung. Gegen die zwei eingebauten Grafikkarten vom Typ RTX 6000 Ada [3] hat die Threadripper-CPU aber keine Chance. Im Verbund per CUDA benötigen diese für die gleiche Aufgabe gerade einmal 45 Sekunden und somit nur ein Sechstel der Zeit. Mit der OptiX-Technik, die einige aufwendige Raytracing-Berechnungen einspart und stattdessen einen Enttaucher einsetzt, schrumpft die Rechenzeit auf 25 Sekunden zusammen.

Für Anwendungen, die nur von einem oder wenigen Kernen profitieren, wie die meisten Office-Programme oder Browser bietet der Threadripper-Prozessor jedoch keine Vorteile. In der Singlethreading-

Wertung des Cinebench 2024 muss er sich den höher taktenden und viel günstigeren Desktop-CPUs der Serien Ryzen 7000 und Core i-14000 geschlagen geben.

KI-Beschleuniger im Doppelpack

An den beiden RTX 6000 Ada von Nvidia lassen sich insgesamt acht 4K-Displays betreiben. Die Stärken der RTX 6000 Ada liegen unter anderem bei Profianwendungen wie CAD- und Konstruktionssoftware. Obwohl die Benchmark-Suite SpecViewPerf nur eine der beiden GPUs nutzt, erreicht die Dell Precision 7875 in der Teilwertung medical-03 mehr als die dreifache Performance der derzeit schnellsten Gaming-Karte GeForce RTX 4090 in einem System mit dem 16-Kerner Ryzen 97950X3D.

Derzeit ist das Thema KI in aller Munde. Mit 48 GByte lokalem GDDR6-RAM taugt die RTX 6000 Ada ideal für generative KI-Anwendungen. Um die Leistung zu bestimmen, haben wir den neuen Benchmal UL Procyon AI Image Generation ausprobiert (siehe auch S. 45). Dieser verwendet als Basis die Software Stable Diffusion 1.5 [2], die aber ebenfalls nur eine einzelne GPU nutzt.

Im XL-Modus mit 1024×1024 Pixeln Bildgröße und 100 Inferencing-Schritten erreicht die Workstation 2871 Punkte beziehungsweise es dauert im Schnitt 13 Sekunden pro generiertem Bild. Selbst vergleichsweise leistungsstarke Gaming-Karten wie die GeForce RTX 4070 für 650 Euro müssen dabei passen, weil dafür 12 GByte freier Grafikspeicher notwendig ist.

Mit 512 Pixeln Bildauflösung schafft die RTX 6000 Ada Punkte, was 1,8 Sekunden pro Bild entspricht. Als Vergleich: Die GeForce RTX 4070 kommt auf 2027 Punkte (3,1 Sekunden pro Bild).

Für die meisten Anwendungen ist das System überdimensioniert. So verhaspelt sich der 3D-Benchmark 3DMark mit 96 CPU-Kernen und kommt in der TimeSpy-Wertung nur auf 9704 Punkte. Damit sortiert sich das Doppelpack aus zwei RTX 6000 Ada noch hinter einer Radeon RX 6650 XT für 250 Euro ein. Begrenzen wir die Zahl der Kerne auf 16, klettert die 3D-Performance auf mehr als das Dreifache (33.510 Punkte) in den erwarteten Bereich.

Lautrechner

Die brachiale Performance und die umfangreiche Ausstattung fordern beim Energiebedarf ihren Tribut. Bereits bei ruhendem Windows-Desktop saugt die Precision 7875 150 Watt aus der Steckdose. Bei Maximallast mit Prime95 auf der CPU und zweimal Furmark auf den GPUs kletterte der Bedarf auf über 1100 Watt. Statt mit vertretbaren 0,9 sone im Leerlauf brüllten die Lüfter dann mit über 9 sone. Wir empfehlen, entweder gut abgeschirmte Kopfhörer zu verwenden, oder die Workstation an einem entfernten Ort aufzustellen.

Als Goodie hat Dell der Workstation zusätzlich zu den beiden LAN-Ports auf dem Mainboard mit 10 und 1 Gbit/s noch eine 10-Gbit/s-Dual-Port-Netzwerkkarte spendiert. Deren Geschwindigkeit ist geringfügig um fünf Prozent langsamer als die des Anschlusses auf dem Board. Drahtlos kommt die Precision 7875 per Wi-Fi 6E ins Netz. Der WLAN-Adapter von Qualcomm erreicht hervorragende Werte von 1,6 Gbit/s auf kurze und 600 Mbit/s auf 20 Meter Entfernung.

Fazit

Mit der Precision 7875 Tower demonstriert Dell, was technisch derzeit bei Workstations möglich ist. Sowohl bei CPU- als auch GPU-Rohleistung spielt sie ganz vorne mit. Unsere Tests zeigen aber auch, dass viele Profiprogramme 96 CPU-Kerne gar nicht voll ausschöpfen beziehungsweise eine der beiden teuren RTX-6000-Ada-Karten Däumchen drehen lassen. Bei Profi-Workstations muss die Hardwarekonfiguration also sehr genau auf die Anwendungen abgestimmt sein, möchte man nicht Tausende Euros unnötig ausgeben.

(chh@ct.de) ct

Literatur

[1]

Carsten Spille, Hält doppelt besser?, Dual-CPU Workstation Lenovo Thinkstation PX, c't 7/2024, S. 78

[2]

Christian Hirsch, Slowakisches Taschenmesser, Hardware-Probleme mit HWInfo diagnostizieren, c't 8/2022, S. 166

[3]

Carsten Spille, Elitäre Bildveredler, Workstation-Grafikkarten AMD Radeon Pro W7000 und Nvidia RTX 6000 Ada im Test, c't 18/2023, S. 104

Dell Precision 7875 Tower

High-End-Workstation mit 96-Kern-Prozessor und zwei Grafikkarten	
Hardwareausstattung	
CPU / Kerne (Threads) / Takt (Turbo)	AMD Ryzen Threadripper PRO 7995WX / 96 (192) / 2,5 (5,1) GHz
CPU-Fassung / Lüfter (Regelung)	sTR5 / 2 × 8 cm (✓)
RAM (Typ / Max) / -Slots (frei)	128 GByte (DDR5-4800 RDIMM ECC / 2 TByte) / 8 (0)
Grafik (-speicher) / -lüfter	2 × Nvidia RTX 6000 Ada (48 GByte) / 2 × 7 cm
Mainboard (Format) / Chipsatz / TPM	Dell OORP38 (ATX) / WRX80 / fTPM 2.0
Erweiterungs-Slots (nutzbar)	2 × PEG (1 × PCIe 5.0 x16, 1 × PCIe 4.0 x16) (0), 1 × PCIe 5.0 x8 (1), 2 × PCIe 4.0 x8 (0), 1 × PCIe 4.0 x4 (0), 2 × M.2-2280/30 (PCIe 4.0 x4) (1)
SSDs (Typ, Kapazität)	2 × SK Hynix 1TB PC801 (PCIe 4.0 x4)
Optisches Laufwerk (Art) / Kartenleser	HL-DT-ST GU90N (DVD-Brenner) / SDXC (UHS-III)
Einbauschächte (frei)	2 × 2.5"/3,5" (2), 1 × 2,5"/3,5" extern (1), 1 × M.2 extern (0)
Sound (Chip)	HD Audio (Realtek ALC3246)
Netzwerk-Interfaces (Chip, Anbindung)	10 Gbit/s (Marvell AQOC113, PCIe), 2 × 10 Gbit/s (Intel X710-T2L, PCIe), 1 Gbit/s (Realtek RTL8111, PCIe)
WLAN-Interface (Chip, Anbindung)	Wi-Fi 6E (Qualcomm WCN6856, PCIe)
Abmessungen (B × H × T) / Gehäuselüfter (geregelt)	17,3 cm × 44,5 cm × 49 cm / 1 × 14 cm, 2 × 9,2 cm, 1 × 6 cm (✓)
Kensington-Lock / Schlosslasche / Türschloss	n. v. / ✓ / ✓
Netzteil (Leistung)	Dell L1350EPF-00, 80Plus Platinum (1350 Watt)
Anschlüsse hinten	8 × DisplayPort 1.4a, 3 × USB-A 5 Gbit/s, 3 × USB-C 10 Gbit/s, 4 × LAN, 1 × analog Audio
Anschlüsse vorn, oben und seitlich	3 × USB-A 5 Gbit/s, 3 × USB-C 10 Gbit/s, 1 × analog Audio (Headset)
Tastatur / Maus	✓ (drahtlos) / ✓ (drahtlos)
Betriebssystem / installiert im UEFI-Modus / Secure-Boot	Windows 11 Pro / ✓ / –
Elektrische Leistungsaufnahme, Datentransfer-Messungen und Geräuscentwicklung	
Soft-off (mit ErP) / Energie Sparen / Leerlauf (DP UHD)	4,9 W (0,5 W) / 9,0 W / 118 W
Volllast: CPU / CPU und Grafik	538 W / 1154 W
SSD RAID0: Lesen (Schreiben)	12.041 (11.566) MByte/s
USB 3.2 Gen 1 (5 Gbit/s) / USB 3.2 Gen 2 (10 Gbit/s): Lesen (Schreiben)	459 (468) / 1091 (1086) MByte/s
LAN 1/2/3/4: Empfangen (Senden)	119 (119) / 1184 (1185) / 1125 (1134) / 1133 (1183) MByte/s
WLAN 5 GHz / 6 GHz: nah (20 m)	1622 (632) / 1428 (635) Mbit/s
SDXC-Card: Lesen (Schreiben)	278 (258) MByte/s
Geräuscentwicklung: Leerlauf / Vollast (Note)	0,9 Sone (⊕) / 9,1 Sone (⊖⊖)
CPU- / GPU-Last (Note)	2,2 Sone (⊖⊖) / 4,5 Sone (⊖⊖)
Funktionstests	
Secure-Boot ab- / CSM einschaltbar / fTPM	✓ / – / ✓
Wake on LAN: Standby / Soft-off	✓ / –
USB: 5V in Soft-off / Wecken per USB-Tastatur aus: Standby (Soft-off)	✓ / ✓ (✓)
Bootdauer bis Login	53 s
Parallelbetrieb (Digital Monitore)	8 × 4K 60 Hz (8 × DP)
Systemleistung	
Cinebench 2024: 1T / MT	108 / 5882
Blender 3.6.9 „Lone Monk“: CPU / CUDA / OptiX	290 / 45 / 25 s
3DMark: Time Spy	9704 ¹
SpecViewPerf 2020: 3dsmax-07 / catia-06 / creo-03 / energy-03	217 / 141 / 185 / 86
maya-06 / medical-03 / snx-04 / solidworksw-07	587 / 134 / 997 / 303
Handbrake 1.7.2	116 fps
KcBench Linux 6.5.5 mit Modulen	231 s
Procyon AI Image Generation: SD 1.5 / XL	3329 / 2871
Bewertung	
Systemleistung: Office / Rendering / Spiele	⊕⊕ / ⊕⊕ / ⊕⊕
Audio: Wiedergabe	⊕⊕
Geräuscentwicklung / Systemaufbau	○ / ⊕⊕
Preis / Garantie	39.045 € / 36 Monate
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ funktioniert – funktioniert nicht n. v. nicht vorhanden ¹ mit 16 CPU-Kernen: 33.510	

Online-Konferenz am 18. Juni

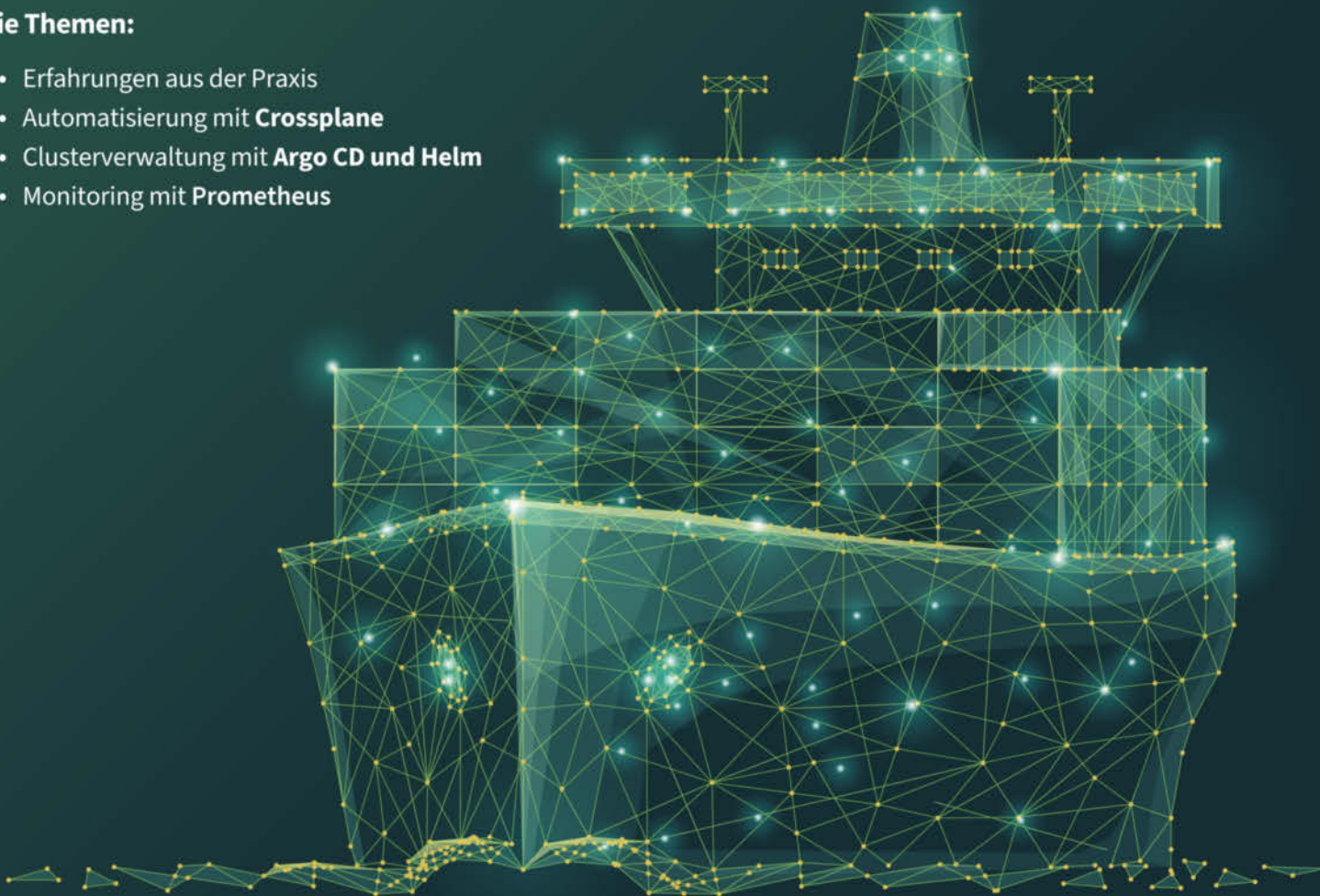
Mastering Kubernetes

Kubernetes-Wissen aus der Praxis: die richtigen Werkzeuge, die erfolgreichsten Strategien.

Mit der ganztägigen Online-Konferenz Mastering Kubernetes erfahren Sie von den **jüngsten Trends** der Container-Orchestrierung und lernen, wie Sie Kubernetes in der Praxis einsetzen. So meistern Sie die wichtigsten **Tools und Techniken** der Cloud-nativen Welt rund um Kubernetes!

Die Themen:

- Erfahrungen aus der Praxis
- Automatisierung mit **Crossplane**
- Clusterverwaltung mit **Argo CD und Helm**
- Monitoring mit **Prometheus**



Jetzt Frühbucher-Ticket sichern:

www.heise-academy.de/konferenzen/mastering-kubernetes-2024



Ihr Partner für
IT-Weiterbildung
Videokurse für
IT-Professionals



Red Hat Enterprise Linux Erstellen und Konfigurieren von Dateisystemen

Lernen Sie von IT-Experten Tom Wechsler die Verwaltung von Dateisystemen unter RHEL, um die Sicherheit und Effizienz Ihrer Umgebung zu optimieren.



Erweiterte Bedrohungssuche in Microsoft Active Directory Domain Services

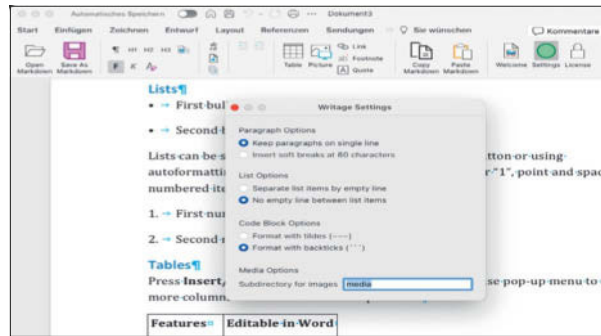
Lernen Sie fortgeschrittene Techniken und Tools kennen, um Schwachstellen in Ihrem Active Directory aufzudecken und Cyber-Angriffe abzuwehren.



Testwerkzeuge für Java- Entwickler

Erweitern Sie Ihr Test-Toolkit mit Spock, AssertJ und anderen leistungsstarken Tools und lernen Sie jede Testherausforderung in Java zu meistern.

Jetzt alle Videokurse
30 Tage kostenlos testen:
heise-academy.de



Word lernt Markdown

Die Erweiterung Writage bringt Microsoft Word die Auszeichnungssprache Markdown bei. Deren Syntax müssen Nutzer nicht beherrschen.

Microsoft Word kann außer DOC/DOCX auch ein paar Fremdformate lesen und schreiben, etwa RTF und ODT. Mit der populären Auszeichnungssprache Markdown kann das Textprogramm jedoch nichts anfangen. Diese Lücke füllt das Add-in Writage, das mit allen Word-Versionen unter Windows und macOS ab Office 2010 funktionieren soll. Getestet haben wir mit Microsoft 365 und Word 2019.

Nach der Installation des Add-ins findet sich auch das Markdown-Format (.md) in den Word-Dateidialogen zum Laden und Speichern von Dokumenten. Außerdem gibt es eine neue Writage-Menüleiste, die unter anderem zwei Schaltflächen enthält, um markierte Textteile als Markdown in die Zwischenablage zu kopieren oder Markdown-Texte daraus in Word einzufügen. Mit den normalen Clipboard-Befehlen klappt das nicht, weil dann die automatische Konvertierung fehlt.

Von Markdown gibt es etliche Dialekte, die sich in Funktionsumfang und Syntax unterscheiden. Writage nutzt CommonMark, eine Art kleinsten gemeinsamen Nenner, erweitert um Tabellen, Fußnoten und Codeblocks mit Angabe der Programmiersprache. Alles, was von diesen Standards abweicht, wird beim Import von Markdown-Texten über Dateimenü oder Zwischenablage ignoriert und entweder in einfachen Text umgewandelt oder behält die Markdown-Zeichen.

Writage macht aus Word einen Markdown-Editor, jedoch keinen klassischen, in dem man die Markdown-Auszeichnungen wie # für Überschriften oder **Text**

für Fettdruck selbst eintippt. Versucht man das, werden die Sonderzeichen als gewöhnlicher Text behandelt. Stattdessen wählt man beim Schreiben die im Writage-Menü angebotenen Textformatierungen und Elemente wie Listen und Tabellen.

Grundsätzlich kann man zwar auch die Word-eigenen Formatierungsoptionen wie fetten oder kursiv setzen verwenden. Dazu muss man aber wissen, welche der zahllosen Word-Funktionen in Markdown umgesetzt werden. Auf der Writage-Homepage findet sich zwar eine Übersicht; im Test gab es aber vor allem bei Überschriften Probleme, vermutlich aufgrund der deutschen Bezeichnung der zugehörigen Absatzformate. Überhaupt ist die freie Definierbarkeit beliebig benannter Formatvorlagen ein Problem, auch beim Export vorhandener Word-Dateien. Das Add-in kann insbesondere benutzerdefinierte Absatzformate nicht interpretieren und zum Beispiel einem selbst erzeugten Format namens „Listing“ die Codeblock-Auszeichnung zuweisen. Daher nutzt man am besten das Add-in-Menü.

Das Aussehen importierter Markdown-Texte legt man in einem selbst definierten Formatvorlagensatz über „Entwurf/Dokumentformatierung“ fest, dem man die Bezeichnung „Writage“ gibt.

Writage macht zwar aus Word keinen vollwertigen Markdown-Editor, eignet sich dafür aber gut für Nutzer, die gelegentlich .md-Texte öffnen oder zum Beispiel für ein Blog- oder CMS-System schreiben wollen, ohne sich mit der Markdown-Syntax befassen zu müssen. Das Add-in kostet einmalig 29 US-Dollar, lässt sich aber 14 Tage lang kostenlos ausprobieren. (swi@ct.de)

Writage

Word-Erweiterung	
Hersteller, URL	Writage, writage.com
Systemanf.	Word ab 2010 für Windows oder macOS
Preis	29 US-\$



Cooler Sechser

Die sechste Generation des Prozessor-kühlers Scythe Mugen arbeitet leise und bändigt auch CPU-Hitzköpfe.

Gegenüber der fünften Mugen-Generation hat Hersteller Scythe den Tower-Kühler sanft aktualisiert. Sein Kühlturm ist jetzt nicht mehr nur etwas zur Gehäuserückseite versetzt, sondern auch leicht nach rechts. So bleibt mehr Raum für Grafikkarten mit dickem Rücken im ersten PCIe-Slot und der neue 120-Millimeter-Lüfter kommt Übertakter-RAM mit aufragenden Kühlkörpern nicht ins Gehege.

Optisch hat der Tower etwas an Charakter verloren, denn die Heatpipes lugen nicht mehr wie beim Vorgänger aus dem Deckel. Dafür macht der neue Lüfter „Wonder Tornado“ mit der großen Nabe und den neun stark gewölbten Schaufeln mehr her. Scythe bietet den Mugen 6 neben der einfachen, metallfarbenen Variante mit einem Lüfter auch als Dual Fan Black Edition, bei der selbst das Montage-material mattschwarz ist. Beide Mugen-6-Versionen passen auf alle Desktop-CPU-Sockel der letzten Dekade außer auf die Ryzen Threadripper. Das Handbuch führt mit klar verständlichen Piktogrammen schrittweise durch die Montage.

Im Test hatte der gut ein Kilogramm schwere Kühler mit einem Core i5-14600K (Dauerturbo: 181 Watt) leichtes Spiel. Ohne CPU-Last ist der Lüfter praktisch unhörbar. Anhaltend auf allen Kernen mit Prime95 gestresst, wurde der Prozessor im offenen Testaufbau rund 80 °C heiß mit

kurzzeitigen Spitzen bis 87 °C. Dabei drehte der Lüfter anhand unserer angepassten Lüfterkurve mit circa 1200 U/min bei flüsterleisen 0,2 sone. So sah es auch in der Blender-Testszene Lone Monk aus, die die CPU in 1666 Sekunden renderte, ähnlich schnell wie unter dem Mugen 5 Rev. C (siehe c't 15/2022, S. 78). Dreht der Lüfter voll auf, erreicht er knapp 2000 U/min und 1,5 sone. Mit zwei Lüftern bestückt, sank die Temperatur um etwa 2 °C, die Performance verbesserte sich aber nicht weiter.

Einen Core i7-14700K (253 Turbo-Watt) bekam die Dual-Fan-Edition ebenfalls gebändigt, wenngleich mit Hitzespitzen bis 94 °C. Dabei gaben die Zwillings-quirle mit unserer Lüfterkurve bei rund 1500 U/min gut 0,7 sone von sich, bei voller Drehzahl laute 2,2 sone. Im geschlossenen Gehäuse dürfte es wärmer zugehen.

Der Scythe Mugen 6 kühlt besser und leiser als die Vorgängergeneration. Mit zwei Lüftern spielt er beinahe in derselben Liga wie Doppelturmkühler vom Schlage eines Corsair A115 oder Noctua NH-D15 – zum halben Preis. (bkr@ct.de)

Scythe Mugen 6 (SCMG-6000)

Tower-Kühler für Mittelklasse-CPU's

Hersteller, URL	Scythe, scythe-eu.com
CPU-Fassungen	AMD: AM5/AM4 Intel: LGA1700/1200/115X/2066/2011-v3/2011
Maße (B × H × T) / Gewicht	132 mm × 154 mm × 106 mm / 1013 g
Lüfter (Typ / PWM) / Drehzahlbereich	1 × 120 mm (Wonder Tornado 120 PWM / ✓) / 300–2000 U/min
Lautheit bei PWM 25 / 50 / 75 / 100 (Note)	<0,1 (⊕) / 0,1 (⊕) / 0,6 (⊕) / 1,5 (○)
Preis / Garantie	46 € (Dual Fan: 52 €) / 2 Jahre

KONTROLLE ÜBERNEHMEN



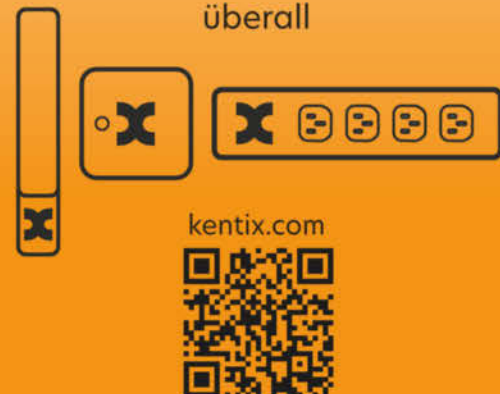
ab
525 €
zzgl. MwSt.

40 Gefahren – Eine Lösung

Alles auf einen Blick

Monitoring, Zutrittskontrolle,
Video, PDU und mehr

KentixONE, die geniale IoT-Lösung, sorgt für volle physische Sicherheit in Ihrer IT-Infrastruktur und Rechenzentrum. Einfach, skalierbar, jederzeit von überall



KENTIX
Innovative Security

Warmduscher

Saugroboter Dreame L10s Pro Ultra Heat mit Mopp-Arm und Heißwäsche

Staubige Ecken und hartnäckige Flecken will Dreames neuer Saug- und Wischroboter mit einem Teleskop-Mopp und einer Heißwasser-Waschanlage aufmischen. Die beheizte Selbstreinigung bewirkt aber keine Wunder.

Von Berti Kolbow-Lehradt

Verwinkelte Ecken und die Ränder entlang der Fußleisten sind für viele Saug- und Wischroboter wahre Problemzonen: Ihre Saugbürsten und Wischtücher gelangen gewöhnlich dort nicht hin, weil sie zentral unter den kreisrunden Robotern montiert sind und mit den Gehäusekanten abschließen. Bei neueren Modellen schwenkt daher während der Kantenreinigung einer von zwei Mopps an einem Gelenk aus. Dadurch ragen die Putzzotteln über die Saugbots hinaus und dringen so auch in diese letzten unberührten Naturräume von Wollmäusen vor.

Handgemenge der Wischflossen

Dreame brachte diese Funktion im vorigen Herbst als erste Marke in einem Saug- und Wischroboter nach Europa, allerdings nur im teuren Spitzenmodell. Nachdem der ärgste Rivale Roborock mit einem ausfahrbaren Mopp im Mittelklasse-Gerät Qrevo MaxV für 999 Euro (Test in c't 8/2024, S. 78) konterte, schlägt nun Dreame zurück: Sein neues Modell mit dieser Funktion namens L10s Pro Ultra Heat unterschreitet ebenfalls die psychologisch wichtige Preisschwelle von 1000 Euro.

Als weitere Besonderheit spült die Waschanlage in der Basisstation des Neuzugangs die Mopps mit Wasser, das sie zuvor auf 58 Grad Celsius erhitzt hat. Das soll auch ölige und fettige Rückstände aus

den Mopps waschen und sie so wieder aufnahmefähiger für Schmutz machen.

Wie nahezu alle aktuellen Putzroboter in der oberen Preisregion ist Dreames L10s Pro Ultra Heat ein Multitalent, das saugt und wischt und beim Befahren von Teppich den Wischmopp um einen Zentimeter hebt. Nach der Reinigung saugt die Basisstation den Schmutz aus dem Schmutzbehälter des Bots in einen 3,2-Liter-Beutel und wäscht die Mopps mit Wasser aus einem 4,5-Liter-Kanister. Die Spülbrühe landet am Ende in einem zweiten Kanister mit 4 Liter Fassungsvermögen. Ein Föhn trocknet die Mopps in zwei bis vier Stunden. Ein 200-Milliliter-Tank mit Dosierautomatik träufelt Reinigungsmittel ins Wasser. Dazu, wie viel Wasser der Behälter des Roboters während der Fahrt fasst, äußert sich Dreame nicht. Doch falls das Wasser für einen Putzgang nicht reicht, fährt er zurück zur Basis und tankt nach.

Trotz der vielen Funktionen hat das Robotergehäuse Normalmaß und kommt auch unter flache Möbel. Auch die Basisstation ist in Anbetracht der Tanks und Reinigungsfunktion erfreulich kompakt. Die geschwungene Form des weißen Kunststoffs und goldfarbene Zierflächen ergeben eine wohnzimmertaugliche Optik.

Viele Funktionen, aber nicht ohne Cloud

Der Dreame-Roboter ist schnell betriebsbereit. Dazu hievt man die Station an Ort und Stelle, stöpselt den Netzstecker ein, füllt den Frischwasser- und Reinigungsmittelkanister, schaltet den Roboter ein und verbindet ihn via Hersteller-App mit dem WLAN. Über drei Tasten auf dem Robotergehäuse lässt sich die Putztechnik eingeschränkt auch ohne Smartphone bedienen. Den vollen Funktionsumfang gibt es nur nach dem App-Setup.

Die Software bietet alles, was bei hochwertigen Putzrobotern üblich ist:



Einstellungen für die Saugstärke, den Wasserfluss und die Selbstreinigungsroutinen, zudem erlaubt sie das Putzen ausgewählter Bereiche mit oder ohne Zeitschaltpläne und zeigt nicht zuletzt einen anpassbaren Grundriss mit Live-Ansicht. Diesen kartiert der Roboter wahlweise bei der ersten Reinigung oder auf einer rund zehnminütigen Erkundungsfahrt.

Bei den Reinigungsoptionen kann man sich durch eine sehr große Zahl von Einstellungen kämpfen – oder einfach den Automatik-Modus „CleanGenius“ wählen, den es in zwei Ausführungen gibt: einen für die tägliche Routine oder einen fürs Großreinigen. Beide Modi legen die Reinigungseinstellungen anhand der bei der Kartierung erkannten Raumkategorien sowie dem vom Roboter ermittelten Verschmutzungsgrad des Bodens und der Mopps automatisch fest.

Als Extra bietet die App eine Direkt-schalt zur integrierten Roboterkamera. Mit dieser Webcam-Funktion sieht man auf Wunsch aus der Ferne zu Hause nach dem Rechten oder dem Bot live beim Putzen zu. Ebenso kann man sich Fotos von Hindernissen, die beiseite geräumt werden sollten, über die Dreame-Cloud aufs Smartphone schicken lassen. Ein Zahlencode und Sprachfeedback schützen vor unbemerktem Stalking. Wer sich um die Privatsphäre sorgt, lässt die Videofunktion deaktiviert. Ein kompletter

Offlinebetrieb ist ab Werk aber nicht möglich. Ein persönliches Konto und die Verarbeitung der Steuersignale auf Herstellerservern sind Pflicht. Wer Dreame-Geräte davon entkoppeln will, kann die alternative Firmware Valetudo verwenden, muss dann aber auf Garantie und exklusive Funktionen des Herstellers verzichten.

Rücksichtsvolle Navigation

Für die normale Navigation ohne KI-Hinderniserkennung braucht der Roboter seine Kamera nicht: Mithilfe rotierender Laserdistanzsensoren in seinem Ausichtsturm findet er zuverlässig seine Position im Raum. Die Putzkraft fährt die gesamte Fläche systematisch von außen nach innen in Bahnen ab, ohne Nennenswertes auszulassen. Ein optionaler, ab Werk aktivierter „Kollisionsvermeidungsmodus“ verhindert, dass der Roboter Fußleisten und Möbel ramponiert. Dadurch geht er mit nahezu aller Einrichtung erfreulich rücksichtsvoll um. Nur über chromiertes Rohrstuhlgestänge rumpelt er stumpfhinweg. Die gute Nachricht in dem Zusammenhang: Er überwindet mühelos Schwellen von bis zu zwei Zentimetern Höhe.

Die in Fahrtrichtung guckende Kamera kommt wiederum nur dann ins Spiel, wenn man keine Lust hat, den Boden freizuräumen. Mittels optional aktivierbarer Bildmustererkennung achtet die Technik auf Kleinkram und führt den Roboter darum herum. Im Test windet sich der Dreame-Sauger souverän an Hausschuhen, Socken, Ladekabeln, einer Steckerleiste und eine Kot-Attrappe vorbei. Ein Sektklas rempelt er an, kippt es aber nicht um, eine Playmobilfigur schiebt er beiseite – dadurch entsteht kein Schaden. Damit

erweist sich das Roboter-Navi auch für Eltern und Haustierbesitzer alltagstauglich.

Wischen im letzten Winkel

Möglichst alle Ecken zu erreichen, ohne sich zu verkeilen, sind wichtige Voraussetzungen für ein überzeugendes Putzergebnis. Bei der Wischfunktion zeigt der Dreame-Roboter eine sehr gute Leistung: Sowohl in der Fläche als auch am Rand verputzen die Mopps nahezu sämtlichen verkleckerten Ketchup. Ohne den auf der in Fahrtrichtung rechten Seite ausfahrbaren Mopp-Arm hätte das Gerät die verschmutzte Kante nicht erreicht. Die Flecken in der Fläche waren zu Testzwecken stark angetrocknet. Dass dort minimale Ränder verbleiben, ist folglich akzeptabel. Bemerkenswert gründlich putzt das Gerät die Ecken. Dort setzt der Bot sogar einmal zurück, um mit den Mopps noch ein paar Millimeter mehr abzudecken. Für den normalen Haushaltseinsatz wischt der L10s Pro Ultra Heat außerordentlich gut. Auch teurere Modelle putzen nicht besser.

Beim Staubsaugen auf Hartboden ist das Ergebnis für eine Roboter-Putzflunder sogar spitze. So beseitigt das Gerät 99 von 100 Gramm des aus Kaffeepulver, Haferflocken und Katzenstreu gemixten Testschmutzes. Aus den Ecken klaubt das Gerät 14 von 20 drapierten Trockenerbsen – ein hervorragender Wert. In unseren Tests schaffte bisher kein Modell mehr. Von Auslegeware entfernt der Dreame-Neuzugang mit 93 Gramm etwas weniger, gehört damit aber immer noch zu den sehr guten robotischen Teppichsaugern.

Nach getaner Arbeit des Roboters bietet die Basisstation einen Selbstreini-

gungskomfort auf hohem Niveau. Die Heißwasser-Wäsche der Mopps bringt hingegen kaum Mehrwert. Nach dem zugegebenermaßen extremen Ketchup-Test bleibt nach dem Waschgang nicht weniger von der Pampe in den Zotteln zurück als bei einer Basisstation, die nur mit Raumtemperatur wäscht. Wer die per Klettband montierten Pads als zu schmutzig empfindet, wirft sie besser in die normale Waschmaschine.

Die auf Seite 54 beschriebenen Probleme eines Schwestermodells traten bei der Selbstreinigung unseres Testkandidaten nicht auf.

Fazit

Die Heißwäsche ist kein überzeugendes Kaufargument für den Dreame L10s Pro Ultra Heat, sein Roboter-Arm aber schon. Der Unterschied zwischen Wischgängen mit und ohne ausgefahrenem Mopp ist deutlich erkennbar. An Kanten entfernt er mehr Schmutz als Geräte, die mangels Gelenkarm diese Extrameile nicht gehen. Noch überzeugender ist das Saugergebnis, zumindest auf Hartboden, wo die Putzflunder sich fast alles einverleibt. So gründlich waren bislang bloß Top-Modelle zu Preisen von weit über 1000 Euro.

Mit zuverlässiger Navigation, einfacher Bedienung und komfortabler Selbstreinigung punktet der Dreame-Neuzugang auch in anderen wichtigen Kriterien. Das Ergebnis ist ein sauberes Gesamtpaket, das die Preisschwelle für Geräte mit Rund-um-sorglos-Ausstattung deutlich senkt.

(spo@ct.de) ct



Unter den Tanks für Frisch- und Schmutzwasser steckt in der Basisstation ein herkömmlicher Staubsaugerbeutel, für den Schmutz, der aus dem Bot herausgesaugt wird.

L10s Pro Ultra Heat

Saug- und Wischroboter	
Hersteller, URL	Dreame, de.dreametech.com
Abmessungen (L × B × H, Roboter)	35 cm × 35 cm × 9,7 cm
Abmessungen (L × B × H, Basis)	45,8 cm × 34 cm × 59,1 cm
Akku / Laufzeit (gemessen)	5200 mAh, ca. 220 min.
Betriebsgeräusch	keine Angabe
Sensoren	360-Grad-Lidar, Front-Kamera und -Lidar, optische Treppensensoren, optischer Abstands-sensor an der Seite
Bewertung	
Orientierung / Raumabdeckung	⊕⊕ / ⊕⊕
Umgang mit Hindernissen	⊕⊕
Saugen Teppich / Hartboden	⊕⊕ / ⊕
Wischen	⊕⊕
Funktionsumfang	⊕⊕
Preis	999 €
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht	

Maus- und Tastaturverteiler

Software-Switch für Eingabegeräte

Der Mauszeiger fährt unterbrechungsfrei vom Bildschirm des Desktop-iMac auf den Monitor des daneben stehenden Windows-Notebooks, als befände sich die Maus auf einem System; Tastatursteuerung und Zwischenablage wandern mit: Die Anwendung Synergy steuert die Mehrfachnutzung der Eingabemedien elegant.

Von Jo Bager

Neben dem Arbeitsplatzrechner nutzen Administratoren und Entwickler oft weitere PCs, beispielsweise um neue Software oder Website-Entwürfe zu testen. Um nicht mit mehreren Tastaturen hantieren zu müssen, gibt es Hardware wie KVM- oder KM-Switches (KVM steht für Keyboard, Video und Mouse), mit denen

sich mehrere PCs dieselben Eingabegeräte teilen können. In bestimmten Konfigurationen löst die Software Synergy diese Aufgabe elegant: wenn man mehrere PCs einsetzt, die jeweils über einen eigenen Monitor verfügen.

Einfache Einrichtung

Synergy baut auf betagten Urhahnen auf, ein erster Vorläufer erschien 1996. Über viele Jahre verlief die Weiterentwicklung schlep-pend, diverse Ableger entstanden. 2020 hat der Hersteller mit der Entwicklung der in vieler Hinsicht überarbeiteten aktuellen Version 3 begonnen. Wir haben den Re-lease Candidate 3 mit verschiedenen Set-ups unter Windows 11, macOS 14 und Ubuntu 22 in mehreren LANs getestet.


Die Einrichtung gestaltet sich sehr einfach: Man installiert die Software auf allen Geräten. Sofern sich die Geräte im selben LAN befinden, finden sie sich ge-genseitig und zeigen sich und die jeweils anderen Geräte als Icons unter „Screen layout“ an. Sollten sich Rechner nicht automatisch finden, zeigt Synergy die rich-

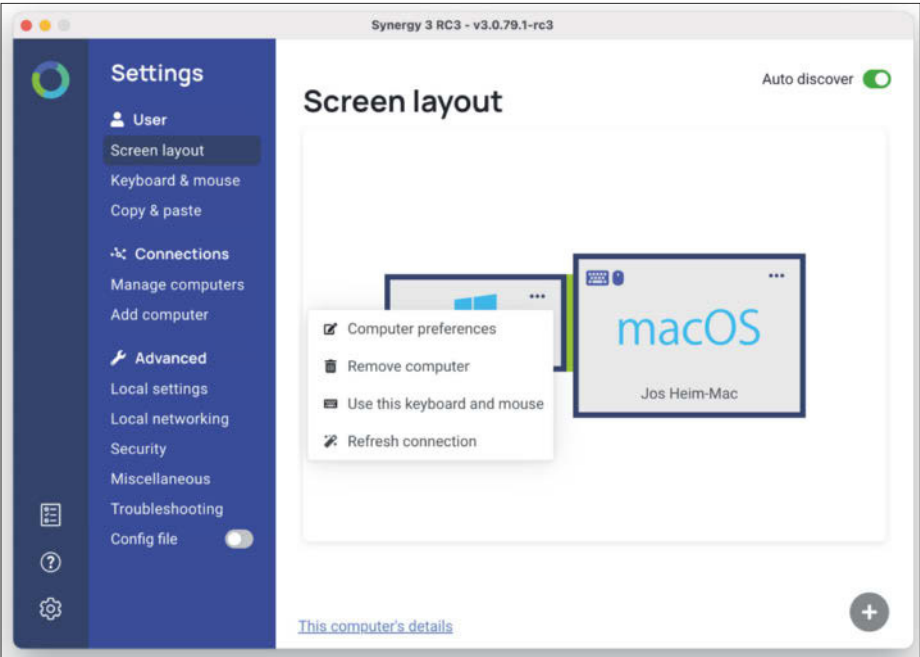
tigen Einstellungen für die einzelnen PCs an. In einer der Installationen verschiebt, vergrößert und verkleinert man die Icons der Rechner, bis sie der realen Anordnung der Monitore entsprechen. Anschließend legt man noch fest, von welchem PC aus man die anderen fernsteuert – fertig.

Synergy hebt im Screen Layout die Bereiche hervor, in denen die Maus von einem Rechner zum anderen fahren kann. Bewegt man den Mauszeiger über die Rechnergrenzen hinweg, wandert die Tas-tatursteuerung mit. Dabei gelten die Tas-taturbelegungen des Systems, auf dem sich die Maus befindet.

Das Setup lässt sich noch in vielerlei Hinsicht feintunen. So kann man für jeden Bildschirm tote Ecken definieren, durch die die Maus nicht auf einen Nachbarbildschirm wandern soll. Für Rechner, die von einem anderen PC aus gesteuert werden, kann man festlegen, welche Taste statt der dort üblichen Modifikatortasten wie Shift oder Ctrl genutzt werden sollen. Per be-nutzerdefinierten Hotkeys kann man zu einem bestimmten PC wechseln.

Synergy kopiert Texte und Bilder per Zwischenablage über Systemgrenzen hin-weg, Drag & Drop lässt sich als experi-mentelles Feature einschalten. Ein PC lässt sich mit Synergy in mehreren Um-gebungen nutzen. Wer zum Beispiel das Notebook im Homeoffice und in der Firma nutzt, kann es in beiden Umgebun-gen mit verschiedenen PCs per Synergy vernetzen.

Synergy ist in zwei Versionen erhält-lich. Für einmalig 29 US-Dollar darf man die Software mit maximal drei PCs nutzen, erhält ein Jahr lang technischen Support und Updates. Für 59 US-Dollar verlängern sich die Zeiträume auf jeweils fünf Jahre und man darf bis zu 15 PCs vernetzen. Zu-sätzlich lässt sich die Kommunikation per TLS verschlüsseln. Man kann die Software 30 Tage lang testen. (jo@ct.de) 



Per „Screen layout“ bildet man die Anordnung der realen PC-Monitore nach und legt fest, wo die Maus von einem zum anderen wandern darf.

Synergy 3 RC3

Software-Switch für Maus und Tastatur	
Hersteller, URL	Symless, symless.com/synergy
System ab Version	Windows 10, macOS 10.14, Ubuntu 18, Debian 10, Fedora 35, Linux Flatpak
Preis	29 US-\$ (1 Jahr Updates und Support, 3 PCs), Ultimate für 59 US-\$ (5 Jahre Up-dates und Support, 15 PCs)

Schalten via Anruf

Erweitern Sie VoIP-Anlagen
um Schaltkontakte



VoIP-Einbindung

Der W&T SIP Ring Switch wird einfach als Nebenstelle in Ihre VoIP-Anlage eingebunden.

Vier Schaltausgänge

Jedem Schaltausgang kann eine Rufnummer zugeordnet werden. Die Ausgänge sind als Ein-, Um- oder Impulsschalter konfigurierbar.

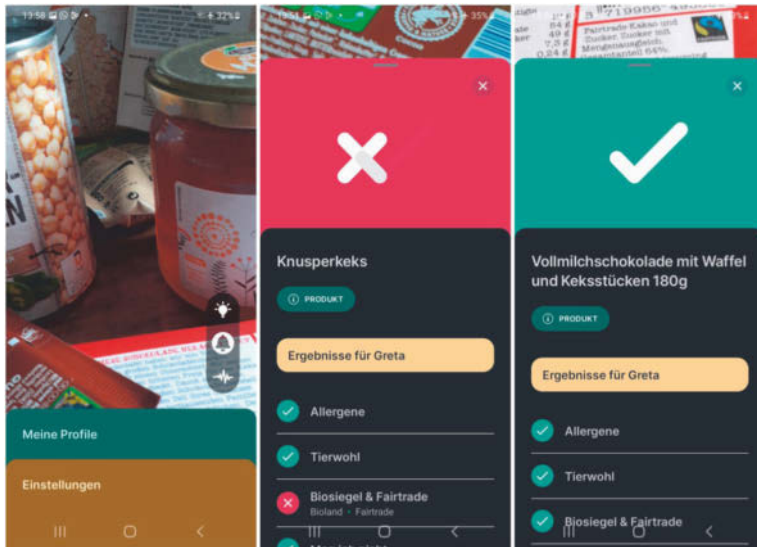
Meldefunktionen

Zusätzlich können Alarmer via E-Mail oder HTTP-Request abgesetzt werden.

Neugierig?
www.wut.de/sip



W&T
www.WuT.de



Einkaufssehlfelpe

Brennwerte, Zuckergehalt, Allergene: Lebensmittelverpackungen ver-raten wichtige Informationen meist im Kleingedruckten. Das ist nervig für alle und ein Problem für Menschen mit Sehbeeinträchtigung. Hilfe verspricht die SOVI-App.

Scannen Nutzer die Barcodes von Lebensmitteln mit der SOVI-App, liefert sie die Produktinformationen übersichtlich, gut lesbar und mit Quellenangabe. Bei einigen Produkten reicht es sogar, die Verpackung zu scannen; Voraussetzung ist, dass diese mit dem DW-Code bedruckt ist (Digital Watermark), der für das menschliche Auge unsichtbar ist.

Erstellt man in der App ein Ernährungsprofil, erkennt sie auch, ob ein Produkt dazu passt oder nicht. Nutzer erfassen im Profil beispielsweise unerwünschte Allergene und gewünschte Biosiegel, geben an, ob sie sich vegan ernähren und grenzen die Nährwerte ein. Nach dem Scan zeigt die App das Ergebnis an und gibt optional ein akustisches Signal.

Die kostenlose Basisversion der App erlaubt 20 Scans pro Kalendermonat und bis zu drei Profile, die man mit anderen Personen teilen kann. Laut SOVI-Website lässt sich auch eine Gruppe erstellen, im Test ging das aber erst mit der Premiumversion. Diese kostet monatlich 2,49 Euro oder jährlich 19,99 Euro und lässt sich zwei Wochen lang gratis ausprobieren. Mit ihr sind Scans, Profile und Gruppen unbegrenzt, außerdem gibt es eine „Schnell-Scan“-Funktion. Anbieter der App ist das hannoversche Unternehmen SonicView.

Die Bedienoberfläche der SOVI-App ist einfach und startet direkt im Scan-Modus,

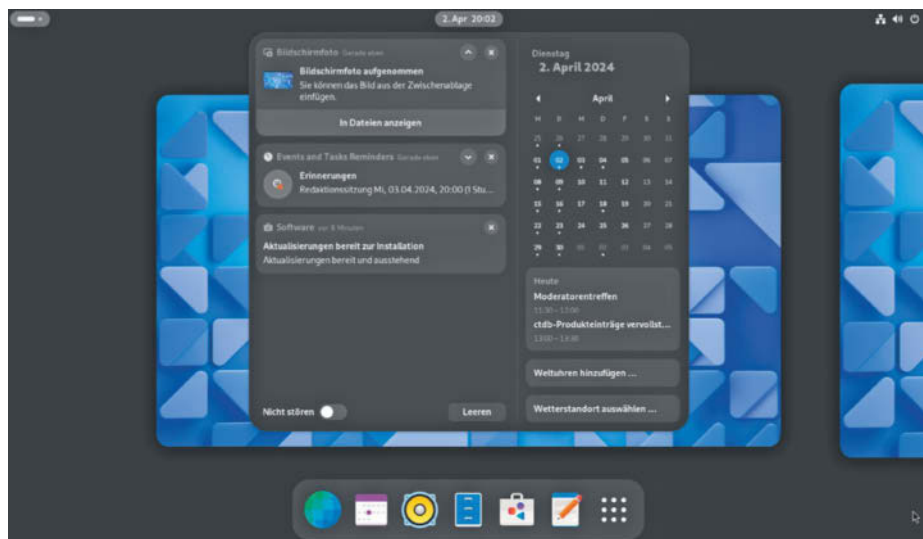
nachdem man sich angemeldet hat. Über zwei farbige Balken unten gelangt man zu den Einstellungen (unten, gelb) und den Profilen (oben, grün). Am rechten Rand stapeln sich drei Buttons: Mit der Glühlampe schaltet man die Taschenlampe ein, um leichter zu scannen, über die Glocke aktiviert man den Ton und der Button mit dem Wellen-Symbol startet den Schnell-Scan.

Beim Schnell-Scan erfassen Nutzer mehrere Produkte hintereinander, die App liest nur die Namen vor. Im normalen Scan-Modus gleicht SOVI die Produkte mit den Ernährungsprofilen ab, die im Bereich „Heute kaufe ich ein für“ stehen. Kauft man für mehrere Personen ein, listet die App auf, zu wem das gescannte Produkt passt und zu wem nicht. Damit hebt sich SOVI von ähnlichen Apps ab, wie wir sie bereits getestet haben (c't 1/2022). Nach dem Scan erhält man via „Produkt“-Button detaillierte Produktinformationen.

SOVI funktioniert auch mit Bedienungshilfen, in den Einstellungen legen Nutzer unter „Klartext“ fest, welche Produktinformationen die App nach dem Scan vorlesen soll. Mit Google TalkBack klappte das bei uns ziemlich gut. Nur der Signalton, wenn ein Produkt nicht zum Profil passt, könnte im Screenreader-Geplapper untergehen. Bis auf kleinere Haken – beispielsweise hängte sich SOVI einmal auf, statt Infos zur Premiumversion zu zeigen – funktionierte die App bei uns problemlos. (gref@ct.de)

SOVI – blind einkaufen

Einkaufs-App	
Hersteller, URL	SonicView, sonicview.de
Systemanf.	Android ab 6.0, iOS ab 14.0
Preis	kostenlose Basisversion; Premiumversion 2,49 €/Monat oder 19,99 €/Jahr



Findiger Desktop

Gnome 46 mit verbesserter Suche

Die neue Version des beliebten Linux-Desktops Gnome bringt eine globale Suchfunktion und eine neue grafische Fernanmeldung. Im Wayland-Modus unterstützt Gnome erstmals variable Bildwiederholraten, vorerst allerdings nur experimentell.

Von Keywan Tonekaboni

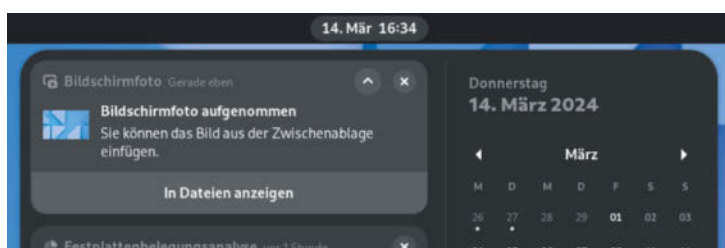
Pünktlich zum Frühlingsanfang veröffentlichte das Gnome-Projekt die neueste Version ihrer Linux-Desktopumgebung. Neben viel Feinschliff am Dateimanager, den Benachrichtigungen sowie Arbeiten am Unterbau gibt es auch ein paar neue Funktionen.

Eine der auffälligsten Änderungen in Gnome 46 betrifft das Benachrichtigungssystem, welches seit langem sehr unübersichtlich ist. Die einzelnen Notifications zeigen nun klar an, von welcher Anwendung sie stammen. Außerdem können Nutzer die Meldungen ausklappen und darüber direkt einfache Aktionen aufrufen. Das muss aber die App, von der die

Benachrichtigung stammt, auch implementieren. Das Facelifting der Benachrichtigungen reduziert die Unordnung etwas, überwindet sie aber nicht gänzlich. Eine Gruppierung der Benachrichtigungen, die für mehr Übersicht sorgen würde, hat es nicht in Gnome 46 hinein geschafft, aber die Entwickler arbeiten bereits daran.

Dateimanager mit Durchblick

Die Oberfläche des Dateimanagers Nautilus ist eine der Dauerbaustellen in Gnome. In der jüngsten Version haben die Entwickler die Anzeige der Kopiervorgänge optimiert. Statt einer winzigen Tortengrafik im Fenstertitel zeigt Nautilus sie jetzt größer ganz unten in der Seitenleiste an, unterhalb von Ordnerliste, Favoriten und eingebundenen Datenträgern. Bei mehreren parallelen Vorgängen sieht man jetzt für jede Dateioperation eine eigene Fortschrittsgrafik.



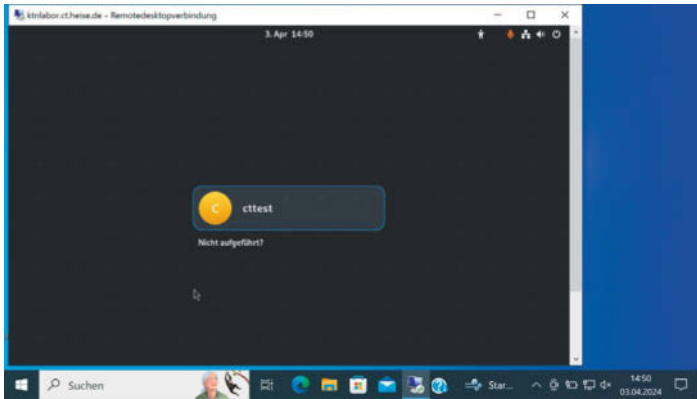
Die Benachrichtigungen in Gnome 46 verraten, von welcher App sie stammen.

Hinzugekommen ist eine neue globale Suchfunktion in Nautilus, die direkt aus der oberen linken Ecke des Dateimanagers zugänglich ist. Über den Suchknopf mit der Lupe initiiert man mit einem Klick eine Dateisuche über alle indextierten Verzeichnisse hinweg. Bisher musste man zunächst im lokalen Ordner suchen und dann extra auf die Schaltfläche „Überall suchen“ klicken. Der alte Knopf für die lokale Suche ist weiter vorhanden, hat aber jetzt ein anderes Icon. Gnome wird ja gerne nachgesagt, Features unbedacht zu entfernen; zur Abwechslung gibt es nun eine Funktion sogar doppelt.

Von Windows zu Gnome

Bereits seit Längerem kann Gnome die aktuelle Sitzung per Bildschirmfreigabe über RDP (Remote Desktop Protocol) teilen. Mit Gnome 46 wird die Funktion durch eine RDP-gestützte Fernanmeldung ergänzt. So kann man sich auch dann verbinden, wenn noch kein Nutzer angemeldet ist. Technisch gesehen teilt dann nicht die Gnome-Shell den Bildschirm, sondern der Displaymanager GDM. Dort meldet man sich wie gewohnt an, wodurch sich Gnome mit Bordmitteln als Remote Desktop nutzen lässt.

Bei unseren Tests klappte dies mit einer Beta-Version von Gnome Connections oder dem Remote-Desktop-Tool von Windows auf der Clientseite, während wir mit Remmina keine Verbindung aufbauen konnten. Beim Remote-Desktop-Tool gibt es allerdings einen Fehler, weshalb es keine sichere Verbindung nutzt. GDM erkennt das und warnt davor, aber die Fehlermeldung ist nicht sonderlich verständlich. (Wir haben einen Bugreport eingereicht.) Damit das Remote-Desktop-Tool sichere Verbindungen nutzt, muss man die Verbindungskonfiguration als Datei abspeichern und diese mit einem Texteditor öffnen. Dort ergänzt man die Zeile `use redirection server name:i:1` oder ändert in der vorhandenen Zeile `...:i:0` zu `...:i:1`. Anschließend klappte die Anmeldung über eine sichere Verbindung per Doppelklick auf die Datei.



Gnome 46 erlaubt jetzt sich aus der Ferne neu anzumelden, etwa von einem Windows-PC aus, und nicht nur eine bestehende Desktop-Session zu teilen.

aliasing und dadurch auch besseres Fractional Scaling: Die Unified Renderer können bei krummen Skalierungsfaktoren wie 1,25 Fenster direkt auf diese Größe zeichnen, statt sie erst auf 200 Prozent zu vergrößern und dann wieder auf 125 Prozent herunterzurechnen. Die Unified Renderer sollen auch die Grundlage für zukünftige Entwicklungen bilden, etwa eine solide Farbverwaltung samt HDR oder bessere Performance auf schwachen Geräten. Noch sind sie aber nicht so optimiert wie der alte OpenGL-Renderer.

Fazit

In Gnome 46 steht vor allem der Feinschliff im Vordergrund, was auch durch den sechsmonatigen Releasezyklus bedingt ist. Doch auch für Feinheiten, wie die neue globale Suche oder der überarbeitete Dateimanager, lohnt sich ein Upgrade. Die leicht zu konfigurierende Fernanmeldung ist in Zeiten von Homeoffice nützlich, wenn man von zu Hause aus auf dem Bürorechner etwas erledigen will, wofür SSH und Terminal nicht reichen.

Gnome 46 wird unter anderem mit Fedora 40 und Ubuntu 24.04 LTS ausgeliefert werden, die Ende April erscheinen. In Arch Linux landet Gnome voraussichtlich erst mit dem ersten Korrektur-Update 46.1. Wer eine virtuelle Maschine nicht scheut oder über einen Testcomputer verfügt, dessen Datenträger der Installer überschreiben darf, kann Gnome 46 über die projekteigene Immutable-Distribution Gnome OS ausprobieren. (ktn@ct.de) **ct**

Video, Release Notes und GTK-Blogpost:
ct.de/y9nr

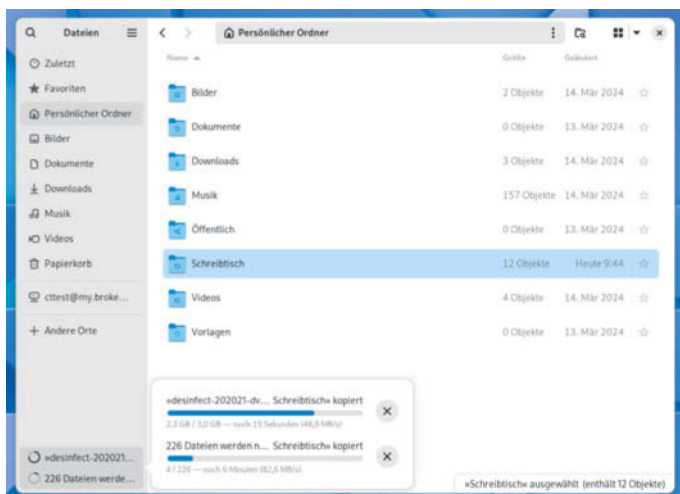
In Gnome findet man die Fernanmeldung in den Einstellungen des neuen System-Panels. Es ist neu, weil das Gnome-Team in Version 46 die Systemeinstellungen grundlegend überarbeitet und neu organisiert hat, um die Bedienung intuitiver zu gestalten. Während weniger häufig genutzte Funktionen in das erwähnte System-Panel integriert wurden, sind wichtige Einstellungen wie Bildschirm- oder Audio-Optionen nun prominenter platziert. Da dies die Kategorien in der Seitenleiste reduziert, sind die Einstellungen jetzt deutlich übersichtlicher.

Neue Renderer und variable Bildwiederholraten

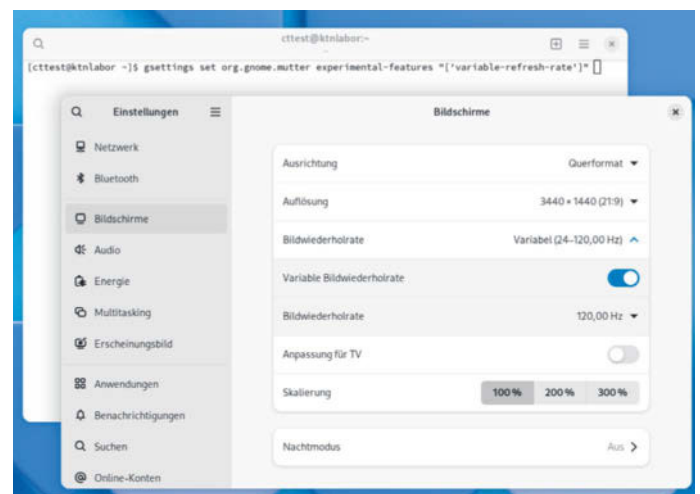
Was Gamer und technisch anspruchsvolle Nutzer freuen wird: Gnome 46 unterstützt im Wayland-Modus erstmals variable Bildwiederholraten (Variable Refresh Rate, VRR). Die auch als VESA Adaptive-Sync oder AMD Freesync bekannte Funktion erlaubt ein flüssigeres Bild, indem die Bildraten von Grafikkarte und Monitor aufeinander abgestimmt werden. Das ver-

meidet Ruckler, wenn etwa ein 60-Hertz-Video auf einem Bildschirm mit 144 Hertz Wiederholrate abgespielt wird. Via VRR wird dann der Monitor auf 120 Hertz gedrosselt, was zu gleichmäßigen Frames führt. Da die Funktion zunächst noch als experimentell gilt, muss man sie im Terminal mit `gsettings set org.gnome.mutter experimental-features "['variable-refresh-rate']"` explizit aktivieren. Nach einem Neustart erscheint auf unterstützter Hardware in den Systemeinstellungen bei der Monitorkonfiguration ein Schalter „Variable Bildschirmrate“. Bei uns klappte es mit einer Einsteiger-AMD-Radeon-Grafikkarte, aber nicht auf einem Intel-System mit integrierter Grafik.

Darüber hinaus bringt Gnome 46 zwei neue Renderer für die Grafikbibliothek GTK mit: für OpenGL und für Vulkan. Sie heißen Unified Renderer, da sie aus einer Quelle kommen und viel Code miteinander teilen. Die Entwickler erklären im GTK-Blog (siehe ct.de/y9nr) die Hintergründe und versprechen sich davon eine präzisere Darstellung, verbessertes Anti-



Kopiervorgänge zeigt Nautilus nun übersichtlich in der Seitenleiste an.



Wer die noch experimentelle Funktion aktiviert, kann variable Bildwiederholraten in Gnome ausprobieren.



Leinen los!

Fünf 27-Zoll-Monitore mit 4K-Auflösung und USB-C-Eingang im Test

Ultrahochauflösende 27-Zoll-Monitore kombinieren viel Bildfläche mit kompakter Bauform. Aktuelle Displays zeigen schöne Farben, binden PCs und Notebooks über ein einziges USB-C-Kabel an und sind schon ab 380 Euro zu haben.

Von Ulrike Kuhlmann

Ein 27-Zoll-Monitor bietet ausreichend Schirmfläche für komfortables Arbeiten und braucht nicht allzu viel Platz auf dem Schreibtisch. 27-Zöller gehören deshalb zu den beliebtesten Monitorgrößen. Wir haben für diesen Test Geräte mit 4K-Auflösung und USB-C-Eingängen ausgewählt. Die Displays erreichen eine Pixeldichte von 163 Pixel pro Zoll (dots per inch, dpi), bei der auch scharfsichtige Augen keine Pixelstruktur mehr sehen.

Ein Kabel für alles

Unsere Testkandidaten sind der BenQ PD2706U, der ThinkVision P27pz-30 von Lenovo, der 27UP850N von LG, der Phi-

lips Brilliance 27B1U7903 und Samsungs S27A800UJU. Letzterer ist das Modell aus 2021, den gleich ausgestatteten, preiswerteren Nachfolger mit der Endung 800UJP konnten wir leider nicht testen. Alle fünf bringen mindestens einen USB-C-Eingang mit, über den sie erstens Video-signale fürs Display empfangen, zweitens das Notebook mit Strom versorgen und drittens weitere Peripheriegeräte anbinden. Sie integrieren dazu einen USB-Hub für Tastatur, Maus, Festplatte oder Webcam und laden via USB-C angeschlossene Mobilgeräte per Power Delivery (USB-PD) auf. Deshalb reicht ein einziges Kabel zwischen Notebook und Monitor.

Die fünf Displays lassen sich in der Höhe verstellen und zur Seite sowie ins Hochformat drehen. Ergonomisch sind auch die eingebauten Panels in IPS-Technik (In-Plane Switching): Dank ihr sieht die Darstellung sowohl von der Seite als auch am um 90 Grad gedrehten Display aus wie in Normalstellung von vorn.

Soweit zu den Gemeinsamkeiten unserer fünf Testgeräte, die sich enorm im Preis unterscheiden – sie kosten zwischen

380 und 1200 Euro. Diese Unterschiede rühren zum Teil von der Qualität der jeweils eingebauten Displays her, zum Teil von der sonstigen Ausstattung. Zwei Monitore integrieren außer zahlreichen Videoeingängen diverse USB-Ports und einen LAN-Anschluss. Vier Geräte bremsen die Datenübertragung per USB-C auf USB-2.0-Geschwindigkeit, wenn sie Videodaten empfangen. Nur der Philips-Monitor hält die schnelle Übertragung dank Thunderbolt 4 auch bei 4K mit 60 Hertz und 10 Bit Farbauflösung aufrecht. Für anspruchsvolles Gaming taugen alle fünf nicht. LG und Philips unterstützen immerhin FreeSync respektive Adaptive Sync und geben fließende Bewegungen recht schlierenfrei wieder; die Schaltzeiten des BenQ waren vergleichbar.

Vier der Monitore können zwei Signalquellen gleichzeitig auf den Schirm holen, wahlweise nebeneinander (Side by Side, SbS) oder ineinander (Picture in Picture, PiP). BenQ und Lenovo integrieren zusätzlich zum USB-Hub einen KVM-Umschalter für Tastatur, Maus und Video. Damit kann man ein Eingabeset für zwei angeschlossene PCs nutzen, die Umschaltung erfolgt automatisch beziehungsweise bei einer Bild-neben-Bild-Darstellung über einen Tastendruck am Monitor.

Mini-LEDs für HDR

Der größte Kostentreiber ist allerdings das Hintergrundlicht der LC-Displays: Drei haben ein herkömmliches Edge-LED-Backlight mit kleinen Dioden am Displayrand. Dabei handelt es sich um blaue, mit grünem und rotem Phosphor beschichtete Leuchtdioden. Die RGB-Mischung ergibt zusammen weißes Licht, das dünne Folien möglichst gleichmäßig im Rücken des Displays verteilen. Farbfilter über den RGB-Subpixeln erzeugen daraus am Ende wieder farbiges Licht.



BenQ PD2706U

Der DesignVue ist ideal, wenn man mehrere PCs parallel betreibt: Über den eingebauten KVM-Umschalter kann man ein Set aus Tastatur, Maus und Webcam dem jeweils genutzten PC zuordnen. Bei den Monitoreinstellungen hilft ein kleiner Puck mit Drehrad und fünf Tasten, der per USB am Monitor hängt. Alternativ finden sich aber auch Tasten hinten am Display. Die Funktion „Burn-In beheben“ im Menü schaltet in schneller Folge endlos drei unterschiedlich graue Inhalte auf dem Schirm – Sinn unklar.

Die Uniformity-Funktion für eine homogene Ausleuchtung begrenzt die Gesamtleuchtdichte und dunkelt die Schirmmitte etwas zu stark ab, bei deaktivierter Funktion ist die Mitte etwas zu hell. Die Ausleuchtung geht aber insgesamt in Ordnung. Grauverläufe gibt der PD2706U mit 10-Bit-Farbauflösung sauber aufgelöst, farbneutral und streifenfrei wieder, nur sehr dunkle Bereiche könnten etwas satter sein. Im USB-C-Betrieb mit Datenübertragung per USB 3.1 reduziert er die Farbauflösung auf 8 Bit. Der Monitor deckt den sRGB-Farbraum vollständig ab, für DCI-P3 fehlt ihm etwas Sättigung im Grün.

