c't magazin für computer technik
18.11.2023 27
Europas größtes IT- und Tech-Magazin

Gute Luft:
CO_2-Schnüffler
im Test

Hacker-Projekte mit Raspi

Hacken lernen • Lücken finden • Angreifern zuvorkommen
Passwortklau, WLAN-Hacks, USB-Angriffe, Portscanning

TEST

Mini-PC mit Ultraschallkühlung
Telekom-Tablet mit 5G und Dual-SIM
Grafikkarten: Radeon Pro W7500 und W7600
AV-Receiver mit Dolby Atmos
Google Pixel Watch 2

Gesund & fit mit Ernährungs-Apps

Kalorien, Makro- und Mikronährstoffe im Blick

FOKUS

Neuer Whistleblower-Schutz in der Praxis
Facebook: Geld oder Daten!
Eintastenkürzel für Microsoft Teams
Matter: Marktübersicht und Smart-Home-Tipps
Authenticator für 2FA selbst betreiben

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

NAS-Aufrüstung: Aus alt mach schnell

Mehr Speed durch RAM, SSD-Cache, flotte Platten und Netzwerktuning
NAS-zu-NAS-Backup • Die besten Umbaustrategien

4 199148 405900 27

exone®
IT für Unternehmen

Microsoft

Mit Sicherheit weiße Weihnachten

Mit Windows 11 – das sicherste Windows

exone Business Slim X12

- **Intel® Core™ i5-12400**
- **8 GB DDR4 PC3200**
- **500 GB SSD M.2 PCIe®3.0x4 NVMe®**
- **Windows 11 Pro**

Windows 11 Pro

intel. CORE i5

Weitere Informationen finden Sie hier!

EXTRA COMPUTER GMBH

Kryptoschmu

Banken kann man nicht trauen, gerade die kleinen Leute werden von ihnen immer wieder übervorteilt. Die Lösung ist – wissen Sie es noch? Genau: Blockchains, Kryptowährungen, "DeFi", das dezentrale Finanzwesen. Unter dem Eindruck der Finanzkrise 2007/2008 war das ein mächtiges Narrativ. Nun liegt es mir fern, Banken menschenfreundliche Motive zu unterstellen, aber die Nonchalance und Hemmungslosigkeit, mit der die Kryptobörse FTX Kundengelder veruntreut hat, sucht ihresgleichen (siehe Seite 41). Und dabei war FTX auch noch bekannt (und in Teilen der Kryptowelt verrufen) dafür, sich für striktere Regulierung einzusetzen. Hauptkonkurrent und aktuelles Schwergewicht Binance hat berühmt-berüchtigterweise nicht einmal einen erklärten Firmensitz.

Nun betonen Krypto-Fans oft, dass es sich dabei eben um zentralisierte Börsen handelt, der Witz an Bitcoin & Co. sei ja gerade, dass man damit auch dezentrale Börsen, Handelsunternehmen et cetera konstruieren könne. Das stimmt und solche Plattformen gibt es. Aber erstens lässt sich über die tatsächliche (De)zentralisierung von Bitcoin, Ethereum und so weiter trefflich streiten. Zweitens sind auch dezentrale Institutionen so sehr von dramatischen Fehlern geplagt und mit Betrügereien durchsetzt, dass man mit hohem Risiko sein Geld verliert – und ohne Molly Whites web3isgoinggreat.com auch rettungslos den Überblick in all der Täuschung und Inkompetenz verlöre. Und drittens kommt das Krypto-Universum nicht ohne zentralisierte Institutionen wie FTX, Binance oder Tether aus: Sie stellen den relevanten Zugang für Fiatgeld (also Dollar, Euro etc.) dar. Denn wie sonst sollen die von den Banken malträtierten kleinen Leute an den schönen Kryptosystemen teilhaben? Die Zeiten, als sie sinnvoll Bitcoin oder Ether am heimischen Computer minen konnten, sind lange vorbei.

Dank Implosionen wie der von Terra/Luna, Celsius und zuletzt FTX ist der Lack jedenfalls ab von der Krypto-Welt. "TradFi", also das herkömmliche Finanzwesen, wirkt dagegen gar nicht mehr so schäbig – und das muss man mit Firmen wie Wirecard erst mal schaffen. Kleine Leute, die Banken misstrauen, sollten vor jeder Kryptounternehmung jedenfalls schreiend weglaufen.

Sylvester Tremmel

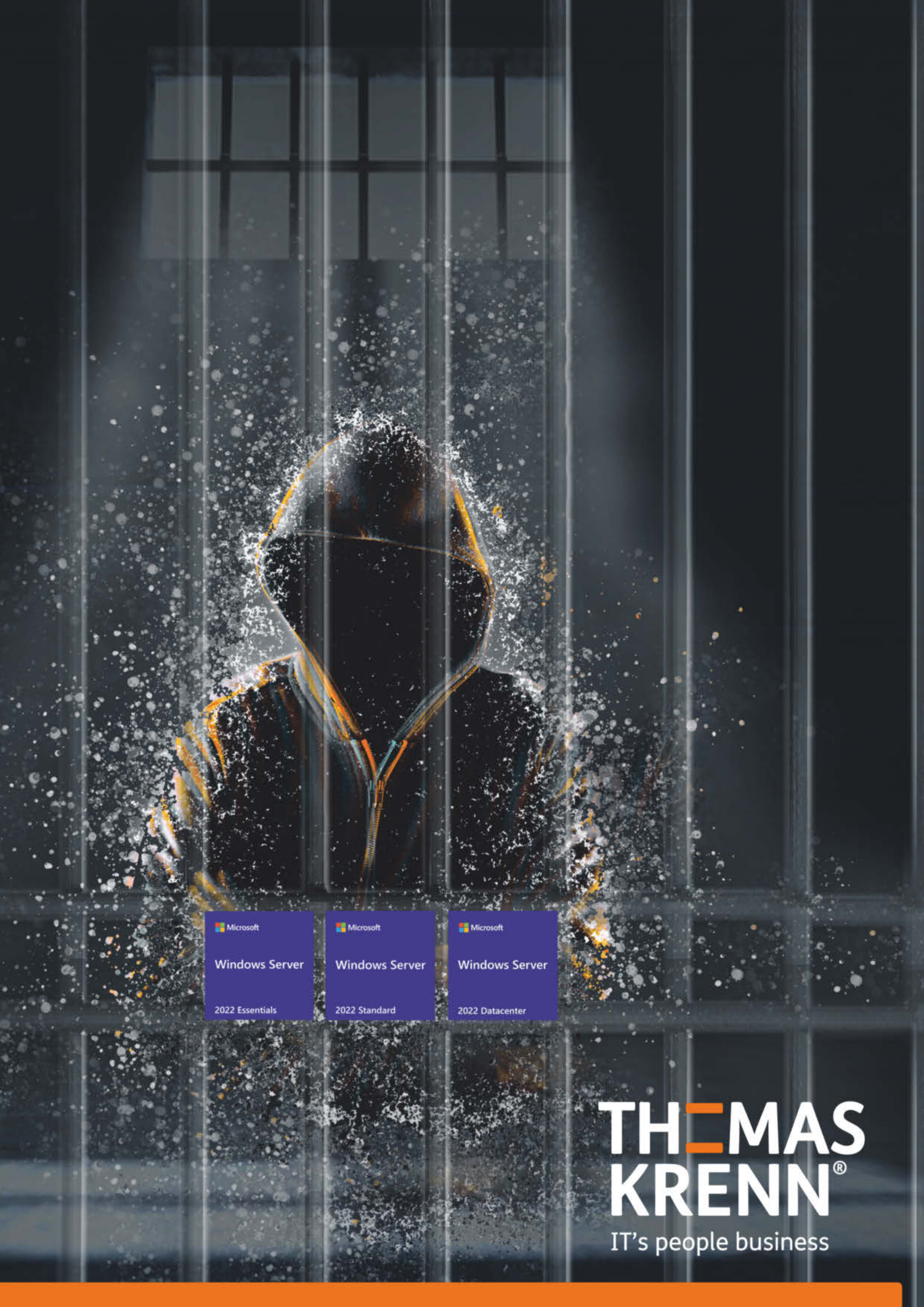
Hacker müssen draußen bleiben!

Windows Server 2022

Kein Platz für Sicherheitslücken und Cyber-Angriffe

Nach dem Support-Ende für Windows Server 2012/R2 diesen Jahres am 10. Oktober entstehen täglich neue Sicherheitslücken – und Hacker nutzen das gnadenlos aus. Der Wechsel zu Windows Server 2022 schließt diese Einfallstore durch regelmäßige Updates und umfassende Security-Features. Riskieren Sie nicht die Integrität Ihrer IT und schützen Sie sich vor den gravierenden Konsequenzen eines erfolgreichen Cyber-Angriffs. Sichern Sie sich noch heute Ihre Lizenz für Windows Server 2022 – und genießen Sie den Schutz eines modernen Server-Betriebssystems.

ACHTUNG
Jetzt absichern:
thomas-krenn.com/ws2022
+49 (0) 8551.9150-300


Microsoft
Windows Server
2022 Essentials
Microsoft
Windows Server
2022 Standard
Microsoft
Windows Server
2022 Datacenter
THOMAS KRENN®
IT's people business

Inhalt c't 27/2023

Titelthemen

Aktuell

Test & Beratung

Wissen

Praxis

Immer in c't

54 NAS-Aufrüstung: Aus alt mach schnell

Je älter ein Netzwerkspeicher wird, desto mehr Aufgaben bekommt er und desto mehr schnauft er. Viele lassen sich aber mit mehr RAM, besseren Platten oder schnellerem Ethernet päppeln. Wir stellen die Umbaustrategien vor.

Frisch aus c't Nerdistan

c't Hardcore

Leserforum

Zur Überwachung am Arbeitsplatz merken Admins unter unseren Lesern an, dass dafür auch Software nutzbar sei, die eigentlich anderen Zwecken dient.

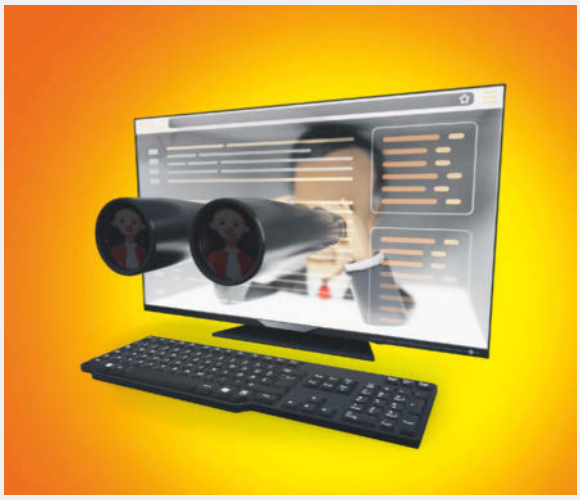


Bild: Moritz Reichartz

Überwachung als Abfallprodukt

Wie Überwachungsprogramme Mitarbeiter minutiös ausspionieren, c't 25/2023, S. 18

Fast immer können positiv gemeinte Vorgänge auch negativ genutzt werden. Wenn eine Software permanent das aktive Nutzerverhalten protokolliert, ist die ursächliche Verwendung durchaus klar. Wenn man das aber macht, um Abstürzen auf den Grund zu gehen, weiß das der Kollege auch und es wird nur über einen definierten Zeitraum aktiv gemacht.

Es fehlen Gesichtspunkte wie Power Automate oder Ui Path und sicher ähnliche Automatisierungsmechanismen. Wenn jemand einen Antrag über MS Forms stellt, erfolgt ein neuer Eintrag auf einer bestimmten Sharepoint-Seite. Ich erhalte ohne Wissen des Antragsstellers automatisch eine Benachrichtigung über den Eingang des Antrags. Ich sehe auch den Arbeitsstil des Antragstellers. Nämlich wenn ich zahlreiche E-Mails erhalte, weil der Antragsteller immer wieder Änderungen an seinem Antrag vornimmt oder nach jedem Feld zwischenspeichert. Ich muss das nicht wissen, es fällt als Abfallprodukt automatisch an.

Andere Software (gängig ist hier SAP zu nennen), protokolliert seit Jahren annähernd jeden Mausklick mit Datum, Uhrzeit und Nutzernamen. Es ist besonders im Fehlerfall sehr nützlich, den Vorgang anschauen zu können und auch Ansprechpartner zu finden und teils unbewusst nebeneinanderher agierende Kollegen am selben Objekt ins Gespräch zu bringen. Aber ich sehe auch, mit welchen unzulässigen Eingriffen Daten im Nachhinein manipuliert wurden, wann und durch wen. Wenn man weiß, wie die Workflows funktionieren, ist das leicht zu erkennen.

Name der Redaktion bekannt

Super Timing

Aus für das Gratisupgrade von Windows 7 auf 10 und 11, c't 25/2023, S. 16

Danke Microsoft, super Timing. Genau jetzt vor Black Friday, Weihnachten und jährlichem c't-Bauvorschlag, also genügend Anlässen, um mal wieder an der Hardware rumzuschrauben. Denn wenn man die falschen oder zu viele Komponenten ändert, dann darf man den Lizenzkey neu eingeben. Der wird aber jetzt nicht mehr akzeptiert, wenn man den „falschen" Upgradepfad benutzt hat.

DerGo

Nobara ausprobieren

Zwei Linux-Distributionen für Gamer vorgestellt, c't 25/2023, S. 66

Ich besitze ein Surface Book und fand die native Unterstützung für Surface-Geräte von Nobara sehr interessant. Gibt es eine Möglichkeit, Nobara mal als Live-Linux ohne Installation zu testen?

Johannes Jungmann

Der Installationsstick, den Sie mittels der ISO-Datei von der Entwicklerseite erstellen können, funktioniert auch als Livesystem. Mit dem können Sie problemlos Nobara erst ausprobieren, ehe Sie sich entscheiden, es zu installieren. Sie können es auch auf einem externen Datenträger (USB-SSD) oder einer microSD-Karte einrichten, falls die interne SSD zu klein ist oder Sie sie nicht partitionieren wollen.

Besseres Tool für Apple

Keylogger macht sich Apples Ortungsnetz zunutze , c't 25/2023, S. 80

Der erwähnte BLE Scanner taugt nicht. Der findet nichts, weder meine Fitbit Versa Lite noch meine Maginon Smart Tags. Ich nutze LightBlue, das wenigstens alle meine eigenen Geräte auf dem iPhone findet. Es reicht IMHO, irgendwo in die Pampa zu gehen und zu schauen, welche Geräte um einen herum aktiv sind. Damit kann man feststellen, ob Tracker darunter sind.

Thorsten Maverick

Keine Extravaganzen, bitte

Linux-Distribution Ubuntu 23.10 im Test, c't 25/2023, S. 102

Vor vielen Jahren bin ich vom doch etwas altbackenen Debian auf das viel modernere Kubuntu umgezogen und habe es nie bereut. Jetzt aber ärgere ich mich zunehmend über diesen immer stärker werdenden Zwang zu Snap. Ich fürchte, die 24.04

Wir freuen uns über Post

redaktion@ct.de

c't Forum

c't Magazin

@ctmagazin

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

Anonyme Hinweise
https://heise.de/investigativ

Alpha Astro

Ein kleiner Schritt ...

Collapse all

Apollo11@Florida
ruft an ...

Alpha Astro

Hä?! Ihr ruft von Zuhause aus an????
Seid ihr ohne mich zurückgeflogen? 😱

zoom X
powered by T

Bekannte Nummer.
Egal, von wo der Anruf kommt.

Digitale Zusammenarbeit mit Zoom X powered by Telekom.
Mit Festnetz-Integration für optimale Erreichbarkeit.
Virtuelle Meetings. Team Chats. VoIP Telefonanlage u .v. m.
Jetzt 30 Tage kostenfrei testen! telekom.de/zoom-x

wird das dann auch an jeder Ecke haben. Ich bin ein alter Mann und möchte deshalb ein Debian-nahes Ubuntu mit einem gut integrierten KDE-Desktop und nicht diese Extravaganzen.

anutosho1

6Armband juckt

Whoop: Fitnessarmband mit OpenAI-Coach im Test, c't 25/2023, S. 112

Nach sieben Monaten recht guter Erfahrungen mit dem Whoop 2 bekam ich schlagartig eine nässende und juckende Hautirritation an der Stelle, an der der Sensor am Arm aufliegt – trotz täglicher Reinigung von Sensor und Haut. Einen Warnhinweis konnte ich seitens Whoop nicht finden. Stattdessen wird das kontinuierliche Tragen 24/7 ausdrücklich empfohlen, um lückenlos Daten zu sammeln.

Auf meine mehrfache Anfrage bei Whoop erhielt ich bis heute, Wochen nach dem Vorfall, keine Antwort. Meine Antwort war, den Vertrag zu kündigen. Aber mit der Irritation habe ich auch heute noch zu tun. Mit anderen Smartwatches und Sensoren hatte ich keine derartigen Probleme.

Ein weiterer Nachteil dieses Sensors sind die Bänder. Selbst die neuen angeblich sehr schnell trocknenden Bänder bleiben so nass nach Training und Duschen, dass sie jedes Hemd von innen her durchnässen, was sehr unschön ist. Metallbänder wie bei anderen Anbietern sind hier praktisch direkt trocken.

Wolfgang Schäfer

Privacy-first-Protokolle

Chatkontrolle: Lobby bestellt – EU-Kommission will liefern, c't 24/2023, S. 14

Zum Glück sind diverse Lösungen wie Threema, Signal und Matrix ja relativ quelloffen und können entgegen beschlossenem Recht unter eigener Administration mit etwas Security-Know-how nicht personenbezogen im Internet betrieben werden. Wenn es wirklich zur Chatkontrolle kommt, werden die Selfhosting-Lösungen nur so aus dem Boden sprießen.

Kinder werden sich wohl eher nicht auf dieser Ebene im Internet bewegen. Das Ziel der Verhinderung des Groomings wäre dann ja fast erreicht, auch ohne jedes existente Chatprotokoll zu überwachen.

GottZ

Fragen zu Artikeln

Mail-Adresse des Redakteurs am Ende des Artikels

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

Zertifikatsspeicher auf dem ePerso

Wie Sie mit den Mängeln von E-Mail umgehen können, c't 24/2023, S. 22

Sie schreiben: „Der gut gemeinte Zertifikatsspeicher auf dem ePerso wurde von kaum einen Bürger befüllt, weil dafür ein teurer Kartenleser nötig war." Für mich war der Grund, dass ich meinen privaten Schlüssel mit dem Staat teilen müsste. Der Staat darf gerne meinen Certificate Signing Request erhalten, aber wenn er meinen privaten Schlüssel will, ist das für mich keine ernstzunehmende Verschlüsselung.

iMil

Export ist wichtig

Fünf offlinetaugliche Musikverwaltungen im Test, c't 24/2023, S. 106

In dem Test kommt der Export ein wenig zu kurz. Ich habe viele Musikvideos von YouTube geladen, die ich gern samt Playlist als Audio auf einen USB-Speicher exportieren möchte. Es gibt für macOS diverse Programme, die das können und dafür auch auf die Apple-Music/iTunes-Bibliothek zurückgreifen. Das wurde interessant, weil unser BMW leider keinen CD-Spieler mehr hat und sein Medienspieler keine Alben in Ordnern erkennt. Jedes Album braucht eine eigene Playlist.

Thorsten Maverick

Wenig Sachverstand

Hackback: Was soll der Staat dürfen?, c't 24/2023, S. 152

Einmal mehr zeigt sich, dass die Hackback-Protagonisten technisch wenig Sachverstand besitzen und basierend auf klassischen militärischen Vorgehensweisen argumentieren.

Zur Zuständigkeit des BKA: Anstatt mal ins Blaue hinein umfangreiche Gesetzesänderungen auf den Weg zu bringen, wäre es vielleicht überlegenswert, das BKA lediglich als helfende Kompetenzstelle zu etablieren, welche die jeweiligen Länderdienststellen bei notwendig erscheinender Gefahrenabwehr unterstützt. Je nachdem, wie das in der Praxis läuft, kann man dann schnell mit allen Betroffenen an einem Tisch sitzen und eine endgültige Lösung ausarbeiten, mit den ganzen Gesetzesänderungen, die das nach sich zieht.

Patrik Schindler

Ergänzungen & Berichtigungen

Falsche Seitenzahl

Inhaltsverzeichnis, c't 25/2023, S. 6

Der „**Vergleichstest** Vier Ryzen-Notebooks ab 900 Euro" steht auf Seite 114 und nicht auf Seite 78, wie im Inhaltsverzeichnis irrtümlich angegeben.

Raspi 5 kann H.265

Raspberry Pi 5: erste Erfahrungen, Messwerte und Zubehör, c't 24/2023, S. 72

Anders als behauptet hat der BCM2712-Chip des Raspberry Pi 5 einen Hardwaredecoder für das Videokompressionsformat H.265 (HEVC). Onlinevideos kommen allerdings häufiger in den Formaten H.264 (MP4/AVC1), VP9 und AV1, für die der BCM2712 keine Hardwaredecoder hat. Laut den Raspi-Entwicklern spielt der Raspi 5 MP4-Videos in Full-HD-Auflösung je nach Bildrate mit 10 bis 60 Prozent CPU-Last ab.

Beim unter Raspberry Pi OS vorinstallierten Browser Firefox lässt sich YouTube zur Auslieferung von MP4-Videos überreden, wenn man in about:config die Option `media.webm.enabled` auf `false` setzt.

Des Rätsels Lösung

40 Jahre c't: Wir verlosen ein Apple iPad Pro 2022, c't 25/2023, S. 60

Für das erste gesuchte Wort im Alien-Chinesisch-Rätsel hatten wir `GLEITKOMMA-OPERATIONEN` nicht als richtig zugelassen. Für das zweite Wort galt auch `RECHENTECHNIK` als richtig.

Brilliant simplicity

#software #development #ecosystem #evolution
#digital #b2b #products #ecommerce #checkout

yatta.de

Yatta

WIR TEILEN KEIN HALBWISSEN
WIR SCHAFFEN FACHWISSEN

Einführung in GitLab

Der Workshop bietet einen Einstieg in den Betrieb einer eigenen Gitlab-Instanz. Sie lernen GitLab initial aufzusetzen, sowie Ihre Instanz zu konfigurieren und an eigene Anforderungen anzupassen.

Docker und Container in der Praxis

Der Workshop für Entwickler und Administrierende behandelt neben theoretischem Wissen über Container auch Herausforderungen im Alltag und eigene Container-Erfahrungen auf der Kommandozeile.

CI/CD mit GitLab

Der zweitägige Workshop bietet eine praktische Einführung in die GitLab-CI-Tools und zeigt, wie man damit Softwareprojekte baut, testet und veröffentlicht.

ChatGPT und KI-Textwerkzeuge in der Praxis

Das c't-Webinar hilft, die ChatGPT-Technik zu verstehen und ihren Einfluss auf Ihre Arbeit, Ihre Branche und Ihr Unternehmen einzuschätzen.

ChatGPT, Midjourney & Co. –

Rechtliche Aspekte beim Einsatz von KI-Generatoren im beruflichen Umfeld

Wir erklären die bestehende Rechtslage und ihre Auswirkungen auf den beruflichen Alltag.

Kluge Strukturen für Microsoft 365 entwickeln

Lernen Sie in dem Workshop, wie Sie gemeinsam mit Ihrem Team Leitlinien entwickeln, um in Zukunft das volle Potenzial für die Zusammenarbeit auszuschöpfen.

Sichern Sie sich Ihren Frühbucher-Rabatt:

heise.de/ct/Events

Weitere Schlagseiten auf ct.de/schlagseite

Bild: Bernd Weißbrod/dpa

Meta pur

Warum es Facebook und Instagram nun auch im kostenpflichtigen Abo gibt

Würden Sie für Facebook und Instagram zehn Euro pro Monat zahlen, wenn Meta dafür verspricht, Ihre Daten nicht für Werbeeinblendungen zu nutzen? Genau dies bietet der US-Konzern nun an, um drakonischen Strafen der EU zu entgehen.

Von Holger Bleich

Nun also tatsächlich: Meta hat für seine Plattformen Facebook und Instagram ein kostenpflichtiges Abonnement eingeführt. Anfang November ging das neue Angebot an den Start – allerdings nur im Europäischen Wirtschaftsraum (EWR), der neben allen EU-Staaten auch Island, Liechtenstein und Norwegen umfasst, sowie in der Schweiz. Für knapp zehn Euro monatlich gibt es den Zugriff auf alle Facebook- und Instagram-Konten eines Nutzers im Web ohne eingeblendete Werbung. iOS- und Android-Nutzer zahlen drei Euro mehr, weil Meta auf den mobilen Plattformen die Abgaben an Apple und Google einpreist.

Um diesen ungewöhnlichen Schritt zu verstehen, lohnt ein kurzer Blick in die Vergangenheit. Denn freiwillig handelt der US-Konzern keineswegs. Über die letzten Jahre hinweg hat die EU ihren Druck immer weiter erhöht. Im Kern geht es darum, dass Meta innerhalb des EWR dieselben datenschutzrechtlichen Vorgaben umsetzen soll, wie sie Unternehmen auferlegt sind, die ihren Hauptsitz im EWR haben. Weil genau diese aus der DSGVO hergeleiteten Regeln aber dem Geschäftsmodell von Meta zuwiderlaufen, hat sie der Konzern bislang mehr oder weniger geschickt umschifft.

Eine große Rolle spielt, dass Facebook und Instagram möglichst viele personenbezogene Daten ihrer Nutzer erfassen, um sie anschließend zur Profilbildung auszuwerten. Je genauer Meta seine Nutzer kennt, desto besser funktioniert das Kernangebot an die Werbekunden, Nutzergruppen zu selektieren und zielgenau mit Werbung bespielen zu können. Der Deal mit den Nutzern lautet nach Metas Lesart: Wir tracken euch, im Gegenzug erhaltet ihr kostenlos Zugriff auf unsere Dienste.

Lange Jahre hatte Meta behauptet, DSGVO-konform zu handeln, indem man diesen Deal irgendwo versteckt in den Nutzungsbedingungen erwähnt hatte. Tracking und Werbung seien Teil des Dienstes und benötigten deshalb keine gesonderte Rechtsgrundlage nach DSGVO. Anfang 2023 hatte der Europäische Datenschutzausschuss (EDSA) Meta dieses Gebaren untersagt, daraufhin setzte es außerdem ein Bußgeld von 390 Millionen Euro der irischen Datenschutzbehörde DPC. Seitdem berief sich Meta auf das sogenannte „berechtigte Interesse“ als Rechtsgrundlage (Art. 6 Abs. f DSGVO), weigerte sich aber, das Tracking zu unterlassen oder eine Einwilligung der Nutzer dafür einzuholen.

Dies führt zum Status quo, den der EDSA nun offensichtlich für untragbar hält: Portale von Medienhäusern etwa müssen sich mit Cookie-Bannern das Tracking von Nutzern widerrufbar erlauben lassen und sich vor Datenschutzbehörden immer wieder wegen Feinheiten verantworten. Die US-Konzerne, allen voran Meta, scheren sich nicht um diese Regeln und kamen bislang fast immer damit durch. Eine unrühmliche Rolle spielte dabei die irische Datenschutzaufsicht, die für einen großen Teil der europäischen Niederlassungen von US-Tech-Firmen verantwortlich ist. Der Vorwurf: Sie fasst die US-Konzerne bislang mit Samthandschuhen an, weil sie viel Geld ins Land bringen.

Radikaler Schritt

Da hatte sich einiges aufgestaut, am 27. Oktober ging der EDSA schließlich einen radikalen Schritt: Zum ersten Mal nutzte er die von der DSGVO vorgesehene Möglichkeit, mit einer sogenannten verbindlichen Eilentscheidung eine nationale Aufsichtsbehörde zum Handeln zu zwingen. Er wies die irische DPC an, „innerhalb von zwei Wochen endgültige Maßnahmen in Bezug auf Meta Ireland Limited zu ergreifen und ein Verbot der Verarbeitung personenbezogener Daten für verhaltensbezogene Werbung auf der Rechtsgrundlage von Verträgen und berechtigten Interessen im gesamten Europäischen Wirtschaftsraum (EWR) zu verhängen.“ Bereits am 31. Oktober begann diese 14-Tage-Frist zu laufen.

Im Klartext heißt das: Innerhalb des EWR muss Meta sein Nutzertracking be-

enden oder sich dafür beispielsweise mit rechtlich einwandfreien Cookie-Bannern eine widerrufbare Einwilligung einholen. So oder so bedeutet das für den Konzern, etliche Vorgänge umbauen zu müssen, und zwar rasch. Denn alternativ drohen eben Strafen und Anordnungen bis hin zum Verbot der Meta-Plattformen in der EU. Zuständig fürs Strafmaß wäre allerdings zunächst wiederum die irische DPC.

Die Finnin Anu Talus, seit Mai 2023 die EDSA-Vorsitzende, versicherte, die aktuelle Entscheidung sorgfältig abgewogen zu haben. Meta habe nach Berichten der DPC bislang nicht nachweisen können, sich an die vergangenen Entscheidungen gehalten zu haben. „Es ist höchste Zeit, dass Meta seine Verarbeitung in Einklang mit den Vorschriften bringt und die unrechtmäßige Verarbeitung einstellt“, erklärte Talus.

Am 30. Oktober überraschte Meta die Öffentlichkeit und die Behörden mit der Ankündigung von einem kostenpflichtigen, werbefreien Abo für Facebook und Instagram. Augenscheinlich orientiert sich der Konzern dabei an den sogenannten Pur-Abos, die mittlerweile viele deutsche Verlagshäuser eingeführt haben (auch der Heise-Verlag, der c’t herausgibt). Solche Pur-Abos haben ökonomisch betrachtet einen guten Grund: Nach gängiger Meinung von Datenschutzexperten dürfen Webdienste ihre Nutzer nicht ausschließen, falls diese nicht darin einwilligen, sich etwa mit gesetzten Cookies tracken zu lassen. Die Einwilligung muss ohne Zwang, also informiert und freiwillig geschehen.

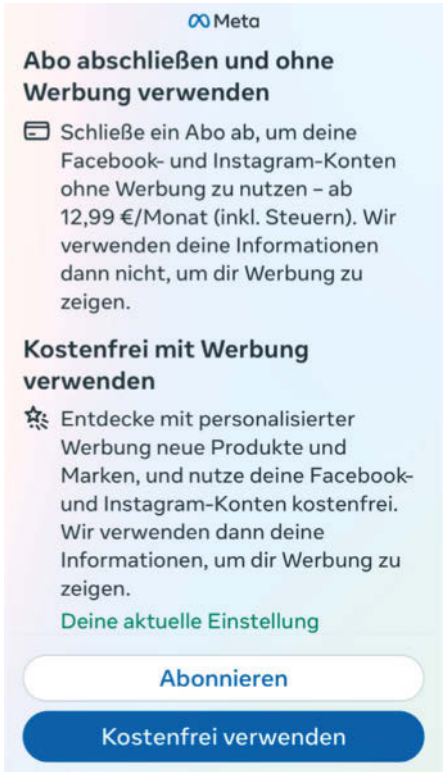
Hier kommt die Deutsche Datenschutzkonferenz (DSK), also das gemeinsame Gremium der deutschen Aufsichtsbehörden, ins Spiel. Die DSK hat sich lange mit den Pur-Abos als kostenpflichtige Alternative zur Trackingeinwilligung befasst, weil dazu etliche Beschwerden – unter anderem von der Datenschutzorganisation noyb – vorlagen. Im März hat die DSK ihren Beschluss in der Sache veröffentlicht. Darin heißt es: „Grundsätzlich kann die Nachverfolgung des Nutzendenverhaltens (Tracking) auf eine Einwilligung gestützt werden, wenn alternativ ein trackingfreies Modell angeboten wird, auch wenn dies bezahlpflichtig ist.“

Nach diesem Beschluss entstand ein Pur-Abo nach dem anderen, denn nun war es quasi amtlich: Man darf Nutzer dazu zwingen, entweder ins Tracking einzuwilligen oder zu bezahlen, falls sie das Angebot in Anspruch nehmen wollen. Die Bedingung: Die Abokosten müssen laut DSK „marktüblich“ sein, und der trackingfreie Pur-Zugang muss denselben Leistungsumfang haben. Dass zehn Euro marktüblich sind, kann man mit Fug und Recht bezweifeln. Angesichts der im Geschäftsbericht von Meta ausgewiesenen Margen beim Werbeumsatz pro Nutzer zumindest wären drei Euro wohl realistischer.

Alternative mit Zähneknirschen

Nun schließt sich der Kreis: Facebook und Instagram befürchten, dass viele Nutzer Tracking verweigern, wenn sie etwa mit einem Banner vor die Wahl gestellt werden. Das Pur-Abo gibt Meta nun die Option, formal eine Alternative anzubieten. Sicherlich werden nur wenige Nutzer zehn Euro monatlich für einen Dienst bezahlen, den sie seit Jahren kostenlos nutzen. Und falls doch, kommt dafür bei Meta wenigstens etwas Geld rein.

Im Rahmen der Aboankündigung hat Meta einige Erklärungen abgegeben, die das Zähneknirschen in der Konzernzentrale erahnen lassen. So hieß es: „Wie andere Unternehmen werden wir uns weiterhin für ein werbefinanziertes Internet einsetzen, auch mit unserem neuen Abonnementangebot in der EU, dem EWR und der Schweiz. Aber wir respektieren den Sinn



Mit einem Overlay-Fenster bietet Meta in der Facebook-App nach dem Motto „friss oder stirb“ das neue Pur-Abo an.

Bild: EU-Kommission

Anu Talus, die Vorsitzende des Europäischen Datenschutzausschusses: „Es ist höchste Zeit, dass Meta seine Verarbeitung in Einklang mit den Vorschriften bringt und die unrechtmäßige Verarbeitung einstellt.“

und Zweck dieser sich entwickelnden europäischen Vorschriften und verpflichten uns, sie einzuhalten.“ Man habe deshalb auch die Absicht, „in der EU, dem EWR und der Schweiz auf die DSGVO-Rechtsgrundlage ‚Einwilligung‘ umzustellen“.

Die Datenschutzbehörden der EU-Mitgliedsstaaten dürften Metas Ankündigungen mit Argwohn verfolgen. Weil Facebook seinen deutschen Firmensitz in Hamburg hat, äußerte sich hierzulande der Hamburgische Datenschutzbeauftragte Thomas Fuchs zuerst. Die Anforderungen an Pur-Abos würden „durch die deutschen Aufsichtsbehörden bei nationalen Anbietern geltend gemacht und von diesen umgesetzt“, ließ er verlauten. Es sei noch offen, ob das Meta-Angebot rechtskonform sei. Man sei dazu mit der irischen DPC „in einem laufenden Dialog“ und erwarte von der Behörde bald „eine überprüfbare rechtliche Bewertung“.

Weil das Pur-Abo kurz vor Redaktionsschluss startete, konnten wir noch nicht prüfen, welche Daten Meta hier tatsächlich erhebt. Die Beschreibung geriet allerdings schwammig und zeigt offene Hintertüren. Es heißt darin lediglich: „Wir verwenden deine Informationen dann nicht, um dir Werbung zu zeigen.“ Und in der Ankündigung versicherte Meta nur: „Solange die Nutzer ein Abonnement abgeschlossen haben, werden ihre Daten nicht für Werbung verwendet“. Einen Verzicht auf die Erhebung personenbezogener Daten im Pur-Abo kann man aus diesem Statement jedenfalls nicht ableiten. Es könnte folglich sein, dass die Auseinandersetzungen lediglich in die nächste Runde gehen. *(hob@ct.de)* c't

Hackberry Pi

Raspi als Hacker-Tool

Bild: Moritz Reichartz

Viele Raspberry Pi werkeln als treue Smart-Home-Zentrale oder NAS-Server, doch die Einplatinenrechner haben auch eine dunkle Seite: Als Hacker-Tools konfiguriert gehen sie zum Angriff auf Rechner, Server, Smartphones & Co. über und zeigen so Sicherheitslücken in unserem digitalen Alltag auf.

Von Ronald Eikenberg

Wenn Sie einen Raspberry Pi als Hacker-Tool einsetzen und damit nach Schwachstellen in Ihrem vernetzten Zuhause suchen, verschaffen Sie sich einen wertvollen Wissensvorsprung: Sie können geeignete Schutzmaßnahmen treffen, lange bevor ein Angreifer auf die Idee kommt, die Lücken auszunutzen. Getreu dem Motto: Hack Dich selbst – bevor es jemand anderes tut. Und ganz nebenbei lernen Sie auch noch eine Menge über die Tricks der Hacker. Auf den folgenden Seiten stellen wir vier Hacking-Projekte für Raspi-Modelle vor, vom winzigen Pico W bis hin zum größten, dem Tastatur-Raspi 400. Alle genutzten Raspis sind inzwischen wieder zu moderaten Preisen lieferbar. Im besten Fall finden Sie noch einen in irgendeiner Schublade.

Unsere Projekte reizen die Fähigkeiten der jeweiligen Modelle voll aus: Der Raspi Pico W etwa, der gerade mal rund sieben Euro kostet, gibt sich als WLAN-Hotspot aus und phisht nach Zugangsdaten (Seite 18). Damit können Sie zum Beispiel herausfinden, wie gefährdet Ihr Smartphone oder Notebook für Hotspot-Angriffe ist. Im schlechtesten Fall baut Ihr Gerät automatisch eine Verbindung zu dem Hacking-Raspi auf, weil das WLAN den Namen eines zuvor genutzten Netzes trägt, und öffnet anschließend auch noch selbstständig eine – in diesem Fall harmlose – Phishing-Seite. Auf dem Weg dorthin lernen Sie die MicroPython-Bibliothek phew! kennen, mit der Sie Ihren Raspi auch für ganz andere WLAN-Anwendungen programmieren können.

Noch weiter treibt es unser Hacking-Projekt für die Raspis 3, 4 und 5 (Seite 26): Damit wird Ihr Raspi zu einem vielseitigen WLAN-Hacking-Tool, das nicht nur vorhandene WLANs imitieren kann, etwa um den Datenverkehr mitzuschneiden oder zu manipulieren, sondern auch Router attackiert, um Sicherheitslücken aufzuspüren. So können Sie herausfinden, wie sicher Ihr WLAN-Passwort tatsächlich ist und ob Ihr Router noch für WPS-Angriffe anfällig ist. Zum Einsatz kommt das Hacking-Skript airgeddon, das viele gängige WLAN-Tools miteinander kombiniert und mit den passenden Einstellungen füttert.

Raspi als BadUSB-Gerät

Unser drittes Projekt zielt ganz auf USB ab: Das Raspi-Image P4wnP1 A.L.O.A. verwandelt den Raspi Zero W in ein mächtiges BadUSB-Tool, das sich beispielsweise als USB-Tastatur am Rechner meldet, in Windeseile Angriffs-Skripte eintippt und das System so kapert (Seite 22). Darüber hinaus kann der BadUSB-Raspi auch Mausbewegungen ausführen, zum Beispiel um einen sogenannten Mouse Jiggler zu simulieren: Er bewegt den Mauszeiger minimal, um vorzugaukeln, dass jemand am Rechner arbeitet. Dadurch sperrt sich das System nicht automatisch, wenn der Nutzer seinen Arbeitsplatz verlässt – ein Angreifer vor Ort kann so auf den Rechner zugreifen, während sich der Nutzer einen Kaffee holt. Außerdem bleibt der Anwesenheitsstatus bei Microsoft Teams & Co. grün, was Mouse Jiggler zu einem beliebten Home-Office-Gadget gemacht hat.

Last, but not least zeigen wir im vierten Projekt, wie Sie den Tastatur-Computer Raspi 400 mit Kali Linux als vielseitigen Hacking-Rechner nutzen (Seite 30). Kali ist die Linux-Distribution der Wahl für Hacker, weil es die wichtigsten Tools gleich mitliefert und man sich deren komplizierte Installation erspart. Neben der Einrichtung von Kali zeigt der Artikel, wie Sie Ihr lokales Netzwerk mit dem Tool legion nach Schwachstellen durchforsten. Es spürt nicht nur Systeme und Dienste im Netz auf, sondern bietet auch gleich die passenden Werkzeuge an, um die Funde näher zu untersuchen. Ein zweiter Raspi kann Ihnen ein Übungsnetz mit garantiert verwundbaren Servern zur Verfügung stellen, in dem Sie die Kali-Tools gefahrlos ausprobieren können. Das ist eine ideale Lernumgebung für angehende Security-Spezialisten.

Try this at home

Nutzen Sie unsere Projekte gern, um Ihre eigene Technikwelt auf Sicherheitslücken abzuklopfen – aber keinesfalls, um fremde Systeme zu attackieren! Bestimmte Handlungen wie das Ausspähen von Daten bleiben strafbar, auch wenn dies mit einem Raspi geschieht. Nutzen Sie das hier erlangte Wissen für einen guten Zweck. Vielleicht finden Sie ein neues Hobby oder es eröffnet Ihnen eine neue berufliche Perspektive als Pentester. Happy Hacking! *(rei@ct.de)* c't

Hacker-Tools im Selbstbau: Mit unseren Raspi-Projekten lernen Sie die Tricks der Hacker, um Sicherheitslücken aufzuspüren und sich vor Angriffen zu schützen. Passende Projekte gibt es für viele gängige Raspi-Modelle.

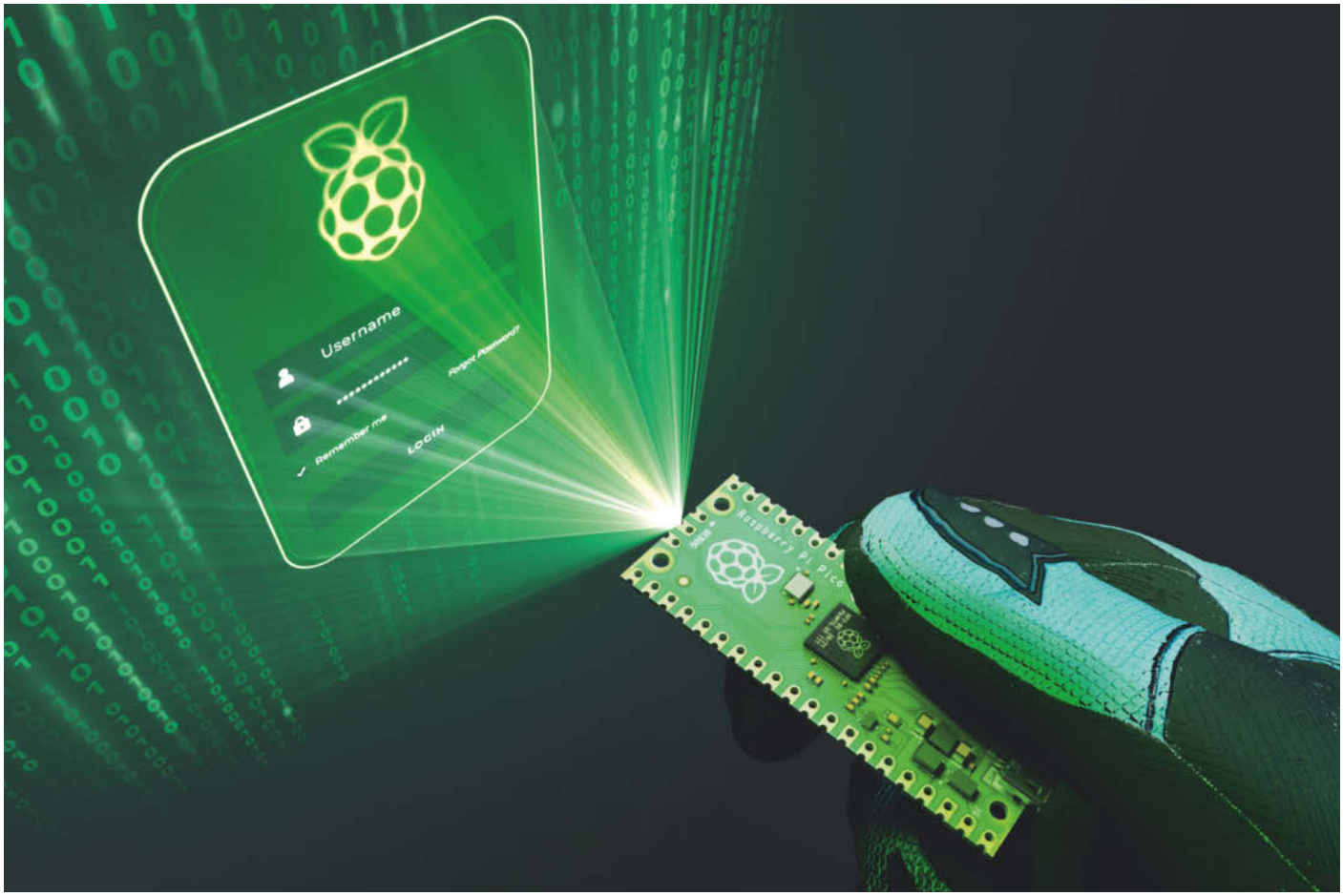


Bild: Moritz Reichartz

Phishers Fritze

Raspi Pico veranschaulicht Phishing-Angriff via Captive Portal

Hacking-Werkzeuge müssen nicht teuer sein: Mit dem Raspberry Pi Pico W bekommen Sie für unter zehn Euro ein Gadget, das als WLAN-Hotspot Informationen verbreitet oder demonstriert, wie leicht WLAN-Nutzer zur Eingabe sensibler Zugangsdaten zu bewegen sind. Dazu genügen schon wenige Zeilen Python-Code.

Von Mirko Dölle

Gut oder böse: Es ist meist schwierig, Hacking-Gadgets in eine bestimmte Schublade zu stecken. Es hängt vom eigenen Standpunkt und vom Einsatzzweck ab. Ein gutes Beispiel dafür ist unser Projekt „Capito“, ein WLAN-Hotspot mit **Ca**ptive Portal auf Basis des Raspberry Pi **Pi**co W als Hacking-**To**ol. Sie können den Capito zum Beispiel als digitales Flugblatt benutzen, um etwa in Autokratien trotz Internetzensur unabhängige Informationen zu verbreiten – er demonstriert aber auch, wie leicht sich illegal Zugangsdaten abphishen lassen, wenn WLAN-Nutzer nicht auf der Hut sind. Hard- und Software sind in beiden Fällen gleich, einzig die über den Raspi Pico verteilten Inhalte machen den Unterschied.