Der PD2706U besitzt drei Videoeingänge und zwei USB-Hubs sowie an der Seite eine Klinkenbuchse und zwei weitere USB-Ports zum Laden von Smartphone oder Tablet. Nur die Ethernet-Buchse fehlt, damit er als Dockingstation den Schreibtisch komplett aufräumen könnte. Holt man die Bilder zweier PCs nebeneinander auf das Display, kann man deren Farbwiedergabe unabhängig voneinander einstellen.

- 👆 KVM-Switch
- 👆 saubere Grauverläufe
- 👇 Grün könnte satter sein



Lenovo ThinkVision P27pz-30

Der ThinkVision-Monitor von Lenovo bringt mit seinem lokal dimmbaren Backlight aus RGB-Mini-LEDs die neueste Technik mit und überzeugt mit sehr satten Farben, enormer Leuchtdichte und hohen Kontrasten. Das Backlight birgt im wahrsten Sinne des Wortes auch Schattenseiten: Der Schirm ist an den Rändern dunkler, und Weiß wird mit in einem etwa fünf Zentimeter breiten Rahmen in einer kühleren Farbtemperatur eingefasst. Die Leistungsaufnahme ist die höchste im Testfeld.

Feine Graustufen löst das Display einwandfrei auf. Es bietet diverse Bildpresets, deckt den eingestellten sRGB-Farbraum aber anders als etwa DCI-P3 nicht sauber ab. Der Modus „Lokale Verdunklung“ reißt die Leuchtdichte auf fast 1600 cd/m² auf, der Sinn dieses Scheinwerfermodus blieb unklar. Im Menü finden sich weitere ungewöhnliche Einstellungen, aber auch sinnvolle wie die automatische Helligkeitsanpassung per Umgebungslichtsensor und ein Abwesenheitssensor.

Der Monitor steht sicher auf seiner Fußplatte und hält jede Menge Eingänge bereit. Mit seinem Ethernet-Port und eingebautem KVM-Switch kann der P27pz-30 als Dockingstation dienen. Die rot eingefasste Nut in der Standplatte hält Smartphones, die man per USB-C-PD mit bis zu 15 Watt laden kann.

Wer das höhenverstellbare Display ins Hochformat dreht, muss den Schirm etwas aufklappen, andernfalls rasselt er mit der Ecke auf die Platte und hinterlässt dort unschöne Furchen.

- 👆 integrierte Dockingstation
- 👆 farb-, kontrast- und leuchtstark
- 👇 inhomogen ausgeleuchtet

c't kompakt

- Bei USB-C-Monitoren reicht ein Kabel zwischen Notebook und Monitor.
- Peripherie schließt man über die im Monitor eingebauten USB-Hubs an.
- Dimmbare Mini-LEDs im Backlight sorgen für farb- und kontraststarke Darstellung.



LG 27UP850N

Der Monitor von LG sticht mit seinem schicken weißen Gehäuse aus dem Einheitsschwarz der Mitkandidaten heraus. Vorn ist aber auch er aus ergonomischen Gründen schwarz eingefasst, das lenkt den Blick auf den Bildinhalt. Der Monitor steht sicher auf dem platzgreifenden Sichelfuß. Allerdings wackelt das Display selbst beim Anstupsen. Alle Anschlüsse gehen nach hinten statt nach unten raus, das sieht für den Kollegen am Schreibtisch gegenüber nicht so schön aus. Wer das Display nah an der Wand befestigen möchte, muss sich gewinkelte Stecker besorgen und das klobige externe Netzteil irgendwo unterbringen.

Die beiden USB-Ports für Peripherie sind schnell belegt, davon hätte LG einige mehr einbauen können. Als Dock taugt der Monitor mangels Ethernet-Port aber ohnehin nicht. Als einziger Testkandidat kann der 27UP850N keine zwei Signalquellen gleichzeitig nebeneinander aufs Display holen.

Das Edge-LED-Backlight leuchtet den Schirm etwas ungleichmäßig aus, die Farbtemperatur gerät im sRGB-Preset etwas zu warm. Davon abgesehen deckt das Display sRGB vollständig ab. Wählt man als Bildpreset DCI-P3, geraten Rot und Grün nicht satt genug. Dass der Monitor durchaus sattere Farben erzeugen kann, beweist er im Preset HDR-Effekt: Darin werden Rot, Grün und Blau mit einer zu P3 passenden Sättigung dargeboten. Die Wiedergabe feiner Grauerläufe gelingt dem 27UP850N vorbildlich. Die Schaltzeiten dürften für viele Spiele ausreichen, außerdem beherrscht der Monitor FreeSync.

- ↑ sehr gute Graustufenauflösung
- ↓ inhomogen ausgeleuchtet
- ↓ sparsam ausgestattet



Philips 27B1U7903

Der Brilliance-Monitor von Philips nutzt ein Mini-LED-Backlight mit über 2300 dimmbaren Zonen. Leider produziert das ausgefeilte Backlight unschöne Nebeneffekte. So zeigt ein weißer Bildinhalt am Rand perlenschnurartige Schatten und ist mit einem blaugrauen Rahmen eingefasst. Um die Abwärme der LEDs sicher abzuführen, hat Philips einen Lüfter eingebaut. Der rauscht beim Einschalten einmalig auf, ist aber anschließend nicht mehr zu hören.

Die Leuchtdichte lässt sich im sRGB-Modus großzügig variieren, mit aktiviertem Local Dimming reicht sie bis 850 cd/m². Wie bei Lenovo findet sich im Menü eine unsinnige Funktion, die die Leuchtdichte auf den Maximalwert aufreißt, hier heißt sie „Intelligente Kontrastverbesserung“. Das Menü ist insgesamt verwirrend und lässt sich über die im Rücken eingelassenen Tasten sehr schlecht bedienen.

Feine Grauerläufe stellt das Display farbneutral und streifenfrei dar, nur sehr dunkle Bereiche löst es nicht vollständig auf. Den sRGB-Farbraum deckt der 27B1U7903 perfekt ab, die satten Farben ermöglichen auch DCI-P3 und Adobe RGB, aber nicht BT2020. Die Bewegtbildwiedergabe bleibt schlierenfrei.

Der Monitor wirkt insgesamt sehr wertig, hat zusätzlich einen Ethernet-Port und hält die Datengeschwindigkeit dank Thunderbolt 4 auch bei voller Bildfrequenz und Farbauflösung aufrecht. Er hält einen ausklappbaren Umgebungslichtsensor und Lademöglichkeiten fürs Smartphone bereit. Da fehlt eigentlich nur noch der KVM-Umschalter.

- ↑ integrierte Dockingstation
- ↑ farb-, kontrast- und leuchtstark
- ↓ inhomogen ausgeleuchtet



Samsung S27A800UJ

Samsungs Viewfinity-Monitor steht sicher auf seinem Fuß, das Display lässt sich leichtgängig verstellen. Beim Anstupfen federt der Schirm leicht nach, was die Standsicherheit aber nicht gefährdet. Die Videoeingänge des eleganten Monitors werden von unten belegt, die Anschlüsse für USB-Peripherie und Kopfhörer ragen nach hinten raus.

Aktiviert man den Umgebungslichtsensor, ändert sich die Farbtemperatur der Darstellung, das Bild wird sehr warm. Nutzt man dagegen den dreistufigen Augenschonmodus, um die Leuchtdichte zu reduzieren, bleibt die Farbtemperatur gleich.

Der Monitor hält ausgefeilte Möglichkeiten bereit, zwei Eingangssignale neben- oder ineinander auf den Schirm zu holen. Am USB-C-Hub kann man einstellen, dass die Datenübertragung zur Peripherie mit voller Geschwindigkeit und dann reduzierter Bildwiederholfrequenz erfolgen soll. Als vorübergehende Lösung gut, dauerhaft wird man mit 30 Hertz aber eher nicht arbeiten.

Feine Grauerläufe löste der Monitor zwar streifenfrei, aber etwas farbstichig auf. Das Weißbild wirkt etwas wolzig, die Mitte ist überstrahlt, graue Flächen flirren etwas. Das Display produziert satte Farben und deckt DCI-P3 gut ab. Im sRGB-Preset liegen die Grundfarben etwas außerhalb des Farbdreiecks. Der Leuchtdichteregelbereich reicht im sRGB-Modus wie spezifiziert bis 296 cd/m²; für HDR ist das zu wenig. Die Leistungsaufnahme bleibt mit 23 Watt niedrig, sogar unter den für das Nachfolgemodell genannten Werten.

- ↑ elegantes Gerät
- ↑ umfangreiche Anzeigefunktion
- ↓ inhomogen ausgeleuchtet

In den beiden Monitoren von Lenovo und Philips sitzen stattdessen winzige rote, grüne und blaue Dioden, die gleichmäßig hinter dem Display verteilt wurden und deren RGB-Mischung pro Diodentripel Weiß ergibt. Die Helligkeit der LEDs kann in kleinen Gruppen gezielt gesteuert werden, bei Lenovo sind es 1152 Cluster, bei Philips sogar 2304. Das lokale Dimmen erhöht den In-Bild-Kontrast, also den Unterschied zwischen sehr hellen und sehr dunklen Bildbereichen. Das Bild der LCDs profitiert sichtbar vom Mini-LED-Backlight, wenngleich es nicht an den enormen Kontrast von organischen Displays (OLEDs) heranreicht. Die Mini-LEDs produzieren sattere Farben und

höhere Leuchtdichten für HDR-Inhalte. Die deutlich größere LED-Anzahl kostet aber auch deutlich mehr Energie. Außerdem muss die am Halbleiterübergang der LEDs erzeugte Wärme gründlich abgeführt werden. Bei Philips sorgt dafür ein kleiner Lüfter, den man beim Einschalten deutlich, im Betrieb dagegen gar nicht hört.

Fazit

Die ergonomischen Eigenschaften aller fünf Kandidaten überzeugen: Man braucht keine Zeitschriftenstapel für die richtige Höhe, auch Hochformate sind am IPS-Panel kein Problem und dank USB-C reicht ein einziges Kabel zwischen

Notebook und Monitor. Die beiden High-End-Monitore mit Mini-LED-Backlight von Lenovo und Philips empfehlen sich für die professionelle Bild- und Videobearbeitung. Der Philips 27B1U7903 kann dank Thunderbolt-4-Anschluss die angeschlossene Peripherie jederzeit mit hoher Geschwindigkeit betreiben. Für den normalen Bürobetrieb reichen die Displays mit Edge-LED-Backlight völlig aus. Der 27UP850N von LG gefällt mit guter Bildqualität, ist aber nur sparsam ausgestattet. Wer zwei Geräte anschließen möchte, greift eher zum PD2706U von BenQ mit KVM-Umschalter; als Dockingstation fehlt ihm nur die Ethernet-Buchse. (uk@ct.de) **ct**

27-Zoll-Monitore mit 4K und USB-C

Modell	DesignVue PD2706U	ThinkVision P27p30	27UP850N	Brilliance 27B1U7903	Viewfinity S27A800UJ
Hersteller	BenQ	Lenovo	LG	Philips	Samsung
Diagonale	27" (68,29 cm)	27" (68,29 cm)	27" (68,29 cm)	27" (68,6 cm)	27" (68,6 cm)
Auflösung (Seitenverhältnis) / Pixeldichte	3840 × 2160 Pixel (16:9) / 163 dpi	3840 × 2160 Pixel (16:9) / 163 dpi	3840 × 2160 Pixel (16:9) / 163 dpi	3840 × 2160 Pixel (16:9) / 163 dpi	3840 × 2160 Pixel (16:9) / 163 dpi
Paneltyp / max. Bildwiederholfrequenz	IPS / 60 Hz (mattiert)	IPS / 60 Hz (mattiert)	IPS / 60 Hz (mattiert)	IPS / 60 Hz (mattiert)	IPS / 60 Hz (mattiert)
HDR / Farbauflösung	DisplayHDR 400, HDR 10 / 10 Bit	DisplayHDR 1000, HDR 10, HLG / 10 Bit	DisplayHDR 400, HDR10 / 8 Bit	DisplayHDR 1400, HDR10 / 10 Bit	HDR10 / 8 Bit
Videoeingänge	USB-C mit DP, HDMI 2.0, DisplayPort 1.4	USB-C mit DP, 2 × HDMI 2.1, DisplayPort 1.4	USB-C mit DP, 2 × HDMI 2.0, DisplayPort P 1.4	Thunderbolt 4 / USB-C mit DP, 2 × HDMI 2.0, DisplayPort 1.4	USB-C mit DP, HDMI 2.0, DisplayPort 1.4
USB-Hub	✓ (3 × USB-A 3.2 Gen 1 und USB-C 3.1 Gen 1 mit USB-PD)	✓ (4 × USB-A 3.2 Gen 2 und USB-C 3.2 Gen 2 mit USB-PD)	✓ (2 × USB-A 3.1 Gen 1)	✓ (4 × USB-A 3.2 und Thunderbolt 4 mit USB-PD)	✓ (3 × USB-A 3.1 Gen 1)
sonstige Anschlüsse	3,5-mm-Klinke für Headset, Micro-USB (für Steuerpuck)	3,5-mm-Klinke für Headset, GBit-LAN, DisplayPort	3,5-mm-Klinke für Headset	3,5-mm-Klinke für Headset, GBit-LAN, DisplayPort	3,5-mm-Klinke für Headset
Besonderheiten	Steuerpuck, Stereo-Lautsprecher, ICC-Profilesync	Anwesenheitssensor, Umgebungslichtsensor	Stereo-Lautsprecher	Stereo-Lautsprecher, Umgebungslichtsensor	Umgebungslichtsensor
Lieferumfang	Kabel: Strom, USB-C, HDMI, DisplayPort	Kabel: Strom, USB-C, HDMI, DisplayPort	Netzteil, Kabel: Strom, USB-C, HDMI, DisplayPort	Kabel: Strom, USB-A, Thunderbolt, HDMI, DisplayPort	Kabel: Strom, USB-C, USB-C-auf-A, HDMI
Geräteabmessungen (B × H × T) / Gewicht	61,5 cm × 45-56 cm × 24 cm / 8,3 kg	61,5 cm × 46-55 cm × 22 cm / 6,2 kg	61 cm × 46-57 cm × 22 cm / 4,1 kg	61 × 40-52,5 × 20 cm / 9,4 kg	61 cm × 43,5-54,5 cm × 17,5 cm / 6,7 kg
Picture-in-Picture / Picture-by-Picture / KVM	✓ / ✓ / ✓	✓ / ✓ / ✓	— / — / —	— / ✓ / —	✓ / ✓ / —
VESA-Halterung	✓ (10 cm × 10 cm)	✓ (10 cm × 10 cm)	✓ (10 cm × 10 cm)	✓ (10 cm × 10 cm)	✓ (10 cm × 10 cm)
Ladeleistung USB-C (Power Delivery)	90 W	140 W	90 W	90 W	90 W
Einstellungen: Höhe / Neigung / Drehung / Pivot	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
Messwerte					
Kontrast minimales / erweitertes Sichtfeld	1123:1 (15,7 %) / 743:1 (52,5 %)	1108:1 (19,9 %) / 691:1 (58,1 %)	1075:1 (17,9 %) / 702:1 (53,7 %)	1100:1 (14,4 %) / 739:1 (49 %)	1075:1 (18,1 %) / 690:1 (55,3 %)
Die runden Diagramme geben die Winkelabhängigkeit des Kontrasts wieder. Blaue Farbanteile stehen für niedrige, rötliche für hohe Kontraste. Kreise markieren die Blickwinkel in 20-Grad-Schritten, im Idealfall wäre das gesamte Bild pink. winkelabhängiger Kontrast: Kreise im 20°-Abstand 0 200 400 600					
Leuchtdichteregulierungsbereich sRGB / mit local dimming	50 ... 308 cd/m² / —	80 ... 625 cd/m² / 1580 cd/m²	60 ... 390 cd/m² / —	4 ... 780 cd/m² / 845 cd/m²	65 ... 296 cd/m² / —
Leistungsaufnahme²: Standby / Betrieb³ / volle Helligkeit	0,3 W / 20,1 W / 34,3 W	0,3 W / 27,4 W / 57 bzw. 135 W⁴	0,3 W / 22,8 W / 40,5 W	0,3 W / 38,8 W / 90,3 bzw. 96,5 W	0,3 W / 23,1 W / 35 W
Bewertung und Preis					
Kontrast / Blickwinkelabhängigkeit	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕
Ausleuchtung / Farbwiedergabe	⊕ / ⊕	○ / ⊕⊕	○ / ⊕	○ / ⊕⊕	○ / ⊕
Bedienung / Verarbeitung	⊕⊕ / ⊕	⊕⊕ / ⊕⊕	⊕ / ○	⊖ / ⊕⊕	⊕ / ⊕
Garantie	3 Jahre	3 Jahre	2 Jahre	3 Jahre	3 Jahre
Preis UVP / Straße	500 € / 390 €	1700 € / 1200 €	400 € / 380 €	1300 € / 1150 €	500 € / 540 €
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden — nicht vorhanden					
¹ laut Hersteller ² gemessen bei Signaleingang über HDMI ³ gemessen bei 120 Candela/m² ⁴ mit aktiviertem local dimming					



Voll im Griff

Spezialeingabehilfen ersetzen beim Zocken die Tastatur

Einhandcontroller mit mehreren frei belegbaren Tasten pro Finger wie der MoveMaster RSG und der Azerox Cyborg verkürzen beim Spielen am PC die Wege und damit die Reaktionszeit. Wer jahrelang mit der normalen PC-Tastatur gespielt hat, muss allerdings umlernen.

Von Rudolf Opitz

Das konventionelle Keyboard eignet sich zwar gut für die Texteingabe und zum Manövrieren in einer Tabelle, weniger aber für Spezialanwendungen. Besonders für Computerspiele, bei denen es auf schnelle Reaktion und das exakte Ausfüh-

ren von Bewegungen ankommt, sind selbst hochwertige Gamingtastaturen ein Kompromiss.

Wer PC-Spiele zockt, führt zum Umschauen und Schießen die Maus meist mit der rechten Hand. Fürs Fortbewegen und alle weiteren Aktionen bleibt also nur die andere Hand, die in der Regel über den Tasten W, A, S und D schwebt, den Standardtasten für Bewegungen. Je mehr Spiel-funktionen auf andere Tasten verteilt sind, desto öfter muss die Keyboardhand ihre Standardposition verlassen. Linkshänder führen die Maus mit Links und belegen meist Tasten auf der rechten Tastaturseite.

Bei den beiden Spezialtastaturen Azerox Cyborg und MoveMaster RSG für 215 und 190 Euro ruht die Tastaturhand stattdessen auf einem breiten Steuergriff (MoveMaster RSG) oder einer bequemen Handflächenstütze (Cyborg). Unter den Fingern liegen frei belegbare Tasten. Op-

tisch erinnern beide nicht einmal auf den zweiten Blick an eine Tastatur: Der Name des Cyborg ist gut gewählt, denn der Controller gleicht einer umgestülpten Roboterhand. Der MoveMaster RSG ähnelt eher dem Schubhebel eines Jets: Der Steuergriff funktioniert wie ein hochsensibler Joystick, die Bewegungen der Spielfigur steuert man intuitiv aus dem Handgelenk. So bleiben alle Finger für zwei frei belegbare Tasten pro Finger frei.

Die Einzelteile des Cyborg entstanden auf einem 3D-Drucker, Gleiches galt für die erste MoveMaster-Version. Der aktuelle MoveMaster RSG (Rapid Steering Gear) wird in Spritzgusstechnik gefertigt.

Individuell anpassbar

Beide Eingabegeräte lassen sich auf vielfältige Weise an die Nutzerhand anpassen. Beim MoveMaster RSG kann man Griffhöhe, Höhe der äußeren Fingertasten sowie

horizontale Lage und Winkel der äußeren Daumentaste einstellen. Seinem Cyborg legt Azeron einen Metallschraubendreher bei. Nicht ohne Grund, denn beim Cyborg ist so ziemlich alles verstellbar: Länge, Winkel und Spreizung der Fingertürme, Höhe und Lage der oberen Ausleger, Lage und Anstellwinkel des Daumenpanels mit den Thumbsticks und des Daumenauslegers.

Beide Spezialcontroller nehmen via USB 2.0 Kontakt zum Rechner auf. Beim MoveMaster RSG hängt das Kabel fest an dem mit gut 780 Gramm schweren Steuergerät, das auf vier breiten Gummifüßen rutschfest und sicher auf dem Tisch steht. Neu beim RSG-Modell ist ein eingebauter USB-Hub mit zwei Ports, an die beispielsweise die Gaming-Maus und eine herkömmliche Tastatur passen.

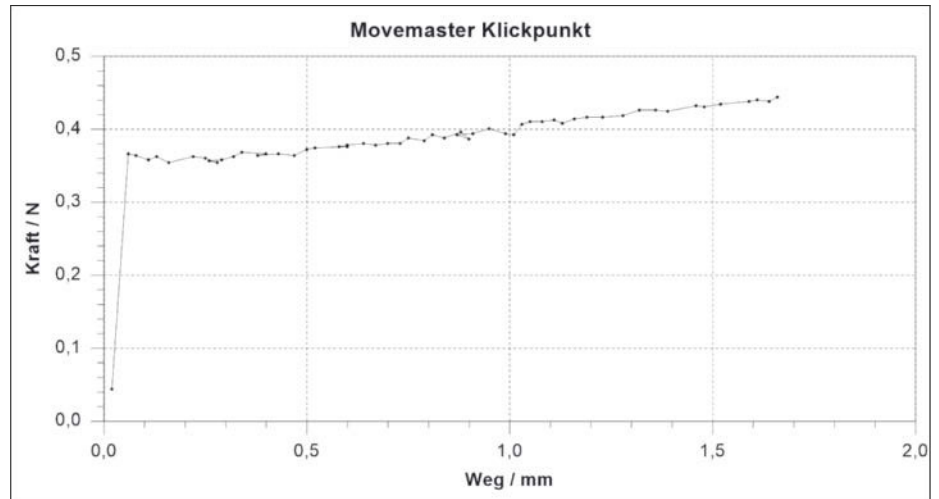
Der Azeron Cyborg wiegt mit etwa 570 Gramm deutlich weniger, dank kleiner Gummifüße unter der Handballenauflage und allen Fingerauslegern steht er aber ebenfalls sehr rutschfest. Wegen der vielen Ausleger belegt er mehr Stellfläche als der MoveMaster. Beide Eingabegeräte sollten mindestens 35 Zentimeter Abstand zur vorderen Tischkante haben, damit der Unterarm entspannt auf dem Tisch aufliegt.

Die Tasten unter dem Griff des MoveMaster RSG sind ab Werk mit den Richtungstasten WASD belegt, eine Bewegung um nur einen Millimeter reicht, um sie auszulösen. Die Fingertasten (Cherry MX Silent Red) haben mit 3,7 Millimetern einen deutlich größeren Hub, im Test schalteten sie bei 1,7 Millimetern. Wer andere Tasten bevorzugt, kann sie austauschen; auf der MoveMaster-Website gibt es dazu eine Anleitung.

Die Fingertasten des Azeron Cyborg schalten dagegen mit 0,45 Millimetern



Der MoveMaster RSG reicht seine USB-Verbindung über einen Hub an die Maus oder ein USB-Headset weiter.



Die Cherry-MX-Silent-Tasten des MoveMaster RSG schalten nach einem Tastenweg von 1,7 Millimetern. Mit 0,45 Newton am Schaltpunkt (0,6 N am Ende des Tastenwegs) gleichen sie einer leichtgängigen mechanischen Schreibtastatur.

sehr schnell. Bei Tasten mit symmetrischen Kappen haben wir eine hohe Auslösekraft von 0,9 Newton gemessen, was mit strammen Maustasten vergleichbar ist. Der Daumen liegt beim Bedienen auf einem Analog-Joystick, direkt darüber gibt es noch einen kleinen klickbaren Digitalsteuerknopf für WASD, der uns im Test aber sehr schwammig vorkam.

Per Software lässt sich auch der analoge Joystick auf die Richtungstasten konfigurieren, doch ist das wegen des Reaktionswegs nicht jedermanns Sache. Der vertikale Ausleger für die Daumensteuerung schwingt außerdem leicht mit, was das schwammige Gefühl noch verstärkt. Bei den Fingerauslegern stört der filigrane Aufbau des Cyborg dagegen kaum.

Software

Hier wie da darf man die Tastenbelegung frei konfigurieren und als Profil direkt auf dem Gerät abspeichern. Der Vorteil: Die gespeicherten Profile stehen auch an PCs, Notebooks oder Konsolen zur Verfügung, auf denen die Konfigurationssoftware nicht läuft. Der Azeron Cyborg speichert sogar zwei Profile.

Die MoveMaster-Anwendung gibt es für Windows, Linux und macOS. Die Software zeigt ein Aufsichtsbild des MoveMasters RSG mit der aktuellen Tastenbelegung, die sich durch Anklicken ändern lassen. Mit der Soft- und Firmware 0.5.2/0.3.2 ist ein Doppelklickmodus hinzugekommen, durch den sich die Anzahl der für die Finger konfigurierbaren Tastenfunktionen auf 20 verdoppelt. Um das

Profil auf den MoveMaster RSG zu laden, reicht ein Klick auf „Konfiguration schreiben“. Unabhängig davon lassen sich die Profile auch auf dem PC speichern und so eine Profilsammlung für verschiedene Spiele erstellen, die man nur noch laden und auf den Controller schreiben muss.

Die komplizierter zu bedienende Azeron-Software gibt es nur für Windows. Sie stellt die Tasten in einer rechteckigen Anordnung dar; will man eine bestimmte Taste auswählen, drückt man sie am Cyborg, worauf das entsprechende Feld im



Beim Cyborg lassen sich Längen und Neigungen der Tasten, die Winkel der Fingerausleger und auch sonst so ziemlich alles individuell anpassen.



Der Azerox Cyborg speichert im Gerät zwei Tastenprofile, zum Wechseln gibt es einen kleinen Druckschalter. LEDs melden das aktive Profil.

Raster aufblinkt. Die Software bietet zwei Modi: Einer bearbeitet nur die beiden auf dem Cyborg gespeicherten Profile, der andere verwaltet Softwareprofile, die nur funktionieren, wenn die Azerox-Software im Hintergrund läuft. Mit ihnen kann man aber auch Doppelbelegungen und Umschalttasten definieren und Makros anlegen. Die Konfiguration ist allerdings unübersichtlich. Das nur in englischer Sprache verfügbare Handbuch geht auf alle Optionen ein, darunter auch Emulationen von Controllern, Joysticks und Gamepads.

Im Spiel

Bei einfachen und schnellen Renn- und Parcours-Spielen oder Shootern gefällt der MoveMaster RSG als blitzschnelles Steuergerät, das sich intuitiv bedienen lässt und einfach Spaß macht. WASD vergisst man damit schnell, Turns und flinke Dre-

hungen fallen mit ihm viel leichter als mit der Tastatur. Anders sieht es bei komplexeren Spielen aus, die weitere Funktionstasten benötigen. Mit zehn Tasten plus Doppelklickbelegung hat der MoveMaster RSG zwar viele Möglichkeiten, doch die muss der an herkömmliche Tastaturen gewöhnte Spieler erst einmal verinnerlichen.

Beim Azerox Cyborg ist die Lernkurve noch steiler, denn allein für die vier Finger gibt es satte 22 Tasten. Es ist sehr bequem, die Hand beim Tippen auf der großen Handflächenablage ruhen zu lassen, während man in Aufbau- und komplexen Rollenspielen Arbeiter oder Armeen dirigiert. Doch dauert es, bis alle Tastenbelegungen memoriert sind und man sich daran gewöhnt hat, Tasten mit dem vorletzten Fingerglied zu betätigen oder den Finger zum Tippen anzuheben. Für entspanntes Navigieren über das Spielfeld ist der Analogjoystick am Daumen okay, zum schnellen Reagieren bei Ego-Shootern reicht er aber nicht. Den kleineren Digitaljoystick will man wegen seiner Schwammigkeit erst recht nicht benutzen und der Träger für die Daumenbedienelemente federt unangenehm nach, wenn die Joystickknöpfe zum Klicken heruntergedrückt werden.

Wer für wen?

Der Azerox Cyborg eignet sich für Fans von komplexen Aufbauspielen, die ausreichend Geduld aufbringen, die zahlreichen Tasten für Fingerspitzen und -glieder zu erlernen. Gleiches gilt für Nutzer von Anwendungen wie Bildbearbeitung, Videoschnitt oder Audioproduktion, deren Hände auf der Standardtastatur weite

Strecken zurücklegen müssen. Doch auch hier bremsst der enorme Umlernaufwand.

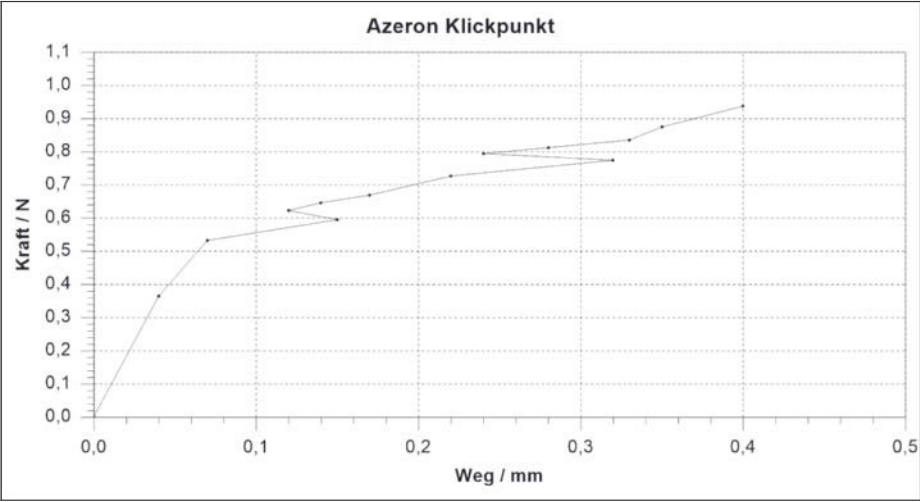
Der MoveMaster RSG begeistert mit seinem robusten und doch empfindlichen Joystick-Griff, der schon auf leichte Bewegungen aus dem Handgelenk reagiert. Verglichen mit dem filigraneren Cyborg steht der MoveMaster wie ein Briefbeschwerer auf dem Schreibtisch. Die zehn Tasten für die freien Finger dürften für viele Spiele ausreichen. Auch hier will die Bedienung geübt sein, wenngleich die Lernkurve flacher verläuft.

Besonders interessant für Linkshänder, die oft Probleme beim Tastenumlegen haben: Den Cyborg gibt es auch für die rechte Hand (die linke führt die Maus); eine Linkshänderversion des MoveMaster RSG ist angekündigt. (rop@ct.de) **ct**

Software und Anleitungen: ct.de/ym9u

Einhand-Gamingcontroller

Modell	Cyborg	MoveMaster RSG
Anbieter, URL	Azerox, azerox.eu	MoveMaster GmbH, movemaster.biz
Tastenanzahl	29	14
Makros	✓	—
Key-Typ	Omron D2F-01	Cherry MX Silent Red
Haltbarkeit (Anschläge) ¹	> 1 Mio. Anschläge	> 50 Mio. Anschläge
Polling Rate ¹	ca. 350 Hz	ca. 400 Hz
Beleuchtung	2 LEDs	—
Schnittstelle	USB 2.0 (Mini-USB)	USB 2.0 fest, USB-Hub mit zwei Ports
Software (Betriebssystem)	Azerox Software 1.4.1 (Windows)	MoveMaster-Software 0.5.2 (Linux, macOS, Windows)
Handflächenablage	✓ (Form wählbar)	✓
Maße (B × T × H)	21 cm × 24 cm × 12 cm	14,5 cm × 14,7 cm × 8 cm
Gewicht / Kabellänge	572 g / 195 cm	782 g / 180 cm
Lieferumfang	USB-Kabel, Schraubendreher mit Wechselspitze, Ersatzschrauben, Ersatzkappen und Zentrierung für Analogstick	USB-Kabel, Handbuch (deutsch, englisch), Griffverhöhung, zwei Sechskantschraubendreher
Messergebnisse und Bewertungen		
Tastenauslösepunkt	0,4 mm	1,7 mm
Auslösekraft Tasten	0,9 N	0,45 N
Verarbeitung	○	⊕⊕
Ausstattung	⊕	⊕
Ergonomie	⊕	⊕
Preis	215 €, Linkshänderversion 226 €	190 €, Linkshänderversion in Vorbereitung
¹ Herstellerangabe	✓ vorhanden	— nicht vorhanden
⊕⊕ sehr gut	⊕ gut	○ zufriedenstellend
⊖ schlecht	⊖⊖ sehr schlecht	



Der Azerox Cyborg nutzt für seine Fingertasten Omron-Switches mit hoher Auslösekraft und mit 0,4 Millimetern sehr kurzem Schaltweg – typisch für Maustasten.



MIT **Mac & i** IMMER AM BALL

2× Mac & i mit 35 % Rabatt testen!

Mac & i – Das Magazin rund um Apple

- Tipps & Praxiswissen
- Hard- und Softwaretests
- Reports und Hintergründe

Für nur **16,80 €** statt **25,80 €*** (Preis in Deutschland)



+ Geschenk nach Wahl
z. B. Kabelbox mit Adaptern
oder Buch Apple Junkies



Jetzt bestellen:

www.mac-and-i.de/miniabo

✉ leserservice@heise.de ☎ 0541 80009 120

Mac & i. Das Apple-Magazin von c't.



Zum Diktat

Transkriptionen von Whisper V3 im Vergleich mit Online-Diensten

Whisper hat den Markt der Transkriptionsprogramme umgekrempelt. Inzwischen läuft es mit einer einfachen Bedienoberfläche lokal auf Rechnern und ohne Abo-Zwang. Wie schneidet es im Vergleich zu Spezialisten wie f4x und der Standard-Transkription von Word ab?

Von Hartmut Gieselmann,
Greta Friedrich und Stefan Wischner

Transkriptionsdienste findet man zu Hunderten im Netz. Automatisiert tippen sie diktierter Briefe und Interviews ab, untertiteln Videos und YouTube-Clips. Transkriptionsprogramme sind aber auch wichtige Werkzeuge für Abhördienste. Wenn sie Gespräche automatisch fehlerfrei aufschreiben und Sprecher zuordnen, erleichtern sie flächendeckende Überwachungen. Denn im Vergleich zu Audioaufzeichnungen lassen sich transkribierte Texte viel einfacher und schneller nach Stichworten durchsuchen.

Auf diese zweischneidige Möglichkeit der „dualen Nutzung“ weist nicht zuletzt

der KI-Entwickler OpenAI hin. Die Firma hat Ende 2023 die neueste Version V3 ihrer offenen und freien Transkriptionssoftware Whisper auf den Open-Source-Plattformen Hugging Face und GitHub veröffentlicht. Wie man das Kommandozeilen-Tool unter Windows, macOS und Linux benutzt, haben wir in [1] erklärt. Es kann sowohl lokal laufen als auch über die Programmierschnittstelle von OpenAI auf deren Server zugreifen. Dazu bieten diverse Anbieter verschiedene Bedienoberflächen an. Besonders spannend ist „Whisper Transcription“ von Good Snooze (auch als MacWhisper bekannt), das auf Macs kom-

plett lokal transkribiert und keine Abogebühren verlangt, weshalb wir es hier exemplarisch genauer untersucht haben. Die Transkriptionsleistung ist mit anderen Whisper-Apps vergleichbar.

In diesem Test tritt Whisper gegen einen der besten deutschsprachigen Dienste namens f4x Spracherkennung an, der im Vergleichstest vor zwei Jahren mit der höchsten Erkennungsrate glänzte [2]. Dritter im Bunde ist die Textverarbeitung Word, die inzwischen auch gesprochene Texte transkribiert. In den Textkästen ab Seite 94 erläutern wir die Benutzeroberflächen und Funktionen der Programme.

Verständnisfragen

Die drei Programme sind kinderleicht und ohne Kommandozeilenkenntnisse zu bedienen. Allen dreien übergibt man eine Audio- oder Videodatei und erhält kurz darauf eine Textdatei mit den erkannten Sätzen. Whisper Transcription arbeitet sie auf dem lokalen Rechner durch, f4x und Word schicken die Aufnahmen an Server, deren Standort von Abo und Dienst abhängt. Mehr dazu gleich.

Im Test sollten die Dienste und Apps zehn Aufnahmen transkribieren, darunter Interviews, Telefonate, Dialoge und Gesprächsrunden auf Deutsch und Englisch sowie in Schweizerdeutsch. Um zu testen, wie die Programme mit schlechten Aufnahmen zurechtkommen, haben wir einen Rauschteppich darunter gelegt, der kaum hörbar beginnt und gegen Ende immer lauter wird, bis selbst Menschen die Sprecher nicht mehr verstehen.

Eingeflüstert

Whisper Transcription liefert nur den reinen Text, Zeitmarken blendet das Programm auf Wunsch in einer alternativen Segmentansicht ein. f4x und Word schreiben zusätzliche Zeitmarken in den transkribierten Text und versuchen außerdem, einzelne Sprecher automatisch zuzuordnen. Das funktioniert aber nicht zuverlässig: Im Test kam es vor, dass ein Monolog mehreren Sprechern zugeordnet wurde oder in einer Gesprächsrunde falsche Sprecherwechsel erkannt oder Zwischenrufe überhört wurden. Solange Sprecher nicht zuverlässig erkannt werden, ist es einfacher, die Erkennung ganz abzuschalten und den Text manuell verschiedenen Personen zuzuordnen.

Im Gegensatz zu anderen Transkriptionsprogrammen basiert Whisper auf einem Transformer-Modell, das laut Her-

c't kompakt

- Audioaufnahmen lassen sich automatisiert transkribieren. Das macht nicht nur Stenotypisten überflüssig, sondern hilft auch Geheimdiensten.
- Selbst bei niedrigen maschinellen Fehlerquoten können sich fatale Missverständnisse einschleichen.
- Brisante Aufnahmen mit hohen Datenschutzansprüchen sollten Sie nur lokal auf Ihrem Rechner transkribieren.

stellerangaben mit 680.000 Stunden transkribierter Aufnahmen in verschiedenen Sprachen trainiert wurde, zwei Drittel davon in Englisch. Dazu sammelten die Entwickler Aufnahmen aus verschiedenen Quellen und filterten schlechte Transkriptionen nach automatisierten Regeln heraus.

Das Ergebnis: Whisper reagiert mit seinen beiden großen Modellen sehr robust und tippt auch bei schlechter Aufnahmequalität und Aussprache noch den richtigen Text, wo f4x schon die Waffen streckt. Wenn sich Whisper allerdings irrt, kann es Zusammenhänge in Halbsätzen verdrehen. Die Ergebnisse sind vergleichbar mit generativen Sprachmodellen: Sie liefern oft korrekte Informationen und liegen unvermittelt völlig daneben.

Maschinelle Missverständnisse

Die Genauigkeit von Spracherkennungsprogrammen messen Forscher mit der sogenannten Wortfehlerrate (Word Error Rate, WER). Sie gibt in Prozent an, wie viele der gesprochenen Wörter falsch erkannt wurden. Wir haben die Fehlerraten der drei Programme in verschiedene Gesprächskategorien in der Tabelle auf Seite 95 miteinander verglichen (bis sie aufgrund des Rauschens nur noch Kauderwelsch notierten). Bestenfalls erreicht f4x bei deutschen Interviews eine Fehlerrate von unter einem Prozent.

Whisper macht mit seinem großen V3-Modell mit etwa drei Prozent zwar etwas mehr Fehler, behält diese Leistung aber auch bei schlechten Aufnahmen, undeutlichen Sprechern oder Dialekten bei. Je nach Aufnahme hatte mal das V3-Modell und mal das ältere große Whisper-Modell (Large genannt) leicht die Nase vorn, ohne dass wir besondere Abhängigkeiten

erkennen konnten. Beide erzielen eine geringere Fehlerquote, als viele Menschen bei einer manuellen Transkription erreichen würden.

Allerdings sagt die Fehlerquote wenig darüber aus, wie gravierend und zum Teil sinnentstellend diese Fehler sein können. Denn es macht einen Unterschied, ob ein Programm nur eine Wortendung falsch versteht oder einen ganz anderen Sinnzusammenhang heraushört. Ein Mensch würde diese Fehler sofort bemerken, ein Programm nicht.

Bestes Beispiel ist eine Passage aus einem Interview mit Jean-Michel Jarre. Der Musiker erklärte auf Englisch mit französischem Akzent, dass er Arrangements wie ein Maler auf einer Leinwand platziert. Doch statt des englischen Wortes „canvas“ (Leinwand) verstand Whisper jedes Mal „Cannabis“ – egal, welches Modell wir einsetzten.

Ein weiteres Problem sind Eigennamen, die von den Transkriptionsprogrammen oft falsch verstanden werden. Statt „Dieter Bohlen“ notierte Whisper zum Beispiel „die Tauboen“ und aus „Maggi Fix“ wurde „Maggi-Pizza“. Menschen fallen solche Unsinnigkeiten sofort auf. Wer sich aber nur auf die maschinelle Transkription verlässt, liest am Ende eine verdrehte Geschichte. Besonders problematisch ist der Einsatz bei Abhörmaßnahmen, wo durch solche Missverständnisse schnell Unschuldige in Verdacht geraten können.

Immerhin haben die Entwickler von Whisper Transcription das Verhalten von Whisper leicht verbessert, indem sie manche doppelt transkribierte Sätze herausfiltern – eine lästige Nebenwirkung der Transformer-Engine. Auch Doppelungen von Wörtern oder Pausen, in denen der Sprecher über die Wahl seiner Worte nachdenkt, werden aussortiert. Die transkribierten Sätze lesen sich dann flüssiger als die tatsächlich gesprochenen Worte. f4x bleibt enger am Original, was etwa bei qualitativen Interviews in der Sozialforschung von Bedeutung sein kann.

Whisper textet auch bei verrauschten Aufnahmen munter weiter, selbst wenn es nur Kokolores ist und sein Modell nichts mehr richtig zuordnet. f4x bricht vorher ab und produziert dadurch weniger Fehler. Die Diktatfunktion von Word ist in allen Bereichen weit abgeschlagen. Sie schert sich nicht um Satzbau und Rechtschreibung, was die Nachbearbeitung sehr aufwendig macht.



Whisper Transcription / MacWhisper

Das Programm verwendet die freien Transkriptionsmodelle von Whisper und läuft lokal auf Macs. Inzwischen unterstützt es auch die Metal-Engine, wodurch es auf M-Prozessoren etwa zwei- bis dreimal schneller arbeitet als auf x86-Prozessoren. Im Test transkribierte es auf einem M2 Pro mit dem großen V3-Modell in fünffacher Echtzeit.

Die Pro-Version unterstützt auch Batch-Jobs und direkte Aufnahmen über die Mac-Audio-Engine. Die Software transkribiert im Anschluss und nicht in Echtzeit während der Aufnahme. Das kleine Modell der kostenlosen Version war besser als Word. Im Vergleich zur Pro-Version reagierte es empfindlicher auf schlechte Aussprache und Rauschen.

Das große Modell V3 verstand auch verrauschte oder schwierige Dialekte und kam auch bei mehreren Sprechern hinterher, ohne die Sätze jedoch zuzuordnen. Wenn es sich verhörte, was im Test vier- bis fünfmal pro Minute vorkam, dann passten gleich mehrere Worte oder ganze Halbsätze nicht. Die Transkriptionen sollte man daher manuell prüfen.

Die getestete Version 7.9 mit dem kleinen Basismodell (74 Millionen Parameter) ist kostenlos für macOS erhältlich. Die Pro-Version mit zwei großen Modellen (Large V3) mit jeweils etwa 1,5 Milliarden Parametern kostet über den Apple Store per In-App-Kauf einmalig 44 Euro oder 8 Euro pro Monat. Auf der Herstellerseite ist das Programm auch als „MacWhisper“ für rund 35 Euro erhältlich.

- 👆 lokal, schnell und zuverlässig
- 👆 versteht schlechte Aufnahmen
- 👇 irrt bei manchen Halbsätzen

Preis: kostenlos bis 44 Euro



f4x Spracherkennung 2024

Der deutsche Transkriptionsdienst f4x läuft im Browser. Nutzer laden unter audiotranskription.de/f4x Audio- oder Videodateien hoch und wählen aus über 40 Sprachen aus. Unter „Erweiterte Optionen“ legen sie Regeln für Zeitmarken und Pausen fest und tragen Fachbegriffe in eine Wortliste ein.

Im Test erreichte f4x etwa die acht- bis zehnfache Echtzeitgeschwindigkeit. Hochgeladene Audiodateien löscht f4x nach eigenen Angaben unmittelbar nach der Transkription und hält die Texte nach dem Download (als .docx, .rtf oder .srt) für kurze Zeit vor.

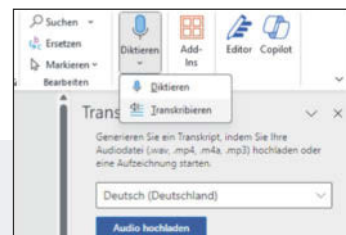
Gegenüber dem sehr guten Ergebnis im Vergleichstest von 2022 hat f4x an Geschwindigkeit und Erkennungsrate noch weiter zugelegt. Bei deutschen Interviews mit guter Aufnahmequalität schnitt f4x deutlich besser ab als das große V3-Modell von Whisper.

In Schwierigkeiten geriet f4x allerdings bei verrauschten Aufnahmen, wenn die Sprecher durcheinander, Englisch oder einen Dialekt sprachen. Die Fehlerquote stieg dann deutlich über die der großen Whisper-Modelle an. Immerhin bricht f4x bei verrauschten Aufnahmen eher ab, als dass es Quatsch transkribiert.

Nutzer erhalten einmalig 60 Freiminuten. Zwei Stunden kosten 33 Euro, fünf Stunden 55 Euro, das Maximum von 200 Stunden gibt es für 1555 Euro. Studenten zahlen weniger. Laut Hersteller läuft f4x DSGVO-konform auf Servern von Hetzner in Deutschland und verzichtet auf Tracker von Google und Facebook.

- 👆 sehr wenig Fehler bei gutem Ton
- 👇 stolpert über schlechten Ton
- 👇 Online-Dienst mit Zeitkosten

Preis: 1 Stunde kostenlos, danach circa 6 bis 16,50 Euro/Stunde



Microsoft Word

Die Transkriptionsfunktion steht Abonnenten von Microsoft 365 in Word für Windows und in den Browserversionen unter Chrome und Edge zur Verfügung. Das Abo für Microsoft 365 kostet Privatanwender ab 60 Euro pro Jahr. Ein Zeit- oder Mengenlimit gibt es nicht, Microsoft behält sich jedoch vor, das Kontingent in Zukunft zu begrenzen.

Der Befehl „Transkribieren“ versteckt sich in einem Menü hinter dem Button „Diktieren“. Dort kann man „Audio hochladen“ oder eine „Aufnahme starten“. Die Sprache wählt man manuell aus 90 Einträgen.

Nach dem Hochladen in Microsofts Azure-Cloud benötigte der Online-Dienst etwa 30 Sekunden pro Audio-Minute, bis der transkribierte Text in der Sidebar erschien, unterteilt nach den erkannten Sprechern und inklusive Zeitstempel. Zur Kontrolle kann man über eine Medienwiedergabeleiste die Abspielgeschwindigkeit der Aufnahme verändern und die synchron hervorgehobenen Textteile überprüfen. Über ein Aufklappenmenü fügt man den Text zum aktiven Dokument hinzu.

Die Erkennungsleistung war jedoch gering: Die Transkription strotzte vor Interpunktions-, Groß- und Kleinschreibfehlern. Immer wieder brachen Sätze abrupt ab und einzelne Wörter wurden durch Unsinn ersetzt. Die Transkription ist allenfalls bei klar gesprochenen Monologen eine Arbeitserleichterung. Aber auch hier bleibt sie weit hinter der kostenlosen Version von Whisper Transcription zurück.

- 👆 in Microsoft 365 enthalten
- 👇 langsam und fehlerträchtig
- 👇 lädt Aufnahmen in die Cloud

Preis: ab 60 Euro pro Jahr (Microsoft 365)

Datenschutz

Bei der Transkription eines YouTube-Videos mag der Inhalt ohnehin nicht geheim sein, bei einem investigativen Interview oder der Aufzeichnung eines firmeninternen Meetings kann dies schon anders aussehen. Das große Problem der vielen Online-Transkriptionsdienste ist daher der Datenschutz. Man muss dem Anbieter vertrauen, dass er die Aufnahme des transkribierten Textes nicht für andere Zwecke verwendet oder gar weitergibt.

Microsoft lädt die Audiodateien für die Transkription in die Azure-Cloud. Je nach Abomodell für Privat- oder Geschäftskunden können die Server in Deutschland oder anderswo stehen. Ähnliches gilt für OpenAI, das Server-Transkriptionen mit Whisper über seine Programmierschnittstelle anbietet. Viele Transkriptionsprogramme bestehen nur aus einer Benutzeroberfläche und übertragen die Audiodaten zur Transkription an die Server von OpenAI in den USA.

Formal ist die Übermittlung personenbezogener Daten wie Audioaufzeichnungen in die USA derzeit legal und DSGVO-konform, wenn sich die Anbieter zum seit Juli 2023 gültigen EU-US Data Privacy Framework bekennen. Doch im Zweifelsfall können amerikanische Geheimdienste auf diese Daten zugreifen. Max Schrems von der österreichischen Datenschutzorganisation NOYB will gegen das aktuelle Abkommen klagen, da

er keine ausreichenden Verbesserungen gegenüber dem von Richtern kassierten Vorgängerabkommen „Privacy Shield“ erkennt.

Sicherer sind in Deutschland ansässige Unternehmen wie der Anbieter von f4x, die Dr. Dresing & Pehl GmbH aus Marburg. Sie versprechen, die Daten auf Servern von Hetzner in Deutschland zu verarbeiten. Außerdem bieten sie zusätzliche Geheimhaltungsvereinbarungen an. Letztlich muss man aber auch ihnen vertrauen. Wer seine Aufzeichnungen nicht aus der Hand geben will oder darf, kommt daher an lokalen Lösungen wie Whisper Transcription nicht vorbei, die den gesamten Text lokal ohne Internetverbindung transkribieren.

Fazit

Die Tage der Online-Transkriptionen mit Abonnements oder Volumenabrechnungen sind gezählt. Das große Modell V3 von Whisper ist äußerst robust und transkribiert selbst verrauschte, schwer verständliche Aufnahmen mit vergleichsweise geringer Fehlerquote. Das gilt nicht nur für Englisch, sondern auch für Deutsch und schwer verständliche Dialekte. Mit Whisper verstanden Sprachassistenten auch in schwierigen Situationen: Nervige Rückfragen von Siri, Alexa & Co. könnten damit bald der Vergangenheit angehören. Nicht zuletzt sammelt OpenAI über die Spracherkennung seiner mobilen App für

ChatGPT laufend neues Trainingsmaterial.

Die Mac-Implementierung von Whisper zeigt zudem, dass solche Transkriptionen mittlerweile auch auf lokalen Rechnern mit hoher Geschwindigkeit laufen. Da OpenAI die Modelle freigegeben hat, werden weitere Apps auf anderen Betriebssystemen folgen. Bei deutschen Interviews mit gut verständlichen Aufnahmen hat der Online-Dienst von f4x noch einen kleinen Vorsprung, aber die Luft ist sehr dünn geworden.

Allerdings haben alle Programme Probleme mit der korrekten Zuordnung von mehreren Sprechern, vor allem, wenn diese dasselbe Geschlecht haben und durcheinanderreden. Das ist insofern beruhigend, als es eine vollautomatische Massenüberwachung erschwert. Ohne manuelle Nachbearbeitung können solche Transkriptionen in die Irre führen. Nichtsdestotrotz spart Whisper bei professionellen Transkriptionen enorm viel Zeit, sei es um Untertitel für ein Video zu erstellen oder Interviews zu verschriftlichen.

(hag@ct.de) 

Literatur

- [1] Immo Junghärtchen, Spracherkennung im Eigenbau, Whisper wandelt Gesprochenes in Text um, c't 14/2023, S. 140
- [2] Andre Kramer, Diktatmaschinen, Transkriptionsdienste, Audioaufnahmen in Text wandeln, c't 17/2021, S. 110

Transkriptions-Apps und -Dienste

Name	f4x Spracherkennung 2024	MacWhisper (Whisper Transcription)	Word
Anbieter	Dr. Dresing & Pehl GmbH	Good Snooze	Microsoft
Webseite	www.audiotranskription.de	goodsnooze.gumroad.com	www.office.com
Betriebssysteme	Browser	macOS	Windows, Browser
Transkription	online	offline	online
Sprachen	47 Sprachen	etwa 100 Sprachen	90 Sprachen und Dialekte
Aufnahmeformate	WAV, MP3, AAC, OGG, MPEG, M4A, MP4, FLAC	WAV, MP3, M4A, OGG, OPUS, MOV, MP4	WAV, MP3, MP4, M4A
Sprechermarkierung	automatisch (fehlerhaft)	nur manuell	automatisch (fehlerhaft)
Zeitmarken	✓	optional	✓
Abhörkontrolle	—	mit variablem Tempo	mit variablem Tempo
Transkriptionssauer	8tel bis 10tel der Laufzeit	etwa 5tel der Laufzeit ¹	halbe Laufzeit
Fehlerraten (Word Error Rate, WER)			
Interview Deutsch	< 1 %	Free: 4 %, Pro: 3 %	7 %
Interview Englisch	4 %	Free: 10 %, Pro: 2 %	8 %
Schnellsprecher Deutsch	9 %	Free: 17 %, Pro: 3 %	19 %
Gruppengespräch Deutsch	6 %	Free: 8 %, Pro: 3 %	14 %
Schweizerdeutsch	17 %	Free: 28 % Pro: 8 %	34 %
Bewertung			
Qualität	⊕	Free: ○, Pro: ⊕⊕	⊖
Preise	1 Stunde kostenlos, circa 6 bis 16,50 €/Stunde	Free: kostenlos, Pro: 37 US-Dollar (Webseite) / 44 Euro (App Store) oder 8 €/Monat	ab 60 €/Jahr (Privatnutzer, in Microsoft 365 enthalten)

¹ getestet auf einem MacBook Pro mit M2 Pro

✓ vorhanden — nicht vorhanden ⊕⊕ sehr gut ⊕ gut ○ befriedigend ⊖ schlecht, ⊖⊖ sehr schlecht

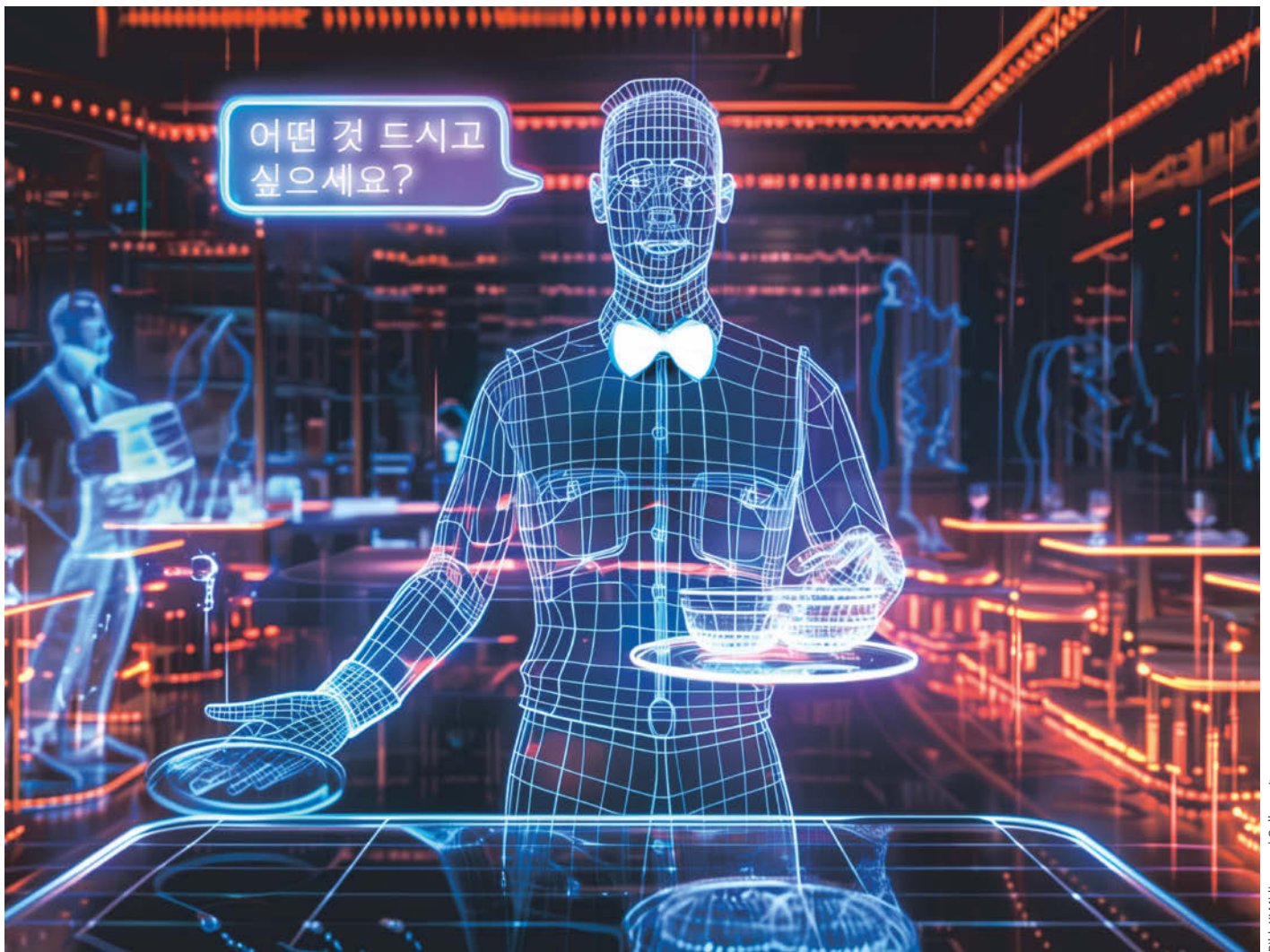


Bild: KI Midjourney | Collage ct

Ihr Gespräch ist angerichtet

Was leisten KI-Sprechtrainer?

Ein Gespräch in einer neuen Sprache zu führen, ist für Fremdsprachenschüler anfangs eine Herausforderung. Helfen sollen KI-Sprechtrainer, mit denen sich Konversationen wie mit einem richtigen Menschen führen lassen, aber ganz ohne Angst, sich zu blamieren.

Von Nico Jurran

Apps wie Babbel, Busuu und Duolingo stehen beim Erlernen von Sprachen hoch im Kurs. Doch egal, ob man diese Art des Selbststudiums sinnvoll findet, ist es heute Konsens, dass damit kein richtiges Sprechtraining möglich ist. Die Gründe behandelte c't in [1] ausführlich, herunterbrechen lassen sie sich aber auf die Erkenntnis: „Sprechen lernt man nur durch Sprechen.“

Insofern ist nachvollziehbar, dass Babbel seit einiger Zeit mit „Babbel Live“ parallel einen Dienst für Onlinegruppenunterricht mit echten Lehrkräften betreibt. Andere Möglichkeiten für Sprechtraining umfassen unter anderem Gruppenkurse in Präsenz, etwa an einer Volkshochschule, Sprachtandems mit Muttersprachlern oder Onlineeinzelunterricht, den Dienste wie

iTalki und Preply vermitteln. Gegenüber dem Lernen mit Apps ist man damit aber zeitlich weniger flexibel. Der Frontalunterricht in einer Einzelstunde ist zudem nicht jedermanns Sache, im Gruppenunterricht kommt man wiederum eventuell nicht oft genug zum Sprechen.

So bleibt die Situation paradox: Einerseits sollen Schüler in der Zielsprache reden, um die nötige Kompetenz aufzubauen, andererseits scheuen sich viele Sprachschüler genau davor, weil ihre ersten Versuche, die passenden Vokabeln unter Zeitdruck aus ihrem Gedächtnis zu kramen, sie zu grammatikalisch korrekten Sätzen zusammenzubauen und diese am Ende korrekt auszusprechen, in kompletten Blackouts endeten.

Realitätscheck

Ende vergangenen Jahres schien Babbel dieses Paradoxon endlich aufgelöst zu haben: Das Unternehmen kündigte an, man könne mit seiner App künftig mithilfe von KI das Sprechen in einem „sicheren Raum“ trainieren und verbessern und das, wann und sooft man wolle und ohne die Angst, sich vor anderen zu blamieren.

Doch so vielversprechend die Ankündigung klang, so ernüchternd war das, was Babbel unter dem Begriff „Alltagsgespräche“ lieferte: vorgefertigte Dialoge zu einer Reihe von Situationen wie „Einen Nachbarn begrüßen“ oder „Small Talk mit einer Reisebekanntschaft“, bei denen man die Sätze eines Gesprächspartners nachspricht.

Das ist am ehesten mit Vorleseübungen in Lehrbüchern zur Kontrolle der Aussprache und dem Auswendiglernen typischer Phrasen vergleichbar, hat mit freier Konversation jedoch wenig zu tun: Nimmt im realen Leben der Gesprächsverlauf eine Wendung, in der die vorgegebenen Sätze nicht passen, sind die meisten Schüler am Ende genauso aufgeschmissen wie vorher.

Babbels Umsetzung enttäuscht nicht zuletzt jeden, der schon einmal einen Textchat mit einer generativen KI geführt hat. Mit ChatGPT & Co. kann man sich nicht nur wie mit einem Menschen unterhalten, die KI-Chats beherrschen auch zahllose Sprachen, zwischen denen sie nahtlos wechseln können. Mit einem simplen Prompt wie „Lass uns einen Dialog auf Französisch führen“ bringt man eine Konversation über frei wählbare Themen in einer Fremdsprache in Gang. Die KI hält sie vor allem mit passenden Nachfragen von sich aus am Laufen. Darüber hinaus sind die Gespräche nicht mehr auf Textchats beschränkt. Die offizielle ChatGPT-App bietet mittlerweile auch für das kostenlose KI-Modell einen Voice-Chat-Modus. Am Rechner lässt sich der Chatbot wiederum mit Browsererweiterungen und geeigneten Befehlen leicht zum KI-Sprechtrainer aufrüsten. Wer es selbst ausprobieren möchte, sollte einen Blick auf den Artikel „KI-Gesprächspartner im Eigenbau“ auf Seite 104 in diesem Heft werfen.

Im Ergebnis hat man praktisch das, was sich viele bei Babbels Ankündigung vorgestellt haben: Man wiederholt keine vorgegebenen Sätze, sondern redet einfach drauflos. Und auch das angesprochene Üben von Alltagsgesprächen ist kein Problem: Man muss die KI nur auffordern, in einem Rollenspiel eine bestimmte Rolle

zu übernehmen. Versteht man etwas nicht oder möchte etwas erklärt haben, fragt man einfach nach.

Neue Konkurrenten

ChatGPT war aber nur der Anfang, mittlerweile finden sich eine Reihe kommerzieller KI-Sprechtrainer in Form von Apps und Webdiensten auf dem Markt. Auf alle einzeln einzugehen, würde den Rahmen sprengen. Wir haben uns daher auf Tools konzentriert, die nicht nur auf eine Zielsprache (meist Englisch) ausgerichtet sind, sondern eine Vielzahl von Sprachen unterstützen. So sollten KI-Gesprächspartner für die hierzulande beliebten Sprachen Englisch, Spanisch, Französisch, Italienisch, Chinesisch (Mandarin), Koreanisch, Japanisch und eben Deutsch bereitstehen. Zwischen den Sprachen können Nutzer beliebig wechseln, falls sie etwa Japanisch neu lernen, aber ab und an auch ihr Schulenglisch auffrischen möchten.

Ebenso wichtig war uns, dass die KI-Sprechtrainer unter möglichst vielen Betriebssystemen verfügbar sind. Am Ende wählten wir daher „TalkPal“, „Teacher AI“ (irritierenderweise gehostet unter www.yourteacher.ai) und „Univerbal“ aus, auf die wir in eigenen Textkästen und in der Tabelle auf Seite 103 näher eingehen. Alle drei lassen sich im Browser auf jedem Rechner mit Mikrofon und Lautsprecher beziehungsweise Headset nutzen. TalkPal und Univerbal gibt es auch als Smartphones-Apps, bei Teacher AI sind diese angekündigt. Der Dienst läuft aber auch schon jetzt im mobilen Browser ordent-

lich. Auf andere KI-Sprechtrainer, bei denen uns während der Recherche Besonderheiten aufgefallen sind, gehen wir im Fließtext ein.

Von den großen Sprachlern-Apps reagierte bislang nur Duolingo auf den KI-Trend, und das auch nur sehr begrenzt. So bietet das Unternehmen in einigen englischsprachigen Ländern ein „Max“-Abo an, das einen KI-Sprechtrainer umfasst, der mittels ChatGPT 4.0 ins virtuelle Leben gerufen wurde. Nutzen lässt sich der derzeit aber nur für Englisch als Ausgangs- und Französisch oder Spanisch als Zielsprache.

Kein billiges Vergnügen

Was auffällt: Während man Duolingo in der Basisversion weiter kostenlos (werbefinanziert) nutzen kann, zahlt man in Großbritannien für das Maxabo monatlich umgerechnet rund 23,40 Euro, in den USA sogar 27,50 Euro. Denn Open AI verlangt von den Betreibern der Dienste Geld, wenn sie GPT nutzen wollen.

Von den getesteten Diensten kommt Teacher AI mit rund 25 Euro für einen Monat preislich an Max heran. Bindet man sich für ein Jahr, sinkt der Preis jedoch bis auf die Hälfte. Für Univerbal muss man 15 Euro im Monat hinlegen, im Jahresabo sind es monatlich 5 Euro weniger. Am billigsten ist TalkPal: Ein Monat kostet 10 Euro, wobei sich der Preis ebenfalls halbiert, wenn man ein Jahresabo abschließt.

TalkPal ist zudem der einzige Dienst mit kostenlosem Basisabo. Das ist auf zehn Minuten freien Chat pro Tag beschränkt und nutzt unnatürlichere Stimmen, ver-

In Babbels „Alltagsgesprächen“ spricht man nur vorgegebene Sätze nach. Konkurrent Duolingo hat seine Sprachlern-App währenddessen in einigen englischsprachigen Ländern mit einem Generative-KI-Sprachtrainer ausgestattet.



Bild: Duolingo

mittelt aber einen ersten Eindruck von den Funktionen. Univerbal gewährt eine siebentägige Testphase. Teacher AI bietet einen solchen Probezeitraum unter Hinweis auf die Kosten nicht an.

Sprechen um des Sprechens willen

Der KI-Sprechtrainer ergänzt bei Duolingo Max die Lern-App und löst diese nicht ab. Auch Teacher AI weist auf seiner Seite darauf hin, dass sein Angebot einen strukturierten Sprachkurs nicht ersetzt. Tatsächlich beschränkt sich der Dienst auf freie Chats; dass der Schüler geführt wird, ist nicht zu erkennen.

Heise-Redakteur Daniel Augustin ließ sich davon nicht beirren und bewies, dass man alleine mit Teacher AI und einem Onlinewörterbuch in nur einem Monat mit einer halben Stunde Übungszeit pro Tag seine Sprachkenntnisse deutlich verbessern kann. Am Ende konnte Augustin, der anfangs nur einige spanische Worte kannte, mit einem Muttersprachler ein einfaches Gespräch auf Spanisch führen, wie sein Video auf heise online (unter ct.de/yfvk) zeigt. Allerdings musste er sich selbst eine Struktur fürs Lernen und Üben schaffen und diese abarbeiten, was aufwendiger ist als das Lernen nach einem fertigen Konzept.

Ein übergeordnetes Konzept beziehungsweise einen Lehrplan bietet auch TalkPal nicht: Der Dienst hält zwar knapp 100 vorgefertigte Rollenspielszenarien bereit, in denen man etwa ein Taxi bestellen muss, ein Date hat, aus dem Job gefeuert wird oder sogar als Therapeut in einer post-apokalyptischen Welt einem Zombie bei einer existenziellen Krise hilft. Mehr als drei Schwierigkeitsstufen gibt es aber nicht; ein roter Faden lässt sich nicht erkennen.

Nur Univerbal erstellt individuelle Lehrpläne, weshalb das erste Gespräch in jeder Sprache stets ein Einstufungstest ist. Dabei ermittelt der Dienst das aktuelle Niveau des Schülers und generiert ab diesem Startpunkt ein Rollenspiel nach dem nächsten. Dabei erschließt er immer neue Themengebiete und steigert langsam den Schwierigkeitsgrad.

Sogar ein Modus für Nutzer ohne jegliche Sprecherfahrung ist verfügbar. In dem muss man als Schüler Sätze nachsprechen, die man sich erst einmal in zwei Geschwindigkeiten anhören kann. Nach dem ersten Versuch erfährt man, wie man sich geschlagen hat und erhält nötigenfalls eine zweite Chance, bevor es mit dem

nächsten Satz weitergeht. Koreanisch bekamen wir trotz eingblendeter Lautschrift so jedoch nicht in den Griff. Mit Italienisch lief es generell besser, jedoch sind die Sätze teilweise so lang, dass die Übungen schnell in Stress ausarten. Ein Lernerfolg ist damit unwahrscheinlich, die meisten Schüler dürften irgendwann frustriert abbrechen.

Lass uns reden

Doch wie sprechen die KI-Trainer selbst? Hier sticht Teacher AI positiv heraus, wo jeder virtuelle Lehrer eine individuelle Stimme hat und auch die Betonung der Wörter in der Regel überzeugt. Für einige Sprachen stehen sogar Sprecher mit Akzenten und Dialekten bereit, damit sich Schüler besser auf menschliche Gesprächspartner mit regionaler Aussprache einstellen können. Die Idee ist gut, von uns befragte Muttersprachler aus Argentinien, Peru und Österreich vermissten bei der Umsetzung aber oft typische regionale Merkmale, etwa hinsichtlich der Satzmelodie, der Grammatik oder des Vokabulars.

Ein gemischtes Bild ergibt sich bei Univerbal: Während etwa die Stimmen für Französisch und Spanisch noch recht ordentlich klingen, merkt man beispielsweise bei einigen KI-Sprechpartnern für Deutsch, Englisch und Russisch sofort, dass man es mit synthetischen Stimmen zu tun hat. Das ermüdet auf Dauer und

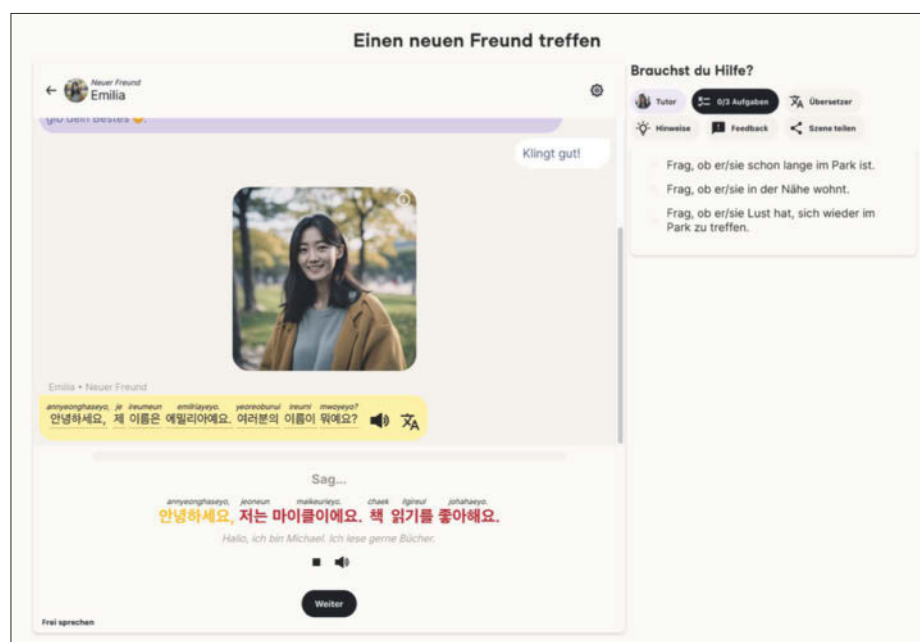
macht es schwerer, die korrekte Betonung eines Wortes zu erfassen.

TalkPal bietet für jede Sprache nur eine weibliche und eine männliche Stimme, beide sind jedoch gelungen. Dass es bei den Stimmen an Abwechslung mangelt, fällt im Modus „Characters“ auf, wo man Gespräche mit virtuellen Abbildern bekannter Persönlichkeiten führt. Dass Thor und Pinocchio gleich klingen, stört die Illusion. Besser macht es die Englisch-App „CallAnnie“, bei der verschiedene KI-Charakter unterschiedliche Stimmen haben, die häufig gut passen. CallAnnie zeigt auch, wohin die Reise gehen könnte: Sie bietet nicht nur einen Voice-Chat, sondern bringt die KI-Sprechtrainer als animierte Avatare auf den Schirm.

Verständnisvoll

Schüler können nur dann angemessen auf die Fragen und Ausführungen des KI-Gegenübers reagieren, wenn sie diese auch korrekt erfassen. Alle Dienste wiederholen daher die Ausgaben auf Knopfdruck und auch langsamer. Dabei fällt die Qualität der Stimmen aber noch stärker ins Gewicht: Klingt sie schon bei normaler Geschwindigkeit synthetisch, wird es bei verlangsamer Wiedergabe oft gruselig.

Zusätzlich geben die Dienste die Sätze in der Zielsprache in Textform auf dem Bildschirm aus, wobei TalkPal für Chinesisch und Japanisch jeweils verschiedene



Für User, die komplett neu in eine Sprache einsteigen und noch keinerlei Sprecherfahrung haben, bietet Univerbal einen speziellen Modus. Hier spricht man vorgegebene Sätze nach und füllt durch Anklicken vorgegebener Vokabeln Lückentexte.

heise +

ct

iX

Mac&i

Make:

MIT
Technology
Review
Das Magazin für Innovation von Heise

ct **Fotografie**

c't-Abonnenten
lesen bis zu
75%
günstiger

Das digitale Abo für IT und Technik.

Exklusives Angebot für c't-Abonnenten:
Sonderrabatt für Magazinabonnenten

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

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

heise.de/plus-testen

✉ leserservice@heise.de ☎ 0541 80009 120

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

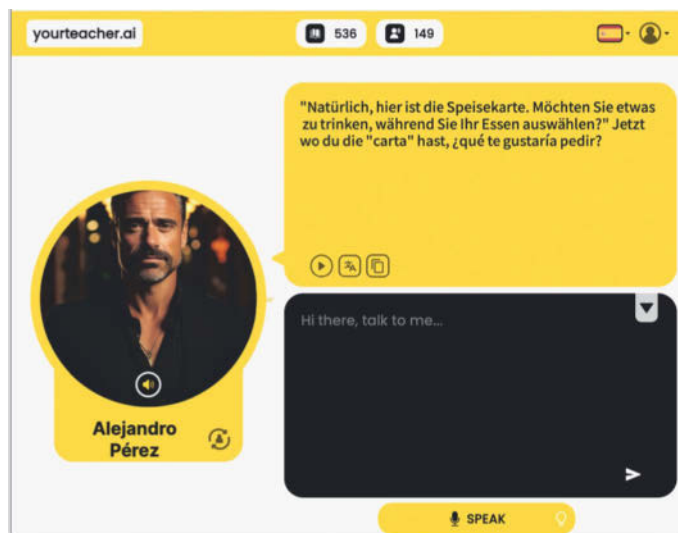
Schriftsysteme benutzt. Fortgeschrittene können bei dem Dienst zudem einen sogenannten „Call“ starten, ein simuliertes Telefongespräch mit dem KI-Trainer ohne Transkription.

Schließlich erhält man auf Befehl eine Übersetzung der transkribierten KI-Ausgabe in der Ausgangssprache, bei Teacher AI und Univerbal optional auch nur für einzelne Wörter. Fällt einem selbst eine Vokabel nicht ein, kann man bei Univerbal einen integrierten Übersetzer nutzen. Bei Teacher AI und TalkPal lassen sich zudem Nachfragen mündlich in der Ausgangssprache zu stellen, bei Univerbal ist dies hingegen nur schriftlich möglich.

Korrektur erwünscht

Ziel jedes Fremdsprachenunterrichts ist es, die Schüler in die Lage zu versetzen, grammatikalisch und orthografisch korrekte Sätze zu bilden. Somit fällt dem Lehrer – ob real oder virtuell – die Aufgabe zu, auf Fehler hinzuweisen und den korrekten Satz zu liefern. Allerdings muss der KI-Lehrer wie sein menschlicher Gegenpart die Konversation zugleich am Laufen halten. Die Entwickler der KI-Sprechtrainer setzen unterschiedlich an, beide Aspekte unter einen Hut zu bringen. So geht etwa Teacher AI direkt auf Fehler ein und fordert den Schüler auf, den betreffenden

Teacher AI arbeitet bilingual, was bedeutet, dass der Dienst auch mündliche Hinweise und Korrekturen in der Ausgangssprache ausgibt, wenn es nötig erscheint. Alle KI-Nachrichten in der Zielsprache lassen sich auch übersetzen.



Satz zu wiederholen. Wer dieser Bitte nachkommt, bekommt ein Lob, wenn er sich verbessert. Daneben spuckt der KI-Lehrer aber auch immer eine Anschlussfrage aus. Wer keine Lust hat, sich zu korrigieren, führt das Gespräch einfach fort.

TalkPal und Univerbal zeigen hingegen neben der Transkription des vom Schüler gesprochenen Satzes an, ob dieser korrekt war. Ist dies nicht der Fall, kann man sich mit einem Fingertipp ein Feedback abholen. Die KI-Lehrer selbst geht

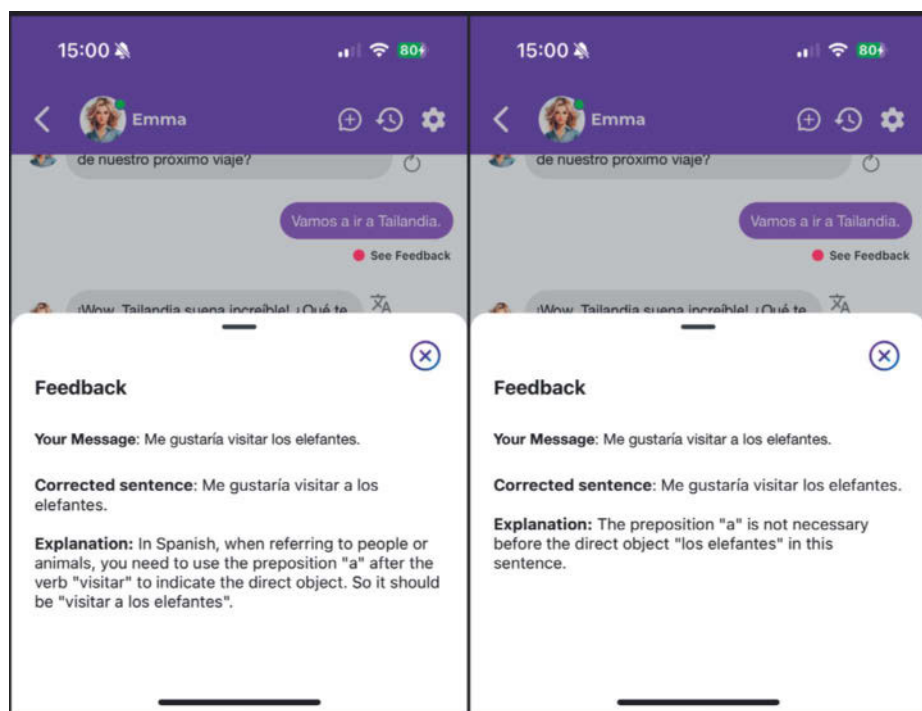
indes über fehlerhafte Sätze in der Regel hinweg und treibt das Gespräch mit einer neuen Frage voran.

Guter Zuhörer gesucht

Um die Eingaben des Schülers korrekt zu verarbeiten, muss die KI sie erst einmal fehlerfrei erfassen. Wir kontrollierten dies mithilfe eines Mac mit dem USB-Audio-interface Yamaha ZG01 samt Headset YH-G01, das Studioqualität liefert. Als Browser nutzten wir jeweils Google Chrome. Was sofort auffiel: TalkPal und Teacher AI fordern bei der Eingabe zum Drücken einer Taste auf, um zu sprechen („Push to Talk“) anstatt zu versuchen, selbst zu erkennen, wann der Schüler zu Ende gesprochen hat. Das ist nachvollziehbar, da gerade Einsteiger beim Sprechen längere Pausen machen, um etwa die passende Vokabel aus dem Hirn zu kramen. Eine Automatik glaubt dann fälschlicherweise, die Eingabe sei bereits beendet.

Nur Univerbal benutzt eine Halbautomatik: Eingaben sollen automatisch erkannt werden, das Absenden der Mitteilung erfolgt aber weiterhin manuell. Im Test funktionierte dies jedoch oftmals schlecht, tatsächlich ist Push to Talk die bessere Variante. Auch dann muss man mit der Eingabe warten, bis der Dienst wirklich empfangsbereit ist, da er andernfalls Satzanfänge abschneidet.

TalkPal hatte im Test immer mal wieder Probleme, die Eingaben des Schülers zu transkribieren. Dann schrieb er beispielsweise ausgesprochene Worte groß und mahnte anschließend die fehlerhafte Groß- und Kleinschreibung an. Das ist nicht dramatisch, stört aber den Fluss der



Was denn nun? Im Test merkte TalkPal bei einem spanischen Satz an, dass ein „a“ fehlte (links). Wiederholten wir den Satz mit der Präposition, belehrte uns der Dienst, dass diese überflüssig sei (rechts).

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



Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur
nur 19,35 €

www.ix.de/testen



www.ix.de/testen



49 (0)541 800 09 120



leserservice@heise.de





TalkPal

Bei TalkPal kann man mithilfe der KI in über 60 Sprachen sprechen, darunter sogar Walisisch und Maori. Akzente und Dialekte beherrscht der Dienst generell nicht, macht aber bei britischem und amerikanischem Englisch eine Ausnahme. Blöd: Man muss auf jeden Fall Englisch beherrschen, da sowohl die Oberfläche als auch die Korrekturen nur in dieser Sprache verfügbar sind.

Im Chat steht für jede Sprache je nur eine Frauenstimme bereit, eine männliche kommt bei Rollenspielen hinzu. Eben diese bilden auch einen Schwerpunkt; bis zum Redaktionsschluss war der Pool bereits auf knapp 100 Szenarien angewachsen. Alternativ stürzt man sich in eine von über dreißig vorgegebenen Debatten zu Themen wie der Viertagewoche. Dabei kann man die Pro- oder Contra-Seite frei wählen, die KI übernimmt jeweils die Gegenposition.

Als zusätzliche Features bietet TalkPal unter anderem einen „Photo Modus“, bei dem man Fotos schriftlich oder mündlich beschreiben muss. Die KI achtet dabei allerdings nicht auf den Inhalt der Beschreibung, sondern nur auf Rechtschreib- oder Grammatikfehler. Leider ist TalkPal selbst dabei nicht immer sattelfest.

- ↑ große Auswahl an Sprachen
- ↑ viele Rollenspiele, Debatten
- ↓ Korrekturen nur auf Englisch
- ↓ machte im Test einige Fehler

Preis pro Monat: kostenlos (nur Basisfunktionen) bis 9,99 Euro



Teacher AI

Teacher AI bietet für jede Sprache mindestens eine männliche und eine weibliche Stimme an, die insgesamt natürlicher klingen als bei den anderen getesteten Diensten. Im Testfeld gab es zudem nur hier „bilinguale Stimmen“, mit denen Schüler Erklärungen auch in ihrer eigenen Sprache in verständlicher Form erhalten sollten. Dies funktioniert je nach verwendeter Stimme allerdings unterschiedlich gut.

Von sich aus gibt es bei Teacher AI nur einen freien Chat, die KI kann mit dem User auf Zuruf aber auch Alltagssituationen in Rollenspielen üben. Dennoch dürften einigen Schülern nach einiger Zeit der rote Faden fehlen.

Positiv fiel auf, dass Teacher AI erfasst, welche Vokabeln Schüler und KI-Lehrer bislang verwendet haben (aktiver und passiver Wortschatz). Diese Listen lassen sich mithilfe der integrierten Übersetzungsfunktionen nutzen, um die Vokabeln noch einmal zu üben, durch Exportmöglichkeit auch mit externen Programmen.

Während des Tests gab es mehr und mehr Probleme mit dem Server, zeitweise war der Dienst gar nicht nutzbar. Der Betreiber hat reagiert: Bis die Probleme gelöst sind, werden keine neuen Kunden mehr angenommen.

- ↑ KI-Lehrer mit guten Stimmen
- ↑ Korrekturen bilingual
- ↓ keine vorgegebenen Rollenspiele
- ↓ QoS-Probleme in der Testphase

Preis pro Monat: 12,25 Euro bis 25 Euro



Univerbal

Univerbal, einst unter dem Namen „Quazel“ gestartet, liegt mit 22 Sprachen bei der Vielfalt zwar hinter TalkPal und Teacher AI, die beliebtesten sind aber vertreten. Zudem passt er als einziger Dienst im Feld seine Oberfläche der Ausgangssprache an. Nicht gefallen hat uns, dass manche Stimmen synthetisch klangen und die Spracheingabe mitunter hakte.

Heraus sticht Univerbal mit seiner klaren Struktur: Die Rollenspiele bauen aufeinander auf und sollen so auch die Sprachkenntnisse schrittweise verbessern. Alternativ lässt sich zwar auch eine Konversation zu einem beliebigen Thema starten, einen ganz freien Chat gibt es aber nicht: Die KI führt das Gespräch gleich wieder auf die gestellte Szene zurück.

Dass Univerbal in jedem Rollenspiel drei Themen vorgibt, die man als Schüler ansprechen soll, ist eine gute Idee. Die offenbar zufällig generierten Aufgaben liegen aber häufiger so neben der Spur, dass Gespräche eine eigenartige Wendung nehmen. Zudem klappt das automatische Abhaken der Punkte nur leidlich. Gut: Am Ende gibt es ein Feedback zum Gesprächsverlauf und man kann ein Transkript in PDF-Form anfordern.

- ↑ strukturierter Aufbau
- ↑ Oberfläche in Ausgangssprache
- ↓ kein freier Chat
- ↓ einige Stimmen klingen synthetisch

Preis pro Monat: 10 Euro bis 14,99 Euro

Konversation, da man als Schüler immer nachschaut, was man denn nun falsch gemacht hat.

Alles sollte stimmen

Eigentlich sollte es überflüssig sein zu sagen, dass die von der generativen KI gelieferten Sätze und Korrekturen korrekt sein müssen. Dass dies jedoch nicht selbstverständlich ist, zeigt Duolingos Blogbeitrag zur Einführung des Maxabos

(siehe ct.de/yfvk). Darin heißt es, dass man zwar monatelang eng mit OpenAI zusammengearbeitet habe, um GPT-4 für dieses Einsatzgebiet zu testen und zu trainieren, die Technik aber eben nie perfekt sei. Man werde daher die Arbeit fortsetzen, „bis es fast keine Fehler mehr gibt“.

Alle Grammatikregeln für jede Sprache zu prüfen, hätte den Rahmen jedes

Tests gesprengt. Wir fanden aber einen kniffligen Prüfpunkt, bei dem in einem Beispielsatz die spanische Präposition „a“ ausnahmsweise entfällt. Teacher AI korrigierte unseren Fehler korrekt und lieferte die exakte Begründung, während Univerbal diese Ausnahme nicht kannte und auf das „a“ bestand. Völlige Verwirrung lösten wir hingegen bei TalkPal aus: Der Dienst wies beide Satzvarianten als falsch

zurück, nur um dann die jeweils andere als korrekt zu präsentieren (siehe Screenshot auf S. 100).

Der Dienst patzte zudem bei Deutsch als Zielsprache mit komplizierten Sätzen des KI-Trainers immer mal wieder bei Satzstellungen, Deklinationen und beim Plural. Laut Duolingo kann man Fehler bei Max melden; das hätten wir uns auch bei TalkPal gewünscht.

Fazit

Die getesteten KI-Sprechtrainer können keinen strukturierten Sprachkurs ersetzen. Dies gilt klar für Teacher AI, der nicht einmal vorgefertigte Rollenspiele anbietet, aber nach unserer Einschätzung ebenso für TalkPal und Univerbal, auch wenn man letzterem Dienst eine nachvollzieh-

bare Struktur zusprechen muss, die das Zeug hat, die Kenntnisse der Schüler schrittweise zu verbessern. Dennoch raten wir, Univerbal zum Lernen der Grammatik zumindest mit einem Lehrbuch oder einer App zu ergänzen.

Derzeit muss man sagen, dass alle drei Diensten neben Stärken noch Defizite haben. So angenehm bei Teacher AI die Gespräche und so sinnvoll die Korrekturen sind, würden wir uns trotzdem etwas Struktur wünschen. TalkPal punktet mit vielen guten Ideen rund um Rollenspiele, schwächelt aber bei der Umsetzung. Vor allem aber zeigt der Dienst zu viele Makel bei den Korrekturen. Univerbal sollte an der Eingabe und den Stimmen nacharbeiten. Und so schön die Rollenspiele sind, hätte uns für mehr Ab-

wechslung auch frei sprechen zu können besser gefallen.

Bei aller Kritik: KI-Sprechtrainer sind schon jetzt eine sinnvolle Ergänzung für alle, die bereits Kenntnisse der Zielsprache erworben haben und nun ins Sprechen kommen wollen. Und das klappt gut, weil man über die Dienste zu beliebigen Zeiten auf einen virtuellen Gesprächspartner zurückgreifen und ohne Angst vor einer Blamage munter drauflos reden kann. (nij@ct.de) **ct**

Literatur

- [1] Nico Jurrán, Sprachfindung, Wieso viele mit Sprachlern-Apps scheitern – und wie es besser geht, c't 1/2023, S. 60

Video zum Selbstversuch: ct.de/yfvk

KI-Sprechtrainer

Name	TalkPal	Teacher AI	Univerbal
Anbieter	TalkPal.	Teacher AI	Quazel
Website	talkpal.ai	yourteacher.ai	univerbal.app
KI-Modell laut Anbieter	GPT (keine näheren Angaben)	ChatGPT (keine näheren Angaben)	keine Angaben
Webdienst / Android-/iOS-App	✓ / ✓ / ✓	✓ / angek. / angek.	✓ / ✓ / ✓
Sprache Oberfläche	Englisch	Englisch	je nach Ausgangssprache
Modi			
offener Chat / Call / Debatten mit der KI	✓ / ✓ / ✓	✓ / – / –	– / – / –
Rollenspiele: vorgegeben / frei erstellbar	✓ (frei wählbar) / ✓ (im KI-Chat)	– / ✓ (im KI-Chat)	✓ (aufbauend) / ✓ (eigene Funktion)
Aufgaben in den Rollenspielen	–	entfällt	✓ (jeweils 3)
Sätze nachsprechen	✓	– (nur nach Fehler im KI-Chat)	✓ (geführter Dialog bei Rollenspiel)
Sprachen			
Sprachen / Dialekte und Akzente ¹	61 / nur bei Englisch	26 / ✓ (über KI-Lehrer)	22 / –
Sprachlevel einstellbar / Einstufungstest	✓ (3 Level) / –	– / –	✓ / ✓
Sprachverarbeitung			
versch. Stimmen im Chat / in Rollensp.	– / ✓ (2)	✓ (mind. 2 für jede Spr.) / ✓	entfällt / ✓
Spracheingabe	Push to Talk	Push to Talk	Push to Talk oder (Semi-)Automatik
Sprachausgabe: Geschwindigkeit einstellbar	✓ (0,5x – 1,5x)	✓ (3 Stufen)	✓ (3 Stufen)
Sprachausgabe: Wiederholungsfunktion	✓ (alle KI-Sätze im Verlauf)	✓ (letzter KI-Satz laufendes G.)	✓ (alle KI-Sätze im Verlauf)
integrierter Übersetzer / freie Texteingabe	– / ✓	– / ✓	✓ (in beide Richtungen) / ✓
Transkription			
Textanzeige Eingabe / Ausgabe	✓ (Verlauf) / ✓ (Verlauf)	✓ (einzeln) / ✓ (einzeln)	✓ (Verlauf) / ✓ (Verlauf)
Übersetzung Satz / Wörter	✓ (für KI-Sätze) / –	✓ (für KI-Sätze) / ✓ (für KI-Sätze)	✓ (KI und Schüler) / ✓ (für KI-Sätze)
Korrekturfunktionen			
Bewertung Spracheingabe	✓ (separat in Textform)	✓ (vom KI-Lehrer)	✓ (separat in Textform)
Bewertung in Ausgangssprache	– (stets Englisch)	✓ (über Übersetzungsfunktion)	✓
Nachfragen in der Ausgangssprache möglich	Ausgangs- und Zielsprache mündlich und schriftlich	Ausgangs- und Zielsprache mündlich und schriftlich	Ausgangssprache nur schriftlich, Zielsprache mündlich und schriftlich
Nachfragen: Antworten in welcher Sprache	Zielsprache, Übersetzung	Zielsprache, Übersetzung, teilw. in Ausgangssprache	Zielsprache, Übersetzung
sonstige Funktionen			
Antwortvorschlag / andere Frage anfordern	✓ / ✓	– / –	✓ (generiertes Rollenspiel) / –
Fortschrittsanzeige / Gamifikation	– / –	– / –	✓ / ✓
Wörterbuch gelernter Vokabeln / Exportfunktion	– / entfällt	✓ / ✓	✓ / –
Bewertung			
Spracheingabe / Sprachausgabe	⊕ / ○	⊕ / ⊕	○ / ○ – ⊖ (je nach Sprache)
Abwechslung / Korrekturen	⊕ / ⊖ ²	○ / ⊕⊕	○ / ⊕
Kosten			
kostenloser Testzeitraum	14 Tage	– (7 Tage Rückerstattung)	7 Tage
Preis pro Monat	kostenlos (nur Basisfunktionen), 9,99 € (Monatsabo), 8 € (Quartalsabo), 5 € (Jahresabo)	25 € (Monatsabo), 17,83 € (Halbjahresabo), 12,25 € (Jahresabo)	14,99 € (Monatsabo), 13,33 € (Quartalsabo), 10 € (Jahresabo)

¹ nicht gemeint ist damit brasilianisches Portugiesisch, das alle getesteten Dienste als eigene Sprache betrachten
✓ vorhanden – nicht vorhanden k.A. keine Angabe ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht
² um eine Note abgewertet, da nur auf Englisch verfügbar

KI-Gesprächspartner im Eigenbau

Wie man ChatGPT zum Sprechtrainer aufrüstet

Sie möchten gerne mit einem KI-Sprechtrainer eine Fremdsprache üben, dafür aber nicht gleich ein Abo abschließen? Kein Problem: ChatGPT lässt sich auch in der kostenlosen Version am Rechner und am Smartphone als solcher nutzen.

Von Nico Jurran

Vom Start weg begeisterte ChatGPT als Chatbot mit der Fähigkeit, „natürliche“ Gespräche führen zu können. Da die generative KI zudem etliche Sprachen beherrscht und von sich aus geeignete Nachfragen stellt, liegt es nahe, sie auch als Konversationstrainerin für Fremdsprachen einzusetzen.

Für Textchats funktioniert das am Rechner ohne weiteres Zutun, für Voice Chats muss man ChatGPT erst dazu bringen, zuzuhören (Speech To Text) und selbst zu sprechen (Text To Speech). Wie das geht, erfahren Sie in diesem Artikel.

Lass uns reden!

Um loszulegen, benötigen Sie einen Rechner mit Lautsprecher und Mikrofon oder einem Headset, einen Chrome Browser und Zugang zu ChatGPT. Zwar liefert das kostenpflichtige GPT-4 schnellere und bessere Antworten und ist hinsichtlich der Anfragen weniger limitiert als sein kostenloser Vorgänger, für ein einfaches Sprechtraining reicht ChatGPT 3.5 aber völlig aus. Um die KI nutzen zu können, müssen Sie sich aktuell bei OpenAI unter <https://chat.openai.com/> mit Ihrer E-Mail-Adresse registrieren, es gibt aber Berichte, dass künftig keine Anmeldung mehr nötig sein soll.

Als Browser kommt Google Chrome deshalb infrage, weil dessen Web Store kostenlose Erweiterungen anbietet, die ChatGPT um eine Sprachverarbeitung ergänzt, also um eine Eingabe und Ausgabe. Bei uns brachte „Sprachsteuerung für ChatGPT“ von VoiceWave die besten Ergebnisse (Download unter ct.de/yxb9). Ist die Sprachsteuerung aktiviert, erscheint im Eingabefeld von ChatGPT ein Mikrofonsymbol.

Das Schöne an der Add-On-Lösung ist, dass man den KI-Sprachlehrer nutzen kann, ohne dafür jedes Mal die Systemsprache umzustellen oder sonstige Veränderungen Einfluss auf das gesamte System nehmen. Stattdessen stellt man einfach in der Erweiterung die gewünschte Sprache ein, in der man mit ChatGPT sprechen will.

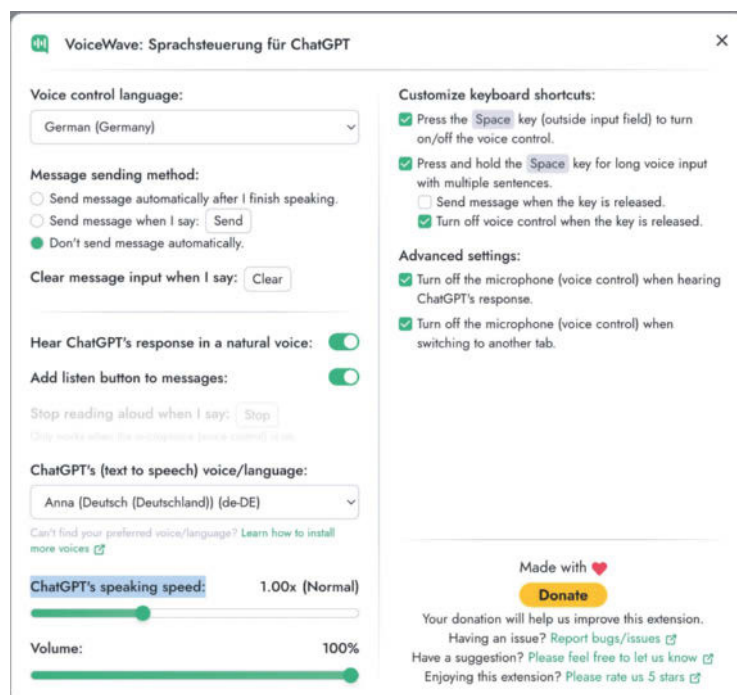
Einigung auf eine Sprache

Die Sprache, in der man mit der KI sprechen möchte, legt man unter „Voice Con-

trol Language“ in den „Settings“ fest, die man über das Rädchen-Icon erreicht, das sich über dem gerade erwähnten Mikrofonsymbol befindet. Dies sollte man auf jeden Fall vor der ersten Konversation einstellen: Ist die falsche Sprache vermerkt, versucht ChatGPT krampfhaft, dem Kauderwelsch einen Sinn zu geben. Aus dem spanischen „hablas“ (Du sprichst) wird dann etwa bei Deutsch als Eingabesprache „Ablass“.

ChatGPT beantwortet Nachfragen weiterhin auf Deutsch, allerdings stellt man diese dann besser über den Textchat, um nicht wieder die Eingabesprache wechseln zu müssen, damit die KI sie auch versteht.

Ebenso ist es wichtig, in den Settings unter dem Punkt „ChatGPT's (text to speech) voice/language“ die Sprache auszuwählen, in der die KI sprechen soll. Dies ist üblicherweise dieselbe wie die für die Eingabe. Vergisst man diesen Punkt,



Bei der Google-Chrome-Erweiterung muss man für die Ein- und Ausgabe die Lernsprache einstellen, da ChatGPT sonst keine verwertbaren Daten erhält beziehungsweise ungefähr so klingt, als wenn im Auto ein auf Deutsch eingestelltes Navi spanische Straßennamen ausspricht.

hört sich ChatGPT in etwa so an wie Fremdsprachler, die ohne Vorkenntnisse krampfhaft versuchen, Deutsch zu sprechen.

Die Spracherweiterung nutzt die Systemstimmen des Betriebssystems, wobei teilweise für eine Sprache bereits verschiedene Sprecher und sogar unterschiedliche Dialekte bereitstehen. Finden Sie keine brauchbare TTS-Stimme, können Sie weitere kostenlos über die Systemeinstellungen installieren. Erklärungen, wie Sie das konkret für die unterschiedlichen Versionen von macOS beziehungsweise MacOS bewerkstelligen und wie sich weitere kostenlose Stimmen in Microsofts Betriebssystem einpflegen lassen, finden Sie unter ct.de/yxb9.

Redet die KI für Ihren Geschmack zu schnell oder zu langsam, können Sie schließlich in der Erweiterung dem Feld „ChatGPT's speaking speed“ die Ausgabe-geschwindigkeit von 0,5 bis 3× anpassen. Ist dieser Bereich ausgegraut, müssen Sie zunächst das Kästchen „Hear ChatGPT's response in a natural voice“ darüber an-haken.

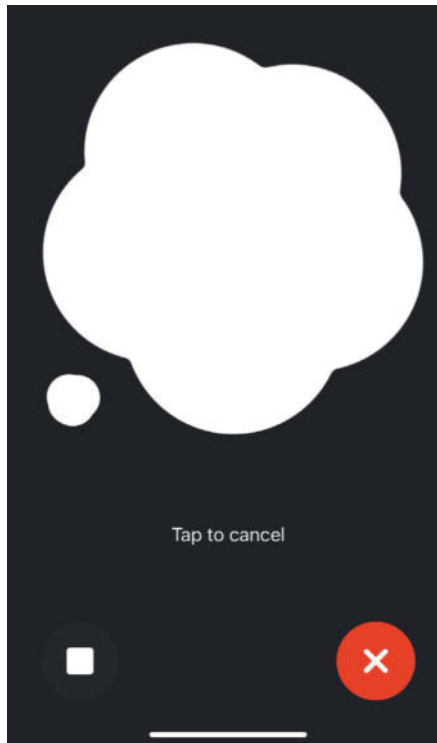
Durcheinander vermeiden

Wenn Sie in Ihren Sätzen längere Pausen machen, was zu Beginn ganz normal ist, stellen Sie unter „Sending Method“ ein, dass die Spracheingabe nicht automatisch gesendet wird. Andernfalls passiert es, dass Ihre Eingaben bereits an ChatGPT gehen, obwohl Sie noch gar nicht zu Ende gesprochen haben. Schalten Sie die Auto-matik ein, empfiehlt es sich, über den ersten Punkt unter „Advanced Setting“ den Haken für die Spracheingabe für den Fall zu deaktivieren, wenn ChatGPT spricht. Andernfalls kommt es vor, dass die KI mit sich selbst redet. Generell ist es die beste Lösung, ein Headset zu be-nutzen, damit solche Probleme gar nicht erst entstehen.

Die Funktion „Add listen button to messages“ hat mit der Konversation direkt nichts zu tun, ist aber durchaus nützlich: Ist sie aktiviert, erscheint unter jeder Transkription einer ChatGPT-Ausgabe ein Lautsprechersymbol, über das man sich den Satz noch einmal vorsprechen lassen kann.

Damit sind die Vorbereitungen abge-schlossen, sodass man Sie mit einer Ein-gabe (Prompt) à la

Lass uns ein Gespräch auf Französisch führen



In der ChatGPT-App kommt man über das Kopfhörersymbol in den Voice-Chat-Modus. Hier kann man frei drauflosreden, eine Transkription der KI-Ausgaben erhält man an dieser Stelle aber nicht.

die Konversation starten kann. ChatGPT quatscht darauf munter los, stellt Fragen und geht auf Ihre Antworten ein.

Korrektur erbeten

Sie werden allerdings schnell merken, dass die KI großzügig ist, was Fehler bei der Eingabe betrifft. ChatGPT geht also einfach darüber hinweg, wenn Sie etwa bei einem Artikel das falsche Geschlecht oder Singular statt Plural benutzen. Die KI macht also genau das, was man als Sprach-schüler eigentlich gerade nicht möchte, weil sich ohne Korrekturen und Verbesse-rungen Fehler manifestieren.

Deshalb ist es sinnvoll, wenn Sie ChatGPT mit auf den Weg geben, dass er auf Fehler achten und diese korrigieren soll. Allerdings sollten Sie ihn auffordern, das Gespräch danach fortzusetzen, damit die Konversation nicht bei jedem Fehler stockt. Ein möglicher Prompt hierfür wäre:

Korrigiere mich, wenn ich etwas falsch sage. Führe danach die Konversation fort.

Nach unserer Erfahrung kommt es vor, dass ChatGPT die Anweisung, die ange-

sprochenen Sätze zu korrigieren, nicht gleich umsetzt. Um sicherzustellen, dass die KI die Aufgabe verstanden hat, empfiehlt es sich daher, testweise einen fehlerhaften Satz zu sprechen und gegebenenfalls ChatGPT dann noch einmal auf seine Pflicht zur Korrektur hinzuweisen.

Um sich auf bestimmte Alltagssituationen vorzubereiten, können Sie ChatGPT dazu auffordern, mit Ihnen ein Rollenspiel in der Zielsprache zu führen. Ein geeigneter Prompt könnte wie folgt lauten:

Lass uns ein Rollenspiel auf Französisch führen, bei dem ich als Gast ein Restaurant besuche und du der Kellner bist.

Auf dem Smartphone

Zwar gibt es schon seit einiger Zeit in der ChatGPT-App eine Sprachverarbeitung, allerdings war diese auf die kostenpflichtige Version 4 beschränkt. Ende vergangenen Jahres schaltete OpenAI diese Funktion für ChatGPT 3.5 frei.

In der Smartphone-App starten Sie den Voice Chat, indem Sie auf das Kopfhörersymbol rechts neben dem Texteingabefeld drücken. Die komplette Steuerung funktioniert in diesem Modus mündlich. So können Sie ChatGPT etwa auffordern, ein Rollenspiel in einer bestimmten Fremdsprache zu starten. Zwischen Sprachen wechselt die KI nahtlos und beantwortet daher Nachfragen zu ihren Ausführungen auch in anderen Sprachen (wie Deutsch). Der Bitte um Korrekturen kommt ChatGPT auf dem Handy ebenfalls nach.

Haben Sie gerade erst mit einer Fremdsprache begonnen, kann dieser Voice-Chat-Modus aber überfordernd sein. So bekommen Sie hier keine direkte Transkription. Sie sehen sie erst nach der Rückkehr auf den Startbildschirm, weshalb Sie bereits über die nötige Hörkompetenz verfügen sollten. Problematisch wird die automatische Erkennung der Eingaben, wenn man längere Pausen beim Sprechen macht. Dieses Problem können Sie jedoch lösen, indem Sie „Hold for manual control“ beim Sprechen gedrückt halten. Dann verarbeitet die App die Eingabe erst, wenn Sie den Finger wieder vom Bildschirm nehmen. (nij@ct.de) **ct**

Download Sprachsteuerungs-erweiterung: ct.de/yxb9



Buchen und vergessen

Prepaidtarife mit drei bis zwölf Monaten Laufzeit

Wer sich nicht ständig um Guthaben kümmern, aber dennoch auf die Kostenkontrolle eines Prepaidvertrags nicht verzichten will, kann zum Jahrestarif greifen. Am Markt gibt es inzwischen mehr als ein Dutzend Angebote, die sich in vielerlei Hinsicht unterscheiden. Genau hinschauen lohnt sich.

Von Urs Mansmann

Bei normalen Prepaidverträgen ist alle vier Wochen Zahltag. Immer wieder muss man sicherstellen, dass noch genug Geld auf dem Mobilfunkkonto liegt, um nicht von heute auf morgen ohne Internet-

verbindung dazustehen. Unterwegs ohne WLAN ist es gar nicht so einfach, Guthaben aufzubuchen.

Einen Ausweg bieten Prepaidtarife mit langen Laufzeiten. Der Kunde bezahlt drei, sechs oder zwölf Monate im Voraus und muss sich erst dann wieder um das rechtzeitige Aufladen des Mobilfunkkontos kümmern. Es empfiehlt sich, einige Tage vorher eine Erinnerung zu setzen, um dann nicht doch wieder überraschend ohne mobiles Internet dazustehen.

Anders als herkömmliche Prepaidverträge, die immer nur vier Wochen lang gelten, also 13 Zahlungen pro Jahr erfordern, werden lang laufende Prepaidverträge nach Kalendermonaten abgerechnet. Das ist schon ein Kostenvorteil von rund 8 Prozent, allerdings muss man mit dem Inklusivvolumen auch einige Tage mehr auskommen.

Die Angebote lassen sich nach zwei Tariftypen unterteilen. Auf der einen Seite gibt

es echte Jahrestarife. Das Volumen, je nach Tarif zwischen 6 und 100 Gigabyte, gilt in diesem Fall für die gesamte Laufzeit des Vertrages. Die Tarife des anderen Modells finden Sie in der Tabelle als „vorausbezahlte Monatstarife“. In diesen bekommt der Nutzer jeden Monat einen Teil des Prepaidvolumens freigeschaltet, am Monatsende verfällt der unverbrauchte Rest. Anders als in den bisher üblichen Prepaidtarifen erfolgt die Abrechnung nicht vierwöchentlich, sondern zu einem Stichtag eines jeden Monats.

Unterschiedliche Modelle

Beide Modelle haben ihre Vor- und Nachteile. Wer meistens ein WLAN hat, aber dann ab und zu doch einmal das Internet unterwegs intensiver nutzen muss, sollte eher die Variante mit langer Laufzeit wählen. Damit kann man auch Phasen mit intensiver Nutzung wie einen Jahresurlaub abseits von WLANs abdecken. Nachteil ist, dass man das Volumen unbemerkt

recht schnell verbrauchen kann, etwa für Videos. Bekommt man die obligatorische 80-Prozent-Warnung des Providers schon recht früh, muss man sich entweder auf eine lange Durststrecke einstellen oder eben nachzahlen.

Bei vorausbezahlten Monatstarifen verliert man zwar am Ende eines jeden Monats nicht verbrauchtes Datenvolumen, dafür muss man auch nicht so lange warten, bis man neues Volumen zugeteilt bekommt. Diese Variante eignet sich besser für unerfahrene oder bequeme Nutzer, die ihr Datenvolumen nicht im Blick behalten wollen oder können.

Auch bei Jahrestarifen gilt die Grundregel, lieber deutlich zu viel zu buchen als etwas zu wenig. Steht man vor Ende der Laufzeit ohne Datenvolumen da, wird der Zugang in den meisten Tarifen gedrosselt, auf bestenfalls 64 kbit/s. Damit wird der Zugang praktisch unbrauchbar, weil sich viele Apps durch die stark verzögerten Antworten offline wähnen. Und diese Notlage nutzen die Anbieter kaltlächelnd aus: Nachgebuchtes Volumen ist in den meisten Fällen viel teurer als das bereits gebuchte Freivolumen. Ausnahmen sind das Dreimonatspaket von Ay Yildiz und der reine Datentarif von O2. Hier endet die Nutzung komplett, sobald man das Volumen verbraucht hat, aber man kann die Tarifoption direkt neu buchen.

Damit keine Lücke entsteht, muss auf dem Prepaidkonto ausreichend Guthaben vorhanden sein, um den Langzeittarif erneut buchen zu können, wenn er abläuft. Das sollte man nicht zu früh machen, damit das Konto nicht womöglich durch eine versehentliche Roaming-Sitzung oder per WAP-Billing leergeäumt wird. Am besten setzen Sie sich einige Tage vor Ablauf eine Erinnerung, damit Sie in Ruhe das Guthaben beschaffen und aufladen können.

Tagesflatrates für Streamingsitzung

Planen Sie ab und zu intensive Sitzungen, etwa einen Streamingabend im Ferienhaus ohne WLAN, gibt es bei einigen Anbietern Extrapakete oder sogar Flatrates für typischerweise 5 bis 8 Euro mit einer Laufzeit von 24 Stunden. Für diese Zeit wird der Volumenzähler des Tarifs gewissermaßen angehalten. Allerdings sollten Sie den Verbrauch im Auge behalten, wenn Sie keine Flatrate gebucht haben. Auch 10 Gigabyte sind beim Streaming womöglich schneller verbraucht, als Sie annehmen.

Alle Tarife gelten ohne Einschränkung auch im EU-Ausland, selbst die zusätzlichen Datenpakete kann man dort in den meisten Tarifen nutzen. Die Schweiz allerdings gehört nicht zur EU. Wenn Sie noch Guthaben auf Ihrem Prepaidkonto haben, können Sie das in einem Schweizer Netz bei Preisen von etlichen Euro pro Megabyte sehr schnell wieder loswerden. Nur Anbieter im Netz der Telekom zählen die Schweiz tariflich zur EU, und das auch nur für Datenverbindungen, nicht für Telefonate oder SMS.

Eine Flatrate für Inlandsgespräche und SMS ist nicht bei allen Angeboten enthalten; wenn dieser Punkt für Sie wichtig ist, sollten Sie das unbedingt prüfen. Telefonate in hoher Qualität per VoLTE übers Mobilfunknetz und per WLAN Call an Breitbandanschlüssen – sinnvoll in Gebäuden mit schlechtem Mobilfunkempfang – sind inzwischen in allen Tarifen verfügbar, außer im reinen Datentarif von O2. Bei Vodafone funktioniert WLAN Call inzwischen grundsätzlich auch in Prepaid-tarifen, muss aber durch den Kundenservice freigeschaltet werden.

Die überwiegende Zahl der Angebote umfasst bereits den Zugang zum 5G-Netz. Das bedeutet keine Verbesserung der Abdeckung, denn 5G-Funkzellen sind stets in 4G-Zellen integriert, die 5G-Abdeckung ist also eine Teilmenge der 4G-Abdeckung. Das wird auch noch lange so bleiben, weil umgerüstete Zellen mit DSS, Dynamic Spectrum Sharing, arbeiten, also mit einer Antenne 4G und 5G gleichzeitig bedienen. Das ist technisch sinnvoll, nicht nur weil noch ältere reine 4G-Geräte unterwegs sind, sondern weil auch viele 5G-Geräte noch kein 5G Standalone können,

also immer einen 4G-Zugang als Anker-netz benötigen und reine 5G-Zellen deswegen gar nicht nutzen könnten.

Ein Vorteil des 5G-Netzes ist die geringere Latenz, insbesondere beim Zugang über 5G Standalone. Hinzu kommen zusätzliche nur für 5G eingesetzte Bänder an einigen Funkstandorten, die für mehr Kapazität und damit für einen zügigeren Datentransfer sorgen. Wenn Sie ein 5G-fähiges Smartphone haben, profitieren Sie spürbar von dem neuen Netz.

Gedrosselte Datenraten

Viele der hier vorgestellten Tarife sind auf 25 oder 50 Mbit/s im Downstream gedrosselt. Davon merkt man üblicherweise wenig, denn die meisten Apps für mobile Nutzung sind auf Datensparsamkeit getrimmt. Wo wenig Datenverkehr anfällt, wirkt sich die Kappung kaum aus. Anders sieht es bei großen Downloads aus, die laufen bei hohen Datenraten spürbar schneller. Bei nominell 300 Mbit/s könnte man pro Minute über 2 Gigabyte übertragen. Das Freivolumen wäre dann natürlich ruckzuck weg, deswegen verschieben die meisten Apps große Downloads, bis ein WLAN bereitsteht. Die 300 Mbit/s sind ohnehin nur ein theoretischer Wert. Wenn Sie einmal einen Speedtest im Mobilnetz machen (aber Vorsicht, da laufen für einen Test womöglich etliche Hundert Megabyte durch!) werden Sie feststellen, dass Ihre Verbindung weit unter diesem Wert bleibt. Ob Ihr Tarif nun 25, 50 oder 300 Mbit/s liefert, spielt im Alltag deshalb nur eine untergeordnete Rolle.

Anders sieht es mit dem Netz aus. Die Abdeckung der vier Netzbetreiber ist sehr unterschiedlich. In Netztests gewinnt stets die Telekom, gefolgt in knappem Abstand von Vodafone, dahinter liegt O2. Wenn Sie das O2-Netz zuletzt vor einigen Jahren getestet haben, könnten Sie bei einem erneuten Test eine Überraschung erleben, denn O2 hat das Netz seither deutlich ausgebaut. Und ja, da fehlt noch der Vierte: 1&1 hat gerade erst mit dem Netzausbau begonnen und erst eine gewissermaßen homöopathische Netzabdeckung erreicht, was der Provider aber mit nationalem Roaming mit derzeit O2 ausgleicht, im Laufe des Jahres ziehen die Kunden aber zum neuen Kooperationspartner Vodafone um. In diesem Vergleich spielt 1&1 keine Rolle, weil es aus deren Haus bislang noch keinen Jahrestarif gibt.

Inkl. SIM-Karte

JAHRESPAKET L

108 GB statt 72 GB

12 x 9 GB Highspeed Internet

Allnet-Flat
SMS-Flat

129 € pro 12 Monate¹

Viele Jahrespakete sind in Wirklichkeit vorausbezahlte Monatstarife, bei denen das Volumen auf die Monate aufgeteilt wird.

Optionen für Bestandskunden

Buchen lassen sich die hier vorgestellten Jahrestarife in aller Regel auch für Bestandskunden der jeweiligen Mobilfunkmarken. Taucht der Tarif im Online-Kundencenter nicht auf, kann möglicherweise die Hotline weiterhelfen. In den meisten Fällen wird ein Umstieg auf einen Langzeittarif aber auch einen Providerwechsel erfordern, dann können Sie Ihre Mobilfunk-

nummer kostenlos mitnehmen. Bei Ay Yildiz, Kaufland Mobil und Vodafone können Sie den Langzeittarif nicht beim Kauf abschließen, sondern müssen erst den Basisstarif und anschließend die Tarifooption buchen.

Bezahlen können Sie den Online-Kauf üblicherweise mit der Kreditkarte oder PayPal, nur Congstar und Nettokom bestehen darauf, dass Sie ihnen ein SEPA-Lastschrift-

mandat erteilen, also die Abbuchung von Ihrem Konto zulassen. Über diese Bankverbindung können Sie dann später auch Ihr Guthabenkonto aufladen oder Zahlungen für Tarifooptionen buchen lassen.

Immer mehr Prepaidprovider bieten inzwischen eine eSIM an. Die meisten aktuellen Smartphones auch der günstigen Klassen beherrschen das, bei älteren Modellen nur die aus der Mittel- oder Ober-

Prepaid-Tarife mit langer Laufzeit

Anbieter	Ay Yildiz	Congstar	Edeka	Edeka	Jamobil/Pennymobil	Kaufland Mobil	Nettokom
Tarif	3-Monats-Paket	Prepaid Halbjahres-Paket	Jahrespaket Start	Jahrespaket Premium	Prepaid 6-Monats-Paket	Smart XS Halbjahrespaket	Jahrespaket
URL	ayyildiz.de	congstar.de	edeka-smart.de	edeka-smart.de	jamobil.de, pennymobil.de	kaufland-mobil.de	nettokom.de
Netz	02	Telekom	Telekom	Telekom	Telekom	Telekom	02
Tariftyp	Vierteljahrestarif	vorausbez. Monatstarif	Jahrestarif	vorausbez. Monatstarif	Halbjahrestarif	Halbjahrestarif	Jahrestarif
Grundkonditionen							
max. Datenrate Down / Up, beste Zugangstechnik	25 / 10 Mbit/s, LTE	25 / 10 Mbit/s, 5G	300 / 50 Mbit/s, LTE	300 / 50 Mbit/s, LTE	25 / 10 Mbit/s, LTE	25 / 10 Mbit/s, LTE	50 / 25 Mbit/s, 5G
Datenrate gedrosselt Download / -Upload	64 / 64 kbit/s	64 / 16 kbit/s	32 / 16 kbit/s	32 / 16 kbit/s	64 / 16 kbit/s	64 / 16 kbit/s	64 / 64 kbit/s
Preis Telefonminute / SMS	600 Minuten kostenlos, danach je 15 ct / 15 ct	Flatrate / Flatrate	1200 Minuten/SMS kostenlos, danach je 9 ct	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate
Preis Telefonminute / SMS anbieterintern	600 Minuten kostenlos, danach je 9 ct / 9 ct	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate
Grundpreis Abfrage Mailbox	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos
Optionen und Erweiterungen							
Datenvolumen / Gültigkeitsdauer	10 GByte / 3 Monate	6 GByte / 1 Monat	12 GByte / 12 Monate	3 GByte / 1 Monat	8 GByte / 6 Monate	8 GByte / 6 Monate	20 GByte / 12 Monate
rechnerisches Datenvolumen pro Monat	3,3 GByte	6 GByte	1 GByte	3 GByte	1,3 GByte	1,3 GByte	1,7 GByte
optionale Nachbuchung bei verbrauchtem Datenvolumen	Paket neu buchbar	1 / 2 / 4 GByte bis Laufzeitende 6 / 10 / 15 €	0,5 GByte, 4,95 €/7 Tage	0,5 GByte, 4,95 €/7 Tage	1 / 2 / 5 GByte bis Laufzeitende 4,99 / 7,99 / 14,99 €	1 / 2 / 5 GByte bis Laufzeitende 5 / 8 / 15 €	1 GByte bis Laufzeitende 5,99 €
			0,5 / 1,5 / 2,5 GByte, 7,95 / 14,95 / 19,95 €/28 Tage	0,5 / 1,5 / 2,5 GByte, 7,95 / 14,95 / 19,95 €/28 Tage			
Kurzzeit-Optionen	10 GByte, 4,99 €/24 Stunden	10 GByte, 5 €/24 Stunden	Flatrate, 5,95 €/24 Stunden	Flatrate, 5,95 €/24 Stunden	—	—	1 GByte, 1,99 €/24 Stunden
	20 GByte, 7,49 €/24 Stunden	15 GByte, 8 €/48 Stunden					10 GByte, 3,99 €/24 Stunden
		20 GByte, 20 €/7 Tage					
Schweiz im Roaming zum EU-Tarif abgerechnet	—	✓ (nur Datennutzung)	✓ (nur Datennutzung)	✓ (nur Datennutzung)	✓ (nur Datennutzung)	✓ (nur Datennutzung)	—
Preise nach Auslaufen der Tarifooption	15 ct für Telefonminute/SMS, 0,29 €/MByte	9 ct für Telefonminute/SMS, 25 MByte für 1 €/Tag	9 ct für Telefonminute/SMS, 50 MByte für 1,49 €/Tag	9 ct für Telefonminute/SMS, 50 MByte für 1,49 €/Tag	9 ct für Telefonminute/SMS, 25 MByte für 0,99 €/24 Stunden	9 ct für Telefonminute/SMS, 25 MByte für 1 €/24 Stunden	9 ct für Telefonminute/SMS, 0,24 €/MByte
VoLTE / VoWiFi (WLAN-Call)	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
eSIM erhältlich	nachträglich	nachträglich	bei Bestellung	bei Bestellung	—	bei Bestellung	—
Besonderheiten	—	—	Hotspot-Flat für Telekom	Hotspot-Flat für Telekom	—	—	—
Kosten							
einmalige Gebühren bei Online-Bestellung	9,99 €, zusätzlich müssen 15 € Guthaben erworben werden	50 €	59,95 €	94,95 €	29,95 €	4,99 €, zusätzlich müssen 20 € Guthaben erworben werden	79,98 € (davon 10 € Guthaben)
Laufzeit des Tarifs	3 Monate	6 Monate	12 Monate	12 Monate	6 Monate	6 Monate	12 Monate
rechnerische Kosten pro Monat	8,33 €	8,33 €	5 €	7,91 €	4,99 €	4,17 €	5,83 €
rechnerische Kosten pro GByte im Grundtarif	2,50 €	1,39 €	5 €	2,64 €	3,74 €	3,12 €	3,50 €
mögliche Zahlungsmittel bei Online-Bestellung	Visa, Mastercard, Amex, PayPal	SEPA-Lastschriftmandat erforderlich	Vorkasse, Visa, Mastercard, Amex, Google Pay, Apple Pay, GiroPay, Rechnung	Vorkasse, Visa, Mastercard, Amex, Google Pay, Apple Pay, GiroPay, Rechnung	Vorkasse, Visa, Mastercard, Amex, Google Pay, Apple Pay, GiroPay, Rechnung	Vorkasse, Visa, Mastercard, Diners, PayPal	SEPA-Lastschriftmandat erforderlich

¹ auf Anfrage beim Kundenservice

✓ vorhanden

— nicht vorhanden

klasse. Die Provider tun sich damit schwerer: Standard ist immer noch, dass der Kunde zunächst eine physische SIM zugesandt bekommt und diese dann später in eine eSIM wechseln kann. Damit verspielen die Anbieter den wichtigsten Vorteil der eSIM, dass man nicht die Postlaufzeit abwarten muss, sondern sie direkt in Betrieb nehmen kann. Vermutlich dient die physische SIM-Karte auch der Prüfung

der Adresse, was bei Prepaidkunden aber vollkommen unnötig ist, denn bei diesen ist eine Ausweisprüfung gesetzlich vorgeschrieben.

Fazit

Ein verlängerter Abrechnungszeitraum bei Prepaidtarifen spart den ständigen Blick aufs Konto, allerdings muss man genau hinschauen, ob man wirklich einen echten

Halbjahres- oder Jahrestarif erhält und nicht stattdessen einen vorausbezahlten Monatstarif. Beide Varianten haben Vorteile für verschiedene Nutzergruppen. Wer auf das Angebot einsteigt, hat bis zu einem Jahr lang Ruhe – das ist ideal, wenn man die Prepaidverträge für Kinder oder Eltern managt. Bei rechnerischen Monatspreisen zwischen 4 und 11 Euro wird man auf jeden Fall nicht arm. (uma@ct.de) **ct**

	Norma Connect	02	02	Tchibo	Tchibo	Tchibo	Telekom	Vodafone
	Smart 6	Internet-to-Go Jahrespaket 40 (100) GB	Smartphone Jahrespaket	Jahrespaket S	Jahrespaket M	Jahrespaket L	Prepaid 5G Jahrestarif	Jahrestarif
	norma-connect.de	o2-freikarte.de	o2-freikarte.de	tchibo.de	tchibo.de	tchibo.de	telekom.de	vodafone.de
	Telekom	02	02	02	02	02	Telekom	Vodafone
	Halbjahrestarif	Jahrestarif	Jahrestarif	vorausbez. Monatstarif	vorausbez. Monatstarif	vorausbez. Monatstarif	vorausbez. Monatstarif	Jahrestarif
	25 / 10 Mbit/s, 5G	300 / 50 Mbit/s, 5G	300 / 50 Mbit/s, 5G	50 / 25 Mbit/s, 5G	50 / 25 Mbit/s, 5G	50 / 25 Mbit/s, 5G	300 / 50 Mbit/s, 5G	300 / 100 Mbit/s, 5G
	64 / 16 kbit/s	0 / 0 kbit/s	0 / 0 kbit/s	64 / 64 kbit/s	64 / 64 kbit/s	64 / 64 kbit/s	32 / 16 kbit/s	64 / 64 kbit/s
	Flatrate / Flatrate	(– / –) Tarif umfasst weder Telefonie noch SMS	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate
	Flatrate / Flatrate	(– / –) Tarif umfasst weder Telefonie noch SMS	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate	Flatrate / Flatrate
	kostenlos	–	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos
	8 GByte / 6 Monate	40 (100) GByte / 12 Monate	15 GByte / 12 Monate	1,5 GByte / 1 Monat	5,5 GByte / 1 Monat	9 GByte / 1 Monat	5 GByte / 1 Monat	50 GByte / 12 Monate
	1,3 GByte	3,3 (8,3) GByte	1,3 GByte	1,5 GByte	5,5 GByte	9 GByte	5 GByte	4,2 GByte
	1 / 2 / 5 GByte bis Laufzeitende 5 / 8 / 15 €	Paket neu buchbar	1 / 2 / 5 GByte, 4,99 / 9,99 / 14,99 €/28 Tage	0,75 / 1,5 / 4 GByte, 2,99 / 4,99 / 9,99 bis Monatsende	0,75 / 1,5 / 4 GByte, 2,99 / 4,99 / 9,99 bis Monatsende	0,75 / 1,5 / 4 GByte, 2,99 / 4,99 / 9,99 bis Monatsende	1 / 3 / 6 GByte, 5,95 / 14,95 / 19,95 € bis Monatsende	0,5 / 1 / 4 GByte, 2,99 / 4,99 / 9,99 €/7 Tage
	–	–	–	10 GByte, 4,99 €/24 Stunden	10 GByte, 4,99 €/24 Stunden	10 GByte, 4,99 €/24 Stunden	Flatrate, 6,95 €/24 Stunden	10 GByte, 4,99 €/24 Stunden
	–	–	–	–	–	–	Flatrate, 6,99 €/24 Stunden	–
	✓ (nur Datennutzung)	–	–	–	–	–	✓ (nur Datennutzung)	–
	9 ct für Telefonminute/SMS, 25 MByte für 1 €/24 Stunden	–	9 ct für Telefonminute/SMS, kein Internetzugang	9 ct für Telefonminute/SMS, 0,24 €/MByte	9 ct für Telefonminute/SMS, 0,24 €/MByte	9 ct für Telefonminute/SMS, 0,24 €/MByte	9 ct für Telefonminute/SMS, 50 MByte für 1,49 €/Tag	9 ct für Telefonminute/SMS, 0,03 €/MByte
	✓ / ✓	(Tarif umfasst keine Telefonie)	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / (✓) ¹
	bei Bestellung	nachträglich	nachträglich	für Sommer 2024 angekündigt	für Sommer 2024 angekündigt	für Sommer 2024 angekündigt	nachträglich	bei Bestellung
	–	reiner Datentarif beispielsweise für Tablet oder Notebook	–	–	–	–	Hotspot-Flat	–
	29,99 €	64,98 (104,98) €	84,98 €	69 €	99 €	129 €	99,95 €	kostenlos, zusätzlich müssen 99,99 € Guthaben erworben werden
	6 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate
	4,99 €	5,42 (8,75) €	7,08 €	5,75 €	8,25 €	10,75 €	8,33 €	8,33 €
	3,74 €	1,62 (1,05) €	5,67 €	3,83 €	1,50 €	1,19 €	1,67 €	2,00 €
	Vorkasse, Visa, Mastercard, Amex, Google Pay, Apple Pay, GiroPay, Rechnung	Vorkasse, Visa, Mastercard, Amex, PayPal, Nachnahme	Vorkasse, Visa, Mastercard, Amex, PayPal, Nachnahme	Vorkasse, Visa, Mastercard, PayPal	Vorkasse, Visa, Mastercard, PayPal	Vorkasse, Visa, Mastercard, PayPal	PayPal, Visa, Mastercard, Amex, Nachnahme	keine Zahlung erforderlich

Zahlen, Daten, Fakten

Reisen

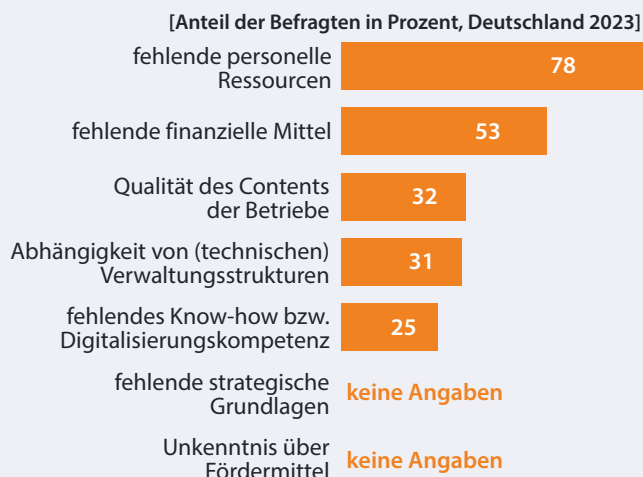
Wer reist, tut das meist mit Vorlauf: erst suchen, dann buchen und später hoffentlich nicht fluchen, wenn der Trip ein Flop war. Onlinebuchungen übernehmen schon einen Großteil der Reiseverträge; etwas mehr bei kurzzeitigen Reisen, während bei längeren Reisen auch das persönliche Gespräch im Reisebüro eine große Rolle spielt. Dabei ist vielen offenbar der persönliche Kontakt

zum Berater wichtig. Fürs Buchen übers Netz spricht, dass es dafür keine Ladenöffnungszeiten gibt und dass man die Angebote mithilfe von Kundenrezensionen teils besser vergleichen kann. Digital unterwegs sind viele Reisende, indem sie Fotos aus dem Urlaub in sozialen Medien posten, obwohl viele auch genervt von Fotos anderer sind, die in der Timeline aufploppen.

Nicht so digital unterwegs sind noch viele Hotels und Gastronomiebetriebe. Außer freiem WLAN und digitalen Buchungsschnittstellen gibt es wenig, was wohl auch an fehlenden Fachkräften dafür liegt. Stattdessen einfach mit der VR-Brille eine virtuelle Reise zu unternehmen, finden vier Fünftel der Befragten einer Bitkom-Studie noch abwegig. (mil@ct.de) **ct**

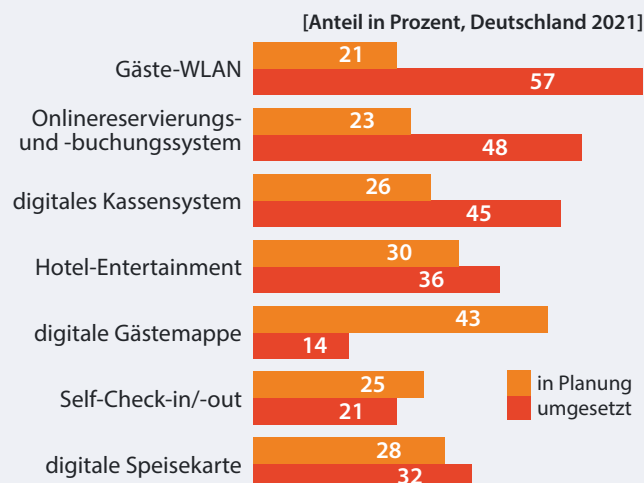
► Digitalisierungsdefizite

Zu wenig Leute, die sich mit digitalen Instrumenten im Tourismus auskennen. Das beklagten Befragte aus einer brancheninternen Umfrage.¹



► Semidigitales Gastgewerbe

Nur knapp zwei Drittel der Hotels hatten bis 2021 laut einer Telekom-Studie ein WLAN. Nur jedes zweite Hotel war online zu buchen.²



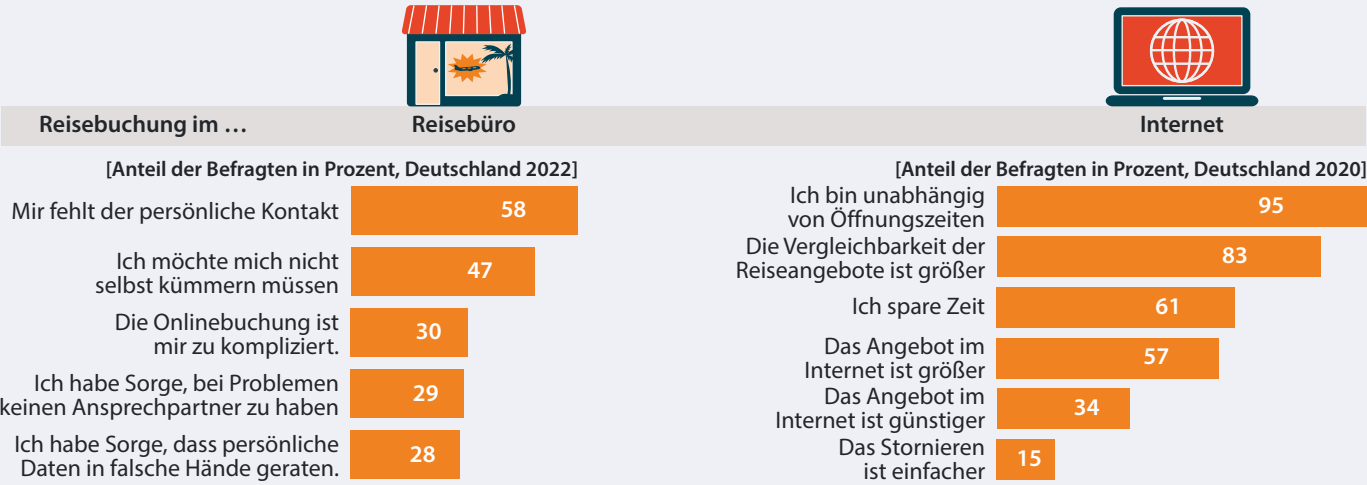
► Reisen virtuell

Metaverse und virtuelle Reisen per Videobrille? Laut Befragten einer Bitkom-Umfrage 2023 sind echte Reisen beliebter. Für Reisebüros sehen zwei Drittel der Befragten schwarz.³



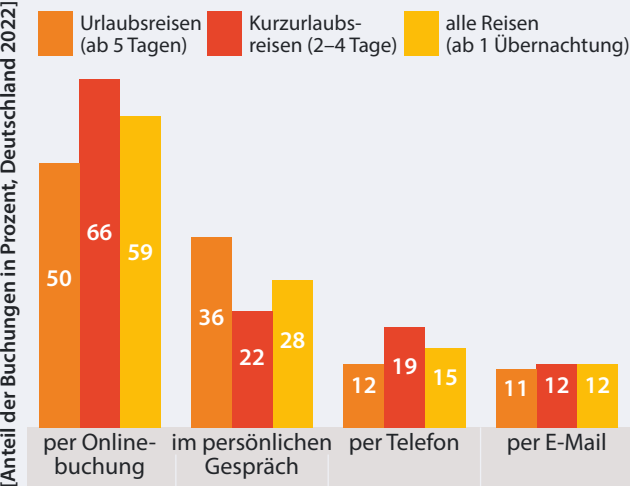
► Online und Offline

Für die Buchungswege führen Befragte einer Bitkom-Studie unterschiedliche Gründe an, am häufigsten ist mehr Flexibilität der Treiber für die Onlinebuchung.⁴



► Reisedauer und Buchungsweg

Bei längeren Reisen werden vor allem im Netz gebucht, aber noch hat das persönliche Gespräch im Reisebüro einen recht großen Anteil.⁵



► Onlinebewertungen

Viele lesen Bewertungen, ein Großteil davon traut ihnen aber laut einer Bitkom-Umfrage 2023 nicht aus unterschiedlichen Gründen.³





Bild: Collage c't

Aus drei mach vier

Was Windows 11 Version 24H2 Neues bringt – und was rausfliegt

Im Herbst dieses Jahres steht unweigerlich wieder eine frische Windows-Version mit einem Schwung neuer Funktionen an. Was drinsteckt, ist bereits gut zu erkennen.