Der Raspberry Pi Pico ist mit sieben bis acht Euro sehr viel günstiger als die bekannten Minicomputer Raspberry Pi und Raspberry Pi Zero, spielt aber auch in einer ganz anderen Liga. Der Pico ist eher mit einem Arduino Nano vergleichbar. Das Herzstück ist der Mikrocontroller RP2040 der Raspberry Pi Foundation, der einen ARM Cortex M0+ mit bis zu 133 MHz Taktfrequenz als CPU, 264 kByte RAM und 2 MByte Flash-Speicher enthält. Auf dem Pico W ist außerdem ein WLAN-Modul (Infineon CYW43439) aufgelötet. Mit fast 30 GPIO-Anschlüssen und diversen Schnittstellen eignet sich der Raspi Pico genau wie die verschiedenen Arduino-Boards gut für allerlei Basteleien.

Ein Betriebssystem gibt es beim Raspi Pico nicht, stattdessen werden Programme zusammen mit den nötigen Bibliotheken zu einer prozessorspezifischen Firmwaredatei übersetzt und hochgeladen. Eine solche Firmwaredatei bietet auch das MicroPython-Projekt zum Download an (siehe ct.de/y95e), sie enthält eine auf den RP2040 angepasste Version des Python-Interpreters MicroPython. Mit dem können Sie Python-Programme auf dem Raspi Pico ausführen, ohne eigene Firmwaredateien erstellen zu müssen.

Aufgespielt

Um MicroPython auf einem nagelneuen Raspi Pico W zu installieren, halten Sie die

BOOTSEL-Taste auf dem Pico gedrückt und verbinden ihn per USB-Kabel mit Ihrem PC. Daraufhin meldet sich der Pico als USB-Speichermedium. Sobald Sie die Firmwaredatei mit der Endung .uf2 auf dieses USB-Gerät kopiert haben, installiert der Pico automatisch die neue Firmware und führt einen Reset durch.

Um den Pico in Python zu programmieren und Dateien auszutauschen, empfehlen wir die Entwicklungsumgebung Thonny von thonny.org. Der erste Schritt ist, die MicroPython-Bibliothek „phew!“ (siehe ct.de/y95e) auf den Pico zu kopieren. Sie enthält diverse Webserver- und WLAN-Funktionen sowie einen DNS und erlaubt es, mit wenigen Zeilen Python einen Hotspot mit integriertem Webserver zu schreiben. Dazu laden Sie die aktuelle Version von Phew herunter – bei Redaktionsschluss war es Version 0.0.3 – und entpacken das Tar-Archiv. Anschließend wechseln Sie in Thonny in das Verzeichnis mit den entpackten Inhalten, klicken mit der rechten Maustaste auf das Unterverzeichnis `phew` und wählen aus dem Kontextmenü „Upload to /“, woraufhin das Verzeichnis mit allen Dateien auf den Raspi Pico übertragen wird.

Fortan können Sie die Phew-Bibliothek wie in Python üblich einbinden. Um etwa die Access-Point-Funktion zu importieren und damit einen offenen Hotspot mit der SSID „Capito“ aufzusetzen, genügen zwei Zeilen Code:

```
from phew import access_point
ap = access_point("Capito")
```

Da der Raspi Pico keine Internetanbindung hat, benötigen Sie einen lokalen DNS-Server, der sämtliche Anfragen auf den Capito umleitet. Auch diesen gibt es fix und fertig in der Phew-Bibliothek:

```
from phew import dns
...
ip = ap.ifconfig()[0]
dns.run_catchall(ip)
```

Nachgebaut

Die typische Verhaltensweise von Hotspots in Hotels oder von Internetanbietern ist, eine Login-Seite mit den Nutzungsbedingungen sofort nach der Verbindung anzuzeigen. Diese Technik wird Captive Portal genannt und eignet sich auch hervorragend für Dissidenten, um Informationen zu verteilen. Die WLAN-Clients öffnen die Captive-Portal-Seite automatisch, sobald die WLAN-Verbindung zum Hotspot steht. Damit der Raspi Pico die Seite ausliefern kann, muss er überhaupt erstmal HTTP-Anfragen auf Port 80 entgegennehmen. Dazu starten Sie den Webserver aus der Phew-Bibliothek:

```
from phew import server
...
server.run()
```

Fehlt noch die Funktion, die die HTML-Seiten aus dem Unterverzeichnis `htdocs` ausliefert:

```
from phew.template ⮦
↳import render_template
from os import stat
...
HTDOCS = "htdocs"
...
@server.catchall()
def catch_all(request):
    try:
        stat(HTDOCS + request.path)
        return render_template(HTDOCS
           + request.path)
    except OSError:
        return "Not found.", 404
```

Wie der Name schon sagt, ruft der Server die `catchall()`-Funktion immer dann auf, wenn er eine HTTP-Anfrage nicht anderweitig beantworten kann. Ob es die gewünschte Datei gibt, überprüfen Sie einfach, indem Sie die Dateieigenschaften mittels `stat()` abrufen. Klappt das, gibt es die Datei, und `render_template()` liefert ihren Inhalt als `Response`-Objekt mit dem passenden HTTP-Header und dem HTTP-Status 200 („OK“) zurück.

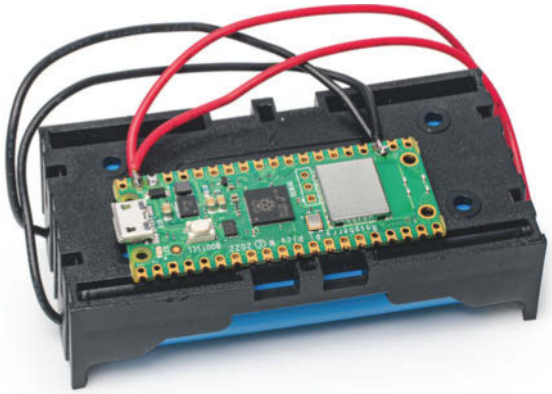
Gibt es die Datei nicht, so wirft `stat()` den Fehler `OSError` aus – der gleich danach abgefangen wird, um eine entsprechende Fehlermeldung mit dem HTTP-Status 404 zu erzeugen. Der Rückgabewert der Fehlerbehandlung ist erklärungsbedürftig, denn als Rückgabewert von `catch_all()` wird ein `Response`-Objekt erwartet. Die Schreibweise in der Fehlerbehandlung ist eine Kurzform des Objekts, bestehend aus dem Inhalt als Zeichenkette gefolgt vom HTTP-Status.

Damit sind die Grundfunktionen des Capito einsatzbereit und liefern an die verbundenen WLAN-Clients HTML-Seiten aus. Es fehlt noch die Funktionalität, damit sich das Captive Portal automatisch beim Verbinden mit dem Capito öffnet. Hier gibt es mehrere konkurrierende Standards, wie mobile Geräte feststellen, dass sie den Nutzer zunächst auf eine Startseite umleiten müssen, damit er die Nutzungsbedingungen akzeptieren und sich einloggen kann, bevor er Zugriff aufs Internet erhält.

Richtig antworten

Einige dieser Methoden haben wir bereits in [1] beim digitalen Flugblatt auf Basis des Raspberry Pi Zero W vorgestellt. Sie basieren darauf, dass die verschiedenen Betriebssysteme nach dem WLAN-Verbindungsaufbau versuchen, bestimmte URLs abzurufen. Erhalten sie vom Webserver den HTTP-Status 404, weil es die Seite nicht gibt, so gehen sie davon aus, dass das WLAN keine Anmeldung erfordert. Liefert der Aufruf jedoch den Status 302 („Moved Temporarily“) gefolgt von einer Internetadresse, so öffnen sie die URL im Browser, damit man sich anmelden kann.

Welche URL für den Verbindungstest abgerufen wird, ist von Betriebssystem zu Betriebssystem unterschiedlich. Da der DNS ohnehin sämtliche Domains zur IP-Adresse des Capito auflöst, müssen Sie nur die unterschiedlichen Dateipfade berücksichtigen. Apple-Geräte zum Beispiel fragen nach einer Seite `/hotspot-detect.html`,



Von zwei LiPo-Akkus gespeist kann der Capito etwa in Städten an belebten Orten ausgesetzt werden, wo er möglichst viele Leute erreicht. Als Wetterschutz kann eine Brotdose dienen.

Android-Geräte nach `/generate_204` und Windows nach `/redirect`. Diese Pfade müssen den HTTP-Status 302 und die URL des Captive Portals zurückgeben:

```
DOMAIN = "ca.pi.to"

@server.route("/hotspot-detect.html",
    methods=["GET"])
@server.route("/generate_204",
    methods=["GET"])
@server.route("/redirect",
    methods=["GET"])
def hotspot(request):
    return redirect(
        f"http://{DOMAIN}/", 302)
```

Die Domain dürfen Sie übrigens frei wählen, diese wird dann vom Endgerät angezeigt.

Für Windows benötigen Sie noch zwei zusätzliche Pfade, die ein leeres Dokument mit dem HTTP-Status 200 zurückliefern:

```
@server.route("/ncsi.txt",
    methods=["GET"])
@server.route("/connecttest.txt",
    methods=["GET"])
def hotspot(request):
    return "", 200
```

Es gibt noch einen Sonderfall, den Sie berücksichtigen müssen. Ruft ein WLAN-Client die Startseite der Domain auf, also `/`, so soll wie bei anderen Webservern üblich die `index.html` ausgeliefert werden:

```
@server.route("/", methods=['GET'])
def index(request):
    return render_template(HTDOCS
        + "/index.html")
```

Sie können auch leicht Informationen aus einem Formular sammeln, zum Beispiel E-Mail-Adressen für einen Newsletter oder Handy-Nummern:

```
from phew import logging
...
@server.route("/data.html",
    methods=["GET"])
def hotspot(request):
    logging.info("Got data: "
        + request.query_string)
    return render_template(HTDOCS
        + "/index.html")
```

Das Objekt `request` enthält etliche Eigenschaften, darunter `uri` mit der vollständigen URL inklusive etwaiger Formulardaten, in `path` steht der aufgerufene Pfad ohne Domain und Formulardaten, und `query_string` liefert die reinen Formulardaten – sofern sie mittels `GET` übertragen wurden. Indem die gerade gezeigte Funktion die Daten aus `query_string` an `logging.info()` weitergibt, landen sie in der Log-Datei `log.txt`.

Um die Log-Datei später über WLAN auslesen zu können, benötigen Sie noch folgende Funktion:

```
@server.route("/log.txt",
    methods=["GET"])
def hotspot(request):
    return render_template("log.txt")
```

Damit ist der Code des Capito komplett. Das vollständige Listing finden Sie zum Download auf ct.de/y95e.

Ausgetrickst

Mit dem Capito könnten Sie Kolleginnen und Kollegen aber auch demonstrieren, wie anfällig vor allem Mobilgeräte für Phishing von Zugangsdaten mittels Captive Portals sind. Würde man etwa die Anmeldeseite zu einem öffentlichen Hotspot nachempfinden, so wäre auf den ersten Blick schwer zu erkennen, dass man sich in Wahrheit auf einem modifizierten Captive Portal an Bord eines Capito anmeldet. Kaum jemandem dürfte auffallen, dass der Capito mit HTTP und nicht wie bei den offiziellen Hotspots üblich mit HTTPS arbeitet – man muss schon sehr genau hinsehen, um zu bemerken, dass vor der Adresse das Schloss-Symbol fehlt. Auch gibt es keine Warnung, dass die Daten unverschlüsselt übertragen werden. Solche Experimente dürfen Sie aber auf keinen Fall in öffentlichen Bereichen unternehmen, wo Ihnen unbekannte Passanten auf den Trick hereinfallen könnten.

Die Möglichkeiten des Capito sind jedoch eingeschränkt. Das liegt in erster Linie am äußerst begrenzten RAM des Raspi Pico, von den 264 kByte stehen mit geladener Phew-Bibliothek nur noch rund 145 kByte zur Verfügung. Die Beschränkung für eine einzelne HTML-Datei liegt bei etwa der Hälfte, also rund 70 kByte, denn die Funktion `render_template()` verarbeitet die Daten noch und benötigt dafür ebenfalls Speicherplatz. Das ist zu wenig für die Captive-Portal-Seiten von der Telekom, Vodafone und anderen Anbietern wie Hotels. Auch der Flash-Speicher ist mit 2 MByte ziemlich klein.

Ausgesetzt

Um den Capito als Flugblatt etwa in einer Stadt an einem belebten Ort auszusetzen, sollten Sie ihn in einem wassergeschützten Gehäuse unterbringen und über eine Powerbank, Batterien oder Akkus versorgen. Dabei ist der Pico wenig wählerisch, denn der RP2040 enthält einen Spannungswandler, der mit Eingangsspannungen von 1,8 bis 5,5 Volt zurechtkommt. Im einfachsten Fall verwenden Sie eine Powerbank und speisen den Raspi Pico über den USB-Anschluss. Günstiger ist es, ein oder zwei parallel geschaltete 18650er LiPo-Zellen am Pin `VSYS` (Pin 39) des Pico anzuschließen. Damit hält der Pico, bei einer Leistungsaufnahme von durchschnittlich 0,3 Watt, gut zwei Tage durch. Sie müssen dann allerdings unbedingt die LiPo-Zellen entfernen, bevor Sie den Pico zum Programmieren wieder über USB mit dem Rechner verbinden! Gleiches gilt für herkömmliche Alkaline-Batterien, hier genügen zwei oder drei Primärzellen, um den Pico über den `VSYS`-Eingang mit Strom zu versorgen.

Als Gehäuse haben wir für unseren Pico eine Frischhaltedose verwendet. Darin sind Platine und Akkus wasserdicht untergebracht und überstehen selbst schwere Regenschauer. Wenn es darum geht, den Capito an öffentlichen Plätzen unterzubringen, sind erfahrene Geocacher klar im Vorteil: Mit Magneten etwa lässt sich die Plastikdose leicht an Metallsitzbänken oder Mülleimern unterbringen, mit Gummiseilen an Bäumen oder Sträuchern anbinden oder einfach auf das Dach einer Litfaßsäule oder einer Bushaltestelle werfen. Dort haben Sie gute Chancen, dass der Capito lange unentdeckt bleibt und viele Personen erreicht. Bei einem Gesamtwert von unter 20 Euro für Raspi Pico, Akku und Dose lässt es sich verschmerzen, wenn Sie die das Gerät nicht zurückholen können, weil Sie sonst ins Visier von Ermittlern geraten könnten. Das Log mit etwaigen Formulardaten können Sie ja leicht aus der Entfernung per WLAN abrufen. *(mid@ct.de)* c't

Literatur

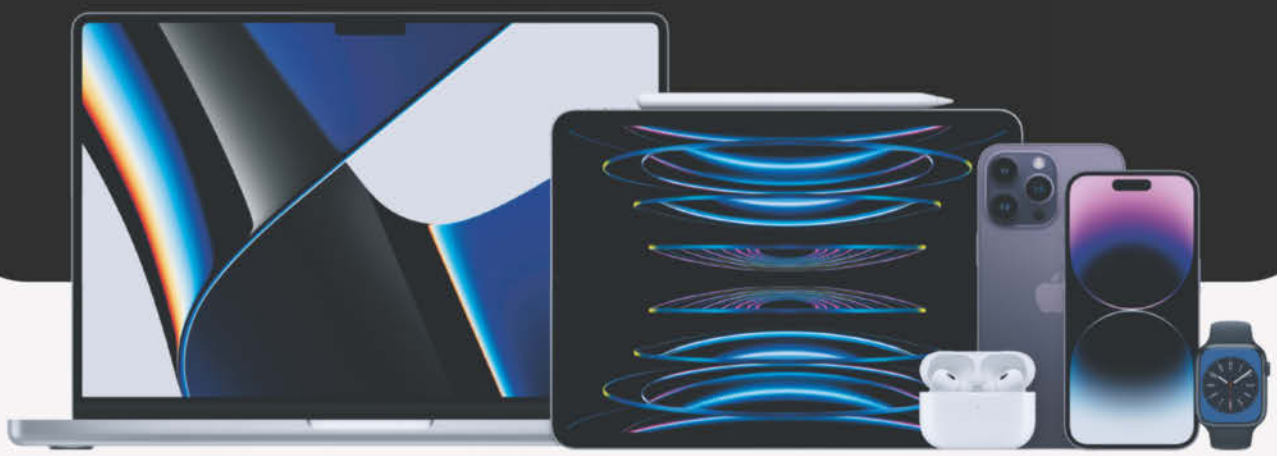
[1] Daniel Cooper, In die Freiheit entlassen, Digitales Flugblatt: Raspberry Pi mit Batterie als anonymer WLAN-Hotspot und Webserver, c't 22/2017, S. 144

Listing und Downloads: ct.de/y95e

17.–27. November

BLACK WEEK

Premium Technik von
A wie Apple Produkte bis
Z wie Zubehör



Gravis

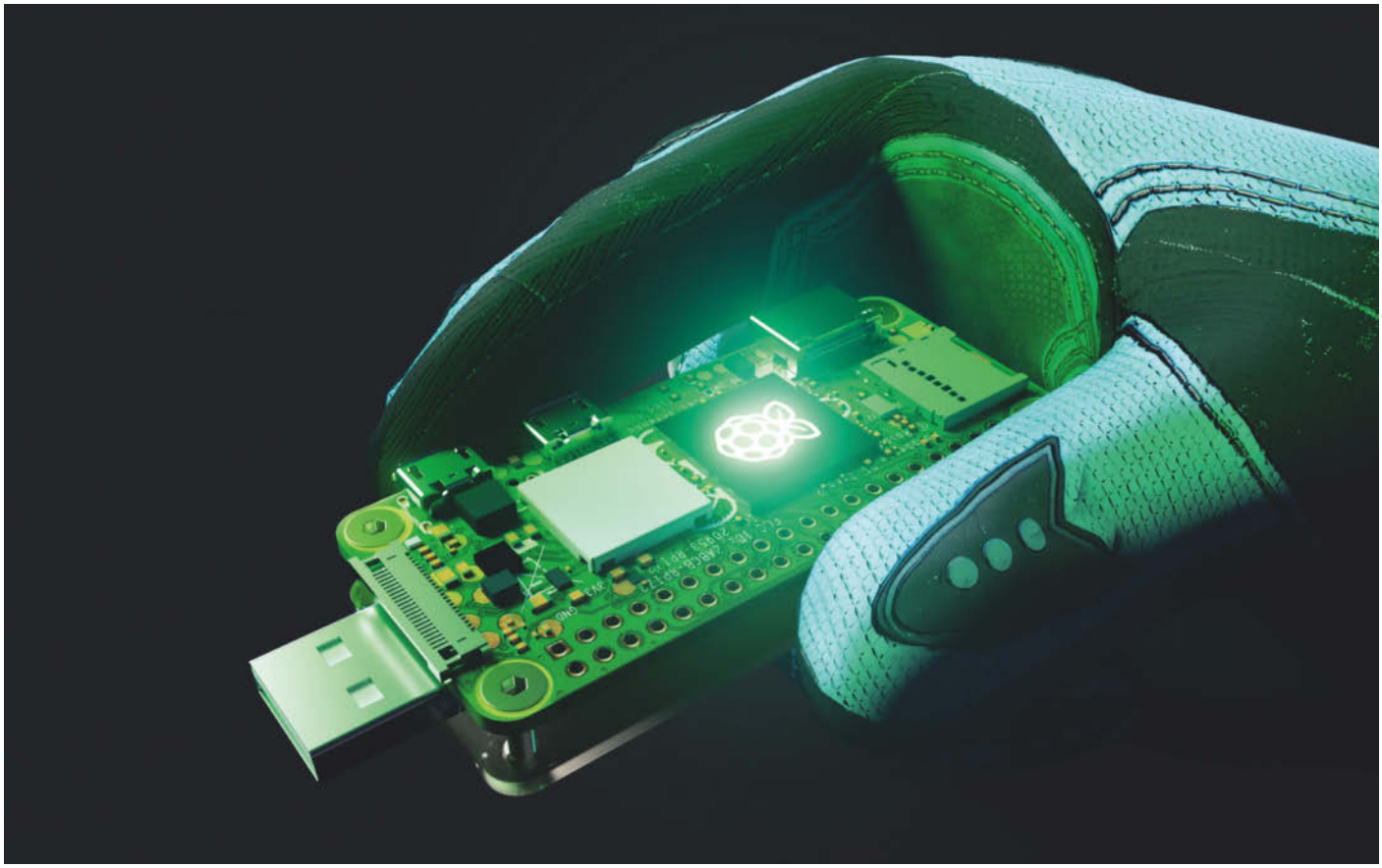


Bild: Moritz Reichartz

Böses USB

Raspi Zero W als BadUSB-Tool

Von BadUSB-Angriffen haben Sie vielleicht schon mal gehört: Hacking-Gadgets geben sich als Tastatur, Netzwerkkarte und vieles mehr aus und attackieren den Rechner, während der Virenscanner Däumchen dreht. Mit dem Raspberry Zero W können Sie das selbst ausprobieren.

Von Ronald Eikenberg

Ein USB-Anschluss ist nicht nur praktisch, sondern auch gefährlich: BadUSB-Geräte können darüber den Rechner kapern und Daten erbeuten. Das ist technisch aufwendiger, als einen Trojaner auf einem USB-Stick zu verteilen, aber auch viel perfider: Denn den Trojaner auf dem Stick kann das Virenschutzprogramm abfangen, gegen BadUSB kann es hingegen wenig ausrichten. In die Kategorie BadUSB fallen Geräte, die die Möglichkeiten von USB geschickt für IT-Angriffe ausnutzen. Schließt man etwa eine Tastatur an, wählt das Betriebssystem dank Plug & Play automatisch einen passenden Treiber und man kann sofort beliebige Befehle eingeben. Gibt sich ein BadUSB-Gerät als Tastatur aus, kann es das auch.

Am bekanntesten ist der USB Rubber Ducky von Hak5 (siehe ct.de/yhhf). Wird er an den Rechner angeschlossen, meldete er sich als Tastatur an und feuert in Windeseile vom Angreifer vorprogrammierte Tastatureingaben ab. Los geht es häufig mit der Tastenkombination Windows+R, um den Ausführen-Dialog zu öffnen. Mit `powershell` und Enter hat der Rubber Ducky dann auch schon die mächtige PowerShell geöffnet und kann dort zum Beispiel ein Backdoor-Skript eintippen und ausführen. Kurz gesagt: Alles, was Sie können, kann der Rubber Ducky auch – nur viel schneller.

Hacker haben längst Wege gefunden, auch USB-Mäuse, -Laufwerke, -Netzwerkkarten und so weiter zu simulieren und für Angriffe zu nutzen. Besonders vielseitige Hacking-Gadgets wie der Bash Bunny Mark II (siehe ct.de/yhhf) setzen diese Techniken in Kombination ein, etwa um sich als USB-Massenspeicher am System zu melden und als Tastatur einen Kopierbefehl einzutippen, der die Datenbeute auf den integrierten Speicher schaufelt.

In deutschen Shops kostet die aktuelle Ausführung des Bash Bunny mindestens 160 Euro. Für ungefähr ein Zehntel dieses Preises gibt's jedoch den Raspberry Pi Zero W der ersten Generation, der mit der passenden Software ebenfalls zu einem äußerst vielseitigen BadUSB-Gerät mutiert, das dem Bash Bunny in nichts nachsteht. Mit so einem Raspi können Sie selbst überprüfen, wie leicht Ihr Rechner über USB gehackt werden kann und ob Ihre Schutzmaßnahmen greifen. Der Raspi eignet sich mit der BadUSB-Software aber auch zur Automatisierung des Rechners, der Fantasie sind hier kaum Grenzen gesetzt.

Neben dem Raspi Zero W – mit dem Nachfolgemodell Zero 2 W ist die Software nicht kompatibel – benötigen Sie nur noch eine MicroSD-Speicherkarte mit mindestens 8 GByte. Zusätzlich empfehlen wir für dieses Projekt eine Erweiterungsplatine mit USB-A-Anschluss, damit Sie den Raspi wie einen USB-Stick in den Rechner stecken können, ohne mit einem Kabel hantieren zu müssen. Solche USB-Boards gibt es online schon ab sieben Euro. Über USB wird der Raspi nicht nur mit Strom versorgt, er ist darüber auch steuerbar – und steuert umgekehrt den angeschlossenen Rechner.

Software bereitmachen

Die Verwandlung des Raspi in ein Hacking-Tool erfordert nur wenige Klicks. Laden Sie sich das Image „P4wnP1 A.L.O.A." bei GitHub herunter (siehe ct.de/yhhf) und schreiben Sie es auf Ihre Speicherkarte. Besonders einfach klappt das mit dem offiziellen Raspberry Pi Imager (siehe S. 30): Klicken Sie links auf „OS WÄHLEN" und anschließend auf „Eigenes Image" (ganz unten).

P4wnP1 A.L.O.A. basiert auf einer älteren Kali-Linux-Version (siehe S. 30). Um Ihren BadUSB-Raspi in Betrieb zu nehmen, verbinden Sie ihn mit einem Rechner – entweder per Kabel über den mit USB beschrifteten Micro-USB-Port oder per USB-A-Platine. Der Raspi spannt nach kurzer Zeit ein Konfigurations-WLAN namens P4WNP1 auf. Verbinden Sie sich damit, indem Sie das Passwort „MaMe82-P4wnP1" nutzen. Rufen Sie anschließend http://172.24.0.1:8000/ (nicht https) im Browser auf, um die funktionsreiche Weboberfläche zu öffnen.

Los geht es mit den USB-Einstellungen, über die Sie festlegen, welche Gerätetypen der Raspi Ihrem Rechner vorgaukeln soll. Standardmäßig sind unter anderem die Modi „Keyboard" und „Mouse" aktiv, zudem der Schalter „Enabled", der die USB-Funktionen einschaltet. Falls Sie die Einstellungen verändern, müssen Sie abschließend auf „Deploy" klicken, um die Änderungen zu übernehmen.

Angriff nach Skript

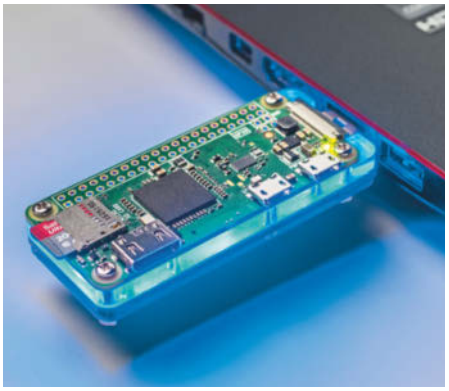
Um jetzt einige harmlose Tastaturbefehle auszuführen, wechseln Sie oben auf „HID-SCRIPT". Daraufhin erscheint der Skript-Editor mit einem simplen Beispielskript, das auf Windows abzielt. Wenn Sie schon mal mit JavaScript gearbeitet haben, dürften Sie sich schnell zurechtfinden. Der erste Schritt bei Tastaturskripten ist stets das Einstellen der Tastaturbelegung. Sie muss zum im Betriebssystem eingestellten Tastaturlayout passen, hierzulande meist QWERTZ. Zeile 1 des Beispielskripts stellt allerdings das US-Layout ein (QWERTY): `layout('us');`

Ersetzen Sie `us` einfach durch `de`, um zu QWERTZ zu wechseln. In Zeile 4 wartet das Skript durch `waitLEDRepeat(NUM);` darauf, dass wiederholt die NUMLOCK-Taste auf einer an den Rechner angeschlossenen Tastatur gedrückt wird. Sie können die Zeile einfach löschen oder mit `//` auskommentieren. Wenn Sie anschließend auf „RUN" drücken, können Sie sich zurücklehnen und das folgende Schauspiel beobachten, wenn Sie Windows nutzen: Ihr Rechner öffnet wie von Geisterhand das Windows-Notepad und tippt einige Textzeilen wie „Hello from P4wnP1 run 0 !" ein. Zwischendurch bewegt sich der Mauszeiger. Nach wenigen Sekunden ist der Spuk auch schon wieder vorbei.

Um zu verstehen, was da gerade vor sich gegangen ist, reicht ein Blick in die folgenden Zeilen des Skripts. In Zeile 5 gehts los: `press("GUI r");` drückt die Tastenkombination Windows+R, um den Ausführen-Dialog zu öffnen. `GUI` steht für die Windows-Taste, das `r` für den Buchstaben. Anstelle von `GUI` akzeptiert P4wnP1 auch die Bezeichnung `WIN` für die Windows-Taste, andere wichtige Sondertasten heißen zum Beispiel `CTRL`, `ALT`, `DEL`, `SHIFT`, `BACKSPACE`, `ENTER` oder `F1` bis `F12`.

Danach wartet das Skript mit `delay(500);` 500 Millisekunden, damit sich der Ausführen-Dialog öffnen kann. Das Timing ist bei Tastatur- und Mausskripten sehr wichtig. Baut man nicht genügend Pausen ein, erreichen die Eingaben das falsche Fenster. Nach der kurzen Verschnaufpause startet das Skript das Notepad: `type("notepad\n")`. Während `press()` für Tastenkombinationen genutzt wird, tippt `type()` den gewünschten Text Zeichen für Zeichen ein. Das `\n` steht für die Return-Taste. Nach einer weiteren Pause beginnt eine `for`-Schleife mit dem Tippen in das geöffnete Notepad: `type("Hello from P4wnP1 run " + i + " !\n");`.

Wie schnell das Skript tippt, gibt Zeile 2 vor: `typingSpeed(100,150)`. Die erste Zahl steht für eine garantierte Pause von 100 Millisekunden. Die zweite Zahl hängt noch eine zufällige Dauer hintendran, die Zahl entspricht dabei der Maximallänge – in diesem Beispiel 150 Millisekunden. So kann man ein menschliches Tippverhalten simulieren. Das Einstellen der Tippgeschwindigkeit ist jedoch optional.



Mit einem passenden Erweiterungsboard für wenige Euro können Sie den BadUSB-Raspi wie einen USB-Stick in den Rechner stecken.

Die Mausbewegungen entstehen durch den Befehl `moveStepped()` im Skript, der die Maus um 500 DPI-Punkte nach rechts und dann wieder nach links verschiebt. Früher oder später möchten Sie die Maus wahrscheinlich nicht nur bewegen, sondern auch klicken. Für einen Klick mit der linken Maustaste geben Sie den Befehl `click(BT1);` ein. `BT2` entspricht der rechten Taste, `BT3` der mittleren.

Damit kennen Sie auch schon die wichtigsten Funktionen, um eigene Eingabeskripte zu bauen. Probieren Sie doch mal das folgende Skript aus:

```
layout('de');
press('GUI r');
delay(500);
type('https://ct.de\n');
```

Das Skript öffnet die c't-Website im eingestellten Standardbrowser, sofern eine Internetverbindung besteht.

Weitere praxisnahe Beispiele finden Sie in der Dokumentation bei GitHub (siehe ct.de/yhhf). Die Doku ist etwas lückenhaft, wenn Sie aber gezielt in den Issues des GitHub-Projekts suchen, finden Sie Antworten auf viele Fragen. Ein Blick lohnt sich auch auf die mitgelieferten Beispielskripte, die Sie mit „LOAD & REPLACE" öffnen. Bei mousejiggle.js handelt es sich um einen einfachen Mouse Jiggler, der durch subtile Mausbewegungen Nutzeraktivität am Rechner vorgaukelt – ein beliebter Trick am Arbeitsplatz, der verhindert, dass Microsoft Teams & Co. den Status auf „Abwesend" ändern,

wenn man nicht am Rechner sitzt. „helper.js“ enthält einige Hilfsfunktionen, etwa um Befehle als Admin auszuführen.

Speichern und automatisieren

Die Weboberfläche speichert Änderungen nicht dauerhaft, auch nicht das im HID-Script-Editor bearbeitete Skript. Hierzu gibt es auf jeder Einstellungsseite einen Knopf „STORE“, mit dem Sie die jeweiligen Änderungen der Seite unter einem beliebigen Namen speichern können. Mit den LOAD-Buttons lesen Sie die gespeicherten Daten wieder ein. Mitunter gibt es davon gleich zwei: einen, um die aktuellen Einstellungen zu ersetzen, einen um sie zu ergänzen.

Sie werden schnell feststellen, dass es sehr lästig sein kann, die Skripte auf den Rechner loszulassen, mit dem Sie die Weboberfläche bedienen. Im schlechtesten Fall programmieren Sie versehentlich eine Schleife, die dauerhaft die Maus auf Reisen schickt oder irgendwas eintippt. Um die Kontrolle zurückzugewinnen, können Sie den Raspi einfach vom Rechner trennen. Die bessere Strategie ist, den Raspi von vornherein an einen anderen Rechner zu stecken, damit Sie ungestört programmieren können. Alternativ können Sie die Weboberfläche auch per Smartphone oder Tablet bedienen.

Bei einem echten Einsatz möchte man sich nicht erst via WLAN verbinden, um das Skript per Weboberfläche zu starten. Der Raspi legt im Idealfall nach dem Anschließen einfach los. P4wnP1 kennt hierfür eine Reihe von Triggern, die zu verschiedenen Anlässen ausgeführt werden – etwa, nachdem der Raspi mit dem Rechner verbunden ist. Um einen solchen Trigger einzurichten, wechseln Sie auf „TRIGGER ACTIONS“ und klicken auf „ADD ONE“. Dort wählen Sie zum Beispiel „USB gadget connected to host” und „start a HIDScript“, damit das Skript startet, sobald die USB-Verbindung steht. Anschließend können Sie ein gespeichertes Skript auswählen. Die Trigger-Konfiguration müssen Sie wieder mit „STORE“ speichern.

P4wnP1 A.L.O.A. startet nach dem Booten mit einem sogenannten Master Template, das festlegt, welche Konfigurationen für die einzelnen Funktionen, also etwa TRIGGER, HIDSCRIPT und auch USB, geladen werden sollen. Sie haben den Trigger jetzt zwar gespeichert, er wird nach dem Starten aber noch nicht geladen. Um das zu ändern, wechseln Sie auf „GENERIC SETTINGS“. Stellen Sie im „Master Template Editor“ ein, welche der gespeicherten Profile für die einzelnen Funktionen geladen werden sollen. Diese Master-Konfiguration speichern Sie wieder mit „STORE“. Danach können Sie sie unter „Startup Settings“ als „Startup Master Template“ auswählen. Achten Sie darauf, dass Sie eine USB-Konfiguration hinterlegen, die die im Skript genutzten Funktionen wie Tastatur und Maus bereitstellt.

Weitere USB-Geräte und SSH

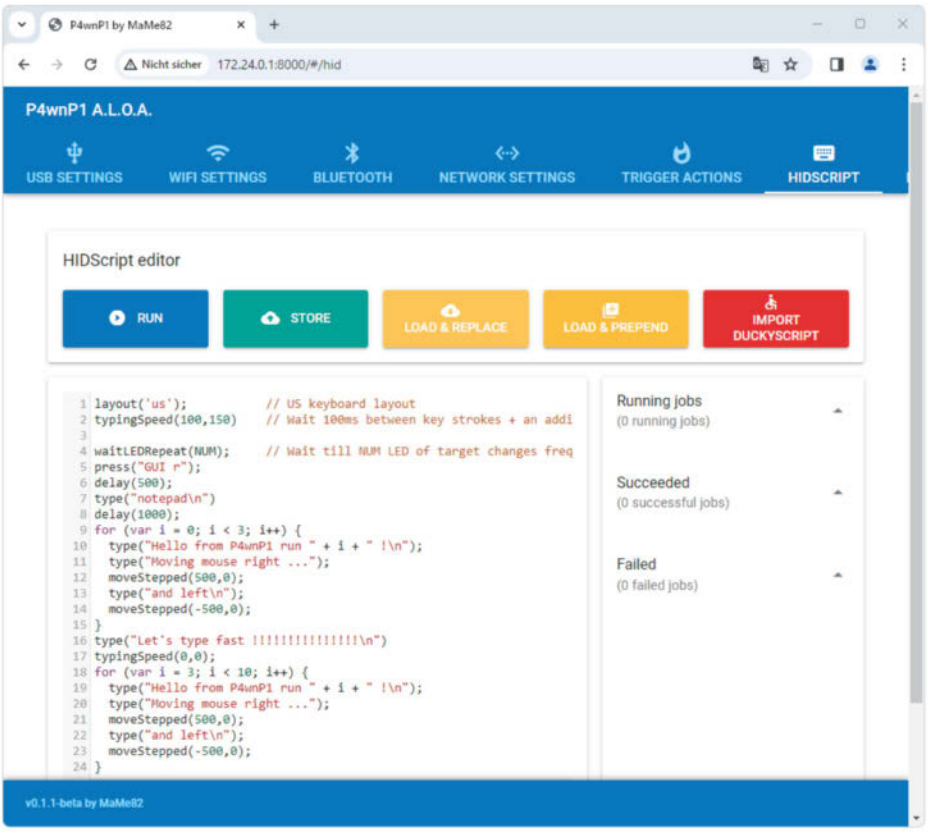
Dieser Artikel kratzt nur an der Oberfläche der Möglichkeiten. Allein die USB-Funktionen bieten noch viel mehr, als wir hier unterbekommen. Mit den Modi „CDC ECM“ und „RNDIS“ etwa meldet sich der Raspi als USB-Netzwerkkarte, über die Sie ihn direkt ohne WLAN ansprechen können. Seine IP-Adresse lautet dann 172.16.0.1. Über „Mass Storage“ stellt P4wnP1 den Inhalt einer Image-Datei als USB-Stick oder CD-ROM-Laufwerk bereit, zum Beispiel um mitgebrachte Tools auszuführen.

Wie eingangs erwähnt, basiert P4wnP1 A.L.O.A. auf Kali Linux. Sie können sich per SSH damit verbinden und Hacking-Tools von Kali ausführen. Hierzu bauen Sie eine SSH-Verbindung zur Raspi-IP (im P4wnP1-WLAN 172.24.0.1, über USB 172.16.0.1) mit dem Benutzernamen root und dem Passwort toor auf. Über das Trigger-Event „run a bash script“ können Sie Linux-Befehle sogar automatisiert ausführen lassen. Auch das Webinterface hält noch einige Schmankerl für Sie bereit: So kann sich P4wnP1 etwa auch als WLAN-Client mit einem vorhandenen Netz verbinden oder Steuerbefehle über Bluetooth empfangen.

Gut und günstig

Mit dem Image P4wnP1 A.L.O.A. wird der Raspi Zero W zu einem günstigen und flexiblen Hacker-Tool, mit dem Sie viel lernen können – ganz gleich, ob Sie damit die Sicherheit Ihrer Rechner auf die Probe stellen oder Geräte per USB-Eingaben automatisieren. Per JavaScript erstellen Sie leicht passende Skripte für jeden Zweck. Es versteht sich von selbst, dass Sie damit keine fremden Systeme angreifen dürfen. *(rei@ct.de)* c't

Download & Doku: ct.de/yhhf



Das Verhalten des BadUSB-Raspi programmieren Sie per JavaScript. Das mitgelieferte Beispiel steuert den Rechner per Tastatur und Maus.

FRITZ!

GLASFASER UND FRITZ!

WIE EIN HERZ UND EINE SEELE

avm.de/dreamteam

Bild: Moritz Reichartz

Funkfrüchtchen

Raspi 3/4/5 als WLAN-Schreck

Drahtlose Netzwerke sind immer noch ein begehrtes Angriffsziel für Cyberschurken. Dafür braucht es keine Profiausrüstung: Mit einem Raspi, einem WLAN-USB-Adapter und Airgeddon schlüpfen Sie in die Rolle der Hacker und spüren Sicherheitslücken auf.

Von Niklas Dierking

Eines der populärsten Hacking-Gadgets, das die Augen von Hackern zum Leuchten bringt, ist der WiFi Pineapple von Hak 5 (siehe ct.de/ys2v). Der Spezialrouter mit modifizierter OpenWRT-Firmware nimmt Pentestern und Cyberschurken bei Angriffen auf drahtlose Netzwerke viel Arbeit ab. Er stellt eine moderne Weboberfläche zur Verfügung, über die man viele WLAN-Angriffe auf Knopfdruck ausführen kann.

Um Ihre drahtlosen Netze auf Sicherheitslücken abzuklopfen, reicht aber auch schon ein Raspberry Pi, der ja vielleicht schon in einer Ihrer Schubladen auf einen neuen Einsatzzweck wartet. Weil die hier demonstrierten Angriffe etwas mehr Rechenleistung benötigen, sollten Sie zum Raspberry Pi 3 oder neuer greifen.

Geht es um Hacking und Pentesting, ist Kali Linux die erste Wahl. Es ist die Grundlage für die folgenden Schritte. Bespielen Sie für dieses Projekt daher zunächst eine Speicherkarte mit Kali, wie auf Seite 30 beschrieben. Ein offizielles Image für den Raspi 5 lag zum Redaktionsschluss noch nicht vor, soll laut den Entwicklern aber noch dieses Jahr erscheinen.

Zusätzlich brauchen Sie einen WLAN-USB-Adapter, der den sogenannten Monitor-Modus beherrscht. In diesem Modus sehen Sie auch WLAN-Pakete, die nicht an Sie adressiert sind, und können auch spezielle Pakete verschicken, die anfällige Clients aus dem Netz schießen. Eine Liste kompatibler Adapter haben wir unter ct.de/ys2v verlinkt. Für unseren Test haben wir einen WLAN-USB-Stick mit RT5572-Chipsatz für etwa 15 Euro benutzt.

Mit unserer Anleitung klopfen Sie Ihre drahtlosen Netzwerke auf Lücken ab und lernen, wie Sie verdächtige WLAN-Aktivitäten erkennen. Richten Sie die Angriffe, die in diesem Artikel beschrieben werden, ausschließlich gegen eigene WLANs oder gegen Netze, für die Sie explizit eine Erlaubnis eingeholt haben!

Wir haben uns bei diesem Projekt dafür entschieden, den Raspi „headless“, sprich ohne angeschlossenes Display, Maus und Tastatur zu betreiben, damit er portabel ist. Die Konfiguration und Bedienung erfolgt

mittels SSH von einem anderen Gerät. Damit Sie sich mit SSH einloggen können, muss der Raspi sich im gleichen Netzwerk befinden wie der Rechner, von dem aus Sie ihn bedienen. Geben Sie dem Raspi deswegen vor dem ersten Start die nötigen Informationen mit, um sich mit Ihrem WLAN zu verbinden. Am einfachsten geht das, indem Sie auf der Kommandozeile eines Linux-Rechners folgenden Befehl ausführen:

```
wpa_passphrase SSID↵
↳> wpa_supplicant.conf
```

Ersetzen Sie den Platzhalter `SSID` durch den Namen Ihres Netzes. Sie werden dann nach dem WLAN-Passwort gefragt. Die Datei kopieren Sie anschließend auf die BOOT-Partition der MicroSD-Karte. Wenn Sie keinen Linux-Rechner zur Hand haben, erstellen Sie die Datei mit einem beliebigen Texteditor und ersetzen die Werte aus der folgenden Vorlage durch Ihre eigenen:

```
country=DE

network={
    ssid="SSID"
    psk="PASSWORT"
}
```

Stecken Sie Karte in den Raspi und verbinden Sie ihn mit dem Netzteil. Beim Start verbindet er sich automatisch mit dem konfigurierten WLAN. Loggen Sie sich dann via SSH auf dem Raspi ein: `ssh kali@192.168.178.10`

Ersetzen Sie die IP-Adresse im obigen Befehl durch die Adresse des Raspi, die Sie in der Weboberfläche Ihres Routers nachschauen können. Das Passwort des Benutzers kali lautet ebenfalls kali. Bringen Sie zunächst die Software auf den neuesten Stand und ändern Sie dann das Standardpasswort:

```
sudo apt update && sudo apt↵
↳full-upgrade -y

passwd kali
```

Airgeddon

Ähnlich wie beim WiFi Pineapple ist es das Ziel, sich vom Hacking-Raspi möglichst viel Arbeit abnehmen zu lassen. Deswegen greifen wir zu dem umfangreichen Bash-Skript Airgeddon, das voll und ganz auf WLAN-Hacking ausgerichtet ist. Klonen Sie das GitHub-Repository und wechseln dann in den neu entstandenen Ordner:

```
git clone --depth 1 https://github↵
↳.com/v1s1t0r1sh3r3/airgeddon.git

cd airgeddon
```

Um alle Angriffe auszuführen, müssen Sie folgende Pakete nachinstallieren:

```
apt install bettercap hcxtools \
hostapd asleap beef-xss mdk4 \
hostapd-wpe isc-dhcp-server lighttpd
```

Das Skript nutzt standardmäßig xterm für das Fenstermanagement, aber in einer SSH-Session wird das nicht funktionieren. Bearbeiten Sie mit einem Texteditor die versteckte Datei .airgeddonrc (etwa mit `nano .airgeddonrc`) und ändern Sie in der letzten Umgebungsvariable `xterm` zu `tmux`.

Jetzt können Sie Airgeddon mit folgendem Befehl starten: `sudo bash airgeddon.sh`

Es begrüßt Sie mit einer niedlichen Ufo-Animation und prüft, ob die nötige Software installiert ist. Sie navigieren im Skript, indem Sie die Ziffer eintippen, die zur gewünschten Option im Menü gehört.

Im Hauptmenü werden Sie zunächst gebeten, sich für ein Netzwerk-Interface zu entscheiden. Das Interface `wlan0` ist der integrierte WLAN-Chip des Raspi. Wählen Sie stattdessen mit `wlan1` den WLAN-Stick, der den Monitor-Modus unterstützt. Versetzen Sie das Interface jetzt mit der dritten Menüoption in ebendiesen.

Risiko unsichere Passwörter

Airgeddon kennt mehrere Wege, um an ein WPA-/WPA2-Passwort zu kommen. Bei einer der bekannteren, aber auch weniger Erfolg versprechenden Attacken legen Sie sich auf die Lauer und hoffen, dass Ihnen ein Handshake zwischen einem Client und einem Access Point ins Netz geht. Dabei wird ein Hash des Passworts mitgeschnitten, auf den Sie im zweiten Schritt eine Wörterbuchattacke ansetzen.