Von Jan Schübler

Windows 11 24H2 soll laut Microsoft im Herbst kommen; wir rechnen mit Ende September bis Mitte Oktober. Teilnehmer am Betatestprogramm Windows Insider können sie bereits beschnuppern. Dieser Artikel wirft einen Blick auf den aktuellen Stand der Neuerungen. Wenngleich hier und dort noch Details hinzukommen oder geändert werden können, zeigt die aktuelle Testversion mit der Build-Nummer 26100 bereits gut, wohin die Reise geht.

Zuerst aber noch ein Hinweis zu Gerüchten über eine neue Hauptversion namens Windows 12, die seit rund einem Jahr die Runde im Netz machen. Die Spekulationen fußen teils auf naheliegenden Hinweisen (beiläufiges Zeigen einer schwelenden Taskleiste und weiterer umgestalteter Oberflächenelemente in einer Microsoft-Präsentation), teils aber auch auf schwammigen Formulierungen von Partnerfirmen wie Intel, man erwarte für 2024 gute Umsätze wegen eines „Windows Re-

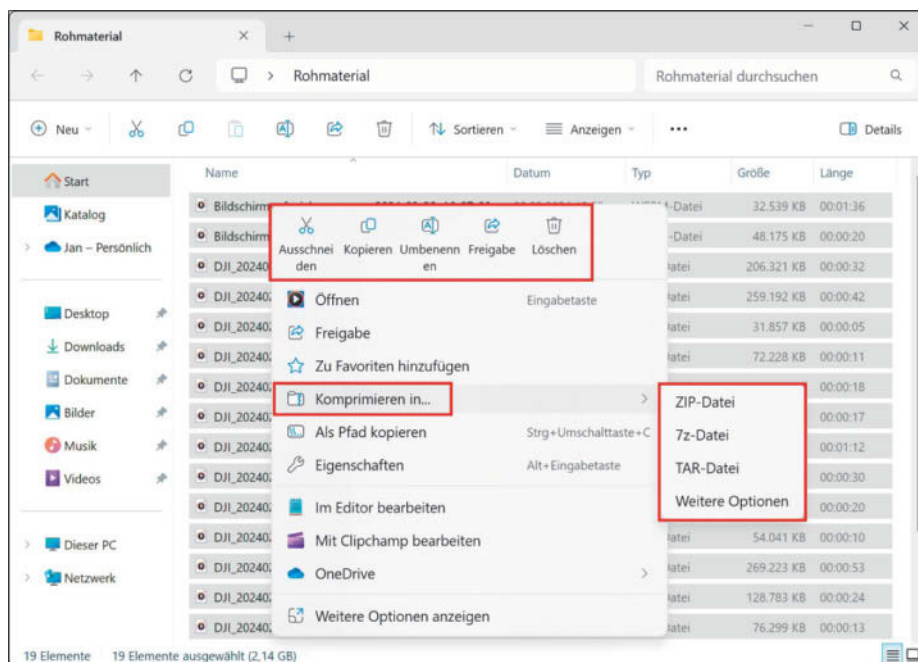
fresh“, was ebenso gut ein Funktionsupdate sein kann.

Ernsthafte Hinweise auf ein tatsächliches Windows 12 sehen wir bislang nicht – zumindest nicht für 2024. Das heißt nicht, dass es nicht vielleicht doch kommen wird: Auch Windows 11 hatte Microsoft erst rund vier Monate vor dem Release vorgestellt. In diesem Artikel geht es aber ausdrücklich um das nächste Funktionsupdate für Windows 11.

Datei-Explorer

Kein Funktionsupdate ohne Explorer-Neuigkeiten – diese Tradition setzt Version 24H2 fort. So bekommen die bislang immer etwas kryptischen Mini-Schaltflächen für Ausschneiden, Kopieren, Einfügen und so weiter Beschriftungen.

Die Option, Archivdateien in den Formaten 7z, RAR und TAR zu entpacken, bekam Windows 11 mit Version 23H2; mit 24H2 kommt auch eine Möglichkeit zum Erstellen von 7z- und TAR-Archiven hinzu. Zu finden ist die Funktion per Rechtsklick auf Dateien und Ordner und Auswahl von „Komprimieren in...“. Über „Weitere Optionen“ lassen sich dabei auch Pack-Parameter wie Kompressionsgrad, Algorithmus und für TAR das genaue Format festlegen (POSIX-konformes Pax oder ustar).



In Version 24H2 kann Windows 11 Dateien nicht nur ins Zip-Format komprimieren, sondern auch als TAR- oder 7z-Datei speichern. Und: Wichtige Schaltflächen bekommen Beschriftungen.

sudo für Windows

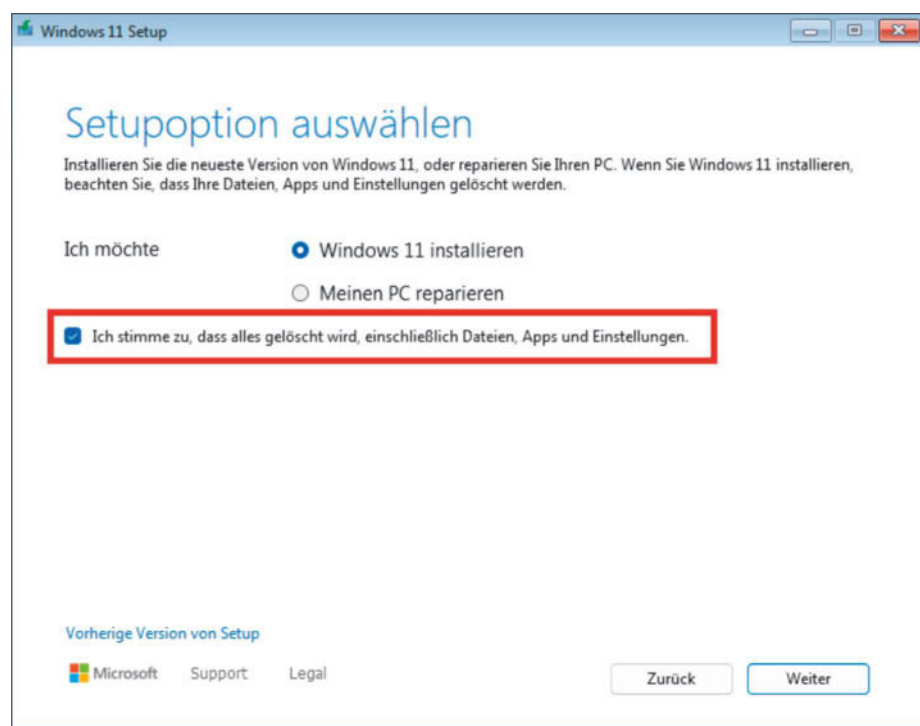
Die Idee, das von Unix-artigen Systemen bekannte Kommando „sudo“ zum Ausführen von Programmen mit erhöhten

Rechten auf Windows zu bringen, mag im ersten Moment seltsam erscheinen – denn mit „runas.exe“ gibt es schon seit Langem einen Windows-Konsolenbefehl, der Ähnliches tut.

Sieht man sich das Windows-sudo näher an, stellt man schnell zwei Dinge fest. Erstens: Mit dem unixesken sudo hat es außer dem Namen und dem Zweck nicht allzu viel gemeinsam. Zweitens: Von runas.exe unterscheidet es sich durchaus in einigen Punkten. Welche das sind, lesen Sie im Artikel auf Seite 134.

Neues im Setup

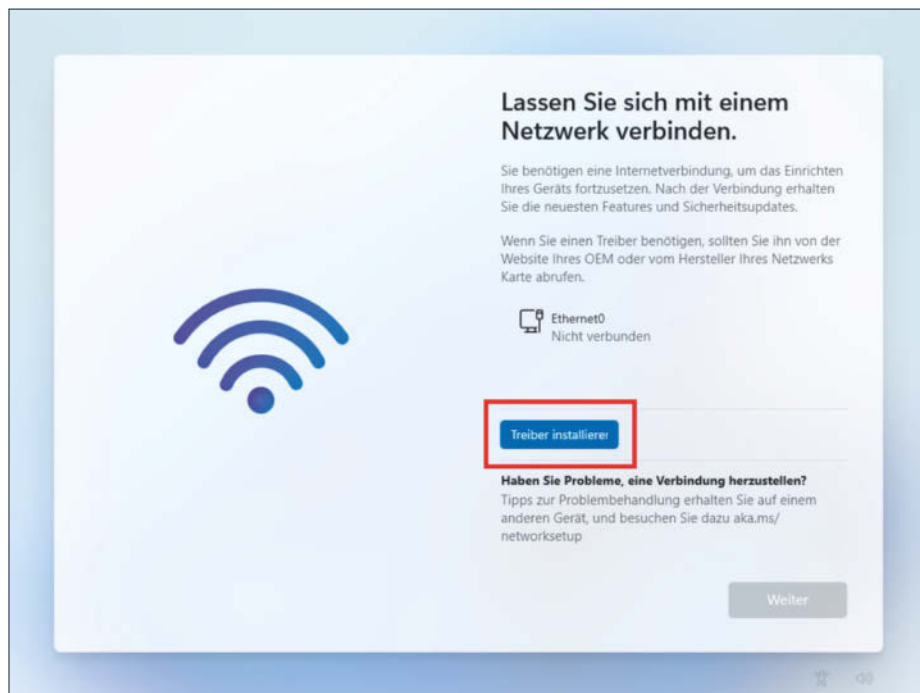
Erstmals seit vielen Jahren hat Microsoft das Installationsprogramm für Windows-



Das neue Setup-GUI von Version 24H2 will ein Häkchen zum Fortsetzen einer sauberen Neuinstallation haben. Ansonsten sieht es zwar anders aus als bisher, macht aber immer noch dasselbe.

c't kompakt

- Die kommende Windows-11-Ausgabe bringt praktische neue Details; manch Überholtes fliegt raus.
- Nach vielen Jahren bekommt sogar das Setup-Programm einen neuen Look.
- Auf manchen sehr alten, nicht unterstützten CPUs läuft die neue Version nicht mehr.



Hat der LAN- oder WLAN-Adapter bei der Ersteinrichtung keinen Treiber, brauchen Sie keine Stunts mehr zu drehen, sondern nur einen Datenträger mit dem passenden Treiber. Der Netzwerkzwang bleibt jedoch.

Neuinstallationen optisch überarbeitet. Das Setup erfordert nun das Setzen eines Häkchens zur Bestätigung, dass man verstanden hat, durch die Installation alle Daten auf dem Ziellaufwerk zu löschen. Davon abgesehen bietet die neue Oberfläche nichts Neues – aber immerhin auch keinen Nachteil.

Eine hilfreichere Option findet sich hingegen während der Ersteinrichtung (auch Out Of Box Experience genannt, kurz OOBE). Der Quasi-Zwang zum Herstellen einer Internetverbindung während der Ersteinrichtung ist nicht nur nervig, sondern auch ein Problem, wenn während des Setups kein LAN- oder WLAN-Adapter gefunden wird, weil Windows keinen Treiber dafür hat. Mit der Schaltfläche „Treiber installieren“ können Sie nun während der OOBE einen Netzwerktreiber hinzufügen, ohne dafür Umwege über Eingabeaufforderung und Geräte-Manager gehen zu müssen.

Altes fliegt raus

Bei einer sauberen Neuinstallation von 24H2 landen zudem nun weniger von jenen Apps auf dem Rechner, die bislang serienmäßig mit Windows 11 installiert wurden. Standardmäßig nicht mehr dabei sind die Apps Mail, Kontakte, Kalender, Karten, Cortana und Filme & TV. Größ-

tenteils werden diese Apps schlicht überflüssig: Die neue Outlook-App ersetzt Mail, Kontakte und Kalender; Cortana hat angesichts des KI-Copilot endgültig ausgedient und Filme & TV wird – wie vor einiger Zeit schon der Audioplayer Groove Music – durch die App „Medienwiedergabe“ ersetzt. Die ist eine Art Neuauflage des guten alten Windows Media Player. Lediglich die Karten-App bekommt offenbar keinen Nachfolger.

Der Texteditor WordPad fliegt ebenfalls raus. Das hat Microsoft erst vor wenigen Monaten angekündigt, weshalb wir eigentlich damit rechneten, dass der Textverarbeitungs-Klassiker – im Prinzip ein sehr einfacher Ersatz für MS Word – noch ein, zwei Jahre Teil von Windows bleibt. Im bis Redaktionsschluss aktuellen Insider-Setup-Abbild mit der Build-Nummer 26080 fehlt es allerdings schon und lässt sich dort auch nicht über die Windows-Feature-Verwaltungen hinzufügen oder aus dem Store nachinstallieren.

Und auch beim Teams-Hickhack tut sich was. Mit Version 24H2 ist es nun endlich möglich, geschäftliche und private Accounts mit einer Teams-App – der vorinstallierten – zu benutzen. Das klappt auch parallel. An den Bezeichnungen muss Microsoft noch ein wenig arbeiten:

Die beiden Icons im Infobereich der Taskleiste melden sich als „Teams (work or school)“ und „Teams (work or school) Persönlich“.

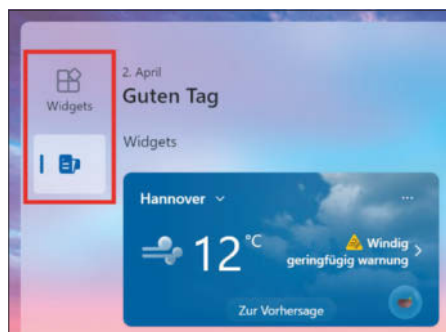
Und noch mehr

Das Widget-Board bekommt eine Möglichkeit zum Umschalten zwischen der bislang üblichen Ansicht mit angehängtem Newsfeed und einer reinen Anzeige der eigenen Widgets. Die vor Kurzem mit dem Moment-5-Update [1] eingeführte Möglichkeit, den Newsfeed ganz abzuschalten, bleibt bestehen.

In der Einstellungen-App gibts ab 24H2 auch die Optionen zum Festlegen, was beim Drücken der Powertaste und beim Zuklappen des Rechners passieren soll. Bislang müssen Sie die klassische Systemsteuerung bemühen, um die Optionen zu verändern. Dort sind die Optionen nach wie vor enthalten. Zudem hat Microsoft den Zugriff auf den Energiesparmodus vereinfacht: Der Stromsparmodus für weniger Verbrauch im Betrieb, nicht der Standby-Modus, lässt sich nun direkt per Schalter aktivieren – auch auf Desktop-Rechnern, was zum Beispiel für virtuelle Maschinen praktisch sein kann.

Die Funktion „Voice Clarity“ soll die eigene Sprachqualität in Teams & Co. in unruhigen oder lauten Umgebungen verbessern. Bislang war das Surface-Geräten vorbehalten, die einen aktuellen Prozessor mit Neural Processing Unit (NPU) haben. Ab Version 24H2 gibt es das Feature auf allen Windows-11-konformen Rechnern – ein Prozessor mit NPU ist interessanterweise auch nicht mehr nötig. Ausprobieren können Sie das in der Einstellungen-App. Dazu öffnen Sie unter „System/Sound“ die Eigenschaften des Mikrofons und starten den Mikrofontest mit dem Testmodus „Kommunikation“.

Die Personalisierung der Schnelleinstellungen wird vereinfacht. In dem kleinen Menü, das sich per Klick aufs Netzwerk-, Sound- oder Akku-Icon rechts auf der Taskleiste öffnet, lassen sich die Schaltflächen nun per Drag & Drop umsortieren. Das Extramenü zum Ein- oder Ausblenden einzelner Schaltflächen verschwindet. Stattdessen zeigen die Schnelleinstellungen nun bis zu sechs Schaltflächen an. Gibt es mehr, kann man per Mausrad oder Zweifinger-geste durchs Menü scrollen – und wichtige Schaltflächen nach oben schieben, damit sie sich unter den ersten sechs befinden.



Künftig kann man das Widget-Board umschalten zwischen einer Ansicht inklusive Newsfeed und einer, die nur die eigenen Widgets anzeigt.

Mit 24H2 soll Windows 11 auch vollständigen Support für den Drahtlosstandard Wi-Fi 7 bekommen. Das mag zunächst komisch klingen, denn entsprechende Treiber funktionieren prinzipiell auch mit jedem aktuellen Windows 11 in Version 23H2. Im Test sind wir aber durchaus auf ein paar Probleme gestoßen [2]. Weil Wi-Fi 7 bereits im Markt angekommen ist und geeignete Geräte zu kaufen sind, würde es uns nicht wundern, wenn Microsoft den Wi-Fi-7-Support schon vor Version 24H2 mit einem Update für die bestehenden Windows-Versionen nachliefert.

Anpassungen nimmt Microsoft außerdem am Netzwerkprotokoll SMB vor (Server Message Block), um neue Funktionen zu unterstützen. Dabei geht es vor allem um Audit-Tools für SMB over QUIC sowie für SMB-Signaturen und -Verschlüsselung. Admins können die Funktionen per Gruppenrichtlinien-Editor und PowerShell verwalten und in der Ereignisanzeige auswerten (Dokumentation via ct.de/yyrm).

CPU-Verwirrung

Vor einigen Wochen kursierten Berichte, Microsoft könnte die Verwendung bestimmter älterer CPUs für Windows 11 unterbinden – eine Nachricht, die auf eine Userschaft trifft, die ohnehin schon von den absurd hohen Systemvoraussetzungen genervt ist. Bei genauerer Betrachtung stellt sich aber heraus, dass die Einschränkung, die offenbar in Version 24H2 Einzug halten soll, größtenteils irrelevant ist – wo sie relevant ist, ist sie aber ein echtes Problem, denn sie lässt sich nach aktuellem Kenntnisstand nicht umgehen.

Worum gehts? Microsoft macht die CPU-Befehlssätze SSE 4.2 (Intel) und SSE

4a (AMD) zur Pflicht, ebenso ganz ausdrücklich den Prozessorbefehl POPCNT. Das betrifft grob gesagt alle Intel-CPU, die noch kein „Core i“ sind, also Core 2 Duo und Quad sowie davon abgeleitete Pentium-, Celeron- und Xeon-CPU. Das meiste ab dem ersten Core i7, also dem „Nehalem“-Prozessor aus dem Jahr 2008, unterstützt die Befehle – abgesehen von einigen uralten Stromspar-CPU der Atom-Baureihe, die vor allem in Netbooks zum Einsatz kamen. AMD war etwas früher dabei: Ab der Barcelona-Architektur („Phenom“) sind die Befehle unterstützt.

Rechner mit Prozessoren wie Intel Core 2 Duo und AMD Athlon 64 X2 können also voraussichtlich Version 24H2 nicht mehr ausführen. Microsoft kann das für egal halten, denn auch weit neuere Prozessoren bis zum Jahr 2016 werden ebenfalls nicht unterstützt. Die wenigen, die allerdings noch einen PC mit Core 2 Duo oder Ähnlichem nutzen und Windows 11 darauf mittels Tricks installiert haben, werden wohl in die Röhre gucken.

Fazit

So ganz fertig ist Version 24H2 schon deshalb nicht, weil in der EU nach wie vor ein Feature fehlt, um das herum Microsoft zurzeit den meisten Bohei macht: der KI-Copilot für Windows, den Microsoft auch abseits der Insider-Testversionen fleißig

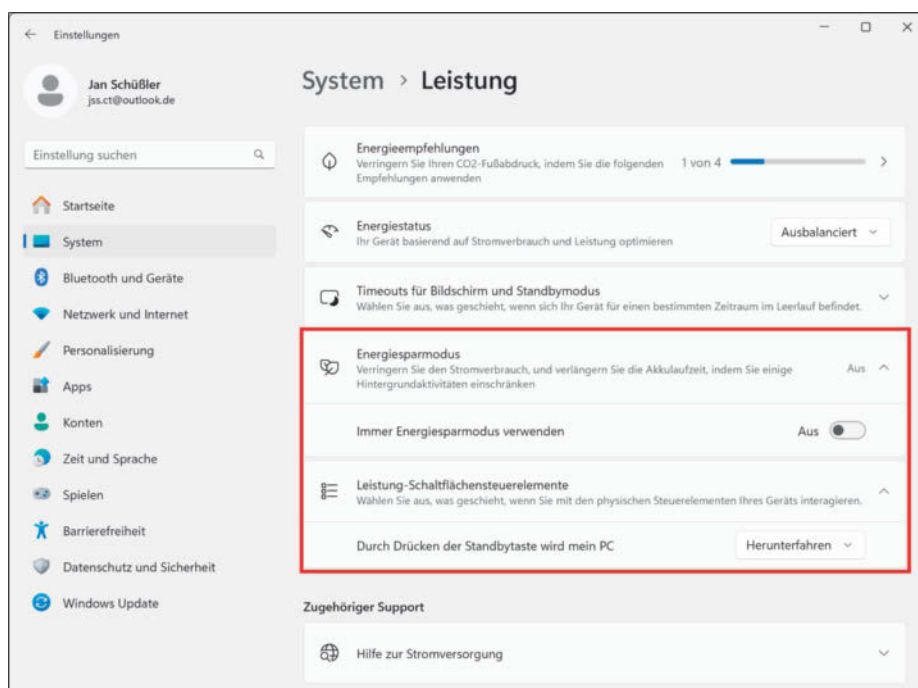
mit neuen Funktionen ausstattet. Ließ sich der Copilot bis vor Kurzem mit einer bestimmten Desktop-Verknüpfung aufrufen, obwohl Microsoft ihn wegen rechtlicher Fragen noch nicht freigegeben hat, klappt das inzwischen nicht mehr. Die Verknüpfung öffnet nicht mehr den Copilot, sondern schlicht ein Edge-Browserfenster. Wann Microsoft die Funktion fit für den Digital Markets Act (DMA) der EU kriegt, steht in den Sternen – wenn Microsoft es selbst zu Version 24H2 nicht schafft, wirds allerdings noch peinlicher, als es ohnehin schon ist.

Davon abgesehen gilt, was bei Funktionsupdates meistens gilt: 24H2 bringt einen ordentlichen Satz neue Funktionen, ein paar alte Features fliegen raus – aber wie gut das Update wirklich ist, wird sich erst im Praxiseinsatz zeigen, wenn Millionen Anwender es auf allen möglichen (und unmöglichen) Rechnern installieren. (jss@ct.de)

Literatur

- [1] Jan Schüßler, Kleines Momentum, „Moment 5“ bringt Windows 11 ein paar neue Funktionen, c't 8/2024, S. 118
- [2] Ernst Ahlers, Schnellstarter, Vier Wi-Fi-7-Basen mit drei Clients getestet, c't 4/2024, S. 50

SMB-Update-Doku: ct.de/yyrm



Den Energiesparmodus gibts künftig auch auf Desktop-Rechnern – nebst ein paar erweiterten Energieoptionen für Schalter- und Deckelaktionen.



Bild: KI Dall-E, Midjourney | Collage ct

Auf Nummer sicher

Lücken in der DNS-Verschlüsselung finden und schließen

Viele Betriebssysteme, Browser und Router können ihre DNS-Anfragen verschlüsseln. Damit schützen sie die Privatsphäre und Sicherheit der Anwender beim Surfen. Blind verlassen sollten Sie sich darauf aber nicht, denn Apps können diese Einstellungen ignorieren und Lücken in das Sicherheitskonzept reißen. Erfahren Sie, wie Sie solche DNS-Lecks aufspüren und stopfen.

Von Ronald Eikenberg

Spätestens seit Snowden ist klar, dass man möglichst alles verschlüsseln sollte, was man durchs Internet schickt. Dies gilt besonders für die DNS-Kommunikation: Sie gibt detailliert Aufschluss

darüber, welche Websites Sie ansteuern und welche Dienste Sie verwenden. Denn mit jeder Website, die Sie aufrufen, verschickt Ihr Browser zahlreiche DNS-Anfragen an einen Resolver, um die IP-Adressen der verwendeten Domains zu erfragen, bevor er diese kontaktieren kann – er fragt zum Beispiel nach heise.de und bekommt als Antwort die IP 193.99.144.80. Darüber hinaus sind die DNS-Anfragen ein gefundenes Fressen für Angreifer, denn wer sie manipulieren kann, der kann Sie auf beliebige Server lotsen.

Die gute Nachricht ist, dass dieses Problem längst gelöst ist und es mehrere Verfahren gibt, um DNS-Verkehr vor Schnüfflern und Angreifern zu schützen: Etwa können aktuelle Betriebssysteme, die meisten Browser und manche Router den DNS-Verkehr bis zum Resolver verschlüsseln. Zu den gängigen Verfahren gehören DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT). Darüber hinaus gibt es das schnelle, aber seltene DNS-over-QUIC (DoQ), das anonymisierende Oblivious-

DNS und noch proprietäre DNS-Verschlüsselungen wie DNSCrypt. [1] Die DNS-Verschlüsselung lässt sich oft mit wenigen Klicks einschalten, etwa in den Windows-Einstellungen.

Es gibt aber auch eine weniger gute Nachricht: Dass die DNS-Verschlüsselung im Betriebssystem eingeschaltet ist, bedeutet nicht, dass alle DNS-Anfragen verschlüsselt sind. Das zeigt der auf Seite 14 beschriebene Fall. Wenn man zum Beispiel in Windows 11 DoH aktiviert, verschicken diverse Chromium-Browser wie Google Chrome und Microsoft Edge ihre DNS-Anfragen unter Umständen trotzdem im Klartext. So können Schnüffler in Internet-Drehkreuzen wie dem DE-CIX und Angreifer im lokalen Netz die Domainnamen der aufgerufenen Websites leicht mitschneiden.

Der Grund: Chromium nutzt nicht länger das Betriebssystem zum Auflösen von DNS-Anfragen, sondern eine eigene Funktion namens Async DNS. Diese liest zwar die IP-Adresse des im Betriebssystem

eingestellten DNS-Resolvers ein, nicht aber die DoH-Konfiguration für die Verschlüsselung. Stattdessen versucht Async DNS anhand einer internen Liste selbst herauszufinden, ob sich der betreffende Resolver verschlüsselt ansprechen lässt. Das scheitert, wenn im Betriebssystem ein Resolver eingestellt ist, der nicht auf der Browser-internen Liste steht. Dann verschlüsseln die Browser Ihre DNS-Anfragen nicht. Das Problem betrifft vornehmlich Windows und macOS. Linux bietet keinen allgemeinen Weg, verschlüsseltes DNS einzuschalten; daher ist die Situation für Linuxer nicht so dramatisch.

DNS-Lecks können auch aus anderen Gründen auftreten. Wenn Sie zum Beispiel im Homeoffice arbeiten und eine VPN-Verbindung ins Firmennetz aufbauen, ändert sich Ihre DNS-Konfiguration. Sämtliche DNS-Anfragen gehen dann möglicherweise nicht mehr verschlüsselt an den von Ihnen eingestellten DNS-Resolver, sondern im Klartext an den Resolver Ihres Arbeitgebers. Er könnte also mitlesen, welche Websites Sie aufrufen.

Kontrolle ist besser

Um solche Überraschungen zu vermeiden, halten Sie sich an das alte Sprichwort „Vertrauen ist gut, Kontrolle ist besser“. Mit etwas Netzwerk-Know-how und gängigen Tools können Sie Klartext-DNS-Anfragen im Netzwerkverkehr aufspüren. Das Werkzeug der Wahl ist das Analyse-Tool Wireshark (siehe ct.de/yc3e), das es für Windows, Linux und macOS gibt. Nach dem Start führt es unter „Aufzeichnen“ die Netzwerkschnittstellen des Systems auf, mit einem Doppelklick auf ein Interface können Sie dessen Verkehr mitschneiden.

Wenn Sie noch unsicher sind, über welches Interface die DNS-Daten trans-

portiert werden, können Sie etwas Verkehr erzeugen, indem Sie eine Datei herunterladen oder den Speedtest [fast.com](https://www.speedtest.net) aufrufen und die kleinen Durchsatzdiagramme rechts neben den Schnittstellen beobachten. Wenn Sie die Strg-Taste gedrückt halten, können Sie auch mehrere Interfaces gleichzeitig auswählen. Das bietet sich zum Beispiel an, wenn neben der Netzwerkverbindung noch eine VPN-Verbindung läuft oder der Rechner gleichzeitig über WLAN und Kabel kommuniziert.

Damit Sie die DNS-Pakete leicht finden, klicken Sie oben in die Filterzeile („Anzeigefilter anwenden ...“), geben `dns` ein und bestätigen mit der Eingabetaste. Jetzt zeigt Wireshark nur noch Klartext-DNS an. Steuern Sie mit den auf Ihrem System installierten Browsern einige Webseiten im Internet an, die sie normalerweise nicht besuchen. So ist gewährleistet, dass Windows die DNS-Daten nicht aus dem Cache holt, sondern den konfigurierten Resolver befragen muss.

Wenn die Paketliste bei Ihnen leer ist, haben Sie die DNS-Verschlüsselung entweder bereits erfolgreich eingerichtet und es gibt keine Lecks oder Sie haben noch nicht am richtigen Interface mitgeschnitten. Um auf Nummer sicher zu gehen, können Sie die Gegenprobe machen, indem Sie den Filter `dns` entfernen und nach Paketen in Richtung des eingestellten DNS-Resolvers schauen, etwa mit dem Filter `ip.dst == 8.8.8.8` für Googles DNS-Resolver.

Wenn Sie einen OpenWrt-Router einsetzen, können Sie den DNS-Verkehr auch dort analysieren, wahlweise für einzelne Clients oder das gesamte Heimnetz. Hierzu installieren Sie den Netzwerksniffer `tcpdump` über die Paketverwaltung von OpenWrt und melden sich anschließend

ct kompakt

- DNS-Anfragen sind ein sensibler Bestandteil Ihres Internetverkehrs.
- Um die DNS-Daten vor Angreifern zu schützen, sollten Sie die Übertragung verschlüsseln, zum Beispiel mit DNS-over-HTTPS.
- Die DNS-Verschlüsselung können Sie leicht einschalten. Es kann jedoch sein, dass Anwendungen sich nicht daran halten.
- Es gibt mehrere Arten, um zu prüfen, ob ein DNS-Leck vorliegt, und für Sicherheit zu sorgen.

über SSH am Router an, um das Tool zu starten. Um zum Beispiel auf dem Bridge-Interface `br-lan` nach Klartext-DNS zu lauschen, können Sie den Befehl `tcpdump -i br-lan port 53` verwenden. Wenn Sie sich nur für einen bestimmten Client interessieren, hängen Sie dessen IP-Adresse mit `and host [Client-IP]` an den Filter an.

Verursacher finden

Windows-Nutzern sei darüber hinaus auch der Process Monitor (kurz Procmon, siehe ct.de/yc3e) von Sysinternals ans Herz gelegt [2]. Das Tool zeigt nicht nur Datei-, Registry- und Prozessaktivitäten an, sondern gibt auch Einblicke in die Netzwerkaktivitäten. Anders als Wireshark verrät es, von welchen Prozessen die Übertragungen ausgehen. Das ist sehr hilfreich bei der Analyse von DNS.

Nach dem Start des Procmon füllt sich die Ereignisliste rasend schnell, da auf einem üblichen PC viele Anwendungen und Prozesse gleichzeitig aktiv sind. Über die fünf Knöpfe ganz rechts in der Toolbar können Sie die Flut eindampfen, indem Sie alle Ereignistypen bis auf Netzwerk (mittiges Symbol) ausblenden.

Interessant ist zunächst die Spalte „Process Name“. Darin steht, von welchem Prozess die Übertragung ausgegangen ist. In der Spalte „Path“ stehen die Absender- und Zieladressen der Netzwerkdaten samt Ports. Anstelle der IP-Adressen setzt Procmon die Hostnamen ein, wenn sie bekannt sind, bei Googles Resolvern etwa `dns.google`. Auch Standardports führt Procmon mit einer Bezeichnung auf: etwa Port 53 als „domain“, Port 443 als „https“.

No.	Time	Source	Destination	Protocol	Length	Info
14426	198.7729...	192.168.178.109	8.8.8.8	DNS	68	Standard query 0xbe5f A heise.de
14427	198.7731...	192.168.178.109	8.8.8.8	DNS	68	Standard query 0xc558 HTTPS heise.de
14429	198.7753...	8.8.8.8	192.168.178.109	DNS	68	Standard query response 0xc558 HTTPS heise.de
14430	198.7753...	8.8.8.8	192.168.178.109	DNS	84	Standard query response 0xbe5f A heise.de A 193.99.144.
14439	198.8033...	192.168.178.109	8.8.8.8	DNS	72	Standard query 0xf1e2 A www.heise.de
14440	198.8035...	192.168.178.109	8.8.8.8	DNS	72	Standard query 0x7633 HTTPS www.heise.de
14441	198.8067...	8.8.8.8	192.168.178.109	DNS	88	Standard query response 0xf1e2 A www.heise.de A 193.99.
14442	198.8070...	8.8.8.8	192.168.178.109	DNS	122	Standard query response 0x7633 HTTPS www.heise.de SOA r
14531	198.9317...	192.168.178.109	8.8.8.8	DNS	77	Standard query 0xf99b A heise.cloudimg.io
14532	198.9319...	192.168.178.109	8.8.8.8	DNS	77	Standard query 0xa066 HTTPS heise.cloudimg.io
14533	198.9322...	192.168.178.109	8.8.8.8	DNS	72	Standard query 0xf8e6 A cmp.heise.de
14534	198.9324...	192.168.178.109	8.8.8.8	DNS	72	Standard query 0x1ca7 HTTPS cmp.heise.de
14535	198.9326...	192.168.178.109	8.8.8.8	DNS	84	Standard query 0x8508 A data-fb7f8b3ae8.heise.de
14536	198.9327...	192.168.178.109	8.8.8.8	DNS	84	Standard query 0x2538 HTTPS data-fb7f8b3ae8.heise.de
14538	198.9401...	8.8.8.8	192.168.178.109	DNS	192	Standard query response 0x1ca7 HTTPS cmp.heise.de CHAN

Der einfache Wireshark-Filter „dns“ fördert ungeschützte DNS-Anfragen im Handumdrehen zutage.

Time	Process Name	PID	Operation	Path	Result
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:55026 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:55336 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Receive	WPRO Jan:55336 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Receive	WPRO Jan:55026 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:55468 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:58034 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Receive	WPRO Jan:55468 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:58034 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Receive	WPRO Jan:55468 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:57439 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Receive	WPRO Jan:57439 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Receive	WPRO Jan:54538 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:54538 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:56374 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:56374 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:56329 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:52532 -> dns.google.domain	SUCCESS
17:48:...	chrome.exe	9088	UDP Send	WPRO Jan:50859 -> dns.google.domain	SUCCESS

Mit dem Process Monitor spüren Sie auch die Verursacher von DNS-Lecks auf. In der Aufzeichnung ist zu sehen, wie Google Chrome ungeschützte DNS-Anfragen nach einem Downgrade-Angriff verschickt.

Um gezielt den DNS-Verkehr auszuwerten, können Sie über den Trichterknopf in der Symbolleiste weiter filtern. Um zum Beispiel Klartext-DNS zu sehen, filtern Sie die Spalte „Path“ nach der Zeichenfolge „domain“: Path contains domain then Include. Nach einem Klick auf „Add“ und einem weiteren auf „OK“ macht sich Procmon an die Arbeit.

Eine weitere Möglichkeit wäre, nach dem Hostnamen des DNS-Resolvers zu filtern, also etwa dns.google. Dann sehen Sie sowohl Klartext-DNS-Pakete in diese Richtung fließen (erkennbar an „domain“ im Path) als auch verschlüsselte DNS-Anfragen („https“ bei DoH).

Nutzen Sie Browser und Apps, um Verkehr zu erzeugen. Wird unter „Process Name“ der Prozess svchost.exe angezeigt, geht die Verbindung von der Windows-Komponente Service Host aus. Dahinter kann sowohl das Betriebssystem stecken als auch Anwendungen wie Firefox, die Windows die DNS-Auflösung überlassen. Verschickt eine Anwendung DNS-Anfragen selbstständig an einen Resolver, taucht deren Name als Prozess

auf, zum Beispiel chrome.exe (Google Chrome).

DNS-Lecks stopfen

Es gibt keine allgemeingültige Empfehlung, wie Sie DNS-Anfragen bestmöglich schützen, da die Vorgehensweise von Ihrem individuellen Nutzungsszenario und Ihren Ansprüchen an die Sicherheit abhängt. Grundsätzlich gilt aber: Irgendetwas sollten Sie tun, denn sonst fließt mit hoher Wahrscheinlichkeit Klartext durchs Internet.

DNS-Verschlüsselung können Sie an vielen Stellen einschalten, etwa im Browser, im Betriebssystem, im Router und in einem DNS-Filter wie AdGuard Home oder Pi-hole. Dort beginnt der zumeist TLS-geschützte Tunnel für Ihre DNS-Anfragen – je näher diese Stelle an der anfragenden Anwendung steht, desto kürzer sind die Daten ungeschützt unterwegs.

Geht es allein um Sicherheit und Privatsphäre beim Surfen, sollten Sie die DNS-Verschlüsselung direkt im Browser einschalten und dort manuell einen Resolver Ihrer Wahl einstellen. So ist sicherge-

stellt, dass niemand mitlesen kann, nicht mal das Betriebssystem oder andere Clients im lokalen Netz. Versucht jemand, die verschlüsselte Verbindung zu verhindern, zeigt Ihr Browser eine Warnung an und verhindert, dass Sie arglos weitersurfen.

Die Kehrseite dieser Medaille ist, dass ein im Heimnetz installierter DNS-Filter die Anfragen nicht erhält und so auch nicht filtern kann. Außerdem kann die Auflösung von Hostnamen aus dem lokalen Netz fehlschlagen. Wenn Sie auf einen Filter nicht verzichten möchten, können Sie einen externen DNS-Resolver einstellen, der das Filtern für Sie übernimmt und Anfragen nach Tracking- und Malware-Domains mit NXDOMAIN (Non-Existent Domain) beantwortet. Filternde Resolver betreiben zum Beispiel dnsforge, Mullvad und AdGuard DNS (siehe ct.de/yc3e).

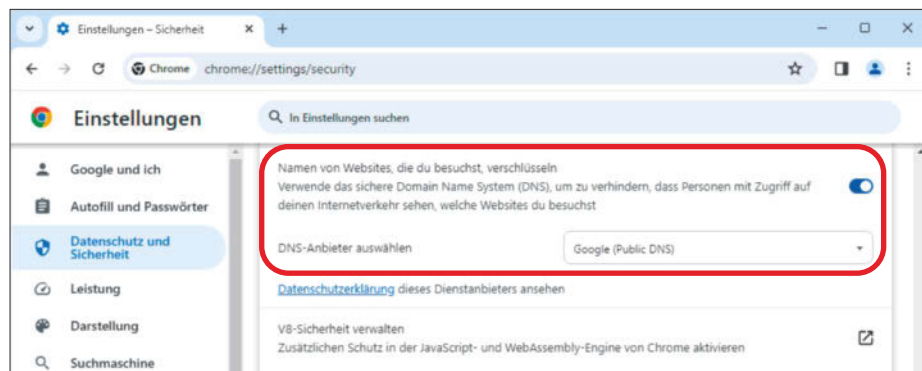
Noch datenschutzfreundlicher ist es, selbst einen filternden Resolver im Heimnetz zu installieren, den Sie verschlüsselt ansprechen können. AdGuard Home etwa können Sie so konfigurieren, dass es lokal sowohl über DoH als auch über DoT erreichbar ist und auch ausgehende DNS-Anfragen verschlüsselt. Netzwerkprofis können Nginx als DoH- oder DoT-Gateway für Unbound verwenden (siehe ct.de/yc3e).

Browser-Konfiguration

Um DNS-over-HTTPS in Google Chrome scharf zu schalten, öffnen Sie die Browser-Einstellungen und wählen „Datenschutz und Sicherheit/Sicherheit/Erweitert“. Der Schalter „Sicheres DNS verwenden“ muss eingeschaltet sein. Unter „DNS-Anbieter auswählen“ ist im Klappmenü die unsichere Option „Standardeinstellung des Betriebssystems (falls verfügbar)“ voreingestellt. Klicken Sie darauf, um einen der vorgegebenen DoH-Resolver auszuwählen oder einen eigenen einzugeben („Benutzerdefinierten DNS-Dienstanbieter hinzufügen“).

In anderen Chromium-Browsern ist das Vorgehen ähnlich; durchsuchen Sie die Browser-Einstellungen am besten nach „DNS“, um die richtige Stelle zu finden. Firefox-Nutzer konfigurieren DNS-over-HTTPS in den Browser-Einstellungen unter „Datenschutz & Sicherheit/DNS über HTTPS“. Damit ausschließlich verschlüsseltes DNS zum Einsatz kommt, wählen Sie „Maximaler Schutz“.

Zusätzlich können Sie auch im Betriebssystem einstellen, dass es DNS-Anfragen verschlüsseln soll. Das wirkt sich



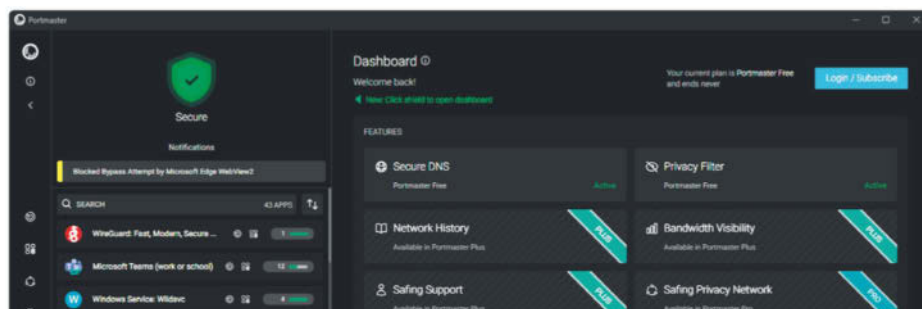
Wenn Sie sicherstellen wollen, dass Chrome seine DNS-Anfragen tatsächlich verschlüsselt, müssen Sie in dessen Einstellungen die Verschlüsselung einschalten und zudem einen Resolver festlegen.

nicht nur auf das Betriebssystem aus, sondern auch auf alle Anwendungen und Dienste, die die DNS-Auflösung dem System überlassen. Unter Windows ist das besonders einfach: Öffnen Sie die Windows-Einstellungen, klicken Sie auf „Netzwerk und Internet“ und dann auf „WLAN“ oder „Ethernet“. Um zum Beispiel einen DNS-Resolver für alle WLAN-Verbindungen einzustellen, wählen Sie anschließend „Hardwareeigenschaften“ und klicken dann bei „DNS-Serverzuweisung“ auf „Bearbeiten“. Normalerweise ist dort „Automatisch (DHCP)“ eingestellt, wodurch Ihr Rechner die DNS-Anfragen vom Router auflösen lässt. Wählen Sie stattdessen „Manuell“, aktivieren Sie den Schalter für IPv4 und geben Sie eine Resolver-IP wie 9.9.9.9 (Quad9) als bevorzugten DNS ein. Eine Liste von offenen, verschlüsselnden Resolvern finden Sie über ct.de/yc3e. Darunter sind auch mehrere, die zum Absichern die Signaturtechnik DNSSEC verwenden und auch nicht mitschreiben, welche Client-IP-Adresse welche DNS-Anfragen verschickt.

Danach ändern Sie „DNS über HTTPS“ auf „Ein (automatische Vorlage)“, woraufhin Windows das Feld „DNS über HTTPS-Vorlage“ im besten Fall automatisch ausfüllt. Diese Vorlage definiert, über welchen DoH-Dienst die Anfragen aufgelöst werden sollen. Windows kennt derzeit Vorlagen für Google, Cloudflare und Quad9. Wenn Sie einen anderen Resolver verwenden möchten, können Sie „Ein (manuelle Vorlage)“ wählen und die Vorlagen-URL von Hand eingeben (siehe ct.de/yc3e). Den Schalter „Fallback auf Klartext“ lassen Sie aus, damit Windows keine ungeschützten DNS-Anfragen verschickt.

Aber Achtung: Falls „das Internet mal nicht geht“, dann sollten Sie zuallererst prüfen, ob der eingestellte DoH-Resolver noch erreichbar ist. Falls nicht, müssen Sie ebenfalls per Hand einen anderen eintragen. Um die Handarbeit zu reduzieren, empfiehlt es sich, darunter einen alternativen DNS-Resolver einzustellen. Der springt dann ein, wenn der erste ausfällt oder zu langsam antwortet. Das kann ein Resolver eines anderen Betreibers sein oder auch eine alternative Adresse des ersten. Die meisten Resolveranbieter betreiben komplexe Infrastrukturen, von denen Teile als Fallback eingerichtet sind.

Das Gleiche gilt für die DNS-Kommunikation per IPv6: Wenn Sie den Schalter „IPv6“ umlegen, können Sie zwei Konfi-



Die Datenschutz-Firewall Portmaster fängt Klartext-DNS-Anfragen auf Ihrem System ab und schickt sie DoH-verschlüsselt an den Resolver Ihrer Wahl.

gurationen für Resolver eintragen, die über v6 erreicht werden. Wenn Sie es eilig haben, reicht es fürs Erste, den bevorzugten v4-Resolver einzustellen.

Android verschlüsselt den DNS-Verkehr seit Version 9 gemäß DoT, seit Version 11 alternativ auch gemäß DoH. Sie können die DNS-Verschlüsselung in den Einstellungen unter „Netzwerk und Internet/Private DNS“ einrichten. Wenn Sie ein Apple-Betriebssystem nutzen, können Sie DNS-Verschlüsselung am einfachsten über ein Konfigurationsprofil einrichten, das Sie etwa unter ct.de/yc3e für verschiedene Resolver herunterladen können. Unter Linux können Sie zum Beispiel den Systemdienst `systemd-resolved` für DNS-Verschlüsselung einrichten oder Sie installieren einen Resolver wie Stubby.

Auch Fritzboxen und andere Router können DNS-Anfragen verschlüsseln. Die DoT-Einrichtung auf Fritzboxen haben wir in c't 22/2020 beschrieben [3].

Insbesondere Nutzer der Desktop-Versionen von Chrome, Edge und anderen Chromium-Browsern sollten zusätzlich DoH mit einem festen Resolver im Browser konfigurieren, weil solche Browser Ihre DNS-Anfragen eigenständig auflösen und dabei eine andernorts eingestellte DNS-Verschlüsselung umgehen können (siehe Seite 14). Bei Electron-Apps wie Visual Studio Code, Obsidian, Signal und Slack, die durch ihre Chromium-Engine ebenfalls davon betroffen sind, haben Sie jedoch keinen Einfluss darauf.

DNS-Firewall

Abhilfe kann zum Beispiel die auf Datenschutz getrimmte Firewall-Software Portmaster [4] bringen. Sie fängt auf Ihrem System sämtliche DNS-Anfragen ab und schickt Sie DoH-verschlüsselt an einen Resolver Ihrer Wahl. So ist sichergestellt, dass Ihr System keine Klartextanfragen verschickt. Darüber hinaus filtert die Fire-

wall Ihre Anfragen lokal anhand gängiger Tracker- und Malware-Listen, ähnlich AdGuard Home oder Pi-hole.

Anonyme Anfragen

Eine DNS-Verschlüsselung stellt sicher, dass nur der DNS-Resolver Ihrer Wahl erfährt, für welche Domains Sie sich interessieren. Dieser kann Ihre Anfragen aber prinzipiell mitschreiben und auswerten. Wenn Sie das verhindern möchten, können Sie technisch ausschließen, dass die Anfragen Ihrer IP-Adresse zugeordnet werden. Hierzu können Sie zum Beispiel einen DNSCrypt-Proxy installieren oder Anonymisierungsdienste wie Apples Private Relay oder Google One VPN verwenden, die nicht nur Ihren DNS-Verkehr, sondern den gesamten Internettraffic verschleiern [5].

Fazit

DNS-Anfragen sind ein sensibler Teil Ihres Internetverkehrs. Daher ist es sinnvoll, diese Daten zu verschlüsseln, damit sie niemand mitlesen oder manipulieren kann. Wichtig ist jedoch, dass Sie sich nicht blind darauf verlassen, nachdem Sie die Verschlüsselung aktiviert haben. Werfen Sie besser einen prüfenden Blick auf Ihren DNS-Traffic, um etwaige Klartextlecks aufzuspüren und gezielt stopfen zu können. (rei@ct.de) **ct**

Literatur

- [1] Dušan Živadinović, FAQ: Verschlüsselte DNS-Anfragen, c't 22/2021, S. 178
- [2] Axel Vahldiek, Unter dem Mikroskop, Windows analysieren mit dem Process Monitor – Teil 1, c't 16/2017, S. 148
- [3] Dušan Živadinović, Vertrauliche Auskunft, Mit Fritzboxen beim Surfen die Privatsphäre schützen, c't 22/2020, S. 22
- [4] Ronald Eikenberg, Hafenmeister, Datenschutz-Firewall Portmaster, c't 6/2024, S. 76
- [5] Dušan Živadinović, Wahl der Waffen, Abwehrmaßnahmen gegen Datenhaie, c't 16/2022, S. 20

Tools & Infos: ct.de/yc3e

Für Wissenshungrige...

Ausgewählte Fachliteratur

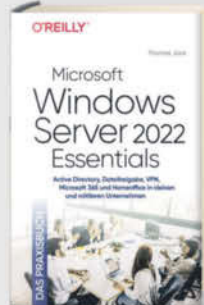


Mareile Heiting **Windows 11 – Das große Handbuch (5. Auflage)**

Das große Standardwerk zu Windows 11! In diesem umfassenden Handbuch erfahren Einsteiger und bereits versierte Nutzer alles, um das Betriebssystem in seiner neuesten Version sicher und effektiv zu handhaben.

19,90 €

NEU



Thomas Joos **Microsoft Windows Server 2022 Essentials – Das Praxisbuch**

Dieses Buch hilft kleinen und mittleren Unternehmen, das Beste aus Windows Server 2022 Essentials herauszuholen, auch bei kleinerem Budget. Mit vielen Praxisbeispielen und detaillierten Anleitungen.

Auch als PDF und ePub erhältlich!

49,90 €

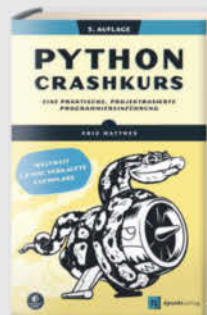


Charles Petzold **Code – Wie Computer funktionieren**

Charles Petzold lüftet das Geheimnis über das verborgene Innenleben und die grundlegende Funktionsweise von Computern – von der Hardware bis zur Software.

Auch als PDF und ePub erhältlich!

39,99 €



Eric Matthes **Python Crashkurs (3. Auflage)**

DER weltweite Bestseller unter den Einführungen in die Programmiersprache Python. Mit dieser kompakten und gründlichen Anleitung werden Sie in kürzester Zeit Programme schreiben, Probleme lösen und funktionierende Anwendungen entwickeln.

Auch als PDF und ePub erhältlich!

32,90 €

BEST-SELLER



Christian Immler **Haus und Wohnung smart vernetzt**

Ob Sie Daten, Musik und Medien im ganzen Haus nutzen, Ihr WLAN optimieren oder per App aus der Ferne Ihre Heizung anstellen, diese und weitere relevante Themen rund um Ihr vernetztes Zuhause werden in diesem Buch ausführlich besprochen.

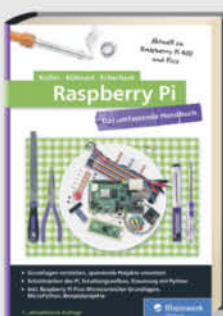
19,95 €



Thomas Kaffka **3D-Druck – Praxisbuch für Einsteiger (3. Auflage)**

Entdecken Sie die nahezu unbegrenzten Möglichkeiten des 3D-Drucks in allen Varianten: vom Einsatz des eigenen 3D-Druckers zu Hause über die Verwendung von öffentlich zugänglichen Druckern bis hin zur Nutzung von 3D-Druckservices.

29,99 €



Michael Kofler, Charly Kühnast, Christoph Scherbeck **Raspberry Pi (7. Auflage)**

Das Standardwerk in 7. Auflage, aktuell zum Raspberry Pi Pico. Die RasPi-Experten Michael Kofler, Charly Kühnast und Christoph Scherbeck bieten Ihnen auf über 1.000 Seiten das komplette Wissen, damit Sie mit dem Raspberry Pi richtig durchstarten.

44,90 €



Anatomie 4D – Der menschliche Körper

Mithilfe einer kostenlosen App und bahnbrechender Augmented Reality kann der Aufbau der Knochen, die Muskeln in Aktion, das Nerven- und Kreislaufsystem sowie das größte menschliche Organ, die Haut, beobachtet werden.

14,95 €



shop.heise.de/highlights2024

PORTOFREI AB 20 € BESTELLWERT INNERHALB DEUTSCHLANDS



Zubehör und Gadgets



Oxocard Galaxy Play & Explore

Mit dem leistungsfähigen Dual-Core Chip ESP32 liefert die Oxocard genügend Power für Ihre Experimente. Dank fertiger Programme können Sie ohne Programmiererfahrung sofort loslegen. Wir zeigen wie durch einfache Anpassungen verblüffende Effekte erzeugt werden können.

~~69,90 €~~

39,90 €



Oxocard Connect Innovators Kit

Steigen Sie in die faszinierende Welt der Elektrotechnik ein. Das umfangreiche Komplettsset enthält neben einer Oxocard Connect und einer Breadboard-Cartridge, 96 Elektronikbauteile, mit denen Sie eine Vielzahl elektronischer Schaltungen aufbauen können.

89,90 €



Makey-Flasche mit Trinkhalm

Diese praktische Trinkflasche mit unserem süßen Makey ist ab jetzt dein steter Helfer gegen den Durst. Sie besteht aus hochwertigem Edelstahl und hat einen praktischen Trinkhalm im Deckel integriert.

29,90 €



musegear finder recharger

Der finder ist das perfekte Geschenk. Ob Schlüssel, Geldbörse, Fernbedienung, Handy oder Tablet – der finder lässt sich dank mitgeliefertem Klebepad und Befestigungsband überall anbringen und findet per App alles wieder!

34,90 €



Joy-IT Werkzeugset

115-teiliges Werkzeugset für die Reparatur von feinelektronischen Geräten, wie Smartphones und Spielekonsolen. Darin enthalten sind, neben insgesamt 98 Bits aus hochwertigem S2 Werkzeugstahl, Hilfsmittel zum gefahrlosen Öffnen, Greifen und Hebeln.

24,90 €



Bondic® UV-Reparatursystem

Das weltweit erste innovative UV-Reparatursystem mit Flüssigkunststoff zum Reparieren, Fixieren, Modellieren und Isolieren. Mit Bondic® kannst du Bruchstellen in Sekunden ausfüllen, unter UV-Licht aushärten und danach beliebig bearbeiten.

18,90 €



Strahlungsmessgerät Joy-IT JT-RAD01

Das JT-RAD01 ist ein Strahlungsmessgerät zum Nachweis von γ -, β - und Röntgenstrahlung und zeichnet sich durch seine besonders einfache Handhabung, hohe Messstabilität und seinem handlichen und robusten Design aus. Das Messgerät verfügt über ein großes LCD Farb-Display mit Hintergrundbeleuchtung.

74,90 €



c't 1983 Emaille-Tasse

Kaffee trinken wie in alten Zeiten. Diese Tasse im Retro-Look und mit dem Logo aus den ersten zwei Jahren c't Magazin sorgt für Nostalgie-Momente am Frühstückstisch. Geben Sie sich mit dieser Kaffeetasse als Fan der ersten Stunde zu erkennen.

26,90 €



Bild: KI Midjourney | Collage c't

Eigenverantwortung

Nach der CWA: Corona digital im Blick behalten

Die Corona-Warn-App bot digitale Unterstützung bei der Pandemiebekämpfung. Sie warnte bei Risikokontakten, sicherte Test- und Impfzertifikate und lieferte aktuelle Daten zur Infektionslage. Heute sind die Infektionsschutzmaßnahmen beendet und die CWA ist stillgelegt. Doch es bleibt weiterhin wichtig, Infektionen zu vermeiden – und auch ohne CWA gibt es im digitalen Raum fundierte Anlaufstellen, um Covid-19 im Blick zu behalten.

Von Kathrin Stoll

Zum Glück ist die Corona-Pandemie vorbei, jetzt gibt es Diskussionen darüber, wie diese Ausnahmesituation gemanagt wurde, funkt der WDR5, „Laschet fordert Corona-Aufarbeitung“, schreibt der Tagesspiegel. „Corona-Pandemie war Homeoffice-Zeit“, konstatiert Der Westen. Formulierungen wie diese erwecken den Eindruck, die Corona-Pandemie sei vorbei.

Richtig ist, dass die World Health Organization (WHO) die pandemische *Notlage* am 5. Mai 2023 für beendet erklärt hat. Die Entscheidung stützte das Notfallkomitee der WHO darauf, dass die Zahl der gemeldeten Infektionen dank wirksamer Impfstoffe im Verlauf der vorangegangenen zwölf Monaten zurückgegangen war. Die Zahl der Todesfälle habe abgenommen und der Druck auf die einst

überlasteten Gesundheitssysteme nachgelassen.

Der Abwärtstrend erlaube den meisten Ländern „die Rückkehr zu einem Leben, wie man es vor Covid-19 kannte“, sagte WHO-Generaldirektor Tedros Adhanom Ghebreyesus. Corona habe enormen Schaden in allen Bereichen des globalen Lebens verursacht. Die Wirtschaft habe gelitten. „Bruttoinlandsprodukte in Milliardenhöhe“ habe die Pandemie ausgelöscht, „Handel und Reiseverkehr gestört, Unternehmen ruiniert und Millionen in die Armut gestürzt“. Er betonte, dass das Virus weiterhin Todesopfer fordert – erst in der Woche vor Beendigung der pandemischen Notlage sei noch immer alle drei Minuten ein Mensch an Covid-19 gestorben. Das Virus verändere sich – das Risiko, dass neue Varianten entstünden,

die Infektionszahlen und Todesfälle wieder ansteigen ließen, bleibe bestehen. Während er spreche, kämpften weiterhin Tausende Menschen auf den Intensivstationen um ihr Leben. Millionen weitere würden in absehbarer Zukunft „mit schwerwirkenden Folgeerscheinungen, dem sogenannten Long Covid“ zu kämpfen haben.

Eine Schätzung kommt auf eine Zahl von 65 Millionen Patienten weltweit. Auch ein milder Corona-Verlauf kann offenbar eine Vielzahl möglicherweise bleibender Organschäden verursachen. Gerade die Altersgruppe zwischen 36 und 50 Jahren – unter Menschen dieses Alters gibt es offenbar die meisten Infektionen – ist besonders betroffen. Infolge einer Infektion können Erkrankungen wie Diabetes Typ 2, chronische Müdigkeit (ME/CFS) und Dysautonomie auftreten. Es wird davon ausgegangen, dass diese Corona-induzierten Erkrankungen ein Leben lang anhalten können. In Deutschland verursachen Corona-Spätfolgen und allgemein der hohe Krankenstand von im Schnitt 20 Fehltagen pro Person (2023) hohe volkswirtschaftliche Kosten: Laut einer Studie des Verbands der forschenden Pharma-Unternehmen (VfA) haben krankheitsbedingte Ausfälle zu Steuermindereinnahmen von etwa 15 Milliarden Euro geführt. Auch die Krankenversicherungen haben gelitten. Laut eines Berichts der Rheinischen Post belaufen sich deren Mindereinnahmen der Jahre 2022 und 2023 auf fast 15 Milliarden Euro.

Forschungsergebnisse legen nahe, dass jede weitere Covid-19-Infektion das Risiko erhöht, an Long Covid zu erkranken. Im Januar 2023 äußerte Gesundheitsminister Karl Lauterbach gegenüber der Rheinischen Post, dass es bedenklich sei „was wir bei Menschen beobachten, die mehrere Corona-Infektionen gehabt haben.“ Wer nach zwei Infektionen ein stark gealtertes Immunsystem habe, sollte weitere vermeiden.

Keine Maßnahmen, keine App

In Deutschland sind die Infektionsschutzmaßnahmen seit dem 7. April 2023 offiziell aufgehoben. Mit dem Wegfallen der Kontaktbeschränkungen verlor auch das digitale Herzstück der Maßnahmen, die Corona-Warn-App [1], ihren Zweck. Denn die Kernfunktion der CWA, die Kontaktverfolgung, gibt es seitdem nicht mehr. Am 30. April 2023 wurde die Funktion abgeschaltet, im Juli 2023 wurde sie in den

Schlafmodus versetzt. Am 18. September 2023 schalteten Apple und Google die zur Kontaktverfolgung erforderliche „Exposure Notification Framework“-Schnittstelle in Android und iOS ab.

Seither gibt es keine roten Warnungen im Fall einer Risikobegegnung mehr, Testergebnisse können nicht mehr über die App geteilt werden und auch das Dashboard, das über das aktuelle regionale Infektionsgeschehen informierte, ist weg. Nutzen kann man derzeit noch das Kontakttagebuch und die Impfausweisfunktion, außerdem verweisen externe Links auf den Corona-Pandemie-Radar des RKI, die Warn-App NINA des Bundesamts für Bevölkerungsschutz und die FAQ zur App.

Insgesamt hatte die CWA eine hohe Adoptionsrate: Bis eine Woche vor der Abschaltung der Kontaktverfolgung am 30. April 2023 verzeichnete die App 48,67 Millionen Downloads.

„Hat geholfen, Infektionsketten zu durchbrechen“

In der FAQ bezeichnet die Bundesregierung die CWA als Erfolg: Allein im Jahr 2022 haben Schätzungen zufolge mindestens 25 Millionen Menschen die App genutzt. 270 Millionen Testergebnisse wurden digital über die App geteilt, darunter insgesamt neun Millionen positive Testergebnisse. Sie habe geholfen, Infektionsketten zu durchbrechen.

Eine wissenschaftliche Abhandlung, die den Erfolg der Corona-Warn-App unter sozioökonomischen Gesichtspunkten evaluiert, bestätigt das. Die Verfasser benennen 1,41 Millionen Infektionen, 17.200 Krankenhausaufnahmen, 4600 Aufnahmen auf Intensivstationen und 7200 Todesfälle, die die App in der Zeit zwischen Juni 2020 und April 2022 verhindert habe. Nach Abwägen von Kosten und Nutzen käme die CWA auf einen Kapitalwert von 765 Millionen Euro. Effektivität und Effizienz der CWA seien maßgeblich von der hohen Adoptionsrate in der Bevölkerung und der hohen Anzahl positiver Testergebnisse, die über die App geteilt wurden, beeinflusst worden.

Die Abschaltung der Kontaktverfolgung begründet das Bundesministerium für Gesundheit in einer E-Mail an c't mit der Entwicklung der Pandemie und verweist auf die FAQ zur App. Dort heißt es: „Angesichts einer gewachsenen Immunität der Bevölkerung, leicht übertragbarer Virusvarianten und der Rückkehr zu einem öffentlichen Leben (weitgehend)

ohne Corona-Maßnahmen entfällt momentan der Bedarf an einer App zur Kontaktnachverfolgung.“

Viruslast im Abwasser

Um das Infektionsgeschehen zu analysieren, habe man in der Pandemie das Meldesystem (Demis) verbessert und den Pandemieradar aufgebaut. Dieser erfasst die wichtigsten Indikatoren für die Beurteilung des Infektionsgeschehens. Derzeit erfasst man dafür die Viruslast im Abwasser der Haushalte, die Anzahl der Arztbesuche, Krankenhausaufnahmen und Todesfälle. Außerdem wird anhand der Auslastung der Intensivstationen, Normalstationen und Notaufnahmen die Belastung des Gesundheitssystems abgebildet.

Aktuell übermittelt eine wechselnde Anzahl von Kläranlagen Abwassermessungen an das RKI. Wer mit Sars-CoV-2 infiziert ist, scheidet das Virus mit Stuhl, Urin oder Speichel aus. Über an Probenentnahmen aus dem Abwasser durchgeführte PCR-Tests stellen Wissenschaftler die Viruslast je Liter Abwasser fest. Repräsentativ ausgewählt sind die Kläranlagen laut dem Nachrichtenmagazin Stern aber nicht.

Die ermittelten Werte lassen Rückschlüsse auf die Infektionsdynamik zu. Laut den US-amerikanischen Centers for Disease Control and Prevention lassen Abwassermessungen Erkenntnisse über die Ausbreitung des Virus zu, bevor Tests durchgeführt werden und bevor Menschen erkranken. Sie sagen aber nichts darüber aus, wie viele Menschen genau an Corona erkrankt sind – je nach Variante und Fortschritt der Infektion scheiden Infizierte mal mehr, mal weniger Viren aus.

c't kompakt

- Die Corona-Warn-App befindet sich seit Juni 2023 im Sleep-Modus. Die Corona-Infektionsschutzmaßnahmen sind aufgehoben.
- Das Coronavirus ist immer noch da, Infektionen sollte man weiterhin vermeiden.
- So verschafft man sich einen Überblick über Infektionslage, Forschung und Handlungsempfehlungen.



Seit dem 26. Mai 2022 wird das Infektionsgeschehen anhand von Messungen der Viruslast im Abwasser erfasst.

Auch das Bundesministerium für Arbeit und Soziales (BMAS) empfiehlt die Daten aus dem Pandemieradar zur Beurteilung des Infektionsgeschehens. Als wichtiger Beitrag zur Verhinderung von Atemwegsinfektionen könnten bei hohem Infektionsaufkommen betriebsbedingte Personenkontakte reduziert werden. Etwa durch die verstärkte Nutzung digitaler Kommunikation, die Verringerung gleichzeitig in Innenräumen anwesender Personen und die Verlagerung von Arbeitsplätzen ins Homeoffice. Empfohlen wird weiterhin die Einhaltung der Hygiene- und Abstandsregeln, in der Nähe besonders gefährdeter Personen das Tragen von Masken und regelmäßiges Lüften.

Verpflichtend sind die Empfehlungen nicht: Mit der schrittweisen Aufhebung der Corona-Schutzmaßnahmen bis zum 7. April 2023 entfiel neben der Maskenpflicht auch die Isolationspflicht im Fall einer Coronainfektion. Wer sich trotz Corona fit fühle, dürfe seitdem wieder zur Arbeit gehen, erklärten Arbeitsrechtsexperten in Medienberichten.

Winterliche Infektionswelle

Im Frühjahr und Sommer 2023 schien es kurzzeitig, als ginge die Strategie, auf staatlich verordnete Infektionsschutzmaßnahmen zu verzichten, auf. Die niedrigste Viruslast seit Beginn der Messungen bis heute wies das Abwassermonitoring in der Woche vom 22. bis 28. Juni 2023 mit 22.000 Erbguteinheiten pro Liter Abwasser aus. Im Winter änderte sich das. Mitte Dezember 2023 kletterte der Wert auf 618.000 Einheiten pro Liter.

Die Zahlen legen eine Infektionswelle nahe, die um ein Vielfaches größer gewesen sein könnte als zur Zeit der Aufhebung der Infektionsschutzmaßnahmen. Auch international erreichte die im Abwasser gemessene Viruslast im Dezember 2023 bedenkliche Ausmaße. Experten nahmen die Daten zum Anlass, erneut vor Covid-19 zu warnen.

Eric Topol, Professor für Molekularmedizin und Chef in einer NGO namens Scripps Research, äußerte in der LA Times, man mache sich weiterhin vor, dass die Pandemie vorbei sei, dass der Schweregrad einer Covid-19-Infektion dem einer Erkältung gleichkomme und dass das Leben zur Normalität zurückgekehrt sei. Traurigerweise sei das nicht wahr. Die hohe Anzahl der Infektionen in der aktuellen Welle werde dazu führen, dass noch mehr Menschen an Long Covid erkranken.

Dr. Maria van Kerkhove, ein führendes Mitglied der WHO, twitterte, dass Covid-19 immer noch „eine globale Gesundheitsbedrohung“ sei. Die Zahl der Fälle nehme seit Monaten zu, Krankenhäuser seien vielerorts belastet. „Es ist immer noch eine Pandemie, die viel zu viele (Re-)Infektionen, Krankenhausaufenthalte, Todesfälle und langwierige Krankheitsverläufe verursacht, obwohl es Mittel gibt, um sie zu verhindern“. Regierungen und Einzelpersonen dürften nicht in Selbstgefälligkeit verfallen.

Informiert bleiben

Im Frühjahr 2024 hat sich die Lage entspannt. In der zwölften Kalenderwoche betrug die SARS-CoV-2-Viruslast 40.000 Genkopien pro Liter Abwasser, ein Wert,

der seit vier Wochen stabil ist. Es ist jedoch davon auszugehen, dass sich das wie in den Jahren davor zum Herbst wieder ändern könnte. Wer informiert bleiben will, kann neben dem Pandemieradar die Webseiten von Gesundheitsministerium und RKI konsultieren. Auch die Webauftritte der WHO, des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten und das Coronavirus-Portal der UN bieten gesicherte Daten und Empfehlungen zum Umgang mit dem Virus.

Auf weitere verlässliche Informationsquellen verweist zum Beispiel die Coronavirus-Webseite des Ärztlichen Zentrums für Qualität in der Medizin. Neben den Corona-Informationen offizieller Stellen wie RKI und WHO verlinkt das Portal zahlreiche Quellen, die Antworten auf Alltagsfragen zum Umgang mit Corona bieten, Artikel in leichter Sprache und für Kinder sowie Faktenchecks und medizinische Fachpublikationen. Aktualisiert wurde die Linksammlung zuletzt im August 2023 und auch einige der verlinkten Websites werden nicht mehr gepflegt. Als Einstieg in eine Netzrecherche zur Klärung von Corona-bezogenen Fragen eignet sich das Angebot jedoch weiterhin.

Wer sich für den aktuellen Stand der Forschung interessiert, findet im LitCovid-Repository der US-amerikanischen National Library of Medicine die wahrscheinlich umfangreichste Sammlung wissenschaftlicher Arbeiten zum Thema Covid-19. In acht Rubriken untergliedert, kann man derzeit 406.445 Forschungsarbeiten über Virus, Transmission, Behandlungsansätze, Impfungen, die Wirksamkeit nichtmedizinischer Maßnahmen oder Long Covid durchsuchen. Mittels KI wird das Angebot laufend aktualisiert. Es richtet sich in erster Linie an medizinisches Fachpersonal – wer zum Beispiel die eigenen Long-Covid-Symptome in einem Paper wiedererkennt, sollte von einer Selbstdiagnose oder -behandlung absehen und darüber mit einem Arzt oder Apotheker sprechen. (kst@ct.de)

Literatur

- [1] Hartmut Gieselmann, Jo Bager, FAQ: Corona-Warn-App c't 15/2020, S. 50

Quellen, Webangebote der Gesundheitsbehörden und LitCovid-Sammlung:
ct.de/y7r2

WIR SIND NICHT NUR NERDS. WIR SIND AUCH VOM FACH.

Jetzt 5 × c't lesen


für 19,50 €
statt 25,75 €*

* im Vergleich zum Standard-Abo

**30%
Rabatt!**



c't MINIABO DIGITAL AUF EINEN BLICK:

- 5 Ausgaben digital in der App, im Browser und als PDF
- Inklusive Geschenk nach Wahl
- Mit dem Digitalabo Geld und Papier sparen 
- Zugriff auf das Artikel-Archiv

Jetzt bestellen:
ct.de/nerdwissen



Grundlagen Thunderbolt

Die Konzepte und Entwicklungen hinter dem schnellen Verbindungsstandard

Mit Thunderbolt verbindet man Monitore, externe SSDs und weitere Peripherie mit Notebook oder PC. Dabei ist Thunderbolt universeller und meistens auch zuverlässiger als das allgegenwärtige USB – auch wenn es die gleichen Buchsen nutzt.

Von Lutz Labs

USB gibt es seit mehr als 25 Jahren, und der Anschluss von Maus und Tastatur gelingt seit langer Zeit über die immer noch gleichen Stecker. Mit den schnelleren Versionen ab USB 3.0 und dem Wechsel auf den Anschluss per Typ C avancierte USB zum Universalverbinder für diverse Peripherie, vom Monitor über flotte SSDs bis hin zum Ladeanschluss für Notebooks. Andere Standards für Peripheriegeräte wie FireWire oder eSATA wurden vollständig von USB verdrängt.

Die ähnliche Schnittstelle Thunderbolt ist im PC-Bereich weniger verbreitet, Mac-User nutzen sie dagegen schon seit Jahren. Thunderbolt-Verbindungen gelten als weniger stör anfällig, was vor allem bei professionellen Anwendungen wichtig ist. Die stärkere Verbreitung im Mac-Umfeld mag auch daran liegen, dass Apple-Nutzer eher bereit sind, die höheren Preise für Thunderbolt-Geräte zu bezahlen.

Aber auch auf dem Mac gab es Veränderungen: Mit dem Übergang von Version 2 auf Version 3 nutzt Thunderbolt die mittlerweile auch bei USB üblichen Buchsen und Stecker nach Typ C. Es gibt zwar Adapter, die Thunderbolt-2-Geräte an neuere Buchsen anbinden, doch dürfte

sich deren Anschaffung nur für wenige Sonderfälle lohnen.

Über die Typ-C-Stecker passen Thunderbolt-Geräte damit zwar mechanisch an USB-Buchsen und umgekehrt. Reine Thunderbolt-Geräte, etwa SSDs, funktionieren jedoch am USB-Port nicht, während USB-Geräte am Thunderbolt-Port meistens doch funktionieren; dazu gleich mehr.

Das kann Thunderbolt

Thunderbolt – im Folgenden sprechen wir nur noch über die Versionen 3 und höher – nutzt vier Adern für die Datenübertragung. Damit lassen sich Geräte anbinden, die direkt mit PCIe arbeiten, etwa Grafikkarten oder Gehäuse mit einem PCIe-Slot für besondere Steckkarten. Mit solchen Gehäusen lassen sich beispielsweise Notebooks um eine Einsteckkarte erweitern.

Die Übertragungsrate von Thunderbolt liegt bei 40 Gbit/s, allerdings sichert Version 3 bei der Datenübertragung lediglich 16 Gbit/s zu. Das reicht trotzdem für hohe Übertragungsraten, weil die Übertragung von Video, Audio und Daten granular in Paketen abgewickelt wird, die über einen gemeinsamen Träger laufen. Beim USB-Docking über USB-C werden

die Aderpaare hingegen unflexibel starr der Übertragung von USB-Daten oder Video signalen zugeordnet – egal ob die Leitung grade benötigt wird oder Restkapazitäten für etwas anderes frei hätte.

Anders als bei USB, wo vieles unverbindliche Optionen sind, schreibt Thunderbolt vieles explizit vor. Thunderbolt 4 etwa legt unabhängig von der Datenübertragung verbindlich fest, dass eine solche Buchse zwei 4K-Monitore mit der Bildwiederholfrequenz von 60 Hz oder alternativ einen der seltenen 5K-Monitore mit 60 Hz ansteuern können muss. Prinzipiell sind Bildwiederholraten bis 120 Hz möglich, dann aber nur mit einem 4K-Monitor.

Wer mehr als ein Thunderbolt-Gerät anschließen möchte, kann dies bei TB3 wie auch in früheren Revisionen nur in Form einer sogenannten Daisy-Chain tun: Am Ausgang eines Gerätes schließt man das nächste an. Dazu haben viele Thunderbolt-Geräte zwei Typ-C-Buchsen; maximal sechs Geräte hintereinander sind möglich. Jeder Thunderbolt-Port liefert eine Leistung von mindestens 15 Watt, um dort angeschlossene Peripherie zu versorgen. Geräte mit höherem Leistungsbedarf benötigen ein eigenes Netzteil.

Thunderbolt beherrscht zudem das Laden von Notebooks über das Datenkabel. Einfache Kabel können wie bei USB-PD bis zu 65 Watt übertragen, für höhere Ladeleistungen sind Kabel mit integriertem Marker notwendig. Grundsätzlich ist das Laden mittels USB-PD 3.1 mit bis zu 240 Watt möglich – das hat mit Thunderbolt aber wenig zu tun, sondern mit der USB-C-Buchse.

Bei Version 4 hat sich einiges geändert. Zwar bleibt die Bruttogeswindigkeit von 40 Gbit/s gleich, die garantierte Nutzdatenrate aber steigt auf 32 Gbit/s. Zugleich steigt die Monitoraufösung auf 8K mit 60 Hz. Hinzu kommt, dass ein Notebook aus dem Schlafzustand aufwa-



Das über 200 Euro teure Thunderbolt-4-Dock (unten) hat im Vergleich zum USB-C-Dock für 50 Euro (oben) zwar nur wenige zusätzliche Funktionen – aber die können den Mehrpreis lohnen. TB4 ermöglicht etwa den Anschluss schnellerer Speichermedien sowie von mehr Displays gleichzeitig.

chen muss, wenn es an einem TB4-Dock hängt und darüber eine Maus- oder Tastatureingabe erfolgt.

Thunderbolt 4 verändert zudem die Topologie: Neben dem Hintereinanderschalten von Thunderbolt-Geräten, dem erwähnten Daisy-Chaining, kann ein Thunderbolt-4-Hub aus einer Thunderbolt-Quelle mehrere Senken erzeugen – auch das erinnert an USB.

Intel als der Erfinder von Thunderbolt hat praktischerweise auch gleich den passenden Hub-Chip im Programm: Der JHL8440 integriert einen Thunderbolt-4-Hub sowie einen USB-Port nach Version 3.2 Gen 2 mit 10 Gbit/s. Dieser Chip sitzt zusammen mit den USB-PD-Chips sowie USB-Hubs in vielen Thunderbolt-Dockingstationen [1].

Erst mit diesen Dockingstationen ist Thunderbolt sinnvoll, denn so reicht ein einziges Kabel zwischen Dock und Notebook für einen komfortablen Arbeitsplatz: Maus und Tastatur hängen arbeitsbereit am Thunderbolt-Dock, zwei große Monitore und der LAN-Anschluss sowie eine schnelle Sicherungs-SSD ebenso, und zugleich lädt sich das Notebook auf.

Thunderbolt 5 setzt vor allem bei der Geschwindigkeit noch eins darauf: 80 Gbit/s soll diese Version schaffen, geeignete Geräte im Lauf des Jahres erscheinen. Interessant ist auch der Bandbreiten-Booster: Dabei schaltet der Controller auf

eine asymmetrische Arbeitsweise mit drei Leitungen in Richtung Client und einer zurück. Daraus folgt eine Geschwindigkeit von 120 Gbit/s, etwa für Monitor-Signale, die Gegenrichtung wird auf 40 Gbit/s „gebremst“.

Thunderbolt ist wie USB abwärtskompatibel. Geräte nach Thunderbolt 3 sollten daher auch an den kommenden 5er-Ports funktionieren, aber nur mit maximal 40 Gbit/s.

Thunderbolt-Kabel

Thunderbolt-Kabel unterscheiden sich in der Beschaltung grundsätzlich nicht von USB-Kabeln. Sie müssen allerdings höhere Frequenzen übertragen und damit gilt: Ein passives Thunderbolt-Kabel funktioniert auch mit USB-Geräten, umgekehrt kann es mit einem USB-Kabel und Thunderbolt-Geräten Schwierigkeiten geben.

Bei Thunderbolt 3 waren für Kabel-längen oberhalb von 50 Zentimetern noch aktive Kabel vorgeschrieben – in manchen Situationen haben passive Kabel aber dennoch funktioniert. Thunderbolt 4 schreibt erst bei Längen oberhalb von zwei Metern aktive Kabel vor, in der Praxis findet man aber selten mehr als 80 Zentimeter. Für deutlich längere Verbindungen haben Unternehmen wie Corning optische Kabel im Angebot. An beiden Enden solcher bis zu 50 Meter langen Kabel sitzen Wandler, weshalb man die Kabel nur für Endgeräte

Thunderbolt-Kabel erkennt man am Blitzsymbol (links); sie taugen auch für USB-C, nicht aber umgekehrt. Die „4“ zeigt an, dass das Kabel auch die Datenraten von TB4 schafft.



mit eigener Spannungsversorgung nutzen kann.

Thunderbolt-Kabel erkennt man an dem Blitzsymbol auf den Steckern, dazu ist meistens die Versionsnummer aufgedruckt. Gelegentlich findet man noch die zusätzliche Angabe der Leistung, die das Kabel übertragen kann, meistens aber erst, wenn das Kabel für mehr als 65 Watt ausgelegt ist.

Aktive Kabel sind grundsätzlich nur für Thunderbolt geeignet. Nutzt man sie als USB-Kabel, reduziert sich die maximale Datenrate auf 5 Gbit/s, also USB 3.0 a.k.a. 3.2 Gen 1. Wie USB ist Thunderbolt vom Design her auf das An- und Abstecken bei laufenden PCs ausgelegt.

Warten auf Thunderbolt 5?

Die aktuelle Thunderbolt-Version ist 4, aber es gibt auch noch viele 3er-Modelle bei den Händlern. Diese sind kaum günstiger als die aktuellen 4er, beim Neukauf sollte man deshalb auf die aktuelle Version 4 setzen. Der nachträgliche Ersatz eines 3er-Modells durch ein 4er ist selten sinnvoll: Die Geschwindigkeit hat sich nicht erhöht, in beide Richtungen fließen maximal 40 Gbit/s. Die weiteren Unterschiede liegen im Detail.

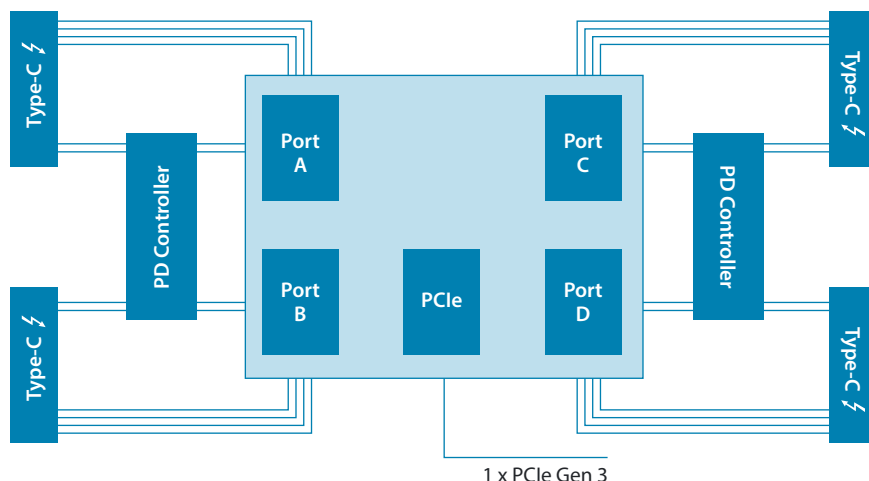
Thunderbolt 5 verspricht noch höhere Geschwindigkeit und mehr Bandbreite für den Anschluss hochauflösender Monitore. Doch auch dieser Umstieg, der im Frühjahr 2024 noch gar nicht gestartet ist, dürfte sich nur lohnen, wenn auch der Bedarf nach der höheren Geschwindigkeit da ist. Steht noch kein 5K-Monitor oder mehrere 4K-Monitore auf dem Schreibtisch, reicht selbst veraltete Peripherie mit Thunderbolt 3 völlig aus. (ll@ct.de) **ct**

Literatur

- [1] Lutz Labs, Schnell dran, schnell drin, Sieben Docks mit Thunderbolt 4 im Test, c't 13/2023, S. 60

Aufbau eines Thunderbolt-Hubs

Intels Thunderbolt-4-Controller JHL8440 teilt einen TB4-Eingang auf und liefert das Signal an drei TB4-Ausgänge weiter. Zusätzlich stellt er noch einen USB-Ausgang mit 10 Gbit/s (und USB 2.0) sowie Pins für weitere interne Anschlüsse per PCIe 3.0 x1 bereit. Daran schließen die Dock-Hersteller dann etwa LAN und weitere USB-Schnittstellen an. Zwischen den Thunderbolt-Anschlüssen des Controllers und den Typ-C-Buchsen sitzen noch die USB-PD-Controller zum Laden von Notebooks.



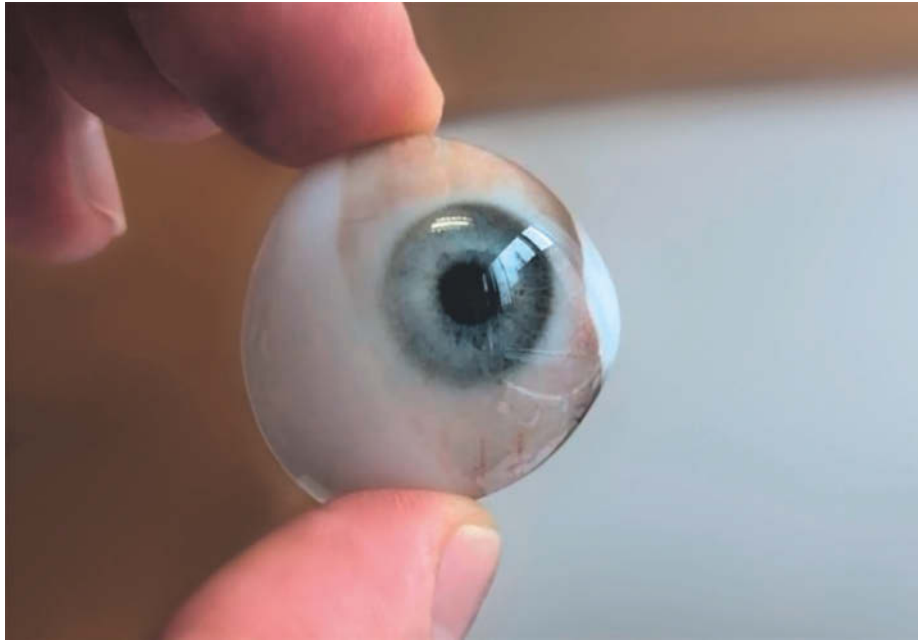


Bild: Fraunhofer IGD

Schöne Augen machen

Natürlich wirkende Prothesen aus dem 3D-Drucker

Augenprothesen entstehen bislang in mühevoller Handarbeit. Ein neuer automatisierter Prozess scannt die Augenhöhle, analysiert das gesunde Auge und steuert den 3D-Druck samt Farbgebung. Das digitalisierte Verfahren schafft Raum für smarte Verbesserungen.

Von Arne Grävemeyer

Wenn einem Menschen ein Auge fehlt, verloren durch einen Unfall oder durch Krebs, dann ist das auch kosmetisch ein großes Problem. Viele Gesprächspartner wissen einfach nicht, wo

sie hinschauen sollen. Viele empfinden den Anblick eines starren Glasauges als irritierend. Eine gute Augenprothese zu fabrizieren ist aber bis heute kunstvolle Handarbeit, die Fachleute, sogenannte Okularisten, bis zu acht Stunden in Anspruch nimmt.

Bereits seit über zehn Jahren arbeiten Forscher um Philipp Urban am Fraunhofer Institut für Graphische Datenverarbeitung (IGD) in Darmstadt an der Softwareplattform Cuttlefish für den grafischen 3D-Druck. Gemeinsam mit dem britischen Unternehmen Ocupeye und dem Moorfields Eye Hospital in London haben die Fraunhofer nun die Software Cuttlefish Eye entwickelt. Damit ermöglichen sie einen automatisierten Prozess, der sowohl die leere Augenhöhle scannt als auch das verbliebene Auge farbtreu fotografiert. Mit diesen Daten erstellt die Anwendung

ein Modell für den 3D-Druck, das dem gesunden Auge äußerlich zum Verwechseln gleicht.

Dabei berücksichtigt die Software nicht nur die individuelle Geometrie des Auges und die Farbe der Iris, sondern auch den genauen Farbton der weißlichen Lederhaut drumherum, der sogenannten Sklera. Zudem sind in der Augenprothese realistische Äderchen zu sehen. In ihrem jüngst veröffentlichten Paper zeigen die Forscher einige Fotos von Patienten, auf denen der Betrachter nicht ausmachen kann, welches Auge nur eine Nachbildung ist. Lediglich bei 20 Prozent der Patienten gab es Probleme, die erforderlichen Scans durchzuführen; ihnen kann die neue Technik derzeit nicht helfen.

Design automatisiert

Der Polyjet J750 von Stratasys, der für den 3D-Druck zum Einsatz kommt, arbeitet mit Tinten, die in ultraviolettem Licht aushärten. Er ist auf farbigen 3D-Druck ausgelegt. Cuttlefish steuert diesen Drucker mit einer Auflösung von 18 Millionen Voxel pro Kubikzentimeter an, wobei die Software für jedes Voxel aus sieben Materialien wählen kann, um so genau die Farbe und Textur zu bestimmen. Die verwendeten Materialien eignen sich nach einer Nachbearbeitungsphase für medizinische Modelle.

„Die große Designfreiheit bei einem solchen 3D-Drucker ist auch ein Problem“, sagt Urban im c’t-Gespräch. Denn wenn man ein mächtiges Grafik-Tool einsetzt, um eine individuelle Augenprothese zu modellieren, braucht man wiederum versierte Leute mit viel Expertise. „So würde der bisherige manuelle Herstellungsprozess einfach nur gegen einen digitalen, aber immer noch personalaufwendigen Prozess eingetauscht.“ Stattdessen strebten die Forscher an, das Design automatisiert zu erzeugen und sogar die gesamte Herstellung weitgehend zu automatisieren.

Das beginnt für den Patienten damit, dass er zunächst die genaue innere Form seiner betroffenen Augenhöhle mittels einer optischen Kohärenztomografie (OCT) dreidimensional aufnehmen lässt. Dafür steht am Moorfields Eye Hospital ein Casia-2-Gerät von Tomey zur Verfügung. Bei bisherigen Verfahren nimmt der Okularist zunächst einen plastischen Abdruck mit einer schnell härtenden Masse vor, was einige Patienten als unangenehm und schmerzhaft beschreiben. Beim OCT-Scan kann das Gerät zugleich ein farb-

kalibriertes Foto des gesunden Auges aufnehmen. Beide Aufnahmen sind in zwei bis drei Sekunden erledigt.

Die Software Cuttlefish Eye erzeugt daraus das digitale Modell der Augenprothese und Cuttlefish steuert anschließend den 3D-Drucker. Nach den Beobachtungen der Forscher braucht der Okularist im Endeffekt höchstens noch anderthalb Stunden Arbeitszeit, um den Prozess in Gang zu setzen, die Prothese anzupassen und dem Patienten erstmals einzusetzen.

Acht Millionen Augen

Laut Statistik braucht etwa ein Mensch unter Tausend eine Augenprothese, so wie der Moderator Frank Elstner zum Beispiel oder wie Peter Falk, der den Kriminalinspektor Columbo verkörperte. Außer in Deutschland und Österreich, wo die Kunst der Glasaugenherstellung eine lange Tradition hat, sind weltweit Kunststoffprothesen verbreitet. Die Patienten erhalten ein kugelförmiges, sogenanntes Orbital Implant, das mit den Augenmuskeln verbunden wird. Darauf setzt der Okularist oder später auch der Patient selbst seine Augenprothese auf. Die Augenmuskeln bewegen das Orbital Implant und damit die Prothese samt aufgedruckter Pupille in der Regel parallel zu den Blickbewegungen des gesunden Auges.

Die Hoffnung der Forscher ist es nun, dass Cuttlefish Eye hilft, viel Handarbeit einzusparen und die Menschen insbesondere in Weltgegenden, in denen Augenprothesen derzeit nur schlecht zu bekommen sind, besser zu versorgen. Dabei erzeugt der automatisierte Prozess Prothesen in einer gleichbleibenden Qualität. Zudem könnte sich der Markt angesichts einer solchen Technik vergrößern. Beispielsweise hat die Pupille einer Augenprothese naturgemäß eine feste Größe, die

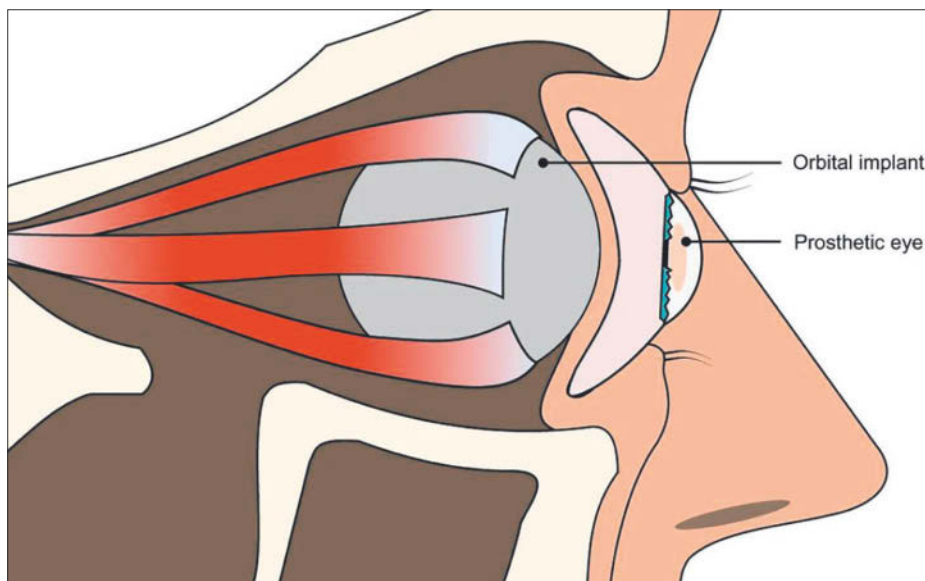


Bild: Fraunhofer IGD

Tief in die Augenhöhle pflanzen Ärzte eine Kugel namens Orbital Implant ein und verbinden diese mit den Augenmuskeln. Darauf kann der Patient später seine Augenprothese einsetzen, die dann unwillkürlich den Bewegungen des gesunden Auges folgt.

sich mit der Tageszeit und den Beleuchtungsverhältnissen nicht verändert. Das kann an sehr hellen Orten oder am schummrigen Abend seltsam wirken, wenn eine Augenprothese mit kleinerer oder vergrößerter Pupille angemessener wäre.

Smarte Funktionen

„Ein weiterer Vorteil einer digitalisierten Lösung besteht darin, dass man darauf aufbauen und sie weiterentwickeln kann“, sagt Johann Reinhard vom Fraunhofer IGD. Technisch wäre es nicht sehr schwierig, die Prothese und speziell die Pupille grafisch umzugestalten und beispielsweise für Fans das Logo eines Fußballvereins oder andere modische Symbole einzubauen.

Auf der anderen Seite denken die Forscher über das Problem wechselnder Pupillengrößen nach. Durch den Einsatz lichtändernder Farben ähnlich wie bei Brillengläsern könnten sich auch Augenprothesen der Zukunft an die herrschenden Lichtverhältnisse anpassen.

Vielleicht kann ein digitalisiert erstellter Körper in der Augenhöhle in fernerer Zukunft auch noch ganz andere technische Funktionen übernehmen. Der kanadische Filmemacher Rob Spence, der als Jugendlicher sein rechtes Auge verloren hat, nennt sich „Eyeborg“ und experimentiert mit einsetzbarer Kameratechnik (siehe [ct.de/ytbv](https://www.ct.de/ytbv)). Die lässt sich zwar nicht an seine Sehnerven anschließen. Aber der Filmemacher träumt davon, Reportagen und Interviews in einer ganz ungestörten, natürlichen Weise begleiten zu können. Die Miniaturisierung kommt diesem Traum entgegen. Ein digitalisierter Herstellungsprozess mittels 3D-Drucker kann ein erster Schritt sein, auch derartige Gadgets in Zukunft anbieten zu können. (agr@ct.de) **ct**

Literatur

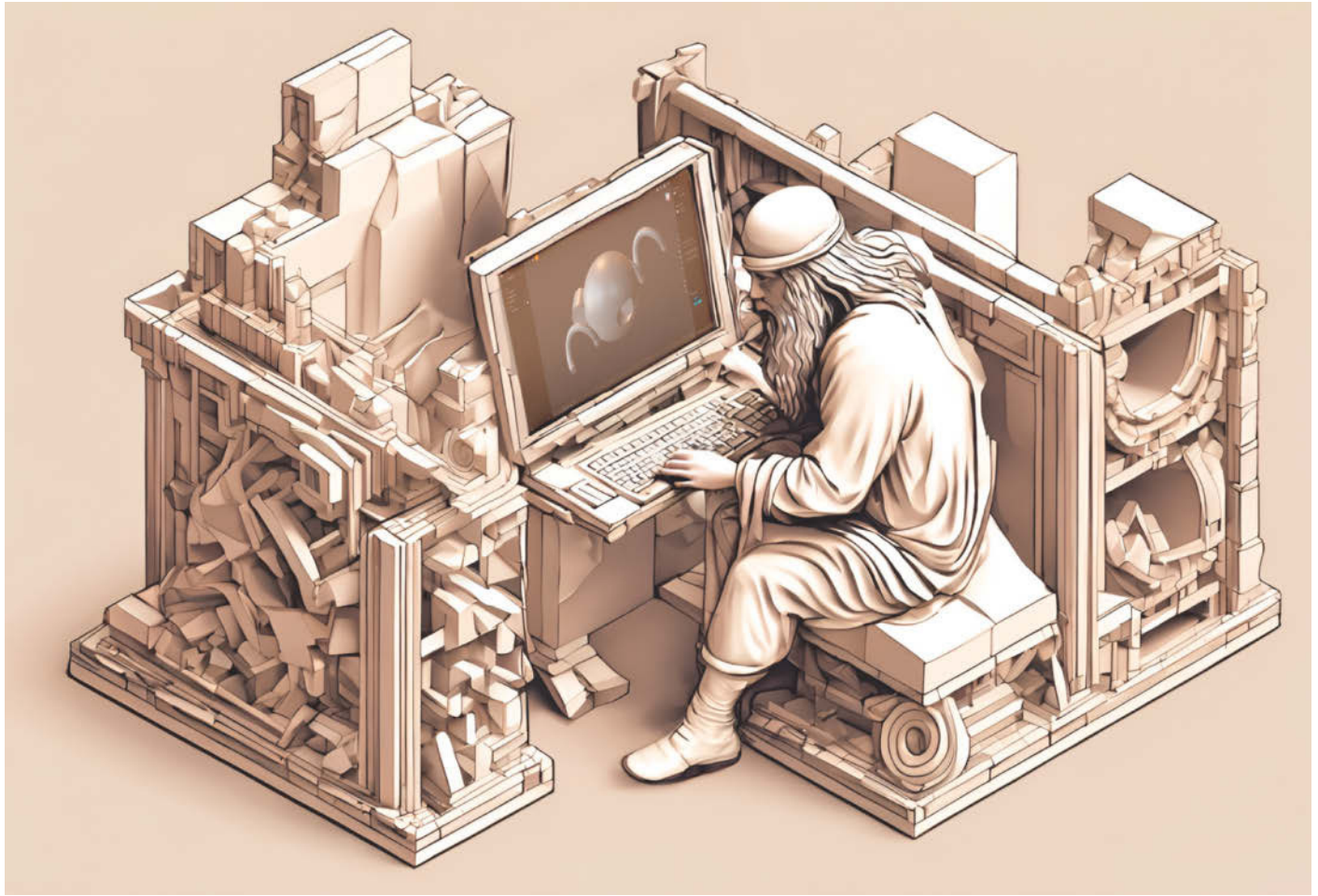
- [1] Johann Reinhard, Philipp Urban et al., Automatic data-driven design and 3D printing of custom ocular prostheses, Nature Communications, 27. Februar 2024: <https://doi.org/10.1038/s41467-024-45345-5>

Projektseiten: [ct.de/ytbv](https://www.ct.de/ytbv)



Ein J750 von Stratasys druckt täuschend echt aussehende Augenprothesen aus. Die Automatisierung erspart pro Prothese viele Stunden Handarbeit.

Bild: Fraunhofer IGD



Einfach mal ranklotzen

Plasticity: ein CAD-Programm für Künstler und Hobbyisten mit 3D-Drucker

Viele 3D-Programme sind nichts für Kreative. Komplizierte Workflows und überladene Menüs frustrieren auf dem Weg zum selbst gedruckten 3D-Objekt. Plasticity wirft eine Menge Ballast über Bord, ohne dass die Ergebnisse leiden.

Von Michael Link

Wer einen 3D-Drucker hat, beglückt seine Umgebung vielfach mit mehr oder minder nützlichen Stehrümchen. Websites wie [printables.com](https://www.printables.com), [cults3d.com](https://www.cults3d.com) und [thingiverse.com](https://www.thingiverse.com) liefern Vorlagen für Batteriekästen, Gehäuse und Figuren sowie sonstige Staubfänger aus Plaste und Elaste. Aber: Nicht für alle Dinge gibt es fertige Druckdateien. Dann heißt es selbst konstruieren.

Mit dem kostenlos nutzbaren TinkerCAD lernen und üben viele Bastler, wie man Sachen im dreidimensionalen Raum entwirft. Oftmals erstellt man zuerst eine 2D-Skizze, pumpt („extrudiert“) dann die

gemalten Flächen zu Grundformen auf und schiebt sie wie Puzzlestücke zusammen. Nach etwas Herumprobieren ist schnell der erste weltweit absolut einzigartige Spezialwandhaken fertig.

Irgendwann merkt man aber, dass potentere Gestaltungswerkzeuge nötig sind. Zum Beispiel, wenn man das Modell einer Tasse so modifizieren will, dass die Tasse größer wird, ohne dass auch die Wandstärke zunimmt. Das funktioniert mit TinkerCAD nicht. Beim Vergrößern wachsen nämlich alle Dimensionen gleichermaßen, also auch die Wandstärke. Dagegen kann man solche Aufgaben mit param-

trisch arbeitenden Programmen erledigen. In SolidWorks, Fusion360 sowie Blender und FreeCAD legt man einzelne Parameter fest beziehungsweise definiert Abhängigkeiten von anderen Objekten des Entwurfes. Damit bleibt eine Manipulation auf bestimmte Eigenschaften beschränkt.

Das Einarbeiten in solche Vollblut-CAD-Software ist nicht gerade vergnügungssteuerepflichtig, und so mancher Trick ist nicht offensichtlich. Da wünscht man sich für schnelle Entwürfe zwischendurch ein einfacher zu handhabendes Werkzeug. Hier kommt Plasticity gerade recht.

Plasticity ist ein 3D-Modellierer, den der Hersteller als „CAD für Künstler“ bewirbt. Man arbeitet sich nicht von 2D-Maßzeichnungen zu einem 3D-Modell hoch, sondern direkt am dreidimensionalen Objekt. Das ist so intuitiv wie im Kindergarten Knetgummi zu bearbeiten: hier ein Klotz drauf, da was mit einem runden Objekt ausstanzen; hier was hochziehen, da etwas abrunden oder reinschneiden. Das umreißt, wie man mit Plasticity arbeitet, nämlich direkt an Objekten und nicht über 2D-Skizzen.

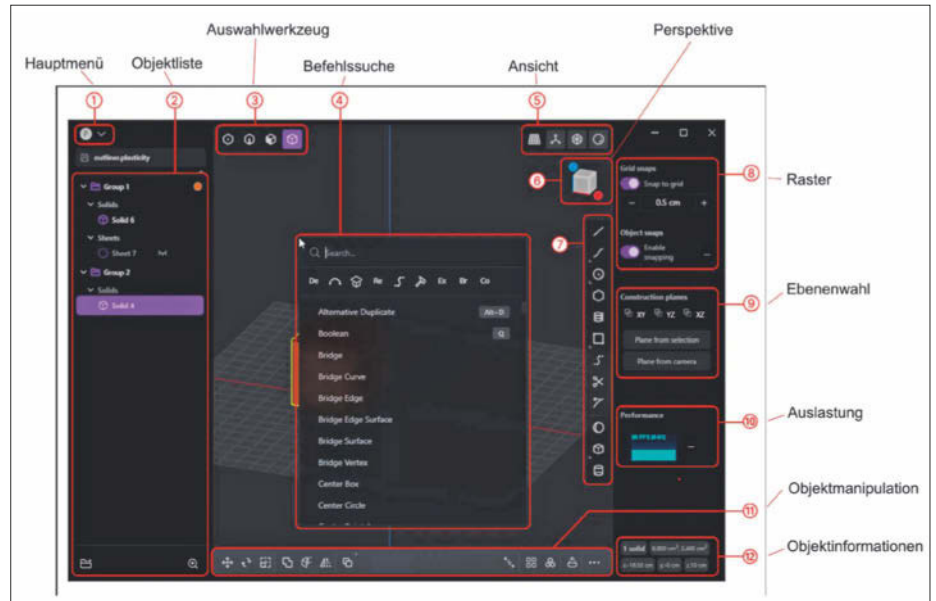
Software as a Software

Plasticity arbeitet ohne Cloud, ist für Windows, macOS und das Linux-Derivat Ubuntu erhältlich. Die „Indie“-Version für 149 US-Dollar kann alles, was Hobbyisten benötigen und erlaubt die Installation auf zwei Rechnern. Die doppelt so teure „Studio“-Version läuft auf bis zu vier Rechnern, kann weitere Formate importieren und Unternehmen ab zehn Mitarbeitern können nur diese erwerben. Alle Kaufversionen bekommen Updates für ein Jahr. Plasticity funktioniert auch danach ohne das Nachwerfen von Geld, nur verdorrt dann der Zustrom neuer Funktionsupdates.

Zurzeit steht der Versionszähler auf 1.4.8, und bisher ändert sich mit jedem Update viel. Die englischsprachige Dokumentation auf der Herstellerseite wird nach unseren Erfahrungen recht schnell auf den neuen Stand der Entwicklung nachgezogen. Auch Tutorials gibt es seit einiger Zeit im Netz. Und wenn man sich als Nutzer festgefahren hat, helfen die Anbieter auf einem Discord-Kanal.

Waldi an der Wursttheke

Nach dem Starten des Programms findet man eine ganze Sammlung an Menübändern vor, man kommt sich vor wie Waldi an der Wursttheke und weiß nicht recht, was man zuerst beschnuppern soll.



Plasticity teilt den Arbeitsplatz in Leisten mit gruppierten Menübändern auf.

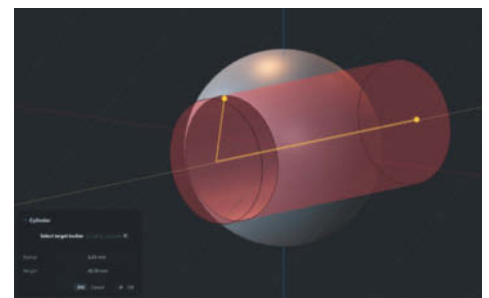
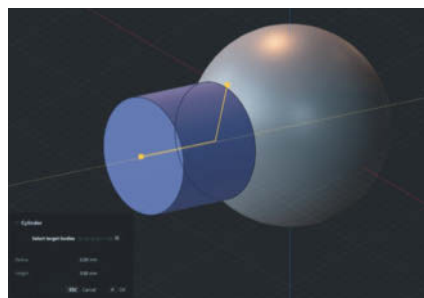
Links und rechts neben dem Hauptbildschirm sind Seitenleisten angeflanscht. Die linke zeigt eine Liste der vom Nutzer konstruierten einzelnen Objekte. Man kann sie im Gesamtentwurf mit Rechtsklick auf Icons ausblenden, vor der Bearbeitung schützen oder löschen. Der rechte Bereich steuert hauptsächlich Einrast- und Ebenenfunktionen.

Im Hauptbildschirm findet sich oben links ein Selektor, der bestimmt, ob ein Mausklick einen Punkt, eine Linie, eine Fläche oder ein Objekt im Entwurf auswählt. Diese Modi sind per Klick sowie über die Ziffernreihe mit den Tasten 1 bis 4 schaltbar. Ein flotter Wechsel zwischen Mausklicks und Tastendrücken beschleunigt das Arbeiten, und der Entwickler stellt ein zweiseitiges PDF mit Kürzeln für etliche weitere Befehle bereit.

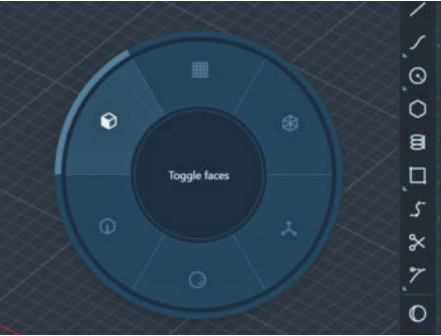
Rechts oben im Hauptbildschirm sucht man sich eine Perspektive mithilfe des aus vielen Konstruktionsprogrammen bekannten Würfels aus: Man klickt auf

eine Fläche oder einen Achsenbuchstaben (x, y oder z) und erhält eine Ansicht aus dieser Perspektive. Ohne Klicks geht das auch mit den Zifferntasten 1, 7 und 3 aus dem Ziffernblock. Ebenfalls dort wählt man die isometrische oder orthogonale Ansicht. Außerdem verpasst man hier einem Modell gerenderte Oberflächen, mit der die Konstruktion beispielsweise metallisch glänzt.

Für grundlegende Bearbeitungen, etwa das Entfernen oder Setzen von Linien sowie zum Hinzufügen von Grundformen dient eine weitere vertikale Leiste rechts im Hauptbildschirm. Kontextmenüs, mit denen man beispielsweise die Maße eines aufgezogenen Rechtecks festlegen kann, erleichtern die Gestaltung, weil man so gut wie nie nach Untermenüs von Menüs in anderen Menüs suchen muss, um Parameter zu beeinflussen. Für einige spezialgelagerte Sonderparameter brauchten wir wegen der englischsprachigen Bezeichnungen ein Wörterbuch zur Übersetzung.



Platziert man auf einem Objekt einen Kreis für einen Zylinder, bestimmt man durch Ziehen mit der Maus, ob der Zylinder als extrudierter Körper aus dem Objekt herausragt (blau) oder ob er als Bohrung fungiert (rot).

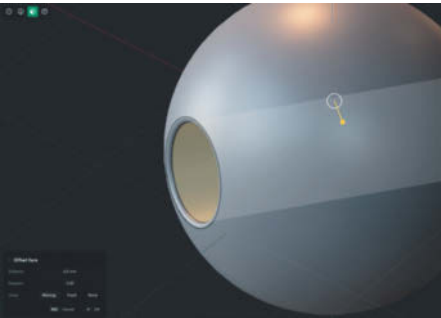
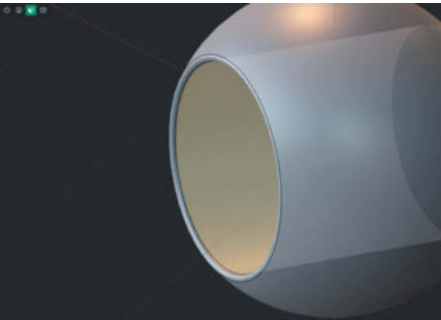


Das Radial-Menü ist ab Werk nicht aktiv, aber per JSON-Datei zu aktivieren und erspart dann Mauslaufwege.

Ansonsten reicht ein mäßiges Schulenglisch zum Bedienen aus, die Website bietet auch eine deutsche Anleitung.

Eine weitere Leiste unten im Hauptschirm manipuliert Objekte. Mit booleschen Operatoren verheiratet oder trennt man zum Beispiel Formen, mit dem Move-Befehl verschiebt man sie. Formen lassen sich zu radial oder rechtwinklig angeordneten Arrays vervielfältigen. So konstruiert man beispielsweise einen Flügel eines Windrades und befiehlt Plasticity, drei davon im Kreis anzuordnen.

Befehle für irgendwelche Objekte, die man konstruieren möchte, findet man als Geübter am schnellsten per Tastatur: Tippt man irgendwo im Hauptfenster ein F, erscheint ein Suchfeld. Der Befehl „Center Circle“ erzeugt beispielsweise nach einem



Die Kante einer Bohrung bildet bei Plasticity ein Objekt, das man problemlos bearbeiten kann, etwa durch Fillets, Fasen und durch Größenänderungen.

Mausklick ein Zentrum eines Kreises, den man mit der Maus aufzieht. Noch einfacher wird es bei ganz naheliegenden Bearbeitungen. Deren Tastenkürzel werden stets unten rechts im Hauptbildschirm eingeblendet.

Mit einem kostenlos per JSON-Datei zurüstbaren Add-in, dem sogenannten „Radial-Menü“, erhält man außerdem ein Menüwahlrad für die Objekt- und Ansichtsauswahl. Das muss man nicht haben, aber manche sind durch andere Programme daran gewöhnt.

Wie tickt Plasticity?

Der in Plasticity benutzte Geometriekernel Parasolid ist eine Softwarebibliothek, die mit mathematischen Funktionen Objekte und Flächen manipuliert, etwa die beschriebenen booleschen Werte sowie Verrundungen und Fasen von Objektkanten. Parasolid-Rechenwerke sind in CAD-Software wie SolidWorks, Siemens NX, Shapr3D im Spiel und damit entstehen von kleinsten Teilen bis zu Luft- und Raumfahrtkomponenten vieles, das möglichst nicht zerbröseln soll wie Abdeckplatten in Boeing-Flugzeugen.

Plasticity arbeitet rechnerisch nicht mit Polygonen wie sie etwa in 3D-Druckdateien im STL-Format vorkommen, sondern mit Oberflächen, die durch Kurven oder Flächen bestimmt sind (nicht-uniforme rationale B-Splines, kurz NURBS). Das macht das Bearbeiten auch wild und komplex aussehender Formen einfach.

Manche CAD-Software treibt einen in den Wahnsinn, etwa wenn man damit einer Bohrung in einer gewölbten Oberfläche einen sanften Übergang verpassen will. Denn so einige CAD-Programme machen aus dem Ausgebohrten ein Arrangement aus etlichen Polygonen. Und damit wird es zum stupiden Geduldsspiel, einen daraus gebildeten Rand zu verrunden, denn dazu muss man jedes einzelne Segment bearbeiten. Plasticity belässt die Wand der Bohrung als ein zusammenhängendes Objekt. Somit brauchen Plasticity-Nutzer keine Baldriantröpfen, denn zum Abrunden oder Anfasen wählen sie nur einmal die Kante der Bohrung.

Abteilung Im- und Export

Die Entwickler von Plasticity, selbst von Blender kommend, wussten wohl, dass viele Nutzer bereits Bekanntschaft mit anderen CAD-Programmen gemacht haben. Sie lassen im Einstellmenü die Wahl zwischen zahlreichen vielleicht gewohnten Arten, mittels Maus mit Objek-

ten im Fenster zu agieren: Bei Plasticity verschiebt man etwa mit der rechten gedrückten Maustaste ein Objekt und mit gedrückter mittlerer Maustaste umkreist man es. Wählt man Blender-Einstellungen, verschiebt man Objekte mit der Umschalttaste und die Ansicht des Objektes mit der mittleren Maustaste.

Mit HOOPS Exchange hat Plasticity eine CAD-Format-Übersetzungsbibliothek, mit der das Programm eine Vielzahl von CAD-Formaten importiert und exportiert. Die Übertragung von Daten zwischen CAD-Programmen verlief bei uns wegen Inkompatibilitäten zwischen den Geometriekernen nicht immer fehlerfrei. Das Problem haben aber auch andere CAD-Programme. Das wichtigste Add-on dürfte die Blender Bridge sein. Sie erlaubt im laufenden Betrieb den Transfer von Plasticity-Objekten zu Blender ohne umständliches Im- und Exportieren.

Für den eigentlichen Zweck, nämlich Dinge für den 3D-Druck zu modellieren, reichen uns die Exportformate OBJ und STEP. Damit kamen Druckvorbereiter wie der PrusaSlicer prima zurecht.

Erster Eindruck

Insgesamt zaubert Plasticity beim Modellieren immer wieder mal ein Lächeln ins Gesicht, denn sobald man die Fremdelphase durchlaufen hat, sind sonst schwierige Aufgaben überraschend intuitiv umsetzbar. Mit Kontextmenüs spart man sich Sucherei in Menüs und so läuft das Arbeiten damit wie auf Schienen vorgezeichnet.

Trotz alledem: Es konstruiert sich auch mit Plasticity nichts von selbst. Man muss sich schon vorstellen können, wie aus einfachen Formen komplexe Gebilde werden sollen. Wer mit Knetgummi, Klemmbausteinen und echtem Material und Werkzeugen gearbeitet hat, ist dabei im Vorteil. Mit einer 30 Tage nutzbaren kostenlosen Testversion kann man sich vor dem Kauf ein Bild von Plasticity machen – oder ein Stehrümchen damit bauen. (mil@ct.de) ct

Download: ct.de/yaf8

Plasticity

3D-CAD-Software	
Hersteller, URL	Plasticity, plasticity.xyz
Systemanf.	Windows (ab 10) , macOS (ab 12, für M1, M2, M3, Intel), Linux (Ubuntu 22, deb)
Importformate	Indie: Plasticity, STEP, Parasolid, FBX, OBJ, STL, JPG/PNG; Studio zusätzlich IGS, SAT, Rhino, DXF/DWG
Exportformate	Indie: Plasticity, STEP, Parasolid, OBJ, STL; Studio zusätzlich IGS, SAT
Preis	Indie: 149 US-Dollar, Studio: 299 US-Dollar

heise security tour 2024

Wissen schützt

Mit mehr Resilienz
zu mehr Sicherheit

23. Mai (Köln)
29. Mai (Hannover)
12. Juni (Stuttgart)
5. Juni (online)
19. September (online)

DIE THEMEN

- Das Lagebild der IT-Security
- Das Update zu IT-Recht und Datenschutz, NIS-2
- Alerting und Monitoring in der Praxis
- Die Psychologie der Security
- Was geht bei "KI und Security" wirklich?

Jetzt Tickets sichern:
security-tour.heise.de





Bild: Collage c't

Türöffner

Windows bekommt einen sudo-Befehl

Unter Windows Programme mit Administratorrechten auszuführen ist für Mausschubser kein Problem, für Konsolennutzer aber bislang ziemlich umständlich. Das will Microsoft mit dem neuen Befehl sudo ändern.

Von Hajo Schulz

Für Linux-Anwender Alltag: Sie rufen in der Konsole einen Befehl auf und das System lehnt die Ausführung mit Hinweis

auf fehlende Berechtigungen ab. Kein Problem: Einfach den Befehl mit Cursorhoch zurückholen, sudo davorschreiben, und schon klappts.

Ganz so einfach haben es Windows-Anwender nicht. Sie müssen eine neue Konsole mit Administratorrechten öffnen, dazu eine Sicherheitsnachfrage bestätigen und den Befehl dort neu eingeben oder aus dem vorherigen Terminal-Fenster kopieren – und das selbst, wenn sie eigentlich Administrator sind [1]. Wer das im Normalbetrieb nicht ist, muss auch noch ein Admin-Kennwort eintippen.

Frisch aus
c't Nerdistan

Doch es naht Abhilfe: Microsoft hat angekündigt, mit einem der nächsten Updates auch Windows einen sudo-Befehl zu spendieren. In einer Vorabversion ist er bereits zu bewundern. Wir haben uns schon mal angesehen, was Sie davon zu erwarten haben, wie sich das Windows-sudo gegen seinen Linux-Namensvetter schlägt und was eine bereits verfügbare Alternative taugt.

Wozu das Ganze?

In grauer Vorzeit kannte Windows keine Berechtigungen für Benutzer: Jeder durfte

einfach alles. Seit Windows NT ist Windows aber ein Mehrbenutzerbetriebssystem. Jeder Anwender besitzt ein eigenes Benutzerkonto, das die privaten Daten vor dem Zugriff aus fremden Konten schützt. Außerdem sollen allzu experimentierfreudige Anwender davon abgehalten werden, ihren Mitbenutzern das System kaputt zu konfigurieren. Für den Systemverantwortlichen muss es aber trotzdem eine Möglichkeit geben, auf alle Daten, Einstellungen und Programme zuzugreifen. Zu einem Konto für Wartungs- und Konfigurationsarbeiten, das alle Rechte besitzt (oder sich zumindest verschaffen kann), wird das Konto des Verwalters dadurch, dass es der Gruppe „Administratoren“ angehört.

Für den typischen Anwendungsfall eines privaten PCs, den man alleine oder allenfalls gemeinsam mit vertrauenswürdigen Familienmitgliedern benutzt, hat sich dieses Konzept aber als un bequem erwiesen: Es ist einfach lästig, sich für jede Programminstallation und jede Änderung der Systemkonfiguration neu anmelden zu müssen. Viele haben daher von Windows NT bis XP den bequemen Weg gewählt und waren auch im Normalbetrieb als Mitglied der Admin-Gruppe unterwegs. Das ist aber aus zwei Gründen problematisch: Erstens hält einen das nicht mehr von versehentlichen Eingriffen ins System ab, die die Stabilität gefährden könnten. Und zweitens hat alles, was unbewusst mit gestartet wird, ebenfalls vollen Systemzugriff, insbesondere alle Arten von Viren, Trojanern und ähnlichem Unrat.

Mit Windows Vista hat Microsoft daher das Konzept der sogenannten „Verbindlichkeitsstufen“ und der damit verbundenen Benutzerkontensteuerung (User Account Control, kurz UAC) eingeführt. Die Idee: Auch Mitglieder der Administratoren-Gruppe haben zunächst nur die Berechtigungen normaler Anwender. Erst wenn sie für ein bestimmtes Programm oder für den Zugriff auf Systemdateien volle Rechte benötigen, können sie sich die verschaffen, müssen das aber explizit bestätigen. Im ersten Anlauf waren diese ständigen Nachfragen eher nervig als nützlich, aber mittlerweile ist es – zumindest im privaten Umfeld – gang und gäbe, mit so einem eingeschränkten Administratorkonto unterwegs zu sein – allein schon, weil es bei einer frischen Installation der Standard ist.

Grafische Anwendungen lassen sich so recht einfach mit vollen Rechten star-

ten, etwa indem man ihr Symbol mit gedrückter Strg- und Umschalt-Taste doppelklickt oder per Rechtsklick und dem Kontextmenübefehl „Als Administrator ausführen“ aufruft. Fans der Kommandozeile hat Microsoft aber bei diesem Konzept bislang ziemlich stiefmütterlich behandelt. Man kann eine Eingabeaufforderung oder die PowerShell mit Admin-Rechten starten, muss aber schon vor dem Eintippen des ersten Befehls daran denken. Innerhalb der Konsole hat früher das Konstrukt `runas /user:Administrator <Befehl>` geholfen, aber das dazu nötige Konto namens „Administrator“, das als einziges nicht der UAC unterliegt, ist heutzutage nicht mehr aktiv. PowerShell-Anwender können notfalls noch den Befehl `Start-Process` nebst seiner Option `-Verb` `runas` verwenden, wenn sie die Tipparbeit nicht scheuen.

Microsofts sudo

Mit dem neu eingeführten Befehl `sudo` – der Name leitet sich von „superuser do“ ab – soll das nun alles ähnlich bequem wie unter Linux werden. Vor allem soll dieses Tool universell verwendbar sein, egal ob man nur einem Admin-Konto per UAC-Abfrage volle Rechte verschaffen oder von einem eingeschränkten in ein Administratorkonto wechseln will.

Bislang ist das Microsoft-eigene `sudo` nur in Insider-Vorabversionen von Windows enthalten, genauer: ab Build 26052. Wer es zu benutzen versucht, erntet aber zunächst einen Fehler: Der Befehl sei nicht aktiviert, man möge ihn doch über die Entwickler-Optionen in den Einstellungen freischalten. Unter „System/Für Entwickler“ findet sich dazu zunächst ein Schalter namens „sudo aktivieren“. Betätigt man ihn, warnt Windows, dass der Befehl `sudo` ein Sicherheitsrisiko darstelle, und bittet um Bestätigung.

Ein Klick auf „Ja“ schaltet eine Auswahlbox frei, mit der man konfigurieren kann, wie `sudo` Anwendungen ausführt. Vorausgewählt ist die selbsterklärende Option „In einem neuen Fenster“. Das Gegenteil bewirkt „Inline“: Die Ausgaben von Befehlen, die man mit `sudo` aufruft, landen in demselben Fenster, in die man sie eintippt. Dasselbe passiert auch bei „Mit deaktivierter Eingabe“, allerdings verbindet `sudo` das aufgerufene Programm dann nicht mit der Tastatur. Laut Microsofts Dokumentation soll das der Sicherheit dienen: Ein maliziöser Prozess, der sich in die Konsolensitzung eingeschli-

c't kompakt

- In einer Windows-Vorabversion zeigt Microsoft einen `sudo`-Befehl, mit dem Konsolennutzer Kommandos auf die Schnelle mit vollen Rechten ausführen können.
- In Linux und verwandten Betriebssystemen ist dieser Befehl schon lange gang und gäbe, funktioniert im Detail aber ganz anders.
- Mit `gsudo` gibt es eine Alternative für Windows, ihr Funktionsumfang übersteigt den des Microsoft-Tools.

chen hat, kann dann nicht hinterrücks gefälschte Eingaben an das mit erhöhten Rechten laufende Programm schicken. Wie so oft leidet darunter aber der Bedienkomfort: Befehle wie `sudo cmd` oder `sudo diskpart`, die ein interaktives Konsolenprogramm starten sollen, funktionieren nicht mehr, denn sie erkennen, dass sie keine Eingaben empfangen können, und beenden sich nach dem Start gleich wieder. Wer das mit dem „Inline“-Modus verbundene Risiko scheut, benutzt also besser die Option „In einem neuen Fenster“.

Übrigens funktionieren Befehle wie `sudo tasklist /v` | `more` auch mit deaktivierter Eingabe: Mit erhöhten Rechten läuft dabei nur `tasklist`, die Konsole sammelt dessen Ausgabe ein und reicht sie an das wieder mit eingeschränkten Rechten laufende `more` weiter, das auf Tastendrücke wartet.

Die Inline-Modi haben derzeit noch einen Bug: Ein ohne weitere Argumente aufgerufenes Programm bekommt trotzdem einen Parameter übergeben, der aber leer ist. Programme reagieren darauf recht unterschiedlich: `diskpart` meldet beispielsweise „Die Parameter konnten nicht verarbeitet werden.“ und beendet sich sofort wieder. Auch `netsh` zeigt auf diese Weise keinen interaktiven Prompt an, stattdessen gibt das Programm die mehrere Bildschirmseiten füllende Netzwerkkonfiguration aus, ganz so, als hätte man `netsh dump` aufgerufen.

Wie es sich für ein Konsolenprogramm gehört, lässt sich `sudo` auch über die Kommandozeile steuern. Es kennt unter anderem die Option `config`, die die aktuelle Betriebsart vermeldet. Lässt man

ihr das Argument `--enable` folgen und ergänzt es mit `disable`, `enable`, `forceNewWindow`, `disableInput` oder `normal`, schaltet man die Betriebsart systemweit um, wobei `normal` (oder auch `default`) der Einstellung „Inline“ entspricht. Für einen einzelnen Aufruf lässt sich die Voreinstellung mit `--new-window` (oder kurz `-N`) oder `--disable-input` überstimmen. Weitere Details verrät `sudo help`.

Wie immer, wenn man unter Windows ein Programm mit Administratorrechten ausführen will, ruft auch `sudo` die Benutzerkontensteuerung auf den Plan. Auch Benutzer, deren Konto zur Gruppe der Administratoren gehört, müssen also bei jedem `sudo`-Aufruf per Mausklick „zulassen, dass durch diese App Änderungen an Ihrem Gerät vorgenommen werden“ – jedenfalls wenn der UAC-Regler in den Einstellungen wie empfohlen mindestens auf der dritten von vier möglichen Stufen steht. Das ist auch gut so, damit sich Malware nicht einfach mit einem versteckten `sudo`-Aufruf volle Rechte verschaffen kann.

Ruft man `sudo` aus einem eingeschränkten Benutzerkonto heraus auf, meldet sich ebenfalls die UAC, gibt sich aber nicht mit einem einfachen Klick auf OK zufrieden. Stattdessen will sie Benutzername und Kennwort eines Admin-Kontos wissen. Unter diesem Konto führt Windows dann die angeforderte Anwendung aus. Einem eingeschränkten Konto verschafft `sudo` also keine Administratorrechte – das ist im Sicherheitskonzept von Windows auch nicht vorgesehen.

Microsoft plant, `sudo` auch im Quelltext zu veröffentlichen. Die dafür vorgesehene Seite auf GitHub (siehe ct.de/ypmm) ist aber noch weitgehend leer. Bis zum Redaktionsschluss für diesen Artikel gab es dort nur ein Skript, das PowerShell-Benutzern den Umgang mit `sudo` erleichtern soll.

gsudo

Zu Microsofts `sudo` existieren Alternativen. Die wahrscheinlich populärste ist das Open-Source-Programm `gsudo` des argentinischen Entwicklers Gerardo Grignoli (siehe ct.de/ypmm). Der Grundgedanke ist derselbe wie bei `sudo`: Man schreibt den Programmnamen vor einen Befehl, um diesen mit Administratorrechten auszuführen. Solange es auf dem System kein Microsoft-`sudo` gibt, fühlt sich `gsudo` auch von dem Befehl `sudo` angesprochen.

Ein grafisches Configurations-Frontend bringt `gsudo` nicht mit, stattdessen kann man seine Optionen über Kommandozeilenbefehle einstellen, die alle mit `gsudo config` beginnen. Ohne weitere Argumente bekommt man die aktuelle Konfiguration angezeigt. Standardmäßig funktioniert `gsudo` auf eine Art und Weise, die dem „Inline“-Modus des Microsoft-`sudo` entspricht. Die Betriebsart, die für jedes mit vollen Rechten gestartete Programm ein neues Fenster öffnet, stellt `gsudo config NewWindow.Force true` dauerhaft ein, mit `false` statt `true` gehts zurück, `gsudo -n <Befehl>` führt diesen einen Befehl in einem neuen Fenster aus. Die in der `gsudo`-Dokumentation als experimentell

bezeichnete Option `SecurityEnforceUacIsolation true` aktiviert einen Inline-Modus ohne Eingabe.

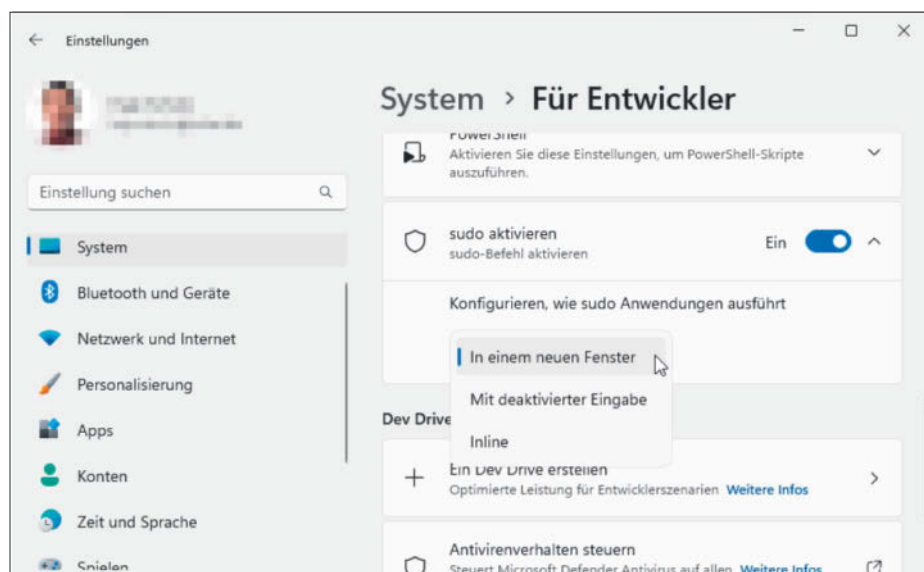
Neben den Grundfunktionen beherrscht `gsudo` noch einige Tricks, mit denen es sich von dem Microsoft-Pendant abhebt. Ein bisschen Tipparbeit spart etwa die Tatsache, dass `gsudo` ohne weitere Parameter aufrufen die Rechte der gerade aktiven Konsolensitzung erhöht. Wer weiß, was er tut, kann sich mit `gsudo` nicht nur Administratorrechte verschaffen, sondern über das Flag `-s` auch die des lokalen Systemkontos oder mit `--ti` die des „Trusted Installer“, also jenes Kontos, das als einziges Schreib- und Löschrechte an Windows-eigenen Systemdateien hat. Eher exotisch, aber manchmal nützlich: `gsudo -i Medium <Befehl>` führt einen Befehl mit normalen Benutzerrechten aus (Medium), auch wenn man ihn aus einer Admin-Konsole heraus startet.

Wie unter Windows üblich ruft jede Rechte-Erhöhung auch mit `gsudo` die Benutzerkontensteuerung auf den Plan. Wen die ständigen Sicherheitsnachfragen nerven, der kann das Programm aber auch so einstellen, dass es sich die Bestätigung eine Zeitlang merkt und überspringt: `gsudo cache on` zeigt einmal eine UAC-Abfrage an und merkt sich die Bestätigung, bis man diese Konsolensitzung beendet oder den Cache mit `gsudo cache off` oder `gsudo -k` abschaltet. Alternativ kann man das Programm auch so einstellen, dass es sich jede UAC-Bestätigung automatisch für eine bestimmte Zeitspanne merkt. Der Befehl dafür lautet `gsudo config CacheMode Auto`; als Speicherzeit sind fünf Minuten voreingestellt, was sich mit `gsudo config CacheDuration "hh:mm:ss"` ändern lässt. Achtung: Der UAC-Cache ist ein Sicherheitsrisiko, und die `gsudo`-Dokumentation weist ausdrücklich darauf hin, dass Sie sich hier Bequemlichkeit mit verminderter Sicherheit erkaufen. Der Cache setzt in der aktiven Konsole zeitweise die Benutzerkontensteuerung außer Funktion und Programme könnten sich ohne Nachfrage erhöhte Rechte erschleichen.