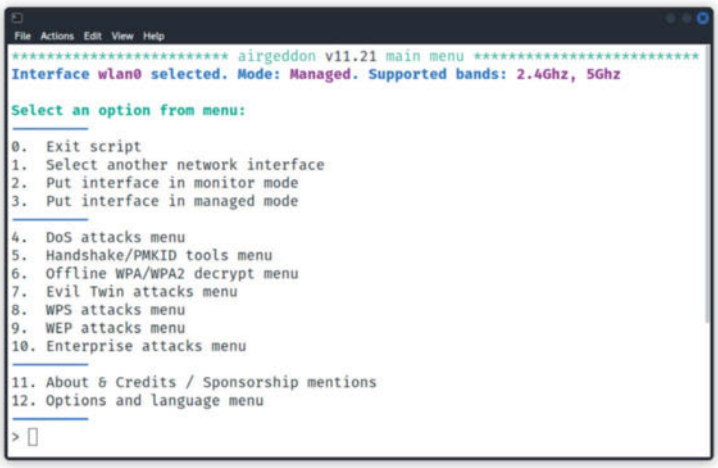
Navigieren Sie in das Menü „Handshake/PMKID tools“. Zunächst müssen Sie mit „Explore Targets“ das Zielnetz an Airgeddon übergeben. Sobald Ihr WLAN in der Liste erscheint, brechen Sie den Scan mit Strg+C ab und wählen anschließend das Zielnetz aus. Mit „Capture Handshake“ leiten Sie die Attacke ein.

Bis sich zufällig ein Client mit dem Zielnetz verbindet, können Sie alt werden, aber Airgeddon hilft nach: Mit „Deauth aireplay attack“ im nächsten Menü schießen Sie verwundbare Clients frech aus dem WLAN, damit sie sich neu verbinden.

Wenn die Jagd erfolgreich war, meldet das Skript „Congratulations!!“. Bestätigen Sie mit Enter, um die Datei zu speichern. Navigieren Sie zurück zum Hauptmenü und wählen „Offline WPA/WPA2 decrypt menu“, dann „Personal“. Die hier angebotenen Bruteforce-Attacken mit hashcat können Sie getrost ignorieren, dafür brauchen selbst kräftige Workstations viel zu lange. Versuchen Sie Ihr Glück stattdessen mit aircrack, um eine der Wortlisten durchzuprobieren, die es zuhauf im Netz gibt. Laden Sie außerhalb von Airgeddon die Liste german-words.txt runter (siehe ct.de/ys2v):

```
curl -o ↵
↳~/airgeddon/wordlist-german.txt↵
↳https://gist.githubusercontent.com/M↵
↳arvinJWendt/2f4f4154b8ae218600eb091a↵
↳5706b5f4/raw/36b70dd6be330aa61cd4d4c↵
↳dfda6234dcb0b8784/wordlist-german.txt
```

Geben Sie jetzt den Pfad zur Wortliste (/home/kali/wordlist-german.txt) und zur erbeuteten Handshake-Datei an; letztere



Airgeddon vereinfacht viele gängige WLAN-Angriffe mit dem Raspberry Pi.

liegt im Verzeichnis /root. Damit haben Sie alles für die Attacke zusammen und können aircrack starten. In unserem Testlauf hat aircrack das sehr unsichere Passwort „Achterbahn“ blitzschnell herausgefunden.

Risiko WPS

Man muss sich gar nicht immer die Mühe machen, einen Passwort-Hash zu erbeuten und zu entschlüsseln. Stattdessen kann man darauf hoffen, dass beim Access Point die WPS-Funktion (WiFi Protected Setup) aktiv ist, der Hersteller die Komfortfunktion unsicher implementiert hat und die Lücke noch nicht gepatcht ist. Bei der WPS-PIN-Methode muss man auf dem Client statt dem WLAN-Passwort eine kurze PIN eingeben. Die PIN generieren Router manchmal aus der MAC-Adresse, die jeder sehen kann, oder sie nutzen schwache Zufallszahlen. Die sogenannte Pixie-Dust-Attacke macht sich diese Schwachstellen zunutze. Sie finden Sie im Hauptmenü unter „WPS attacks menu“.

Das Prinzip ist bekannt: Schalten Sie das Interface `wlan1` in den Monitor-Modus („Put interface in monitor mode“) und suchen nach dem Ziel („Explore for targets“). Beenden Sie den Scan mit CTRL + C und wählen Sie Ihr WLAN aus der Liste. Mit dem Tool reaver, das Sie einfach über den entsprechenden Menüeintrag starten können, gelang es uns, eine erfolgreiche Pixie-Dust-Attacke auf einen ausgemusterten D-Link-AC2600-Router mit der neuesten verfügbaren Firmware auszuführen. Nach weniger als zehn Sekunden erbeutete das Skript das WLAN-Passwort.

Risiko Mensch

Neben Wörterbuch- und WPS-Angriffen hat Airgeddon auch mehrere Evil-Twin-Attacken im Köcher. Das sind Social-Engineering- und Phising-Angriffe, die Nutzer mit technischen Tricks dazu bringen, sich mit einem Access Point zu verbinden, der unter Kontrolle des Angreifers steht und einen bekannten Access Point imitiert. Auch bei dieser Methode kegelt man Clients aus dem Ziel-WLAN (Deauthentication). Es ist nicht unwahrscheinlich, dass sich ein unbedarfter Nutzer danach mit dem Evil Twin verbindet.

Das Menü „Evil Twin Attacks“ bietet verschiedene Ausführungen dieses Angriffs. Aktivieren Sie zunächst nach dem bekannten Muster den Monitor-Modus. Mit der Option „Evil Twin AP attack with captive portal“ geht es erneut darum, das

Airgeddon phisht bei der Evil-Twin-Attacke mit einem Captive Portal nach WLAN-Passwörtern.

WLAN-Passwort zu erbeuten. Dafür setzen Sie dem Nutzer, der in die Falle gegangen ist, ein sogenanntes Captive Portal vor. Das ist ein Login-Formular, das man so ähnlich von Hotels oder Zügen kennt, hier aber dazu dient, das Passwort zu erbeuten. Ein Captive Portal öffnet sich normalerweise automatisch, sobald die Verbindung zum WLAN steht.

Zu Beginn der Attacke müssen Sie Ihr Ziel-WLAN wählen, danach eine Deauthentication-Attacke. Bei uns hat die zweite Option „deauth aireplay attack“ zuverlässig funktioniert. Das Skript fragt Sie dann, ob Sie den „DoS pursuit mode“ aktivieren wollen, was Sie verneinen können. Das ist nützlich, wenn ein Access Point im Channel-Hopping-Modus läuft, also häufiger den WLAN-Kanal wechselt, braucht aber einen weiteren WLAN-Adapter mit Monitor-Modus, der die Verfolgung aufnimmt. Die MAC-Adresse müssen Sie nicht verbergen, wenn das Skript fragt.

Clever: Der Evil Twin mit Captive Portal kann eine zuvor erbeutete und noch nicht entschlüsselte Handshake-Datei nutzen, um zu prüfen, ob das eingegebene Passwort stimmt. Wenn das Opfer ein falsches Passwort einträgt, meckert das Portal. Geben Sie dazu den Pfad zu einer Handshake-Datei an. Im nächsten Schritt wählen Sie die Sprache für das Captive Portal. Sie können außerdem entscheiden, ob Sie ein generisches Portal nutzen möchten oder Airgeddon die BSSID des angegriffenen Access Points analysieren soll, um das Portal dem erkannten Router-Hersteller nachzuempfinden.

Wenn Sie die Attacke starten, öffnen sich am unteren Rand des Terminals mehrere Tabs mit Logs der Tools, die das Skript automatisch für Sie gestartet hat. Zwischen den Tabs können Sie mit Strg+B und dann N vor- und Strg+B und dann P zurückblättern. Darunter befinden sich beispielsweise hostapd, das den Access Point bereitstellt, der DHCP-Server dhcpd und der Webserver lighttpd für das Captive Portal. Wenn Airgeddon meldet, dass Ihnen das korrekte Passwort ins Netz gegangen ist, beenden Sie die Attacke im Hauptmenü mit Enter.

Bei den anderen Evil-Twin-Attacken geht es eher darum, zu spionieren und den Traffic des Opfers mitzuschneiden. Wählen Sie dazu aus dem Menü „Evil Twin AP attack with sniffing and bettercap-sslstrip2“. Die Funktionsweise ist ähnlich wie bei den anderen Angriffen, es braucht aber ein Netzwerk-Interface mit Internetzugriff, damit das Opfer im Internet surfen kann, etwa eth0 oder wlan0 des Raspi.

Auch bei diesem Angriff öffnet Airgeddon eine Reihe von Tabs, die Sie durchschalten können. Hier verfolgen Sie beispielsweise, welche Seiten aufgerufen werden. Wenn das Opfer Zugangsdaten auf Websites eingibt, die nicht TLS-verschlüsselt sind, schneidet Airgeddon sie mit. Airgeddon versucht bei dieser Attacke auch, mittels ssltrip2 die HTTPS-Anfragen zu HTTP umzuleiten, aber die meisten Browser und Clients sind inzwischen dagegen gefeit.

Hacker spannen böse Access Points besonders gerne an Orten wie Cafés auf, wo die Nutzer eher mit einem offenen Netz rechnen. Dass Sie öffentlichen Netzen nicht trauen sollten, hat sich inzwischen hoffentlich herumgesprochen, aber mit Airgeddon lässt sich demonstrieren, dass auch geschlossene Netzwerke anfällig für diese Art von Attacke sind. Wenn Sie in Ihrem Netzwerk-Manager über zwei Access Points mit der gleichen SSID stolpern, von denen einer kein Passwort verlangt, sind Sie vermutlich Zeuge einer Evil-Twin-Attacke.

Fazit

Mit Kali Linux und Airgeddon verwandeln Sie den Raspberry Pi im Handumdrehen in eine WLAN-Hacking-Station. Die hier demonstrierten Angriffe zeigen, warum drahtlose Netzwerke weiter ein attraktives Einfallstor für Cyberschurken sind. Richten Sie die gezeigten Hacks ausschließlich gegen eigene Netze oder Netze, für die Sie eine Erlaubnis eingeholt haben. *(ndi@ct.de)* **ct**

Downloads und Doku: **ct.de/ys2v**

1blu

12 .de-Domains inklusive!

Explosives Angebot: Homepage XL

12 .de-Domains inklusive

- 100 GB Webspace
- 1.000 E-Mail-Adressen
- 80 GB E-Mail-Speicher
- 80 MySQL-Datenbanken
- Kostenlose SSL-Zertifikate per Mausklick
- Viele 1-Klick-Apps inklusive
- Webbaukasten & Webkonferenzlösung

2,49 €/Monat*

Angebot gültig bis 30.11.2023!
Preis gilt dauerhaft.

* 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/xl**

Bild: Moritz Reichartz

Hacker-Terminal

Raspi 400 als Hacking-Rechner mit Kali Linux

Durch seine Tastatur ist der Raspberry Pi 400 der ideale Hacking-Rechner. Sie schließen nur noch Strom und Monitor an und können etliche Hacking-Tools von Kali Linux nutzen. Mit einem zweiten Raspi finden Sie auch gleich ein passendes Opfer.

Von Ronald Eikenberg

Der Raspi 400 versprüht einen ganz besonderen Charme, der Erinnerungen an die glorreichen Zeiten der Homecomputer von Commodore & Co. weckt. Im kompakten Tastaturgehäuse steckt ein Einplatinen-PC mit der Leistung eines Raspi 4 und vier GByte Arbeitsspeicher. Der Tastatur-PC ist ideal für Ihre ersten Schritte mit Kali Linux: Sie schließen nur noch Netzteil, Monitor und bei Bedarf eine Maus an und können sofort loshacken.

Auch einen anderen Raspi, den Sie vielleicht schon besitzen, können Sie zum Hacken mit Kali benutzen, da Kali Linux auf allen Generationen des Raspberry Pi sowie dem Raspberry Pi Zero läuft, nicht jedoch auf dem Raspi Pico. Wenn Sie die grafische Bedienoberfläche nutzen möchten, empfehlen wir einen Raspberry Pi 4 aufwärts mit möglichst viel RAM, denn je flinker der Raspi, desto flüssiger reagiert das GUI. Ältere Semester steuern Sie am besten über einen anderen Rechner fern, indem Sie via SSH auf den Raspi zugreifen.

Ein alter Raspi kann aber auch noch eine ganz andere Aufgabe auf Ihrem Weg zum Hacker übernehmen: Er stellt sich bereitwillig als Opfer zur Verfügung, an dem Sie sich mit den Hacking-Tools von Kali gefahrlos vertraut machen. Sie können einen Kali-Raspi einfach per WLAN mit einem Opfer-Raspi verbinden und so erste Praxiserfahrungen sammeln, ohne Angst zu haben, irgendwas kaputtzumachen, denn die beiden sind in einem eigenen Netz und haben von dort weder Zugriff auf Ihr Heimnetz noch auf das Internet. Der Opfer-Raspi stellt eine Reihe verwundbarer Dienste bereit, etwa eine steinalte Wordpress-Installation, damit Sie schnell erste Erfolge haben.

Los geht es mit der Einrichtung von Kali Linux. Hierzu laden Sie den Raspberry Pi Imager herunter, den es für Windows, macOS und Linux gibt (siehe ct.de/yspn). Installieren Sie das Tool und starten Sie es. Anschließend legen Sie eine microSD-Karte mit mindestens 16 GByte in den Kartenleser Ihres Rechners. Den Inhalt der Karte sollte Sie entbehren können, denn er wird gleich überschrieben. Klicken Sie anschließend links auf „OS WÄHLEN“ und wählen Sie unter „Other specific-purpose OS“ Kali Linux aus. Sie haben daraufhin die Wahl zwischen verschiedenen Images für die verschiedenen Raspis. Für modernere Modelle ab dem Raspi 2 nutzen Sie am besten „Raspberry Pi 2 (v 1.2), 3, 4 and 400 (64-bit)“.

Danach wählen Sie über den mittleren Knopf „SD-KARTE WÄHLEN“ ebendiese aus und starten den Schreibvorgang mit „SCHREIBEN“. Wenige Minuten später ist Ihre Speicherkarte mit Kali bespielt und einsatzbereit. Sie können die Karte jetzt in den Raspi stecken und ihn booten, indem Sie sein Netzteil anschließen. Da sich dieser Artikel an der grafischen Bedienoberfläche orientiert, sollten Sie auch noch Monitor und USB-Maus angeschlossen haben – und eine Tastatur, sofern Sie nicht den Raspi 400 einsetzen.

Kali einrichten

Der erste Start dauert etwas länger, da das System zunächst das Partitionsschema der Speicherkarte an die vorhandene Speicherkapazität anpasst. Wenn Sie nach Benutzernamen und Passwort gefragt werden, geben Sie bei beidem „kali“ ein. Kali wird mit einer Standardkonfiguration ausgeliefert, unter anderem ist das QWERTY-Tastaturlayout eingestellt. Sie sollten das System daher zunächst an die hiesigen Bedingungen anpassen.

Starten Sie hierzu den Terminal Emulator, zum Beispiel über das Startmenü oben links oder mit der Tastenkombination Strg+Alt+T. Rufen Sie das Konfigurationsprogramm mit dem Befehl `sudo kalipi-config` auf. Den Bindestrich geben Sie mit dem eingestellten US-Layout mit der ß-Taste ein, alternativ können Sie nach „sudo kalipi“ dreimal auf die Tabulatortaste drücken, um den Befehl vervollständigen zu lassen.

Wählen Sie im Config-Tool mit den Pfeiltasten die „Localisation Options“ und bestätigen Sie mit Enter. Hier arbeiten Sie sich von oben nach unten durch, begonnen bei „Change Locale“, um die Systemsprache zu ändern. Markieren Sie „de_DE.UTF-8 UTF-8“ mit der Leertaste, bestätigen Sie mit Enter und wählen Sie im nächsten Schritt erneut den Eintrag mit „de_DE“, um Deutsch als Systemsprache zu setzen. Die Änderung sollte ab dem nächsten Login aktiv sein. Bei der von uns getesteten Kali-Version 2023.3 klappte das nicht, möglicherweise haben die Entwickler diesen Bug aber bereits behoben, wenn Sie es ausprobieren.

Weiter geht es in den „Localisation Options“ mit „Change Timezone“. Wenn Sie sich in Deutschland aufhalten, wählen Sie „Europe“ und „Berlin“. Bei „Change Keyboard Layout“ belassen Sie es im ersten Schritt bei „Generic 105-key PC”, danach wählen Sie „Other/German/German“. Bei den folgenden drei Schritten passen wieder die vorgegebenen Antwortoptionen. Zu guter Letzt stellen Sie unter „Change Wi-fi Country“ noch „DE Germany“ ein, damit Ihr Raspi auf den in Deutschland zulässigen Frequenzen funkt. Wenn Sie das Tool über „Finish“ verlassen, wird Ihnen ein Neustart angeboten, den Sie erstmal ablehnen.

Denn im nächsten Schritt kümmern Sie noch um den schwarzen Trauerrand, der den Desktop einrahmt. Öffnen Sie mit dem folgenden Terminal-Befehl die Boot-Konfiguration: `sudo mousepad /boot/config.txt`. Entfernen Sie in Zeile 10 das Rautesymbol vor `disable_overscan=1`. Nachdem Sie die Datei gespeichert haben, können Sie mit `reboot` einen Neustart anstoßen, um die Änderungen zu übernehmen. Das System nutzt danach die volle Bildschirmfläche Ihres Monitors.

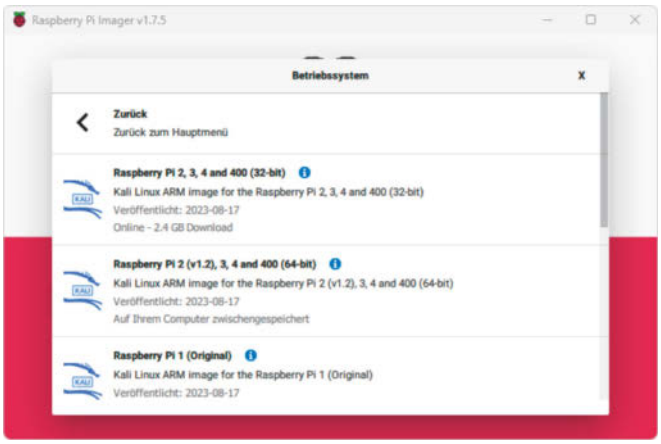
Tools auffrischen

Im Prinzip könnten Sie jetzt schon loshacken, aber da das heruntergeladene Kali-Image im Zweifel mehrere Wochen oder Monate alt ist, sollten Sie vorher noch das System und die mitgelieferten Tools auf den aktuellen Stand bringen. Das ist wichtig, weil die aktuellen Versionen der Tools häufig neue Funktionen mitbringen oder lästige Bugs beseitigen. Zum Aktualisieren benötigen Sie eine Internetverbindung. Schließen Sie entweder ein Netzwerkkabel an oder stellen Sie eine WLAN-Verbindung her, indem Sie auf das rechteckige Symbol oben rechts klicken, das wie eine Netzwerkbuchse aussieht. Wählen Sie unter „Available networks“ ein WLAN aus und tippen Sie das WPA-Passwort ein.

Danach rufen Sie die aktuellen Softwarepaketlisten ab, indem Sie den Befehl `sudo apt update` in den Terminal-Emulator tippen. Kommt es dabei zu einem Fehler, dann sind wahrscheinlich Datum oder Uhrzeit falsch eingestellt. Um das zu korrigieren, klicken Sie mit der rechten Maustaste auf die Uhrzeit in der oberen rechten Bildschirmecke und auf „Properties / Time and Date Settings.../Unlock“. Danach können Sie Datum und Zeit ändern.

Um die vorhandenen Updates zu installieren, geben Sie schließlich `sudo apt full-upgrade -y` ein. Danach können Sie sich erstmal einen Kaffee holen, da die Installation einige Zeit in Anspruch nimmt. Die Dauer ist abhängig von der Anzahl der verfügbaren Updates sowie der Geschwindigkeit von Raspi, Speicherkarte und Internetverbindung. Bei uns dauerte die Installation von rund 900 Updates eine gute halbe

Der Tastatur-Raspi 400 eignet sich hervorragend als Hacking-Maschine. Er kostet 80 Euro und ist so flink wie ein Raspi 4.



Der Raspberry Pi Imager schreibt das Hacking-Linux Kali in Minuten auf Ihre Speicherkarte.

Stunde. Abschließend sollten Sie sicherheitshalber noch einen Neustart durchführen. Danach ist Kali startklar. Über das Startmenü finden Sie die wichtigsten Hacking-Tools, einsortiert in Kategorien wie „05 - Password Attacks“, „07 - Reverse Engineering“ oder „09 - Sniffing & Spoofing“.

Die erste Programmkategorie ist nicht ohne Grund „01 - Information Gathering“, also die Informationsbeschaffung. Dies ist für einen Pentester, also einen Berufshacker, normalerweise der erste Schritt. Er versucht über sein Ziel so viel wie möglich herauszufinden. Dabei sucht er vor allem nach Systemen im Netz, die sich als Angriffsziel eignen könnten, etwa weil sie schlampig konfiguriert wurden oder Sicherheitslücken besitzen.

Um die Tools zu testen, benötigen Sie erstmal ein Ziel. Lassen Sie die Tools unter keinen Umständen auf fremde Systeme los, da Sie damit mit hoher Wahrscheinlichkeit gegen Gesetze verstoßen und sich juristischen Ärger einhandeln können. Es spricht jedoch nichts dagegen, im Heimnetz nach verwundbaren Geräten zu scannen, um diese gezielt absichern oder aus dem Verkehr ziehen zu können. Noch besser ist ein Testnetz, in dem Sie nichts kaputtmachen können.

Raspi vs. Raspi

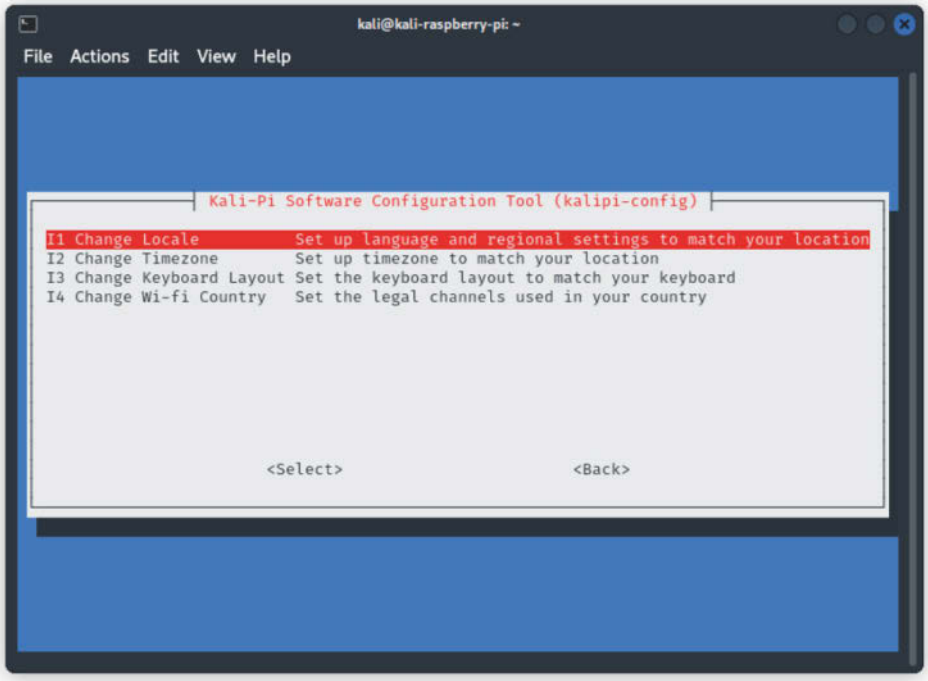
Wie eingangs erwähnt, eignet sich ein zweiter Raspi hervorragend als Angriffsziel. Mit dem Raspi-Image RasPwn OS für den Raspi 3 Model B (alternativ Raspi 2 B plus USB-WLAN-Adapter) schlagen Sie gleich mehrere Fliegen mit einer Klappe: Es spannt automatisch ein Test-WLAN auf, in dem sich auch schon zahlreiche verwundbare Dienste tummeln. Zur Installation laden Sie RasPwn einfach herunter (siehe ct.de/yspn), entpacken die Image-Datei und spielen Sie mit dem Raspberry Pi Imager auf eine Speicherkarte. Sie können das Image laden, indem Sie bei der Betriebssystemauswahl ganz unten „Eigenes Image“ wählen.

Danach müssen Sie die Karte nur noch in den Opfer-Raspi stecken und ihn mit Strom versorgen. Sobald Sie sich mit dem RasPwn-WLAN verbunden haben (SSID: „RasPwn OS“, Passwort: „In53cur3!“), können Sie über die Adresse http://playground.raspwn.org/ die verwundbaren Webdienste einsehen, zudem laufen in dem Testnetz angreifbare Server für Mail, SMB, SSH und vieles mehr.

Zurück zur Informationsbeschaffung: Wenn Sie sich in einem geeigneten Netz befinden, sollten Sie sich dort erstmal umsehen. Finden Sie mit `ifconfig` heraus, welche IP-Adresse Kali bekommen hat, um Ihre Netzwerknachbarn zu finden. Hierfür hat sich der Netzwerkscanner `nmap` bewährt. Lautet Ihre IP-Adresse zum Beispiel 192.168.99.145, scannen Sie mit dem folgenden Befehl das ganze /24-Subnetz, also die IPs von 192.168.99.1 bis .254:

```
nmap 192.168.99.0/24 --stats-every 5s
```

Der Anhang `--stats-every` bewirkt, dass Sie nmap regelmäßig über den Fortschritt informiert und nicht erst am Ende. Nach kurzer Zeit liefert Ihnen der Netzwerkscanner einen Bericht über die gefundenen Hosts, der nicht nur deren IP-Adressen offenbart, sondern auch, auf welchen Ports die Hosts lauschen. Hinter diesen Ports stecken mit hoher Wahrscheinlichkeit Serveranwendungen, die man näher untersuchen kann.



Mit kalipi-config ändern Sie nach dem ersten Start die Tastaturbelegung auf QWERTZ.

Hacking ganz einfach

nmap ist kein simpler Netzwerkscanner, sondern kann auch Berichte generieren und Skripte abarbeiten, die etliche Funktionen bereitstellen. In c’t 23/2021 [1] gehen wir näher darauf ein. Um diese Extras zu nutzen, müssen Sie sich in die Syntax hineinfuchsen. Unter Kali gibt es jedoch einen deutlich leichteren Weg: In Kategorie 01 des Startmenüs finden Sie das Tool legion, das nmap und weitere interessante Tools über eine grafische Oberfläche bedienbar macht und sinnvoll miteinander verknüpft.

Nach dem Start von legion klicken Sie auf den Plus-Button, um ein Angriffsziel hinzufügen, etwa die bereits genutzte IP-Range 192.168.99.0/24. Nach einem Klick

auf „Submit“ macht sich das Tool gleich ans Werk und setzt nmap auf das Ziel an. Das können Sie unten bei „Processes“ live mitverfolgen. Bei einem einfachen Scan bleibt es aber nicht, legion versucht unter anderem herauszufinden, welche Server-Software hinter den entdeckten Ports steckt, und fertigt Screenshots von Webanwendungen an.

Die gefundenen Hosts listet das Tool oben links auf. Wenn Sie einen davon auswählen, finden Sie rechts daneben die dazugehörigen Ports und Dienste. Weitere potenziell spannende Ergebnisse warten auf den darauffolgenden Tabs auf Sie: Unter „Scripts“ etwa finden Sie die Ausgaben von nmap-Skripten und unter „Information“ eine allgemeine Zusammenfassung über den Host. „Notes“ bietet Ihnen Raum für eigene Notizen, und etwaige Screenshots tauchen auch als Tabs auf.

Zurück auf dem ersten Tab „Services“ bietet Ihnen legion per Rechtsklick auf einen Dienst jeweils passende Tools und Skripte an, die Sie per Klick ausführen können. Besonders groß ist die Auswahl bei Webservern. Hier können Sie auf dem Webserver zum Beispiel mit dirbuster oder nikto nach Unterverzeichnissen suchen oder eine WordPress-Installation mit wpscan auf Sicherheitslücken und Konfigurationsfehler abklopfen.

Nur der Anfang

Dieser Artikel kann nur an der Oberfläche kratzen, denn über Kali und die mitgelieferten Tools – für Webangriffe, Funkattacken, Forensik und vieles mehr – kann man mühelos viele Bücher schreiben. Wenn Sie auf den Geschmack gekommen sind, finden Sie in c’t 23/2021 Informationen über einige weitere Tools und deren Bedienung. Dort erfahren Sie zum Beispiel, wie Sie ein vergessenes Zip-Passwort mit John The Ripper knacken oder die Sicherheit Ihres WLAN-Passworts mit wifite überprüfen.

Weitere Starthilfe leistet die Kali-Dokumentation, die Sie bei bestehender Onlineverbindung über die eingestellte Firefox-Startseite erreichen. Unter ct.de/yspn haben wir die Tool-Übersicht von Kali verlinkt, die Funktion und Bedienung der Tools erklärt. Sollten Sie einmal ein bestimmtes Hacking-Tool benötigen, das nicht vorinstalliert ist, können Sie in den Kali-Repositories danach suchen: `apt search [toolname]`. Werden Sie fündig, installieren Sie es mit `sudo apt install [toolname]` nach. Werfen Sie auch einen

Die Qual der Wahl: Kali Linux bringt etliche Hacking-Tools mit.

Blick auf das Hilfsprogramm `kali-tweaks`, mit dem Sie zum Beispiel diverse Sicherheitseinstellungen feinjustieren können oder gleich ganze Tool-Pakete für bestimmte Anwendungsfälle nachrüsten, etwa für Bluetooth-Angriffe.

Fazit

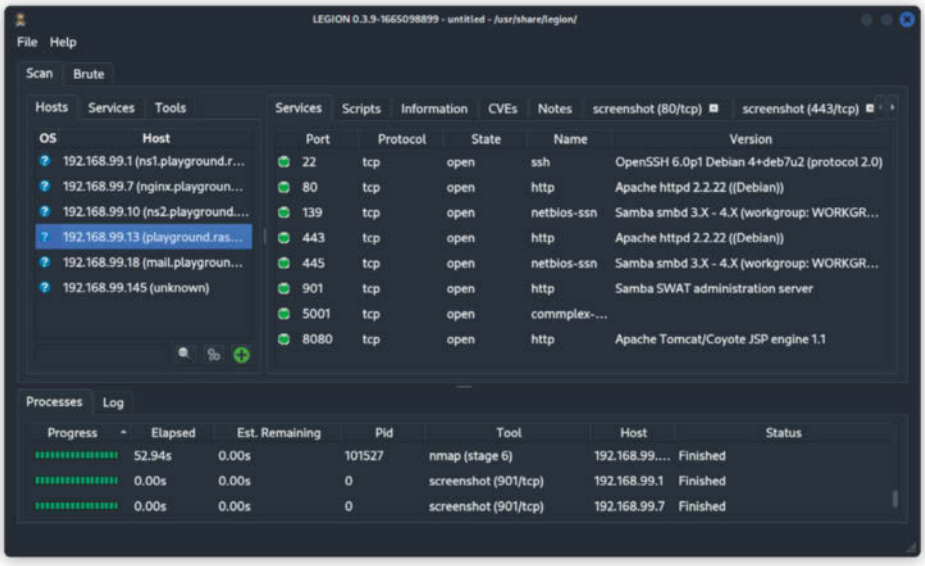
Der Raspi 400 ist das ideale Sprungbrett in die Welt der Hacker. Der Tastatur-PC für rund 80 Euro ist flott genug für Kali Linux und sofort einsatzbereit. Für rund 30 Euro Aufpreis gibt es ihn auch als Kit mit Netzteil, Speicherkarte, HDMI-Kabel und Maus. Das ist ein praktisches Weihnachtsgeschenk – und falls der oder die Beschenkte kein Interesse an IT-Security hat, findet sich ganz sicher eine andere Beschäftigung für den Raspi, da er mit vielen Raspi-Projekten kompatibel ist.

Wer bereits einen Raspi besitzt, kann darauf ebenfalls Kali installieren und erste Erfahrungen mit Hacking-Tools sammeln. Bietet sich dann noch ein alter Raspi 3B oder 2B als Übungsziel an, hat man eine geschlossene Trainingsumgebung, in der man sich beliebig austoben kann, ohne Schaden anrichten zu können. *(rei@ct.de)* c't

Literatur

[1] Ronald Eikenberg, Alexander Königstein, Gute Tools, böse Tools, Hacking-Werkzeug für Fortgeschrittene, c’t 23/2021, S. 24

Downloads & Doku: ct.de/yspn



Legion findet Server im Netzwerk und bietet anschließend passende Hacking-Tools an, die man darauf ansetzen kann.

Photovoltaik-baukasten

Große Solaranlagen zur Selbstmontage

Im Angesicht der Preisanstiege für PV-Anlagen geht der Trend zur Eigenleistung. Das hat auch der Leipziger Balkonkraftwerkanbieter Priwatt erkannt und sein Angebot erweitert.

Von Andrijan Möcker

Die Solarbranche boomt wie seit zehn Jahren nicht mehr und wer jetzt eine Anlage installiert haben möchte, sieht sich häufig mit saftigen Preisen und langen Wartezeiten auf Handwerker konfrontiert. Immer mehr Menschen greifen in Konsequenz selbst zum Akkuschrauber. Deswegen erweitert der Leipziger Balkonkraftwerkanbieter Priwatt sein Angebot um größere Photovoltaikanlagen zum Eigenbau.

Kern des „priwatt Solar“ genannten Angebots ist ein Webkonfigurator, mit dem Kunden in sogenannten Modulgruppen definieren, wie viele jeweils zusammenhängende Modulfelder in welcher Orientierung sie installieren möchten. Daraus leitet Priwatt das nötige Material für das Set ab: Definiert der Heimwerker etwa zwei Modulgruppen, um rechts und links einer Gaube jeweils sechs Module zu errichten sowie eine weitere für die Fassade, bekommt er dafür geeignetes und ausreichendes Installationsmaterial angeboten.

Bis zu 25 Module

Derzeit erlaubt der Konfigurator für ein Anlagenset 5 bis 25 Module über alle Modulfelder hinweg. Priwatt liefert ausschließlich zweiseitige (bifacial) Glas-Glas-Module mit 420 Watt Spitzenleistung vom chinesischen Hersteller Jolywood (HD108N-11BB). Der Modulhersteller gibt 30 Jahre Leistungs- und 25 Jahre Produktgarantie.

Die Wechselrichter der Sets kommen aus Huaweis SUN2000-Serie; das Modell wählt Priwatt abhängig von der zu installierenden Solarleistung: Bis 4,6 Kilowatt kommen einphasige Modelle infrage. Darüber liefert Priwatt die dreiphasigen 6- oder 8-kW-Modelle.

Alle zur Wahl stehenden Wechselrichter haben einen Speicheranschluss und im Konfigurator kann man sich wahlweise für einen 5-, 10- oder 15-Kilowattstunden-Speicher entscheiden. Der Smart Power Sensor, ein Digitalzähler für die Hutschiene, ist ebenso im Lieferumfang. Er wird zwischen Zähler und Hausinstallation geschaltet und teilt dem Wechselrichter mit, wie viel das Gebäude gerade bezieht oder liefert, damit dieser das Ein- und Ausspeichern steuern kann.

Preise

Priwatts Sets beginnen ab etwa 1400 Euro für fünf Module ohne Unterkonstruktion mit Wechselrichter und gleichspannungsseitigem Installationsmaterial. Bucht man eine Unterkonstruktion für Schindeldächer dazu, steigt der Basispreis auf rund 1600 Euro. Der kleinste Speicher mit 5 Kilowattstunden erhöht den Setpreis um 4000 Euro.

Wer ein großes Vorhaben plant und 25 Module in einer Modulgruppe sowie 15 Kilowattstunden Speicher bestellt, zahlt rund 15.300 Euro. Teilt man die Module auf weitere Gruppen auf, steigt der Preis entsprechend, da für weitere Modulgruppen extra Installationsmaterialien, etwa längere Verbindungskabel, notwendig sind.

Auf den Setpreis kommen noch 90 Euro Versandkosten. Die Speicher, Module und Unterkonstruktion sind schweres Sperrgut.

Grundlegende Handreichungen

Priwatts Angebot richtet sich an Heimwerker, die selbst planen. Denn während das Unternehmen einen Großteil der nötigen Photovoltaik-Hardware liefert, sind die Planungs- und Sicherheitshinweise auf der Website relativ wenig ausführlich und nur grundlegend. Um die Statik, das nötige Werkzeug und das korrekte Verlegen der Kabel beispielsweise muss man sich selbst kümmern.

Aktuell obliegt einem auch, einen Elektriker zu finden, der die Anlage mit dem Stromnetz verbindet und beim Netzbetreiber anmeldet, denn das darf nach geltendem Recht (§ 13 Abs. 2 Niederspannungsanschlussverordnung) nur von einem beim Netzbetreiber eingetragenen Elektrofachbetrieb erledigt werden.

Weil Elektriker jedoch schwer aufzutreiben sind, will Priwatt seinen Kunden dabei künftig mit einem Partnerunternehmen zur Hand gehen. Dieses soll die wechselspannungsseitige Installation übernehmen. Wann Priwatt diesen Vermittlungsdienst aufnimmt und mit welchem Partner, konnte das Unternehmen auf Nachfrage von c’t nicht sagen.

(amo@ct.de) c't

Bild: Priwatt

Priwatts Webkonfigurator baut aus Angaben zu gewünschten Modulgruppen einen Warenkorb mit dem dafür benötigten Installationsmaterial zusammen.

Wunderheizer

Abzocke mit billigen Heizlüftern

Pünktlich zur Heizsaison versuchen dubiose Händler, vorgebliche Wunderheizgeräte mit falschen Versprechen zu verkaufen. Doch die Geräte sind Ramsch.

Von Andrijan Möcker

Die Heizsaison beginnt und gerade in Deutschland, das in puncto Energie eines der teueren Länder der Welt ist, wird das Thema sparsam heizen jedes Jahr aufs neue aktuell. Das scheinen auch einige Händler ohne moralischen Kompass auf dem Schirm zu haben, denn derzeit häufen sich im Netz wieder die Werbeanzeigen für vermeintliche Wunderheizgeräte, die die Wohnung „zum Nulltarif“ auf Temperatur bringen sollen.

Dabei wird häufig böswillig getäuscht, um Kunden zum Kauf zu überreden: Wir stießen bei YouTube auf die Werbeanzeige des „SmartEco“. Der Wunderheizer wurde angeblich von zwei schwedischen Ingenieuren entwickelt, nachdem diese eine Methode gefunden hatten, äußerst günstig elektrisch zu heizen. Der SmartEco sei über zwei Jahre ausführlich getestet worden und werde nun mit großen Rabatten verkauft, damit jeder von der Erfindung profitieren könne. Um „Wärme wie nie zuvor zum Nulltarif [zu] erleben“, müsse man nur das 84 Euro teure Heizgerät bestellen.

Wir fanden weitere dubiose Angebote, wie etwa die „Deutsche Mini-Wandheizung“, ein Steckdosengerät, etwas größer als ein WLAN-Repeater. Die Versprechen der Angebote laufen immer auf dasselbe hinaus: günstiges Heizen zum kleinen Preis.

Ob Nutzer auf die Angebote hereinfallen, ist sicher eine Frage der Medienkompetenz und der Lockmittel. Nicht selten sind die Werbevideos und Websites gut gemacht und zusätzlich mit erfundenen Positivbewertungen und Referenzen auf angebliche Berichterstattungen in Medien gespickt. Fehlende technische Details zum Gerät und ein unvollständiges Impressum verraten die Abzockabsicht jedoch.

Alibaba-Ware

Technische Details zu den Geräten fanden wir zwar nicht auf den Abzocke-Websites, dafür aber auf der asiatischen Großhandelsplattform Alibaba. Tatsächlich verstecken sich hinter den Wunderheizgeräten simple Heizlüfter mit Keramikheizelement. Die Technik existiert seit den Achtzigerjahren und ist nichts Neues: Sie wandelt die elektrische Leistung eins zu eins in Wärme um, ist also weitaus weniger effizient als eine Wärmepumpe, die typischerweise mit einer Kilowattstunde Strom vier Kilowattstunden Wärme aus der Luft holt.

Der „SmartEco“ ist mit seinen 1200 Watt Ausgangsleistung also alles andere als „eco“ und auch der tatsächliche Preis dürfte sauer aufstoßen lassen: Gerade mal 6,50 US-Dollar verlangt der Originalhersteller für das (keineswegs wundersame) Gerät, zuzüglich Zoll und Versand. Einen Heizlüfter, der dem SmartEco optisch gleicht, haben wir für 25 Euro bei Amazon erworben. Die „Deutsche Mini-Wandheizung“ für 45 Euro kostet bei Alibaba unter anderem Namen bei größeren Stückzahlen sogar keine zwei US-Dollar.

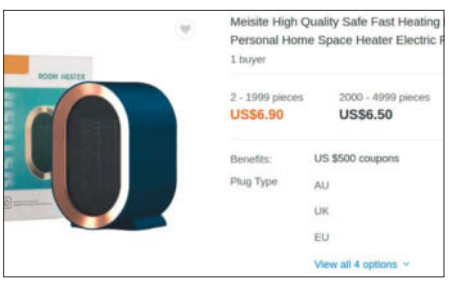
Woher die „Angebote“ genau kommen, lässt sich anhand der Websites und Werbeanzeigen nicht sagen. Ein korrektes Impressum haben die Seiten nicht und meist läuft das Hosting über Provider, bei denen die Website-Betreiber unerkannt bleiben.

Kostenfalle

Was den Verkäufern riesige Gewinne beschert, lässt Ahnungslose durch unbekümmertes Heizen in eine Kostenfalle laufen: Laut Statistischem Bundesamt kostete die Kilowattstunde Strom deutsche Privathaushalte im ersten Halbjahr 2023 im Durchschnitt 42,29 Cent. Eine Kilowattstunde aus Öl oder Erdgas lag dagegen bei 9 bis 15 Cent.

Rechnet man mit den 1200 Watt des „SmartEco“, kosten 180 Tage Heizen bei acht Stunden täglichem Betrieb rund 730 Euro, und das für nur einen Raum. Grund genug, nicht nur vor Abzocke zu warnen, sondern elektrische Heizgeräte höchstens als kurzfristigen Notnagel bei Heizungsausfall zu verwenden. Andernfalls reißt einem die böse Überraschung auf der Stromrechnung ein großes Loch in den Geldbeutel. *(amo@ct.de)* c't

Mit falschen Behauptungen versuchen Verkäufer, Billigware teuer zu verkaufen. Der „Nulltarif“ dieses Geräts (1,2 kW Leistungsaufnahme) kostet in Deutschland im Schnitt rund 51 Cent pro Stunde.



Der 84 Euro teure „SmartEco“ kostet bei Alibaba rund 6 Euro.

Biochip für die künstliche Netzhaut der Zukunft

Aus flexiblen, elektrisch leitenden Polymeren und lichtempfindlichen Molekülen besteht ein erster Prototyp einer künstlichen Netzhaut. Die Bioelektronik kann auch künstliche Nervenzellen bilden oder als Hardwareplattform für KI dienen.

Ein Forscherteam um Francesca Santoro am Forschungszentrum Jülich, an der RWTH Aachen und der Universität Neapel hat einen Biochip entwickelt, der sowohl die Netzhaut als auch deren Verbindung zum Sehnerv nachbildet. Dem Chip liegt ein neuartiger organischer Halbleiter zugrunde, der erkennt, wie viel Licht auf ihn fällt. Er ist verformbar und besteht ausschließlich aus nicht toxischen Komponenten.

Anders als übliche Halbleiterchips aus Silizium, die mit elektrischen Strömen in Form fließender Elektronen funktionieren, entstehen im organischen Halbleiter Ionen, also geladene Moleküle, mit denen der Chip mit Körperzellen kommunizieren kann.

Der neue Biochip stellt zunächst einen Proof of Concept dar. Die Forscher zeigen damit, dass ihr Material die Eigenschaften einer Netzhaut nachahmen kann. Es ermöglicht nicht nur, einfallende Lichtstrahlen auf molekularer Ebene zu detektieren, sondern dient auch als Basis dafür, die Zellschichten einer Netzhaut zu emulieren. Entsprechend dem Lichteingang aktiviert der Chip seine Elektrolytkanäle und kann so die optischen Informationen an die darunterliegenden Nerven der Sehbahn weiterleiten.

Zudem entdeckten die Forscher, dass ihr organischer Halbleiter auch geeignet ist, künstliche Synapsen zu bilden. Sie bildeten mit den Biopolymeren die baumartigen Verästelungen von Nervenzellen nach. Es zeigte sich, dass die künstlichen Synapsen ihre Größe und Leistungsfähigkeit langfristig steigern, je mehr elektrische Signale sie weiterleiten. In kommenden Arbeiten wollen die Forscher ihre organischen Halbleiter mit biologischen Zellen koppeln. *(agr@ct.de)*

Forschungsarbeiten: ***ct.de/yed6***

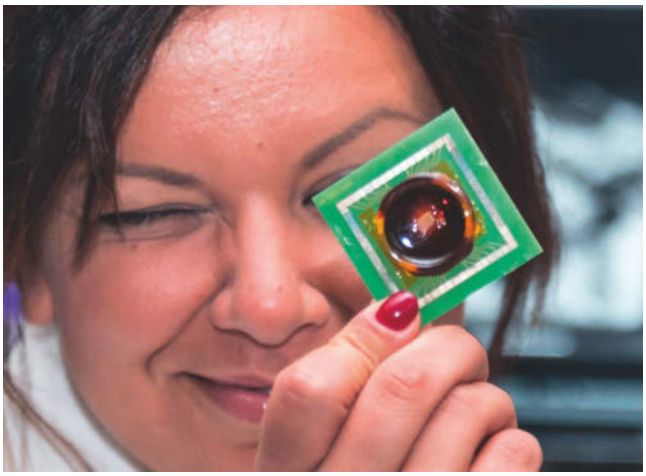


Bild: Istituto Italiano di Tecnologia

Forscherin Francesca Santoro hat einen Meilenstein gesetzt und zeigt einen lichtempfindlichen Chip, der sich über Ionen direkt mit Nervenzellen austauschen kann.