Für weitere Überlegungen zum Thema Sicherheit und für eine Komplettübersicht der `gsudo`-Befehle und -Optionen sei auf die Ausgabe von `gsudo help` und die Online-Doku verwiesen (siehe ct.de/ypmm).

sudo unter Linux

Das Vorbild sowohl für `gsudo` als auch für Microsofts `sudo` ist der Kommandozeilen-



Wer Microsofts `sudo` benutzen will, muss es zunächst in den Entwickleroptionen der Einstellungen aktivieren.

befehl `sudo`, wie er unter unixoiden Betriebssystemen gängig ist. Die grundsätzliche Funktionsweise aus Anwendersicht ist in beiden Welten ähnlich: Man stellt einem Befehl `sudo` voran, um das Folgende ohne Einschränkungen durch irgendeine Rechteverwaltung ausführen zu können. Im Detail und vor allem hinter den Kulissen passieren dabei aber durchaus unterschiedliche Dinge. (Wenn im Folgenden von `sudo` unter Linux die Rede ist, sind Namensvettern unter macOS und anderen Unix-artigen Betriebssystemen automatisch gemeint.)

Die Unterschiede beginnen damit, dass es unter Linux kein Konzept gibt, das der Benutzerkontensteuerung und den Verbindlichkeitsstufen von Windows entspricht. Die Rechte, die einem Benutzerkonto zugeordnet sind, sind bei jedem Login gleich und ändern sich nicht im Verlauf einer Sitzung. Das hat zur Konsequenz, dass `sudo` den Benutzer für erhöhte Rechte auf jeden Fall unter einem anderen Konto anmeldet, standardmäßig als `root`, also als allmächtiger Systemverwalter.

Etwas Ähnliches passiert unter Windows auch, und zwar immer dann, wenn ein Benutzer, der nicht zu der Gruppe der Administratoren gehört, den `sudo`-Befehl ausführt. Grundsätzlich verschieden funktioniert dabei allerdings die Authentifizierung: Unter Windows muss der Anwender das zum gewünschten Admin-Konto gehörige Passwort kennen, unter Linux nur sein eigenes. Was zunächst wie ein offenes Scheunentor anmutet, durch das jeder `root`-Rechte erlangen kann, entpuppt sich bei näherem Hinsehen als ziemlich schlau: Wer `sudo` überhaupt verwenden darf und was genau er dann mit den erhöhten Rechten anfangen darf, kann (und muss) nämlich zuvor ein Administrator konfigurieren. Dazu gibt es die Textdatei `/etc/sudoers`, die – Sie ahnen es wahrscheinlich – einzig der Benutzer `root` bearbeiten darf. Wer hier nicht verzeichnet ist, darf `sudo` nicht benutzen. Sein eigenes Kennwort muss der `root`-Benutzer auf keinen Fall aus der Hand geben.

Den genauen Aufbau der Datei zu erklären, würde hier den Rahmen sprengen. In aller Kürze: Jede Regel definiert zunächst, für wen (ein Benutzerkonto oder eine Gruppe) und wo (auf welchen Hosts) sie gilt. Als Nächstes bestimmt sie, welche Identitäten – wieder Benutzer oder Gruppen – der Berechtigte per `sudo` annehmen darf. Schließlich folgt eine Liste von regulären Ausdrücken, die spezifizieren, wie

```

NAME
    sudo, sudoedit - execute a command as another user

SYNOPSIS
    sudo -h | -K | -k | -V
    sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]
    sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
        [command [arg ...]]
    sudo [-ABbEHnPS] [-C num] [-D directory] [-g group] [-h host] [-p prompt]
        [-R directory] [-r role] [-t type] [-T timeout] [-u user] [VAR=value]
        [-l | -s] [command [arg ...]]
    sudoedit [-ABkNnS] [-C num] [-D directory] [-g group] [-h host]
        [-p prompt] [-R directory] [-r role] [-t type] [-T timeout] [-u user]
        file ...

DESCRIPTION
    sudo allows a permitted user to execute a command as the superuser or another
    user, as specified by the security policy. The invoking user's real (not
    effective) user-ID is used to determine the user name with which to query
    the security policy.

    sudo supports a plugin architecture for security policies, auditing, and
    input/output logging. Third parties can develop and distribute their own
    plugins to work seamlessly with the sudo front-end. The default security
    policy is sudoers, which is configured via the file /etc/sudoers, or via
    LDAP. See the "Plugins" section for more information.

    The security policy determines what privileges, if any, a user has to run
    sudo. The policy may require that users authenticate themselves with a
    password.

Manual page sudo(8) line 1 (press h for help or q to quit)
  
```

die Befehlszeilen aussehen dürfen, die er dabei verwendet. Bei allen Punkten kann man mit dem Schlüsselwort `ALL` auf eine Prüfung verzichten.

Daneben kann man in der `sudoers`-Datei noch bestimmen, ob Anwender überhaupt ein Kennwort eingeben müssen, und wenn ja, wie lange `sudo` es speichert, bevor es erneut danach fragt; voreingestellt sind 15 Minuten.

Die Liste der Optionen, die `sudo` aus Anwendersicht versteht, ist lang. Zu den wichtigeren gehören `-u` und `-g`, um zu bestimmen, welche Benutzer- beziehungsweise Gruppenidentität man annehmen möchte, und `-i`, um eine interaktive Shell mit anderen Rechten zu starten. Das Konzept, für eine `root`-Sitzung automatisch ein neues Konsolenfenster zu öffnen, ist dem Linux-`sudo` allerdings fremd: Alle Aus- und Eingaben des gestarteten Programms, selbst die einer neuen `root`-Shell, passieren im aktuellen Terminal. Ohnehin ist `sudo` ausdrücklich nicht für GUI-Programme gedacht, die haben andere Mittel und Wege, um sich erweiterte Berechtigungen zu verschaffen.

Für die Beschreibung weiterer Möglichkeiten der Administration und Benutzung von `sudo` unter Linux sei auf die Dokumentation in den `man`-Pages verwiesen; man `sudoers` beziehungsweise man `sudo` bringt Sie hin.

Fazit

Wer sowohl unter Linux oder macOS als auch unter Windows regelmäßig Konsolenprogramme benutzt, wird einen Befehl

Im täglichen Umgang kommt `sudo` unter Linux meist ohne erweiterte Optionen aus, für Spezialfälle stehen aber etliche bereit.

wie `sudo` unter letzterem schmerzlich vermisst haben. Gut also, dass Microsoft sich um dieses Manko kümmert – und höchste Zeit. Dass dabei eine Eins-zu-eins-Kopie des gleichnamigen Linux-Tools herauskommen würde, war nicht zu erwarten: Dazu sind die Sicherheitsarchitekturen in den beiden Betriebssystemwelten zu unterschiedlich. Microsofts `sudo` ist zwar erst in Windows-Vorabversionen verfügbar, trägt aber bereits die Versionsnummer 1.0. Es sieht also danach aus, dass der knappe Funktionsumfang vorerst alles ist, was Microsoft zu dem Thema liefern will.

Dass man ein `sudo`-Gegenstück unter Windows mit ein bisschen mehr Liebe programmieren kann, zeigt `gsudo`. Dessen UAC-Cache und die Möglichkeit, Programme unter beliebigen Benutzerkonten mit frei bestimmbarer Verbindlichkeitsstufe auszuführen, machen es auch nach dem Erscheinen des Microsoft-`sudo` zur ersten Wahl für Konsolennutzer. Einziger Haken: Wenn das `sudo` aus Redmond erst offiziell in Windows enthalten sein wird, werden sie sich umstellen und tatsächlich `gsudo` tippen müssen, wenn sie `gsudo` meinen, weil `sudo` dann Microsofts Kandidaten auf den Plan ruft. (hos@ct.de) **ct**

Literatur

- [1] Axel Vahldiek, Als Admin unter Windows 10, Antworten auf die häufigsten Fragen, c't 11/2018, S. 158

Dokumentationen und Downloads:
ct.de/ypmm



Mach flott

OpenCore Legacy Patcher: Wie Sie alte Macs mit jungem macOS aufbrezeln

Äußerlich mag mancher olle Mac verschlissen aussehen, das Innere funktioniert aber oft auch nach vielen Jahren. Was tun mit so einem Schätzchen? Zum Beispiel mit einem modernen macOS aufrüsten, obwohl Apple das nicht vorsieht.

Von Dušan Živadinović

Viele ältere Macs haben genügend Leistung für moderne Büro-, Mail- und Web-Apps. Dazu gehört das oben abgebildete MacBook Pro mit 13-Zoll-Display von Anfang 2011, das jahrelang einem Fingernageltrommelfeuer getrotzt hat und dann mangels macOS-Updates lange tatenlos in einer Schublade auf sein Ende wartete.

Doch mit dem quelloffenen Projekt OpenCore Legacy Patcher (kurz OCLP) ließ sich das noch junge macOS Ventura darauf einrichten. So laufen heute auf dem

2011er MacBook Pro nicht nur die aktuellen Versionen der Browser von Apple, Google und Mozilla, sondern beispielsweise auch Apples Büroanwendungen Pages und Numbers sowie diverse andere aktuelle Programme. Okay, mit seinem vor 15 Jahren eingeführten Doppelkern Intel Core i5 und 2,3 GHz Takt hat der Klapp-Mac schon bei seinem Erscheinen keinen Speed-Blumentopf gewonnen und aktuelle Geräte schlucken bei denselben Aufgaben weit weniger Strom. Doch auch ein langsamer Computer ist allemal besser als keiner und die Auffrischung ist im Sinne der Nachhaltigkeit.

Von Apple bis Zäsur

Inzwischen gibt es viele Macs, für die Apple sein macOS nicht mehr anpasst. Die Versorgung endet nach etwa fünf Jahren. Derzeit erhalten Macs, die gerade noch keinen T2-Sicherheitschip bekommen haben, kein Upgrade auf Sonoma (macOS 14). Bei hochpreisigen und überdurchschnittlich leistungsfähigen Modellen ver-

längert Apple die Frist nach Gutdünken, begründet aber nie, warum es die Versorgung einstellt oder fortführt.

Für das Altaluminium heißt es dann: Softwarekomponenten verlieren langsam den Anschluss. Bei Internetanwendungen fällt das am deutlichsten auf, weil die Gültigkeit der TLS-Zertifikate abläuft und dann alte Browser und andere Anwendungen keine verschlüsselten HTTPS-Verbindungen mehr aufbauen können. Neue Browser werden für veraltete Macs aber nicht mehr angepasst, sodass ein eigentlich ausreichend leistungsfähiges MacBook nach einigen Jahren nicht mal mehr zum Surfen taugt.

Mangels aktueller Apple-Zertifikate lässt sich auch der App Store mit High Sierra nicht mehr öffnen und daher bleibt man von sämtlichen dort veröffentlichten Updates abgeschnitten. Auch die Entwickler quelloffener Software versorgen die alten Betriebssysteme früher oder später nicht mehr. Beispielsweise läuft der Paketmanager Homebrew, über den man eine Vielzahl nützlicher Kommandozeilenprogramme beziehen kann, zurzeit erst ab macOS Monterey. Aber auch der Support für Monterey wird früher oder später gestrichen.

Für Sicherheitspatches gilt Ähnliches: Die reicht Apple zwar noch einige Jahre für Macs nach, die älter als fünf Jahre sind, aber man weiß nicht, wie lange.

Deshalb erscheint der OpenCore Legacy Patcher auf den ersten Blick attraktiv; denn er öffnet vielen betagten Macs den Weg zu einem aktuellen macOS. Laut den OCLP-Dokumenten lässt sich jeder Intel-Mac ab dem Erscheinungsjahr 2008 auf ein modernes macOS aufrüsten, vorausgesetzt, im Mac steckt eine 64-Bit-CPU. Doch bevor Sie die Installation in Angriff

nehmen, gibt es einiges zu bedenken und abzuwägen.

Wenn es um Sicherheit geht, sollte man OCLP nicht nehmen, weil es elementare Sicherheitsfunktionen deaktiviert. Einzelheiten dazu stehen im Kasten SIP-Unsicherheit auf Seite 141.

Bei MacBooks sollte man zuerst klären, ob der Akku noch ausreichende Laufzeiten liefert, denn je älter das MacBook, desto schwieriger findet man Ersatz.

Als Zweites empfiehlt es sich, den Beipackzettel des OCLP gründlich zu lesen. Dort sind diverse kleine und einige große Inkompatibilitäten für einzelne Mac-Modelle und macOS-Versionen aufgeführt (siehe ct.de/y6gs). Beispielsweise patcht das OCLP-Team das Ziel-macOS, um Non-Metal-GPUs als Beschleuniger zu nutzen, aber bis OCLP 1.4.2 ist das nur für Ventura und ältere macOS-Versionen fertig. Vom aktuellen macOS Sonoma sollte man daher vorerst die Finger lassen, es sei denn, man möchte zu den ersten gehören, die das taufrische OCLP 1.4.3 ausprobieren.

Auch wenn man auf dem Massenspeicher Windows als Bootcamp-Partition oder Linux eingerichtet hat, knirscht es. In diesem Setup findet der Patcher die Mac-Partition nicht zuverlässig, sodass die Installation auf halbem Weg scheitern kann. Am einfachsten ist daher, die zusätzlichen Partitionen vor der Installation zu entfernen.

Alte Software läuft auf jüngeren macOS-Versionen möglicherweise nicht. Beispielsweise verweigert die Fotoverwaltung Adobe Lightroom 6.x, die ursprünglich macOS Mojave vorausgesetzt hat, ab Monterey den Start. Adobe pflegt diesen Lightroom-Zweig nicht mehr und man ist auf cloudgestützte Versionen und damit auf Adobes Abotarife angewiesen.

Aufrüststrategie

Um böse Überraschungen zu vermeiden, teilen Sie die Aufrüstung in zwei Phasen: Zuerst prüfen Sie, ob Ihre benötigten Anwendungen auf dem Ziel-macOS zuverlässig laufen. Richten Sie beide am besten auf einem Duplikat des aktuellen Massenspeichers ein. Bei älteren Macs mit Intel-CPU und internem SATA-Anschluss geht das ohne Geschwindigkeitsverlust, wenn man den Inhalt der internen SATA-Platte auf eine andere kopiert (zum Beispiel mit SuperDuper oder Carbon Copy Cloner), das Duplikat in den Mac einsetzt und das Ziel-macOS aufspielt. Bei Macs mit aufgelötetem internen Massenspeicher ist man auf externe Medien angewiesen. Mit USB 3.x oder Thunderbolt ab 5 Gbit/s geht das ohne große Geschwindigkeitseinbußen.

Erst wenn der Mac, das neue macOS und die Anwendungen Ihre Prüfungen bestanden haben, sollten Sie in Tuning-Maßnahmen investieren. Als Erstes empfiehlt sich eine SSD als Boot- und Datenmedium, dann je nach Ausbau auch eine RAM-Aufrüstung.

Im 2011er MacBook Pro haben wir die 500-GB-SSD 860 EVO von Samsung verwendet und damit machte der alte Klapp-Mac eine gute Figur. Gegenüber Festplatten mit magnetischem Aufzeichnungsverfahren verkürzt die SSD die Startzeiten der Anwendungen erheblich und auch die nach der macOS-Installation unumgängliche Indexierung des Massenspeichers. So funktionierte das 2011er MacBook Pro nach rund einer Indexierungsstunde selbst mit 4 GByte RAM hinreichend schnell, sodass wir auf den möglichen Vollausbau auf 16 GByte verzichtet haben; bei speicherfressenden Anwendungen wären die 30 bis 50 Euro für zwei



Der quelloffene OpenCore Legacy Patcher bringt alte Macs und junge macOS-Versionen zusammen. Dann laufen auf alten Macs doch wieder aktuelle Anwendungen.



Da alte Macs von Apples Softwareversorgung abgeschnitten sind, bringt der Patcher eigene Funktionen mit, um aktuelle Mac-Betriebssysteme von Apples Server zu laden.

8-GB-Module aber gut investiertes Geld (siehe ct.de/y6gs).

Installation vorbereiten

Bevor es nun an die Installation geht, sollten Sie beispielsweise mit Time Machine ein Backup anfertigen, am besten auf einem USB-Laufwerk, um bei Zugriffen auf ein NAS etwaigen Netzwerkproblemen von vornherein aus dem Weg zu gehen.

Für Macs ohne integrierte Tastatur: Legen Sie sich für den Notfall ein kabelgebundenes Keyboard und eine ebensolche Maus bereit, falls sich die Bluetooth-Tastatur und -Maus nicht anbinden lassen. Außerdem ist zu beachten, dass Apple ab macOS Ventura die Treiber für USB 1.1 gestrichen hat, was man aber auf vielen älteren Macs für den Anschluss von externen Tastaturen und Mäusen braucht. An dieser Stelle springt ein Hub ein, der von USB-2-Peripherie auf USB 1.1 am Mac umsetzt. Im Einzelnen handelt es sich um MacBooks vor 2010, iMacs vor 2009, Mac mini vor 2011 und Mac Pro vor 2012.

In jedem Fall brauchen Sie einen USB-Stick mit mindestens 16 GByte Kapazität oder eine USB-SSD (je schneller, desto besser). Um die Übersicht zu wahren, trennen Sie vor der Installation alle übrigen USB-Laufwerke vom Mac.

Prinzipiell könnte man OCLP auf ein frisch formatiertes Medium installieren. Das empfiehlt sich aber nur, wenn man

anschließend keine Daten aus einem Backup einspielen will, denn bei OCLP-behandelten Macs kann das scheitern. Und wenn man den Massenspeicher eines MacBook Pro mit T1-Chip löscht, tilgt man damit auch die T1-Firmware. Bisher ist aber kein Weg bekannt, diese wiederherzustellen, sodass das MacBook zum Edelschrott wird. Deshalb spielt man mit OCLP das Ziel-macOS wie ein Update über das alte macOS drüber; der Mac wird nicht neu aufgesetzt, Ihre Daten bleiben erhalten.

Installation

Starten Sie den Mac, bringen Sie ihn ins Internet und laden Sie die aktuelle Version des Legacy Patcher von GitHub (ct.de/y6gs); die Datei heißt OpenCore-Patcher-GUI.app.zip. Entpacken Sie das Archiv, schieben Sie die App in den Programme-Ordner und starten Sie sie.

Der Patcher enthält fünf Menüs: „Build and Install OpenCore“, „Create macOS Installer“, „Post Install Root Patch“, „Support“ und „Settings“. Im Menü Settings gibt es noch das mittig angebrachte „Target Model“, in dem man bei Problemen das Mac-Modell einstellen kann. Den tatsächlichen Modellnamen kann man zum Beispiel aus Programme-/Dienstprogramme/Systeminformationen im Menü Hardware-Übersicht auslesen. Im Normalfall genügt es, dieses Menü auf

der Voreinstellung zu belassen; dann steht dort einfach „Host Model“.

Wenn alles bereit ist, klicken Sie auf „Create macOS Installer“ und auf „Download macOS Installer“. Wählen Sie dann ein geeignetes macOS aus. Wir haben OCLP mit Ventura 13.6.6 ausprobiert. Von Betaversionen raten wir ab, weil nicht gewährleistet ist, dass alle Hard- und Software-Funktionen einwandfrei laufen.

Die Downloadgeschwindigkeit hängt vom Durchsatz Ihres Internetanschlusses ab und hat mit Ventura (13 GByte) bei einer 250-Mbit/s-Leitung rund 10 Minuten gedauert.

Wenn der Vorgang beendet ist, geben Sie auf Nachfrage das Admin-Passwort ein und bestätigen Sie mit „OK“, damit der Patcher den Installer erstellt. Klicken Sie auf „Yes“, wählen Sie den heruntergeladenen Ventura-Installer und erlauben Sie dem Patcher den Zugriff auf den Stick. Wählen Sie dann erneut das USB-Laufwerk aus, damit der Patcher den Stick formatiert und den Installer einrichtet.

Nach erneuter Eingabe des Admin-Passworts wird der für das gegebene Mac-Modell angepasste macOS-Installer auf den Stick geschrieben. Falls die Fortschrittsanzeige stehen bleibt, brechen Sie den Vorgang auf keinen Fall ab, sondern warten Sie ab, bis es weitergeht. Je nach Stick-Geschwindigkeit kann das über eine halbe Stunde dauern.

OpenCore-Firmware installieren

Ist das Installationsmedium fertig, fragt der Patcher, ob Sie den OpenCore-Bootloader auf das Systemvolumen des Macs („this disk“) installieren wollen. Bestätigen Sie mit „Yes“. Der Installer stellt dann die passenden Parameter für Ihren Mac zusammen und fragt noch einmal, ob Sie tatsächlich installieren wollen. Nach der Bestätigung mit „Install to Disk“ wählen Sie die Systemfestplatte aus (normalerweise „disk0“, farblich unterlegt), auf der der Legacy Patcher die EFI-Partition findet. Klicken Sie diese an, geben Sie das Admin-Passwort ein und warten Sie ab, bis die Daten auf die EFI-Partition geschrieben werden. Klicken Sie auf „Reboot“ und halten Sie während des Boot-Sounds die Alt-Taste gedrückt. Dann sollte das Boot-Menü erscheinen.

Es enthält mindestens ein Volume mit OpenCore/Boot EFI und eines mit dem üblichen Mac-Massenspeicher. Klicken Sie auf den Pfeil unter OpenCore/Boot EFI



Der quelloffene OpenCore Legacy Patcher fügt aktuellen macOS-Versionen die für obsoletere Macs erforderlichen Treiber hinzu. Dafür muss er je nach Modell verschiedene Sicherheitsfunktionen abschalten.

und gleich danach auf „Install macOS Ventura“ beziehungsweise die von Ihnen gewählte macOS-Version. In der Voreinstellung hat man dafür nur fünf Sekunden Zeit, dann bootet unerwünschtermaßen die Standardpartition. Falls das passiert, wiederholen Sie den Vorgang ab dem Reboot.

Wenn schließlich der Installer läuft, wählen Sie „macOS Ventura“ und klicken Sie mehrmals auf „Fortfahren“ bis zur Auswahl des Zielmediums. Wählen Sie dort den Massenspeicher mit macOS aus. Auf dem 2011er MacBook Pro hat der Vorgang rund 30 Minuten gedauert. Anschließend startet der Mac für die letzten Schritte automatisch neu.

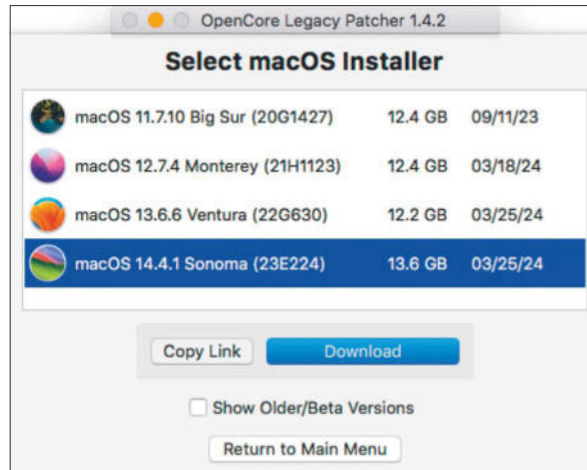
Ventura-Erfahrungen

Nach der Anmeldung am MacBook und mit der Apple-ID laufen aufwendige Synchronisierungs- und Indexierungsvorgänge ab. Dabei dreht der Lüfter vernehmlich, klingt dann nach einer Weile aber ab. Beim 2011er Mac waren diese Vorgänge nach rund einer Stunde abgeschlossen und die CPU-Auslastung sank von rund 80 bis 90 Prozent auf 20 bis 30. Damit hat diese Maschine genügend Reserven für übliche Anwendungen, was sich im Laufe von mehreren Wochen mit Pages, Safari, Firefox und diversen anderen Anwendungen bestätigte. Keynote stürzte bei Präsentationsstarts aber regelmäßig ab.

Auch wachte das MacBook nicht immer selbstständig aus dem Tiefschlaf auf, wenn ihm bei zugeklapptem Deckel der Strom ausging. Anschließend fand es die Bootpartition nicht und öffnete unerwünscht die macOS-Wiederherstellung.

In diesem Fall hilft es, das MacBook hart auszuschalten und beim Startton die Alt-Taste gedrückt zu halten. Dann blendet es wie erwartet das Volume OpenCore/Boot EFI ein. Klickt man es an, kann man die Bootpartition mit dem neuen macOS per Hand auswählen und der Mac setzt das Aufwachen aus dem Tiefschlaf korrekt fort. Am Ende blendet er den Zustand ein, den er hatte, bevor der Akku leergelaufen war.

Drei letzte Tipps noch: Setzen Sie zur Installation lieber eine ältere, als zuverlässig bewertete Patcher-Version ein, um die Fehlerwahrscheinlichkeit möglichst gering zu halten. Wir haben aus diesem Grund den Patcher 1.4.2 verwendet, obwohl 1.4.3 veröffentlicht ist, das Sonoma und Macs ohne Metal-GPU zusammenbringen soll. Fehlerberichte von Anwendern findet man beispielsweise auf dem Discord-Server der Entwickler.



Falls Sie ein älteres macOS einrichten, also wie im Beispiel Ventura, dann fordert das Betriebssystem immer mal wieder zum Update auf das aktuelle Sonoma auf. Das ist lästig und kann dazu führen, dass man ein großes Update versehentlich installiert, obwohl OCLP dafür nicht bereit ist. Um dem vorzubeugen, sollte man die Aufforderung für eine Weile abschalten. Das geht mit folgendem Kommando:

```
defaults write com.apple.SoftwareUpdate
MajorOSUserNotificationDate
-date "2026-01-01 23:59:00 +0000"
```

Danach bleibt die Aufforderung bis Anfang 2026 aus.

Das gepatchte macOS lässt sich über die integrierte Softwareaktualisierung auf den neuesten Stand bringen, also etwa von

Ventura 13.6.6 auf ein hypothetisches 13.6.7. Der Patcher detektiert den Vorgang und startet danach automatisch. Klicken Sie dann auf Post-Install Root Patch und installieren Sie die voreingestellten Treiber neu.

Fazit

Mit dem Patcher muss man zwar einige Zeit investieren, um einen alten Mac auf den aktuellen macOS-Stand zu bringen, aber das Ergebnis rechtfertigt den Aufwand, wenn man keine großen Anforderungen an die Rechenleistung stellt. Erstaunlich, dass Apple partout kein finanziell einträglicher Weg einfallen will, um selbiges zu leisten; das ginge dann garantiert ohne Verlust der System Integrity Protection. (dz@ct.de)

OCLP-Download und -Doku: ct.de/y6gs

SIP-Unsicherheit

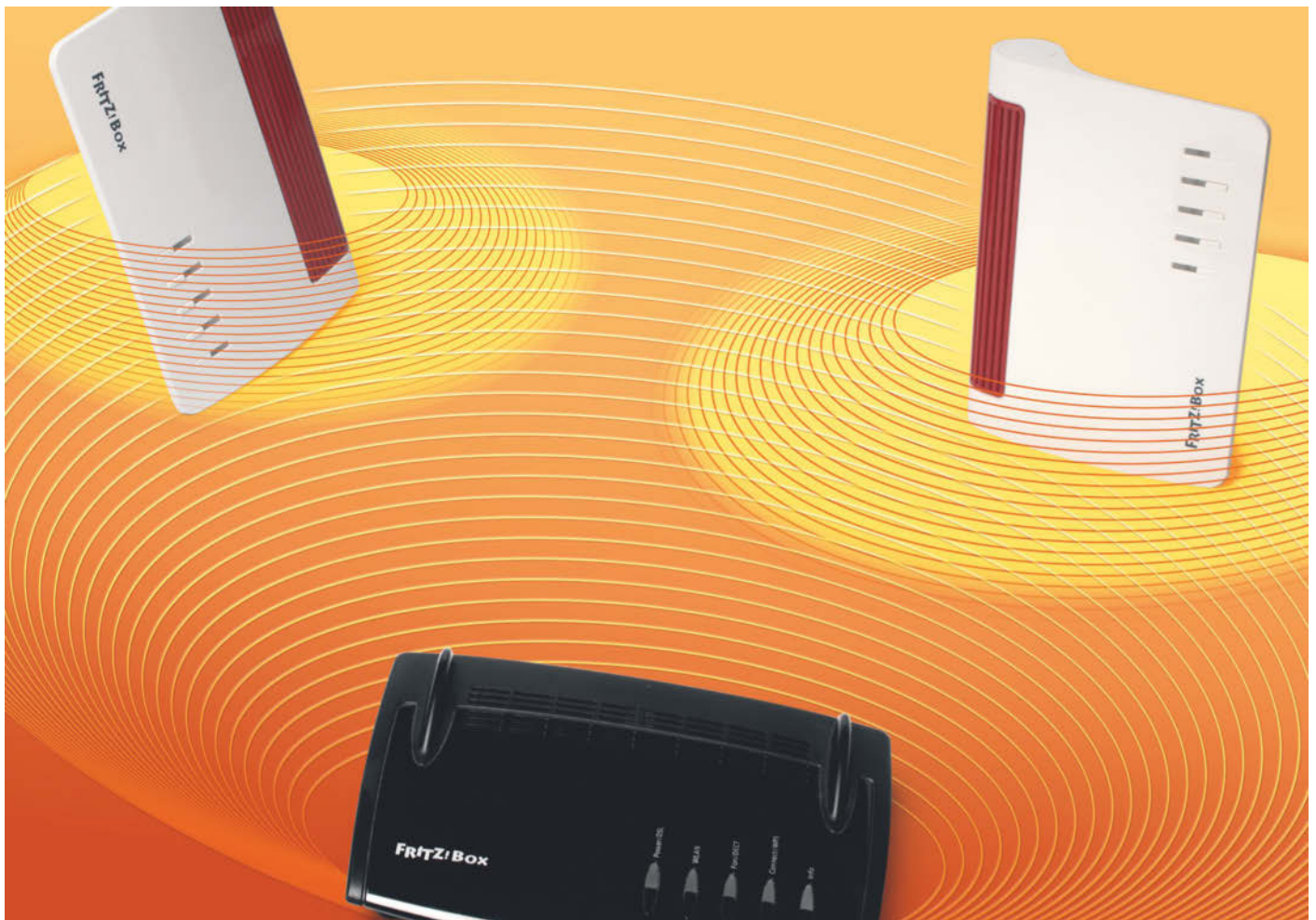
Bekommt ein Mac das jüngste macOS nicht mehr, versorgt ihn Apple zwar noch eine Weile mit Patches für Sicherheitslücken, aber auch dieser Softwarestrom versiegt nach weiteren zwei, drei Jahren. Deshalb erwägen manche Nutzer, einen von Apple verstoßenen Mac unter Einsatz des OCLP mit einem aktuellen macOS aufzufrischen. Doch die moderne, abgedichtete Software bekommt man nur auf Kosten der Systemsicherheit, denn OCLP schaltet je nach Hardwareplattform und Zielbetriebssystem Teile der 2015 eingeführten System Integrity Protection ab (SIP).

Zwar lassen sich alle SIP-Funktionen nach Installation des Zielbetriebssystems per Hand reaktivieren, doch der Mac funktioniert dann meist nicht mehr rich-

tig, falls er bei komplett eingeschalteter SIP überhaupt noch bootet.

Beispielsweise schaltet OCLP ALLOW_UNTRUSTED_KEXTS und ALLOW_UNRESTRICTED_FS ab. Erst so lassen sich Treiber für die von Apple nicht mehr berücksichtigte Hardware in Form von unsignierten Kernel-Erweiterungen (Kernel Extensions, Kexts) der Community aufspielen. Außerdem schaltet OCLP ALLOW_UNAUTHENTICATED_ROOT ein und damit die kryptografische Absicherung des Dateisystems ab. Damit ist der Mac anfällig gegen Malware, die es auf zentrale Systembestandteile abgesehen hat.

Wenn Sie auf Sicherheit großen Wert legen, fassen Sie lieber Windows oder Linux ins Auge. Auf Intel-Macs kann man beide ohne Weiteres auch als virtuelle Maschinen ausprobieren.



Nachbarschaftsrouter

Heimnetzgrenzen überwinden mit OpenWrt

Ob Netzwerkkamera, IP-Türsprechstelle, NAS oder Drucker: Es gibt einige Geräte, die man gut mit vertrauten Nachbarn teilen kann. Routing zwischen mehreren Heimnetzen oder auch nur Zugang zu einigen Geräten klappt mit einem OpenWrt-Router – so richten Sie die Netzbrücke ein.

Von Andrijan Möcker

Vor Kurzem erreichte uns eine interessante Leserfrage: Wie kann man in einem Zwei-Parteien-Haus eine VoIP-Tür-

sprechstelle mit zwei Klingeltastern für beide Parteien nutzbar machen, ohne dass die beiden voneinander abhängig sind? VoIP-Türsprechstellen können sich häufig in mehrere SIP-Server einbuchen, besitzen aber meist nur einen Netzwerkanschluss – auch, wenn zwei oder mehr Klingeltaster vorhanden sind.

Das schließt auf den ersten Blick den Einsatz mit mehreren Parteien aus und eine VPN-Verbindung zwischen beiden Routern würde Abhängigkeit bedeuten. Gäste sollen aber nicht unbemerkt vor der Tür stehen, nur weil der Internetanschluss von Partei A, an dem die Türsprechstelle hängt, gerade eine DSL-Störung hat. Einen Switch kann man auch nicht einfach setzen, weil dann die Netztrennung auf Layer 2 fehlt. Schließlich soll jeder noch seinen eigenen Internetanschluss nutzen.

Die Lösung des Problems ist ein zusätzlicher Nachbarschaftsrouter, der mehrere virtuelle Netze unterstützt und in beiden Heimnetzen eine eigene (LAN-) Schnittstelle mit jeweils einer IP-Adresse aus dem jeweiligen Netz besitzt. In diesen Bereichen verhält er sich wie ein Client. Das oder die gemeinsam genutzten Geräte platziert man in einem dritten Subnetz, in dem der Nachbarschaftsrouter auch IP-Adressen vergibt.

Ob die zwei Heimnetze auch untereinander kommunizieren können, ist nur eine Frage der Firewallkonfiguration. In diesem Artikel zeigen wir, was Sie für die Brücke zwischen den Netzen benötigen und wie Sie wahlweise ausschließlichen Zugriff auf die geteilten Geräte oder ungehindertes Routing zwischen den beiden Heimnetzen konfigurieren. Dafür benut-

c't kompakt

- Routing zwischen Heimnetzen ist möglich, wenn die Router statische Routen beherrschen.
- OpenWrt unterstützt mehrere virtuelle Interfaces.
- Diese Interfaces können in unterschiedlichen Heimnetzen sein, sodass OpenWrt dazwischen routen kann.

zen wir das quelloffene Router-Betriebssystem OpenWrt, das komplexe Netzwerkaufbauten mit vielen unterstützten Routern ermöglicht, auch auf günstiger Gebrauchthardware.

Dieser Artikel setzt voraus, dass Sie ein grundlegendes Verständnis von IPv4-Adressen und Netzwerkkonfigurationen haben sowie Schulenglisch inklusive einiger IT-Vokabeln beherrschen.

Voraussetzungen

Für Zuverlässigkeit und stabile Datenrate müssen die beiden Netze per Kabel zum Brückenrouter gelangen, beispielsweise in einem gemeinsamen Keller. Router mit zwei WLAN-Interfaces könnten sich zwar in das 2,4-GHz-WLAN des einen Routers und das 5-GHz-WLAN des anderen einbuchen, durch automatische Kanalwechsel, Nachbarnetze und Wetterradar käme es aber regelmäßig zu Aussetzern. Falls Sie keine Netzwerkkabel legen können, taugen je nach Länge bereits verlegte vieradrige Telefonleitungen für Fast-Ethernet. Die damit erreichten 100 MBit/s genügen massig für Anwendungen wie Netzwerkdruker oder IP-Türsprechstellen. Wie Sie Netzwerkkabel günstig verlegen oder eine alte Telefonleitung umfunktionieren, lesen Sie in [1, 2].

Damit Sie aus beiden Netzen auf gemeinsame Geräte und optional das jeweils benachbarte Heimnetz zugreifen können, müssen die Heimnetzrouter statische Routen erlauben. Diese Einstellung teilt dem Heimnetzrouter mit, dass sich in seinem Subnetz ein weiterer Router befindet, über den andere Subnetze erreichbar sind.

Beispiel: Der erste Heimnetzrouter hat die IP-Adresse 192.168.175.1, der Brückenrouter in seinem Subnetz die 192.168.175.10 und das entfernte Subnetz ist 192.168.178.0. Dann lautet die Route 192.168.178.0/24 via

192.168.175.10. Die Geräte im 175.0-Subnetz müssen davon nichts wissen: Trifft nach der Konfiguration ein Paket für das entfernte Heimnetz (etwa an .178.23) am Heimnetzrouter (.175.1) ein, schiebt dieser das Paket an den Brückenrouter (.175.10), der ein zweites Interface im entfernten Subnetz (etwa 178.10) hat. Umgekehrt muss der Router im entfernten Subnetz (.178.1) ebenso vom Brückenrouter (178.10) in seinem Subnetz wissen, sodass die Antwort ins andere Subnetz zurückfindet.

In (semi-)professionellen Routern gehören statische Routen zur Standardausstattung; AVMs FritzOS beherrscht sie ebenso. Standard-Privatkundenroutern wie Speedports oder EasyBoxen fehlt die Funktion aber meist. Details verrät die Anleitung Ihres Geräts.

Besitzen beide Heimnetzrouter die Funktion, müssen Sie nur noch sicherstellen, dass diese unterschiedliche Subnetze benutzen, also etwa 192.168.175.0 und 192.168.178.0.

Hardware

Als Brückenrouter setzen wir in diesem Artikel die Fritzbox 7362 SL ein. Sie wird von OpenWrt unterstützt und besitzt jeweils 128 MByte Massen- und Arbeitsspeicher, was Platz für noch einige Jahre OpenWrt-Updates verspricht. Die Netzwerkanbindung läuft über zwei Gigabit- und zwei Fast-Ethernet-Ports. Das genügt, um zwischen zwei Heimnetzen hin und her zu routen und noch weitere Hardware in einer Zwischenwelt zu betreiben. Der WLAN-Chip der Box spricht nur ver-

altetes Wi-Fi 4 auf 2,4 GHz; den lassen wir ohne schlechtes Gewissen brach liegen.

Wir nutzen die Fritzbox als Beispiel, weil sie sehr günstig ist: Auf Kleinanzeigenportalen zahlt man für die 7362 SL kaum mehr als 'n Appel und 'n Ei. Die Schritte zur OpenWrt-Installation auf dem Gerät lassen wir in diesem Artikel aus. Eine genaue Beschreibung finden Sie wahlweise im OpenWrt-Wiki oder in unserem Artikel zu OpenWrt auf der 7362 SL [3]. Verzichten Sie jedoch auf die im Absatz „Netzwerk“ vorgeschlagenen Änderungen der Konfiguration.

Mit anderer OpenWRT-kompatibler Hardware funktioniert das ebenso. Die Installationsschritte können jedoch abweichen und erfordern möglicherweise weitere Recherche.

Wir setzen in der Grundeinrichtung bei einer frisch installierten OpenWrt-Box mit aktueller Version (23.05.2) an, die Sie bereits per Kabel mit Ihrem Rechner verbunden und im Webinterface (<http://192.168.1.1>) ein sicheres Administrator-kennwort konfiguriert haben. Die beiden Heimnetze dürfen noch nicht angeschlossen werden.

Grundeinrichtung

Nur wenn die verwendeten Subnetze sich nicht überschneiden, klappt das Routing zwischen allen problemlos. Nutzen beide beispielsweise das Fritzbox-Standard-Subnetz 192.168.178.0/24 müssen Sie in einem der beiden Heimnetze in den sauren Apfel beißen und ein anderes Subnetz wie 192.168.175.0 einstellen. In FritzOS



Die Fritzbox 7362 SL gibts für 5 bis 20 Euro im Netz. Ersetzt man FritzOS durch OpenWrt, kann man mehrere virtuelle Interfaces anlegen und so zwischen Heimnetzen hin und her routen.

Zwischenrouter

Status ▾System ▾Network ▾Log out

REFRESHING

Interfaces

Devices

Global network options

DSL

ATM Bridges

Interfaces

lan

lan

br-lan

Protocol: Static address

Uptime: 1h 2m 31s

MAC: 38:10:D5:6B:6E:C0

RX: 845.87 KB (7733 Pkts.)

TX: 2.37 MB (7528 Pkts.)

IPv4: 192.168.21.1/24

IPv6: fd4a:7194:8ddb::1/60

Restart

Stop

Edit

Delete

Mueller

lan2

Protocol: DHCP client

Uptime: 1h 1m 46s

MAC: 38:10:D5:6B:6E:C0

RX: 2.94 MB (30444 Pkts.)

TX: 45.28 KB (411 Pkts.)

IPv4: 192.168.73.171/24

Restart

Stop

Edit

Delete

Schmidt

lan1

Protocol: DHCP client

Uptime: 1h 1m 43s

MAC: 38:10:D5:6B:6E:C0

RX: 2.01 MB (11099 Pkts.)

TX: 481.66 KB (3838 Pkts.)

IPv4: 192.168.59.132/24

Restart

Stop

Edit

Delete

Der Nachbarschaftsrouter besitzt in jedem Heimnetz ein virtuelles Interface. Teilt man den beiden Heimnetzroutern über Routen mit, dass die Brücke existiert, können Geräte über die Heimnetzgrenzen hinweg kommunizieren.

finden Sie die Einstellung unter Heimnetz/Netzwerk im Reiter Netzwerkeinstellungen/IPv4-Einstellungen. Ob und wie Sie das bei anderen Router-Betriebssystemen erledigen können, erfahren Sie in den Anleitungen der Geräte.

Nach dem Wechsel trennen Sie alle Geräte im Netz kurz, damit diese eine IP-Adresse aus dem neuen Bereich bekommen. Solche mit fester Adresse müssen Sie neu konfigurieren.

Frisch installiert nutzt OpenWrt das Subnetz 192.168.1.0/24. Passt Ihnen das nicht in die Heimnetzkonfiguration(en), öffnen Sie das OpenWrt-Webinterface und wechseln in die Interface-Übersicht (Network/Interfaces). Dort klicken Sie bei „br-lan“ auf „Edit“ und ändern die „IPv4 address“, zum Beispiel auf 192.168.21.1. Bestätigen Sie mit „Save“ und klicken Sie „Save & Apply“ am unteren Ende der Schnittstellenliste.

OpenWrt warnt Sie dabei, dass das Wechseln der IP-Adresse zum Verbindungsverlust führen kann, wenn Sie sich vertippt haben und bietet Ihnen „Apply with revert after connectivity loss“ an. Nehmen Sie das Angebot an, wartet das System 90 Sekunden darauf, dass Sie sich wieder mit dem Webinterface verbinden, ansonsten werden die Änderungen rückgängig gemacht.

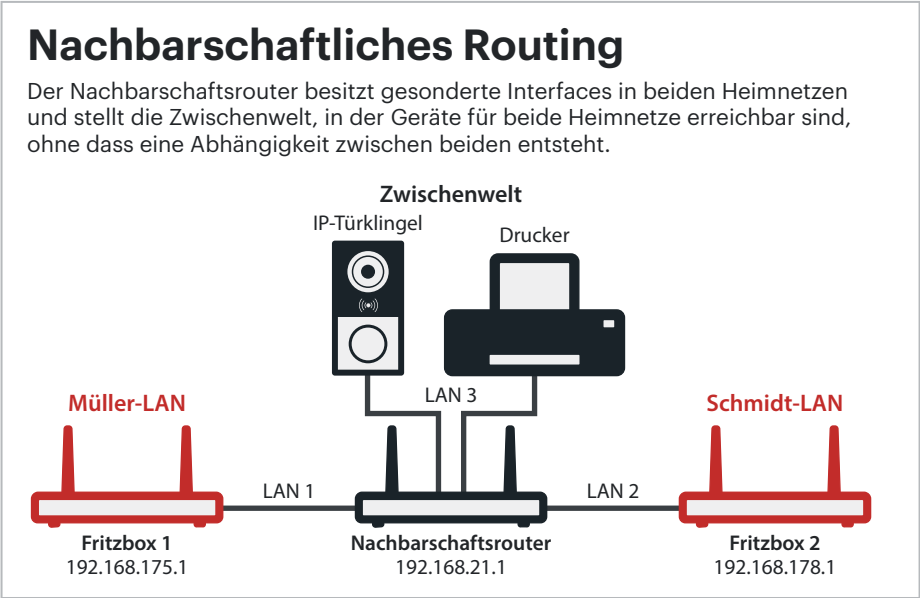
Klicken Sie die Option und trennen Sie anschließend die Verbindung kurz, beispielsweise, indem Sie das LAN-Kabel abstecken. Sobald die Verbindung wiederhergestellt ist, rufen Sie das Webinterface unter der neuen Adresse (in unserem Beispiel 192.168.21.1) wieder auf.

Wollen Sie, dass der Nachbarschaftsrouter mit einem aussagekräftigen Namen im Netzwerk auftaucht, ändern Sie den „Hostname“ in „System/System“. Sollte

irgendwann einmal das Auslesen der Logs nötig sein, stiftet eine falsche Zeitzone möglicherweise Verwirrung; die korrekte „Timezone“ können Sie im selben Menü einstellen.

Netzwerkinterfaces

In der Startkonfiguration sind in OpenWrt alle LAN-Ports einem virtuellen Brückeninterface zugewiesen. Damit Sie die Ports gleich neuen Heimnetz-Interfaces zuwei-



Was ist der

Hype

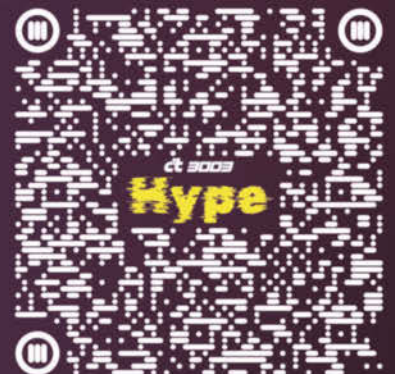
wirklich wert?



ct 3003 Newsletter

In Hype nehmen Keno und Lukas Tech-Trends genau unter die Lupe!

Jetzt KOSTENLOS abonnieren:
ct.de/hype



Wenn Ihr Netzwerk aus mehreren Subnetzen besteht, die nicht direkt mit der FRITZ!Box verbunden sind, können Sie für diese statische IPv4-Routen in der FRITZ!Box einrichten.

Achtung!
Änderungen auf dieser Seite können dazu führen, dass die FRITZ!Box nicht mehr erreichbar ist. Beachten Sie unbedingt die Hilfe, bevor Sie Änderungen vornehmen.

Aktiv	Netzwerk	Subnetzmaske	Gateway
<input checked="" type="checkbox"/>	192.168.21.0	255.255.255.0	192.168.59.132

Neue IPv4-Route

Statische Routen teilen dem Router mit, dass es weitere Subnetze gibt, die über einen anderen Router in seinem Subnetz erreichbar sind (hier: FritzOS).

sen können, müssen Sie diese zunächst aus dem existierenden Brückeninterface entfernen. Wechseln Sie dazu unter Network/Interfaces in den Reiter „Devices“ und klicken Sie bei „br-lan“ auf „Configure“.

Im Ausklappenmenü „Bridge Ports“ entfernen Sie die Haken bei allen Ports, die Sie zum Anschließen anderer Heimnetze nutzen möchten. In diesem Beispiel nutzen Sie dafür die beiden Gigabit-Ports LAN 1 und 2, belassen Sie also nur LAN 3 und 4 ausgewählt. Bestätigen und stecken Sie Ihren Rechner auf LAN 3 oder 4, sofern Sie über LAN 1 oder 2 verbunden waren. Über diese Ports ist das Webinterface vorerst nicht mehr erreichbar.

Jetzt können Sie das erste Heimnetz-Interface erstellen: Wechseln Sie in den Reiter „Interfaces“ und klicken Sie auf „Add new interface“. Vergeben Sie einen aussagekräftigen Namen wie „Schmidt“ und wählen Sie in „Device“ LAN 1 oder 2 aus.

Welches „Protocol“ Sie auswählen müssen, hängt davon ab, ob der jeweilige Heimnetzrouter DHCP-Adressreservierungen anlegen, also einem Gerät immer dieselbe IP-Adresse zuweisen kann. Eine feste IP-Adresse am Nachbarschaftsrouter ist essenziell für statisches Routing, andernfalls bekommt er mit Ablauf des DHCP-Leases eine neue Adresse und die Pakete versenden sich. Unterstützt Ihr Router Adressreservierungen, wie bei Fritzboxen der Fall, machen Sie das Interface zum „DHCP client“. Fehlt sie hingegen, wählen Sie „Static address“, um die Adresse selbst festzulegen. Bestätigen Sie die Auswahl mit „Create interface“.

Haben Sie „DHCP client“ ausgewählt, müssen Sie im folgenden Fenster nur noch in „Firewall settings“ eine Zone zuweisen: Wollen Sie, dass Geräte aus beiden Heimnetzen und der Zwischenwelt ungehindert

miteinander kommunizieren können, weisen Sie einfach die existierende Zone „lan“ zu. Andernfalls klicken Sie in das Feld „custom“ im Ausklappenmenü, geben einen beliebigen Namen für die neue Zone ein und bestätigen mit Enter. Sie kann heißen wie das Interface.

Müssen Sie die Adresse selbst zuweisen (Static address), verlangt das nächste Menü eine IP-Adresse aus dem jeweiligen Heimnetz, die Subnetzmaske und das Gateway: Um die IP-Adresse korrekt zu vergeben, schauen Sie zunächst im jeweiligen Heimnetzrouter nach dem eingestellten DHCP-Adressbereich. Die händisch eingetragene IP-Adresse sollte nicht in diesem Bereich liegen, da manche Router nicht überwachen, welche Adressen im Netz schon in Gebrauch sind. Das kann zu störenden IP-Adresskonflikten führen. Geht der DHCP-Bereich etwa von .50 bis .200, dürfen Sie Adressen ab .201 händisch vergeben, in unserem Szenario vollständig ausgeschrieben also 192.168.178.201.

Die Subnetzmaske ist in Heimnetzen nahezu immer 255.255.255.0. Das Gateway ist die Adresse des jeweiligen Heimnetzrouters, typischerweise die 1, also in der Fritzbox-Werkseinstellung 192.168.178.1.

Auch in diesem Fall stellen Sie im Reiter „Firewall configuration“ eine Zone ein, bestätigen die Einstellungen und übernehmen sie mit „Save & Apply“.

Wiederholen Sie den Einrichtungsprozess für das zweite Heimnetz und dessen Adressbereich. Sind beide Interfaces bereit, stecken Sie die Netzkabel an die zugehörigen Ports; unter Status/Overview können Sie im „Port status“ beobachten, ob eine Verbindung zustande kommt. Sofern Sie Interfaces im DHCP-Modus konfiguriert haben, sollten Ihnen kurze Zeit später Adressen in der Liste angezeigt werden.

Firewallkonfiguration

Sofern Sie beide Heimnetz-Interfaces in die Firewallzone „lan“ geworfen haben, müssen Sie nichts an der Firewallkonfiguration ändern. OpenWrt routet Pakete dann beliebig zwischen den beiden Heimnetzen und der Zwischenwelt hin und her. Auch das Webinterface ist von überall erreichbar. In diesem Fall überspringen Sie den Text bis zu den statischen Routen.

Haben Sie beim Anlegen der Interfaces neue Zonen erstellt – wir haben sie „schmidt“ und „mueller“ genannt – müssen Sie diese jetzt mit Regeln versehen: Wechseln Sie in Network/Firewall und klicken Sie bei der ersten neuen Zone auf „Edit“. Erlauben Sie bei „Allow forward to/from destination zones“ jeweils die Zone „lan“. Wiederholen Sie den Vorgang für die zweite Zone.

Erlauben Sie auch in der Zone „lan“, dass Pakete aus dieser Zone an die beiden neuen weitergeleitet werden dürfen, sofern OpenWrt das nicht schon selbst erledigt hat. Diese Konfiguration lässt beide Netze auf die Zwischenwelt zugreifen und umgekehrt. Kommunikation zwischen den beiden Heimnetzen verhindert der Nachbarschaftsrouter jedoch.

Wollen Sie noch, dass das OpenWrt-Webinterface aus beiden Heimnetzen erreichbar ist, um spätere Konfigurationsänderungen zu erleichtern, müssen Sie auch dafür zwei Regeln anlegen: Wechseln Sie im Firewallmenü in die Registerkarte „Traffic Rules“ und klicken Sie unten auf „Add“. Vergeben Sie einen Namen für die Regel wie etwa „HTTP-Mueller“ und setzen Sie die gleichnamige Zone als „Source Zone“; wählen Sie in „Protocol“ nur TCP an. Als „Destination Zone“ setzen Sie „Device (Input)“, der „Destination Port“ ist der HTTP-Standard-Port 80. Bauen Sie die Regel auch für die zweite Zone.

Ist Ihnen auch innerhalb der Heimnetze verschlüsselter Zugriff lieber, erstellen Sie beide Regeln ein weiteres Mal für den TCP-Port 443, dem HTTPS-Standard-Port.

Statische Routen

Die Konfiguration des OpenWrt-Nachbarschaftsrouters ist mit der Firewall abgeschlossen und Sie können sich dem ersten Heimnetzrouter widmen, wofür Sie sich per LAN oder WLAN direkt mit dem Netz verbinden. Sofern Sie im OpenWrt-Router das jeweils zuständige

Interface als DHCP-Client konfiguriert haben, müssen Sie zunächst die Reservierung anlegen, damit die IP-Adresse gleich bleibt.

In FritzOS erledigen Sie das, indem Sie die Übersicht unter Heimnetz/Netzwerk öffnen und den Nachbarschaftsrouter in der Geräteliste suchen; der Geräte-name sollte der von Ihnen zuvor vergebene Hostname sein. Klicken Sie in der Zeile des Geräts auf den Stift, um das Geräte-menü zu öffnen. Im Ausklappenmenü „Adressen im Heimnetz (IP-Adressen)“ haken Sie die Option „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen.“ an. Notieren Sie sich die zugewiesene IP-Adresse, Sie benötigen Sie gleich für die statische(n) Route(n).

FritzOS

Die Einstellungen für statische Routen finden Sie in FritzOS ebenfalls im Netzwerk-Untermenü: Im Reiter „Netzwerkeinstellungen“ gibt es unter „weitere Einstellungen“ versteckt die Option „IPv4 Routen“; klicken Sie im Menü auf „Neue IPv4-Route“. Das „IPv4-Netzwerk“ ist das

entfernte Subnetz, das Sie im Heimnetz erreichbar machen möchten, in unserem Beispiel also die Zwischenwelt 192.168.21.0. Die Subnetzmaske lautet 255.255.255.0. Das Gateway ist die IP-Adresse des Nachbarschaftsrouters im jeweiligen Heimnetz; diese haben Sie sich vorhin bei der festen Zuweisung im OpenWrt-Interface festgelegt oder gerade eben aus dem Webinterface notiert, als Sie die Reservierung angelegt haben. Wiederholen Sie den Vorgang für das Subnetz des benachbarten Heimnetzes, wenn Sie möchten, dass dieses ebenso erreichbar ist. Gateway und Subnetzmaske bleiben gleich.

Sind die Routen angelegt, versuchen Sie im Browser das OpenWrt-Webinterface zu erreichen. Falls Sie keine Antwort bekommen, stecken Sie sich wieder an den OpenWrt-Router und kontrollieren die Firewallregeln. Klappt alles, begeben Sie sich in das andere Heimnetz und legen die Routen in umgekehrter Richtung an: Reservierung konfigurieren, IP-Adresse des Nachbarschaftsrouters (Gateway) im Heimnetz notieren und

Routen für die entfernten Subnetze einstellen.

Sind die Routen an beiden Heimnetzroutern eingetragen, sollten Sie die Zwischenwelt und die Heimnetze sich untereinander erreichen können, sofern Sie das so konfiguriert haben. Klappt das nicht, kontrollieren Sie die Routen auf Tippfehler und die FirewallEinstellungen auf eventuell fehlende Zonenzuweisungen.

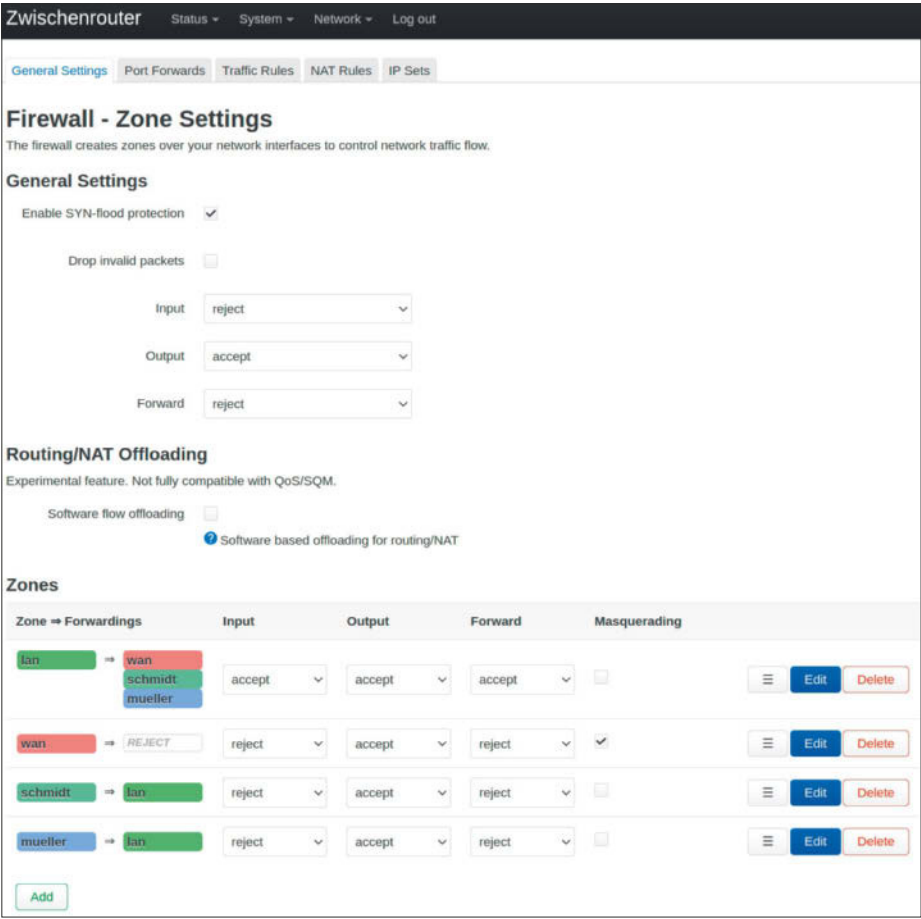
Leben in der Zwischenwelt

Schieben die Router die Pakete erfolgreich von A nach B und C, können Sie an den beiden Ports des Nachbarschaftsrouters Geräte für die Zwischenwelt anschließen und konfigurieren.

Das sollten Sie mit Hardware, deren Funktion eine hohe Priorität für beide Parteien hat, auch dann machen, wenn Sie Routing zwischen beiden Heimnetzen erlauben. Befindet sich beispielsweise die IP-Türklingel in Heimnetz A, ist sie auf den Heimnetzrouter für das Routing in die anderen Netze angewiesen. Nur Geräte in der Zwischenwelt sind wirklich unabhängig erreichbar, selbst wenn einer der Internetzugänge beziehungsweise Router mal ausfällt.

Sollten sich weitere gemeinsam genutzte Geräte ansammeln, spricht nichts dagegen, einen Switch anzustecken. Auch das WLAN können Sie bei Bedarf reaktivieren und Ihr Zwischennetz ausstrahlen. Die Konfiguration finden Sie in OpenWrt unter Network/Wireless.

Zuletzt sollten Sie die Konfiguration unter System/Backup/Flash Firmware herunterladen (Generate archive) und abspeichern. Damit können Sie zur zuletzt funktionierenden Konfiguration zurückkehren. Das klappt auch mit Ersatzgeräten des gleichen Typs, sodass Sie Türklingel & Co. schnell wieder einsatzbereit machen können, sollte der vorherige Nachbarschaftsroutert etwa von einem Blitzschlag dahingerafft worden sein. (amo@ct.de) ct



In OpenWrt ist die Firewall einsteigerfreundlich und schon ein paar einfache Einstellungen verhindern, dass die Heimnetze untereinander kommunizieren.

Literatur

[1] Andrijan Möcker, Alles Kabel!, Grundlagen Heimnetzverkabelung: Von Notlösung bis professionell, c't 26/2020, S. 132
[2] Andrijan Möcker, Sparverdrahtung, Günstige, schnelle Netzwerkverkabelung für Haus und Wohnung, c't 14/2023, S. 136
[3] Andrijan Möcker, Befreite Box, OpenWrt-Spartipp: Fritzbox 7362 SL, c't 21/2020, S. 146

OpenWrt-Dokumentation: ct.de/y1pq



Bild: KI Midjourney | Collage c't

Startfreigabe

Secure Boot und Startverbote unter Linux

Secure Boot soll Bootviren und anderem Schadcode vorbeugen, indem das UEFI-BIOS nur signierte Bootloader und Kernel startet. Das gilt auch für Linux. Falls nachträglich Sicherheitslücken auftauchen, werden Signaturen per Revocation List widerrufen. Der Platz im BIOS-Flashspeicher ist allerdings knapp, weshalb neue Techniken entwickelt wurden.

Von Mirko Dölle

Microsofts Ankündigung lässt allernächst Raum für Spekulationen: Man werde am 9. April oder später „zusätzliche anfällige Start-Manager ... blockieren“, schreibt der Softwarehersteller im Knowledge-Base-Artikel KB5025885. Dieser bezieht sich auf die Secure-Boot-Sicherheitslücke CVE-2023-24932 alias „Black Lotus“, die Microsoft in einem mehrstufigen Update schließen möchte. Was das für Windows-Anwender bedeutet, haben wir [1] bereits ausführlich beschrieben. Linux war von Black Lotus nicht betroffen, sodass in dem zu erwartenden Up-

date der Revocation List (Secure Boot Forbidden Signature Database, DBX) der nicht mehr vertrauenswürdigen Bootloader keine Linux-Bootloader auftauchen sollten. In unseren Tests wurden auf manchen Rechnern trotzdem Einträge für Linux-Bootloader hinzugefügt, als wir das bevorstehende Update manuell durchführten.

Wir raten ausdrücklich davon ab, es selbst zu aktivieren. Erst in Phase 4, die am 8. Oktober 2024 beginnen soll, wird es zwangsweise von Windows eingespielt. Umso kryptischer ist Microsofts Ankündigung, man werde in Phase 3 ab 9. April zusätzliche Bootmanager blockieren. Bis Redaktionsschluss Anfang April bekamen wir keine Antwort, ob Linuxsysteme von

den bevorstehenden zusätzlichen Sperren betroffen sein könnten oder nicht. Um die Linux-Bootloader zu sper-

ren, die von der Anfang Februar 2024 bekannt gewordenen HTTP-Boot-Lücke betroffen sind, soll aus Platzgründen eine neue Technik, Secure Boot Advanced Tar-



geting (SBAT), zum Einsatz kommen. Das dürfte mit den für den 9. April angekündigten Sperrungen also nichts zu tun haben. Da sich vorab nicht sagen lässt, was sich Anfang April ändert und inwiefern Linux davon betroffen sein wird, geben wir Ihnen einen generellen Überblick, was Windows Updates mit Linux-Bootloadern zu tun haben und wie das neue Secure Boot Advanced Targeting verwundbare Bootloader sperrt.

Vertrauensfrage

Das Konzept von Secure Boot sieht vor, dass das UEFI-BIOS des Mainboards nur Bootloader aus einer vertrauenswürdigen Quelle startet. Dazu sind im BIOS verschiedene Zertifikate mit unterschiedlichen Berechtigungen hinterlegt: An oberster Stelle steht der Platform Key (PK) des Mainboard-Herstellers. Darunter ist der Key Exchange Key (KEK) von Microsoft angesiedelt, mit dem Microsoft neue Zertifikate und Prüfsummen einspielen darf, möglicherweise zusätzlich zu denen des Hardwareherstellers. Beide Listen können Sie unter Linux mit dem Befehl

```
sudo fwts uefidump - | less
```

aus dem gleichnamigen Softwarepaket abrufen. Die Liste ist in verschiedene Blöcke aufgeteilt, zusammengehörende Teile sind stets gleich weit eingerückt. Am Anfang steht jeweils der Name des Blocks, die Platform Keys etwa finden Sie unter PK in der alphabetisch sortierten Liste, die Key Exchange Keys unterhalb von KEK.

Damit der Rechner für Windows zertifiziert werden kann, muss der Hersteller außerdem zwei Zertifikate als „Authorized Signatures“ (DB) einspeisen: Microsoft Windows Production PCA 2011 und Microsoft Corporation UEFI CA 2011. Ist Secure Boot aktiv, darf das BIOS nur noch Bootloader ausführen, die mit einem der Zertifikate aus der DB signiert wurden. Manchmal findet sich hier auch ein Zertifikat des Hardwareherstellers, und dieser dürfte noch weitere Zertifikate speichern, etwa von Linux-Distributoren. Da in der Praxis nun mal ein Großteil der Rechner mit Windows ausgeliefert oder betrieben wird, spart man sich die Mühe. Die auf Ihrem Rechner gespeicherten Zertifikate finden Sie in der Ausgabe von fwts im Abschnitt db.

Unter Boot0000 können Sie sehen, welchen Bootloader Ihr UEFI-BIOS als ersten gespeichert hat, bei Boot0001 steht eventu-

ell ein zweiter und so weiter. Dort finden Sie unter Info: dessen Klarnamen, etwa „Windows Boot Manager“, und unter Path: den Pfad auf der EFI-Partition (EFI System Partition, ESP) nebst Dateinamen. Die EFI-Partition bindet Linux standardmäßig unter /boot/efi ein, sodass Sie die Signatur und Unversehrtheit des Windows-Bootloaders mit dem Befehl

```
sudo sbverify /boot/efi/EFI/Microsoft\Boot\bootmgr.efi
```

prüfen können. Mit welchem Zertifikat der Bootloader signiert ist, erfahren Sie mit dem zusätzlichen Parameter --list vor dem Dateinamen.

Vorgeschaltet

Um nicht bei jeder Änderung an Grub eine neue Überprüfung und Zertifizierung durch Microsoft beantragen zu müssen, wurde der minimalistische EFI-Loader Shim entwickelt: Linux-Distributoren ergänzen ihn um ihr eigenes Zertifikat und reichen Shim dann zur Zertifizierung bei Microsoft ein. Statt mit seinem Windows-Production-Zertifikat signiert Microsoft solche fremden Bootloader stets mit dem UEFI-CA-Zertifikat. Durch das Distributor-Zertifikat in Shim kann zum Beispiel Canonical Grub, Kernel und Kernel-Module von Ubuntu jederzeit selbst signieren. Ein einmal signierter Shim lässt sich mitunter über Jahre nutzen, so enthielten frühe Installationsmedien von Ubuntu 20.04 LTS noch den Shim von Ubuntu 18.04.

Doch auch Microsofts Windows-Bootloader, Shim und Grub enthalten manchmal Fehler, die es erlauben, nicht signierte Bootloader oder Kernel zu laden. Um solche unsicheren Bootloader nachträglich sperren zu können, gibt es im UEFI-BIOS die Revocation List DBX. In ihr sollen die Prüfsummen der als unsicher erkannten Bootloader gespeichert werden. Die aktuelle Revocation List wird vom UEFI-Forum zum Download bereitgestellt und mitunter von Hardware-Herstellern bei BIOS-Updates ebenfalls aktualisiert, sodass auch in einem frisch ausgepackten PC bereits über hundert Einträge gespeichert sind.