Intelligenter Drohnenhangar

Für ein **drohnengestütztes Rettungssystem** haben Forscher der TU Chemnitz und der TU Dresden mit Partnern im Projekt RescueFly einen autonomen Drohnenhangar entwickelt. Im Oktober 2023 demonstrierte die Gruppe um Wolfram Hardt den Einsatzfall am Partwitzer See in Sachsen. Der Hangar prüft das Wetter vor Ort und öffnet sich dann innerhalb von fünf Sekunden automatisch. Bei der Vorführung flog die im Standby wartende Drohne dann zum Einsatzort, machte in einer simulierten Notfallsituation einen Ertrinkenden ausfindig, warf einen Schwimmkörper ab und übermittelte die genauen Positionsdaten.

Bild: Jacob Müller / TU Chemnitz

Der autonome Drohnenhangar öffnet und schließt sich automatisch, begutachtet die Drohne nach einem Einsatz und lädt sie wieder auf.

Nach ihrer Rückkehr lädt die Drohne autonom auf. Der Hangar schließt sich automatisch wieder. Sechs Kameras mit Ringlicht liefern gut ausgeleuchtete Bilder für die Inspektion der Drohne durch eine künstliche Intelligenz. So kann der Hangar etwa Rotorschäden erkennen oder ausschließen. Ist alles in Ordnung, meldet der Hangar die Drohne wieder einsatzbereit an die Rettungsleitstelle. *(agr@ct.de)*

Wohnhäuser energieautark?

Angesichts der Leistungsfähigkeit photovoltaischer Technik könnten Eigentümer bereits heute **53 Prozent der Einfamilienhäuser in Europa** unabhängig von Strom- und Wärmenetzen betreiben. Technische Verbesserungen könnten diesen Anteil bis 2050 sogar auf 75 Prozent steigern. Das besagt eine Studie, die eine Gruppe um Max Kleinebrahm am Karlsruher KIT und in Partnerinstituten erstellt haben.

Als Grundlage diente ihnen eine Datenbank, die geografisch hoch aufgelöst den Gebäudebestand und die Haushaltsgrößen sowie die klimatischen Bedingungen verzeichnet. Die Forscher untersuchten 4000 repräsentative Beispielhäuser und rechneten ihre Ergebnisse auf 41 Millionen Einfamilienhäuser in Europa hoch. *(agr@ct.de)*

GitHub: KI-Helfer Copilot Chat erscheint im Dezember

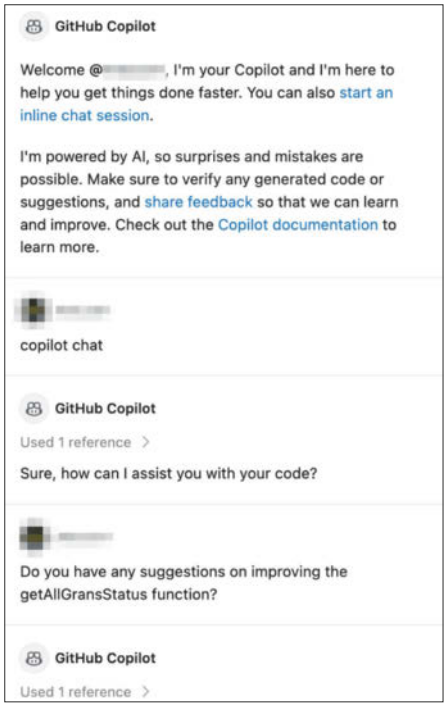
GitHub hat neue Funktionen für seine Onlineplattform angekündigt und stellt dabei KI in den Mittelpunkt.

Bei seiner Entwicklerveranstaltung Universe hat GitHub neue Funktionen angekündigt und trägt dabei dick auf. So wie GitHub einst auf Git aufgebaut wurde, sei künstliche Intelligenz das neue Fundament. Herzstück der Strategie ist GitHub Copilot, der in der ersten Version mit Autovervollständigungen beim Programmieren helfen konnte. Aktuell in der Testphase befindet sich Copilot Chat auf Basis von GPT-4 – ein virtueller Helfer, mit dem man sich unterhalten kann, der Arbeitsaufträge erledigt und den Kontext des geöffneten Programms kennt.

Im Dezember 2023 soll die Testphase enden und die Funktion allen Copilot-Kunden zur Verfügung stehen. Neu in die Testphase schickt GitHub eine Integration des KI-Gehilfen in die Entwicklungsumgebungen von JetBrains. Außerdem soll Copilot Einzug in die Weboberfläche github.com und in die Mobil-Apps halten. Interessierte für die Testphase können sich in eine Warteliste eintragen (siehe ct.de/y2jb).

Damit Copilot den Kontext eines Entwicklungsprojekts besser verstehen und weitere Werkzeuge im Kontext nutzen kann, hat GitHub eine Kooperation mit anderen Unternehmen gestartet. Unter anderem machen Postman, Hashicorp und Datadog mit und bringen Copilot die Funktionsweise ihrer Anwendungen bei. *(jam@ct.de)*

***Warteliste:* ct.de/y2jb**



Githubs Copilot Chat kennt den Kontext eines Entwicklungsprojekts, beantwortet Fragen und verfasst neuen Code.

Kurz & knapp

Der **Cinnamon-Desktop soll in seiner nächsten Version erstmals Wayland unterstützen**. Zahlreiche Funktionen werden der Version allerdings noch fehlen, die Entwickler raten vom produktiven Einsatz der Wayland-Sitzung ab. Erscheinen soll Cinnamon 6.0 gemeinsam mit Linux Mint Ende 2023.

Das fürs Jahresende angekündigte **Elementary OS 8** wird sich auf Ubuntu 24.04 LTS stützen und standardmäßig die moderne Linux-Grafikarchitektur Wayland einsetzen.

Der schlanke **Linux-Desktop LXQt ist in Version 1.4** erschienen. Verbessert wurden beispielsweise der Dateimanager PCManFM, die Terminalemulation QTerminal und der Bildbetrachter.

Die neue Version des **Anonymisierungs-Linux Tails 5.19** ermöglicht eine bessere Kontrolle für die Onion-Circuits des Tor-Netzes. Langsame oder problematische Circuits können damit ausgeschlossen werden. Außerdem aktualisiert die neue Version die Kernkomponenten der Distribution und weitere Software.

Staaten wollen mehr KI-Regulierung

28 Länder wollen bei der Entwicklung und Regulierung von KI enger zusammenarbeiten. Derweil hat US-Präsident Joe Biden Richtlinien für die KI-Nutzung erlassen.

Vertreter zahlreicher Länder haben im Rahmen eines „AI Safety Summit“ auf dem historischen britischen Landsitz Bletchley Park eine Absichtserklärung für mehr Zusammenarbeit bei der Entwicklung und Regulierung von künstlicher Intelligenz (KI) unterzeichnet. Die Regierungsvertreter, darunter der deutsche Minister für Digitales und Verkehr Volker Wissing (FDP), verweisen in der „Bletchley Declaration“ auf die Chancen und Risiken der KI-Technologie. Zu den 28 Unterzeichnern gehören neben europäischen Ländern auch Staaten wie Brasilien, Kanada, die USA, Kenia, Saudi-Arabien und China.

Zuvor hatte US-Präsident Joe Biden eine sogenannte Executive Order erlassen, in der er Richtlinien für KI festlegt. Sie verpflichtet Entwickler, ihre KI-Modelle vor der Veröffentlichung in den USA zu testen und die Ergebnisse den Behörden mitzuteilen; zumindest solche Systeme, die eine Gefahr für die nationale Sicherheit, die Wirtschaft oder die öffentliche Gesundheit darstellen können. Konkret geht es darum, dass Unternehmen reale Bedrohungsszenarien zur Absicherung der Systeme nachstellen müssen. *(jo@ct.de)*

Foto: Soeren Stache/dpa

Der britische Premierminister Rishi Sunak (Bildmitte) lud zum AI Safety Summit. Links im Bild die US-amerikanische Vizepräsidentin Kamala Harris, rechts die italienische Regierungschefin Giorgia Meloni und António Guterres, der Generalsekretär der Vereinten Nationen.

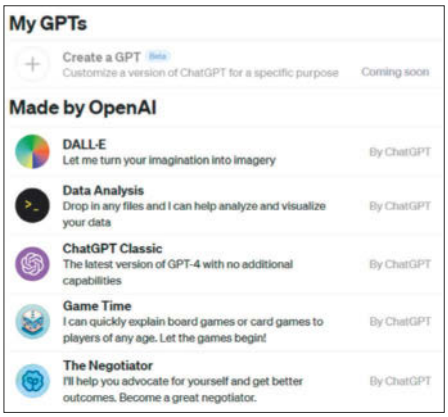
Große KI-Modelle: sehr intransparent

Ein Team aus Forschern der Universitäten Stanford, MIT und Princeton hat einen **Transparenzindex für Foundation Models** erstellt, also für große KI-Modelle. Anhand von 100 Faktoren – von den Datenquellen über die Architektur bis zur Lizenz – bewertet es zehn bekannte Modelle wie GPT-4, Stable Diffusion 2 und PaLM 2. Die Ergebnisse ernüchtern: Die Spitzenreiter erreichen einen Score, der nur knapp über 50 Prozent liegt, die rote Laterne trägt Amazons Titan Text mit einem Score von gerade einmal 12 Prozent. *(jo@ct.de)*

ChatGPT aufgebohrt

OpenAI hat bei einer Entwicklerkonferenz zwei neue, Turbo genannte Versionen seiner Sprachmodelle GPT-3.5 und GPT-4 vorgestellt. Vor allem GPT 4 wurde aufgebohrt: **GPT-4 Turbo** wurde mit Daten bis zum April 2023 trainiert – alle bisherigen GPT-Modelle kennen nur Informationen bis zum September 2021. GPT-4 Turbo kann zudem Kontexte mit bis zu 131.072 Token (128K) auswerten, also viermal so viele wie GPT-4. Der größere Kontext schlägt auch auf den von GPT-4 Turbo abgeleiteten Chatbot ChatGPT durch.

Kunden sollen zukünftig ihre eigenen ChatGPT-Bots bauen können, sogenannte GPTs. Programmierkenntnisse seien laut OpenAI dafür nicht erforderlich, Nutzer passen ChatGPT per Dialog an und füttern die Bots mit individuellen Informationen. GPTs sollen über Programmierschnittstellen auf externe Datenquellen zugreifen können. Entwickler können ihre GPTs in einem Store veröffentlichen. *(jo@ct.de)*



OpenAI hat schon einige GPTs bereitgestellt; eigene ließen sich bis Redaktionsschluss nicht bauen.

Kurz & knapp

Ein Team rund um Ben Zhao, Professor an der University of Chicago, hat ein **neues Tool für Künstler** entwickelt: Nightshade. Die sollen damit für Menschen unsichtbare Änderungen an den Pixeln ihrer Kunstwerke vornehmen können, bevor sie diese online hochladen. Gelangen sie dann als Trainingsdaten in ein bildgenerierendes Sprachmodell, soll dies dazu führen, dass das resultierende Modell auf chaotische und unvorhersehbare Weise gestört wird.

Elon Musks Unternehmen xAI hat ein eigenes **Sprachmodell namens Grok** angekündigt. Seine Größe hat xAI nicht bekannt gegeben, nur dass sein Vorläufer 33 Milliarden Parameter umfasste. Der begrenzte Vorabzugang ist auf verifizierte X-Nutzer in den Vereinigten Staaten begrenzt.

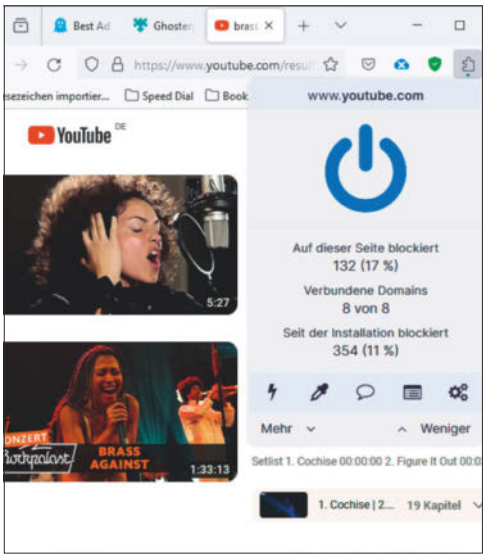
Gut 50 Jahre nach ihrer Auflösung haben die **Beatles** Anfang November den Song „Now and Then“ veröffentlicht. Er enthält auch die Stimme von John Lennon, der 1980 erschossen wurde. Sie wurde dafür mit Hilfe von KI aus alten Demo-Aufnahmen extrahiert.

YouTube: Preiserhöhung und Werbeblocker-Blockade

Google erhöht die Abopreise für das werbefreie Premium-Abonnement von YouTube. Die Preiserhöhungen gehen mit verstärkten Maßnahmen gegen Werbeblocker einher.

Einzelpersonen zahlen für YouTube Premium künftig 13 statt wie bisher 12 Euro pro Monat. Familienabos, die man sich mit bis zu fünf weiteren Personen teilen kann, kosten künftig 24 statt wie bisher 18 Euro.

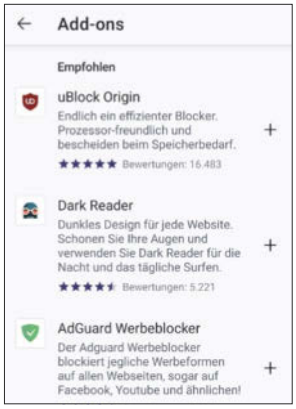
Viele Anwender, die auf der Plattform Videos mit aktiviertem Werbeblocker anschauen möchten, bekommen derzeit Warntafeln angezeigt. Nach einigen Videos kann es passieren, dass sie nicht mehr weiterschauen können. Damit scheint Google Erfolg zu haben, wie das US-Magazin Wired unter Berufung auf Zahlen aus der Branche berichtet. Demnach haben Hunderttausende Menschen ihre Werbeblocker deinstalliert. *(jo@ct.de)*



Wer einen Werbeblocker wie uBlock Origin nutzt, riskiert, dass er nicht mehr weiterschauen darf.

Hunderte Add-ons für mobilen Firefox

Mit der nächsten Version 120, die im Dezember erscheint, soll die **Android-Version von Firefox** ein offenes Ökosystem für Browsererweiterungen erhalten. Bisher stehen nur knapp zwei Dutzend beliebter Add-ons von Anbietern zur Verfügung, mit denen Mozilla zusammenarbeitet. Ab Firefox 120 sollen dann die Add-ons aus der Desktopversion auch mobil genutzt werden können. Entwickler müssen ihre Erweiterungen für die Nutzung unter Android allerdings anpassen. Zum Start im Dezember sollen rund 200 Erweiterungen für den mobilen Browser bereitstehen. *(jo@ct.de)*



Bislang stehen im mobilen Firefox nur knapp zwei Dutzend Add-ons zur Verfügung.

Brave Browser erhält KI-Assistenten

Brave Software hat seinem gleichnamigen Browser einen **KI-Assistenten namens Leo** verpasst. Er lässt sich über die Adresszeile oder über die Seitenleiste des Browsers starten und fasst Webseiten zusammen, transkribiert Videos und beantwortet allgemeine Fragen.

In einer kostenlosen Version nutzt Leo Metas Open-Source-Modell Llama 2 mit 13 Milliarden Parametern ohne zusätzliches Finetuning. Er beherrscht zwar grundsätzlich Deutsch, wechselte in unseren Versuchen aber immer wieder ins Englische.

Für 15 US-Dollar im Monat wechselt man zu Leo Premium, das mit besseren Llama-2-Versionen (Llama 2 70B und Code Llama 2 70B) und Anthropics Claude Instant arbeitet. Der Browser übermittelt Konversationen mit dem Bot dann über einen anonymisierenden Server, damit diese nicht mit der IP-Adresse des Nutzers in Verbindung gebracht werden können. *(jo@ct.de)*

Unachtsam

Erneuter Einbruch bei Security-Dienstleister Okta

Bei dem Security-Dienstleister Okta wurde abermals eingebrochen. Mittelbar betroffen sind unter anderem 1Password und Cloudflare. Der CDN-Anbieter sieht bei Okta Nachholbedarf bei der Einhaltung von Best Practices im Umgang mit sicherheitsrelevanten Vorfällen.

Von Kathrin Stoll

Angreifer sind bei dem Sicherheitsdienstleister Okta erneut eingebrochen und konnten dabei offenbar Anmeldeinformationen von Kunden erbeuten. Diese nutzten sie, um sich in deren Systeme einzuloggen und von dort aus zu versuchen, sich weitere Berechtigungen zu verschaffen.

Betroffen ist offenbar 1 Prozent der rund 18.000 Kunden Oktas – darunter der Anbieter des Passwort-Managers 1Password und der wichtige CDN-Betreiber Cloudflare.

Am 19. Oktober hat Okta die betroffenen Kunden darüber informiert. Die Angreifer haben offenbar Zugangsdaten zu Oktas Support Case Management System erbeutet. Damit war es ihnen möglich, Dateien einzusehen, die Kunden im Rahmen jüngster Support-Fälle hochgeladen hatten. Zur Problembehebung benötigen Oktas Support-Mitarbeiter offenbar oft sogenannte HAR-Dateien. Dabei handelt es sich um Momentaufnahmen einer Browsersitzung – sensible Daten, denn die Dateien können Cookies und Session-Tokens enthalten. Mithilfe erbeuteter Session-Cookies können Angreifer potenziell auf die Benutzerkonten der betroffenen Kunden zugreifen, sie also als Einfallstor in deren interne Systeme nutzen und versuchen, sich von dort aus weitere Berechtigungen zu verschaffen.

Am 20. Oktober veröffentlichte Okta zusätzlich einen Blogpost mit sogenannten Indicators of Compromise (IoC). Das Unternehmen betonte, es habe den Vorfall in Zusammenarbeit mit den betroffenen Kunden geprüft und Maßnahmen ergriffen, um die Kunden zu schützen: In HAR-Dateien eingebettete Session Tokens seien widerrufen worden. Generell sei die Empfehlung an alle Kunden, Login-Daten und Session-Cookies aus HAR-Dateien zu entfernen, bevor man sie teile.

Auch der Anbieter des beliebten Passwortmanagers 1Password wurde in Mitleidenschaft gezogen. Cloudflare und 1Password legten in Blogposts offen, dass jeweils ihre von Okta bereitgestellte Authentifizierungsplattform in Folge des Einbruchs bei Okta kompromittiert sei. Informationen oder Systeme von Kunden beider Firmen sind offenbar nicht betroffen.

Kunden entdecken den Einbruch

Für Cloudflare ist es schon das zweite Mal, dass sie von einem Einbruch in Oktas Systeme betroffen sind. Als die Hackergruppe Lapsus$ sich im März 2022 durch Social Engineering Zugang zu Okta verschaffte, verhinderte offenbar der Einsatz von Hardware-Keys zur Multi-Faktor-Authentifizierung, dass sich die Angreifer darüber hinaus Zugriff auf interne Daten oder Systeme von Cloudflare verschaffen konnten. Der jetzige Vorfall konnte offenbar eingedämmt werden, weil das hauseigene Security-Team den schädlichen Zugriff auf Cloudflares Okta-Instanz so schnell entdeckte und unmittelbar reagierte. Offenbar hatte der CDN-Anbieter Okta über den Breach informiert, bevor Okta die Warnung an seine Kunden herausgab.

IP Addresses

```
23.105.182.19
104.251.211.122
202.59.10.100
162.210.194.35 (BROWSEC VPN)
198.16.66.124 (BROWSEC VPN)
198.16.66.156 (BROWSEC VPN)
198.16.70.28 (BROWSEC VPN)
198.16.74.203 (BROWSEC VPN)
198.16.74.204 (BROWSEC VPN)
198.16.74.205 (BROWSEC VPN)
198.98.49.203 (BROWSEC VPN)
2.56.164.52 (NEXUS PROXY)
207.244.71.82 (BROWSEC VPN)
```

Okta hat einen Blogpost mit sogenannten Indicators of Compromise veröffentlicht.

Unter den betroffenen Kunden ist auch die Security-Firma BeyondTrust. Laut deren CTO Marc Maiffret hatte BeyondTrusts Security-Team den Angriff bereits am 2. Oktober entdeckt. Jemand habe versucht, den Zugriff auf das Benutzerkonto eines BeyondTrust-Mitarbeiters zu nutzen, um einen Admin-Account mit höchsten Berechtigungen in BeyondTrusts Okta-Umgebung zu erstellen. Beim Überprüfen des Benutzerkontos fiel auf, dass ein Support-Mitarbeiter nur 30 Minuten vorher eine HAR-Datei an Okta geschickt hatte. Am selben Tag habe BeyondTrust Okta kontaktiert und den Verdacht auf einen Einbruch in deren Systeme gemeldet.

Gegenüber dem Sicherheits-Blog „Krebs On Security“ sagte die stellvertretende CISO Oktas, Charlotte Wylie, dass man zunächst geglaubt hätte, BeyondTrusts Entdeckung vom 2. Oktober resultiere nicht aus einem Einbruch in Oktas interne Systeme. Jedoch habe man den Vorfall am 17. Oktober als solchen identifiziert und eingedämmt. Dies sei durch Invalidieren der Zugangs-Tokens des gehackten Support-Benutzerkontos geschehen, außerdem wurde das Konto deaktiviert. Dazu, wie lange die Eindringlinge wohl schon Zugriff auf das Support Case Management System hatten oder wer dahinter stecken könnte, machte sie keine Aussage. Sie sagte jedoch, es gebe Grund zu der Vermutung, dass es sich um Angreifer handelt, die bereits in der Vergangenheit versucht hatten, Okta und seine Kunden anzugreifen.

Manöverkritik

Die Verfasser des Cloudflare-Blogs halten sich indes nur bei sehr oberflächlicher Betrachtung mit Kritik an Oktas Umgang mit dem Vorfall zurück. Okta solle „in Erwägung ziehen, Best Practices zu befolgen“ – und Hinweise auf Kompromittierung ernst nehmen, eine Pflicht zur Verwendung von Hardware-Security-Keys auch bei Support-Dienstleistern einführen und betroffene Kunden zeitnah und verantwortungsvoll über etwaige Vorfälle informieren. Für einen Anbieter derart kritischer Sicherheitsdienstleistungen sei das Befolgen der genannten Best Practices eigentlich selbstverständlich. *(kst@ct.de)* c't

Hintergrundinfos: ***ct.de/yvpj***

Kryptoabgründe

Der Prozess gegen Sam Bankman-Fried offenbarte haarsträubende Geschäftspraktiken

Unendlicher Kredit für die eigene Firma, veruntreute Kundengelder, erfundene Fonds-Einzahlungen, hanebüchene Bilanzen und Schlampereien, die Hunderte Millionen kosten: Nach all dem, was der Prozess gegen Sam Bankman-Fried und das Insolvenzverfahren seiner Kryptobörse FTX zutage förderte, kam der Schuldspruch wenig überraschend.

Von Sylvester Tremmel

Vor etwas mehr als einem Jahr kollabierte die Kryptowährungsbörse FTX spektakulär: Innerhalb weniger Tage ging das Vertrauen in die Liquidität der Börse verloren, immer mehr Kunden versuchten, ihre Gelder abzuziehen, und FTX konnte den Auszahlungsforderungen in Milliardenhöhe schließlich nicht mehr nachkommen. Im darauf folgenden Prozess gegen den Gründer und Ex-CEO Sam Bankman-Fried ist nun ein Urteil ergangen: Nicht einmal fünf Stunden brauchte die Jury, um „SBF“ in allen sieben Anklagepunkten schuldig zu sprechen, von Betrug an FTX.com-Kunden unter Einsatz von Telekommunikationsmitteln („wire fraud“) bis Verschwörung zur Geldwäsche. Das Strafmaß soll im März 2024 verkündet werden, theoretisch sind bis zu 110 Jahre Haft möglich. Für denselben Monat ist auch noch ein zweiter Prozess gegen Bankman-Fried wegen anderer Vergehen angesetzt.

Kern der Anklage war, dass Bankman-Fried wusste und zuließ, dass seine Krypto-Handelsfirma Alameda Research auf Gelder von FTX-Kunden zugriff – noch dazu, ohne dafür entsprechende Sicherheiten zu hinterlegen: Alamedas Konto bei FTX habe beliebig tief ins Minus rutschen dürfen – und Alameda habe das auch massiv ausgenutzt.

Belegt wurde das durch Aussagen aus Bankman-Frieds ehemaliger Führungsriege (deren Mitglieder fast alle auf schuldig plädiert hatten und als Belastungszeugen auftraten), durch inkriminierende Chatnachrichten, Auszüge aus FTX' Programmcode und vieles mehr, nicht zuletzt diverse öffentliche Äußerungen Bankman-Frieds, die er vor und nach dem Kollaps fleißig tätigte.

„Vollkommenes Versagen“

Dass bei FTX vieles im Argen lag, war schon vor Prozessbeginn klar: Insolvenzverwalter John J. Ray III – der bereits Enron abgewickelt hatte – erklärte, er habe niemals in seiner Karriere „ein solch vollkommenes Versagen unternehmerischer Aufsicht auf jeder Ebene einer Organisation gesehen“. Unter anderem hätten 56 Organisationen der FTX-Gruppe keine Bilanzen erstellt und 35 hätten sich auf „ein Sammelsurium an Google-Docs, Slack-Chats, geteilten Laufwerken und Excel-Dateien“ gestützt, um ihre Vermögenswerte und Verbindlichkeiten zu verwalten.

Überhaupt wurde wohl vieles bei FTX sehr schlampig umgesetzt – oder gar nicht. Nur ein Beispiel, das im Prozess zur Sprache kam: FTX' oft gerühmte „Risk-Engine“ sollte für die Stabilität der Börse garantieren, indem sie Kundenkonten mit unzureichenden Sicherheiten automatisch auflöste, bevor sie zu viel Verlust anhäufen konnten. (Alamedas Konto war davon insgeheim ausgenommen.) Allerdings versagte die Engine beim Mobilecoin-Vorfall (siehe ct.de/y9he) und ermöglichte einem Kunden Marktmanipulationen, die FTX einen Verlust von etwa 800 Millionen Dollar bescherten. Nach Bankman-Frieds Darstellung hatte aber nicht die Engine an sich versagt; stattdessen habe er erst die Parameter für diesen Kunden fehlerhaft angepasst und dann nicht mehr aufgepasst.

Bild: Bebeto Matthews/AP/dpa

Dem FTX-Gründer und ehemaligen Multimilliardär Sam Bankman-Fried drohen bis zu 110 Jahre Haft.

Jedenfalls wurde der Verlust einfach Alameda zugeschlagen (das keine Bilanzen veröffentlichte), womit er auch kein Fall für FTX' „Versicherungsfonds“ wurde. Der sollte in solchen Fällen eigentlich einspringen, hatte aber ohnehin einen fantasierten Füllstand: Die Anklage legte GitHub-Commits vor, nach denen der angebliche Zuwachs des Fonds per Zufallszahlengenerator bestimmt wurde.

Auswirkungen

Mit dem Schuldspruch ist die FTX-Krise nicht abgeschlossen. Weitere Prozesse drohen, unter anderem weil FTX' Insolvenzverwaltung versucht, möglichst viele Zahlungen aus besseren Zeiten zurückzuholen – auch auf dem Rechtsweg. Das verläuft offenbar recht erfolgreich und weil sich einige der mit Kundengeldern getätigten Investitionen als lukrativ erwiesen (allen voran eine Beteiligung am KI-Startup Anthropic), könnten FTX-Kunden unerwartet glimpflich davon kommen.

Unterdessen richten sich skeptische Blicke auf FTX' einstige Partner und Konkurrenten, etwa die weltgrößte Kryptobörse Binance. Deren Firmengeflecht beschreibt die US-amerikanische Börsenaufsicht SEC als „Spiegelkabinett“. Auch die Stablecoin Tether (USDT) wird mal wieder kritisch beäugt. USDT im Gegenwert von etwa 40 Milliarden Dollar soll Alameda Research direkt von Tether erhalten haben. Wie Alameda sich das leisten konnte, ist nicht bekannt. *(syt@ct.de)* c't

Bit-Rauschen

Neue Hoffnungen auf schnelle ARM-Notebooks

Qualcomm präsentiert den besonders starken Snapdragon X Elite. Bei RISC-V knirscht es – aber nicht nur. AMD und Intel machen mehr Umsatz.

Von Christof Windeck

Mit beeindruckenden Benchmark-Ergebnissen weckt Qualcomm neue Hoffnungen auf attraktive Windows-Notebooks mit ARM-Prozessoren. Zwar muss man auf die ersten Geräte mit Snapdragon X Elite wohl mindestens bis Mitte 2024 warten und bisher gibt es keine unabhängigen Messungen. Doch laut Qualcomm überflügelt der Snapdragon mit den Oryon-Kernen des zugekauften CPU-Start-ups Nuvia den Apple M2 Pro, den AMD Ryzen 7 7840U und Intels Core i7-1360P. 2024 tritt der Qualcomm-Chip allerdings gegen Apple M3, AMD Ryzen 8000 und Intel Meteor Lake an. Doch es dürfte jedenfalls spannender werden als in den vergangenen zehn Jahren.

Erste Geekbench-Ergebnisse des Apple M3 wiederum sind auch hoch, verraten jedoch, dass er im Vergleich zum M2 vor allem durch höhere Taktfrequenzen zulegt. Apple ist es also ähnlich wie beim iPhone-Chip A17 Pro nicht gelungen, die Rechenleistung der CPU-Kerne pro Taktzyklus deutlich zu steigern. Beim M3 Pro gibt es im Vergleich zum M2 Pro sogar produktpolitisch bedingte Rückschritte bei der Anzahl der P-Kerne und der Datentransferrate. Die 3-Nanometer-Fertigungstechnik von TSMC bietet damit bisher ein eher ernüchterndes Bild. Immerhin passen damit mehr Transistoren auf jeden Quadratmillimeter als in der 5-Nanometer-Generation, was Apple beim M3 Max ausnutzt: Mit 92 Milliarden Transistoren hat er satte 37 Prozent mehr als der M2 Max (67 Milliarden) und unter anderem zwölf statt acht starke CPU-Kerne.

RISC-V-Wechselbad

Die RISC-V-Entwicklerfirma SiFive schockierte die Freunde der offenen Befehlssatzarchitektur mit Entlassungen: Rund 20 Prozent der weltweiten Arbeitsplätze fielen weg. SiFive beteuert jedoch, es gebe kein grundsätzliches Problem. SiFive ist nicht irgendein RISC-V-Entwickler, sondern mit nun wohl rund 400 Mitarbeitern immer noch einer der größten und auch der bekannteste. SiFives „Chief Architect“ Krste Asanović und CTO Yunsup Lee gehören zu den Gründervätern der RISC-V-Technik, Asanović war Professor an der Uni Berkeley.

Auch beim Raspberry Pi hat RISC-V auf Jahre hinaus kaum Chancen – nicht nur aus technischen Gründen: ARM hat Anfang November eine Minderheitsbeteiligung an Raspberry Pi Ltd. erworben, der kommerziellen Tochterfirma der Raspberry Pi Foundation. Beide Firmen haben ihren Hauptsitz in Cambridge, die Beziehungen sind traditionell eng.

Bessere RISC-V-Nachrichten kommen aus Deutschland: Die vom Bundesministerium für Bildung und Forschung geförderte Projektgruppe „HEP“ hat innerhalb von zwei Jahren einen Sicherheitschip mit RISC-V-Kern entwickelt und auch noch mit der offengelegten 130-Nanometer-Fertigungstechnik des IHP in Frankfurt/Oder produzieren lassen. Solche Projekte sind kleine Schritte, um die europäische Souveränität bei Halbleitern zu verbessern.

Wie wichtig das ist, zeigt eine repräsentative Umfrage des Branchenverbandes Bitkom unter 404 Firmen, darunter produzierendes Gewerbe und ITK-Dienstleister. 83 Prozent von ihnen antworteten, dass Halbleiter für ihr Geschäft essenziell sind – und 25 Prozent kaufen sie in China. Damit liegt China als Chipzulieferer für diese deutschen Firmen deutlich vor den USA, Taiwan, Korea, Singapur und anderen Ländern. Das überrascht einerseits, weil der Umsatzanteil chinesischer Chipfirmen am Weltmarkt eigentlich viel kleiner ist. Andererseits kommen aus China auch Chips von Firmen mit Sitz in anderen Ländern, die dort Fabriken betreiben. Und über 90 Prozent der befragten Firmen, die in China einkaufen, beschaffen von dort diskrete Bauelemente. Bei diesen einfachen, aber wichtigen Komponenten hat China einen sehr hohen Marktanteil und es geht dabei vor allem um niedrige Preise. Schließlich kaufen viele Firmen keine einzelnen Bauelemente, sondern komplette Baugruppen oder Module von chinesischen Produzenten.

Der Weg zu mehr Unabhängigkeit von China ist also noch weit. Die meisten der vom Bitkom befragten Firmen kämpfen weiterhin mit Lieferengpässen und Preissteigerungen bei Chips und erwarten obendrein, dass sich diese Probleme 2024 noch verschärfen.

x86 im Börsenhoch

AMD und Intel haben turnusmäßig Quartalszahlen vorgestellt, laut denen ihre jeweiligen Geschäfte von Juli bis September besser liefen als zuvor. Beide x86-Prozessorfirmen schrieben wieder schwarze Zahlen, wozu Intel etwas mehr tricksen musste als AMD. Die Börse wertete das als gute Zeichen und die Kurse stiegen. Nvidia verkündet seine Zahlen stets etwas später als AMD und Intel, musste aber eine Delle im Aktienkurs hinnehmen. Weil Nvidia sehr viele KI-Beschleuniger nach China verkauft, befürchteten Anleger, dass verschärfte Exportregeln der USA gegen China das Geschäft trüben. Der Aktienkurs erholte sich dann aber rasch wieder. *(ciw@ct.de)* c't

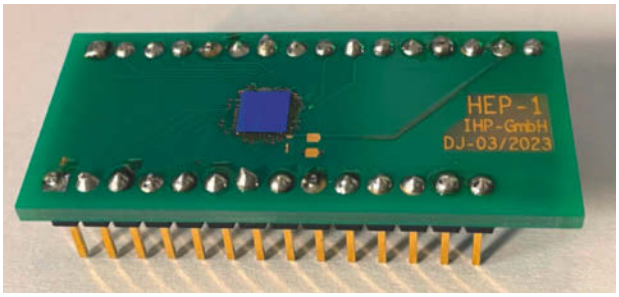


Bild: IHP/Franziska Wegner

Der mit offengelegter Fertigungstechnik in Deutschland produzierte Sicherheitschip HEP-1 hat einen ebenfalls offengelegten RISC-V-Kern.

Gaming-Grafikkarte mit SSD-Steckplatz

Asus bietet eine GeForce RTX 4060 Ti mit M.2-Slot an. Letzterer funktioniert allerdings nicht auf allen Mainboards.

Auf den ersten Blick unterscheidet sich die Asus Dual RTX 4060 Ti SSD kaum von anderen Grafikkarten mit gleichem Grafikchip. Auf der Rückseite bringt der Hersteller jedoch unter einer abnehmbaren Abdeckung einen M.2-Steckplatz unter. Dieser nimmt NVMe-SSDs mit 80 Millimeter Länge (M.2-2280) auf.

Der zusätzliche Flash-Speicher erweitert jedoch nicht den Grafikspeicher, wie bei der 2017 von AMD vorgestellten Profigrafikkarte Radeon Pro Solid State Graphics (SSG). Stattdessen verhilft die Asus Dual RTX 4060 Ti SSD lediglich zu einem weiteren Steckplatz, falls auf dem Mainboard schon alle M.2-Slots belegt sind.

Möglich ist das, weil die auf der RTX 4060 Ti verwendete AD106-350-GPU nur 8 der 16 PCI-Express-Lanes des PEG-Slots verwendet. Von den übrigen freien acht nutzt Asus bei der Grafikkarte vier PCIe-Lanes für den M.2-Slot. Das Aufspalten der Lanes auf mehrere Geräte (PCIe Bifurcation) unterstützt jedoch nicht jedes Mainboard und jede Prozessorplattform gleichermaßen. Ausgeschlossen sind zum Beispiel LGA1700-Mainboards mit B760-, B660- und H610-Chipsatz. Bei den teureren Chipsätzen Z790, Z690, H770 oder H670 für Core i-12000/13000/14000 und den Plattformen AM4 und AM5 für Ryzen-Prozessoren hängt es von der jeweiligen Hauptplatine ab, ob PCIe Bifurcation funktioniert. Für PCIe 5.0 gibt Asus die Karte nicht frei; eine PCIe-5.0-SSD mit großem Kühler passt auch nicht darauf.

Die GPU der Asus Dual RTX 4060 Ti SSD taktet mit 2565 MHz und ihr stehen 8 GByte GDDR6-RAM zur Seite. Die Grafikkarte belegt zweieinhalb Erweiterungsplätze und sie steuert über 3 × DisplayPort 1.4a und 1 × HDMI 2.1a vier 4K-Displays gleichzeitig an. Sie kostet rund 480 Euro und soll Ende des Monats in den Handel kommen. *(chh@ct.de)*

Bild: Asus

Den M.2-Slot für eine SSD versteckt Asus auf der Rückseite Dual RTX 4060 Ti SSD unter einer verschraubten Abdeckung.

AMD startet ins Hybridprozessoren-Zeitalter

Rund zwei Jahre nach Intel bietet AMD die Mobil-CPUs Ryzen 5 7545U und Ryzen 3 7440U „Phoenix2“ als **erste Prozessoren mit unterschiedlich leistungsstarken Kernen** an. Allerdings wählt AMD eine andere Strategie: Statt aus Performance- und Effizienzkernen unterschiedlicher Architektur besteht der Sechskerner Ryzen 5 7545U aus zwei Zen-4- und vier Zen-4c-Kernen mit jeweils identischen Recheneinheiten und Caches. Ein Zen-4c-Kern belegt dennoch nur 2,48 mm² statt 3,84 mm² Fläche, weil die Schaltkreise auf niedrigeren Takt optimiert sind und die Caches kompaktere SRAM-Zellen verwenden. Bei geringem thermischen Budget von unter 20 Watt soll laut AMD die Kombination aus zweifach Zen 4 und vierfach Zen 4c effizienter rechnen als sechs gleiche Zen-4-Kerne.

Weil sich die beiden Kernsorten nach außen hin lediglich bei der maximalen Taktfrequenz unterscheiden, kann der Scheduler des Betriebssystems sie im Vergleich zu den heterogenen Kernen der Intel Core i-12000/13000/4000 leichter verwalten. Bereits seit den Ryzen 3000 gibt es unterschiedlich schnelle Kerne, deren Zuordnung die CPU über die Funktion Collaborative Processor Performance Control (CPPC2) dem Betriebssystem mitteilt.

Anhand des Namensschemas sind die Hybridprozessoren nicht direkt zu erkennen: Der Ryzen 5 7545U ersetzt den Zen-4-Sechskerner Ryzen 5 7540U, den wir kürzlich im HP EliteBook 845 G10 getestet hatten und bei dem ebenfalls nur zwei Kerne den maximalen Boost von 4,9 GHz erreichten (siehe c’t 25/2023, S. 114). Der „alte“ Quad-Core Ryzen 3 4770U hatte es bisher in kein einziges Notebook geschafft und wird deshalb durch die neue Variante mit einem Zen-4- und drei Zen-4c-Kernen ersetzt. *(chh@ct.de)*

Glasfaser-Internet mit 20 Gbit/s

Google Fiber baut sein Glasfasernetz der nächsten Generation mit Nokia-Hardware auf: 25G-PON beschleunigt das noch seltene XGS-PON aufs 2,5-fache, Kunden sollen 20-Gigabit-Anschlüsse ordern können.

Das ewige Rennen um die schnellste Internethardware geht weiter: Kaum deutet sich an, dass jetzt erhältliche Geräte für den nächsten WLAN-Standard Wi-Fi 7 10-Gigabit-Internetanschlüsse (XGS-PON) mit Spitzendatenraten jenseits von 7 Gbit/s weitgehend ausschöpfen können (c't 16/2023, S. 12), strebt Google Fiber die nächste Geschwindigkeitsstufe an. In den US-Bundesstaaten Missouri und Utah ertüchtigt die Alphabet-Tochter die ersten Glasfasernetze mit Nokia-Hardware, die nach dem 25G-PON-Standard arbeiten – gelegentlich auch 25GS-PON genannt, mit eingeschobenem S für symmetrisch. Die Spezifikation steht auf der Website 25gspon-msa.org.

Bisher bot Google Fiber maximal 8 Gbit/s im Downstream an, mit 25G-PON sollen es 20 Gbit/s werden. Erste Nutznießer der Technik werden laut Nokia die Universität Missouri in Kansas City und die gemeinnützige Organisation United Ways in Utah County.

25G-PON schreibt die XGS-PON-Technik für 10 Gbit/s symmetrisch über Glasfaser linear fort, es zieht lediglich protokollseitig eine Adaptionsschicht ein (Transmission Convergence Layer, TC). Optisch nutze es den IEEE-Standard 802.3ca (25G EPON). So funktioniert 25G-PON wie XGS-PON und GPON auf denselben Monomode-Fasern, die bereits in der Erde liegen oder zurzeit eingezogen werden. Wegen wählbarer Wellenlängen für den Upstream kann 25G-PON parallel zu anderen Techniken im Medium laufen. Provider müssen deshalb nicht alle Kunden an einem Faserstrang mit neuer Hardware versorgen, sobald der erste auf 25G-PON umsteigt. *(ea@ct.de)*

Bild: Nokia

Nokia bietet seine Konzentratoren (OLT) für die 25G-PON-Technik nicht nur im üblichen Switch-Format für Rechenzentrumsgestelle an, sondern auch in einem robusten Gehäuse für den Außenbetrieb (Lightspan SF-8M).

Kompakter 10GE-Switch für Glas und Kupfer

Mit **zwölf Ports für Datenverbindungen von 100 Mbit/s bis 10 Gbit/s** wartet QNAPs neuer Switch QSW-M3212R-8S4T auf. Er hat acht SFP+-Slots sowie vier RJ45-Buchsen für Kupferverbindungen. Letztere arbeiten neben Fast-, Gigabit- und 10-Gigabit-Ethernet auch mit 2,5 und 5 Gbit/s (NBase-T).

Der M3212R ist für kleine Unternehmen oder ambitionierte Heimanwender gedacht und kann sowohl als Desktopgerät eingesetzt als auch in 19-Zoll-Gestelle montiert werden. Dort belegt der Switch nur 8,1 Zoll (20,7 Zentimeter), also etwas weniger als die halbe Breite, und eine Höheneinheit (1U, 44 mm). QNAP bietet Halterungen, um zwei Stück nebeneinander zu montieren. Die beiden Lüfter des Switches sollen drehzahlgesteuert arbeiten.

Das Management des Netzwerkverteilers läuft ausschließlich über das Webinterface und beschränkt sich auf grundlegende Layer-2-Funktionen wie VLAN, RSTP, LACP oder LLDP. Ein Konsolenzugang via SSH und das Management mittels SNMP fehlen.

Einen hiesigen Preis für den QSW-M3212R-8S4T hat QNAP noch nicht genannt. In Nordamerika ist das Gerät für umgerechnet rund 500 Euro gelistet. *(amo@ct.de)*

Bild: QNAP

Der 10-Gigabit-Switch QSW-M3212R-8S4T ist knapp 21 Zentimeter schmal und passt mit einem Zwilling in ein 19-Zoll-Gestell.

Powerline-WLAN-Basis mit Wi-Fi 6

AVM hat sein Angebot um einen **Wi-Fi-6-fähigen Powerline-Access-Point** erweitert: Der Fritz-Powerline 1240AX besitzt ein 2-Stream-WLAN-Modul, das ausschließlich auf 2,4 GHz funkt. Die maximale Datenrate beträgt somit rund 600 Mbit/s brutto. Zwei Gigabit-Ports verbinden Geräte ohne WLAN. An der Steckdose erreicht der Adapter bis zu 1200 Mbit/s (HomePlug AV2).

Das Set aus Fritz-Powerline 1240AX und einem Ethernet-zu-Powerline-Adapter Fritz-Powerline 1210 ist für 170 Euro erhältlich. *(amo@ct.de)*

Bild: AVM

Der Fritz-Powerline-Access-Point 1240AX funkt ausschließlich auf 2,4 GHz und ist für Gebäude mit dicken Wänden und starker Signaldämpfung gedacht.

Serverfestplatte mit 24 TByte

Seagate kündigt seine letzte neue Festplatte mit konventioneller Aufzeichnungstechnik an. Dank erneut erhöhter Datendichte kommt die Exos X24 auf 24 TByte Speicherplatz.

Seagate erweitert seine Serverfestplattenserie Exos X mit einem Modell mit 24 TByte. Dabei nutzt Seagate keine neue Technik, sondern quetscht die Bits noch ein wenig näher aneinander. Im Inneren des heliumgefüllten Gehäuses drehen sich wie beim 22-TByte-Modell zehn Scheiben mit insgesamt 20 Köpfen, als Schnittstellen stehen SATA 6G oder SAS 12G zur Verfügung. Neben der Standardversion ist eine verschlüsselnde erhältlich, das SAS-Modell zudem noch mit FIPS-Zertifizierung.

Seagate nennt als Maximalgeschwindigkeit 285 MByte/s, auf den inneren Ringen dürfte die Platte maximal die Hälfte erreichen. Die maximale Wahrscheinlichkeit nicht korrigierbarer Lesefehler beziffert der Hersteller mit einem Sektor pro 10^{15} (eine Billiarde) gelesener Bits, die Ausfallwahrscheinlichkeit auf 0,35 Prozent pro Jahr.