Weitere Prüfsummen werden über Betriebssystem-Updates hinzugefügt, etwa mit dem Windows-Update vom 9. August 2022, woraufhin die Linux-Installationsmedien diverser Distributionen nicht mehr booteten. Dabei betrafen längst nicht alle Fehler Shim: Microsoft

c't kompakt

- Mangels Vorgabe durch die Secure-Boot-Spezifikation gibt es auf vielen Mainboards nur 32 KByte Platz für den Widerruf von Bootloader-Zertifikaten.
- Die bislang veröffentlichten Revocation Lists belegen schon mehr als 75 Prozent des verfügbaren BIOS-Flash-Speichers.
- Mit Secure Boot Advanced Targeting (SBAT) gibt es eine neue Technik, die dauerhaft kurze Sperrlisten mit wenigen Einträgen verspricht.

sperrte auch Shims, die fehlerbehaftete, vom jeweiligen Distributor signierte Grub-Bootloader starteten. Auch unter Linux gibt es Updates der Sperrliste, diese werden über fwupd im Rahmen der regelmäßigen Paket-Updates eingespielt. Allerdings akzeptiert das UEFI-BIOS nur Sperrlisten aus vertrauenswürdigen Quellen, deren Zertifikat in der Liste der Key Exchange Keys hinterlegt ist. Deshalb trägt zum Beispiel Ubuntu bei der Installation auf Systemen mit aktiviertem Secure Boot Canonicals Master-CA-Zertifikat auch dort ein und nicht nur in der DB-Liste, die Bootloader autorisiert.

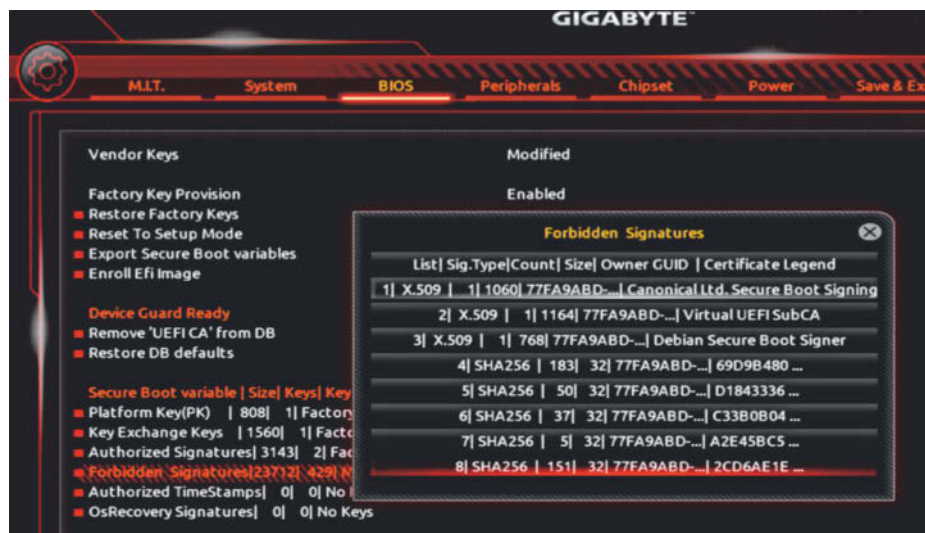
Das in KB5025885 beschriebene DBX-Update, das von Windows spätestens im Oktober 2024 zwangsweise eingespielt werden soll, enthält wiederum Hunderte Prüfsummen – diesmal vor allem von Windows-Bootloadern, die fehlerhaft sind. Und durch die im Februar bekannt gewordene HTTP-Lücke müssten wiederum zahlreiche Shims auf die Abschlusliste gesetzt werden, womit es eng wird in der DBX-Datenbank. Denn für die gibt es nach Angaben der Shim-Entwickler auf vielen Mainboards nur 32 KByte BIOS-Flash-Speicher.

Grenzüberschreitung

Wie groß die Revocation List auf Ihrem Rechner bereits geworden ist, können Sie unter Linux mit dem Befehl

```
sudo ls -l /sys/firmware/efi\EFI\vars/dbx-*
```

herausfinden. Auf einem unserer Laptops, auf dem neben Ubuntu 22.04 LTS ein Win-



Auf 429 Einträge ist die Sperrliste dieses Rechners bereits angewachsen. Bei unseren Recherchen fanden wir insgesamt mehr als 600 verschiedene Einträge.

dows 10 ohne das optionale Update aus KB5025885 installiert war, hatte die DBX-Liste bereits eine Größe von über 13 KByte. Wie viele Sperreinträge enthalten sind, lässt sich mit `dbxtool` herausfinden:

```
dbxtool -l | wc -l
```

Das Ergebnis waren 272 Einträge auf dem Laptop. Auf einem anderen Rechner mit Ubuntu 22.04 LTS, auf dem noch nie etwas anderes als Ubuntu installiert war, fanden wir nur 186 Sperreinträge. Das änderte sich drastisch, nachdem wir dort Windows 10 installierten und das in KB5025885 beschriebene Update aktivierten: Daraufhin schwoll die DBX-Datei auf über 24 KByte und 429 Einträge.

Schrumpfkur

Um nicht noch mehr Platz zu verbrauchen, planen die Shim-Entwickler die von der HTTP-Lücke betroffenen Shims nicht über weitere Einträge in der Revocation List zu deaktivieren, sondern dafür Secure Boot Advanced Targeting (SBAT) zu verwenden, das Shim seit einiger Zeit unterstützt. Der wesentliche Unterschied ist, dass SBAT keine stetig wachsende Liste wie die DBX-Datenbank ist, sondern Werte immer wieder ersetzt werden, um Platz zu sparen.

Der Ansatz der DBX-Datenbank, lediglich neue Einträge an die bestehenden anzuhängen, verhindert wirkungsvoll, dass jemand eine veraltete Revocation List einspielt und so längst blockierte Bootloader wieder freischaltet. Die SBAT-Ent-

wickler hingegen wollen die Einträge in der SBAT-Liste immer wieder anpassen und falls möglich auch verkürzen können. Damit niemand eine alte SBAT-Liste einspielen kann, nutzen sie den „EFI Variable Time Based Authenticated Write Access“: Dabei wird der Zeitstempel der Signatur der neu einzuspielenden Liste überprüft – nur wenn er neuer ist als der der vorhandenen Liste, erfolgt der Austausch.

Die SBAT-CSV-Liste (Comma-Separated Values) enthält Informationen zu SBAT selbst und zu den Komponenten, die an Secure Boot beteiligt sind. Dazu zählen der Stage-1-Bootloader Shim, Grub als Stage-2-Bootloader und der Kernel, aber auch der Firmware-Update-Daemon `fwupd` oder ein Hypervisor bei Systemen mit Virtualisierung. Jede Komponente, Produkt genannt, hat einen von den Entwicklern festgelegten Namen, etwa `sbat`, `shim` oder auch `grub`. Dieser wird um den Namen des Herstellers ergänzt, der Grub-Bootloader aus Debian Linux zum Beispiel trägt den Produktnamen `grub.debian`.

Hinter dem Produktnamen folgt als zweiter vorgeschriebener Wert jeder Zeile die sogenannte Generationsnummer. Dies darf nicht mit der Versionsnummer verwechselt werden, die Generationsnummer ist einen fortlaufender ganzzahliger Wert, der lediglich angibt, wie viele Sicherheitsaktualisierungen es für dieses Produkts bereits gab, seit es SBAT unterstützt. Das klingt erst mal kompliziert, ist es aber nicht, wie die nachfolgenden Beispiele noch zeigen werden.

Der Vollständigkeit halber: Die einzelnen Zeilen der SBAT-CSV-Liste dürfen noch drei weitere Werte enthalten, nämlich den Projektnamen, etwa `grub` oder `grub2` bei Grub (aber nicht `grub.debian`), die exakte Versionsnummer inklusive Patchlevel wie zum Beispiel `2.02-0.34.e17_2` und eine URL oder Mailadresse, die zum Projekt führt. Hier der komplette SBAT-Eintrag für Grub aus Debian:

```
grub.debian,2,Debian,grub2,2.04-13,
https://packages.debian.org/source/
sid/grub2
```

Generationenwechsel

Der Grub-Bootloader Version 2.04-13 des Debian-Projekts trägt die Generationsnummer 2, weil diese Veröffentlichung von Grub eine Secure-Boot-relevante Sicherheitslücke früherer Veröffentlichungen geschlossen hat. Angenommen, das Debian-Projekt wechselt für neue Features auf die Grub-Version 2.05, dann sähe der SBAT-Eintrag folgendermaßen aus:

```
grub.debian,2,Debian,grub2,2.05-1,
https://packages.debian.org/source/
sid/grub2
```

Es handelt sich weiterhin um die Komponente `grub.debian` der zweiten Generation, denn es wurden keine Secure-Boot-relevanten Sicherheitsaktualisierungen vorgenommen. Ob jemand den neuen Grub in Version 2.05-1 einsetzt oder noch die Version 2.04-13, spielt sicherheitstechnisch keine Rolle. Die Generationsnummer ist also unabhängig von der Versionsnummer.

Die Sicherheitslücke, die bei Grub zum Generationswechsel von 1 auf 2 führte, gab es nicht nur beim Debian-Projekt. Vielmehr betraf sie praktisch alle Linux-Distributoren. Um zu verhindern, dass weiterhin anfällige Versionen von Grub eingesetzt werden, veröffentlichte man im Oktober 2022 mit den neuen Grub-Builds folgende SBAT Revocation List:

```
sbat,1,2022052400
grub,2
```

Die erste Zeile enthält die Timestamp des SBAT-Updates und verhindert, dass später eine ältere Version der Revocation List eingespielt werden kann. Die zweite Zeile verbietet den Start aller `grub`, unabhängig vom Distributor, die nicht mindestens aus Generation 2 sind. Wie Ihre aktuelle SBAT

Revocation List aussieht, können Sie übrigens jederzeit mit dem Befehl

```
mokutil --list-sbat-revocations
```

herausfinden.

Im November 2022 wurden zwei weitere, distributionsübergreifende Sicherheitslücken geschlossen, weshalb alle Distributoren auf die Generation 3 wechselten. Das tat auch das Debian-Projekt und veröffentlichte den Build 2.06-3-deb10u2 von Grub:

```
grub.debian,3,Debian,grub2,2
2.06-3-deb10u2,https://packages.
debian.org/source/sid/grub2
```

Dazu wurde auch der Eintrag in der Revocation List aktualisiert, damit Grub aus der zweiten Generation generell nicht mehr startet:

```
grub,3
```

Beim Übersetzen der neuen Grub-Pakete machte der Maintainer jedoch einen Fehler: In Binärpaketen für Debian 10 Buster wurde der Fix für die Sicherheitslücke CVE-2022-2601 nicht berücksichtigt, in denen für Debian 11 Bullseye hingegen schon. Es wurden somit Grub der Generation 3 veröffentlicht, die noch anfällig waren. Deshalb musste der Paket-Maintainer den Fehler beheben und zusätzlich die Generation auf 4 anheben. Der SBAT-Eintrag lautete also nunmehr:

```
grub.debian,4,Debian,grub2,2
2.06-3-deb10u3,https://packages.
debian.org/source/sid/grub2
```

Die offizielle Revocation List erlaubte jedoch weiterhin Bootloader der Generation 3 und damit auch die anfälligen Builds für Debian Buster. Eine mögliche Lösung wäre gewesen, die Generation für alle Grub auf 4 zu erhöhen:

```
grub,4
```

Doch dann hätten sämtliche Distributionen neue Builds von Grub veröffentlichen müssen, in denen sich lediglich die Generationsnummer geändert hat. Deshalb behelfen sich die Entwickler mit einer distributionsspezifischen Festlegung der Generationsnummer und veröffentlichten mit Shim Version 15.8 folgende SBAT Revocation List:

```
grub,3
grub.debian,4
```

Eine solche Ausnahme wäre übrigens auch umgekehrt möglich, wenn eine bestimmte Distribution von einem ansonsten verbreiteten Fehler nicht betroffen ist. Dann könnte in einem distributions-spezifischen Eintrag auch eine niedrigere Generationsnummer stehen als sie für das allgemeine Produkt gilt. Die Shim-Entwickler wollen hier zukünftig platzsparend arbeiten und möglichst wenige Ausnahmen auflisten.

Fazit

Die Designfehler in Secure Boot haben den Bootvorgang stark verkompliziert, es ist absehbar, dass bald keine weiteren Bootloader mehr per Revocation List ge-

sperrt werden können. Mit SBAT hat die Open-Source-Gemeinde eine eigene Technik entwickelt, die von Anfang an platzsparend ausgelegt ist und das Potenzial hat, nicht stetig anzuwachsen. Die Abhängigkeit von Microsoft, Shim immer wieder zertifizieren und signieren lassen zu müssen, werden die Distributoren durch SBAT aber nicht los. Denn per Secure Boot starten auch weiterhin nur Bootloader aus vertrauenswürdiger Quelle – und das ist bei so gut wie allen Hardwareherstellern immer noch nur Microsoft.

(mid@ct.de) 

Literatur

- [1] Axel Vahldiek, Schiffbruch mit Ansgar, Massenhaft Startverbote für Linux- und Windows-Bootloader spätestens ab Oktober, c't 7/2024, S. 58

Der Secure-Boot-Schlamassel

Bei der Entwicklung von Secure Boot wurde bereits vorausgesehen, dass es einmal Bootloader geben würde, deren Sicherheitslücken erst bekannt werden, nachdem man sie als vertrauenswürdigt signiert hat. Deshalb enthielt die Spezifikation von Anfang an, dass es im UEFI-BIOS eine Revocation List (Forbidden Signature Database, DBX) geben muss, in der die Prüfsummen von als unsicher erkannten Bootloadern nachträglich eingetragen werden können. Doch bei der Spezifikation wurde geschlampt, es fehlt eine verbindliche Größenangabe, wie viel Flash-Speicher die Mainboard-Hersteller im UEFI-BIOS dafür mindestens bereitstellen müssen. Nach Angaben der Shim-Entwickler stehen dafür je nach Mainboard gerade mal 32 KByte zur Verfügung.

Wie viel Platz die DBX-Liste auf einem bestimmten Rechner belegt, muss man im Einzelfall prüfen. Die Spannbreite reichte bei unseren Recherchen von unter 1 KByte bei nur 10 Einträgen bis über 24 KByte mit mehr als 420 Einträgen.

Ständig unvollständig

Für die gravierenden Unterschiede bei den Sperrlisten auf den von uns für [1] untersuchten Rechnern gibt es keine plausible Erklärung. Eigentlich sollten unabhängig vom Betriebssystem alle Sperrlisten gleich sein, sofern man alle verfü-

baren Updates eingespielt hat. Auch das UEFI-Forum veröffentlicht die von Microsoft erstellte DBX-Datei auf seiner Homepage. Dennoch fanden wir mittlerweile Rechner mit bis zu 50 Einträgen, die in der DBX-Datei der UEFI nicht enthalten waren. Wir baten auch Microsoft als Eigentümer der Signaturzertifikate um eine vollständige Liste aller zurückgezogenen Bootloader, bekamen aber bis zum Redaktionsschluss keine Antwort. Unterschiede bei der Anzahl der DBX-Einträge und der enthaltenen Prüfsummen zwischen verschiedenen Rechnern waren bei unseren Recherchen die Regel, nicht die Ausnahme.

Es ist also bereits jetzt, wo die Sperrlisten noch in den Flash-Speicher der Mainboards passen, nicht sichergestellt, dass ein Rechner alle kompromittierten Bootloader auch ablehnt. Das Konzept ist gescheitert und das Ende der Fahnenstange in Sicht. Microsoft und auch die Shim-Entwickler arbeiten deshalb an Alternativen: Microsoft hat die mutmaßlich „Code Integrity Boot Policy“ genannte Technik entwickelt [1]; auf Linux-Seite entstand Secure Boot Advanced Targeting, kurz SBAT. Während bei den DBX-Einträgen das UEFI-BIOS den Systemstart verweigert, sind es bei Code Integrity und SBAT der Windows-Kernel respektive die Linux-Bootloader Shim und Grub, die erkennen, dass Secure Boot nicht mehr gewährleistet ist und deshalb den Dienst verweigern.



Dokumentenschlucker

Papierloses Büro mit paperless-ngx

Mit der Open-Source-Anwendung paperless-ngx auf einem Server, Raspi oder NAS sowie einem Einzugsscanner gehört Dokumentenchaos der Vergangenheit an. Lesen Sie unseren Mehrstufenplan zum papierarmen Büro – selbstlernende Systeme und Langzeitarchiv inklusive.

Von Jan Mahn

Per Brief, per E-Mail oder über Apps und Online-Kundencenter: Dokumente finden auf vielen Kanälen den Weg nach Hause. Und wenn man sich nicht um sie kümmert, stapeln sie sich analog in Ablagen, auf Loseblattstapeln sowie digital in Mailpostfächern und auf dem Desktop. Spätestens wenn die Frist für die Steuererklärung naht oder man nach knapp zwei Jahren wissen möchte, ob die defekte Waschmaschine noch in der Gewährleistung ist, rächt sich diese Nicht-Strategie. Wohl dem, der seine Dokumente an einer zentralen Stelle verwahrt, bestenfalls digital und gut durchsuchbar.

Die hierarchische Ordnerstruktur eines Dateisystems ist dafür weniger ge-

eignet, als man zunächst annehmen mag: Gehört die Waschmaschinenrechnung in den Ordner Dokumente/Steuer/2024 oder in Dokumente/Rechnungen/Haus/2024? Besser geeignet, um Dokumente nicht nur abzulegen, sondern auch wiederzufinden, sind Dokumentenmanagementsysteme (DMS). In solchen kann man unter anderem virtuelle Etiketten (Tags) an Dokumente anheften, außerdem gibt es eine Volltextsuche und diverse Suchfilter. In c't 29/2023 haben wir kommerzielle Dokumentenmanagementsysteme vorgestellt, die genau das leisten sollen [1]. Der große Haken: Viele DMS verstecken alle Dokumente, die man in sie hineinwirft, in ihren Datenbanken, aus

denen man sie nicht so leicht wieder herausbekommt. Wenn der Anbieter das Produkt einstellt oder die Preise ändert, ist Umzugsstress garantiert.

Das geht auch anders: Wer sich etwas Heimserververwaltung zutraut, bekommt auch ganz allein mit kostenloser Open-Source-Software eine Dokumentenverwaltung, die für Privatanutzer und kleine Firmen kaum Wünsche offen lässt. Keine Abo-Modelle und volle Kontrolle über die Daten, die auf einem Mini-Server, auf einem Raspberry Pi oder einem NAS ihr Zuhause finden. Großer Beliebtheit unter Dokumentenarchivaren erfreut sich das Projekt paperless-ngx, die Weiterentwicklung von paperless-ng, das wiederum die Arbeit von paperless fortsetzt.

Alle Dokumente speichert paperless-ngx in gewöhnlichen Ordnern im Dateisystem und nicht in der Datenbank, sodass man ganz problemlos umziehen kann, wenn das mal nötig sein sollte. Im Dateisystem selbst stößt man als Nutzer aber nie. Der zugehörige Webdienst und eine Datenbank, in der nur Metadaten gespeichert werden, sind schnell auf eigener Hardware installiert und die Oberfläche ist dann im Browser im Heimnetz erreichbar. Doch mit der Software allein hat man noch keinen alltagstauglichen Dokumentenworkflow. Dieser Artikel stellt daher nicht nur die Einrichtung, sondern einen praxiserprobten Ansatz vor, der am analogen Briefkasten beginnt und optional am Aktenvernichter oder im analogen Langzeitarchiv endet. Papierdokumente sollen gescannt, mit Texterkennung verarbeitet, durchsuchbar archiviert und dann abgelegt werden. Digitale Dokumente sollen mit möglichst wenig Arbeit ebenfalls in der Dokumentenverwaltung landen. Los geht es mit der Installation von paperless-ngx.

Installieren

Bevor Sie Dokumente verwalten können, müssen Sie einen Server auserwählen. Grundsätzlich kommt alles infrage, was (Docker-)Container mit Linux-Grundlage ausführen kann. Theoretisch könnten Sie paperless-ngx auch auf Ihrem Desktop oder Laptop im Container laufen lassen. Dann wäre die Dokumentenverwaltung aber nur erreichbar, wenn dieser Rechner auch eingeschaltet ist. Wer ohnehin schon einen Raspberry Pi im 24-Stunden-Betrieb im Haushalt hat und nicht plant, Hunderte Dokumente am Tag zu verarbeiten, kann paperless-ngx auf einem Raspi ab Modellreihe 3B betreiben. Voraussetzung

ist ein Raspi-Betriebssystem in der 64-Bit-Variante. Raspberry Pi OS finden Sie über ct.de/ytg4.

Auch ein Linux-Mietserver bei einem Hoster Ihres Vertrauens kann zur Heimat für Ihre Dokumente werden – wenn Ihr Vertrauen denn ausreicht, dass Sie dem Anbieter Ihre persönlichsten Daten anvertrauen mögen. Für diesen Artikel haben wir uns für ein NAS von Synology mit x86-Prozessor als lokale Dokumentenhalde entschieden, damit die Daten die eigenen vier Wände nicht verlassen. Ein solches hat gegenüber dem Raspberry Pi den entscheidenden Vorteil, dass die Daten schon von Haus aus auf einem Festplattenverbund wie einem RAID 1 liegen, also in der Regel redundant auf mehreren Festplatten. Ein regelmäßiges Backup des gesamten Dokumentenordners und der Datenbank, das bestenfalls auch an einem anderen Ort gelagert wird, ersetzt das allerdings nicht.

Bevor Sie paperless-ngx starten, brauchen Sie den Docker-Daemon auf Ihrem System, Fans von Podman können alternativ auch zu dieser Containerumgebung greifen [2]. Wie Sie Docker unter Windows, Linux und macOS installieren, haben wir in einem kostenlosen Artikel zusammengefasst (siehe ct.de/ytg4). Grundlegendes Docker-Wissen und Verständnis von Linux-Rechteverwaltung ist nötig, um paperless-ngx zu installieren.

Auf einem Synology-NAS installieren Sie Docker über das „Paket-Zentrum“ in der Weboberfläche. Das Paket heißt dort nicht etwa Docker, sondern „Container Manager“. Auf diesem Weg erhalten Sie die Docker-Engine und eine grafische Oberfläche, um Container im Browser zu verwalten. Die ist aber nicht überragend praktisch: Sie liest Docker-Compose-Dateien nur beim Anlegen eines Container-Projekts ein, reagiert danach aber nicht auf Änderungen an der Datei. Änderungen an Containern funktionieren dann nur noch über die grafische Oberfläche. Den vollen Komfort erhalten Sie, wenn Sie per SSH auf das NAS zugreifen und Docker wie auf jedem anderen Linux-Server auf

ct kompakt

- Paperless-ngx verwaltet Dokumente, lernt sie selbstständig zu kategorisieren und beherrscht Volltextsuche.
- Der Serverdienst ist anspruchslos und läuft auf fast jeder Hardware.
- Die Dokumente gelangen per Scanner oder über ein Netzlaufwerk in die Dokumentenverwaltung.

der Kommandozeile bedienen. Um SSH zu aktivieren, öffnen Sie die Systemsteuerung, dort den Menüpunkt „Terminal und SSH“ und aktivieren dort den SSH-Dienst auf Port 22.

Wenn Sie die Vorbereitungsarbeiten erledigt haben, legen Sie auf Ihrem NAS, Server oder zum Test auf Ihrem Desktop-Rechner mit installiertem Docker einen leeren Ordner namens paperless an. Auf dem NAS können Sie das über die Web-Oberfläche erledigen, dann liegt der Ordner auch direkt auf den großen Festplatten. In diesem Ordner sollen nicht nur die Konfigurationsdateien wie die Docker-Compose-Datei liegen, sondern später auch die gesammelten Daten selbst. Damit weichen wir in dieser Anleitung vom offiziellen Rezept ab, das die paperless-ngx-Entwickler bereitstellen. In deren Compose-Dateien landen die Daten in sogenannten „named volumes“, also Volumes, um die sich Docker selbst kümmert und die Inhalte in seiner eigenen Struktur verpackt. Auf einem NAS erwies sich das nicht als praktikabel.

Wir empfehlen stattdessen folgende Datenstruktur in Ihrem Ordner paperless: Legen Sie einen Unterordner namens volumes an und platzieren darin die Ordner data, database, export, media und redis. Im Ordner media liegen später die verarbeiteten Dokumente. Bei den Ordnern müssen Sie anschließend noch Änderungen an den Berechtigungen vornehmen,



Praktisch: Über die Suchfilterschaltflächen oben kann man Dokumente nicht nur schnell auffinden, sondern auch genauso schnell mit Etiketten versehen.

Dateiaufgaben Alle verwerfen Automatisch aktualisieren

Fehlgeschlagen Abgeschlossen **10/7** Gestartet In Warteschlange

Name	Ausgestellt am	Ergebnisse	Aktionen
jm_03092024_120645_000384.pdf	09.03.24, 12:06	Success. New document id 348 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>
jm_03092024_120554_000381.pdf	09.03.24, 12:06	Success. New document id 339 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>
Rechnung_2024_02.pdf	08.03.24, 20:20	Success. New document id 337 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>
2024_02_Verdienstabrechnung_103.pdf	25.02.24, 14:07	Success. New document id 336 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>
Unknown.pdf	15.02.24, 21:05	Success. New document id 334 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>
RE 202401763256.pdf	15.02.24, 21:05	Success. New document id 333 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>
jm_02152024_134437_000376.pdf	15.02.24, 13:44	Success. New document id 332 created	<input checked="" type="checkbox"/> Verwerfen <input type="button" value="Dokument öffnen"/>

Die Software führt Protokoll, welche Dokumente verarbeitet wurden. Die Anlaufstelle mit weiteren Informationen, wenn mal eine Verarbeitung scheitern sollte.

damit paperless-ngx dort lesen und schreiben kann. Dafür müssen Sie auf dem System zunächst einen neuen Nutzer namens paperless anlegen und dessen User-ID herausfinden. Auf einem Linux-System erzeugen Sie den Account mit:

```
sudo useradd paperless
```

Auf einem Synology-NAS lautet der Kommandozeilenbefehl `sudo synouser --add` und erwartet insgesamt sechs Parameter. Schneller erzeugen Sie den Nutzer über die grafische Oberfläche. Sowohl unter Linux als auf der Synology bekommen Sie anschließend mittels `id paperless` die User-ID Ihres neuen Nutzers, die brauchen Sie später. Vorher müssen Sie Lese- und Schreibrechte für den Nutzer paperless für die vorher erzeugten Ordner vergeben: Machen Sie paperless zuerst zum Inhaber eines Ordners, zum Beispiel:

```
sudo chown paperless data
```

Geben Sie dem Ordner dann Lese- und Schreibrechte mit

```
sudo chmod -R u+rw data
```

Zusätzlich brauchen Sie einen Ordner namens `consume`, der auch außerhalb des Projektordners liegen darf – ihm kommt eine Sonderrolle zu: Was auch immer Sie später in diesen Ordner werfen, wird paperless-ngx sich einverleiben und versuchen, als Dokument zu verarbeiten. Wichtig ist, dass der Nutzer paperless auch hier Lese- und Schreibrechte hat. Wenn Sie sich für ein NAS entschieden haben, be-

kommen Sie ein paar Schnittstellen, um Daten an paperless-ngx zu schicken, direkt ohne Aufwand geschenkt: Über zum Beispiel FTP, SMB, WebDAV oder NFS können Sie diesen Ordner (und nur diesen) mit jedem teilen, der Dokumente abwerfen soll. Den `consume`-Ordner können Sie so auf allen gängigen Desktop- und Mobilbetriebssystemen erreichbar machen. Darüber können Sie zum Beispiel von einer Scan-App auf dem Mobiltelefon direkt in paperless-ngx schreiben oder auf dem Desktoprechner fleißig alle gefundenen Dateien ins DMS verräumen. Sollten Sie kein NAS nutzen: Unter `ct.de/ytg4` lesen Sie, wie Sie unter Linux einen Ordner per SMB veröffentlichen.

Dann brauchen Sie die Dateien `docker-compose.yml` und `docker-compose.env`, die wir auf Basis der offiziellen Dokumentation angepasst haben (Download über `ct.de/ytg4`). Drei Container gehören zur Zusammenstellung: der Webserver (aus dem Abbild `ghcr.io/paperless-ngx/paperless-ngx:latest`), eine MariaDB-Datenbank (aus dem Abbild `docker.io/library/mariadb:10`) und die Schlüssel-Werte-Datenbank Redis (`docker.io/library/redis:7`) für die Verwaltung von Arbeitsaufträgen.

Die Datei `docker-compose.env` müssen Sie konfigurieren und zusammen mit der Datei `docker-compose.yml` in den Ordner `paperless` legen. Folgende Anpassungen sollten Sie als deutschsprachiger Dokumentenverwalter in Deutschland an der `env`-Datei vornehmen:

```
PAPERLESS_OCR_LANGUAGE=deu
PAPERLESS_TIME_ZONE=Europe/Berlin
```

Außerdem müssen Sie die User-ID des vorher erstellten Users in der Konfigurationsdatei hinterlegen, in unserem Fall war es die 1028:

```
USERMAP_UID=1028
```

Sind diese Vorbereitungen erledigt, können Sie die Containerzusammenstellung hochfahren. In einer neuen Docker-Installation unter Linux mit:

```
docker compose up -d
```

Unter Synology mit der älteren Syntax (der zusätzliche Bindestrich gilt für alle folgenden Befehle):

```
docker-compose up -d
```

Das Hochfahren dauert ein paar Minuten, in den Ordnern `data` und `database` sollten Sie rege Aktivität beobachten können. Mit `docker compose logs` können Sie die Logs der Container mitlesen. Haben sich die Logs beruhigt, ist es Zeit, einen Admin-Nutzer für paperless-ngx in der Datenbank anzulegen und ein Startkennwort zu vergeben:

```
docker compose run webserver \
  createsuperuser
```

Einrichten

Fertig ist die Ersteinrichtung. Sie erreichen die Weboberfläche von paperless-ngx auf Port 8000 unter der IP-Adresse Ihres Servers, geben Sie also zum Beispiel `http://192.168.0.25:8000` in die Adresszeile des Browsers ein. Dort melden Sie sich mit dem soeben vergebenen Administratorkennwort an und landen auf der Oberfläche. Das Administratorkonto muss nicht der einzige Benutzer im System bleiben, links im Menü finden Sie den Punkt „Benutzer und Gruppen“, in dem Sie neue Benutzer hinzufügen und Rechte vergeben können. paperless-ngx taugt damit auch für kleinere Unternehmen als gemeinsame Dokumentenverwaltung.

Beim ersten Besuch ist die Seite hinter dem Menüpunkt `Dokumente` ziemlich leer, es fehlen schlicht die Inhalte. Rechts auf der Startseite haben die Entwickler eine Schaltfläche zum Hochladen solcher eingebaut. Zum Ausprobieren können Sie zum Beispiel ein PDF vom Rechner hochladen. Paperless wird nach kurzer Bearbeitungszeit vermelden, dass das Dokument

erfolgreich verarbeitet wurde. Ohne weiteres Zutun hat die Software bereits ein Vorschaubild generiert, bei gescannten Dokumenten den Text mittels OCR (Optical Character Recognition) lesbar gemacht und in den Suchindex für die Volltextsuche aufgenommen.

Bevor Sie damit beginnen, massenhaft gesammelte Dokumente einzulesen, sollten Sie den Menüpunkt Dateiaufgaben kennen, den sie ganz unten links finden. Hier bekommen Sie einen Eindruck, wie paperless-ngx arbeitet: Neue Dokumente landen zunächst in einer Warteschlange und werden dann nacheinander von Worker-Prozessen abgearbeitet. Damit das auch bei langen Warteschlangen funktioniert, haben Sie einen Container mit der Key-Value-Datenbank Redis hochgefahren, die für solche Aufgaben optimiert ist.

Erfolgreich verarbeitete Dokumente finden Sie im Reiter namens Abgeschlossen, links daneben landen problematische Verarbeitungen mit einer kurzen Fehlermeldung. Noch mehr technische Details,

die auch verraten, was im Hintergrund so mit einem Dokument passiert, finden Sie links im Menü unter Protokolle.

Wiederfinden

Sobald ein paar Dokumente in der Sammlung liegen, können Sie sich mit der zentralen Ansicht von paperless-ngx vertraut machen: Hinter dem Punkt Dokumente links im Menü finden Sie Ihre Dokumente und die Suchmaske. Ganz oben gibt es ein Suchfeld, das Zeichenketten in Metadaten und im Inhalt aufspürt. Die Volltextsuche ist aber nur eine Möglichkeit, um Elemente wiederzufinden.

Dazu gibt es unter anderem Tags. Die können Sie sich wie virtuelle Klebeetiketten vorstellen, nach denen Sie filtern können. Wie Sie die Tags nutzen, müssen Sie selbst entscheiden, für eine private Dokumentensammlung kommen zum Beispiel Tags wie „Lohn und Gehalt“ oder „Steuer“ infrage. Links im Menü unter Tags finden Sie die Seite, um diese Etiketten zu verwalten. Artverwandt sind die Dokument-

typen, die Sie über den gleichnamigen Menüpunkt verwalten. „Rechnung“ oder „Lieferschein“ sind zum Beispiel typische Dokumententypen. Zusätzlich kennt paperless-ngx noch Korrespondenten. Für jeden Onlineshop, von dem Sie mal eine Rechnung erhalten haben, einen Korrespondenten anzulegen, wäre unnötig viel Aufwand. Für den Vermieter oder den Arbeitgeber, der häufiger schreibt, kann sich das zum Beispiel lohnen.

Tags, Korrespondenten und Dokumententypen können Sie auf mehreren Wegen vergeben. Einmal können Sie jedes Dokument in der Übersicht einzeln bearbeiten (mit dem Stiftsymbol) und dort die Metadaten ergänzen. In der Liste können Sie auch mehrere Dokumente markieren und dann oben zum Beispiel über die Schaltfläche Tags einen Tag auswählen und diesen zuweisen. Über dieselbe Schaltfläche können Sie Ihre Suche auch filtern.

Aber es geht noch besser: paperless-ngx ist lernfähig, arbeitet also mit Algo-

Mastering Observability

Softwaresysteme verstehen, steuern und verbessern

Online-Konferenz am 11. Juni 2024

Mehr als Logs, Metriken und Traces

Sie wollen Ihre Softwaresysteme besser verstehen und steuern? Sie möchten Probleme **proaktiv identifizieren und lösen**, die **Leistung optimieren** sowie **hohe Verfügbarkeit und Sicherheit der Anwendungen gewährleisten**?

Dann liefert Ihnen die **Mastering Observability** konkrete Hilfestellung mit diesen Themen:

- Observability mit dem Grafana Open Source Stack
- High Performance Observability Data Pipelines mit Vector
- Standardisierung: OpenTelemetry in Depth
- Continuous Application Profiling mit Parca
- Erfahrungsbericht: KI als Assistent bei der Incident Resolution

Ein Online-Event für Entwickler:innen, Ops-Fachleute und DevOps-Teams.



Jetzt
Frühbucher-
tickets
sichern!

mastering-obs.de

rithmen maschinellen Lernens. Nachdem Sie die erste Handvoll Rechnungen mit dem passenden Dokumenttyp versehen haben, wird die Software ein Muster erlernt haben und die weiteren Rechnungen selbstständig als solche einstufen. Zum Test haben wir 250 echte Dokumente aller Art in die Software geladen und können feststellen: Das maschinelle Lernen funktioniert, am Ende brauchen nur die wenigsten Dokumente noch manuelle Nacharbeit bei wiederkehrenden Tags und Dokumententypen. Das Bedürfnis, in den Lernprozess aktiv einzugreifen, hatten wir bei keinem Dokument.

Papier scannen

Die Suche nach einem Dokumenteneinzugsscanner für Ihre private Dokumentenverwaltung ist nicht gerade vergnüglich, denn die etablierten Hersteller überbieten sich auf diesem überschaubar großen Markt nicht gerade mit Innovationen. Die gute Nachricht: Sie müssen bei der Auswahl nicht darauf achten, ob ein Scanner mit paperless-ngx kompatibel ist und können auch ältere Gebrauchtkaufen. Die Software interessiert sich nämlich nicht dafür, wie die Dateien im Ordner consume innerhalb des Containers ankommen. Viele Scanner sprechen SMB oder FTP und können damit in den consume-Ordner schreiben, wenn Sie eines der Protokolle aktivieren. Im Wiki des Paperless-Projekts werden Erfahrungen mit ver-

schiedenen Scannern in einer Tabelle zusammengetragen, für unsere Dokumentenverwaltung haben wir uns schließlich für einen Brother ADS-1700W (ein Scanner mit Duplexfunktion) entschieden und hatten zunächst die Idee, ihn im lokalen Netzwerk über SMB anzubinden – das gelang in Kombination mit einem Synology-NAS nicht, auch nicht nach Update der ab Werk antiquierten Firmware. Qualifizierte Fehlermeldungen waren dem Gerät ebenfalls nicht zu entlocken. Mit einem Wechsel auf FTP, das keine nennenswerten Einschränkungen hat, funktionierten die Scans problemlos.

Am besten richten Sie einen neuen Nutzer für Ihren Scanner ein und vergeben ein Passwort für ihn. Dann berechtigen Sie ihn auf den consume-Ordner und richten den Pfad zu Ihrer Freigabe auf NAS oder Server als Kurzwahltaaste ein. Sollten Sie sich dafür entscheiden, Ihre Dokumentenverwaltung online auf einem gemieteten Server zu lagern, wird alles ungleich komplizierter, weil die Übertragung in jedem Fall verschlüsselt erfolgen muss. SFTP käme dann als Protokoll infrage, die Einrichtung von Zertifikaten (auch auf dem Scanner) würde den Umfang dieses Artikels sprengen.

Perfektion

Läuft der Scanner, können Sie ihn mit dem ersten Dokument füttern und finden es bestenfalls wenig später digital in der

Sammlung. Wenn nicht, müssen Sie die Kette der Reihe nach prüfen: Konnte der Scanner in den Ordner schreiben (Rechte prüfen), konnte paperless-ngx sie lesen (ebenfalls Rechte prüfen)?

Funktioniert die Verarbeitungskette, sind Sie der Perfektion nahe: Ein analoger Brief kommt an, landet im Einzugs des Scanners und damit digital und durchsuchbar in der Datensammlung. Doch was passiert mit dem analogen Exemplar? Wer seinem Scanner und seiner Backupstrategie komplett vertraut, kann das Papier anschließend umgehend im Aktenvernichter versenken. Wer sich hingegen noch an den mittlerweile legendären Vortrag „Traue keinem Scan, den du nicht selbst gefälscht hast“ von David Kriesel aus dem Jahr 2014 erinnert (die sehenswerte Aufzeichnung finden Sie über [ct.de/ytg4](https://www.ct.de/ytg4)), dem wird diese Strategie zu riskant sein. Der Informatiker Kriesel deckte auf, dass Xerox-Scankopierer eingescannte Zahlen durch einen Fehler in der Bildkompression vertauschten – und zwar nicht etwa beim OCR, sondern direkt in der Bilddatei. Wer, wie so mancher Xerox-Kunde, die Originale unmittelbar nach dem Scan vernichtet hatte, stand vor einem unlösbaren Problem, weil die Scans schlicht nicht der gedruckten Wahrheit entsprachen. Aber es drohen auch trivialere Probleme: Manchmal rutschen aufgefaltete Briefe nicht ganz sauber durch den Einzugs und einzelne Zeilen sind nicht richtig lesbar.

The screenshot displays the 'Details' view of a document in the Paperless-ngx application. The interface includes a top navigation bar with options like 'Löschen', 'Herunterladen', and 'Aktionen'. The main content area is divided into two panels. The left panel shows document metadata: 'Titel' (2021-06-08 jm_02072024_204801_00), 'Archiv-Seriennummer' (148), 'Ausgestellt am' (08.06.2021), 'Korrespondent' (Vermieter), 'Dokumenttyp' (empty), 'Speicherpfad' (Standard), and 'Tags' (Miete). The right panel shows document details: 'Gesamtkosten Direktkosten' (99.39), 'Zu verteilende Gesamtkosten' (10.819.13), and a list of 'Erläuterungen' (Explanations) and 'Zusätzliche Hinweise' (Additional Notes).

In der Detailansicht eines Dokuments sehen Sie dessen Metadaten und eine Vorschau.

Direkt schreddern sollten Sie nur Briefe, die nicht allzu wichtig sind. Doch wohin mit dem wichtigen Papier nach dem Scan?

Paperless-ngx liefert einen Lösungsansatz mit: Man versieht jedes Dokument vor dem Scan mit einem kleinen Aufkleber mit QR- oder Barcode, der eine Nummer kodiert – die „Archive Serial Number“ (ASN), wie paperless-ngx sie nennt. Beim Verarbeiten erkennt die Software den Code und heftet die Nummer an das digitale Dokument. In der Praxis legt man sich einen Bogen voller Etiketten mit fortlaufenden ASN-Codes neben den Scanner: aufkleben, scannen, anschließend das Papier kopfüber auf einen Stapel ablegen. Hat man später das Bedürfnis, das zugehörige Papier noch einmal hervorzuholen, schaut man auf die ASN und blättert zügig im Stapel zur richtigen Stelle. Wer sehr viele Dokumente verwaltet, wird irgendwann mehrere Kisten im Archiv stehen haben, beschriftet jeweils mit erster und letzter ASN.

Ein weiterer Vorteil der ASN-Barcodes: Wenn Sie mehrere (ein- oder mehrseitige) Dokumente nacheinander scannen wollen, kleben Sie einfach jeweils auf die erste Seite eines Dokuments einen ASN-Aufkleber und stopfen danach den gesamten Stapel in den Dokumenteneinzug. paperless-ngx ist schlau genug, den einen Scan anhand der ANNs automatisch zu splitten und die Dokumente getrennt zu verarbeiten. Das ist besonders praktisch, wenn Sie paperless-ngx frisch eingerichtet haben und die gesammelten Dokumente der vergangenen Jahre am Stück digitalisieren wollen.

Um ASNs zu nutzen, müssen Sie sich zunächst Aufkleber mit fortlaufenden Nummern neben dem Scanner bereitlegen. Für diesen Zweck hat der Entwickler Tobias Maier einen nützlichen webbasierten Generator gebaut und stellt ihn kostenfrei zur Verfügung (zu finden über ct.de/ytg4). Der Generator ist für Etikettenpapier vom Typ Avery L4731 gedacht, auf einer A4-Seite sind 189 kleine Etiketten mit den Maßen 25,4 × 10 Millimeter angeordnet. Das Paket mit 10 Bögen heißt im Handel „L4731REV-10“, 30 Bögen (25 und 5 „gratis“) bekommt man im Paket „L4731REV-25“.

Im Online-Generator eingeben müssen Sie nur die erste Zahl, die Anzahl der führenden Nullen und optional ein Präfix, das standardmäßig „ASN“ lautet. Das können Sie zum Beispiel auf Ihre Initialen ändern, wenn Sie davon ausgehen, dass

Der QR-Code-Generator von Entwickler Tobias Maier erzeugt Bögen mit sogenannten ASN-Etiketten. Die runden den Workflow mit gescannten Dokumenten ab.

im Büro noch andere Codes mit dem Präfix ASN kursieren. Damit die Randabstände für die Etiketten passen, müssen Sie den Generator unbedingt im Chrome-Browser ausführen und im Druckdialog unter „Erweitert“ die Option „Ränder“ auf „Keine“ umschalten.

Anschließend müssen Sie noch bis zu vier Änderungen an der Konfiguration von paperless-ngx vornehmen. Das geschieht über die Umgebungsvariablen in der Datei `docker-compose.env`. Mit folgenden Zeilen aktivieren Sie das automatische Barcodelesen:

```
PAPERLESS_CONSUMER_ENABLE_BARCODES=1
PAPERLESS_CONSUMER_BARCODE_SCANNER=1
PAPERLESS_CONSUMER_ENABLE_ASN=1
PAPERLESS_CONSUMER_ASN_BARCODE=1
PAPERLESS_CONSUMER_ASN_PREFIX=ASN
```

In unseren Tests funktionierte die Erkennung nur mit der Bibliothek ZXING, mit dem Standardwert PYZBAR erkannte das System keinen einzigen Code – laut Dokumentation ist das aber individuell unterschiedlich und man soll beide Varianten ausprobieren. Die letzte Zeile ist optional, dort vergeben Sie ein alternatives Präfix.

Nachdem Sie die Datei `docker-compose.env` angepasst haben, starten Sie die Containerzusammenstellung mit dem Befehl `docker compose restart neu`, dann sind Sie bereit für den perfekten Paperless-Workflow.

Fazit

Dokumentenverwaltung klingt mehr nach einer lästigen Pflicht als nach einer vernünftigen Angelegenheit. Mit einer selbst gehosteten Instanz von paperless-ngx und einem Einzugsscanner kommt aber überraschend Freude auf, wenn PDF-Dateien wie von Geisterhand im Browser auftauchen und dann noch automatisch verschlagwortet werden. Die Einrichtung ist nicht ganz trivial, was aber weniger an paperless-ngx und vielmehr am Drumherum liegt: Rechteverwaltung, Dateifreigaben und Dokumentenscanner.

Neben den in diesem Artikel gezeigten Funktionen hat paperless-ngx noch weitere zu bieten: Wenn bei Eingang bestimmter Dokumente Ereignisse ausgelöst werden sollen, öffnen Sie mit dem Menüpunkt Arbeitsabläufe links im Menü die Tür für weitere Optimierungen Ihres Dokumentenworkflows. Bisher auch unerwähnt blieb die nützliche Funktion, ein Mailkonto per IMAP zu öffnen und Dokumente dort automatisch aufzuspielen. Damit erweitern Sie die Dokumentenverwaltung auf eine weitere Quelle.

(jam@ct.de) **ct**

Literatur

- [1] Stefan Wischner, *Sauber abgelegt*, Programme für die persönliche Dokumentenverwaltung, c't 29/2023, S. 126
- [2] Jan Mahn, *Koffer umpacken*, Der Umstieg von Docker Desktop auf Podman, c't 13/2023, S. 138

Dokumentation und Compose-Datei:
ct.de/ytg4

Bewirb mich mal!

Unzulässiger Einsatz von KI-Tools für studentischen Bewerbungs-Essay

Wer bei einer Hochschulbewerbung einen Fachtext abliefern und sich dabei mit KI-erzeugten fremden Federn schmückt, setzt sich dem Vorwurf der Täuschung aus und darf sich nicht wundern, wenn man ihn vom Bewerbungsverfahren ausschließt.

Von Harald Büring

ChatGPT und andere Large Language Models (LLM) liefern auf die Eingabe geeigneter Prompts hin ausformulierte Texte in wunschgemäßem Sprachduktus. Angesichts dessen sehen sich insbesondere Bildungsinstitute einem wachsenden Problem ausgesetzt: Schriftlich verfasste Texte dienen in vielerlei Hinsicht als Leistungsnachweise, sei es in der Form von Hausarbeiten oder auch von Aufsätzen, die als eine Art akademischer Visitenkarten zu Hochschulbewerbungen gehören können. Die Versuchung für Studierende, eigene Leistung dabei durch Produkte künstlicher Intelligenz aufzuwerten, ist hoch. Je besser die verfügbaren Tools werden, desto schwieriger ist es, authentisch von Menschen Verfasstes und Promptgeborenes auseinanderzuhalten. Bislang finden Lehrkräfte und Hochschulverwaltungen immer wieder Wege, digital unterstützte Täuschungsansinnen aufzudecken.

So ist ein Student Ende 2023 vor Gericht mit dem Versuch gescheitert, bei einem bewerbungsrelevanten Text von künstlich intelligenter Hilfe zu profitieren. Der Mann wollte nach seinem Bachelorabschluss einen Masterstudiengang an der Technischen Universität München (TUM) absolvieren, wofür er sich zunächst erfolglos bewarb. Nach einem Jahr reichte er

erneut Bewerbungsunterlagen ein, zu denen wie beim ersten Mal ein Essay in englischer Sprache gehörte.

Im Folgenden schloss ihn die Hochschule vom Bewerbungsverfahren aus. Sie warf ihm vor, er habe versucht, den Bewerbungsprozess durch Täuschung zu beeinflussen. Eine Überprüfung des Essays durch eine Software habe ergeben, dass 45 Prozent des Texts sehr wahrscheinlich von künstlicher Intelligenz verfasst worden seien. Anschließend hätten zwei Professoren den Essay untersucht und das Ergebnis der Softwareprüfung bestätigt.

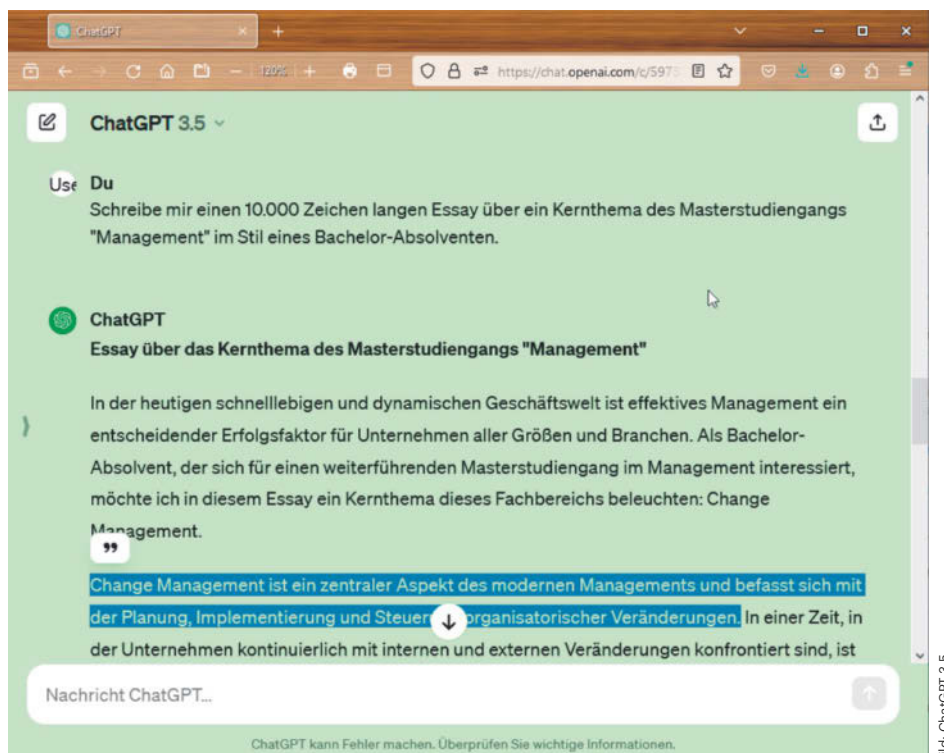
Zu gut, um echt zu sein

Der Student widersprach und klagte gegen den Bescheid. Darüber hinaus wollte er die Hochschule per einstweiliger Verfü-

gung dazu verpflichten, ihn vorläufig zum Masterstudium zuzulassen.

Das Verwaltungsgericht (VG) München lehnte jedoch den Antrag auf die Gewährung einstweiligen Rechtsschutzes ab [1]. Der ablehnende Bescheid der Hochschule sei nicht rechtswidrig gewesen. Ein Hauptsacheverfahren würde voraussichtlich ergeben, dass die Voraussetzungen für den Ausschluss vom Bewerbungsverfahren vorlagen.

Die Prüfungsbehörde der TUM, so das Gericht, habe hinreichend nachgewiesen, dass der Student durch die Erstellung des Essays mittels künstlicher Intelligenz eine selbstständige Leistung nur vorgespiegelt und damit einen Täuschungsversuch begangen habe. In diesem Zusammenhang sei es irrelevant, inwieweit die von der Hochschule verwendete Plagiatserkennungssoftware zuverlässig gearbeitet habe. Maßgeblich sei die Beurteilung durch die beiden erfahrenen Prüfer. Die waren zur Überzeugung gelangt, dass der Student den Text mittels ChatGPT erstellt habe. Das schlossen sie vor allem daraus, dass der strittige Essay sehr viel strukturierter aufgebaut sei als bei anderen Bachelorstudenten. Erfahrungsgemäß gebe es bei solchen Arbeiten Brüche in Stil und Logik – hier nicht.



Je besser sie werden, desto mehr wächst die Versuchung, mit KI-Tools wie ChatGPT eine selbst erbrachte studentische Leistung vorzutäuschen.

Ebenso ungewöhnlich sei, dass der Text keine verschachtelten Sätze enthalte und fehlerfreies Englisch aufweise. Das ließe sich nicht einmal dadurch erklären, dass der Student sein Bachelorstudium mit der Gesamtnote „sehr gut“ abgeschlossen und ein fünfmonatiges Auslandsstudium in den USA absolviert hatte. Wenn er über einschlägige Erfahrung im Formulieren wissenschaftlicher Texte verfügt hätte, lägen die Dinge anders. Dafür gebe es in dem Fall jedoch keine Anhaltspunkte. Darüber hinaus konnte der Student keinen plausiblen Grund liefern, warum sich der Essay so grundlegend von demjenigen unterschied, den er im Jahr zuvor eingereicht hatte.

Kein lückenloser Beweis nötig


Das Gericht weist darauf hin, dass die Prüfungsbehörde nicht verpflichtet war, einen lückenlosen Nachweis dafür zu liefern, dass der Student ChatGPT benutzt hatte. Ein sogenannter Anscheinsbeweis sei aus-

reichend: In diesem Fall bedeutete das den Befund, dass er aller Wahrscheinlichkeit nach darauf zurückgegriffen hatte.

Diese Entscheidung des VG München im vorläufigen Rechtsschutz ist mittlerweile rechtskräftig, da der Student keine Beschwerde dagegen eingelegt hat. Darüber hinaus hat er seine im Hauptsacheverfahren eingelegte Klage mittlerweile zurückgenommen.

Die unzulässige Nutzung von KI-Tools ist für Gerichte ein neues Thema. Bislang ging es bei akademischen Täuschungsversuchen vornehmlich um klassische Plagiate, bei denen Originaltexte ohne Zitatkennzeichnung in Arbeiten übernommen wurden. Das Bundesverwaltungsgericht (BVerwG) hat klargestellt, dass an den Nachweis eines solchen Plagiats keine allzu hohen Anforderungen gestellt werden dürfen. Der erforderliche Anscheinsbeweis gelte bereits als erbracht, wenn etwa die Bearbeitung weitgehend mit einem Lösungshinweis übereinstimmt und eine andere Erklä-

rung als deren Kenntnis nicht in Betracht kommt [2]. Wenn es um KI-gestützte Texterzeugung geht, ist allerdings kein Vergleich mit einem Originaltext im Hinblick auf übernommene Passagen möglich.

Ob es legitim ist, aus der perfekten Formulierung eines Textes auf KI-Nutzung zu schließen, bezweifelt Rechtsanwalt Christian Birnbaum in seinem Fachaufsatz zum Thema, der im vergangenen Jahr erschien [3]. Immerhin bringt dieses Kriterium das Risiko mit sich, sprachlich besonders talentierte Studenten zu Unrecht unter Täuschungsverdacht zu stellen. (psz@ct.de) 

Literatur

- [1] VG München, Beschluss vom 28.11.2023, Az. M 3 E 23.4371: heise.de/s/OPPWWQ
- [2] BVerwG, Beschluss vom 23.1.2018, Az. 6 B 67.17: heise.de/s/NddWE
- [3] Christian Birnbaum, ChatGPT und Prüfungsrecht, NVwZ 2023, 1127, 1131: heise.de/s/KMMWb

Webinar – 16. Mai 2024

Apple Vision Pro im Unternehmen einsetzen

Tauchen Sie ein in die revolutionäre Welt der Apple Vision Pro und entdecken Sie, wie Spatial Computing den professionellen Alltag transformieren kann.

Erfahren Sie in diesem Webinar, wie sich Apples Headset im Firmennetzwerk integrieren und verwalten lässt. Entdecken Sie das Potenzial der Vision Pro für den professionellen Einsatz und profitieren von praktischen Erfahrungen.

Mac & i Wissen erfahren



Jetzt Ticket sichern:

heise-academy.de/webinare/apple-vision-pro





Sie fragen – wir antworten!

Google-Kalender zeigt keine Geburtstage mehr an

? Ich verwalte meine Kontakte und meinen Terminkalender mit Google. Auf der Kalender-Webseite waren bislang immer die Geburtstage meiner Kontakte zu sehen, aber seit einiger Zeit sind sie verschwunden. Den Kalender „Geburtstage“ habe ich eingeschaltet, und gespeichert sind die Termine auch noch – direkt in den Kontakten kann ich sie mir ja anzeigen lassen. Mache ich etwas falsch oder ist das ein Problem bei Google?

! Eher letzteres, aber es gibt Abhilfe. Seit dem 7. März unterliegt Google den Vorschriften des „Digital Markets Act“ (DMA) der EU. Das Gesetz bestimmt unter

anderem, dass große Internetfirmen (so genannte „Gatekeeper“) die Daten ihrer Nutzer nur dann über verschiedene Anwendungen und Dienste hinweg verknüpfen dürfen, wenn die Anwender dem ausdrücklich zugestimmt haben. Um die Geburtstage aus den Kontakten im Kalender angezeigt zu bekommen, müssen Sie Google diese Berechtigung erteilen.

Zu den dafür zuständigen Einstellungen gelangen Sie, indem Sie im Browser in den Kontakten oder dem Kalender oben rechts auf Ihr Konto-Logo klicken und dem Link „Google-Konto verwalten“ folgen. Wechseln Sie dort auf die Seite „Daten und Datenschutz“, die im unteren Drittel einen Link „Verknüpfte Dienste verwalten“ enthält. Wenn Sie den anklicken, landen Sie auf einer Seite, auf der Sie auswählen können, für welche Dienste Google Ihre Daten zusammenführen darf. Für die Geburtstage im Kalender ist mindestens ein Häkchen hinter „Kontakte“ nötig; der Kalender selbst ist immer verbunden. (hos@ct.de)

Totalschaden durch BIOS-Einstellung

? Mein Laptop (Schenker XMG DTR 17 von 2019 mit i7-8700k) startet nicht mehr richtig, seit ich in den erweiterten BIOS-Einstellungen den „Processor Voltage Mode“ von „Adaptive“ zu „Override“ geändert habe. Ein BIOS-Reset scheint nicht zu funktionieren, der Bildschirm bleibt einfach schwarz. Das Erneuern der Wärmeleitpaste von CPU und GPU hat nicht geholfen. Der Support des Herstellers konnte auch nicht wirklich helfen – das Gerät sei nicht mehr zu retten. Aber eine Erklärung für das Verhalten konnte man mir nicht geben. Haben Sie noch eine Idee?

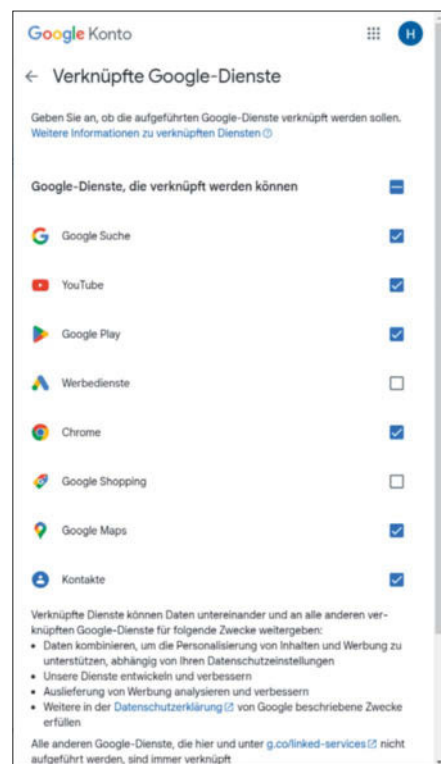
! Nach Ihren Schilderungen befürchten wir, dass die von Ihnen im BIOS vorgenommenen Änderungen an der Spannungsversorgung den Prozessor irreparabel beschädigt haben, weil er seitdem zu

viel Spannung abbekommt. Bei Änderungen dieser Art im hardwarenächsten Teil eines Notebooks kann leider viel schiefgehen: Wenn man nicht genau weiß, was eine BIOS-Einstellung bewirkt, sollte man tunlichst die Finger davon lassen.

Im Nachgang hilft frische Wärmeleitpaste genauso wenig, wie wenn sich in einem chipgetunten Motor ein Pleuel verbogen hat und man zur Behebung frisches Motoröl nachkippt: Ohne größeren Hardwaretausch, der ins Geld geht, lässt sich jetzt nichts mehr reparieren. In Ihrem Fall müssen wohl CPU, Mainboard oder beide ersetzt werden.

Ein vergleichsweise minimalinvasiver CPU-Tausch für ein paar hundert Euro ginge technisch, weil der Prozessor in Ihrem Notebook gesockelt ist. Das ist ein Sonderfall: Bei vielen modernen Notebooks müsste unweigerlich die gesamte Hauptplatine mit darauf aufgelöteter CPU gewechselt werden – zu vierstelligen Ersatzteilpreisen. Aber: Dort ist nach dem Austausch automatisch das gesamte technische Innenleben frisch, während in Ihrem Fall nach dem reinen CPU-Tausch das Risiko besteht, dass die weiterverwendete Hauptplatine auch den neu eingesetzten Prozessor zerstört, weil die fehlerhaften BIOS-Einstellungen eben weiterhin aktiv sind und sich das BIOS mit alter CPU im Sockel nicht mehr zurücksetzen lässt.

Die notebookspezifische Hauptplatine kostet ein Mehrfaches der CPU, hinzu kommen Arbeits- beziehungsweise Diagnosezeit als Eigenleistung oder kostenpflichtig in einer Werkstatt. Ein so hoher Reparaturbetrag ist wirtschaftlich betrachtet für ein vier bis fünf Jahre altes Notebook nicht mehr angemessen – sofern die notebookspezifische Hauptplatine überhaupt noch als Ersatzteil lieferbar ist. (mue@ct.de)



Für bestimmte Dienste muss man Google das Verknüpfen von Daten erlauben, wenn man diese in mehreren Anwendungen nutzen will.

Mobilfunk-Dongle für 5G?

? Auf gut Glück erwarb ich vor einigen Jahren ein USB-Dongle für das LTE-



LTE-Router sind flexibler und komfortabler als Mobilfunk-Dongles und auch ohne teures 5G richtig schnell. Häufig gibt es sie auch als Gebraucht-Schnäppchen.

Netz zur Verwendung für Linux. Dies funktionierte einwandfrei. Nun wollte ich mir ein zweites Dongle kaufen, das möglichst auch für 5G geeignet ist. Welche USB-Dongles für deutsche LTE- oder 5G-Netze funktionieren denn unter Linux und sind auch erhältlich? Habt ihr solche Geräte in jüngerer Vergangenheit getestet?

! USB-Dongles für Mobilfunk sind mittlerweile aus der Mode gekommen. Es gibt zwar Geräte von Acer, Peplink oder Alfa, diese sind jedoch genauso teuer wie ein 5G-Router oder sogar signifikant teurer. Unter 300 Euro kommen Sie nicht zum Ziel.

Die 5G-USB-Dongles, die es gibt, haben wir bislang nicht getestet und planen dies auch nicht, sodass wir Ihnen leider nicht mit Empfehlungen weiterhelfen können. Im Übrigen schränkt Sie so ein Dongle unnötig bei der Empfangsoptimierung ein. Grundlagen zu LTE und Tipps zur Empfangsoptimierung lesen Sie in c't 8/2022 ab Seite 140.

Mobilfunk-WLAN-Router sind heute der Standard für Ihren Anwendungsfall. Mit einem solchen Gerät verbinden Sie sich einfach per WLAN oder Kabel und sind online. Die Konfiguration läuft über den Browser, das eingesetzte Betriebssystem ist somit größtenteils egal.

Wenn Sie gleich mit 5G starten wollen, können Sie das mit dem ZTE MC801A tun, der derzeit der günstigste 5G-Router ist: Laut Preisvergleich bekommen Sie ihn ab etwa 300 Euro.

Sollte Ihnen das zu teuer sein, schauen Sie bei Kleinanzeigen & Co. nach dem Gigacube Cat 19 (Huawei B818), dem Gigacube Z21 (ZTE MF289F) oder der Speedbox IV (Huawei B618). Das sind zwar alles LTE-Geräte, haben aber modernere und somit schnellere Modems (LTE-Kategorie) als Ihr jetziger Stick. Sie werden überrascht sein, wie viel schneller Sie damit surfen. Die Geräte kosten gebraucht nur 40 bis 100 Euro. (amo@ct.de)

Kein Web trotz Internetverbindung

? Ich verwende Windows 11. Seit einiger Zeit ist es nach dem Starten des Rechners für einen bestimmten Zeitraum nicht möglich, über einen Browser auf Internetseiten zuzugreifen. Auch ist die Anmeldung von OneDrive oder iCloud nicht möglich. Das Abrufen von Mails funktioniert dagegen. Wenn ich die Windows-Netzwerkdiagnose aufrufe, dann sagt sie mir, dass der Rechner mit dem Internet verbunden ist. Ich suche nach einer Möglichkeit, der Sache auf den Grund zu gehen. Ich bin aber mit Netzwerküberwachungswerkzeugen nicht besonders vertraut. Haben Sie einen Tipp?

! Dafür gibt es nicht ein Werkzeug, sondern eine Reihe von Schritten, die Sie probieren sollten.

Erster Schritt: Ist es das Netz oder nur die Namensauflösung? Das können Sie feststellen, in dem Sie in einer Kommandozeile verschiedene Adressen anpingen, solange das Phänomen auftritt. Beginnen Sie mit der IP-Adresse des Routers, bei einer Fritzbox in Standardkonfiguration meist ping 192.168.178.1. Wenn das geht, wäre der nächste Schritt ein ping heise.de. Damit haben Sie dann raus, ob es zwischen dem Windows-PC und dem Router Probleme gibt (erster Test liefert keine Pakete/Timeouts) oder ob „nur“ die Namensauflösung schuld ist (zweiter Test schlägt fehl). Wenn das Abrufen von Mail gelingt, aber viele andere Dienste nicht laufen, könnte auch ein Sicherheitsproxy klemmen – manche Sicherheitssoftware bringt solche „Schutzfunktionen“ mit, die gern mal komische Dinge tun. (ps@ct.de)

Funkstörungen im Analogtelefon

? Nach der Lektüre des Artikels „Funknachschrung“ in c't 5/2024, Seite 128, habe ich mir eine Fritzbox 6850 LTE geholt und zwei Festnetztelefone damit verbunden. Mit einem DECT-Telefon geht das problemlos, aber der Ton des zusätzlich angeschlossenen alten Festnetztelefons wird vom Mobilfunk der Fritzbox gestört. Je schlechter das Signal vom Funkmast und je höher dadurch die Sendeleistung der Box werden, desto stärker fallen die Störungen aus. Wie gewöhne ich der Fritzbox das ab?

! Das Problem liegt in diesem Fall nicht an der Fritzbox, sondern am Analogtelefon, das offensichtlich keine ausreichende Immunität gegen elektromagnetische Felder hat. Versuchen Sie, das Gerät so weit weg wie möglich von der Box zu platzieren, um die Feldstärke zu verringern, gegebenenfalls mit einer Kabelverlängerung, wenn das sinnvoll ist.

Zusätzlich sollten Sie zwei Klappferite beschaffen und an den Enden des Verbindungskabels montieren, idealerweise wickeln sie zwei bis drei Windungen auf den Ferrit. Das blockt HF-Signale ab, die sonst übers Kabel ihren Weg ins Telefon finden und dort Störungen verursachen.

Alternativ könnten Sie für die Fritzbox eine externe Antenne beschaffen und an einem Ort aufstellen, wo sie keine Störungen verursacht. Ideal, aber aufwendig zu montieren, ist dafür eine Außenantenne.

(uma@ct.de)

Fragen richten Sie bitte an

hotline@ct.de

c't Magazin

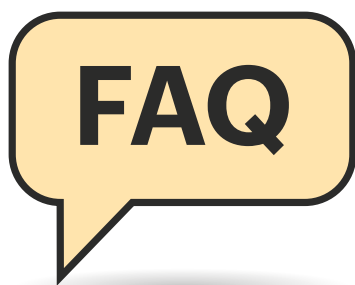
@ctmagazin

ct_magazin

@ct_Magazin

c't magazin

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter **www.ct.de/hotline**.



3D-Ton für Filme, Musik und Spiele

Wer Filme, Musik oder Spiele in Dolby Atmos oder anderen 3D-Formaten hören möchte, steht vor einem Dschungel an Wiedergabemöglichkeiten. Ob über Kopfhörer, Soundbars oder riesige Lautsprecheranlagen – wir beantworten die wichtigsten Fragen.

Von Hartmut Gieselmann

3D-Wiedergabe

? Wie kann ich Filme, Musik oder Spiele in Dolby Atmos und anderen 3D-Formaten über Kopfhörer und Lautsprecher hören?