Verschiedene Preisvergleicher listen bereits die NAS-Festplatte Ironwolf Pro mit 24 TByte, diese hatte Seagate jedoch zum Redaktionsschluss noch nicht angekündigt. Auch ein Preis für die Exos X24 ist noch nicht bekannt, die Platte soll im Dezember verfügbar sein. Seagate stellt ausgewählten Kunden zudem eine Version der X24 zur Verfügung, die mit der überlappenden Aufzeichnungstechnik Shingled Magnetic Recording (SMR) eine Kapazität von 28 TByte erreichen soll. Diese Festplatte nutzt Host Managed SMR und muss vom Storage-Controller passend angesteuert werden.

Mit der Exos X24 ist nach Angaben von Seagate die Entwicklung von Festplatten mit konventioneller Aufzeichnungstechnik (Conventional Magnetic Recording, CMR) abgeschlossen. Zukünftige Laufwerke verwenden zur Kapazitätssteigerung die HAMR-Technik, bei der ein Laser im Schreibkopf zusätzliche Energie in die Magnetpartikel bringt und damit das Beschreiben mit geringerer Magnetfeldstärke ermöglicht (Heat Assisted Magnetic Recording). Seagate will Anfang 2024 die erste HAMR-Festplatte mit einer Kapazität von 32 TByte auf den Markt bringen, in zwei Jahren soll die Laufwerkskapazität dann auf 40 TByte steigen. *(ll@ct.de)*

Bild: Seagate

Noch ein paar Bytes mehr: Seagate quetscht 24 TByte in die Serverfestplatte Exos X24.

Speicherupgrade: Micron 7500 mit 232-Lagen-Flash

Micron rüstet **seine Server-SSDs mit dem aktuellen hauseigenen TLC-Speicher mit 232 Lagen** auf. Damit erreicht die Micron 7500 7 GByte/s beim Lesen und 5,9 GByte/s beim Schreiben, die Maximalwerte beim Zugriff auf zufällige Adressen steigen auf 1,1 Millionen IOPS.

Bild: Micron

Die Micron 7000 Pro soll als Server-SSD täglich bis zum Dreifachen ihrer Kapazität überschreibbar sein.

Wie üblich baut Micron zwei Varianten der Server-SSD: Die Pro-Version hat mehr Kapazität, bei der Max-Version führt ein größerer Overprovisioning-Bereich zu einer höheren Belastbarkeit; sie darf pro Tag mit dem Dreifachen ihrer Kapazität überschrieben werden (3 Drive Writes Per Day, DWPD). So liegen die Kapazitäten der 7500 Pro zwischen 960 GByte und 15,36 TByte, die Maximalkapazität der 7500 Max bei nur 12,8 TByte.

Die 7500 ist ausschließlich im 15 Millimeter hohen 2,5-Zoll-Gehäuse mit U.3-Anschluss (PCIe 4.0) erhältlich, die beim Vorgänger 7450 noch verfügbaren Bauformen E3.S und M.2 entfallen. Die maximale Leistungsaufnahme liegt laut Hersteller bei 18,3 Watt, fast 2 Watt mehr als bei der 7450. *(ll@ct.de)*

Kurz & knapp

Eine **Fusion der Flash-Hersteller Kioxia und Western Digital** findet nicht statt. Einer der indirekten Anteilseigner von Kioxia, der koreanische Flash-Hersteller SK Hynix, hat sein Veto eingelegt und damit den Prozess gestoppt.

Western Digital will **Festplatten- und SSD-Geschäft trennen** und sich dazu in zwei Firmen aufteilen. Die Forderung nach einer solchen Aufteilung kam bereits im vergangenen Jahr von einem Großinvestor.

Der amerikanische Colocation-Provider Standard Power will die für den Betrieb einiger seiner Rechenzentren notwendige Energie in Zukunft mit **24 Mini-Atomreaktoren von NuScale** erzeugen.

Flucht nach vorn

Wie Apple die Macs gegen Konkurrenz rüstet

In nur drei Jahren liefert Apple das dritte Chipupgrade für seine Notebooklinie MacBook Pro. Dieses Innovationstempo legte die Firma bisher nur bei den hauseigenen Smartphones vor. Jedoch ist nicht jede Version des M3 deutlich schneller als ihr Vorgänger.

Von Dušan Živadinović und Christof Windeck

Eigentlich macht Apple bei seiner Chipentwicklung alles richtig: Die Firma führte als erster Hersteller die Fertigung in 3 Nanometer Strukturbreite ein. Die ohnehin nicht langsamen MacBook Pro laufen damit und auch wegen höherer Taktfrequenzen bis zu 20 Prozent schneller als die Vorgänger. Dabei hat Apple den 3-Nanometer-Prozess zunächst mit seinem relativ kleinen Smartphone-Chip A17 Pro geübt und dann die Produktion für die größeren Chips M3, M3 Pro und M3 Max optimiert; das ist der übliche Weg, um die Ausschussrate der Fertigung auf vertretbarem Niveau zu halten.

Allerdings ist der Wechsel von 5- auf 3-Nanometer-Technik nicht komplett, es fehlt der Riesenchip M3 Ultra. Den mochte Apple vermutlich noch nicht bei TSMC in Auftrag geben, um die Käufer des erst seit dem Sommer erhältlichen Mac Pro nicht zu verprellen (siehe ct.de/ybej). Denn dem Mac Pro verpasst Apple nur den M2 Ultra, ebenso wie der Workstation Mac Studio.

Suboptimale Produktpalette

Deshalb das „eigentlich“ und deshalb sieht die Mac-Produktpalette, nun ja ..., suboptimal aus: Denn das neue MacBook Pro mit M3 Max entledigt sich mancher Benchmarks schneller als der buchstäblich größte Mac Pro: Beispielsweise erzielt letzterer im Single-Core-Test rund 2800 Punkte und im Multicore-Test rund 21.900 Punkte, während das MacBook Pro mit M3 Max auf 3200 und 21.800 Punkte kommt (siehe auch ct.de/ybej). Dennoch sind die Tower- und Workstation-Preise bisher unverändert, was besonders beim Mac Pro auffällt, für den Apple mindestens 8300 Euro verlangt.

Ob und wann der Mac Pro den Extrawumms des erwarteten M3 Ultra bekommt, ist offen. Aber Kunden, die einen Mac-Tower oder eine Mac-Workstation brauchen, stehen nun vor dem Dilemma, ob sie noch auf eine solche Wundermaschine warten oder doch die vorletzte Generation ohne Preisnachlass nehmen.

Transistor-König auf Abruf

Gegenüber der N5-Technik der M2-Chips enthält die M3-Generation deutlich mehr Transistoren auf derselben Chipfläche. Beim M3, M3 Pro und M3 Max sind es 25, 37 und 92 Milliarden. Die Transistorkrone unter den Apple-Chips hat aber mit 134 Milliarden Transistoren noch immer der M2 Ultra auf, der genau besehen, aus zwei superschnell vermaschten M2 Max besteht.

Dagegen erscheinen die derzeit schnellsten x86-Prozessoren für Notebooks wie Zwerge: Der AMD Ryzen 7 7840U oder der Ryzen 9 7940HS kommt auf gerade mal 25 Milliarden Transistoren (4 Nanometer-Prozess). Dabei ist zumindest beim Ryzen 7 ebenfalls eine GPU an Bord. Doch wenn Apple den erwarteten M3 Ultra so wie den M2 Ultra konzipiert, dürfte er aus zwei vermaschten M3 Max mit zusammen sogar 268 Milliarden Transistoren bestehen.

Die zusätzlichen Transistoren des M3 nutzt Apple unter anderem für höhere Grafikleistung. Beispielsweise hat Apple für die naturgetreue Bildsynthese in Echtzeit Raytracing-Einheiten integriert. Auch das hat Apple schon beim iPhone-Chip A17 Pro geübt.

Die CPU-Kerne sind zwar auch überarbeitet, aber die starken Kerne (Performance, P-Kerne) legen bei der Rechenleistung pro Takt nur wenig zu. Die Mehrleistung von rund 20 Prozent gegenüber den M2-Varianten holt Apple hauptsächlich mittels deutlich höherem Takt heraus, nämlich maximal 4,05 GHz gegenüber höchstens 3,5 GHz. Auch rechnen die schwächeren Effizienzkerne (E-Kerne) schneller als ihre Vorgänger.

M3 und der M3 Max enthalten ebenso viele CPU-Kerne wie ihre M2-Vorgän-

Bild: Apple

Das neue MacBook Pro ist auch in Schwarz erhältlich, wenn man es mit einem M3-Pro- oder M3-Max-Chip bestellt.

ger, nämlich 8 (4P + 4E) respektive 16 (12P + 4E). Der M3 Pro hat jedoch nur 6 P-Kerne und 6 E-Kerne, sein Vorgänger hingegen 8 P- und 4 E-Kerne. Deshalb ist der M3 Pro kaum schneller als der Vorgänger M2 Pro. Die GPU des M3 Pro schrumpft von 19 auf 18 Shader-Cluster, das RAM-Interface von 256 auf 192 Bit und die Übertragungsrate gegenüber dem M2 Pro und sogar dem M1 Pro um ein Viertel. Das limitiert die Grafikleistung. Den M3 Pro und M3 Max gibt es auch in günstigeren Versionen mit deaktivierten Kernen.

Die von Apple versprochenen Leistungszuwächse des M3 enttäuschen etwas, jedoch auf hohem Niveau. Denn selbstverständlich handelt es sich um sehr schnelle Prozessoren. Doch drei Jahre nach Vorstellung des M1 hatten wir mehr erwartet.

Immerhin scheint Apple mit dem Sprung auf den N3-Prozess gerade noch rechtzeitig die Flucht nach vorn gelungen zu sein, denn ab 2024 will Qualcomm mit dem Snapdragon X Elite im Notebookmarkt mitmischen. Laut ersten Messungen von Qualcomm kommt er nicht über das Niveau der M2-Generation hinaus. Doch bald könnte das Intel-Imperium mit den neuen Meteor-Lake-Prozessoren zurückschlagen.

Wie auch immer das Rennen dann ausgeht, die MacBooks mit den neuen M3-Chips sind schon zum Jahresendspurt erhältlich, zu dem viele Firmen ihre Budgets aufbrauchen. Das MacBook Pro mit 14-Zoll-Display (3024 × 1964 Pixel, maximal 1800 Candela/m² Helligkeit) liefert Apple wahlweise mit M3-, M3-Pro- oder M3-Max-Chip, der Einstiegspreis beträgt 2000 Euro (8-Kern-CPU, 10-Kern-GPU, SSD mit 512 GByte Kapazität und 8 GByte RAM).

Das 16-Zoll-Model (3456 × 2234 Pixel) gibt es ab 3000 Euro mit dem M3-Pro-Chip (ab 11 CPU- und 14-GPU-Kernen, mindestens 512 GByte Massenspeicher und 18 GByte Arbeitsspeicher). Die Variante mit dem M3 Max enthält mindestens 14 CPU- und 30 GPU-Kerne, 1 TByte Massenspeicher und 36 GByte Arbeitsspeicher. In der Maximalausstattung, die 8530 Euro kostet, enthält der M3 Max 16 CPU- und 40-GPU-Kerne, 8 TByte Massenspeicher und 128 GByte Arbeitsspeicher.

Schwarze Messe

Die Pro- und Max-Versionen sind nicht nur in den Gehäusefarben Space Grau und Silber erhältlich, sondern auch in Schwarz, was Apple im Rahmen der Vorstellung am heutzutage ironisch-morbide begangenen Halloween-Feiertag sichtlich genoss. Ach, ja: nur in Schwarz ist die Oberfläche fettabweisend, sodass Fingerabdrücke weniger auffallen.

Alle Modelle enthalten Wi-Fi 6E und Bluetooth 5.3. Die übrigen Merkmale im Telegrammstil: Drei Thunderbolt-4-Ports als USB-C-Buchsen mit je 40 Gbit/s (zwei Thunderbolt-3-Ports beim 14-Zoll-Modell), HDMI 2.1 (8K bei 60 Hz oder 4K bei 240 Hz), SD-Slot, Kopfhöreranschluss (3,5 Millimeter Klinke), 1080p FaceTime-Kamera, sechs Hi-Fi-Lautsprecher inklusive Tieftönern und 3D-Audio, drei Mikrofone und MagSafe-Stromanschluss.

Den 24-Zoll-iMac mit 4,5K-Retina-Display, der 2021 mit dem M1-Chip erschien, gibt es jetzt ebenfalls mit dem M3-Chip. Design, Ausstattung und Farben sind unverändert. Er ist ab 1599 Euro erhältlich. Zur Grundausstattung gehört eine 8-Kern-CPU, magere 8 GByte Arbeitsspeicher und eine 256-GByte-SSD. *(dz@ct.de)* c't

M3-Benchmarks: ***ct.de/ybej***

Neue Spielregeln

Disney+ baut um und bereitet Account-Sharing-Sperre vor

Wie zuvor angekündigt, hat Disney+ auf ein mehrstufiges Tarifmodell inklusive Probeabo umgestellt – und dabei gleich den rechtlichen Rahmen geschaffen, um Trittbrettfahrer künftig rauszuwerfen.

Von Nico Jurran

Am 1. November brach bei Disney+ hierzulande eine neue Ära an: Statt eines Einheitstarifs gibt es bei dem Abo-Videostreamingdienst nun drei Preisstufen, inklusive einer verbilligten Variante mit Werbung. Ein Blick auf die Tabelle unten zeigt, wie frappierend das neue Tarifmodell dem von Netflix ähnelt.

Kurz vor dem Stichtag ließ Disney+ seinen Kunden passend dazu neue Nutzungsbedingungen zukommen – und nutzte die Gelegenheit, um auch gleich die angekündigte Account-Sharing-Sperre (siehe c't 20/2023, S. 54) zu regeln. Diese soll ab einem noch nicht genannten Zeitpunkt wie bei Netflix dafür sorgen, dass der Dienst eine Weitergabe der Zugangsdaten an Dritte außerhalb des Haushalts des Abonnenten sperren kann.

Eine explizite Regelung zu Zweitwohnsitzen und Ferienwohnungen sowie zur Nutzung des Dienstes im Urlaub konnten wir in den neuen Bedingungen nicht finden. Damit nicht genug: Man kann Punkt 1c des neuen Nutzungsvertrags sogar so verstehen, dass der Haushalt alleine auf den „privaten Hauptwohnsitz" beschränkt ist – womit Disney+ den Begriff Haushalt restriktiver auslegen würde als Netflix, das keine Örtlichkeiten nennt.

Andererseits enthält der betreffende Paragraf gleich zweimal die Formulierung „sofern nicht (anderweitig) durch ihre Abo-Optionen erlaubt". Wie Netflix plant also offensichtlich auch Disney+, Kunden die Möglichkeit einzuräumen, gegen Bezahlung den Hauptvertrag so zu erweitern, dass auch Personen außerhalb des eigenen Haushalts diesen (in bestimmtem Maße) nutzen können. Eine Buchungsmöglichkeit gab es bis zum Redaktionsschluss aber noch nicht, ebenso wenig äußerte sich der Dienst zu den Kosten.

Schwache Quote

Aktuell laufen bei vielen Kunden noch Jahresverträge, teilweise über Partner wie die Telekom. Wie sich die Tarifumstellung auf die Abozahlen auswirkt, zeigt sich daher wohl erst in einigen Monaten.

Ob Disney+ seine Kunden halten kann, hängt von der Attraktivität des Angebots ab. Und hier musste der Dienst jüngst einen Rückschlag einstecken: Laut Quotenmesser Nielsen erreichte der Auftakt der zweiten Staffel der Marvel-Serie „Loki" mit 446 Millionen gestreamten Minuten nicht einmal die Top 10 der plattformübergreifenden Charts. Die Premiere der 1. Staffel war 2021 noch 731 Millionen Minuten gestreamt worden. Nun sehen sich Kritiker bestätigt, die die Marvel-Formel bei Disney+ als ausgelutscht betrachten.

Alles Hulu

In den USA gab Disney derweil bekannt, auch noch die verbleibenden 33 Prozent am dortigen Streamingdienst Hulu von der Comcast-Tocher NBCUniversal zu übernehmen. Der genaue Kaufpreis ist noch offen, der Mindestbetrag beläuft sich aber auf 8,6 Milliarden US-Dollar, ausgehend von einer Bewertung für Hulu aus dem Jahre 2019. Ob NBCUniversal mittlerweile mehr zusteht, wird aktuell verhandelt.

Parallel wird in der US-Fachpresse spekuliert, wie es mit Hulu weitergeht. Denkbar ist, dass Hulu in den USA Teil von Disney+ wird; bislang gibt es beide Dienste dort im Bundle. Ebenso steht ein internationaler Launch des Dienstes im Raum. Möglicherweise wurde der bislang nicht in Angriff genommen, um den Wert des Unternehmens vor der kompletten Übernahme nicht zu erhöhen.

Darüber, ob ein deutsches Hulu für hiesige Nutzer vorteilhaft wäre, lässt sich streiten: Disney-Inhalte wie „Futurama" und „Only Murders in the Building", die in den USA als Hulu-Originals laufen, sind hierzulande aktuell bereits im (in den USA fehlenden) Erwachsenenbereich „Star" abrufbar. Hulu-Produktionen anderer Studios kann der Mäusekonzern wiederum aufgrund fehlender internationaler Vertriebsrechte auch nach der kompletten Übernahme wohl nicht bei Disney+ einpflegen. Und noch einen weiteren Dienst dürften die wenigsten deutschen Kunden wollen. *(nij@ct.de)* c't

Abovergleich Disney+ und Netflix

Abovarianten	Standardabo mit Werbung		Standardabo		Premiumabo	
Anbieter	Disney+	Netflix	Disney+	Netflix	Disney+	Netflix
werbefrei	–	–	✓	✓	✓	✓
Videoqualität	bis zu Full-HD (1080p)	bis zu Full-HD (1080p)	bis zu Full-HD (1080p)	bis zu Full-HD (1080p)	bis zu 4K mit HDR	bis zu 4K mit HDR
Audioqualität	bis zu 5.1-Ton	bis zu 5.1-Ton	bis zu 5.1-Ton	bis zu 5.1-Ton	bis zu Dolby Atmos	bis zu Dolby Atmos
gleichzeitige Streams	bis zu 2	bis zu 2	bis zu 2	bis zu 2	bis zu 4	bis zu 4
Downloads möglich	–	✓ (bis zu 15 auf bis zu 2 Geräten)	✓ (auf bis zu 10 Geräten)	✓ (auf bis zu 2 Geräten)	✓ (auf bis zu 10 Geräten)	✓ (auf bis zu 6 Geräten)
Zusatzmitglieder buchbar	–	–	–	✓ (bis zu 1)	–	✓ (bis zu 2)
Preis pro Monat	5,99 €	4,99 €	8,99 €	12,99 €	11,99 €	17,99 €
Preis pro Jahr	–	–	89,90 €	–	119,90 €	–
Preis pro Zusatzmitglied/Monat	–	–	–	4,99 €	–	4,99 €

Alle Angaben beziehen sich auf Abos für Neukunden beziehungsweise Wiedereinsteiger.

Bio-IT: Durchbruch für die Genschere CRISPR

Die erste Gentherapie auf Grundlage der Genschere CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) steht kurz vor der Zulassung. Zwei kooperierende Firmen bessern damit Fehler in der menschlichen Erbinformation aus.

Mit der Genschere CRISPR-Cas9 (kurz CRISPR) lassen sich Erbinformationen punktgenau editieren, sodass sie auch aus IT-Sicht bemerkenswert erscheint: Es handelt sich um ein feines Werkzeug zur Programmierung der Baupläne von Lebewesen. In der Tier- und Pflanzenzüchtung wird sie schon eingesetzt.

Doch für die Behandlung von Erbkrankheiten genügte die Spezifität bisher nicht, weil in Laborexperimenten auch unerwünschte Stellen des Erbguts modifiziert wurden. Deshalb kommt der neuen Methode Exa-Cell der beiden Firmen Vertex und Crispr Therapeutics besondere Bedeutung zu. Exa-Cell richtet sich unter anderem gegen die Erbkrankheit Sichelzellenanämie (SZA). In den USA bringt das Gesundheitssystem für die SZA-Behandlung im Verlauf eines Patientenlebens 4 bis 6 Millionen US-Dollar auf.

Der SZA liegt eine Punktmutation im Bauplan des sauerstofftransportierenden Hämoglobinmoleküls zugrunde. Deshalb bauen Zellen einen falschen Baustein in die Hämoglobinkette ein, was weitreichende Folgen hat: Die Ketten verkleben zu Fibrillen. Die normalerweise diskusförmigen roten Blutkörperchen, die die Hämoglobine enthalten, verformen durch die Fibrillen zu Sicheln. Die Sicheln verstopfen Blutgefäße, und Patienten haben eine verminderte Lebenserwartung.

Die Exa-Cell-Therapie aktiviert ein Ersatzgen: Das Hämoglobingen, das bei Erwachsenen inaktiv ist (fötales Hämoglobin, HbF). Zwar enthalten die behandelten Zellen und somit die daraus hervorgehenden roten Blutkörperchen weiterhin mutiertes Hämoglobin, aber das HbF verhindert die Verklebung.

Für 17 Teilnehmer einer Studie gibt es seit Juni ein erstes Fazit: 16 haben in 12 aufeinanderfolgenden Monaten keine einzige Sichelzellkrise erlitten (zuvor im Schnitt je vier pro Jahr). Noch wichtiger dürfte sein, dass die Genschere nur dort ansetzt, wo sie soll. Das melden die Hersteller unter Berufung auf wiederholte Genomanalysen der 35 Studienteilnehmer (ct.de/yujv).

Deshalb sei Exa-Cell unterm Strich „gutartig“, befand die US-Behörde FDA im Oktober. Im Dezember dürfte sie der Methode grünes Licht für den Einsatz in den USA geben. Die Europäische Arzneimittelagentur hat den Einsatz schon genehmigt. Vertex und Crispr Therapeutics planen schon den Aufbau von Behandlungszentren. *(dz@ct.de)*

Exa-Cell-Infos: **ct.de/yujv**

Exa-Cell gegen Sichelzellenanämie

Anders als erwartet, repariert die Exa-Cell-Technik nicht die defekte Erbinformation, sondern entfernt die Blockade eines normalerweise nicht mehr gebrauchten Gens.

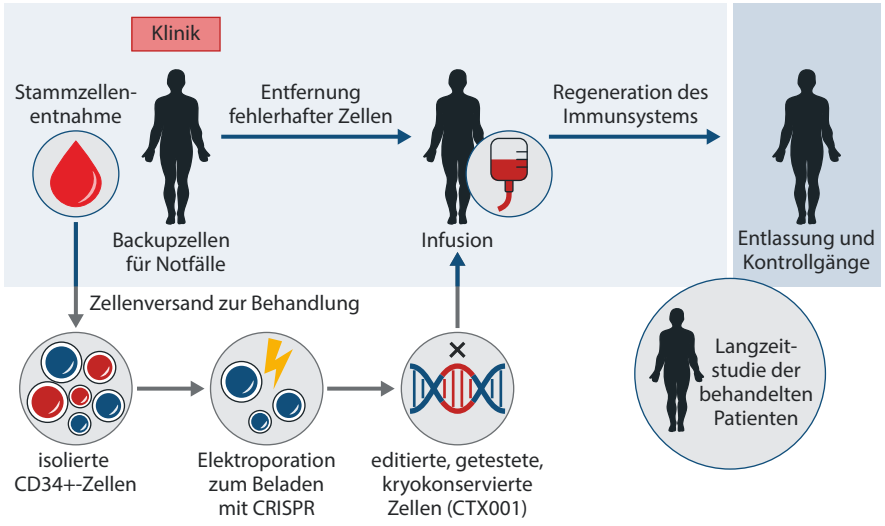


Bild: Crispr Therapeutics

Zugvögel in Amerika

explorer.audubon.org

Die US-amerikanische Umweltorganisation National Audubon Society sensibilisiert Menschen mithilfe einer interaktiven Karte von Nord- und Südamerika für Zugvögel. Auf der Startseite des englisch- und spanischsprachigen **Bird Migration Explorer** schalten Nutzer im „Map Layers"-Kasten rechts Vogelgruppen ein, etwa Land-, Wasser- oder Greifvögel. Auf der Karte erscheinen dann die Zugrouten von einzelnen getrackten Vögeln. Fährt man mit der Maus über die Routen, wird der jeweilige Weg hervorgehoben und der zugehörige Vogel angezeigt, per Klick darauf gelangt man zu Detailinformationen über die jeweilige Art.

In der Leiste oben wählen Nutzer, ob sie mehr über eine der gut 450 Spezies auf der Website lernen wollen (Bird Species), über bestimmte Orte und ihre Bedeutung für Zugvögel (Locations) oder über Herausforderungen beim Vogelschutz (Conservation Challenges). Das sind zum Beispiel Trockenheit, Windkraftwerke oder Lichtverschmutzung. Wählt man eine Vogelspezies aus, erscheinen links mehr Informationen dazu; unten verläuft ein Zeitstrahl und die Amerikakarte zeigt abhängig davon die Lebensräume der Spezies.

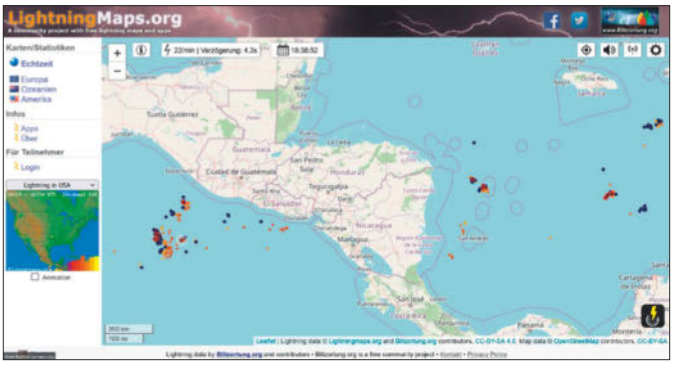
(gref@ct.de)

Blitze in Echtzeit

lightningmaps.org

blitzortung.org/de/cover_your_area

Wo auf der Welt gerade Blitze am Himmel zucken, zeigen bunte Punkte auf der Karte von **LightningMaps.org**. Oben links erklärt eine Legende (i-Symbol) die Farben der Blitzpunkte: Die jüngsten sind rot umkreist, ein weißer Umkreis zeigt ihre Donnerfront; ältere Blitze werden erst gelb, dann orange. Oben rechts blendet man zum Beispiel die Messstationen ein (Antennensymbol), was für Europa nur auf höheren Zoom-Stufen empfehlenswert ist, weil man sonst die Karte mit Stationsnamen zukleistert. Unter dem Zahnradsymbol rechts lässt sich zwischen Karten- und Satellitenansicht wechseln.

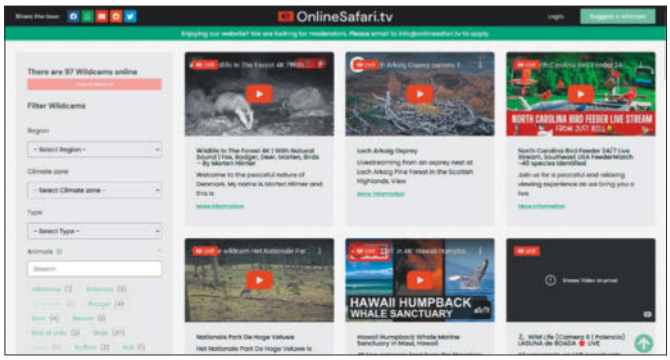


Die Macher warnen, dass man sich keinesfalls auf die Angaben verlassen darf, sie sollen nur der Unterhaltung dienen. Hinter dem Dienst steht das Netzwerk **Blitzortung.org**, eine Gruppe Freiwilliger, die Blitzdaten sammeln und aufbereiten. Dazu entwickeln sie eigene Empfänger für sehr niedrige Frequenzen mit GPS. Wer mitmachen möchte, informiert sich auf der Website der Gruppe über technische Details und die Blitzdetektor-Bauanleitung. *(gref@ct.de)*

Im Netz auf Safari

onlinesafari.tv

Zebras in der Kalahari-Wüste im Süden Afrikas, Rehe in Maine, Fische in Südflorida oder Weißstörche in Schweden: All diese Tiere können Besucher von **Onlinesafari.tv** beobachten, ohne das Haus zu verlassen. Die englischsprachige Website sammelt Livestreams von Wildkameras. Im Menü links lassen sich die Videostreams filtern: nach Region, Klimazone, Landschaftstyp und einzelnen Tierarten. Über den „More information"-Link unter einem Video gelangt man zur Großansicht inklusive Beschreibung und einer Karte der Region, in der die Kamera steht.



Laut der Website begann das Ganze als Hobbyprojekt, Ziel der Macher sei es, „Ehrfurcht und Wertschätzung für die Natur zu wecken und Menschen zu ermutigen, sich aktiv für die Umwelt einzusetzen". Wer auf YouTube einen spannenden Wildtierstream entdeckt, kann ihn über den Button „Suggest a wildcam" oben rechts für das Projekt vorschlagen. *(gref@ct.de)*

***Diese Seite mit klickbaren Links:** ct.de/y6jt*

SCHÜTZE DEINE INHALTE – OHNE VIEL DRUMHERUM!

Cordaware **bestzero**®: Verbindet Menschen mit Applikationen, nicht mit Netzwerken

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

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

Zeitgesteuerter und **2FA** bedingter Appzugriff.

Cordaware
bestzero®

☑ Verfügbar für Windows, macOS, Linux und Android

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

Entzaubert

Lenovo lässt Kunden-Notebook verschwinden

Wer ihm Anvertrautes beschädigt oder verliert, muss es ersetzen. Doch was eigentlich jedem einleuchtet, ist für Lenovo eine größere Herausforderung.

Von Tim Gerber

Ende November 2021 hatte Florian T. sich für knapp 1000 Euro ein Notebook Lenovo Yoga 14s angeschafft. Da der Berufsschullehrer den Rechner für die Arbeit benötigte, erwarb er ein Jahr später für 155 Euro eine Garantieerweiterung für weitere zwölf Monate, die auch einen Vor-Ort-Service umfasste. Damit war der Kunde gut beraten, denn kein halbes Jahr darauf, Anfang Mai, blieb überraschende der Bildschirm seines Rechners schwarz. Dank des gebuchten „Premier-Service“ kam am 12. Mai ein Techniker vorbei, der das Display tauschen sollte.

Zwar funktionierte dieses anschließend wieder, doch der Kunde bemängelte nun, dass der Techniker diverse andere Schäden verursacht habe. Nach seinen Schilderungen hatte der Fachmann das alte Display sehr unsanft aus dem Rahmen gelöst und dabei deutliche Kratzer hinterlassen. Zudem war das Aluminiumgehäuse nach der Aktion verbogen. Deshalb reklamierte Florian T. die Sache nun bei Lenovo. Der Hersteller bat ihn, das Gerät einzuschicken. Das geschah am 19. Mai.

Vier Wochen später, am 15. Juni, erhielt Florian T. die Nachricht, dass sein Notebook repariert sei und an ihn zurückgesendet werde. Doch zwei Wochen später war der sehnlich erwartete Rechner noch immer nicht zurück beim Kunden. Laut Sendungsverfolgung lag er bereits seit dem 24. Juni in einem Depot des Versanddienstleisters und bewegte sich kein Stück weiter. Deshalb wandte sich der Kunde an Lenovo und machte auf diese Ungereimtheit aufmerksam. Er möge noch ein paar Tage warten, vertröstete man den Kunden.

Nix bewegt sich

Aber das Paket mit seinem dringend benötigten Rechner bewegte sich nicht weiter von der Stelle. Deshalb rief Florian T. am 5. Juli erneut bei Lenovo an. Nun hieß es, man werde den Fall eskalieren und den Versanddienstleister beauftragen, nach dem Verbleib der Sendung zu forschen. Am 12. Juli stellte Florian T. fest, dass das

zugehörige Service-Ticket in Lenovos Support-Portal bereits wieder geschlossen worden war. Also rief er aufs Neue an und man sicherte ihm zu, es wiederzueröffnen.

Zwei Tage später meldete sich ein Zusteller bei Florian T. und machte ihn darauf aufmerksam, dass man keine korrekte Anschrift habe, um sein Paket zuzustellen. Die Straße fehle in dem Datensatz. Tatsächlich fehlte sie auch in den Absenderangaben auf dem Retourenlabel, das ihm Lenovo zugeschickt hatte, wie Florian T. aufgrund dieses Anrufes später feststellte. Zunächst aber teilte er dem Zusteller die Straße mit. Das Gerät sollte nun innerhalb einer Woche bei ihm sein, hieß es.

Am 25. Juli meldete sich Lenovo bei dem Kunden und der übermittelte ihnen seine Notiz über das Gespräch mit dem Zusteller zehn Tage zuvor. Per E-Mail vom selben Tag bat Lenovo ihn, sich zu melden, wenn er in den kommende drei Tagen nichts in der Sache hören würde. Dementsprechend rief Florian T. am 28. Juli erneut bei Lenovo an. Abermals vertröstete man ihn mit der Aussage, einen Suchauftrag an den Versanddienstleister richten zu wollen. Was denn aus dem Suchauftrag vom 5. Juli geworden sei, wollte der Kunde wissen. Eine Antwort wusste man bei Lenovo zwar nicht, gab sich aber dennoch optimistisch, dass die Sendung in den nächsten Tagen eintreffen werde.

Geduldsfaden

Doch nach weiteren zwei Wochen war die Sendung immer noch nicht angekommen. Am 14. August schrieb Florian T. deshalb erneut an Lenovo und forderte den Hersteller auf, ihm innerhalb einer Woche zu sagen, wie es mit seinem Notebook weitergehen solle. Da keinerlei Antwort kam, verlangte Florian T. am 13. September per Einschreiben von Lenovo, ihm binnen 14 Tagen das Geld für ein Ersatzgerät zu bezahlen. Gefruchtet hat auch das nichts. So wandte sich der langjährige Leser am 6. Oktober an c't.

Wir sprachen den Pressesprecher von Lenovo am 19. Oktober auf den Fall von Florian F. an und nun kam tatsächlich etwas Bewegung in die Sache. Zunächst aber nicht so, wie man es erwarten würde: Am 23. Oktober schrieb ein Customer Care Manager dem Kunden, man wolle ihm statt seines defekten Notebooks ein Austauschgerät anbieten. Dazu solle er jedoch erst einmal das defekte Gerät einschicken. Wenn er das Angebot annähme, werde er dafür ein Versandlabel zugeschickt bekommen.

Foto: Florian T.

Nach dem Tausch des Displays beim Kunden zu Hause war das Gehäuse deutlich verbogen, sodass der Notebook eingeschickt werden musste – auf Nimmerwiedersehen.

Florian T. war wenig erbaut über dieses Angebot. Wie sollte er denn ein Gerät einschicken, dass er gar nicht hatte? Entsprechend ungehalten antwortete er am selben Tage dem Kundenmanager und bestand auf die schon mit Einschreiben im September geforderte Schadensersatzzahlung. Darauf kam es dann zu einem Telefonat, bei dem die Sache mit dem verschollenen Notebook geklärt werden konnte. In einer weiteren Mail vom selben Tag stellte der Supportmanager klar, dass es sich um einen Verlust handle und der Teil mit der Rücksendung aus dem vorherigen Angebot mithin entfalle. Man werde ihm ein höherwertiges Gerät als Ersatz schicken, eine Barauszahlung lehne man indessen ab.

Im Ergebnis nahm Florian T. das Angebot dann an. Rechtlich ist das auch in Ordnung. Denn wer für einen entstandenen Schaden aufzukommen hat, muss lediglich den Zustand wieder so herstellen, wie er vor Eintritt des Schadens war. Demnach hatte Florian T. Anspruch auf äquivalenten Ersatz für sein anderthalb Jahre altes Notebook und fährt mit der Lieferung eines höherwertigen Ersatzgerätes sogar besser.

Als Kompensation für das ewige Hinhalten und monatelanges Warten auf die Regulierung des Schadens ist das allerdings mehr als billig. Denn dass es für die Anerkennung der Pflicht zur Schadensregulierung durch den Hersteller erst der Einschaltung der c't bedurfte, ist für ein großes Unternehmen wie Lenovo ziemlich unrühmlich. *(tig@ct.de)* c't

Service im Visier

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

Manchmal erreichen uns aber auch Schilderungen von geradezu haarsträubenden Fällen, die deutlich machen, wie einige Firmen mit ihren Kunden umspringen. In unserer Rubrik „Vorsicht, Kunde!" berichten wir über solche Entgleisungen, Ungerechtigkeiten und dubiose Geschäftspraktiken. Damit erfahren Sie als Kunde schon vor dem Kauf, was Sie bei dem jeweiligen Unternehmen erwarten oder manchmal sogar befürchten müssen. Und womöglich veranlassen unsere Berichte ja auch den einen oder anderen Anbieter, sich zukünftig etwas kundenfreundlicher und kulanter zu verhalten.

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

Aus alt mach schnell

Netzwerkspeicher geschickt aufrüsten und erweitern

NAS-Boxen leisten zwar jahrelang treue Dienste, zeigen aber früher oder später Schwächen: Die Festplatten sind irgendwann voll, das RAM zu klein oder der LAN-Port zu lahm. Überraschend viel lässt sich verbessern.

Von Christof Windeck und Dušan Živadinović

Netzwerkspeicher alias Network Attached Storage, kurz NAS, sind eigentlich Geräte zum Aufstellen und Vergessen: Einmal eingerichtet dienen sie als Datentümpel, die Backups, Fotos, Videos und Musikdateien klaglos schlucken und zentral bereitstellen. Doch eines Tages wünscht man sich vielleicht mehr, als ein älteres NAS leistet: mehr Festplattenkapazität, eine schnellere Netzwerkanbindung oder zusätzliche Dienste, in einer virtuellen Maschine (VM) oder einem Docker-Container. Bei vielen NAS-Modellen lassen sich diese Wünsche mit ein bisschen Tüfteln preisgünstig erfüllen.

Technisch spielt es keine Rolle, was Sie zuerst in Angriff nehmen, aber Sie können viel Zeit sparen, wenn Sie kontraintuitiv vorgehen: Rüsten Sie den Massenspeicher nicht zuerst auf, auch wenn da der Schuh am heftigsten zwickt.

Kontraintuitiv aufrüsten

Prüfen Sie stattdessen zuerst die Auslastung des Arbeitsspeichers (RAM): Wenn die am Anschlag ist, dürfte es helfen, zuerst das RAM-Angebot zu vergrößern, denn viele Prozesse laufen bei knappem RAM nur noch gebremst. Beim Aufrüsten muss man aber darauf achten, mit welchen RAM-Bausteinen ein NAS überhaupt klarkommt (siehe S. 62).

Falls das NAS große Datenmengen aus dem LAN beziehen soll, etwa Videos oder große Archive von PCs, empfiehlt es sich außerdem, die Netzwerkanbindung vom üblichen Gigabit-Ethernet auf 2,5 Gigabit/s (2G5) zu beschleunigen. Der Zeitpunkt für 2G5 erscheint günstig, weil die Preise für Aufrüstungen zuletzt erheblich gesunken sind, und weil 2G5 in vielen Heimnetzen mit den bereits verlegten Kabeln auskommt. Üblicherweise handelt es sich dabei um CAT5e-Kabel. Switche für 2G5, die man einfach hinter den Router klemmt, gibt es seit dem Sommer schon ab 70 Euro; PC- und NAS-Erweiterungen für 2,5-Gigabit-Ethernet ab rund 25 Euro. Einzelheiten dazu finden Sie im Schwerpunkt in c't 23/2023 auf Seite 88.

In diesem Heft erklären wir ab Seite 60, worauf Sie bei der Auswahl frischer NAS-Festplatten achten sollten und weshalb SSDs nur selten sinnvoll sind. Aber generell gilt: Je mehr Daten ein NAS schluckt, desto mehr Wichtiges ist darunter. Deshalb spielt die richtige Backup-Strategie mit der Zeit eine immer größere Rolle. Die ist gerade bei Synology-Geräten knifflig, wenn man auch virtuelle Maschinen (VM) automatisch sichern will. Ab Seite 64 spielen wir am Beispiel des Mittelklasse-NAS Synology DS1621+ durch, wie man Daten auf fernen Netzwerkspeichern in Sicherheit bringt.

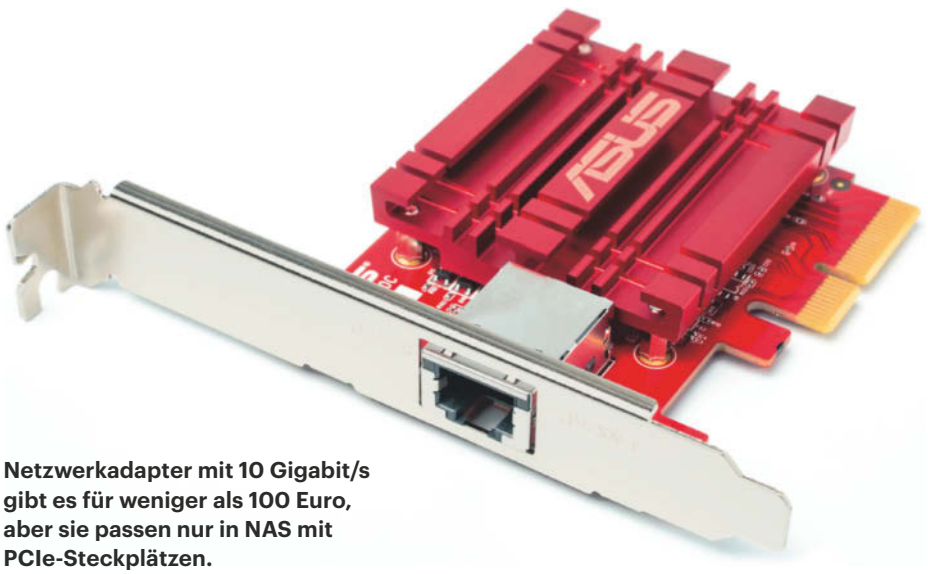
Aufrüstbedarf

Klar ist, dass man aus einem schlichten 150-Euro-NAS keinen pfeilschnellen Heimserver mit üppiger RAM-Ausstattung und 10-Gigabit-Ethernet machen kann. Doch es stellt sich die Frage, woran man NAS-Boxen erkennt, bei denen sich das Aufrüsten lohnt. Um das zu beurteilen, sollten Sie einige Basisdaten kennen.

Gigabit-Ethernet (1GE) befördert maximal 115 MByte pro Sekunde. So dauert die Übertragung einer komprimierten Backup-Datei von 2 GByte Größe rund 20 Sekunden. Selbst zehn Jahre alte Festplatten sind dafür schnell genug und schon einfache NAS mit wenig RAM und sparsamem ARM-Chip liefern vollen Gigabitdurchsatz, zumindest, wenn sie die Daten unverschlüsselt auf der Platte speichern.

Um Gigabit-Ethernet unter gängigen Computerschnittstellen einzuordnen und um abzuschätzen, ob eine Aufrüstung überhaupt lohnt, hier noch einige Vergleichswerte: 115 MByte/s sind mehr als der doppelte Durchsatz von USB 2.0 Highspeed (480 Mbit/s, rund 55 MByte/s), aber gegenüber flinken, per USB 3.0 angekoppelten SSDs (450 MByte/s) gerade mal ein Viertel. Eine mittelmäßige Wi-Fi-5-Verbindung von einem Notebook über 15 Meter durch zwei Wände zum WLAN-Router liefert im Vergleich zu Gigabit-Ethernet nur einen Bruchteil. In günstigen Fällen sind es etwa 10 MByte/s und nur so viel wie eine 20 Jahre alte Fast-Ethernet-Karte.

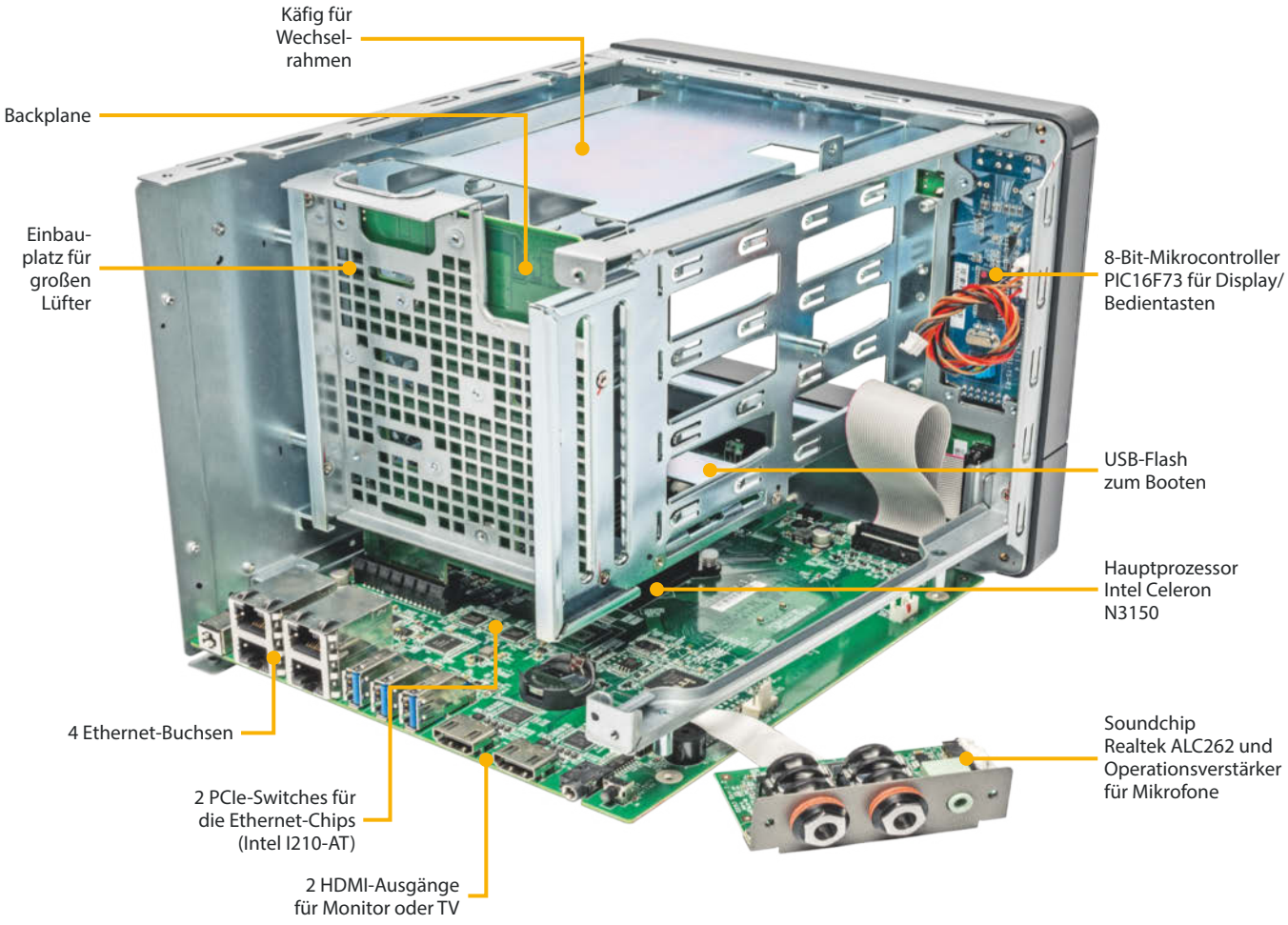
Daraus ergeben sich konkrete Richtwerte: Wenn Sie Backups per WLAN aufs NAS schreiben, genügt oft ein simples oder älteres NAS. Wenn es schneller



Netzwerkadapter mit 10 Gigabit/s gibt es für weniger als 100 Euro, aber sie passen nur in NAS mit PCIe-Steckplätzen.

Innenansicht eines älteren Netzwerkspeichers von QNAP

Hinten sind neben den vier Gigabit-Ethernet-Buchsen drei USB-Ports angebracht, die bis zu 5 Gbit/s befördern. Darüber kann man manches alte Schätzchen auf 2,5 Gigabit/s fürs LAN aufrüsten.



gehen soll, müssen Sie Ihr Backup-Ziel per Gigabit-Ethernet ansteuern oder lokal auf eine USB-SSD schreiben lassen. 2G5 kann die Übertragungsdauer gegenüber 1GE locker halbieren, der maximale Durchsatz von 2G5 beträgt etwa 280 MByte/s. Um diese Datenrate auszuschöpfen, müssen die im NAS eingesetzten Platten mindestens so schnell liefern. Moderne Platten erreichen über 250 MByte/s (siehe S. 60) und sind damit auf demselben Niveau wie 2G5.

Mit 5 und 10 Gbit/s gibt es noch schnelleres Ethernet für übliche Installationen auf Basis von CAT5e-Kabeln. Aber das sind teure Nischenprodukte und übliche Massenspeicher von NAS-Geräten sind dafür zu langsam. Nur bei schnellen RAID5-Konfigurationen reizt ein NAS auch 5GE aus, weil es dann zwei Platten gleichzeitig anzapft und so deren Datenrate addiert. Gleiches gilt für den Fall, dass im NAS ein SSD-Cache steckt.

Um 2G5 auszuschöpfen, braucht man ein NAS mit ausreichend schnellem Prozessor. Die meisten ARM-Kerne von Geräten, die neu unter 200 Euro gekostet haben, sind dafür zu schlapp, zumal, wenn sie auch verschlüsseln sollen. Erst x86-Chips wie der Intel Celeron J4105 schaffen über 200 MByte/s und erfüllen damit die Voraussetzungen für 2G5.

CPU und RAM

Die bequemste Art, den Softwarefunktionsumfang eines NAS zu erweitern, sind vom jeweiligen Hersteller oder anderen Entwicklern bereitgestellte Programmpakete oder Plug-ins. Die installiert man ruckzuck aus Onlineshops, für die das NAS-Betriebssystem vorbereitet ist. Dabei kommt es auch auf den CPU-Typ an, also ARM- oder x86-Architektur. Auf den billigeren und sparsameren ARM-Chips läuft manche Software nicht und falls sich überhaupt VMs oder Container aktivieren lassen, dann nur in Form von ARM-, nicht aber als x86-Software.

Zu beachten ist auch, dass VMs mehr RAM brauchen, als kleine Netzwerkspeicher ab Werk mitbringen. Aber nur sehr wenige NAS mit ARM-Chips haben Speichersteckplätze, weswegen sich bei den meisten der Arbeitsspeicher nicht erweitern lässt. Auch die billigeren NAS mit x86-Chips wie Celeron haben aufgelöteten, nicht erweiterbaren Speicher, oft nur 1 oder 2 GByte. RAM-Aufrüstungen gehen da nur, wenn ein Steckplatz vorhanden ist – mehr dazu ab Seite 62.

Für diesen heiklen Job braucht der Cyberdealer seine Crew!

Doppelter RAM am Orange Friday!

24.11.2023

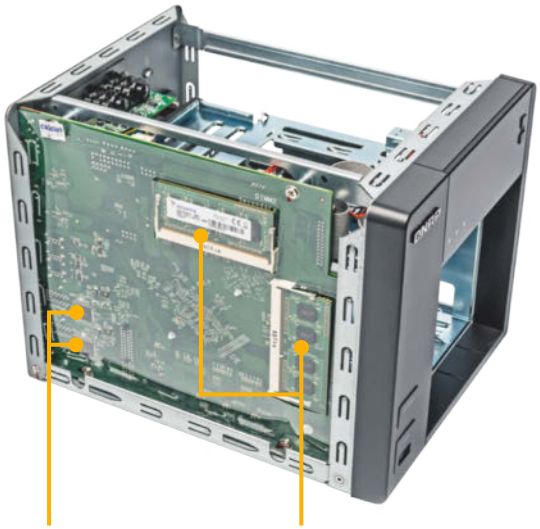
Da gehen selbst dem Cyberdealer die Hände aus: Am Orange Friday zieht er bei Thomas-Krenn seinen nächsten großen Coup durch, und schenkt allen Bestellern ohne Aufpreis den doppelten Arbeitsspeicher für ihre gewählte Konfiguration. Und als wäre dieser verboten gute Deal nicht genug, ist außerdem ein mysteriöses Glücksrad mit wertvollen Sachpreisen in unserer Produktionshalle aufgetaucht...

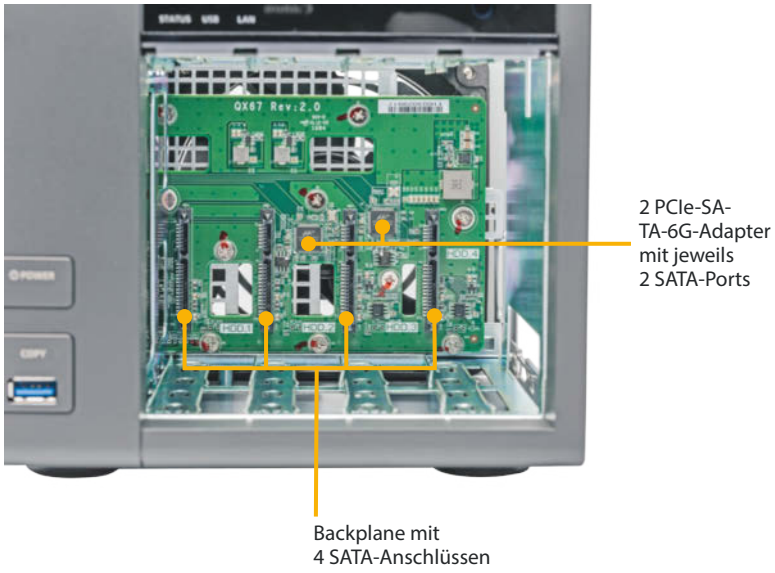
Vorab Infos unter:
thomas-krenn.com/of23
+49 (0) 8551.9150-300

THOMAS KRENN®
IT's people business

Mehr RAM als gedacht

Manche Hersteller geben in den Spezifikationen geringere RAM-Kapazitäten an, als das NAS tatsächlich aufnehmen kann. Beispielsweise lässt sich das QNAP TS-453A auf 16 GByte RAM aufrüsten, obwohl der Hersteller 8 GByte als Maximum nennt.





Bei den meisten NAS der Preisklasse unter 800 Euro ist auch der Prozessor aufgelötet, also nicht austauschbar. CPU-Wechselfassungen enthalten überwiegend erst Geräte ab 1000 Euro, oft zusammen mit ECC-RAM, das per Error Correction Code (ECC) vor den häufigsten Bitfehlern geschützt ist. Im Grunde sind solche NAS kleine Server, weil sie ohne Schnaufen mehrere VMs und Container parallel ausführen.

RAID-Fragen

Die häufigste Art, ein NAS aufzupeppen, dürfte der Austausch der Festplatten sein. Dazu enthalten praktisch alle NAS-Betriebssysteme Umzugsfunktionen. Letztere gründen oft auf Funktionen, die für die Reparatur eines Festplattenverbunds (RAID, Redundant Array of Independent Disks) gedacht sind. Das nennt man auch RAID Rebuild. Ein Beispiel: Beim verbreiteten RAID 1 aus zwei Platten ist die zweite ein „Spiegel“ (Mirror) der ersten. Entfernt man eine der beiden und setzt dafür eine neue ein, kopiert das Betriebssystem die Daten vom Spiegel auf die leere Platte. Doch Achtung: Der Vorgang kann sehr lange, nämlich einige Stunden dauern [1] und währenddessen besteht keine Redundanz. Man kann aber auch ein Backup auf ein anderes NAS oder eine USB-Platte schreiben, dann die Platten tauschen und die Daten vom Backup einspielen. Das geht in manchen Szenarien tatsächlich schneller, siehe [1]: Bei 100 MByte/s Schreibgeschwindigkeit dauert das Kopieren von 10 TByte Daten mehr als 25 Stunden.

Welcher Plattentyp für Ihr NAS infrage kommt, erklärt der Artikel ab Seite 60. Vor dem Kauf sollten Sie abwägen, ob Sie einen redundanten Plattenverbund einrichten wollen und falls ja, in welcher RAID-Stufe. Denn angesichts der riesigen Kapazitäten von mehr als 20 TByte pro Platte ist ein RAID 5 aus drei Laufwerken oft übertrieben, meistens genügt ein RAID 1 oder gar kein RAID. Im Zweifel gibt das Motto: „Keep it simple, stupid“ eine gute Orientierung: RAID 1 ist besonders robust, mehr brauchts in der Regel nicht.

Ohne RAID schluckt das NAS weniger Strom und läuft leiser. Wenn Sie regelmäßig Backups auf einer externen USB-Platte oder einem anderen NAS anlegen, sind diese oft besser gegen Verlust geschützt: Kein Verschlüsselungstrojaner erreicht Daten auf einer nicht angeschlossenen USB-Platte. Und ein NAS in einer anderen Stadt ist von Brand, Überschwemmung und Diebstahl wahrscheinlich nicht betroffen. Wie Sie das auf einem Netzwerkspeicher von Synology mit dem Tool Snapshot Replication auch für virtuelle Maschinen umsetzen, beschreiben wir ab Seite 64.

Plattenboxen

Wenn die Massenspeicherkapazität nicht genügt, muss man nicht zwangsläufig in größere Festplatten investieren. Stattdessen kann man an viele Netzwerkspeichermodelle Erweiterungsboxen über eSATA- oder USB-Ports anschließen und darin weitere Festplatten betreiben. Sie lassen sich dann wie interne Laufwerke über die Benutzeroberfläche des NAS einbinden. Bei Synology-NAS-Geräten ist das auch der einzige Weg, Festplatten mit fremden Dateisystemen wie ZFS einzubinden, um davon Daten wenigstens mittelbar über eine für ZFS konfigurierte VM einzulesen. Plattenboxen der NAS-Hersteller kosten aber leicht mehrere hundert Euro, während einfache USB-Boxen schon ab 50 Euro zu haben sind. Bessere Modelle kann man per USB 3.2 Gen 1 mit 5 Gbit/s ansprechen (ct.de/y4t7).

Für die Betriebskosten sind jedoch wenige größere Platten günstiger als mehrere kleine, denn jede zusätzliche Platte schluckt Strom. Moderne Laufwerke mit

10 TByte und mehr benötigen ohne Zugriffe schon 4 bis 6 Watt, wenn nur ihr Plattenstapel rotiert. Bei Dauerbetrieb kommen jährlich 35 bis 52 Kilowattstunden (kWh) pro Platte zusammen, also mindestens 10 bis 15 Euro pro Laufwerk und Jahr. Daher sparen Sie Geld, wenn Sie die Spindown-Funktion einschalten, sodass die Platten wenigstens in längeren Ruhephasen anhalten.

Für RAID-Verbünde empfehlen einige NAS-Hersteller regelmäßige Prüfläufe (Scrubbing): Das System liest sämtliche Daten aus und vergleicht sie mit den redundanten Informationen. Das beugt Datenverlust durch zuvor unerkannte Lesefehler vor. Weil das Scrubbing von 10 TByte Daten 25 Stunden dauern kann, erhöht das die Stromkosten. Doch weil das typischerweise nur monatlich geschieht, erhöht sich die Leistungsaufnahme nur um etwa 3 Prozent.

Das Foto zeigt ein ehemaliges Mittelklasse-NAS mit vier Plattenschächten (Bays), von denen drei belegt sind. Aus Sicht der Datensicherheit genügt heute oft ein einfacher Festplattenspiegel, bei dem je zwei Platten dieselben Datensätze redundant vorhalten (RAID 1). Aber wer regelmäßig Backups anlegt, kann darauf verzichten und Stromkosten sparen.

Schnelleres Netz

Viele teurere NAS-Boxen haben einen oder zwei PCI-Express-Steckplätze (PCIe). Diese sind vor allem zum Aufrüsten der Netzwerkschnittstellen gedacht, etwa für 10-Gigabit-Ethernet (10GE). Ältere Netzwerkspeicher enthalten Treiber für nur wenige Netzwerkadapter – vorwiegend für Karten, die der jeweilige NAS-Hersteller selbst verkauft. Doch gängige Adapter im Half-Height-Format mit kürzerem Slotblech funktionieren oft auch, sofern sie mechanisch in den Steckplatz passen. Eine Karte mit vier Lanes (PCIe x4) passt nicht in einen Slot mit nur einer Lane (x1). Umgekehrt gibt es längere Steckfassungen (etwa x4 oder x8), die elektrisch mit weniger Lanes beschaltet sind. Da muss man vor dem Kauf einer Erweiterungskarte genau hinschauen.

PCIe ist auf- und abwärtskompatibel: Eine PCIe-x1-Karte läuft auch in einem x4-Slot und eine Karte der dritten Generation (PCIe 3.0) auch in einem älteren Slot (PCIe 1.0 oder 2.0). Doch ihre volle Geschwindigkeit erreicht eine PCIe-3.0-Karte in einem PCIe-2.0-Slot eben nicht.

Die meisten günstigeren NAS-Boxen haben keine PCIe-Slots. Dann kann man den Netzwerkport bestenfalls per USB aufrüsten. Für 2G5 braucht man USB 3.0 alias USB 3.2 Gen 1 mit 5 Gbit/s. USB 2.0 Highspeed ist schon für 1GE zu lahm. Der NAS-Hersteller QNAP hat viele seiner Netzwerkspeicher der Einstiegs- und Mittelklasse für die Aufrüstung auf 2G5 mit einem hauseigenen USB-Ethernet-Adapter ausgelegt (ct.de/y4t7). Daher genügt es, den Adapter QNAP QNA-UC5G1T einfach ans NAS anzustecken; er eignet sich sogar für Ethernet mit 5 Gigabit/s (5GE). Synology hat bisher keine Ethernet-Aufrüstung über USB vorgesehen. Über quelloffene Treiber funktioniert die Aufrüstung aber dennoch. Wir haben den Vorgang in c't 23/2023 ab Seite 138 durchgespielt.

VMs, Container und Gnadenbrot

Zwar gründen die NAS-Betriebssysteme auf Linux und nutzen oft auch Linux-Standardfunktionen etwa für das RAID, sie lassen sich aber nicht einfach gegen alternative Betriebssysteme oder ein quelloffenes Linux austauschen. Daher laufen auf den NAS-Geräten VMs oder Container nur dann, wenn der Hersteller die erforderlichen Funktionen implementiert hat oder Softwarenachrüstungen ermöglicht.

Ebenso hängt es vom Hersteller ab, wie lange man ein NAS sicher betreiben und darauf auch aus der Ferne zugreifen kann. Denn es gibt beispielsweise Verschlüsselungstrojaner, die auf anfällige NAS-Betriebssysteme losgehen. Deshalb empfiehlt es sich, alte NAS-Geräte spätestens dann aus der Schusslinie zu nehmen, wenn der Hersteller die Sicherheitspflege einstellt. Die einfachste und zugleich wichtigste Maßnahme besteht dann darin, die zugehörigen Ports im Router zu schließen und auf die NAS-Dienste aus der Ferne nur über ein VPN zuzugreifen.

Falls sich das NAS selbstständig ein Loch durch die Firewall ins Internet bohrt, zieht man die aus der Ferne erreichbaren Dienste möglichst auf eine moderne Plattform um und schaltet sie im NAS ab. Von außen erreichbare Dienste kann man über eine VM bereitstellen oder auf einem zusätzlichen Raspberry Pi. Im abgesicherten Heimnetz hinter dem Router kann man das alte NAS dann relativ sicher weiternutzen, bis ein neues einzieht. *(dz@ct.de)* c't

NAS-Geräte der Einstiegs- und Mittelklasse lassen sich nicht per PCI-Karte auf schnelles Ethernet aufrüsten. Aber für manche Modelle mit schnellem USB-Anschluss kommen auch USB-Ethernet-Adapter infrage, beispielsweise der links abgebildete Trendnet TUC-ET5G. Er eignet sich sogar für Ethernet mit 5 Gigabit/s.

Literatur

[1] Christof Windeck, RAID-Riesen, Multi-Terabyte-Festplatten zuverlässig im (NAS-)RAID betreiben, c't 6/2021, S. 112

NAS-Aufrüstungen: ct.de/y4t7

Speicher satt

Festplatten für Netzwerkspeicher

Wer viel NAS-Speicherplatz benötigt, greift meistens zu Magnetfestplatten. Der Kauf von speziell für NAS ausgelegten Festplatten scheint naheliegend, doch viele Serverfestplatten eignen sich sogar besser. Wir klären, was in welchem Fall sinnvoll ist.

Von Lutz Labs

Müssen es zehn, zwanzig oder gleich fünfzig Terabyte sein oder reichen vielleicht zwei oder drei? Je mehr Speicher man braucht, desto mehr lohnt es sich, über dafür geeignete Laufwerke nachzudenken. NAS-Laufwerke kosten pro Terabyte meistens deutlich mehr als einfache Desktopfestplatten, doch diese sind für ein dauerlaufendes NAS schlecht geeignet. Es gibt bessere Möglichkeiten, beim Laufwerkskauf zu sparen.

Der persönliche Datenbestand wächst in vielen Fällen stetig, aber nicht rasant; die meisten Anwender können ihren persönlichen Bedarf gut einschätzen. Beim Ersatz vorhandener Laufwerke ist es einfach: Rechnen Sie einen zusätzlichen Bedarf von beispielsweise 10 Prozent pro Jahr über die nächsten fünf Jahre ein, dann sind die Platten aus der Garantie heraus und sollten gegen frische Laufwerke getauscht werden. Beim erstmaligen Einsatz eines NAS schauen Sie sich an, welche Datenmengen zu sichern sind und legen Sie großzügig noch einmal die gleiche Menge drauf – dann passen auch verschiedene Versionen einer Datei und es bleibt etwas Reserve.

Die allermeisten NAS-Gehäuse haben Schächte für 3,5-Zoll-Festplatten mit SATA-Anschluss; dort passen auch 2,5-Zoll-Festplatten oder gleich große SSDs hinein. 2,5-Zoll-Festplatten sind keine echte Alternative: Die größte spezielle NAS-Festplatte fasst lediglich 1 TByte. 2,5-Zoll-Festplatten sind zwar leiser als ihre größeren Verwandten, aber solche geringen Kapazitäten bedient man heutzutage besser mit einer SSD: noch leiser, kaum teurer und wahrscheinlich langlebiger. Einen Geschwindigkeitszuwachs wird man durch den Einsatz einer SSD jedoch kaum erhalten (siehe Kasten „SSD im NAS“ rechts).

Es gibt zwar 2,5-Zoll-Festplatten mit bis zu 5 TByte Speicherplatz, aber diese Laufwerke sind nicht dauerlaufgeeignet und sie nutzen das Aufzeichnungsverfahren Shingled Magnetic Recording (SMR) – und das kann beim Rebuild eines RAID-Verbunds zu Schwierigkeiten führen.

Hersteller: die letzten Drei

Es gibt drei Festplattenhersteller: Seagate, Toshiba und Western Digital. Manchmal laufen einem noch andere Herstellernamen über den Weg, doch nach unseren Erfahrungen kann man sagen: Finger weg!

HGST etwa ist vor einigen Jahren von Western Digital übernommen worden, nun verschwindet der Name so langsam. Jetzt noch unter dem Label HGST angebotene Laufwerke liegen also schon seit einiger Zeit in den Lagern der Distributoren herum. Ähnlich verhält es sich mit Samsung-Festplatten: Die letzte Neuvorstellung ist bald zehn Jahre her. Greifen Sie lieber zu einem aktuellen Festplattendesign.

Gelegentlich findet man Festplatten von i.norys, Walter Panther und Max Digital Data. Von diesen Unternehmen gab es oder gibt es noch Laufwerke, die Geräten von Seagate, Toshiba oder Western Digital nicht nur verblüffend ähnlich sehen: Die Unterschiede bestehen meistens lediglich aus den Aufklebern. Teils stammen die Laufwerke aus Überproduktionen, teils erfüllen sie die Qualitätsanforderungen der Hersteller nicht zu 100 Prozent, teils handelt es sich um reparierte Rückläufer [1].

Eine Ausnahme aber gibt es: Der NAS-Hersteller Synology hat zwei Festplattenserien im Angebot: die HAT5300/5310 [2], welche nahezu baugleich ist mit der Enterprise-Serie von Toshiba; und die HAT3300-Serie basiert auf den NAS-Laufwerken von Seagates Ironwolf. Beide Serien hat Synology mit den Herstellern zusammen auf seine NAS-Gehäuse abgestimmt. Vorteil für den Kunden ist, dass er bei Problemen nur noch einen Ansprechpartner hat, Nachteil ist der etwas höhere Preis. Synology drängt seine Kunden ein wenig zu seinen hauseigenen Laufwerken, indem das Unternehmen immer weniger Laufwerke anderer Hersteller für seine Netzwerkspeicher zertifiziert.

NAS-Plattenkunde

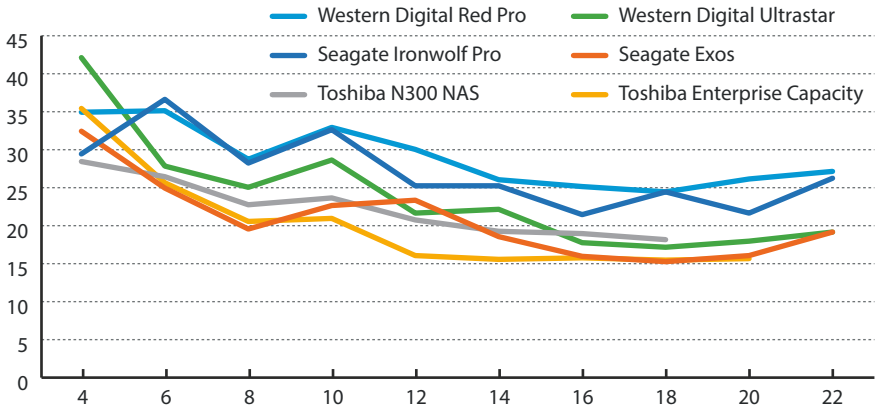
Bei Toshiba ist es einfach: Für NAS gibt es die N300 mit Kapazitäten bis zu 18 TByte. Seagate hat zwei NAS-Serien im Programm: die Ironwolf mit bis zu 12 TByte und die Ironwolf Pro, die maximal 22 TByte Speicherplatz bereitstellt. Innerhalb der einfachen Ironwolf-Serie gibt es Unterschiede, etwa jeweils zwei Modelle mit 8 und 10 TByte mit verschiedenen Eigenschaften: Umdrehungsgeschwindigkeit, Resilienz gegen nicht korrigierbare Lesefehler oder Helium- und Luftfüllung. Gerade letzteres ist wichtig, da die heliumgefüllten Laufwerke im Betrieb deutlich sparsamer sind; im Lauf eines Festplattenlebens können sich damit bei den Stromkosten Unterschiede im Bereich einiger zehn Euro ergeben.

Bei Western Digital gibt es sogar drei NAS-Reihen. Die einfachsten Modelle sind die Red mit Kapazitäten von 2 bis 6 TByte und eventuell problematischer SMR-Aufzeichnung. Nur wenig teurer sind die Red Plus mit konventioneller Aufzeichnungstechnik (Conventional Magnetic Recording, CMR) und Kapazitäten bis 14 TByte, darüber liegen dann die Pro-Versionen der Red, ebenfalls mit CMR-Aufzeichnung und Kapazitäten bis 22 TByte.

Die größten Unterschiede zwischen den einfachen Laufwerken und den Pro-Versionen liegen im Preis und in der Garantiefrist: Während die einfachen Laufwerke nach drei Jahren aus der Garantie fallen, haben die Pro-Laufwerke fünf Jahre Garantie. Doch Achtung: Für im Einzelhandel verkaufte OEM-Platten gilt die Herstellergarantie nicht, sondern nur die gesetzliche Gewährleistungspflicht des Händlers von 24 Monaten Dauer. Prüfen Sie also nach dem Kauf direkt über die Tools der Hersteller, welche Platten man Ihnen wirklich verkauft hat (siehe ct.de/yvyh).

Festplattenpreise im Vergleich

Der Preis pro TByte Speicherplatz schwankt zwischen 16 und mehr als 40 Euro, je nach Kapazität. Serverplatten sind bei gleicher Ausstattung meistens günstiger als die NAS-Modelle der Hersteller.



Warenkunde Serverfestplatten

Bei den Serverlaufwerken gibt es von jedem Hersteller grundsätzlich zwar nur ein Modell, die Vielfalt ist im Detail dennoch größer. Es gibt Laufwerke mit SATA- und SAS-Anschlüssen und mit verschiedenen Sektorgrößen: Während NAS-Laufwerke lediglich mit 512 Byte großen Sektoren erhältlich sind, was für NAS-Boxen auch sinnvoll ist, bauen Toshiba und Western Digital auch welche mit 4096 Byte, die Seagate-Modelle lassen sich gar vom Anwender umkonfigurieren. Außerdem liegt die von den Herstellern spezifizierte Wahrscheinlichkeit für nicht korrigierbare Lesefehler bei einigen Serverlaufwerken um den Faktor 10 oder sogar 100 niedriger als bei NAS- und Desktop-PC-Platten.

Weiterhin gibt es Serverlaufwerke mit Verschlüsselung, teils auch mit FIPS-Zertifizierung (Federal Information Processing Standards Publication 140-2) und mit der Funktion Instant Secure Erase (ISE). Diese löscht Daten sicher innerhalb von Sekundenbruchteilen durch Verwerfen des Schlüssels.

Seagate teilt die Exos-Serie noch in verschiedene Familien auf, etwa die X18-Familie. Diese gibt es mit 18 und mit 16 TByte, beide haben je 9 Scheiben und 18 Schreib-Lese-Köpfe eingebaut. Mechanisch gibt es keinen Unterschied zwischen den beiden, bei der 16er liegen eine Scheibe sowie zwei Köpfe einfach brach.

Die Ultrastar-Serie von Western Digital ist vom Hersteller nicht für den Verkauf im normalen Handel bestimmt; die Laufwerke finden aber trotzdem den Weg dorthin. Da stehen sie dann neben den Gold-Laufwerken, welche den einfacheren SATA-Modellen der Ultrastar mit 512-Byte-Sektoren entsprechen.

Server- oder NAS-Platte?

Grundsätzlich spricht nichts gegen eine Serverfestplatte im heimischen NAS. Schauen Sie jedoch vor dem Kauf in die Kompatibilitätslisten der NAS-Hersteller. Wahrscheinlich werden zwar auch alle anderen dort nicht aufgeführten Laufwerke funktionieren, doch mit den vom Hersteller freigegebenen Laufwerken senken Sie das Risiko für Inkompatibilitäten.

Wie zuverlässig ein spezifisches Modell in einem NAS funktioniert, lässt sich nicht vorhersagen. Auch Statistiken von Cloudprovidern wie Backblaze über die Ausfallraten einzelner Laufwerke haben für den heimischen Einzelfall nur wenig Bedeutung. Daher spricht nichts dagegen, sich nach Festlegung aller Spezifikationen beim Kauf von NAS-Festplatten am Preis zu orientieren. *(ll@ct.de)* c't

SSDs im NAS

In vielen „richtigen" Servern haben SSDs längst die Festplatten abgelöst, aber in NAS für Privatleute oder kleine Arbeitsgruppen bringen SSDs nur in Spezialfällen Vorteile. Denn schon aktuelle Festplatten sind mit Datentransferraten von über 250 MByte/s schneller als Ethernet mit 2,5 Gbit/s, was vielfach der bestimmende Flaschenhals beim Transfer ist. Und der größte SSD-Vorteil, nämlich extrem geringe Latenzen beziehungsweise hohe IOPS-Werte, kommt in NAS nur selten zum Tragen. Hier geht es meistens um sequenzielle Zugriffe.

Somit bleiben ein paar Sonderfälle für SSDs im NAS, beispielsweise für besonders kompakte Geräte, die keine hohe Kapazität bereitstellen, aber sehr leise und sparsam arbeiten sollen. Zudem gibt es auf dem NAS laufende Anwendungen, die von einer SSD profitieren, etwa Datenbanken; auch beim gleichzeitigen Zugriff vieler Nutzer ist eine SSD einer Festplatte überlegen.

Ein weiterer Spezialfall sind Cache-SSDs für das NAS. Im Test mit einer M.2-SSD in einem QNAP-NAS brachte das beim linearen Dateizugriff wenig. Zugriffe auf zufällige Adressen profitieren hingegen von einer Cache-SSD, die IOPS schossen auf das Dreißigfache hoch: Im Netz liegende Datenbanken sind so plötzlich benutzbar. Ob sich der Kauf einer SSD rentiert, lässt sich damit nur im Einzelfall beurteilen.

Literatur

[1] Lutz Labs, Umgelabelt, Billigfestplatte von i.norys, c't 21/2016, S. 100
[2] Lutz Labs, NAS-Spezialisten, Festplatten vom NAS-Hersteller Synology, c't 5/2021, S. 34
[3] Lutz Labs, Plattenkarussell, Festplatten für NAS und Server im Vergleichstest, c't 3/2023, S. 88
[4] Ernst Ahlers, Speicherzwillinge, Zwei 2-Bay-NAS im Vergleich: QNAP TS-264 und TS-253E, c't 6/2023, S. 81

Garantieabfragen der Festplattenhersteller: ***ct.de/yvyh***

NAS-RAM

Arbeitsspeicher von Netzwerkspeichern (NAS) aufrüsten

In manches NAS passt viel mehr RAM, als man erwartet. Ein größerer Arbeitsspeicher bringt virtuelle Maschinen, Container und einige Plug-ins auf Trab.

Von Christof Windeck

Viele NAS-Boxen – vor allem günstige Modelle – sind ab Werk mit sehr wenig RAM bestückt, beispielsweise nur 1 oder 2 GByte. Das genügt für die NAS-Kernaufgabe als zentrales Datenlager im (Heim-)Netz. Doch wer auf dem NAS eine Datenbank betreiben will, eine virtuelle Maschine (VM) oder Docker-Container, wünscht sich oft mehr. Und das ist nicht einmal teuer: Einen 8-GByte-Speicherriegel gibt es schon für weniger als 20 Euro.

Manches NAS lässt sich sehr einfach und günstig mit zusätzlichem Arbeitsspeicher bestücken: Man öffnet das Gehäuse, steckt ein zusätzliches Speichermodul ein oder tauscht das vorhandene gegen eines mit höherer Kapazität aus, schließt das Gehäuse wieder – fertig.

So einfach ist es jedoch nicht bei jedem NAS. Bei manchen ist das RAM etwa fest aufgelötet und nicht erweiterbar. In vielen der billigsten NAS-Boxen stecken ein System-on-Chip (SoC) mit ARM-Kernen sowie beispielsweise 512 MByte oder 1 GByte aufgelötetes RAM. Trotzdem liefern sie Daten fast mit der maximalen Geschwindigkeit, die die 1-Gigabit-Ethernetschnittstelle schafft, also mit rund 100 MByte/s.

Da RAM-fressende VMs und Container eher auf NAS mit x86-Chips von AMD und Intel laufen, haben nur sehr wenige ARM-NAS aufrüstbaren Arbeitsspeicher. Auch bei billigen x86-NAS ist das nicht selbstverständlich. Fassungen für wechselbare Speichermodule sind erst bei Geräten üblich, die mehr als etwa 300 Euro kosten.

Die Faustregel „viel hilft viel“ gilt bei NAS-Arbeitsspeicher nicht. Man sollte ermitteln, ob das RAM wirklich voll ist. Die Konfigurationsoberflächen vieler NAS bieten einen Ressourcenmonitor oder andere Werkzeuge, die die aktuelle Auslastung von CPU und RAM anzeigen. Reagiert eine NAS-Anwendung sehr lahm und ist die CPU weitgehend ausgelastet, dann ist sie womöglich auch der Flaschenhals und mehr RAM bringt wenig Beschleunigung. Ist das RAM hingegen belegt, aber die CPU noch nicht am Anschlag, dürfte mehr RAM helfen.

Was geht?

Bei manchen NAS kommt man erst nach einigem Geschraube an die RAM-Fassungen heran. Daher spart es Zeit, zunächst in die Dokumentation zu schauen. Falls Sie sie nicht zur Hand haben, finden Sie sie meistens auf der Website des NAS-Herstellers. Achten Sie penibel auf die Typenbezeichnung, bei Synology etwa auf ein zusätzliches „+“-Symbol: Es kennzeichnet manchmal Geräte, die sich erheblich von der Variante ohne Plus unterscheiden.

Welches RAM kompatibel ist, hängt von vielen Details ab. Die meisten NAS-Boxen mit Wechselfassungen verlangen Small-Outline Dual Inline Memory Modules (SO-DIMMs), die auch in vielen Notebooks stecken. Sie sind halb so lang wie normale DIMMs. Nur in sehr teure NAS, in denen eigentlich die Technik kleiner x86-Server steckt, passen die normal großen DIMMs, in manche auch welche mit Zusatzchips für die Fehlerkorrektur per Error Correction Code (ECC). In fast allen kompakten NAS-Boxen sitzen jedoch sparsame x86-SoCs wie Intel Celeron J, Celeron N und Pentium Silver, die ECC nicht beherrschen.

Diese Celerons und Pentiums hat Intel eigentlich für Billignotebooks und billige Mini-PCs entwickelt und ihren Funktionsumfang absichtlich beschnitten. In den Datenblättern ist zu lesen, dass sie maximal 8, 16 oder 32 GByte RAM ansteuern. Manche können jedoch mehr, sofern die jeweilige NAS-Firmware mitspielt. Weil es dabei auf mehrere Faktoren ankommt und Intels offizielle Informationen ohnehin falsch sind, gibt es leider keine Liste, welcher Celeron oder Pentium wie viel RAM verdaut. Man kann es nur beim individuell vorhandenen Gerät ausprobieren oder im Web und bei YouTube

Je nach NAS braucht man das passende Speichermodul, etwa ein Small-Outline-(SO-)DIMM der Generation DDR2 (oben), darunter DDR3 mit der Variante DDR3L, dann DDR4 und DDR5.

suchen, ob das schon jemand anderes geschafft hat.

RAM-Typen

Einige sehr alte NAS-Boxen nutzen noch DDR2-SO-DIMMs, die meisten allerdings DDR3 oder DDR3L und aktuelle Geräte auch DDR4. In den nächsten Monaten könnten erste NAS-Boxen mit DDR5-RAM auftauchen. Die DDR-Generationen sind zueinander inkompatibel, man braucht jeweils passende Module. DDR3L ist eine Variante von DDR3, die mit 1,35 statt 1,5 Volt läuft; das „L“ steht für Low Voltage. DDR3L-SO-DIMMs laufen auch in vielen NAS, die eigentlich DDR3 verlangen, aber nicht umgekehrt. Von DDR2, DDR4 und DDR5 gibt es keine „L“-Versionen.

Schnelleres RAM, also Chips mit höherer Taktfrequenz, bringen in einem NAS zwar keinen Vorteil, aber ein zu langsames Modul erkennt das Gerät möglicherweise nicht. Nehmen Sie daher ein DIMM für denselben oder höheren Takt als das bereits vorhandene. DDR2-800, DDR3(L)-1600 oder DDR4-3200 laufen meistens.

Die meisten x86-Chips, die in NAS stecken, haben zwei RAM-Kanäle; manchmal ist davon nur einer nutzbar, weil die NAS-Entwickler eine zweite Modulfassung eingespart haben. Bei Bestückung von zwei RAM-Kanälen verdoppelt sich zwar die Datentransferrate, aber das beschleunigt weder die eigentlichen NAS-Funktionen noch irgendwelche Plug-ins nennenswert. Denn diese Anwendungen reizen schnelles RAM nicht aus.

NAS-Prozessoren können auch mit asymmetrischer Bestückung ihrer beiden RAM-Kanäle umgehen. Das bedeutet aber nicht, dass man die jeweils maximal mögliche Bestückung immer auch mit einem Einzelmodul ausreizen kann. Falls beispielsweise bis zu 16 GByte möglich sind, klappt das meistens nur mit zwei 8-GByte-Modulen und nicht etwa auch dann, wenn man nur ein einziges mit 16 GByte einbaut. Das liegt daran, dass der im jeweiligen Prozessor eingebaute Speichercontroller eine beschränkte Anzahl an Adressleitungen ansteuert. In jeder RAM-Generation gibt es eine gewisse Maximalkapazität pro SO-DIMM, die nicht alle Computer beziehungsweise NAS erkennen. Bei DDR2 sind das 8 GByte, bei DDR3(L) 16 GByte und bei DDR4 32 GByte. Um beim Beispiel des weitverbreiteten DDR3-Speichers zu bleiben: Ein 8-GByte-Riegel funktioniert meistens, ein 16-GByte-Modul nur in manchen NAS.

Ein SO-DIMM der Generationen DDR3(L) und DDR4 mit 4 oder 8 GByte können Sie ab etwa 10 respektive 17 Euro kaufen; die veralteten DDR2-SO-DIMMs sind pro Gigabyte deutlich teurer.

Achten Sie darauf, kein Registered SO-DIMM zu erwischen: Diese etwas exotische Bauform gibt es nur als ECC-Version für kompakte Server-Mainboards, sie eignet sich nicht für gängige Netzwerkspeicher.

Schrauberei

Wir haben die Probe aufs Exempel mit einer Synology DiskStation DS218+ gemacht, die seit 2018 in der c’t-Redaktion läuft. Das Gerät hat auf seinem Mainboard, das hochkant rechts im Gehäuse sitzt, zwei SO-DIMM-Fassungen für DDR3L-RAM. Eine davon ist leer und praktischerweise ohne Schrauberei zugänglich, wenn man die rechte Festplatte herauszieht. Laut Synology kann man dort ein Modul mit 2 oder 4 GByte einstecken, um die ab Werk vorhandenen 2 GByte auf insgesamt 4 oder 6 GByte zu erweitern. Es geht aber viel mehr.

Wir haben probeweise ein 8-GByte-Modul in den freien Slot gesteckt und es wurde auch erkannt: 10 GByte waren nutzbar. 16-GByte-Riegel funktionieren hingegen nicht, weil der 2016 vorgestellte Celeron J3355 (Codename Apollo Lake) damit nicht umgehen kann.

An den zweiten SO-DIMM-Slot des DS218+ kommt man erst nach Gefummel heran, denn man muss dazu das Gehäuse komplett zerlegen. Dafür fanden wir eine Anleitung bei YouTube (siehe ct.de/ym8w). Demnach läuft die Box auch mit zwei 8-GByte-Modulen, also insgesamt 16 GByte.

Ob es bei Ihrem individuellen Gerät klappt, lässt sich nicht vorhersagen. Uns haben auch einzelne c’t-Leser berichtet, dass nach einem solchen Upgrade zwar das gesamte RAM erkannt wurde, das NAS dann aber extrem langsam reagierte oder andere Probleme auftraten. Dann hilft nur, ein anderes Modul oder eines mit weniger Kapazität auszuprobieren.

(ciw@ct.de) c't

Videoanleitung zum Zerlegen der Synology DS218+: ct.de/ym8w

Bei der Synology DiskStation DS218+ lässt sich das RAM besonders leicht erweitern, die SO-DIMM-Fassung liegt gleich neben den Festplatten. Obwohl Synology maximal 4 GByte als Erweiterung freigibt, funktionieren auch 8 GByte.

Mehrwegsicherung

Synology-NAS-Daten schlau sichern, VMs inklusive

Wie sichert man lückenlos alle Daten, die auf Netzwerkspeichern von Synology liegen? Diese unscheinbare Frage zog bei uns eine kleine Forschungsarbeit nach sich und wir fanden gleich mehrere Lösungsvorschläge.

Von Dušan Živadinović

Geschäftsbriefe, Kopien von Urkunden, Urlaubsvideos oder Programmierprojekte, solche und andere wertgeschätzte digitale Dinge kann man als Admin eines Synology-NAS-Geräts mühelos sichern. Dafür bietet der Onlineshop von Synology sogar mehrere kostenlose Backupanwendungen.

Der Ablauf ist schnell skizziert: Man schätzt ab, wie viele Daten gesichert werden müssen, steckt eine Platte mit ausreichender Kapazität in einen freien Slot, konfiguriert sie als separates Volume und stöpselt noch ein USB-Laufwerk an. Das sind die beiden Zielmedien für die beiden lokalen Backups. Um dann die 3-2-1-Regel vollständig zu befolgen (drei Backups insgesamt, davon zwei lokal und eines in der Ferne), bucht man Speicherplatz in einer Cloud oder gewährt sich unter Freunden oder Mitarbeitern Zugang zum entfernten Netz (private Colocation) und stellt dort ein drittes Backupmedium auf. So kann auch eine kleine Firma die wichtigsten Datenbestände zum Beispiel im Heimnetz des Firmenadmins sichern.

Besonders elegant klappt das mit dem Tool Snapshot Replication, das für ferne Backups allerdings ein weiteres Synology-NAS mit aktivem Snapshot Replication erfordert. Mit etwas Know-how und etwa dem Befehl `rsync` kann man auch auf beliebige Freigaben ohne Synology-Bindung sichern, siehe Abschnitt „Auf Händen und

Knien“. Mit Snapshot Replication macht es sogar Spaß, die 3-2-1-Regel für Backups zu befolgen, weil das Tool übersichtlich und zugleich leistungsfähig ist: Drei regelmäßige Backups von den allerwichtigsten Daten zu konfigurieren, das ist mit Snapshot Replication nur ein lockerer Mausspaziergang.

Will man gesicherte Daten einlesen, geht das wahlweise direkt in Snapshot Replication mittels der Option „Wiederherstellung“ oder per Hand. Dafür genügt es, den replizierten Ordner als Netzlaufwerk zu mounten. Dann kann man einzelne Dateien zum Beispiel auf den PC herunterladen.

Doch wenn es um Backups von virtuellen Maschinen geht (VM), für die man auch schon mal manchen Schweißtropfen vergießt, sitzen vor allem Admins von Synology-NAS-Geräten der Einstiegs- und Mittelklasse auf dem Trockenen. Denn für VM-Backups hat Synology nur den Virtual Machine Manager in der Pro-Version vorgesehen, der für private Zwecke einfach zu teuer ist: Ein Jahresabonnement bekommt man erst ab 160 Euro (siehe ct.de/ydsh).

Die kostenlosen grafischen Anwendungen wie „USB Copy“ oder „Active Backup for Business“ können nicht auf die Pfade zugreifen, in denen die VM-Dateien liegen. Mit der einfachen Version des Virtual Machine Manager kann man immerhin regelmäßig lokale Schnappschüsse erzeugen (linke Spalte, Option „Schutz“). Diese liegen im Pfad /volumeN/@iSCSI/Snapshot/BLUN, wobei volumeN dem für VMs konfigurierten Speicherpool entspricht, also etwa volume2. Von dort könnte man sie zum Beispiel mit `rsync` auf ein beliebiges Ziel sichern.

Doch es gibt viel bequemere Wege. Die meisten virtuellen Maschinen kann man wie übliche PCs oder Server mit einem der vielen Backup-Tools von innen heraus sichern. Man richtet das Tool in der VM so ein, dass es über das LAN in einen freigegebenen Ordner des Synology-NAS schreibt, den man mit dem Programm File Station erzeugt. Den freigegebenen Ordner kann man dann leicht mit Snapshot Replication lokal und in der Ferne sichern.

Eine elegantere Lösung bietet sich über das von Synology angebotene Active Backup for Business (kurz ABB) – etwas unerwartet, denn Synology führt nicht auf, wie man damit VMs sichert.

Doch es setzt dasselbe Bedienkonzept mit ähnlichen Begriffen um, das Synology auch bei anderen Programmen verwendet und erscheint für die Aufgabe ausreichend leistungsfähig: Man kann den gesamten Backupclient manuell oder nach Zeitplan sichern, verschiedene Aufbewahrungsrichtlinien konfigurieren und vor und nach dem Backup Skripte ausführen lassen. Das ist ein übliches Mittel, um laufende Server während der Sicherung anzuhalten, um inkonsistente Backupdaten zu vermeiden.

Hat man ABB aktiviert (Registrierung und Anmeldung am Synology-Konto erforderlich) und gestartet, bietet das Tool an, beispielsweise PCs mit Windows oder macOS oder virtuelle Maschinen von VMWare Sphere oder Microsofts Hyper-V zu sichern; Synology-VMs berücksichtigt das Tool nicht ausdrücklich.