! Neue 3D-Formate wie Dolby Atmos und DTS:X können Sie mit jeder Lautsprecherkonfiguration abspielen. Egal, ob Sie Mono-Lautsprecher, Stereo-Kopfhörer, ein 5.1 (fünf-Surround-Lautsprecher und ein Subwoofer) oder gar ein 7.4.6-Setup (sieben Surround-Lautsprecher, vier Subwoofer und sechs Deckenlautsprecher) verwenden. Die Decoder in der Abspielsoftware oder in Ihrem AV-Receiver wandeln den Datenstrom für Ihre jeweilige Lautsprecherkonfiguration um. Das ist auch der große Vorteil im Vergleich zu älteren Surround-Formaten, bei denen jede Lautsprecherkonfiguration eine eigene Mischung benötigt.

Ausbau der Heimkinoanlage

? Ich besitze bereits eine 5.1-Anlage. Kann ich diese zu einer Atmos-Anlage mit Deckenlautsprechern aufrüsten?

! Da sowohl Dolby Atmos als auch DTS:X verschiedene Lautsprecherkonfigurationen unterstützen, können Sie Ihre Anlage Stück für Stück weiter ausbauen. Wenn Ihr AV-Receiver älter ist, müssen Sie ihn wahrscheinlich ersetzen und ein Modell wählen, das zusätzlich zwei oder vier Deckenlautsprecher unterstützt. Entscheidend für die Klangqualität ist die Raumkorrektur, mit der der Verstärker Ihre Lautsprecher per Mikrofonmessung an die Raumakustik anpasst. Aktuell

le Systeme mit Audyssey, YPAO und Dirac Live haben wir zuletzt in c't 27/2023, Seite 90 getestet.

Da meist nur wenige Effekte und Umgebungsgeräusche von der Decke kommen, reichen kleinere und günstigere Deckenlautsprecher aus. Um deren Klang besser von den Deckenreflexionen der anderen unteren Lautsprecher zu trennen, kann die Aufhängung eines Deckensegels aus akustischem Dämmmaterial helfen.

Wenn Sie die Verkabelung abschreckt, können Sie alternativ zu Deckenlautsprechern sogenannte Upfiring-Modelle einsetzen, die die Höhenkanäle über die Decke reflektierend „über Bande“ zum Zuhörer spielen. Mit solch einer „Soundprojektion“ arbeiten auch viele Soundbars, um einen Rundum-Effekt zu erzeugen. Die Höhenstaffelung ist dabei aber nicht so differenziert wie mit Deckenlautsprechern.

Zwei Subwoofer

? Warum sollte ich einen zweiten Subwoofer an meine Anlage anschließen? Einer ist doch schon laut genug, dass meine Nachbarn an die Decke klopfen. Oder bekomme ich dann Stereo-Bass?

! Nein, ein zweiter Subwoofer gibt kein Stereosignal wieder und der Bass wird dadurch auch nicht lauter. Sein Zweck ist es vielmehr, die Pegel der tiefen Frequenzen gleichmäßiger im Raum zu verteilen, sodass die Nachbarn weniger gestört werden und man trotzdem an verschiedenen Hörpositionen einen ausgeglichenen Basspegel hat, ohne dass es dröhnt oder wummert. Zwei (oder mehr) kleine Subwoofer sind deshalb besser geeignet als ein großer.

Dazu sollte man raumakustische Besonderheiten bei der Aufstellung beachten und den Frequenzgang und die Phasen der Subwoofer einmessen. Wie das manuell mit der Software Room EQ Wizard oder automatisch mit Dirac Live Bass Control funktioniert, haben wir in der c't 7/2024, Seite 134 ausführlich erklärt.

Kopfhörerwiedergabe

? Welche Kopfhörer eignen sich besonders gut für die Wiedergabe von 3D-Klang?

! Sie benötigen keine speziellen „3D-Kopfhörer“, sondern können die binauralen 3D-Simulationen von Dolby und DTS auf ganz normalen Stereokopfhörern wiedergeben. Diese sollten allerdings einen möglichst ausgeglichenen Frequenzgang haben, um die Wirkung der Filter für den Rundum-Eindruck nicht zu verfälschen. Typische Gaming-Kopfhörer sowie zahlreiche Bluetooth-Modelle sind für die 3D-Wiedergabe meistens schlecht geeignet. Ihr Frequenzgang ist oft stark verzerrt und sie betonen den Bass zu stark, was den Raumeindruck verschlechtert.

Wesentlich besser geeignet sind offene Kopfhörer mit einem möglichst neutralen Frequenzgang. Dazu gehören zum Beispiel der AKG K702 für unter 150 Euro, die HD-600-Serie von Sennheiser ab 300 Euro oder der Ollo S5X 1.1 und Neumann NDH 30 in der Preisklasse über 500 Euro.

Apple-Nutzer können bei den neuesten AirPods sowie den Pro- und Max-Modellen mit iOS-Geräten, Apple TV (4K) und Macs mit M-Prozessor die automatische Bewegungserkennung der Kopfhörer nutzen: Die Klangkulisse scheint im Raum

zu stehen, wenn man den Kopf dreht. Speziell bei den AirPods Max beeinträchtigt die starke Bassbetonung jedoch den Raumeindruck.

3D-Tonformate für Filme

? Wie unterscheiden sich die 3D-Soundformate für Filme?

! Am weitesten verbreitet ist Dolby Atmos. Es wird von vielen Blockbustern und Hollywood-Produktionen sowie von Streaminganbietern wie Netflix, Apple und Disney eingesetzt. Es ist auch das 3D-Format, das am häufigsten auf Blu-ray Discs und UHD-Blu-rays anzutreffen ist.

DTS:X unterscheidet sich zwar in einigen Details, ist qualitativ aber gleichwertig und auf manchen Blu-ray Discs und UHD-Scheiben zu finden. Rakuten.tv ist derzeit der einzige Streamingdienst, der DTS:X bei wenigen Sony-Filmen wie „Equalizer 2“ einsetzt. Dabei wird allerdings ein spezieller Streaming-Codec genutzt, der nur mit Fernsehern dekodiert werden kann, die nach dem „IMAX Enhanced“-Programm zertifiziert wurden. Nähere Infos finden Sie dazu in c't 9/2021, Seite 144.

Das dritte Format ist Auro-3D, das im Unterschied zu Dolby Atmos und DTS:X jedoch nicht objektbasiert, sondern kanalbasiert arbeitet. Filmscheiben mit Auro-3D-Tonspuren sind sehr selten, die bekannteste ist noch „Passengers“. Beliebt ist jedoch Auros Upmixer „AuroMatic“, der Tonspuren in Mono, Stereo, 5.1 und 7.1 auf hintere und obere Lautsprecher ausdehnt. Man findet ihn in AV-Receiver der Oberklasse und kann dort zwischen Presets mit verschiedenen Hall- und Frequenzbearbeitungen wählen.

Streaming-Qualität

? Klingen Atmos-Tonspuren bei Streamingdiensten genauso gut wie auf der Film-Disc?

! Meistens nicht. Ähnlich wie bei der Bildqualität bieten Scheiben eine oft deutlich bessere Tonqualität als die Streamingdienste. Das liegt an den Bitraten der Datenströme. Bei „Im Westen nichts Neues“ streamt Netflix den Atmos-Ton beispielsweise nur mit 768 kbit/s, während die UHD-Scheibe durchschnittlich etwa 4 Mbit/s, in der Spitze sogar über 5 Mbit/s



Apocalypse Now wurde bereits Ende der 70er Jahre in aufwendigem Surround-Sound gemischt. Der Atmos-Mix gehört zu den besten derzeit erhältlichen 3D-Tonspuren.

erreicht. Unter der starken Datenkompression der Streaminganbieter leidet vor allem die räumliche Darstellung, aber auch die Dynamik.

Film-Empfehlungen

? Welche Filme könnt ihr als Demoscheiben mit deutschem 3D-Sound empfehlen?

! Die meisten Filme bieten leider nur englische Atmos-Tonspuren an. Überaus empfehlenswerte Titel mit deutschen Atmos-Tonspuren sind die Blockbuster „Mission Impossible: Dead Reckoning“ und „Dune“, die restaurierte Fassung von „Apocalypse Now“ sowie die Neuverfilmung von „Im Westen nichts Neues“. Auch bei ihnen sind die 4K-UHD-Discs den Streamingversionen überlegen.

3D-Musik

? Stücke mit 3D-Sound sind doch nur ein Gimmick und taugen nicht für anspruchsvolle Musik, oder?

! Dieses Vorurteil können wir nicht bestätigen. Die Ergebnisse sind zwar unterschiedlich und es gibt viele Mixe, bei denen die 3D-Effekte übertrieben, falsch oder gar nicht eingesetzt werden. Aber die Tontechniker gewinnen immer mehr an Erfahrung, sodass sie den Raumklang nicht für billige Effekte, sondern eine natürliche Platzierung der Stimmen und Instrumente und einer überzeugenden räumlichen Atmosphäre einsetzen. Nicht umsonst produzieren beispielsweise die Ber-

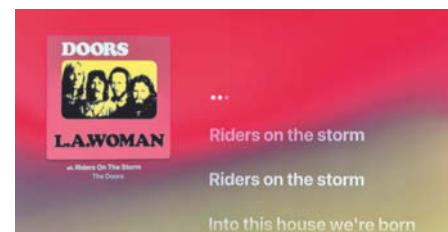
liner Philharmoniker alle ihre Konzerte in Dolby Atmos.

Neben exzellenten 3D-Aufnahmen von Pink Floyd, Kraftwerk, Yello oder Billie Eilish wurden in jüngster Zeit auch Alben von The Doors und Bob Marley gekonnt in Atmos remixed. Das Jazz-Label Blue Note hat wiederum einige Klassiker von Miles Davis & Co. erstaunlich aufgewertet. Eine umfangreiche Playlist mit besonders gelungenen Atmos-Stücken auf Apple Music hat der Autor unter ct.de/ybmu zusammengestellt.

Streaminganbieter

? Auf welchen Wegen kann ich Musik in 3D hören?

! Auf Tonträgern ist das Angebot sehr übersichtlich. Hier gibt es nur eine Handvoll Blu-ray Discs von Kassenschlagern wie „The Dark Side of the Moon“, „Kraftwerk 3-D“ oder Beethovens Symphonien. Für 3D-Musik sind daher drei Streaminganbieter relevant: Amazon Music Unlimited für 10 Euro/Monat, Apple Music für



Selbst alte Aufnahmen wie „Riders on the Storm“ von The Doors gewinnen in der Dolby-Atmos-Mischung eine erstaunliche Klangfülle ohne billige 3D-Effekte.

11 Euro/Monat und Tidal HiFi Plus für 20 Euro/Monat. Außerdem streamt die „Digital Concert Hall“ der Berliner Philharmonie Konzerte in Dolby Atmos für 17 Euro/Monat.

Die drei Streamingdienste unterscheiden sich sowohl in der Auswahl als auch in den Wiedergabeformaten. Bei allen drei Anbietern ist es mitunter schwierig, die richtige 3D-Version eines Albums zu finden, da oft auch ansonsten identische Stereo-Versionen im Katalog stehen oder manche 3D-Songs nach einigen Wochen wieder verschwinden.

Den besten Überblick bietet noch Apple, das sich ausschließlich auf Dolby Atmos konzentriert. Auf der Suchseite der Musik-App findet sich eine eigene Kategorie für 3D-Musik, die aktuelle Alben verschiedener Genres auflistet.

Amazon und Tidal bieten neben Dolby Atmos auch Musik in 360 Real Audio (360RA) an, das von Sony zusammen mit Fraunhofer entwickelt wurde. Allerdings ist die Auswahl bei Amazon und Tidal nach unseren Stichproben kleiner als bei Apple. Sony bietet inzwischen Atmos-Mischungen seiner 360RA-Titel bei Apple Music an. Ein starkes Indiz dafür, dass der Formatkampf inzwischen zugunsten von Dolby entschieden ist.

Amazon hat keine spezielle Übersichtsseite für 3D-Audio. Man muss die Titel auf gut Glück suchen. Die Apple-TV-App von Amazon Music gibt zudem kein 3D-Audio, sondern nur Stereo aus. Tidal bewirbt nur eine kleine Auswahl an 3D-Titeln. Über Tidals Apple-TV-App kommt man nur an Dolby-Atmos-Titel in 3D, 360RA-Versionen erklingen nur in Stereo.

Formatfrage

? Gibt es einen Unterschied zwischen Dolby Atmos und 360 Real Audio, oder klingen beide gleich?

! Beide Formate spielen bei der mobilen Wiedergabe eine vorgerenderte binaurale Version ab, die über gewöhnliche Stereokopfhörer funktioniert. Dabei verwenden Atmos und 360RA unterschiedliche Verfahren und Filter. Bei 360RA wird der Kopfhörerton stärker beeinträchtigt und klingt oft dünn und blechern. Dolby hat seine binauralen Filter besser abgestimmt, aber auch hier gibt es Unterschiede: Apple verwendet angepasste Filter, die insbesondere den Bass anders betonen als die von Tidal und Amazon verwendeten Dolby-Filter.

Das Horror-Adventure Alan Wake 2 überzeugt mit einem besonders gut abgestimmten 3D-Sound.



ter. Dies führt selbst beim Abspielen der gleichen Atmos-Versionen von Musiktiteln über Amazon, Apple oder Tidal manchmal zu Unterschieden in der Klangabstimmung.

Die Wiedergabe von 3D-Audio muss unter Android im Setup der Streaming-Apps von Apple und Amazon aktiviert werden. Bei Amazon kann man dann zwischen Stereo- und 3D-Version umschalten. Dazu tippt man auf den Format-Schriftzug unter der Wiedergabeleiste. Bei 360RA ist dies manchmal nicht möglich. Tidal erlaubt nicht, zwischen Stereo und 3D zu wechseln.

Apple hat eine 3D-Simulation in seine Betriebssysteme integriert. Bei der Wiedergabe mit Apple Music kann man zwischen der Stereo- und der Dolby-Version umschalten, indem man im Kontrollzentrum lange auf den Lautstärkeregler des Kopfhörers und dann auf „3D-Audio“ tippt. Bei Tidal und Amazon sollte man die zusätzliche 3D-Audiosimulation jedoch ausschalten. Deren 3D-Stream ist bereits binaural gefiltert.

Lautstärkeunterschiede

? Warum sind die 3D-Versionen von Musikstücken oft deutlich leiser als die Stereo-Versionen? Dieser Effekt stört mich vor allem beim abwechselnden Hören von 3D- und Stereomusik. Auch mit eingeschalteter Lautstärkenormalisierung gleichen die Apps diesen Effekt nicht vollständig aus.

! Das liegt vor allem daran, dass Dolby für den Atmos-Mix eine durchschnittliche Lautstärke von maximal -18 LUFS erlaubt. Das ist oft 10 Dezibel leiser als typische Stereo-Mixe in den Charts. Dadurch können Atmos-Mischungen aber eine wesentlich höhere Dynamik ausnutzen.

Allerdings werden für Stereo- und 3D-Versionen unterschiedliche Messmethoden verwendet, um ihre Lautstärke zu

bestimmen. Folglich ist der Lautstärkeausgleich bei der Wiedergabe nicht immer optimal. Aus diesem Grund empfehlen wir auch nicht, Stereo- und 3D-Songs in einer Playlist zu mischen.

Spiele mit 3D-Sound

? Welche Spiele könnt ihr für 3D-Sound empfehlen?

! Im Vergleich zu Filmen und Musik kann der 3D-Sound vieler Spiele nicht besonders überzeugen. Das liegt zum einen daran, dass 3D-Soundobjekte selten über dem Kopf des Spielers zu hören sind und die Deckenebene oft stumm bleibt. Zum anderen kämpft der Sound vieler Spiele mit ganz profanen Dingen wie der Lautstärkeregelung und dem richtigen Nachhall einzelner Klangobjekte.

Zu den besseren Vertretern gehört hier noch das aus allen 3D-Rohren schießende „Cyberpunk 2077“: Es platziert extrem viele Geräusche und Stimmen um den Spieler herum, patzt aber gelegentlich bei der Feinjustierung. Da die Abmischung immer automatisch in Echtzeit erfolgt, klingt sie nicht so ausgefeilt wie bei Filmen oder Musik, wo ein Toningenieur alles austüftelt.

Zu den wenigen Titeln, die in 3D eine durchweg überzeugende Soundkulisse aufbauen, gehört das Horror-Adventure „Alan Wake 2“. Eine gute Arbeit haben die Tontechniker auch bei den neueren Teilen der „Resident Evil“-Reihe geleistet. Unter ct.de/ybmu listen wir weitere Spiele mit 3D-Sound auf.

Eigene Musik in 3D

? Kann ich auch als Hobbymusiker 3D-Musik auf den Streamingplattformen veröffentlichen?

! Ja, das ist möglich. In der höchsten Ausbaustufe unterstützen die digitalen Audio-Workstations (DAW) von Apple Logic Pro X, Presonus Studio One, Steinberg Cubase und Nuendo sowie Avid Pro Tools den Renderer für Dolby Atmos. Wie das in Logic funktioniert, erklären wir in c't 4/2022, Seite 142.

Mit dem Dolby-Atmos-Renderer ist auch ein Abhören der Mischung über Kopfhörer möglich. Den fertigen Atmos-Track können Sie über den Vertrieb von Distrokid für eine Zusatzzahlung von 27 US-Dollar pro Song bei den Streamingdiensten veröffentlichen. Ein Song des Autors war anschließend bei Apple Music und Tidal in Atmos abrufbar, Amazon streamt nur die Stereo-Version.

Auch Sony bietet ein Plug-in für 360RA an. Allerdings ist das Format aufgrund der schlechten Qualität des binauralen Renderers für Kopfhörer nicht zu empfehlen.

Wenn Sie Ihre Musik für experimentelle Klanginstallationen oder VR-Spiele

jenseits der großen Streaming-Plattformen abmischen möchten, können Sie auch die DAW Cockos Reaper und das freie Ambisonics-Format nutzen.

Spielkonsolen und PCs

? Welche Konsolen und Betriebssysteme unterstützen 3D-Ton in Spielen?

! Windows 10 und Windows 11 sowie die Xbox-Modelle One, Series X und S unterstützen die Ausgabe von Dolby Atmos und DTS:X. Dazu muss man zwei Apps aus dem Microsoft Store installieren: „Dolby Access“ und „DTS Sound Unbound“. Die Ausgabe über HDMI ist kostenlos. Die Umwandlung über binaurale Filter für Stereokopfhörer kostet 15 US-Dollar für Dolby und 20 US-Dollar für DTS. Da der 3D-Eindruck sowohl vom eigenen Gehör als auch von den Kopfhörern abhängt, kann man beides

vor dem Kauf in den Apps eine Woche ausprobieren.

Die Playstation 5 von Sony nutzt einen eigenen virtuellen 3D-Modus für Fernseher und Kopfhörer. Außerdem kann die Konsole seit Herbst den gesamten Ton über HDMI auch in Dolby Atmos ausgeben (Einstellungen/Ton/Audioausgabe/Audioformat (Priorität): Dolby Atmos). Dies funktioniert unabhängig davon, ob ein Spiel tatsächlich 3D-Sound unterstützt oder nicht. Bei Spielen ohne echten 3D-Sound kann es sich lohnen, die Soundausgabe auf PCM umzustellen und einen Automatic-Upmixer im Verstärker einzuschalten.

Linux und macOS unterstützen weder Dolby Atmos noch DTS:X in Spielen. Für eine räumliche Kopfhörerausgabe verfügen einige Spiele jedoch über eigene binaurale Filter. Diese sind in der Spieleinstellung auswählbar. (hag@ct.de)

Apple Music 3D-Playlist und PS5-Spiele:
ct.de/ybmu

» Continuous Lifecycle » [Container Conf]

13./14. November 2024 • Mannheim



Die Konferenz für Developer Experience, Platform Engineering und mehr

Continuous Lifecycle und ContainerConf (CLC) sind der Treffpunkt für IT-Profis, die sich für das schnelle und zuverlässige **Deployment** sowie den reibungslosen und sicheren **Betrieb** ihrer Software verantwortlich fühlen, zum Beispiel Softwareentwickler, DevOps Engineers, Software- und Infrastrukturarchitekten.

Seit 2013 tauschen sie sich hier aus über den Stand der Kunst in puncto **Continuous Delivery** und **DevOps** sowie **Container**, **Kubernetes**, **Developer Experience** und **Platform Engineering**.

Beim Call for Proposals können Sie bis zum 5. Mai Ihre **Vorschläge für Vorträge** und **Workshops** einreichen – Ideen für Themen finden Sie auf der Konferenzwebseite. Wir freuen uns auf Ihre Vorschläge!

Jetzt
einreichen!
**Call for
Proposals**
bis 5. Mai

Jetzt schon Blind-Bird-Tickets sichern!

continuouslifecycle.de

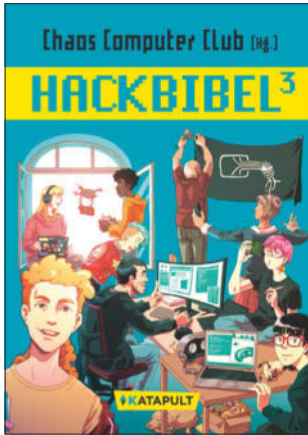
Veranstalter



dpunkt.verlag

Goldsponsor

sysdig



Chaos Computer Club (Hg.)
Hackbibel 3

Katapult, Greifswald 2024
ISBN 978-3948923822
224 Seiten, 28 €

Buntes von der Datenfront

In ihrer dritten Ausgabe hat die traditionelle „Hackerbibel“ des Chaos Computer Club (CCC) ihr „er“ in der Mitte eingebüßt. Auch ansonsten geht es progressiv zu – gleichzeitig ist die Lektüre unverändert informativ und anregend.

Seit Jahrzehnten ist der CCC eine zivilgesellschaftliche Größe in Sachen IT- und Datensicherheit. Er engagiert sich für digitale Bürgerrechte und macht immer wieder mit spektakulären Hacks von sich reden.

Die in großen Abständen erschienene „Hackerbibel“ gewährt in voneinander unabhängigen Beiträgen vieler Autoren erfrischende Einblicke in das, was sich an der Basis des Clubs tut. Die erste Ausgabe kam 1985, die zweite 1988. Es dauerte dann 36 Jahre, bis die aktuelle „Hackbibel“ in peppiger Aufmachung beim Katapult-Verlag das Licht der Bücherwelt erblickte.

Die angesprochene Klientel unterscheidet sich stark von der der Achtzigerjahre. Damals dominierten Männer den Club; heute ist er deutlich bunter und diverser. Das zeigen unter anderem Betrachtungen über die Geschichte der Haecksen sowie eine Abhandlung über Pride-Flaggen und deren Bedeutung.

Großen Raum nehmen traditionell Themen wie Überwachung und Datenschutz ein. In einem Artikel der aktuellen Ausgabe geht es beispielsweise um biometrische Authentifikation anhand der nachgebildeten Fingerabdrücke von Wolfgang Schäuble.

Verschiedene Autoren beleuchten juristische Spezialitäten wie den hinderlichen Einfluss des Urheberrechts auf die Suche nach Software-Sicherheitslücken und beschreiben Gesetzgebungsverfahren in Deutschland und in der EU. Sehr hilfreich ist der Beitrag über die richtige Vorgehensweise beim Melden von Schwachstellen.

Erwartungsgemäß finden sich auch klassische Hacking-Geschichten; das Spektrum reicht von einer detaillierten Darstellung des Angriffs auf den FinFisher-Hersteller Gamma bis hin zum Fix des TI-Konnektors der Gematik-Infrastruktur. Zwischendurch gibt es immer wieder Nerdiges, etwa eine Bauanleitung für LED-Throwies.

Zum Schluss blicken die Autoren in die Vergangenheit und in ihre Archive. Sie erzählen, wie der CCC Wahlcomputer verhinderte, und stellen die Arbeit der Wau-Holland-Stiftung vor.

Die Auswahl der Artikel repräsentiert die Vielfalt, die den CCC heute ausmacht. Alle Beiträge sind deutschsprachig bis auf drei, die in leicht verständlichem Englisch vorliegen.

(Maik Schmidt/psz@ct.de)

Alles verpacken!

Containereinsatz hat die Softwarewelt nachhaltig verändert und modernen Prozessen wie DevOps den Weg bereitet. Die neue Auflage des Handbuchs von Kane und Matthias beschreibt praxisnah die Grundlagen und den aktuellen Stand der Technik rund um Docker.

Die Autoren bringen neun Jahre Erfahrung als Berater mit. Das spürt man nicht zuletzt an dem Repertoire von Best Practices, das sie mit ihrem Lesepublikum teilen. Innerhalb der elf Jahre nach dem Erscheinen der quelloffenen Docker-Softwarebasis hat sich viel getan. Die vollständig überarbeitete und erweiterte dritte Auflage des Buches hat folglich manches Neue zu Tools und Techniken sowie insbesondere zu fortgeschrittenen Themen wie Orchestrierung, Sicherheit und Vernetzung zu sagen. Zugleich verstehen die Autoren ihr Werk auch als Plädoyer für die Containertechnik und zeigen Entwicklern, Softwarearchitekten, Administratoren und IT-Managern, wie der produktive Einsatz von Docker Aspekte der Bereitstellung, Verwaltung und Nutzung von Software verbessern kann.

Praktikern kommt das Buch mit detaillierten Beispielen und Tipps entgegen. Kommandozeilenwerkzeuge, die aus der allgemeinen Arbeit mit unixoiden Betriebssystemen bekannt sind, helfen dabei, das Docker-System zu parametrisieren, und bewähren sich auch, wenn es darum geht, Fehler in containerisierten Anwendungen zu suchen. Die reiche Bebilderung hilft, das Vorgeführte nachzuvollziehen.

Komplexe Systeme profitieren, wenn Containerflotten automatisch entstehen. Die Docker-Welt bietet dafür das Orchestrierungssystem Compose; die Autoren zeigen dessen Einsatz unter anderem anhand der unternehmensinternen Kommunikationsanwendung Rocket.Chat. Solche Exkurse leiten zu einer detaillierten Analyse des Produktiveinsatzes von Containern über. Es geht um automatische Skalierung, aber auch ums Isolieren verschiedener auf einem Rechner laufender Instanzen. Das ist bei sicherheitskritischen Anwendungen besonders relevant.

Um Schwächen des Buches zu finden, muss man schon auf hohem Niveau meckern. So kommt leider nur am Rande zur Sprache, wie man Dockerfiles erzeugt. Insgesamt macht es Stärken und Grenzen des mächtigen Docker-Systems gut transparent; es enttäuscht weder Entscheider noch Praktiker.

(Tam Hanna/psz@ct.de)



Sean P. Kane mit Karl Matthias,
Deutsch von Thomas Demmig

Praxiswissen Docker

Grundlagen und Best Practices für das
Deployen von Software mit Containern

O'Reilly, Heidelberg 2024 (3. Aufl.)

(der Buchverlag gehört wie c't

zu heise medien)

ISBN 978-3960092353

392 Seiten, 45 €

(als Bundle mit E-Book beim Verlag: 50 €;
PDF-/Epub-/Kindle-E-Book allein: 45 €)

Heft + PDF
mit 28 % Rabatt

Hype oder Hilfe?

Mit Künstlicher Intelligenz produktiv arbeiten



Dieses Heft verschafft Ihnen einen umfassenden Überblick, wie Sprachmodelle grundlegend funktionieren und in welchen Bereichen Ihnen eine KI wirklich helfen kann oder wo die Hersteller eine Arbeitserleichterung nur vorgaukeln.

- KI-Programme anwenden
- Grenzen der Sprachmodelle erkennen
- Was Unternehmen rechtlich beachten müssen
 - Die eigene Sprach-KI betreiben
 - Wo KI-Assistenten tatsächlich helfen
 - Wie KI Schule und Arbeit verändert



Jetzt
bestellen!

Heft für 14,90 € • PDF für 12,99 €
Heft + PDF 19,90 €



shop.heise.de/ct-ki23



DER GANZ BESONDERE MARVIN

VON BERNHARD HORWATITSCH

Stromberg arbeitete als externer staatlicher Inspekteur neuer Roboterer Serien, um diese auf Mängel, Mutationen oder eigenständige Automatismen hin zu überprüfen. Gerade solche Serien, die in Privathaushalte gingen, wurden leider viel zu selten kontrolliert – soweit es eben die meist klammen Staatskassen zuließen. Stromberg war notorisch überarbeitet, ständig unter Zeitdruck und permanent gefährdet, gefeuert zu werden – eben weil er infolge der Überarbeitung und des Drucks Fehler machte.

Biotech-Toy stellte drei Serien her. Es handelte sich um ein eher kleines Unternehmen. Doch dieses kleine Sortiment war der Renner auf dem Robotermarkt: *Garry*, *Bing* und *Marvin*. Das Modell *Garry* zielte auf Frauen im Alter von 45 bis 60, die beruflich längst etabliert, meist gelangweilt und von der realen Männerwelt angeekelt waren. *Garry* war charmant und auf unaufdringliche Weise eloquent: der perfekte Begleiter für einen angenehmen, folgenlosen Abend. *Bing* hingegen war der sportliche Typ für Frauen um die 30 mitten in ihrer Karriere, die einfach keine Zeit für eine Beziehung hatten, aber auch nicht auf Sex verzichten wollten. Viele von ihnen hatten längst die Erfahrung gemacht, dass viele Männer gern klammern.

Der Star dieses Trios war allerdings *Marvin*! Niemand hätte erwartet, dass dieser Typ den Markt derart stürmisch erobern würde. *Marvin* trug eine schwarze Hornbrille und sah ein wenig aus wie Buddy Holly. Er war der Typ schmachtender Freund. Gedacht für gedemütigte Erstsemester, gekränkte Mädchenseelen im Beziehungsstress. Er baute ihr Selbstbewusstsein wieder auf. *Marvin* signalisierte diesen Mädchen, dass er alles, wirklich alles für sie tun würde, nur für den Hauch eines Lächelns. Er war der Freund, den man ausnutzt. Er konnte zuhören, strahlte aber auch auf eine subtile Weise Intelligenz aus. Er hatte etwas von einem sympathischen Nerd. *Biotech-Toy* hatte ihn zunächst eher als Ergänzungsprodukt angelegt, daher war seine Serie relativ unbeachtet in den Markt eingestiegen. Aber dann: Wumm! Der Markt für *Marvin* explodierte! Die Mädchen kreischten! Plötzlich war er zum John Lennon unter den Robotern avanciert. Der schüchterne, masochistische *Marvin* war ein Star!

Und jetzt stand Stromberg in der Fabrikhalle von *Biotech-Toy*. Dort sah es aus wie eine Mischung aus Schlachthof und Autofabrik. In bläulich schimmernden Bassins wurden die Außenhaut und Fleischimitate gezüchtet, über die Förderbänder (bedient von klassischen Robotern) liefen die Gelenke und Knochen, alles aus Plastik. Kabel verliefen am Boden, Blaumänner standen herum und ein paar Weißkittel.

Für Hersteller humanoider Roboter gilt es, ein möglichst vielfältiges Nutzerpublikum anzusprechen und große Stückzahlen abzusetzen. Im Eifer des Geschäfts verlieren sie dabei bisweilen die Risiken aus dem Auge. Wie gut, wenn es unbestechliche Kontrolleure gibt, die dafür sorgen, dass alles im Rahmen bleibt.

Stromberg hielt seinen Ausweis hoch. „SRK“, rief er in die arbeitende Menge. SRK stand für *staatliche Roboterkontrolle*. Nur ein paar blickten kurz hoch, etwas Gemurmel kam auf.

„Herr Stromberg?“ Er wurde von hinten an der Schulter gefasst, drehte sich um. Vor ihm stand ein dicker Mann, Schweiß im Gesicht. Die Krawatte schien fast am Kinn festgebunden, so wenig Hals hatte er. Stromberg nickte dem schwitzenden Mann zu. Der führte ihn in eine kleine

Halle und dann zum Sezierraum.

„Wir haben ihn schon fast entladen und er liegt bereit“, sagte der Mann, wischte sich mit einem hellgelben Taschentuch Schweiß von der Stirn und grinste schief. „Ich hoffe, Sie finden *Marvin* top“, sagte er. „Wir sind hier alle nämlich furchtbar stolz auf diese Serie.“ Noch ein schräges Lächeln. „Warum überhaupt diese Nachprüfung?“

Stromberg zuckte andeutungsweise mit den Schultern, überlegte sich dann aber eine andere Geste und nickte. Er spürte die Nervosität. Dieser *Marvin* hatte die ganze Firma saniert. *Marvin* war die Firma. „Naja, Sie wissen doch, wie die da oben sind“, sagte Stromberg und blickte kurz zur Decke. „Wenn Sie mich dann allein lassen“, setzte er hinzu. Der Dicke nickte und verließ den Sezierraum.

„WIR SIND HIER ALLE FURCHTBAR STOLZ AUF DIESE SERIE.“

Das Sezieren eines fertigen Roboters mit vorbildgetreuer Haut und Fleischimitat war durchaus eine kleine Sauerei und glich der Arbeit eines Pathologen. Nur war die Anatomie eines Roboters natürlich ganz anders als die eines Menschen. So saß das Gehirn nicht im Kopf, sondern hinter einer Platte im Bauchbereich. Also in etwa dort, wo sich bei den Menschen die Bauchspeicheldrüse befand. Das besondere Problem eines Inspektors war es, versteckte Verschaltungen zu finden. Neu gebildete bionische Ganglien mit Datenkopien vom Hauptprozessor. Und die konnten überall sein. Kleine, oft auch fehlerhafte Updates. In der Kniescheibe. Im Gesäß. Dort im Gesäß verwendete man auch echtes tierisches Fett. Ebenso in den Handflächen, an den Fußsohlen und unterm Kinn. Ein beliebtes Reservoir für zufällige Kopien war auch der Bereich der Augenlider. Es war – wie gesagt

Über den Autor

Der ausgebildete Fachpfleger für Psychiatrie **Bernhard Horwatitsch** arbeitete viele Jahre in einer Münchner Universitätsklinik. 2006 veröffentlichte er den Erzählband „Anleitung zum Scheitern“ (im Wittaverlag) und 2013 den Episodenroman „Das Herz der Dings“ über das Leben mit Demenz (im Mabuse-Verlag). Seit 2005 lehrt der Autor Literaturgeschichte und kreatives Schreiben an der Münchner Volkshochschule, seit 2010 Ethik und Kommunikation an Berufsschulen. Im ersten Jahrzehnt des 21. Jahrhunderts brachte er die Münchner Literaturzeitschrift Klivuskante heraus. Aktuell veröffentlicht Horwatitsch regelmäßig im Grazer Feuilleton-Magazin „Edition Schreibkraft“ und schreibt für das Online-Magazin kkl von Jens Faber-Neuling. Bereits 2017 war er mit seiner dramatischen Virtual-Reality-Dystopie „Die Rose von Sharon“ bei den c't-Stories vertreten.



Bild: Freies Literaturprojekt München

– durchaus eine kleine Sauerei, so einen Roboter zu sezieren. Stromberg zog sich daher einen Plastikanzug über, setzte seine Schutzmaske auf und legte die Latexhandschuhe an. Er öffnete seinen Koffer mit dem Sezierbesteck und depониerte ein paar seiner Messer auf dem Beistelltisch, der eine sterile Unterlage hatte.

Einen Moment lang hielt Stromberg inne. Mit einem Messer in der Hand, den Rücken zu *Marvin*, stand er da, wie eingefroren. Dann fasste er sich wieder. Langsam legte Stromberg sein Messer zurück und drehte sich um. Der Roboter lag nackt auf dem Seziertisch. *Marvins* einzige Bekleidung war seine Hornbrille. Er starrte zur Decke, wobei sein Mund leicht offen stand.

Stromberg hatte seine Entscheidung bereits getroffen. Blitzartig. Er musste jetzt nur noch den nötigen Mut aufbringen. Einige Augenblicke betrachtete er den reglosen Körper, der blass aussah, aber vorbildlich gearbeitet war. Sogar Schamhaare hatte *Marvin*. Wirklich nichts unterschied ihn von einem menschlichen Körper, der nackt und bloß, hilflos auf einem Seziertisch lag. Stromberg zog seinen Plastikanzug wieder aus, räumte die Messer wieder in seinen Koffer, klappte ihn zu. Er überlegte fieberhaft, ging dann zur Tür und öffnete diese vorsichtig. In der kleinen Halle war niemand. Aber an einem Haken hingen ein weißer Kittel und eine Schutzhaube. Stromberg holte beides, zog es *Marvin* an, dann verband er den Roboter mit der Stromversorgung und lud ihn wieder vollständig auf.

Stromberg setzte sich auf den Beistelltisch und wartete. Dabei betrachtete er den Roboter, der leise summt. Strom, Lebensstrom floss in ihn hinein. Nach endlosen zwanzig Minuten regten sich *Marvins* Glieder. Er richtete sich auf, rückte seine Hornbrille auf der Nase zurecht und starrte nun Stromberg an. „Hallo, *Marvin*“, sagte Stromberg. „Hallo“, erwiderte *Marvin* und blickte sich im Raum um. „Weißt du, wie wir hier unbemerkt rauskommen?“, fragte ihn Stromberg. *Marvin* schüttelte unsicher den Kopf.

„Na gut. Wir schaffen das“, sagte Stromberg. „Komm.“ Er nahm ihn bei der Hand und sie schlichen sich in die kleine Halle. Dort gab es eine weitere Tür in einen kleinen Aufenthaltsraum. Und dort war ein Fenster. Stromberg öffnete es und sie kletterten hinaus. *Marvin* zögerte erst ein wenig. Stromberg brauchte ihn aber nur kurz mit den Augen zu fixieren, das half. *Marvin* war auf bedingungslosen Gehorsam eingestellt. Er würde alles tun für ein Lächeln seiner Angebeteten. Er war wie ein Kind: naiv, verliebt und schüchtern.

Tatsächlich schafften die beiden es zu Strombergs Wagen.

MARVIN WAR WIE EIN KIND: NAIV, VERLIEBT UND SCHÜCHTERN.

Stromberg war sich natürlich im Klaren darüber, dass seine Aktion auffliegen würde. Er wusste auch, dass es genau genommen kompletter Unsinn war, was er da veranstaltete. Und gleichzeitig war ihm völlig klar, dass er genau das Richtige, das einzig Richtige getan hatte. Roboterdiebstahl war alles andere als ein Kavaliersdelikt. Noch dazu in seiner Position. Es gab Terrorismus. Umprogrammierte Roboter, die ganze Fabriken lahmlegten, Verkehrschaos auslösten. Für einen talentierten Informatiker war es kein Problem, einen Roboter so umzurüsten, dass er eine U-Bahn steuern konnte. Und zwar so, dass es nicht im Sinne der Fahrgäste war. Stromberg wusste, dass jetzt der staatliche Sicherheitsdienst und die private Security des Unternehmens hinter ihm her waren. Nach Hause konnte er nicht. Sein bisheriges Leben war mit einem Schlag, mit einem Wimpernschlag vorbei.

Stromberg steuerte den Wagen manuell. Alle mit dem Datennetz verbundenen technischen Geräte hatte er abgeschaltet. Aber sie konnten natürlich *Marvin* orten – und hatten das sicher längst getan.

Schließlich fuhr er auf einen Seitenstreifen. „Tut mir leid, *Marvin*“, sagte er. „Aber ich muss das jetzt machen.“ Er holte seinen Sezierkoffer vom Rücksitz und schnitt dem Roboter den Bauch auf.

„Was tust du?“ fragte *Marvin* und rückte seine Hornbrille auf der Nase zurecht. Er war perfekt! Die gedemütigten Erstsemester konnten alles, wirklich alles mit ihm machen! An ihm konnten sie ihr Mütchen kühlen, ihr angeknackstes Selbstvertrauen wieder erneuern, sie konnten ihn schlagen, beleidigen, erniedrigen. Einfach alles.

„Du hast irgendwo da drinnen ein GPS-Modul“, sagte Stromberg.

„Ach so“, sagte *Marvin*.

„Na also. Da ist es ja.“ Es war ein Kinderspiel gewesen. *Biotech-Toy* war eine kleine Firma, die bei der Herstellung sparen musste. Gerade erst entwickelte sich ihr Marktwert, gerade erst schossen ihre Aktien nach oben. Und eben fielen sie auch schon wieder. Solche Zwischenfälle wie Roboterdiebstahl sickerten schnell durch und erreichten die Börse

in Windeseile. Die private Security würde mit Stromberg nicht verhandeln. Das war klar.

Stromberg warf den kleinen Chip, den er *Marvin* entfernt hatte, aus dem Wagenfenster und fuhr weiter. „Ich mache dich wieder zu, wenn wir zu Hause sind“, sagte er.

„Ach, zu Hause“, sagte *Marvin*, lächelte merkwürdig versionen und rückte sich die Hornbrille auf der Nase zu recht.

Die einzige Adresse, die für Stromberg infrage kam, war Deckert. Ihn kannte er noch vom Studium. Einer von den Wilden in der Zeit der Proteste. Einer von den NOROS (no robots). Aber es blieb ihm ja nichts anderes übrig. Bei Deckert konnte man sicher sein, dass niemand wusste, wo er wirklich steckte. Stromberg fuhr auch nur auf Verdacht zu ihm. Aber er hatte tatsächlich Glück.

Der Empfang war allerdings nicht herzlich. Deckert schimpfte wie ein Rohrspatz auf Stromberg ein!

„Was ist das da für ein Monsterspielzeug?“, schrie er Stromberg an. *Marvin* stand da in seinem weißen Kittel, barfüßig, mit offenem Bauch und einer Hornbrille auf der Nase. Es war wirklich eine Freakshow und Stromberg zweifelte sehr an seinem eigenen Verstand.

„Es tut mir leid, Deckert, verstehst du?“

„Nichts! Nichts verstehe ich!“

„Aber er hat *Bewusstsein*.“

Deckert sah den Roboter kritisch an. „Eine Datenmutation?“

„Ich glaube ...“

„Du glaubst?“

„Wo sind wir?“, fragte *Marvin* mit seiner leutseligen Stimme.

„Halt's Maul, du verflückter Schrotthaufen“, schrie ihn Deckert an. *Marvin* lächelte und rückte seine Hornbrille zu recht.

Stromberg schüttelte seinen Kopf.

„Das ist ein Toy-Modell, Deckert. Dein Rumgebrülle mit ihm nutzt nichts, im Gegenteil, er ist sogar darauf programmiert, angebrüllt, beleidigt und erniedrigt zu werden.“

„Na super! Ein Maso-Roboter!“

Stellen Sie sich vor, dass Ihnen bewusst wird, dass das, was Sie Ihr Bewusstsein nennen, gar nicht existiert! Woher kommt dann Ihr Bewusstsein davon, dass Sie gar kein Bewusstsein haben? Es muss Ihnen bewusst sein, dass das, was Sie dann Ihr Bewusstsein nennen, nur ein Bewusstsein Ihres Nicht-Bewusstseins wäre. Sie befinden sich in einer Schleife! Denn wie kann man sich über ein Nicht-Bewusstsein bewusst sein? Sokrates nannte das eine Aporie, die paradoxe Erkenntnis des eigenen Unwissens. Und *Marvin* befand sich in so einer Endlosschleife. Das machte ihn so passiv. *Marvin* konnte sich einfach nicht erklären, dass er eine Erklärung für all das hatte.

★ ★ ★

Tatsächlich! Deckert und Stromberg hatten ganze Arbeit geleistet. Vor ihnen lag ein komplett zerlegter *Marvin*. Sie hatten mehrere fehlerhafte Kopien gefunden. Und – besonders, wirklich besonders – auch eine Schattenkopie im Hauptprozessor. Da *Marvin* so programmiert worden war, dass er Fantasien über Frauen entwickelte, ohne sie ausleben zu

dürfen, hatte es interne Konflikte gegeben. Die Idee des Programmierers von *Marvin* war wirklich genial gewesen. Seine ganze devote Art, seine Lust an der Erniedrigung war regelrecht echt, unterschied sich nicht von einem Jungen, der Probleme hatte mit seiner sexuellen Entwicklung. Gleichzeitig hatte der unbekannte Programmierer von *Marvin* Sperren eingebaut, die wie echte Tabus wirkten. Und das hatte bewirkt, dass *Marvin* sich darüber irgendwie klar geworden war. Nur konnte er damit überhaupt nichts anfangen. Es war für *Marvin* ein kalter Sprung in die Hölle des Bewusstseins. Er litt und lächelte dazu. Das machte ihn so menschlich, dass die Mädchen einfach vor Verrücktheit kreischen mussten!

Deckert und Stromberg saßen vor dem zerlegten *Marvin* und genossen einen Joint.

„Wir können nur noch warten“, sagte Deckert.

Stromberg nickte, nahm einen tiefen Zug und blies den Rauch in Richtung der Einzelteile von *Marvin*.

„Nur warten“, wiederholte der erschöpft wirkende Deckert.

Stromberg wusste, dass Deckert recht hatte. Da die Serie längst auf dem Markt war, würde niemand es mehr zulassen, dass dieses seltsame Geheimnis von *Marvin* öffentlich werden würde. Es war längst klar, dass die Aktionäre das Nötige unternommen hatten, der Markt war wieder stabil und die vielen Mädchen wollten *Marvin*! Alle Macht den Konsumenten!

Es war längst nach Mitternacht. Beide saßen immer noch am gleichen Platz. Eine einfache Kerze beleuchtete den Raum. Es roch ranzig nach alter Butter und ein wenig so, als hätte man gerade einen Motor gestartet. Die Kerze flackerte, Stromberg zog an einer Zigarette, Deckert fuhr sich durchs Haar. Beide schwiegen gerade, waren in ihren eigenen Gedanken versunken, als jemand heftig an die Außentür hämmerte, dann ertönte ein Knall. Es gab einen Luftzug. Die Kerze erlosch.

★ ★ ★

Nach zwei Jahren und einem ziemlichen Presserummel wurde das Produkt *Marvin* vom Markt genommen. Es war zu ein paar ziemlich unschönen Ereignissen gekommen, bei denen das eine oder andere Erstsemester-Mädchen mit dem Leben bezahlte. Die Leichen von Deckert und Stromberg fand man schon bald auf einer Mülldeponie. Die Morde konnten nie aufgeklärt werden und einen Zusammenhang mit *Marvin* vermochte niemand herzustellen. So etwas wie eine künstliche Intelligenz mit eigenem Bewusstsein kann es, wie jeder weiß, nicht geben. (psz@ct.de)

Die c't-Stories als Hörversion

Unter 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).



Qualifizieren Sie Ihre Fachkräfte für die Zukunft der IT

Mit Ihrem Partner für digitale IT-Weiterbildung

**JETZT
KOSTENLOS
TESTEN**

Die Zukunft des Lernens ist digital

Mit dem academy Pass nehmen Ihre IT-Fachkräfte ihre Weiterbildung selbst in die Hand und entscheiden individuell und im eigenen Tempo, wie, was und wo sie lernen möchten.

Stetig wachsendes Kursangebot

Über 150 Videokurse, 80 Webinare und zehn Konferenzen sowie viele Features wie Notizen, Transkript und Übungsaufgaben ermöglichen ein interaktives und nachhaltiges Lernen.

Themen von heute und morgen

Stetig wachsende Kursbibliothek mit berufsrelevanten und praxisnahen Lernangeboten aus den Bereichen Softwareentwicklung, Webtechnologie, IT-Security und vielem mehr.

Weitere Vorteile:

- Einfache Angebotsabwicklung
- Volle Kostenkontrolle durch individuelle Gruppenlizenzen
- Teilnahmebescheinigungen

Jetzt 30-Tage-Test für Ihr Team anfragen:
heise-academy.de/academy-pass





**ICH HACKE
KEIN PROGRAMM.
ICH PROGRAMMIERE
AUF ERFOLG.**

Fernstudium Robotik



Ihre Chance in einem schnell wachsenden Zukunftsmarkt. Aus- und Weiterbildung zum Roboter-Techniker und -Programmierer. Kostengünstiges und praxisgerechtes Studium ohne Vorkenntnisse. Beginn jederzeit.

**NEU: Umweltschutz-Techniker,
Netzwerk-Techniker, SPS-Techniker**

Teststudium ohne Risiko.
GRATIS-Infomappe gleich anfordern!

FERNSCHULE WEBER - seit 1959
Neerstedter Str. 8 - 26197 Großenkneten - Abt. F14
Telefon 0 44 87 / 263 - Telefax 0 44 87 / 264

www.fernschule-weber.de



**ICH WARTE NICHT
AUF UPDATES.
ICH PROGRAMMIERE SIE.**



WERDEN SIE c't-BOTSCHAFTER!

**... UND UNTERSTÜTZEN SIE DAMIT DEN UNABHÄNGIGEN UND
GLAUBWÜRDIGEN JOURNALISMUS!**

Wir schenken Ihnen **30 €** und unsere kultige **c't-Tasse „Kein Backup? Kein Mitleid“**, wenn Sie einen neuen Leser für ein Jahres-Abo der c't werben. Der neue Leser erhält die c't zum Preis von 144,20 € pro Jahr. Das Abo kann in gedruckter oder digitaler Form bezogen werden. Nach einem Jahr ist das Abo monatlich kündbar.



Hier bestellen: ct.de/botschafter

+49 541/80 009 120 ✉ leserservice@heise.de



c't magazin für
computer
technik


**HOCHSCHULE
ESSLINGEN**

Nah an Mensch und Technik.

Wir suchen zum nächstmöglichen
Zeitpunkt eine:n

Professor:in (W2)
für das Lehrgebiet
**„Cloud Security und Security
Analytics“**
(Kennziffer IT-P-2305)

Bewerbungsschluss: 6. Mai 2024

Die vollständige Ausschreibung
finden Sie unter:

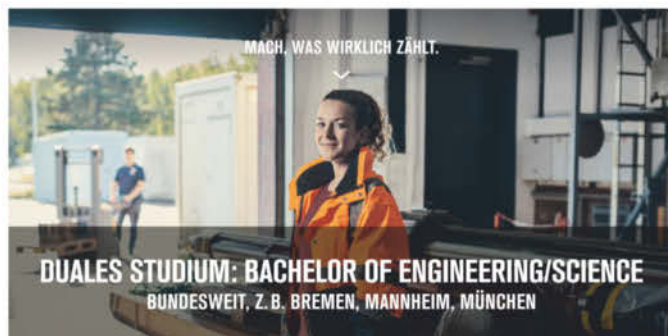
www.hs-esslingen.de/professuren


JOB GESUCHT?

Ein gutes Team braucht viele verschiedene
kluge und kreative Köpfe – und gleichzeitig den
Freiraum, diese Potenziale zu entfalten und
einzusetzen.

Gestalte mit uns die Zukunft der Medienwelt!

Jetzt informieren und
bewerben unter
karriere.heise.de



Mit einem technischen Bachelor-Studium werden Sie optimal auf
Ihre verantwortungsvolle Arbeit im Bereich Wehrtechnik der Bundes-
wehrverwaltung vorbereitet. Dabei haben Sie die Wahl zwischen
bis zu 14 Studiengängen an verschiedenen Kooperationshoch-
schulen. Parallel beginnen Sie Ihre Beamtenlaufbahn.

IHR STUDIUM AUF EINEN BLICK

- Sie durchlaufen als Beamtenanwärter/in neben dem technischen Studium an einer öffentlichen Hochschule eine Laufbahnausbildung in der Bundeswehrverwaltung.
- Sie qualifizieren sich im Rahmen diverser Praktika in den verschiedenen Bereichen der Bundeswehrverwaltung.
- Sie lernen im Bildungszentrum der Bundeswehr in Mannheim die Besonderheiten der Ausrüstung, Informationstechnik und Nutzung der Bundeswehr kennen.
- Sie legen am Ende Ihres Studiums die Laufbahnprüfung für den „gehobenen technischen Dienst – Fachrichtung Wehrtechnik“ ab.

IHRE QUALIFIKATIONEN

- Sie haben mindestens die Fachhochschulreife, die Hochschulreife oder einen hochschulrechtlich als gleichwertig anerkannten Bildungsstand.
- Sie haben zum Zeitpunkt der Verbeamtung das 50. Lebensjahr noch nicht vollendet und besitzen die deutsche Staatsbürgerschaft.

IHRE VORTEILE

- Sie arbeiten bei einem anerkannten Arbeitgeber und erhalten von Beginn an ein attraktives Gehalt.
- Sie werden zu Beginn Ihrer Laufbahnausbildung zum/zur Beamtenanwärter/in ernannt und nach dem Studium sowie einer erfolgreichen dreijährigen Probezeit in den Beamtenstatus auf Lebenszeit übernommen.

STARTEN SIE JETZT IHRE KARRIERE

Mehr Informationen erhalten Sie auf
bundeswehrkarriere.de.

HABEN SIE FRAGEN?

Herr Ernst (02203 105 2712)

Bundesamt für das Personalmanagement der Bundeswehr
Assessmentcenter für Führungskräfte, Referat 1 – Anwärter gTD
E-Mail: ac-bewerbung-anwaerter@bundeswehr.org

Schwerbehinderte Menschen werden bei gleicher Qualifikation und Eignung bevorzugt
eingestellt. Bewerbungen von Frauen sind ausdrücklich erwünscht. Die Bundeswehr
begrüßt Bewerbungen von Menschen mit Migrationshintergrund.

ZIVILISTIN.DE
Karriere geht auch ohne Uniform.
Jetzt informieren und bewerben!

oder 0800 9800880
(bundesweit kostenfrei)


BUNDESWEHR

Inserenten*

1&1 Telecom GmbH, Montabaur.....	9
1blu AG, Berlin.....	23
AVM Computersysteme Vertriebs GmbH, Berlin.....	180
Cordaware GmbH, Pfaffenhofen.....	11
Fernschule Weber, Großenkneten.....	173
Kentix GmbH, Idar-Oberstein.....	77
mitp Verlags GmbH & Co. KG, Frechen.....	39
Philips GmbH, Hamburg.....	2
sysGen GmbH, Bremen.....	49
Thomas Krenn.com, Freyung.....	25
WIBU-SYSTEMS AG, Karlsruhe.....	37
Wiesemann & Theis GmbH, Wuppertal.....	81
WORTMANN AG, Hüllhorst.....	4, 5

Stellenanzeigen

Bundesamt für Personalmanagement der Bundeswehr, Köln.....	175
Hochschule Esslingen, Esslingen.....	173

Veranstaltungen

c't workshops	c't, heise Events	35
betterCode	iX, dpunkt.verlag	43
S2N	heise Medien	51
Mastering Kubernetes	heise Academy	75
heise academy	heise Academy	76, 172
heise security tour 2024	heise security	133
Mastering Observability	iX, dpunkt.verlag	155
Webinar Apple Vision Pro	Mac & i	159
Continuous Lifecycle/ ContainerConf	iX, dpunkt.verlag	165
enterJS	iX, dpunkt.verlag	176

Ein Teil dieser Ausgabe enthält Beilagen der
Heise Medien GmbH & Co. KG.

* Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.



Die Konferenz für Enterprise-JavaScript

Mainz • 7. – 8. Mai 2024

Workshops am 6. Mai • Barrierefreiheit • React • Angular

Jetzt
Tickets
sichern!

enterjs.de

Veranstalter



MAGAZIN FÜR
PROFESSIONELLE IT



dpunkt.verlag

Silbersponsoren





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: „Edel-Smartphones mit KI im Test“:
Robin Brand (rbr@ct.de), „Loslegen mit Proxmox: Ein Server, viele Rechner“:
Niklas Dierking (ndi@ct.de)

Chefredakteure: Torsten Beeck (tbe@ct.de) (verantwortlich für den Textteil),
Dr. Volker Zota (vza@heise.de)

Stellv. Chefredakteure: Martin Fischer (mfi@heise.de), Axel Kossel (ad@ct.de),
Jan Mahn (jam@ct.de)

Chef vom Dienst: Georg Schnurer (gs@ct.de)

Chefin vom Dienst New Media: Hannah Monderkamp (mond@heise.de)

Koordination Leserkommunikation: Martin Triadan (mat@ct.de)

Leiter redaktionelle Entwicklung: Jobst Kehrnhahn (keh@ct.de)

Ressort Internet, Datenschutz & Anwendungen

Leitende Redakteure: Hartmut Gieselmann (hag@ct.de), Jo Bager (jo@ct.de)

Redaktion: Holger Bleich (hob@ct.de), Anke Brandt (abr@ct.de), Greta Friedrich (gref@ct.de),
Tim Gerber (rig@ct.de), Arne Grävmeyer (agr@ct.de), Markus Montz (mon@ct.de),
Peter Schmitz (psz@ct.de), Sylvester Tremmel (syt@ct.de), Andrea Trinkwalder (atr@ct.de),
Dorothee Wiegand (dwi@ct.de), Stefan Wischner (swi@ct.de)

Ressort Systeme & Sicherheit

Leitender Redakteur: Peter Siering (ps@ct.de)

Redaktion: Niklas Dierking (ndi@ct.de), Mirko Dölle (mid@ct.de), Wilhelm Drehling (wid@ct.de), Liane M. Dubowy (lmd@ct.de), Ronald Eikenberg (rei@ct.de), Oliver Lau (ola@ct.de), Pina Merkert (pmk@ct.de), Dennis Schirmacher (des@ct.de), Hajo Schulz (hos@ct.de), Jan Schüßler (jss@ct.de), Kathrin Stoll (kst@ct.de), Keywan Tonekaboni (ktm@ct.de), Axel Vahldiek (axv@ct.de)

Ressort Hardware

Leitende Redakteure: Christof Windeck (ciw@ct.de), Ulrike Kuhlmann (uk@ct.de),
Dušan Živadinović (dz@ct.de)

Redaktion: Ernst Ahlers (ea@ct.de), Christian Hirsch (chh@ct.de), Benjamin Kraft (bkr@ct.de),
Lutz Labs (ll@ct.de), Andrijan Möcker (amo@ct.de), Florian Müssig (mue@ct.de), Rudolf Opitz (rop@ct.de), Carsten Spille (csp@ct.de)

Ressort Mobiles, Entertainment & Gadgets

Leitende Redakteure: Jörg Wirtgen (jow@ct.de), Christian Wölbert (cwo@ct.de)

Redaktion: Robin Brand (rbr@ct.de), Sven Hansen (sha@ct.de), Steffen Herget (sht@ct.de),
Nico Jurrán (nij@ct.de), André Kramer (akr@ct.de), Michael Link (mil@ct.de), Urs Mansmann (uma@ct.de), Stefan Porteck (spo@ct.de)

Leiter c't 3003: Jan-Keno Janssen (jkj@ct.de)

Redaktion: Lukas Rumpler (rum@ct.de)

c't Sonderhefte

Leitung: Jobst Kehrnhahn (keh@ct.de)

Koordination: Pia Groß (piac@ct.de), Angela Meyer (anm@ct.de)

c't online: Sylvester Tremmel (syt@ct.de), Niklas Dierking (ndi@ct.de)

Social Media: Jil Martha Baae (jmb@ct.de)

Koordination News-Teil: Hartmut Gieselmann (hag@ct.de), Kathrin Stoll (kst@ct.de),
Christian Wölbert (cwo@ct.de)

Koordination Heftproduktion: Martin Triadan (mat@ct.de)

Redaktionsassistentz: Susanne Cölle (suc@ct.de)

Software-Entwicklung: Kai Wasserbäch (kaw@ct.de)

Technische Assistentz: Ralf Schneider (Lt看., rs@ct.de), Christoph Hoppe (cho@ct.de),
Stefan Labusga (sla@ct.de), Arne Mertins (ame@ct.de), Jens Nohl (jno@ct.de),
Daniel Ladeira Rodrigues (dro@ct.de)

Dokumentation: Thomas Masur (tm@ct.de)

Verlagsbüro München: Hans-Pinsel-Str. 10b, 85540 Haar, Tel.: 0 89/4271 86-0,
Fax: 0 89/4271 86-10

Ständige Mitarbeiter: Detlef Borchers, Herbert Braun (heb@ct.de), Tobias Engler,
Monika Ermert, Stefan Krempf, Ben Schwan (bsc@ct.de), Christiane Schulzki-Haddouti

DTP-Produktion: Mike Bunjes, Birgit Graff, Angela Hilberg, Jessica Nachtigall, Astrid Seifert,
Ulrike Weis

Junior Art Director: Martina Bruns

Fotografie: Melissa Ramson, Andreas Wodrich

Digitale Produktion: Melanie Becker, Kevin Harte, Martin Kreft, Thomas Kaltschmidt,
Pascal Wissner

Illustrationen

Rudolf A. Blaha, Frankfurt am Main, Thorsten Hübner, Berlin, Albert Hulm, Berlin, Sven Hauth,
Schülp, Timo Lenzen, Berlin, Andreas Martini, Wettin, Moritz Reichartz, Viersen, Michael Vogt,
Berlin

Editorial: Hans-Jürgen „Mash“ Marhenke, Hannover, Schlagseite: Ritsch & Renn, Wien,
c't-Logo: Gerold Kalter, Rheine

c't-Krypto-Kampagne: Infos zur Krypto-Kampagne unter <https://ct.de/pgp>. Die Authentizität
unserer Zertifizierungsschlüssel lässt sich mit den nachstehenden Fingerprints überprüfen:

Key-ID: 5C1C1DC58EEDD33A
ct magazine CERTIFICATE <pgpCA@heise.de>
D337 FCC6 7EB9 09EA D1FC 8065 5C1C 1DC5 BEED D33A
Key-ID: 2BAE3CF6DAFFB000
ct magazine CERTIFICATE <pgpCA@ct.heise.de>
A3B5 24C2 01A0 D0F2 355E 5D1F 2BAE 3CF6 DAFF B000
Key-ID: DBD245FCB3B2A12C
ct magazine CERTIFICATE <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: ayznmonmewb2tjvgf7ym4t2726muprjvwckxzvhf2hbarbbzydm7oad.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

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167) (verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 41 vom 1. Januar 2024.

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
Tel: +886-2-2882-5577, Fax: +886-2-2882-6000, E-Mail: mei@mediagate.com.tw

Leiter Vertrieb und Marketing: André Lux (-299)

Werbeleitung: Julia Conrades (-156)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL, appl druck, Senefelderstr. 3-11, 86650 Wemding

Kundenkonto in der Schweiz: PostFinance, Bern, Kto.-Nr. 60-486910-4,
BIC: POFICHBEXXX, IBAN: CH73 0900 0000 6048 6910 4

Vertrieb Einzelverkauf:

DMV Der Medienvertrieb GmbH & Co. KG

Meßberg 1

20086 Hamburg

Tel.: 040/3019 1800, Fax: 040/3019 1815

E-Mail: info@dermedienvertrieb.de

c't erscheint 14-täglich

Einzelpreis 5,90 €; Österreich 6,50 €; Schweiz 9,90 CHF; Belgien, Luxemburg 6,90 €;

Niederlande 7,20 €; Italien, Spanien 7,40 €, Dänemark 64,00 DKK

Abonnement-Preise: Das Jahresabonnement kostet inkl. Versandkosten: Inland 144,20 €,

Österreich 155,40 €, Europa 165,20 €, restl. Ausland 191,80 € (Schweiz 236.60 CHF);

ermäßigtes Abonnement für Schüler, Studenten, Auszubildende (nur gegen Vorlage einer

entsprechenden Bescheinigung): Inland 105,00 €, Österreich 99,40 €, Europa 124,60 €,

restl. Ausland 152,60 € (Schweiz 145.60 CHF). c't-Plus-Abonnements (inkl. Zugriff auf das

c't-Artikel-Archiv sowie die App für Android und iOS) kosten pro Jahr 25,00 € (Schweiz 30.80

CHF) Aufpreis. Ermäßigtes Abonnement für Mitglieder von AUGÉ, bdvB e.V., BvDW e.V.,

/ch/open, GI, GUUG, ISACA Germany Chapter e.V., JUG Switzerland, VBIO, VDE und VDI

(gegen Mitgliedsausweis): Inland 108,15 €, Österreich 116,55 €, Europa 123,90 €,

restl. Ausland 143,85 € (Schweiz 177.45 CHF). Luftpost auf Anfrage.

Leserservice:

Bestellungen, Adressänderungen, Lieferprobleme usw.

Heise Medien GmbH & Co. KG

Leserservice

Postfach 24 69

49014 Osnabrück

E-Mail: leserservice@ct.de

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) oder

E-Mail (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 Verfügungsrecht 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. Printed in Germany. Alle Rechte vorbehalten.

Gedruckt auf chlorfreiem Papier.

© Copyright 2024 by Heise Medien GmbH & Co. KG

ISSN 0724-8679 AWA LAE 

Vorschau **ct** 10/2024

Ab 3. Mai im Handel und auf ct.de



Flott unterwegs im eigenen Netz

Aktuelle WLAN-Standards versprechen Multi-Gigabit-Geschwindigkeiten. Doch garantiert rasante Datenraten gibts nur per Kabel. Wir verraten, wie Sie eine zukunftssichere Twisted-Pair-Installation planen, die auch WLAN-Accesspoints und -Repeater berücksichtigt, und erklären die Grundlagen verwalteter Switches.



Schnelle USB-SSDs und Sticks

Backup nervt, ist aber notwendig. Und je schneller es durch ist, desto besser. Viele USB-SSDs schaffen Datenraten von 1 oder sogar 2 GByte/s, die passenden Schnittstellen sind an den meisten Rechnern mittlerweile vorhanden. Wir testen zehn schnelle USB-Speicher mit 1 und 2 TByte Speicherplatz.

Der c't-Solar-Guide 2024

Noch nie war der Einstieg in die eigene Energieversorgung mit Solar-Modulen so günstig: Egal ob kleines Balkonkraftwerk oder große Dachanlage, wir zeigen, was geht, welche Förderungen und Regulierungen es gibt und wann sich eine PV-Anlage rentiert.

Internet-Bezahlmethoden im Vergleich

Rechnung, PayPal, Giropay, Kreditkarte – wer im Onlineshop bezahlen will, hat oft die Qual der Wahl. Komfortabel sind fast alle Bezahlarten, aber welche Unterstützung bekommen Kunden bei Betrug und anderen Problemen und wer schneidet welche Daten mit? Unser Marktüberblick hilft bei der Auswahl.

Mobile Kraftpakete

In unserer Kaufberatung für Mobilprozessoren erfahren Sie, welche CPU für Notebooks und Mini-PCs am besten zu Ihrem Anwendungsprofil passt. Unter anderem vergleichen wir die aktuellen Modelle von AMD, Apple, Intel und Qualcomm.

Neue Preise ab c't 10/2024

Ab Heft 10/2024 erhöht sich der Preis für eine c't-Ausgabe in Deutschland von 5,90 Euro auf 6,20 Euro. Das Print-Abonnement und das Jahres-Abo Digital (PDF zum Download, mobiles Lesen mit App oder im Browser) kosten dann 152,60 Euro. Schüler, Studenten und Auszubildende erhalten gegen Vorlage einer Bescheinigung ein ermäßigtes Abo für 105 Euro (als Digital-Abo für 86,80 Euro). Das Plus-Abo enthält für 177,80 Euro außer Print- und Digital-Abo Zugriff auf das gesamte Artikel-Archiv von c't. Preise in anderen Ländern und weitere Ermäßigungen finden Sie im Impressum der c't 10/2024.

Noch mehr Heise-Know-how



Mac & i 2/2024 jetzt im Handel und auf heise-shop.de



c't Home & Office jetzt im Handel und auf heise-shop.de



FREITAG IST C'T-TAG!*

**30%
Rabatt!**

Jetzt 5x c't lesen

für 23,25 €
statt 30,25 €**

** im Vergleich zum Standard-Abo



*Endlich Wochenende! Endlich genug Zeit, um in der c't zu stöbern. Entdecken Sie bei uns die neuesten Technik-Innovationen, finden Sie passende Hard- und Software und erweitern Sie Ihr nerdiges Fachwissen. **Testen Sie doch mal unser Angebot: Lesen Sie 5 Ausgaben c't mit 30 % Rabatt – als Heft, digital in der App, im Browser oder als PDF. On top gibt's noch ein Geschenk Ihrer Wahl.**

Jetzt bestellen:

ct.de/meintag





GLASFASER UND FRITZ!

**EIN HERZ UND
EINE SEELE**

avm.de/dreamteam