Simple Überredung

Aber man kann es mit einem simplen Trick dazu überreden: Man richtet den Backupclient von ABB auf einer VM so ein, als wäre sie ein physischer Server. Das, und die weitere Konfiguration in Snapshot Replication, spielen wir jetzt auf Basis eines Synology DS1621+ mit DSM 7.2 durch. Sollten Sie Snapshot Replication bisher nicht verwendet haben, können Sie den hier geschilderten Vorgang nutzen, um beliebige andere Freigaben Ihres Synology-NAS zu replizieren, sei es lokal oder fern.

Bevor Sie loslegen, stellen Sie sicher, dass der SSH-Dienst auf Ihrem Synology-NAS läuft (Systemsteuerung/Terminal & SNMP) und dass es für jeden SSH-Nutzer ein Home-Verzeichnis anlegt. Öffnen Sie dazu in der Systemsteuerung „Benutzer und Gruppe“. Klicken Sie in der Reiterauswahl auf „Erweitert“ und dann weiter unten auf „Benutzerbasis“. Bei „Benutzer-Dienst aktivieren“ sollte das Häkchen gesetzt und ein Zielvolume ausgewählt sein.

Starten Sie Active Backup for Business und aktivieren Sie es. Klicken Sie links in der Spalte auf „Physischer Server“, wählen Sie entsprechend der virtuellen Maschine Windows oder Linux aus und klicken Sie auf „Gerät hinzufügen“. Im Weiteren gehen wir von einer Linux-VM auf Debian-Grundlage aus.

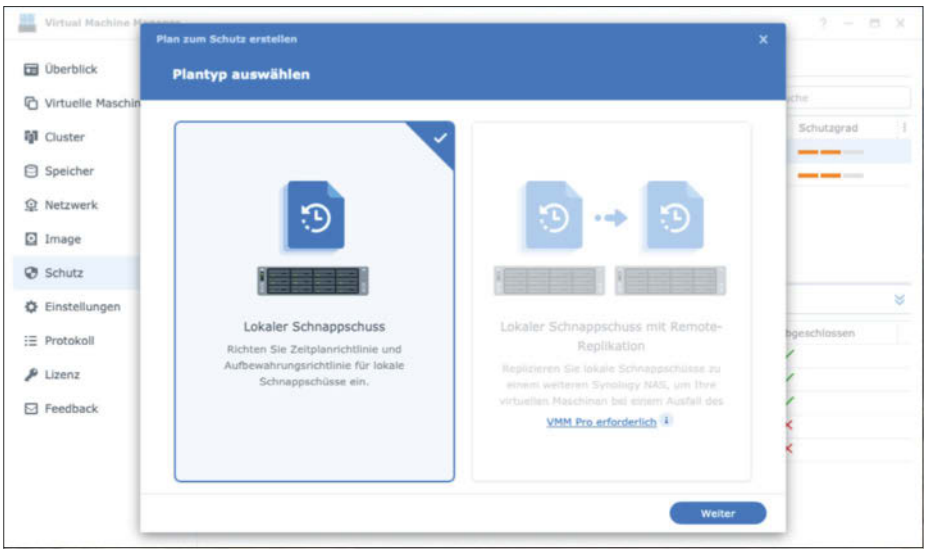
Klicken Sie im Dialog auf „deb_x64“, um das Installationsskript der Linux-Variante des ABB-Clients auf Ihren PC zu laden. Entpacken Sie das Archiv auf dem PC und bringen Sie die Datei install.run in die VM, die Sie sichern wollen. Beispiel:

```
cd "~/Downloads/Synology Active↵
↳ Backup for Business Agent-2.6.1-↵
↳3052-x64-deb"
sftp user@vm
put install.run
```

Ersetzen Sie „user“ mit Ihrem Usernamen und „vm“ mit der IP-Adresse der virtuellen Maschine, auf der der ABB-Client laufen soll; die IP-Adresse verrät der Virtual Machine Manager im Bereich „Virtuelle Maschine“. Melden Sie sich danach per SSH an der VM an und starten Sie die Installation des ABB-Clients:

```
ssh user@vm
sudo su
./install.run
```

Das Skript lädt unter anderem Linux-Header-Dateien, das Kommando



Den Großteil der NAS-Daten kann man auf Synology-Geräten sehr bequem mit Synology-Tools sichern. Doch für virtuelle Maschinen hat der Hersteller nur die im Abonnement erhältliche Pro-Variante des Virtual Machine Managers vorgesehen.

`synosnapshot` und weitere Komponenten, was einige Minuten dauert. Anschließend meldet man den ABB-Client am ABB-Server des NAS-Geräts per Kommandozeile an:

```
abb-cli -c
```

Geben Sie auf Nachfrage die erforderlichen Parameter ein. Zwischendrin blendet das Tool eine Warnung wegen nicht vertrauenswürdigem Zertifikat ein. Erlauben Sie dessen Verwendung. Falls Ihr NAS eine Zwei-Faktor-Authentifizierung erfordert, öffnen Sie die dafür eingerichtete App auf dem Smartphone und geben Sie eine gültige Zeichenfolge ein. Bestätigen Sie zum Schluss die von abb-cli eingeblendeten Anmeldetaten. Damit ist der Client am Server angemeldet.

Kehren Sie nun zurück zum geöffneten Dialog des ABB-Servers auf dem Synology-NAS und klicken Sie auf „Vorlage“ und „Erstellen“, um eine neue Backupkonfiguration zu erzeugen. Tragen Sie oben im Dialog einen Namen für den Vorgang ein, beispielsweise den Namen der VM, wählen Sie den Benutzer aus, der die Vorlage verwenden darf (zum Beispiel admin) und klicken Sie weiter unten die Plattform (etwa Linux) sowie darunter „Physischer Server“ an.

Auf der nächsten Seite empfiehlt es sich, das gesamte Gerät zu sichern und sowohl Kompression als auch Verschlüsselung zu deaktivieren, weil beides in diesem Szenario nur unnötig Rechenzeit kostet. Im nächsten Dialog können Sie das lokale Backupziel festlegen, also zum Beispiel die Freigabe „Active Backup for Business“. Anschließend folgen Einstellungen für etwaige Skripte, das automatische Backup im Aufgabenplaner (etwa täglich um 6 Uhr morgens) sowie Einstellungen für Aufbewahrungsrichtlinien (beispielsweise die letzten 10 Versionen aufbewahren). Damit ist die Backupaufgabe eingerichtet.

Wenn Sie danach links in der Spalte auf „Physischer Server“ und Linux klicken, sollte Ihre neue Backupaufgabe aufgeführt sein. Um die Sicherung sofort zu testen, öffnen Sie die Aufgabenliste, klicken Sie auf die neue Aufgabe und dann auf „Sichern“. In der Spalte Status sollte nach einigen Sekunden der Backupfortschritt aufgeführt werden. Im Test auf dem Mittelklasse-NAS Synology DS1621+ dauerte die Sicherung einer 10-GByte-VM rund fünf Minuten. Wenn Sie in der Spalte „Ziel“ auf den Pfad klicken, öffnet sich die Anwendung „File Station“ und darin der Backupordner. Die Backupdatei einer Linux-VM heißt beispielsweise sda.img. Von dort aus kann man sie zum Beispiel auf den PC downloaden.

Viel nützlicher dürfte aber sein, dass man den ABB-Ordner wie jeden anderen freigegebenen Ordner auf ein fernes Synology-NAS replizieren kann, etwa in einer anderen Stadt. Für die Snapshot Replication eignen sich zwar nicht alle Synology-NAS, aber für viele. Die Liste der Modelle, auf denen der Dienst läuft, finden Sie über ct.de/ydsh. Falls Ihr NAS-Modell nicht aufgeführt ist, können Sie auf den Rsync-Dienst ausweichen. Wie man das Kommando `rsync` auf Synology für die Synchronisierung über SSH-Tunnel konfiguriert, haben wir in c’t 13/22 ab Seite 168 beschrieben.

Replikation per VPN

Die Snapshot Replication klappt am einfachsten, wenn sich beide NAS-Geräte über ein VPN erreichen können; dann ist deren Verkehr verschlüsselt und Sie können sich die Portfreigaben für das Webinterface und die Snapshot Replication sparen.

Wir haben dafür das Peer-to-Peer-VPN ZeroTier verwendet (kurz ZT), weil es sich schnell einrichten lässt und ohne Portweiterleitungen und ohne DynDNS funktioniert. Hier der Vorgang in aller Kürze, falls Sie ebenfalls ZeroTier verwenden wollen: Falls noch nicht geschehen, richten Sie den Container Manager auf dem NAS ein, legen Sie auf zerotier.com ein Konto an, melden Sie sich an und erzeugen Sie mit „Create A Network“ ein neues Netz. Installieren Sie den ZT-Client über eine SSH-Sitzung auf dem lokalen NAS, indem Sie der Anleitung auf docs.zerotier.com/synology/ folgen. Fügen Sie den Client Ihrem ZT-Netz hinzu; kopieren Sie dafür die Netzwerk-ID aus dem ZT-Webinterface und setzen Sie sie in den folgenden Befehl anstelle von Network-ID ein:

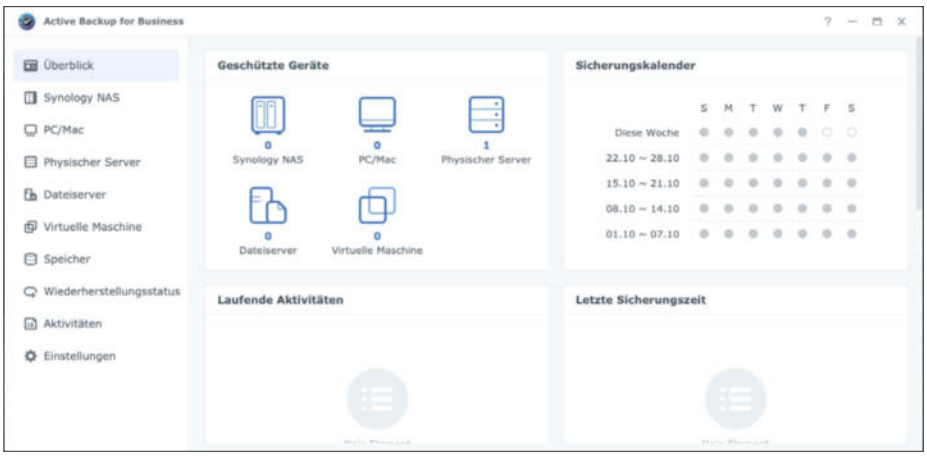
```
docker exec -it zt zerotier-cli↵
↳ join Network-ID
```

Im ZT-Webinterface scrollen Sie nach unten zum Abschnitt Members, um dem neuen ZT-Client Zutritt zu gewähren. Tragen Sie dann im ZT-Webinterface seinen Namen ein (Firmen-NAS). Falls noch nicht vorhanden, richten Sie im fernen Router eine Port-Weiterleitung für den SSH-Zugang zum fernen NAS ein und richten Sie dort ZT ebenfalls ein.

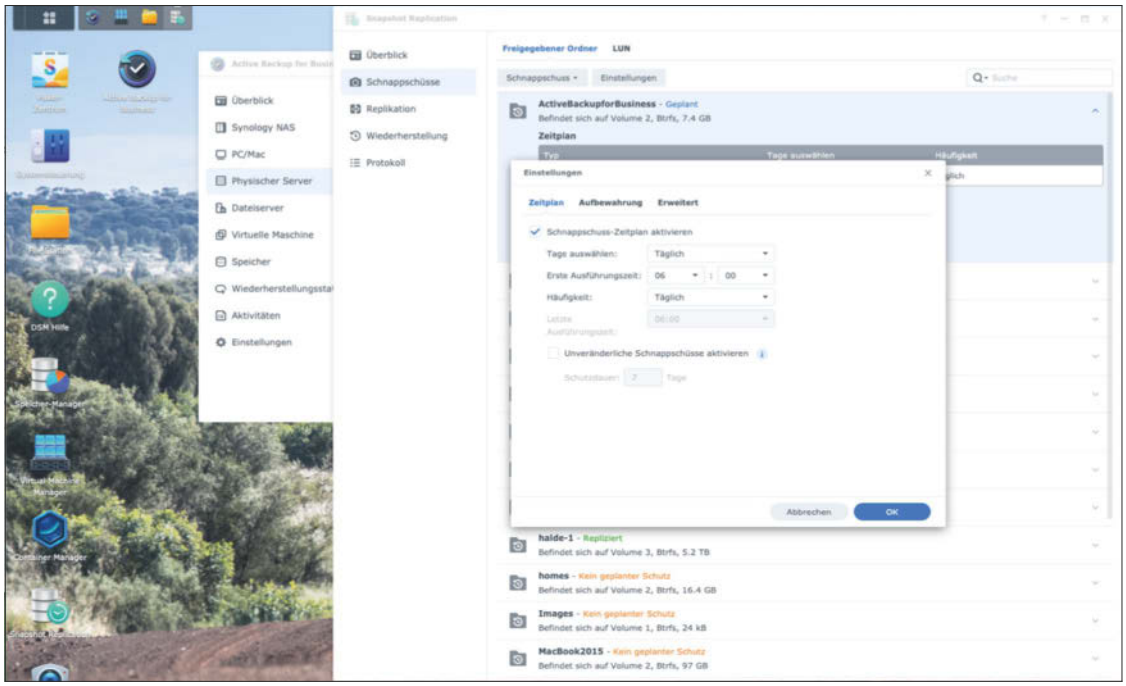
Lesen Sie im ZT-Webinterface die ZT-IP-Adressen der beiden NAS-Geräte aus. Darüber sollten die beiden NAS gegenseitig auf Ping-Pakete antworten (`ping ZT-IP-Adresse`). Wenn Sie auf dem PC ebenfalls ZT einrichten, können Sie beide NAS per Ping erreichen und das Webinterface des fernen NAS auch aus Ihrem lokalen Netzwerk öffnen.

Schnappschüsse replizieren

Im nächsten Schritt richten Sie den Dienst Snapshot Replication auf beiden NAS ein. Melden Sie sich dazu auf beiden Geräten als Administrator an und installieren Sie den Dienst über das Paketzentrum. Stellen Sie sicher, dass auf dem Zielserver ein Btrfs-Volume mit ausreichend freier Kapazität vorhanden ist. Falls Sie keine VPN-



Über einen kleinen Umweg lässt sich das kostenlose Active Backup for Business überreden, auch von den meisten virtuellen Maschinen Backups zu erzeugen.



Hat man erstmal lokale Backups von VMs angelegt, lassen sich diese wie andere NAS-Daten mit dem Tool Snapshot Replication auch auf fernen Netzwerkspeichern von Synology sichern.

Verbindung verwenden (nicht empfohlen), richten Sie im fernen Router Weiterleitungsregeln für die TCP-Ports 5000 und 5566 ein („Webinterface“ und „Gemeinsamer Ordner“).

Öffnen Sie Snapshot Replication, klicken Sie auf „Replikation“, „Erstellen“, „Start“ und wählen Sie „remote“ aus. Tragen Sie dann Servernamen, IP-Adresse (möglichst VPN-Adresse) und die Zugangsdaten für das Replikationsziel ein. Die Authentifizierungsdaten fragt Ihr Browser in einem Pop-up-Fenster ab. Falls Ihr Browser Pop-up-Fenster blockiert, müssen Sie es per Hand öffnen. Falls das ferne NAS eine Zwei-Faktor-Authentifizierung erwartet, geben Sie den zweiten Faktor wie konfiguriert ein und schließen Sie die Authentifizierung mit „Weiter“ ab.

In den nächsten beiden Dialogen legen Sie fest, auf welchem Ziel-Volume des fernen NAS welcher lokale Ordner gesichert wird, zum Beispiel auf Volume1 der Ordner „Active Backup for Business“. Danach zeigt Ihr NAS die zu übertragende Datenmenge und die geschätzte Dauer der ersten Replikation an. Legen Sie dann einen Zeitplan für regelmäßige Sicherungen und eine Aufbewahrungsrichtlinie fest, zum Beispiel täglich um 7:00 Uhr und zehn aufzubewahrende Schnappschüsse. Die Option für „geplante lokale Schnappschüsse“ spielt für die Sicherung von VMs keine Rolle, lassen Sie sie also weg.

Prüfen Sie auf der letzten Seite die komplette Liste der Einstellungen und schließen Sie den Dialog mit „Fertig“. Dann legt Ihr NAS die Aufgabe an, startet gleich die erste Replikation und blendet eine Fortschrittsanzeige ein. Weitere Statusmeldungen finden Sie über den Reiter „Überblick“.

Auf Händen und Knien

Active Backup for Business und Snapshot Replication funktionieren nur im Synology-Kosmos und sie berücksichtigen nur komplette freigegebene Ordner, aber keine Pfade innerhalb dieser Ordner. Ersatzweise bietet sich wiederum `rsync` an.

Die VM-Dateien legt das DSM-Betriebssystem nach dem Muster /volumeN/@iSCSI/LUN/VDISK_BLUN ab. Da Synology zur Virtualisierung die Qemu-Technik nutzt, kann man die VMs auch in anderen Qemu-Instanzen verwenden (und mit dem Befehl `virsh` lokal sichern und vieles mehr …). Um die zu einer VM zugehörige Datei zu finden, melden Sie sich per SSH als root an und lesen Sie zuerst die IDs der laufenden VMs mit `virsh` aus:

```
ssh ip-Adresse-des-NAS
sudo su
virsh list --title
```

Die ausgegebene Tabelle führt in der Spalte „title“ die Namen der VMs und in der Spalte „Name“ die zugehörigen IDs auf. Den Ordner, in dem die Dateien einer VM stecken, verrät der Befehl `virsh dumpxml ID`:

```
virsh dumpxml 7cee6abc-ce77-4894-928f
-b23fd81b498e | grep -i vdisk_
... vdisk_2eccf23c-ec9a-449f-8633-0e04
95144100 ...
```

Das ist in der obigen Ausgabe die Zeichenkette, die auf vdisk_ folgt, also in diesem Beispiel der Ordner 2eccf23c-ec9a-449f-8633-0e0495144100. Um den Ordner zu kopieren, setzt man den VM-Pfad /volumeN/@iSCSI/LUN/VDISK_BLUN vor die ID der VM. Beispiel:

```
cp -r /volume2/@iSCSI/LUN/VDISK_BLUN/↵
↳2eccf23c-ec9a-449f-8633-0e0495144100↵
↳ Zielpfad
```

Setzen Sie statt `volume2` jenes Volume ein, auf dem Ihre VMs gespeichert sind und tragen Sie anstatt der obigen Zeichenkette, jene ein, die zu Ihrer gesuchten VM-Datei gehört. Den so ermittelten Pfad einer VM können Sie nun in `rsync` als Quellpfad verwenden. Eine laufende VM stoppen Sie mit `virsh shutdown ID`. Nach dem Backup starten Sie die VM mit folgendem Befehl:

```
synowebapi --exec api=SYNO.↵
↳Virtualization.API.Guest.Action↵
↳ version=1 method=poweron↵
↳ runner=admin guest_name="VM-Name"
```

(dz@ct.de) c't

Infos zu Snapshot Replication: ct.de/ydsh

Kleine Düse

Hosentaschenrechner mit Ultraschallkühlung

Zotac rüstet den Mini-PC ZBox pico PI430AJ mit einem Solid-State-Kühler von Frore aus. Wir prüfen, wie gut und leise er den darin eingebauten Achtkernprozessor Core i3-N300 kühlen kann.

Von Christian Hirsch

Die ZBox-pico-Serie des in Hongkong beheimateten Herstellers Zotac gehört zu den kleinsten erhältlichen Desktop-PCs mit Windows. Bei den bisherigen, lüfterlosen Varianten diente das Metallgehäuse zugleich als Kühlkörper, allerdings arbeiteten darin nur lahme Celeron-N-Prozessoren. Das ändert sich mit der aktuellen ZBox pico PI430AJ.

In dem etwa kartenspielgroßen Aluminiumblock rechnet der Achtkerner Intel Core i3-N300. Anders als es der Name vermuten lässt, hat dieser wenig mit aktuellen Core-i-Prozessoren zu tun. Er gehört vielmehr zur Serie Alder Lake-N. Das bedeutet: Er verwendet ausschließlich die kompakten, auf niedrige Leistungsaufnahme getrimmten Effizienzkerne der Core-i-12000-CPUs.

Wegen der geringen Thermal Design Power von sieben Watt darf man keine Performancewunder erwarten. Zotac verspricht, dass die Leistung für übliche Office-Aufgaben und zur Medienwiedergabe reicht. Zur weiteren Ausstattung gehören eine NVMe-SSD mit 500 GByte Kapazität sowie 8 GByte LPDDR5-RAM. Inklusive Windows 11 Home kostet der Mini-PC 560 Euro.

Lüfterlose Aktivkühlung

Als Besonderheit rüstet der Hersteller die ZBox pico PI430AJ mit einem Airjet-Kühler von Frore aus. Diese knapp drei Millimeter flachen Module kühlen elektronische Komponenten aktiv, aber lüfterlos. Im Inneren sitzen kleine Membranen, die mit Ultraschallfrequenz vibrieren. Dadurch saugt das AirJet-Modul auf der Oberseite Luft an und bläst sie über einen kupfernen Heatspreader, der auf dem Prozessor sitzt, seitlich aus dem Gehäuse.

Hält man den Finger vor die Öffnung, spürt man einen leichten Luftzug. Im Leerlauf, wenn der Mini-PC lediglich sieben Watt aufnimmt, ist der Rechner auch in sehr leisen Umgebungen nicht zu hören. Unter Volllast emittiert die ZBox pico ein leises weißes Rauschen, was aus mehr als 70 Zentimetern Distanz nicht mehr auffällt. Der Solid-State-Kühler dient jedoch nur als Booster. Einen Großteil der Abwärme gibt das Gehäuse ab. Es heizte sich bis auf 56 Grad Celsius auf. Das ist schon nach wenigen Sekunden schmerzhaft und man zieht seinen Finger weg.

Die Multithreading-Rechenleistung des Core i3-N300 liegt auf dem Niveau des sechs Jahre alten Quad-Cores Core i3-7100, allerdings bei deutlich geringerem Energiebedarf. Beim Browsing merkt man keinen Unterschied zu leistungsfähigeren Prozessoren. Die integrierte Grafikeinheit entlastet die CPU-Kerne, sodass YouTube-Videos im VP9-Format mit 4K-Auflösung ruckelfrei laufen. Für 3D-Spiele ist die GPU jedoch viel zu schwach.

Ein Teil der spürbar höheren Geschwindigkeit geht auf das Konto der M.2-SSD mit PCI-Express-Interface. Im Vergleich zur Vorgängerin ZBox pico PI336, wo noch lahmer eMMC-Speicher eingelötet war, steigt der Durchsatz von 260 auf 2700 MByte/s.

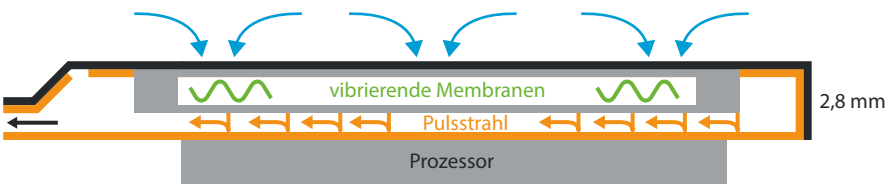
Triple-Monitor-tauglich

Bei den Schnittstellen muss sich der Mini-PC nicht hinter großen Desktoprechnern verstecken. Auf der Rückseite gibt es für Monitore HDMI und DisplayPort. An die USB-C-Buchse in der Front lässt sich ein drittes Display anschließen. Alle drei Ausgänge geben zugleich 4K-Auflösung mit 60 Hertz aus.

Zu Netzwerken nimmt die ZBox pico Kontakt per Ethernet oder WLAN auf. Der Durchsatz im 2,4- und 5-GHz-Band erreicht allerdings nur unterdurchschnittli-

Aufbau von Frore-Airjet-Kühlern

Mit Ultraschallfrequenz pulsierende Membranen saugen durch Schlitze auf der Oberseite kühle Umgebungsluft an. Diese trifft mit rund 200 km/h auf die Gegenseite und reißt die dort anliegende, vom Prozessor erwärmte Luftschicht mit nach außen.



che Werte. Auf 20 Meter Entfernung schrumpft die Übertragungsgeschwindigkeit bei 5 GHz auf 13 Mbit/s, was 1,6 MByte/s entspricht und für moderne Internetanschlüsse viel zu wenig ist.

Fazit

Die ZBox pico PI430AJ von Zotac ist in der Tat einer der kleinsten Windows-PCs. Er bietet genug Rechenleistung als Büro-PC und Medienzuspieler. Mit anspruchsvollen Aufgaben wie 4K-Videoschnitt oder Raw-Fotoentwicklung ist der Rechner jedoch überfordert. Sieben Watt Leistungsaufnahme im Leerlauf sind mehr als bei vielen anderen Mini-PCs.

Im Unterschied zu den passiv gekühlten Vorgängern arbeitet die ZBox pico PI430AJ zwar nicht mehr geräuschlos. Die Airjet-Kühlung erlaubt jedoch, einen deutlich leistungsfähigen Achtkerner einzubauen und sie arbeitet wesentlich leiser als die Winzlüfter vieler anderer Mini-PCs. *(chh@ct.de)* c't

Zotac ZBox pico PI430AJ

Mini-PC mit Ultraschallkühler	
CPU / Kerne / Takt (Turbo)	Intel Core i3-N300 / 8 / 0,8 (1,4 bis 3,8) GHz
RAM (Typ / Max) / -Slots	8 GByte (LPDDR5–4800 / 8 GByte) / aufgelötet
SSD (Typ, Kapazität)	OEM (NVMe (PCIe 3.0 x4), 512 GByte)
Netzwerk-Interface (Chip, Anbindung) / TPM	1 GBit/s (RTL8111, PCIe) / fTPM 2.0
WLAN-Interface (Chip, Anbindung)	Wi-Fi 6 (Intel AX101, PCIe)
Abmessungen (B × H × T)	11,5 cm × 2,4 cm × 7,6 cm
Anschlüsse	1 × HDMI 2.0, 1 × DisplayPort 1.4, 2 × USB-A 10 GBit/s, 1 × USB-C 10 GBit/s mit DisplayPort, 1 × LAN, 1 × analog Audio
Zubehör	Recovery-Stick, VESA-Halterung, Kurzanleitung
Elektrische Leistungsaufnahme, Datentransfer-Messungen und Geräuschentwicklung	
Soft-Off (mit EUP) / Energie Sparen / Leerlauf	1,6 W (0,4) / 1,6 W / 7,4 W
Volllast: CPU / CPU und Grafik	20 W / 21 W
SSD: Lesen (Schreiben)	2,7 (2,5) GByte/s
USB-A hinten / USB-C: Lesen (Schreiben)	1066 (1032) / 1086 (1049) MByte/s
WLAN 2,4 GHz / 5 GHz: nah (20 m)	199 (86) / 487 (13) Mbit/s
MicroSD-Card: Lesen (Schreiben)	42,0 (33,0) MByte/s
Geräuschentwicklung: Leerlauf / Volllast (Note)	< 0,1 Sone (⊕⊕) / 0,2 Sone (⊕⊕)
Systemleistung und Bewertung	
Cinebench R23: 1T / MT / 3DMark: Fire Strike	535 / 2716 / 1544
Systemleistung: Office / Rendering / Spiele	⊕ / ⊖⊖ / ⊖⊖
Audio: Wiedergabe / Aufnahme	⊕ / ⊖
Preis / Garantie	560 € / 60 Monate

✓ funktioniert – funktioniert nicht n. v. nicht vorhanden ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht

Zweiter Smartwatch-Aufschlag

Google Pixel Watch 2 im Test

Optisch bleibt die Pixel Watch 2 genauso schlank und schick wie ihre Vorgängerin. Bei der Technik hat Google aber nachgebessert und sorgt für eine freudige Überraschung.

Von Stefan Porteck

Offenbar verfolgt Google wie bei den Pixel-Telefonen die Strategie, seinen Smartwatches ein unverwechselbares Aussehen zu spendieren. So ist auch die Pixel Watch 2 auf den ersten Blick klar als solche zu erkennen. Das runde Design ohne Ecken und Kanten ist genauso erhalten geblieben wie das schwarz gefärbte Gorilla Glass, das sich in einem geschwungenen Bogen bis fast zur Hälfte der Gehäuserückseite zieht und dort in den ebenfalls abgerundeten Boden aus Aluminium übergeht. Abgesehen von den neuen digitalen Zifferblättern und den zusätzlichen Sensoren an der Unterseite ist die neue Watch äußerlich nicht von ihrer Vorgängerin zu unterscheiden.

Positiv fällt dabei auf, dass Google die proprietäre Arretierung der Armbänder nicht verändert hat. Wer bereits Armbänder für die erste Pixel Watch besitzt, kann diese beim späteren Umstieg weiterverwenden. Erstkäufer profitieren dagegen davon, dass es schon zum Verkaufsstart der Watch 2 im Zubehör unzählige Armbänder in vielfältigen Farben und Materialien gibt. Ausgeliefert wird die Pixel Watch 2 mit einem matten Gummiarmband, das sich wertig anfühlt und gut auf der Haut liegt. In der Packung finden sich ein kurzes Lochband für dünne Handgelenke und ein längeres für größere.

Display und Technik

Der Durchmesser der Pixel Watch 2 ist mit 41 Millimetern gleich geblieben. Da sie über keinen klassischen Bandanstoß verfügt, wirkt sie sehr schlank. Das OLED-Display misst weiterhin 1,2 Zoll (3 cm) und erreicht mit einer Pixeldichte von 320 dpi ein sehr scharfes Schriftbild. Dank des Umgebungslichtsensors passt die Watch 2 ihre Helligkeit automatisch an. Unter Sonnenlicht lässt sie sich gut ablesen, da ihre Spitzenhelligkeit kurzzeitig auf rund 1000 cd/m² ansteigt.

Gleich geblieben ist jedoch auch der rund 3 Millimeter breite Rand, der das Display einfasst. Weiterhin kaschiert Google den Rahmen ganz ansehnlich mittels schwarzer Zifferblätter, bei denen der Übergang von Display, Rahmen und der Wölbung des Uhrenglases optisch verschwindet. Für die von Apps angezeigten Informationen reicht der Platz aus, das Tippen fällt auf der winzigen virtuellen Tastatur aber schwer.

Nachgebessert hat Google dagegen bei zwei anderen Kritikpunkten: Während die erste Pixel Watch mit einem schon beim Erscheinen nicht mehr taufrischen Samsung Exynos 9110 ausgestattet war, ist die Pixel Watch 2 mit einem Qualcomm Snapdragon Wear 5100 bestückt, dem ein Cortex M33-Coprozessor zur Seite steht. Damit lief die Pixel Watch 2 in unserem Test flotter. So starteten Apps ohne Verzögerungen und das Scrollen durch die App-Übersicht oder die Ansichten genannten Widgets fühlte sich geschmeidig an. Der Arbeitsspeicher umfasst 2 GByte und der Flash-Speicher bringt es auf 32 GByte, was für Smartwatch-Apps völlig ausreicht.

Ein Kritikpunkt war zudem die kurze Laufzeit von rund einem Tag. Hier steuert Google mit einem leicht gewachsenen Akku dagegen, der nun eine Kapazität von 306 mAh aufweist. Zusammen mit dem effizienteren Snapdragon-SoC ruft die Pixel Watch nicht mehr ganz so früh nach dem Ladegerät: Bei dauerhaft eingeschaltetem Display erreichten wir mehr als die von Google versprochene Laufzeit von einem vollen Tag. Nach 24 Stunden hatte unser Testgerät noch eine Restkapazität von rund 35 Prozent. Die Vorgängerin schaffte den vollen Tag nur knapp und ohne Always-On-Display. Der Pixel Watch 2 ging dagegen trotz dauerhaftem Display erst nach 34 Stunden die Puste aus. Mit der Einstellung, dass sich das Display nur bei Bedarf durch Drehung des Handgelenks automatisch aktiviert, hielt die Watch 2 sogar noch länger durch.

Damit ergibt das automatische Schlaf-Tracking (dazu gleich mehr) Sinn, da man die Uhr nicht mehr jeden Abend aufladen muss. Sofern man aber Workouts aufzeichnet, verkürzen die Messungen von Puls und der Blutsauerstoffsättigung weiterhin spürbar die Laufzeit; eine Stunde Workout mit eingeschaltetem GPS hat etwa 10 bis 15 Prozent Akkuladung gekostet.

Geladen wird die Pixel Watch 2 weiterhin über eine proprietäre Ladeschale mit USB-C-Anschluss, die mittels Magneten in der richtigen Position an der Uhr einrastet. Anders als in der ersten Generation lädt der Akku aber nicht induktiv, sondern über vier Pogo-Pins. Das geht zwar schneller als Drahtlosladen, hat aber den Nachteil, dass man der Uhr unterwegs nicht mehr über einen Qi-Lader oder das Reverse-Charging eines Pixel-Telefons ein wenig Saft nachtanken kann.

Neuestes Wear OS

Auf der Pixel Watch 2 läuft Wear OS in der vierten und damit neuesten Version. Optisch und funktional unterscheidet sich Wear OS 4 nicht spürbar von der vorheri-

gen Version. Wie bisher erreicht man durch Wischen vom oberen Rand die sogenannten Quick Settings, die über kleine Icons grundlegende Einstellungen anpassen – etwa die Helligkeit oder Nachtmodus und Stummschaltung. Die Benachrichtigungen öffnet eine Wischgeste vom unteren Rand.

Kurze und gewünschte Info-Häppchen erreicht man durch horizontales Wischen, was durch die sogenannten Ansichten scrollt. Sie zeigen beispielsweise Fitness-Fortschritte, das Wetter oder anstehende Termine. Welche Ansichten in welcher Reihenfolge erscheinen, lässt sich in der Companion-App auf dem Smartphone einstellen. Sie übernimmt darüber hinaus die Kommunikation zwischen der Uhr und dem Handy, verwaltet digitale Zifferblätter und legt fest, welche Apps Benachrichtigungen auf der Uhr anzeigen dürfen. Die Kommunikation zwischen Uhr und Telefon läuft über Bluetooth. Als Backup hat die Uhr WLAN an Bord. Wer die Uhr auch draußen ohne Telefon nutzen will, greift zur Variante mit Mobilfunk-Unterstützung.

Die Bedienung an der Uhr ist intuitiv: Ein Druck auf die mechanische Krone öffnet die App-Übersicht, durch die man wiederum durch das Drehen der Krone scrollt. Eine gewünschte App startet man anschließend durch Drücken der Krone. Sobald eine App läuft, fungiert die Krone als Home-Button und wechselt stets aufs Zifferblatt. Wer nur wenige Apps nutzt und nicht immer durch alle Apps scrollen will, gelangt durch einen Druck auf den Knopf oberhalb der Krone in die deutlich kürzere Übersicht der zuletzt aktiven Apps. Wer die Pixel Watch 2 mit Google Wallet (ehemals Google Pay) verknüpft und dort eine Kreditkarte oder einen PayPal-Account hinterlegt, kann die Uhr innerhalb von Sekunden durch einen Doppelklick auf die Krone in den Bezahlmodus schicken.

An der Unterseite der Smartwatch sitzen Sensoren, die unter anderem die Pulsfrequenz, die Blutsauerstoffsättigung und die Hauttemperatur messen.

Körperdaten und Fitness

An ihrer Unterseite ist die Pixel Watch 2 gespickt mit Sensoren, die Körperdaten erfassen. Der optische Sensor zur Pulsrate und zur Messung der Blutsauerstoffsättigung (SpO_2) fällt nun sichtbar größer aus und hat mehr Dioden als bei der ersten Pixel Watch. Google verspricht damit eine exaktere Erkennung der Herzfrequenz. In unseren Tests wurde die Herzfrequenz im Alltag und beim Sport stets akkurat ermittelt, doch die optische Messung hat prinzipbedingt Probleme, sehr kurze Pulsspitzen, etwa beim Gewichtheben, zu erkennen. Ambitionierte und professionelle Sportler greifen deshalb stets besser zu Brustgurten.

Neu hinzugekommen sind Sensoren, die die Körpertemperatur und die Hautleitfähigkeit messen. Letztere wird oft als elektrodermale Aktivität bezeichnet und gilt als Indikator, um daraus kombiniert mit Herz- und Bewegungsdaten unter anderem den Stresslevel zu bestimmen. Sämtliche Körper- und Fitnessdaten landen in der Fitbit-App, die zwingend auf dem Smartphone installiert sein muss. Durch die Stresserkennung ist die Verzahnung mit dem von Google übernommenen Fitnessportal noch enger als bei der vorherigen Smartwatch, da Googles zweite Fitness-App Google Fit keine Stressanalyse beherrscht und offenbar nicht weiter entwickelt wird. Vielen Nutzern dürfte das sauer aufstoßen, denn bei Fitbit gibts den vollen Funktionsumfang nur im gebührenpflichtigen Abo.

Besonders hilfreich fanden wir die Stressauswertung während des Tests jedoch nicht. In unregelmäßigen Abständen präsentiert die Watch 2 einen Hinweis, dass sie eine verstärkte Körperreaktion erkannt hat, die auf Stress hinweist. Diese Meldungen kamen aber meistens eine halbe bis ganze Stunde nach dem Zeitpunkt der Erkennung, zusammen mit der Aufforderung, in der Fitbit-App manuell seinen Gemütszustand anzugeben. Meist lag zwischen Messung und Erinnerung so viel Zeit, dass wir den eigentlichen Stressauslöser dann nicht mehr ausmachen konnten.

Besser schnitt die Uhr bei der Erkennung von aktiver Zeit, Schritten, zurückgelegter Entfernung und bewältigten Höhenmetern ab. Hier entsprachen die Messungen weitestgehend denen anderer Fitness-Tracker. Bei der Schlafanalyse lag sie mitunter daneben. Zwar deckten sich die Schlafphasen überwiegend mit den Ergebnissen anderer Tracker, aber nächtliche Wachphasen hielten laut der Pixel Watch 2 deutlich länger an als von anderen Geräten gemessen.

Gut gefallen hat uns die Aufzeichnung von Workouts. Die Uhr unterstützt dutzende Trainingsmodi und präsentiert während des Trainings relevante Daten wie Dauer oder Entfernung und Pulsrate und abschließend eine Auswertung. Einfache Trainings wie Joggen oder Rudern erkennt die Pixel Watch 2 nach kurzer Zeit von selbst und bietet an, das Tracking automatisch zu starten. Bei Workouts, die sich anhand von Bewegungsdaten nicht zweifelsfrei erkennen lassen, startet man das Tracking hingegen manuell.

Fazit

Bei der Pixel Watch 2 hat Google viele der Kritikpunkte an der vorherigen Uhr verbessert. Wer bereits vorher mit dem Funktionsumfang von Wear OS und den Fitness-Funktionen zufrieden war, profitiert nun davon, dass der Akku länger durchhält, was nun auch Schlaf-Tracking ohne Zwischenladen ermöglicht.

Das Display ist zwar im Vergleich zu anderen Android-Smartwatches recht klein geblieben, dem steht aber der schicke und einzigartige Look der Pixel Watch 2 entgegen. Insgesamt ist die zweite Google-Uhr solide verarbeitet, bringt sinnvolle Sensoren und eine flotte Hardware mit und stellt nützliche Funktionen für sportlich aktive Nutzer bereit oder für solche, die nicht immer für jede Benachrichtigung ihr Android-Telefon aus der Tasche ziehen wollen. *(spo@ct.de)* c't

Google Pixel Watch 2

Smartwatch	
Hersteller, URL	Google, store.google.com/de
Größe / Gewicht / Schutzklasse	Durchmesser: 41 mm, Höhe: 12 mm / 31 g (ohne Armband) / IP 68
Konnektivität	4G LTE (optional), Bluetooth 5.0, WLAN (802.11 b/g/n, 2,4 GHz), NFC
Ausstattung	OLED-Display (320 dpi), 2 GByte RAM, 32 GByte Flash, GPS, Glonass, Beidou, Galileo, Quasi-Zenith Satellite, Kompass, Höhenmesser, Gyroskop, Beschleunigungssensor, Umgebungslichtsensor, Lautsprecher, Mikrofon
Sensoren	Bewegungssensor, optischer Puls- und SpO_2-Sensor, Einkanal-Elektrokardiogramm, Sensor zur Messung der Hautleitfähigkeit
Preis	399 € (ohne LTE), 449 € (mit LTE)

Eigenmarke

Telekom T Tablet mit 5G und Dual-SIM im Test

Das T auf dem Rücken, 5G-Modem samt eSIM-Option im Bauch – das T Tablet ist ein vergleichsweise günstiger Einstieg in die Welt der Tablets mit Mobilfunkmodem. Dem Prozessor fehlt es allerdings an Power.

Von Steffen Herget

Die Telekom baut das Hardwareangebot unter dem eigenen Namen aus. Nach den T Phones kommt das T Tablet, mit ähnlichem Ziel: das 5G-Netz der Telekom samt den passenden Verträgen unter die Leute zu bringen, und das mit Hardware zum Lockvogelpreis. Ohne Vertrag kostet das T Tablet 219 Euro, mit Zweijahrestarif nur einen Euro, dann zahlt man aber monatlich für einen Datentarif, zum Beispiel 25 Euro für 5 GByte Freivolumen.

Für ein Tablet ist der Telekom-Flachmann ziemlich kompakt geraten. Die Displaydiagonale von 10,4 Zoll unterbieten nur wenige aktuelle Tablets; zusammen mit den gleichmäßig rund einen Zentimeter dicken Rändern ringsum ergibt das eine gute Handlichkeit. Mit knapp unter einem Pfund ist das T Tablet außerdem leicht genug, dass auch bei längeren Sitzungen die Arme nicht erlahmen. Ungewöhnlich für ein Gerät knapp über 200 Euro: Das Gehäuse besteht nicht aus schnödem Plastik, sondern aus schwarzem Aluminium. Einziger Farbakzent ist der magenta getünchte Einschalter. Die Verarbeitung ist gelungen und lässt das Tablet hochwertiger wirken als viele andere Einsteigermodelle, einzig der Übergang vom Rand zum Bildschirmglas dürfte etwas fließender sein.

Das T Tablet funkt mobil in 5G-Netzen auf allen derzeit in Deutschland gängigen Frequenzbändern und unterstützt nicht nur eine, sondern zwei SIM-Karten – eine physische und eine eSIM. Dual-SIM in einem Tablet ist eine Rarität, die man selbst in Geräten der Oberklasse (Vergleichstest in [1]) kaum findet. Das moderne GSM-Modem wird konterkariert von einem eher lahmen WLAN-Chip, der nicht mehr als Wi-Fi 5 zu bieten hat.

Weitere Lücken in der Ausstattungsliste: Das Telekom-Tablet besitzt weder NFC noch einen Fingerabdrucksensor. Außer mit der klassischen PIN lässt sich das Gerät nur über einfache und unsichere Gesichtserkennung mit der Frontkamera entsperren.

Verständlich ist die Entscheidung des Herstellers, ein LCD-Panel einzubauen – ein OLED-Display hätte den Preis kräftig nach oben getrieben. Mit 455 cd/m² in der Spitze erreicht das Tablet eine ordentliche Helligkeit für ein Gerät dieser Kategorie, auch in hellerer Umgebung hatten wir keine Probleme, auf dem Bildschirm etwas zu erkennen. Für das Lesen im Dunkeln dürfte die Automatik sogar ruhig noch ein bisschen weiter nach unten regeln, in diesen Situationen bleibt das Display fast ein wenig zu hell. Von der Seite betrachtet legt sich schnell ein grauer Schleier über das Bild und die sonst ansprechenden Farben verblassen merklich. Bei aktivem Nachtlichtmodus, der den Anteil an blauem Licht verringert, um die Augen zu schonen, wird das Bild sehr gelblich.

Die beiden Lautsprecher tun sich überaus schwer damit, vernünftigen Sound zu erzeugen, vor allem wenn der Bass ins Spiel kommt – oder besser kommen sollte, denn davon ist nichts zu hören. Wer unterwegs am Tablet Filme oder Serien schauen möchte, sollte lieber einen Kopfhörer anschließen. Das muss allerdings über Bluetooth oder USB-C geschehen, denn eine 3,5-Millimeter-Klinkenbuchse besitzt das Gerät nicht.

Wenig Speed, viel Geruckel

Der Mediatek Dimensity 700 mit acht Rechenkernen und maximal 2,2 GHz Taktfrequenz ist kein High-End-Prozessor, das darf man zu diesem Preis aber auch nicht erwarten. Trotzdem könnte die Performance besser sein, das T Tablet reagierte im Test immer wieder nur mit Verzögerung, vor allem die Android-Wischgesten mussten wir oft mehrmals ausführen, bis eine Reaktion erfolgte. Apps starteten meist erst nach einer Gedenksekunde, und Animationen ruckelten immer wieder, statt flüssig abzulaufen. Die auf 60 Hertz beschränkte Bildwiederholrate des Displays tut ihr Übriges und verschlimmert

das Geruckel noch. Für technisch anspruchsvollere Spiele oder Videoschnitt taugt das Gerät nicht, zum Lesen, Mailen und Surfen reicht es. Von den beiden Acht-Megapixel-Kameras vorne und hinten sollte man ebenfalls keine Wunderdinge erwarten, Videotelefonie erledigen sie aber zuverlässig, wenn man für gute Beleuchtung sorgt.

Positiv überraschen konnte das T Tablet im Test mit seiner Akkulaufzeit. Vor allem der Standby-Verbrauch ist trotz aktiver SIM minimal, selbst eine ganze Woche untätig und eingeschaltet in der Schublade kosten keine 20 Prozent des 7000-mAh-Akkus. Ist er dann doch einmal leer, dauert es allerdings über dreieinhalb Stunden, bis die Ladestandsanzeige wieder 100 Prozent erreicht. Ein passendes Netzteil muss man selbst mitbringen, im Karton liegt abseits des Tablets nur ein USB-C-Kabel. Zubehör in Form von Stiften, Hüllen oder Tastaturen, welches den Nutzwert eines Tablets deutlich erhöht, bietet die Telekom für dieses Gerät nicht an.

Softwareseitig macht die Telekom keine Experimente. Auf dem Tablet läuft ein weitgehend unverändertes Android 13 mit einigen Telekom-Apps. Darüber hinaus sind auch die Apps von Amazon und Facebook vorinstalliert, nur erstere lässt sich deinstallieren. Multitasking funktioniert mit zwei Apps parallel, die Bildschirmaufteilung lässt sich flexibel verschieben. Insgesamt vier Jahre lang soll es Sicherheitspatches geben, drei Jahre lang monatlich, im vierten Jahr nur noch quartalsweise. Nur zwei große Android-Updates sind vorgesehen, bei Version 15 wird demnach Schluss sein.

Fazit

In der unteren Preisklasse, in der sich das T Tablet einsortiert, sind Tablets mit 5G-Unterstützung kaum zu finden, viel Konkurrenz hat die Telekom in diesem Aspekt nicht zu fürchten. Allzu viel Power darf man allerdings nicht erwarten, das T Tablet ist weit von der Performance teurerer Tablets entfernt. Bei Verarbeitung und Materialauswahl spielt es dafür eine Liga höher, als es das Preisschild vermuten lassen würde. Unter dem Strich ein ordentliches Gesamtpaket, wenn es ein günstiges Tablet mit SIM-Slot sein soll.

(sht@ct.de) c't

Literatur

[1] Steffen Herget, Größer geht immer, Sechs leistungsstarke Tablets mit Android und iOS im Vergleich, c't 23/2023, S. 60

Telekom T Tablet

Android-Tablet	
Hersteller, URL	Telekom, telekom.de
Betriebssystem / Patchlevel	Android 13 / September 2023
Funktionsupdates / Sicherheitspatches laut Hersteller bis min.	Android 15 / August 2027
Ausstattung	
Prozessor / Kerne × Takt / Grafik	Mediatek Dimensity 700 / 2 × 2,2 GHz, 6 × 2 GHz / Mali-G57 MC2
Arbeitsspeicher / Flash-Speicher (frei) / Wechselspeicher (Format)	6 GByte / 128GByte (107 GByte) / ✓ (MicroSD)
WLAN (Antennen) / Bluetooth / NFC / Kompass / Standort	Wi-Fi 5 (2) / 5.2 / – / ✓ / GPS, Glonass, Beidou, Galileo
USB-Anschluss / Kopfhöreranschluss / Fingerabdrucksensor	USB-C 2.0, OTG / – / –
Akku / wechselbar / drahtlos ladbar	7000 mAh / – / –
Maße (H × B × T) / Gewicht / Schutzart	24,8 × 15,7 × 0,78 … 0,92 cm / 490 g / IP52
Kameras	
Hauptkamera Auflösung / Blende / OIS	8 MP / ƒ/2 / –
Frontkamera Auflösung / Blende / OIS	8 MP / ƒ/2 / –
Display	
Diagonale / Technik / Auflösung / Punktdichte	10,4 Zoll / LCD / 2000 × 1200 Pixel / 225 dpi
Helligkeitsregelbereich / Ausleuchtung / max. Bildrate	5,95 … 455 cd/m² / 84 % / 60 Hz
Benchmarks	
Ladezeit 50 % / 100 %	1,2 h / 3,5 h
Laufzeiten[1] lokales Video 720p / 3D-Spiel / Stream	10,8 h / 9,8 h / 11,1 h
Geekbench V5 Single, Multi	530, 1779
3DMark Wild Life / WildLifeExtreme	1185 / 329
GFXBench Car Chase / Manhattan 3.0 / Manhattan 3.1 (je On-, Offscreen)	13 fps, 14 fps / 35 fps, 38 fps / 23 fps, 24 fps
Preis	219 €

[1] gemessen bei 200 cd/m² ✓ vorhanden – nicht vorhanden

Bildkünstler

Amazon hat den Fire TV Stick 4K Max in der zweiten Auflage hardwaremäßig aufgepeppt, das eigentliche Highlight ist aber das Feature „Ambient-TV“, das auf dem Fernseher in der streamingfreien Zeit Kunstwerke zeigt.

Der Quad-Core-Prozessor des neuen Fire TV Stick 4K Max läuft nun mit 2 statt 1,8 GHz, was ihn in der Fire-TV-Familie an die zweite Stelle hinter dem aktuellen Cube mit dessen Octa-Core-CPU (Test in c’t 25/2022, S. 92) platziert. Mit diesem hat der neue Fire TV Stick auch den 16 GByte großen Speicher (doppelt so viel wie vorher), Wi-Fi 6E und die erweiterte Alexa-Sprachfernbedienung mit mehr Tasten (etwa zum Skippen von Programmen) gemein.

Amazon setzt weiter auf eine Micro-USB-Buchse, worüber der Stick Strom bekommt (Netzteil liegt bei) und mit einem optionalen Adapter eine Kabelverbindung zum Internet herstellt. Schön: Im Unterschied zum ersten Max liefert der Neuling schon zur Premiere bei allen Videodiensten Bild und Ton in bestmöglicher Qualität (bis 4K/Dolby Vision und Dolby Atmos).

Abgesehen vom größeren Speicher bemerkt man im Alltag die leistungsfähigere Hardware selten, höchstens etwa bei Rennspielen. Wohl deshalb stellt Amazon auch das neue „Ambient-TV“-Feature heraus, das man vom TV-Spitzenmodell des Herstellers kennt: Spielt der Stick keinen Stream ab, zeigt er auf dem Fernseher ohne Zusatzkosten über 2000 (auch bekannte) Kunstwerke und Fotos sowie andere Bilder (etwa zu aktuellen Filmen) und Videos. Auf Wunsch gibt es dazu Widgets, die etwa das aktuelle Wetter oder To-do-Listen zeigen und mit der Fernbedienung ansteuerbar sind.

Die dynamischen Inhalte eignen sich mit ausgeblendeten Widgets und ohne Rahmen auch für OLED-TVs, die zum Einbrennen neigen. Im Ambient-Modus verbraucht der Fernseher natürlich wieder Strom; der Stick selbst fällt mit rund 1,5 Watt hingegen kaum ins Gewicht. Selbst bei einem Rund-um-die-Uhr-Betrieb käme man nur auf jährliche Kosten von etwa 4 Euro.

Der Fire TV 4K Max liefert eine gute Leistung ab, der Preissprung zur Erstauflage ist aber groß: Kostete der alte Max zum Start 65 Euro, bezahlt man für den neuen Stick 80 Euro. Reichen einem eine auf 1,7 GHz getaktete CPU, Wi-Fi 6 sowie 8 GByte Speicher und braucht man kein Ambient-TV, bekommt man den Fire TV 4K Stick (ohne Max) in der Neuauflage für 10 Euro weniger. *(nij@ct.de)*

Fire TV Stick 4K Max (2. Gen.)

HDMI-Streaming-Stick	
Hersteller, URL	Amazon, amazon.de
Videoformate	bis 2160p, inkl. HDR10/HDR10+, Dolby Vision, HLG; kodiert in H.265, H.264, VP9 oder AV1
Audioformate	PCM/WAV Stereo, Dolby Digital (Plus), Dolby AC4, Dolby Atmos, AAC, MP3, Vorbis, Passtrough: Dolby TrueHD, DTS-HD, MPEG-H
Konnektivität	HDMI, WLAN (Wi-Fi 6E), Bluetooth 5.2 und LE, Micro-USB (Strom / Ethernet-Adapter)
Lieferumfang	Netzteil, Fernbedienung (inklusive Batterien), Micro-USB-Kabel, HDMI-Verlängerung
Leistungsaufnahme	Standby 0,4 W / Ambient-TV 1,5 W / UHD-Video 1,6 W
Maße / Gewicht	99 mm × 30 mm × 14 mm / 43,5 g
Preis	80 €

Fadenverlierer

Die In-Ears Fidelio 2 kommen in einem edlen Metall-Case, ihr Klang lässt sich den eigenen Vorlieben anpassen, die Geräuschunterdrückung überzeugt. Leider verderben Verbindungsprobleme den Spaß.

Unter der Marke Philips hat TP Vision neue Fidelio-Kopfhörer vorgestellt, darunter die In-Ears Fidelio 2. Diese stecken in einem mit schottischem Muir-Leder bezogenen Metallgehäuse, auch an den Touchflächen der In-Ears findet sich das Leder wieder. Geräuschunterdrückung, Start/Stopp und Skippen steuert man durch Tipps auf den linken oder rechten Ohrhörer, die Lautstärke leider nur am Zuspieler oder in der Philips Headphone App.

Die Berührungssteuerung lässt sich in der App deaktivieren, etwa wenn man beim Sport versehentlich an die Touchflächen kommt. Dazu muss man der App allerdings die Standorterkennung erlauben. Das sei nötig, damit man die In-Ears wiederfindet, falls man sie verlegt hat. Unschön. Immerhin funktionieren die Fidelio 2 auch ohne App.

Philips legt flexible Silikonmanschetten in fünf Größen bei. Man verriegelt die Ohrhörer, indem man sie nach dem Einsetzen nach unten verdreht. Anschließend saßen sie auch beim Laufen sicher im Ohr. Nutzt man die In-Ears beim Einschlafen, lassen sie sich nach einer vorgewählten Zeit (30 Minuten bis 2 Stunden) automatisch abschalten. Aufladen per USB-C ist bereits nach zwei Stunden erledigt, der Akku in der recht großen Box reicht für dreimaliges Laden der Stöpsel.

Die dreistufige Geräuschunterdrückung (ANC) schirmt Nutzer mit vier Mikrofonen zuverlässig von Umgebungsgeräuschen ab. Im Hybrid-Modus sind Ansagen weiter zu hören, während Rauschen und Brummen von Bahn und Flugzeug herausgefiltert werden. Die Sprachverständlichkeit beim Telefonieren ist gut. Per Google-Sprachassistent kann man zudem das Smartphone steuern.

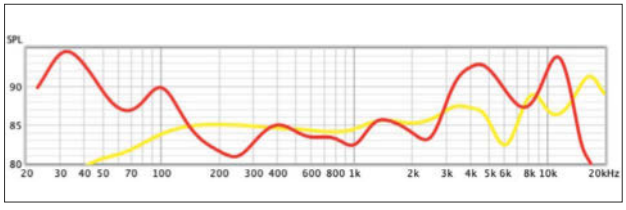
Im Musikeinsatz klingen die Fidelio 2 angenehm warm mit kräftigen Bässen und klaren Höhen. Man kann in der App per Equalizer ein persönliches Klangbild einstellen, zusätzlich finden sich dort vier weitere vordefinierte Modi. Die Ausgangslatenz ist mit 315 Millisekunden etwas hoch, sie lässt sich aber für Spiele und Videos verringern, wobei dann auch die Reichweite der In-Ears abnimmt.

Leider zeigt die Kopfhörer-App zuweilen falsche Ladezustände an und verbindet sich nur verzögert mit den Ohrhörern. Außerdem trennten sich die In Ears im Praxistest häufig unmotiviert vom Smartphone. In solchen Fällen half es meist, sie kurz aus dem Ohr zu nehmen. Im Laufe des Tests stellten sich weitere Verbindungsschwächen ein. Steckten die Fidelio-Ohrhörer in der Box, verbanden sich Box und Ohrhörer schnell per Bluetooth mit dem Smartphone. Doch waren die In-Ears erst im Ohr, brach die Verbindung ab und ließ sich häufig nicht wieder herstellen. In dieser Form machen die eigentlich sehr angenehmen Fidelio-2-In-Ears keinen Spaß.

(uk@ct.de)

Philips Fidelio 2 T2/00

In-Ear-Kopfhörer	
Hersteller, URL	TP Vision, philips.de
Anbindung / Codec	Bluetooth 5.3 / LDAC, AAC, SBC
Systemanf.	App ab Android 5 / iOS 13
Preis	280 €



Die In-Ear-Kopfhörer Fidelio 2 (rote Kurve) setzen die im Benutzermodus gewählte Bassbetonung gut um. Im Vergleich die neutral abgestimmten Sennheiser HD600 (gelb).

Dolmetscher für die Hosentasche

Handheld-Übersetzer: Fluentalk T1 und T1 Mini im Test

Fluentalk T1 und T1 Mini sehen wie Handys aus, aber transkribieren, übersetzen und lesen in anderen Sprachen vor, was man einspricht, eintippt oder abfotografiert. Ob sie besser als Apps wie Google Translate und DeepL sind, haben wir uns genauer angeschaut.

Von Stella Maria Risch

Wer eine Sprachbarriere fühlt, will schnell eine Lösung. Viele greifen dann auf den Google-Übersetzer oder vergleichbare Apps auf ihrem Smartphone zurück. Der chinesische Hersteller Timekettle bringt ähnliche Funktionen in Extrageräten unter, dem Fluentalk T1 für rund 280 und den T1 Mini für rund 140 Euro.

In beiden steckt eine eSIM. Eine Datenflatrate ist im Kaufpreis enthalten, mit der der T1 zwei Jahre und sein kleiner Bruder ein Jahr in 84 Ländern Gesprochenes online übersetzen. Nachdem der Zeitraum abgelaufen ist, können Nutzer für rund 15 Euro (15,90 US-Dollar) im Monat oder 44,90 US-Dollar pro Jahr nachbuchen oder in den T1 eine eigene Nano-SIM-Karte einlegen. Per WLAN funktioniert die Übersetzung auch ohne SIM. Für die Offlinenutzung hat Fluentalk 13 Sprachkombinationen mit Englisch und Chinesisch als Downloadpakete vorbereitet. Für Gesprochenes stehen auf dem T1 40 Sprachen für die Onlineübersetzung bereit, darunter neben Deutsch und Englisch auch Arabisch, Chinesisch, Finnisch, Hindi, Koreanisch und Russisch. Auf dem T1 Mini sind es 4 weniger.

Optisch unterscheiden sich die beiden vor allem durch ihre Größe: Das Display misst im T1 10, 2 cm (4 Zoll) Diagonale, das des Mini nur 7,1 cm (2,8 Zoll). Die rechte Seite beherbergt die Tasten, die man zum Übersetzen gedrückt halten soll. Der Mini hat weniger Knöpfe und das deutet bereits darauf hin: Ihm fehlen Funktionen.

Funktionen

Gesprochenes übersetzen beide Kästchen mittels Ein-Klick-Übersetzung: Der T1 bietet dafür zwei Knöpfe, die der Nutzer im Gespräch abwechselnd drückt – je nachdem, wer gerade spricht. Der T1 Mini besitzt nur einen Knopf und muss deshalb selbst erkennen, wer gerade spricht. Die Sprechererkennung funktionierte im Test gut. Der T1 beherrscht drei weitere Übersetzungsmodi: Im Querformatmodus tippt man auf dem Display des T1 zwei Schaltflächen an, um das Übersetzen zu starten und zu stoppen. Der Hörmodus ist für Monologe etwa bei einem Vortrag gedacht, wohingegen man das Gerät im Modus Chatübersetzung zwischen zwei Menschen legt, die sich unterhalten. Dann erkennt der T1, wer spricht.

Wenn man in das Mikrofon-Array der Übersetzer gesprochen hat, zeigen sie den verstandenen Text klein an. Die Übersetzung folgt in größerer Schrift kurz danach. Anschließend lesen die Geräte den Text laut vor. Dabei betont die deutsche Stimme manche Worte unnatürlich. Wer lieber selbst liest, schaltet das Vorlesen aus. Da die Geräte Bluetooth haben, kann man sich die Übersetzung über Kopfhörer ausgeben lassen. Die Texte und Übersetzungen der geführten Gespräche stehen im Nachhinein zur Verfügung. Wer sie nachvollziehen möchte, kann einfach hochscrollen. Exportieren lassen sie sich nicht.

Mit den sogenannten Schnellsätzen können Nutzer auf beiden Modellen Sätze vorformulieren und per Knopfdruck abspielen. Das kann hilfreich sein, wenn man unterwegs schnell nach etwas fragen möchte.

Praxis

Zum Testen haben wir in jedem Modus dasselbe Gespräch mit den Übersetzungsgeräten, dem Google Übersetzer und der Übersetzungs-App von DeepL geführt. Dabei unterhielten sich eine Grafikerin und ein Entwickler. Die Geräte und Apps sollten dafür zwischen Englisch und Deutsch übersetzen.

Die Übersetzung im Ein-Klick-Modus gefiel uns gut. Der auf Deutsch ausgege-

bene Text enthielt Kommata und hinter manchen Fragen auch Fragezeichen. Gelegentlich kamen beim Übersetzer andere Worte an, als wir gesagt hatten. So hat der T1 aus „He found himself at war“ „Self aware“ gemacht. Wenn wir den Satz langsamer und deutlicher wiederholten, dolmetschte der T1 jedoch in der Regel korrekt. Manche technischen Begriffe wie „etwas zu debuggen“ und „JavaScript“ kannten die Geräte. Das schafften Google Translate und DeepL auch.

Außerdem übersetzte der T1 für uns Smalltalk zwischen Türkisch und Deutsch. Unser menschlicher Tester war mit der Übersetzung sehr zufrieden.

Der Inhalt des übersetzten Gesprächs war nachvollziehbar. Etwas mehr Unstimmigkeiten gab es im Offlinemodus. Die Apps von Google und DeepL hingegen bieten gar nicht an, gesprochene Sprache offline zu übersetzen. Diese Funktion hat Google nur für Text.

Der Chatmodus ist dem Ein-Klick-Modus in Transkribierung und Übersetzung sehr ähnlich. Wir haben ihn bezogen auf die Redegeschwindigkeit auf die Probe gestellt. Dabei zeigte sich: Damit die Geräte alles Gesagte aufzeichnen können, sollte man die vorangegangene Übersetzung in gewöhnlicher Geschwindigkeit durchlesen oder sich die Ansagen anhören. Wer nur flott überfliegt und weiterspricht, ist dem Gerät zu schnell. Wenn sich beide Seiten allerdings auf die Situation einlassen, funktioniert der Übersetzer angenehm.

Weniger hilfreich sind die Geräte in Situationen, in denen man das Gesagte nicht langsamer und deutlicher wiederholen kann, wenn man zum Beispiel mit dem Hörmodus einem fremdsprachigen Vortrag

Der Fluentalk T1 zeigt im Nachhinein den übersetzten und den eingesprochenen Text an – hier im Hörmodus zu sehen.

T1 und T1 Mini sind zwar technisch verwandt, sie unterscheiden sich aber deutlich.

folgt. Je nach Geräuschpegel und Aussprache missverstehen oder verpassen die Geräte Worte oder ganze Sätze. Als wir eine Rede von Joe Biden auf YouTube abspielten, zeichnete der T1 ungefähr ein Drittel falsch auf, trotz Nebengeräuschunterdrückung. Timekettle antwortete auf unsere Nachfrage, dass die Transkribierung von Lautstärke, Akzent und Sprechgeschwindigkeit abhängt. Die Diktierfunktion von Word und die Untertitel auf YouTube verstanden die gleiche Stelle ohne Probleme.

Wenn die Übersetzer das Gesagte korrekt mitgeschnitten und transkribiert hatten, funktionierte die Übersetzung fast wortgleich wie bei den bekannten Onlinediensten von Google oder DeepL. Das verwundert nicht, gibt doch Timekettle auf unsere Nachfrage an, mit DeepL, Google, Microsoft und weiteren zu kooperieren.

Foto-Übersetzung

Die sogenannte Foto-Übersetzung gibt es auf beiden Geräten. Dabei fotografieren Nutzer Texte mit der eingebauten 8-Megapixel-Kamera. Dann übersetzen die Geräte Zeile für Zeile separat, was zu Problemen führt. Zum Beispiel bringen mehrteilige Prädikate sie durcheinander. Der Modus genügt allerdings, um grob den Inhalt nachzuvollziehen, vor allem Kurztexte in Karten und Menüs. Google-Übersetzer und DeepL sind in dieser Disziplin besser und geben für Texte mit mehreren Zeilen sinnvolle Sätze aus.

Beide Geräte haben einen Akku mit 1500 mAh. In unserem Test verlor der T1 in zwei Stunden Dauernutzung 39 Prozent, er dürfte also rund fünf Stunden am Stück übersetzen; der T1 Mini verlor 25 Prozent und kommt damit auf rund acht Stunden. Im Standby hat der T1 in elf Stunden 8 Prozent und der Mini 7 gelassen, sie kommen in diesem Modus also auf mehrere Tage. Für eine volle Ladung müssen die Kistchen per USB-C etwa 80 Minuten an einem Ladegerät hängen.

Das um einige Funktionen kastrierte Betriebssystem Android 10.0 soll laut Hersteller noch Versionsupdates erhalten. Die Security-Patches sind seit über einem Jahr allerdings ohne Update geblieben. Die Bedienoberfläche wurde stark modifiziert, so fehlt zum Beispiel die bekannte Bedienleiste am unteren Rand. Ein Browser oder Apps sind nicht anzutreffen, sie sind auch nicht installierbar, sodass man die Datenflat nur zum Übersetzen nutzen kann.

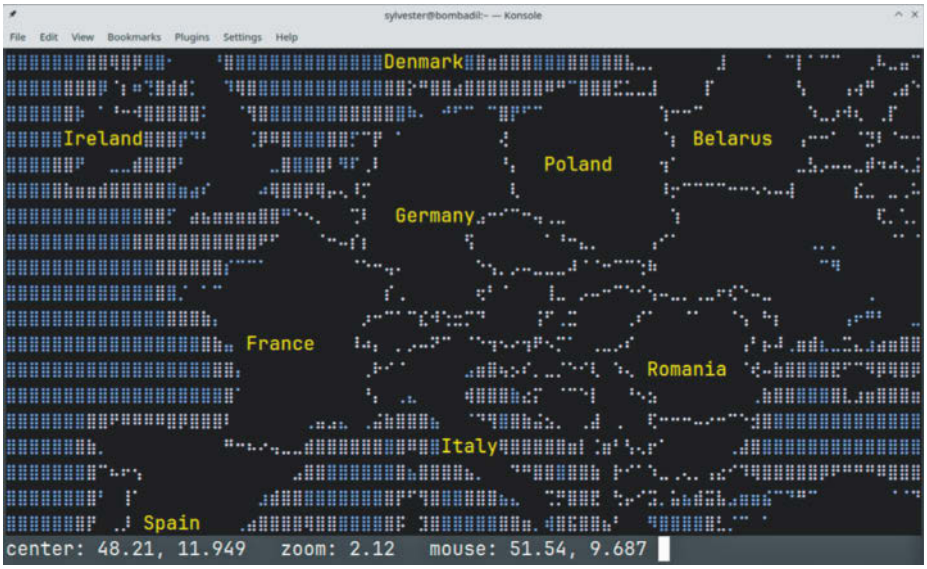
Fazit

Die Fluentalk-Übersetzer haben im Vergleich zu Google Translate und DeepL einige Vorteile: Man kann wegen der Datenflatrate in 84 Ländern online übersetzen, auch außerhalb des EU-Roamings. Außerdem übersetzen sie Gesprochenes zumindest in einigen Sprachen auch offline und sind schneller startklar als die Apps, die man auf dem Handy erst suchen und starten muss. Unserer Erfahrung nach schalten Apps in Gesprächen zudem schneller ab. Auch mag man vielleicht nicht in jeder Situation seinem Gegenüber das eigene Handy in die Hand geben.

Andererseits sind 140 oder rund 280 Euro eine Stange Geld, während man die Apps von Google oder DeepL gratis bekommt. Außerdem muss man den Übersetzer mit sich herumtragen. Dem günstigen Mini fehlen der praktische Chatmodus und der SIM-Steckplatz, das Display ist arg klein geraten. Beide Geräte eignen sich nicht für Nutzer, die sich nicht wohl damit fühlen, ihre Gespräche an ein chinesisches Unternehmen zu übertragen. Diejenigen sollten das Gerät nicht kaufen und stattdessen für das Geld einen menschlichen Übersetzer mieten. Der wird bestimmt keine Daten weitergeben. *(stri@ct.de)* c't

Fluentalk T1 und T1 Mini

Mobile Übersetzer		
Modell	T1	T1 Mini
Hersteller, URL	Timekettle, fluentalk.com	Timekettle, fluentalk.com
Maße und Gewicht	116,8 × 58,6 × 11,2 mm, 115 g	91 × 54,8 × 13,4 mm, 86 g
Display (Auflösung)	10,1 cm (4 Zoll) Diagonale (540 × 1080)	7,1 cm (2,8 Zoll) Diagonale (480 × 640)
Netzwerk	eSIM, Nano-SIM-Steckplatz, WLAN	eSIM, WLAN
Flash-Speicher	32 GByte	8 GByte
Arbeitsspeicher	3 GByte	1 GByte
Sprachen	40 Online-Sprachen, 13 Offline-Sprachen, Foto-Übersetzung in 39 Sprachen	36 Online-Sprachen, 13 Offline-Sprachen, Foto-Übersetzung in 39 Sprachen
Preis	300 Euro (wechselkursabhängig)	150 Euro (wechselkursabhängig)



Die Welt im Terminal

Das kleine Programm MapSCII rendert eine Landkarte ins Terminal. Braucht man das? Vermutlich nicht; aber ein Hingucker ist es allemal.

Sie würden sich lieber Südfrankreich ansehen, statt auf die Kommandozeile zu stieren? Dank MapSCII geht beides gleichzeitig. Das Programm zeichnet eine Landkarte ins Terminal, die Sie – je nach den Fähigkeiten Ihres Terminalemulators – mit dem Mausrad oder den Tasten A und Z zoomen können. Per Drag & Drop oder über die Pfeiltasten verschieben Sie die Karte zum Wegträumort.

Anders als der Name vermuten lässt, benutzt MapSCII primär Unicode-Zeichen für Brailleschrift, um die Karte darzustellen. ASCII-Zeichen dienen lediglich der Beschriftung. Konturen wie Kontinent- und Landesgrenzen in eher kleinen Zoomstufen oder Gebäudeformen in sehr großen stellt das Programm damit erstaunlich gut dar. In den Größenordnungen dazwischen muss man oft ein bisschen rein- und rauszoomen, um eine Darstellung zu finden, in der man beispielsweise das Straßennetz einer Großstadt erkennt – zumindest einigermaßen. Per Druck auf die Taste C schaltet man auf einen Rendermodus um, der Klötzchen statt Braillezeichen anzeigt. Das macht die Karte aber eher schlechter als besser lesbar.

Eine besonders praktische Karten-App ist MapSCII damit nicht und leider ist die Entwicklung der Software auch weitgehend eingeschlafen. Das Projekt sei im „minimalen Wartungsmodus“, kommentierte ein Mitwirkender im Issuetracker. Aber um ernsthafte Konkurrenz zu grafischen Karten-Apps geht es wohl ohnehin nicht. Eher um nerdige Coolness – und die liefert MapSCII zweifellos.

Wer auf die Schnelle mit Landkarten in der Konsole angeben will und (auch 2023 noch) einen Telnet-Client auf dem PC hat, muss das Programm nicht einmal installieren. Es genügt die Eingabe:

```
telnet mapscii.me
```

Um die in JavaScript geschriebene Software stattdessen lokal zu installieren, greift man am einfachsten zum JavaScript-Paketmanager npm:

```
npm install -g mapscii
```

Nutzer des Snap-Paketformats (also vornehmlich Ubuntu-Anwender) können auch ein Paket von snapcraft.io installieren und Arch-Fans finden mapscii als „nodejs-mapscii“ im AUR. Das Kartenmaterial kommt auch nach der Installation von http://mapscii.me, wird aber lokal im Ordner ~/.mapscii gecached. Wer sich ein klein wenig mit JavaScript und etwas mehr mit Kartenformaten auskennt, kann die Software auch dazu bringen, lokal gespeicherte (Vektor-)Karten anzuzeigen.

(syt@ct.de)

MapSCII

Kartenprogramm für die Kommandozeile	
Entwickler, URL	Michael Straßburger, github.com/rastapasta/mapscii
Systemanf.	Node.js, xterm-kompatibles Terminal
Preis	**kostenlos,** Open-Source-Lizenz (MIT)

Hardcore-Datenretter

In unserem Datenrettungsschwerpunkt in c't 21/2023 haben wir ein spannendes Werkzeug übersehen, um Daten von teildefekten Datenträgern zu kratzen: HDDSuperClone.

Wer sich mit Datenträgern herumschlägt, die sich nicht mehr vollständig lesen lassen, weiß Werkzeug zu schätzen, das die noch lesbaren Daten herunterkopieren kann. Das unter GNU-Lizenz entwickelte ddrescue funktioniert dafür recht gut. Doch unter Profis beliebt und bekannt ist HDDSuperClone, das Scott Dwyer von 2015 bis 2022 entwickelt und kommerziell vertrieben hat. Im Jahr 2022 hat er den Quelltext unter GPL2 freigegeben. Auf GitHub gibt es zwei Repositories, in denen eine sanfte Weiterentwicklung stattfindet. Wir haben uns OpenSuperClone angesehen, für das RPM- und Debian-Pakete zu haben sind.

Bei OpenSuperClone handelt es sich um ein Linux-Programm mit grafischer Bedienoberfläche. Seine Hauptaufgabe ist es, möglichst viele Sektoren von einem nicht mehr zuverlässig arbeitenden Datenträger auf einen heilen oder in eine Image-Datei zu übertragen. Wie ddrescue kopiert es alle lesbaren Daten, ohne deren Kontext in einem Dateisystem wie frei oder belegt zu berücksichtigen, also anders als das bei Imagern üblicherweise der Fall ist. Defekte Sektoren bringen das Programm nicht aus dem Tritt. Mit trickreichen und mehrphasigen Vorgehensweisen tastet es sich an defekte Bereiche eines Datenträgers heran.

OpenSuperCloner besticht durch sehr hardwarenahe Funktionen für das Auslesen von Datenträgern. Das betrifft zum einen die Art und Weise, wie es Datenträger anspricht: So lauscht es direkt an ATA- und USB-Geräten und umgeht so eventuelle Wiederholungsversuche des Betriebssystems bei defekten Bereichen. Hardwarenah heißt zum anderen: Auf Festplatten abgestimmte Verfahren sparen einzelne Köpfe aus, wenn dort gehäuft Fehler auftreten und ein physischer Schaden naheliegt.

Damit direkte Zugriffe überhaupt möglich sind, versteckt das Programm Datenträger vor dem Betriebssystem. Das geschieht über Parameter des Linux-Kernels (wie `libata.force=9:disable`), die das Programm eintragen und entfernen kann. Um eventuell im BIOS-Setup nötige Optionen, etwa AHCI-Support, muss sich der Nutzer selbst kümmern. Bei USB-Geräten schiebt das Programm schlicht die Linux-Module beiseite, die sich dieser normalerweise bemächtigen.

Anders als ddrescue überträgt OpenSuperCloner nicht nur Daten. Es zeigt obendrein SMART-Informationen des Datenträgers und bietet verschieden tiefe Schnellanalysen eines Datenträgers durch Lesezugriffe in Zonen über die Gesamtoberfläche. Es kennt nicht nur verschiedene Modi für den Zugriff, sondern diverse Timeouteinstellungen und sogar Funktionen, die einen behandelten Datenträger per Relais aus und wieder einschalten, wenn beim Auslesen ein harter Reset fällig sein sollte, weil der Datenträger nicht mehr reagiert.

Sehr cool ist die Funktion, eine virtuelle Kopie des gerade zum Auslesen konfigurierten Laufwerks als Datenträger unter Linux wieder bereitzustellen: Noch während der Rettung können so andere Werkzeuge auf der virtuellen Kopie arbeiten. Für die direkten Zugriffe und die virtuellen Laufwerke übersetzt das Programm eigeninitiativ spezielle Treiber. Das klappt mit OpenSuperClone 2.4.1 unter Debian 11 (Bullseye) mit einem Kernel 5.10 tadellos, nicht jedoch mit aktuellem Debian 12 (Bookworm). Einsteiger sollten Einarbeitungszeit einkalkulieren.

(ps@ct.de)

OpenSuperClone (HDDSuperClone)

Datenrettung	
URL	https://github.com/ISpillMyDrink/OpenSuperClone (https://github.com/thesourcerer8/hddsuperclone)
Systemanf.	Linux, fertige RPM- und DEB-Pakete
Preis	**kostenlos** (GPL)

Mainstreamig

Workstation-Grafikkarten Radeon Pro W7600 und W7500

Nicht alle Workstation-Grafikkarten kosten Tausende Euro. Für viele Aufgaben genügen deutlich günstigere Versionen, die aber auf dem Stand der Technik sein sollen. AMDs effiziente Radeon Pro W7600 und W7500 sollen diesen Markt bedienen.

Von Carsten Spille

Wer eine Grafikkarte für den professionellen Einsatz braucht, schaut sich oft bei den sogenannten Workstation-Modellen um. Das sind technische Abwandlungen von Spielergrafikkarten; AMD vermarktet sie als Radeon Pro und Nvidia schlicht als RTX. Haben die bis zu 10.000 Euro teuren High-End-Varianten meist doppelt so viel Grafikspeicher wie ihre Gaminggeschwister [1], sind die billigsten Einsteigermodelle wie die Radeon Pro W6400 [2] meist nur das Feigenblatt für fehlende integrierte Prozessorgrafik, da sie für komplexe CAD-Modelle oder aufwendige Berechnungen zu langsam sind.

In die Lücke dazwischen stoßen AMDs Radeon Pro W7500 und W7600, die 440 respektive 600 Euro kosten und damit für eine breitere Nutzergruppe bezahlbar bleiben. Sie belegen anders als die ansonsten eng verwandte Gamingversion Radeon RX 7600 nur einen Steckplatz [3].

Darüber hinaus sind sie mit 70 beziehungsweise 130 Watt anstelle von 160 Watt viel sparsamer unterwegs, die 7500 mit ihren 70 Watt kommt gar ohne einen separaten Stromanschluss aus. Beide Karten haben mit acht Gigabyte Grafikspeicher ausreichend Speicher, protzen aber im Vergleich zur Gamingversion nicht mit verdoppelter Kapazität. Monitore schließt man an einen der vier DisplayPorts an, auf das primär für Fernseher im Wohnzimmer interessante HDMI muss man bei Profikarten verzichten oder einen Adapter bemühen.

Nvidias aktuelle Gegenstücke, die RTX A2000 mit 12 GByte für knapp 600 Euro und die 6-GByte-Variante für rund 390 Euro standen uns für den Test leider nicht als direkte Vergleichsmodelle zur Verfügung.

Ein bisschen Technik

Auf Radeon Pro W7500 und W7600 rechnet der kompakte und damit kostengünstige Navi33-Grafikchip, den AMD anders als die teureren Alternativen noch konven-

tionell als Einzelchip herstellt. Technikschnörkel wie Chiplets oder HBM-Stapelspeicher sucht man in dieser Leistungsklasse vergebens, sie sind hier allerdings auch noch nicht nötig.

Beide Karten haben DisplayPort-Anschlüsse, die sich auf Version 2.1 des Standards verstehen. Pro Anschluss stehen 38,7 Mbit/s zur Verfügung (UHBR10), bei DP 1.4 waren es lediglich 25,9 Mbit/s. Damit sind feinere Auflösungen mit höheren Refreshraten drin oder der Verzicht auf Farbkomprimierung „DSC“, auch wenn die optisch eigentlich verlustfrei sein soll. Praktisch sind damit nun zwei statt einem 8K-Display möglich, 8K mit 120 Hertz anstelle von 60 Hertz oder 10K60-Auflösung statt „nur“ 8K60. Mit an Bord sind auch neue Videoeinheiten, die den Prozessor nicht nur bei der Wiedergabe von AV1- und VP9-kodierten Filmen entlasten, sondern auch Videos mit diesen und anderen Codecs erzeugen können.

In der W7600 hat der Grafikchip 32 Compute Units mit zusammen 2048 Shader-Rechenwerken – genau wie in der Gamingversion. Damit die Kühlung kompakt bleibt und dabei nicht zu laut wird, hat AMD ihm das erlaubte Leistungsbudget gekappt. Die Karte darf nur 130 Watt schlucken. Sie passt damit in denselben Leistungsrahmen wie die Vorgängerin Radeon Pro W6600 und braucht einen sechspoligen PCI-Express-Anschluss ans Netzteil. Gegenüber der Vorgängerin verfügt sie nicht nur über eine modernere Architektur, sondern auch über schnelleren Grafikspeicher, der über seine Schnittstelle mit 128 parallelen Datenleitungen bis zu 288 GByte/s überträgt, rund 29 Prozent mehr als bei der W6600.

Die Radeon Pro W7500 muss mehr Federn lassen und wurde mit 28 CUs (1792 Shader-Rechenkernchen) auf das Level der Pro W6600 gestutzt, außerdem hat sie 23 Prozent langsameren Speicher als die Vorgängerin. Dafür kommt sie bei 20 Prozent mehr nominaler Rechenleistung mit nur 70 Watt aus und braucht keinen separaten Stromanschluss mehr. Die nur acht PCI-Express-4.0-Leitungen, mit denen die Karten ans System angebunden sind, spielen in dieser Leistungsklasse nur eine untergeordnete Rolle. Wer regelmäßig mit größeren Datensets zu tun hat als in den Grafikspeicher passen, greift zu Radeon Pro W7700 (und aufwärts) oder einer entsprechenden Nvidia RTX.

Sparsam und (nicht so) leise

Die kleinen Radiallüfter der W7600 und der W7500 pressen die Luft durch den Kühler und einen großen Teil der Abwärme durch die Slotblende aus dem Rechner hinaus; im Leerlauf halten sie nicht an. Mit den dann anliegenden einstelligen Wattzahlen wurden sie allerdings locker fertig, der Rotor der W7600 war nur fast unhörbare 0,1 sone laut, der der W75600 blieb unterhalb unserer Messgrenze von 0,1 sone. Mit beinahe der doppelten Leis-

Günstige Workstation-Grafikkarten: Leistung in Blender 3.6 LTS

Grafikkarte	Szene „classroom“ RT/default[1] [s]	Szene „Gooseberry Benchmark“ RT/default[1] [s]	Szene „Lone Monk“ RT/default[1] [s]
	◂ besser	◂ besser	◂ besser
AMD Radeon Pro W7600	55,6/61,8	0[2]/ 460,8	453,1/531,6
AMD Radeon Pro W7500	76,7/84,7	0[2]/ 564,2	643,4/741,6
zum Vergleich			
AMD Radeon Pro W7800	24,4/29,1	88,6/145,9	202,2/251,7
AMD Radeon Pro W6800	36,7/41,7	115,1/178,3	288,2/341
AMD Radeon Pro W6600	65,6/73,9	0[3]/0[3]	537,4/653,4
AMD Radeon Pro W5700[4]	0/88,6	0/401,7	0/714,8
AMD Radeon Pro WX 8200[4]	0/103,0	0/977,5	0/869,0
Nvidia RTX A5000	14,2/25,4	61,4/133,4	94,3/225,5
Radeon RX 7900 XTX	17,1/19,6	65,3/110,6	133,8/160,2
GeForce RTX 4090	6,4/10,0	33,3/64,8	43,2/83,0

gemessen unter Windows 11 22H2 mit Ryzen 9 7950X3D (16c/32t), 32 GByte DDR5-5200, VSync aus, rBAR an, Treiber: Nvidia PRD 536.25, AMD Pro 23.Q3, RSAE 23.7.1
[1] RT: Nvidia Optix, AMD HIP+RT; default: Nvidia CUDA, AMD HIP [2] Absturz zum Desktop [3] „Driver Timeout“ [4] WX 8200 und W5700 haben keine RT-Einheiten

Günstige Workstation-Grafikkarten: Leistungsvergleich SPEC ViewPerf 2020 v3.1

	3dsmax-07[1] [fps]	catia-06[2] [fps]	creo-03[3] [fps]	energy-03[4] [fps]	maya-06[5] [fps]	medical-03[6] [fps]	snx-04[7] [fps]	sw-06[8] [fps]
	besser ▸	besser ▸	besser ▸	besser ▸	besser ▸	besser ▸	besser ▸	besser ▸
AMD Radeon Pro W7600	67,5	62,1	97,4	26,2	162,2	32,2	215,5	97,2
AMD Radeon Pro W7500	46,7	46,9	70,0	15,8	112,9	20,8	155,6	69,1
zum Vergleich								
AMD Radeon Pro W7800	129,7	97,2	151	51,0	321,6	64,2	403,9	191,1
AMD Radeon Pro W6800	114,0	93,9	130,6	34,2	332,5	48,5	339,8	162,3
AMD Radeon Pro W6600	47,9	55,7	90,4	14,0	164,4	23,2	229,9	82,3
AMD Radeon Pro W5700	54,2	58,6	98,8	15,6	193,6	25,5	241,7	94,1
AMD Radeon Pro WX 8200	30,0	39,1	61,4	16,2	136,3	21,7	176,7	70,0
AMD Radeon Pro WX 7100	25,3	26,5	42,9	7,8	80,3	13,0	121,1	41,6
Nvidia RTX A5000	112,7	95,6	146,3	31,0	288,0	30,0	372,2	139,0
GeForce RTX 4090[9]	223,6	89,7	129,9	66,7	512,7	43,3	43,0	326,7

gemessen unter Windows 11 22H2 mit Ryzen 9 7950X3D (16c/32t), 32 GByte DDR5-5200 [1] 3dsMax 2016 (DirectX11) [2] CATIA V5/3DExperience [3] PTC Creo [4] OpendTect [5] Autodesk Maya 2017 (ViewPort2.0)
[6] Tuvok library [7] Siemens PLM NX8.0 [8] Dassault Solidworks 2020 [9] Gaming-Grafikkarte, außer Konkurrenz, teils sehr niedrige Werte wegen fehlender Optimierungen

Der kleine Navi33-Grafikchip (Bildmitte) sorgt auf Radeon Pro W7500 und W7600 für die nötige Rechenleistung.

tungsaufnahme hatte das größere Kühlsystem der längeren W7600 damit allerdings etwas mehr Probleme. Der Chip wurde auch unter Volllast nicht kritisch warm, aber der Lüfter musste schneller drehen und erreichte hörbare 1,6 sone in der Spitze. Die 70 Watt der W7500 bekommen deren Gebläse und Kühlrippen dagegen flüsterleise gekühlt – wir maßen sehr gute 0,2 sone.

Kurze Lastspitzen von wenigen Millisekunden Dauer sprengten bei der Radeon Pro W7500 allerdings die PCIe-Spezifikation von 75 Watt, auch wenn aufgrund der kurzen Dauer akut keine Schäden am Mainboard zu befürchten sind.

Günstige Grafikkarten für Workstations – technische Daten und Messwerte

Modell	AMD Radeon Pro W7500	AMD Radeon Pro W7600
Architektur, Grafikchip (Fertigungsprozess / Chipfläche / Transistoren)	RDNA3, Navi 32 (6 nm / 204 mm² / 13,3 Mrd.)	RDNA3, Navi 32 (6 nm / 204 mm² / 13,3 Mrd.)
APIs: Direct3D / OpenGL / OpenCL / Vulkan / Sonstige	DX12 Ultimate (FL 12_1) / 4.6 / 1.3 / 2.0 / ROCm	DX12 Ultimate (FL 12_1) / 4.6 / 2.1 / 1.2 / ROCm
Compute Units (Shader-ALUs / AI-Beschleuniger / RT-Einheiten / Textureinheiten / Rasterendstufen)	28 (1792 / 56 / 28 / 112 / 64)	32 (2048 / 64 / 32 / 128 / 64)
FP32-Rechenleistung[1]	12,2 TFlops	19,99 TFlops
für FP32-Durchsatz rechnerisch nötiger Takt	1701 MHz	2440 MHz
Grafikspeicher: Menge, Typ (Übertragungsrate) / ECC	8 GByte, GDDR6 (173 GByte/s) / –	8 GByte, GDDR6 (288 GByte/s) / –
Displayanschlüsse	4 × DP 2.1 (UHBR 10)	4 × DP 2.1 (UHBR 10)
gleichzeitige Displays (max. Refresh, 4K60 = 4096 × 2160, 60 Hz)	4 × 4K120 (mit DSC) / 4 × 5K60 / 2 × 8K60 / 1 × 10K120 (mit DSC)	4 × 4K120 (mit DSC) / 4 × 5K60 / 2 × 8K60 / 1 × 10K120 (mit DSC)
TDP / Stromanschlüsse	70 W / –	130 W / 1 × 6-Pol
Anbindung Host-System (PCIe-Transferrate pro Richtung)	PCIe 4.0 x8 (16 GByte/s)	PCIe 4.0 x8 (16 GByte/s)
Kühlung	Single-Slot, aktiv (Radiallüfter)	Single-Slot, aktiv (Radiallüfter)
Länge × Höhe × Breite / Gewicht	21,7 cm × 11,2 mm × 1,9 cm / 338 g	24,2 cm × 11,2 mm × 1,9 cm / 566 g
Sonstiges	32 MByte Infinity-Cache	32 MByte Infinity-Cache
Zusätzliche Messungen		
reale 3D-Taktrate: kurzzeitiges Maximum GPU-z	1894 MHz	2481 MHz
reale Taktrate: Blender Classroom (Teillast) / Furmark 1080p (Volllast)	2160 MHz / 1045 MHz (95 fps)	2657 MHz / 1565 MHz (160 fps)
3DMark Firestrike Extreme / Time Spy / Port Royal (RT) / Speedway (RT)	9197 / 7336 / 3502 / 1235	13394 / 10502 / 5183 / 1861
Technische Prüfungen		
Leistungsaufnahme 2D[2] / Multimonitor[3]	8 (18) / 16 (19) W	9 (32) / 19 (32) W
Leistungsaufnahme 3D / Volllast (Peak[4])	75 / 75 (89) W	135 / 137 (165) W
Lautheit Leerlauf / Last / Max	< 0,1 / 0,2 / 0,2 sone	0,1 / 1,3 / 1,6 sone
Preis Straße (US-UVP)	circa 440 €	circa 600 €

[1] Herstellerangabe [2] bei 60 (120) Hertz [3] mit 2 × 4K60 (3 × 1080p60 + 1 × 4K60) [4] kurzzeitiger Spitzenwert für wenige Millisekunden
✓ vorhanden – nicht vorhanden k. A. keine Angabe

Auf Effizienz getrimmt

Neue Leistungsdimensionen eröffnen beide Karten nicht, aber die Performance profitiert von den Verbesserungen in Architektur und Fertigung – davon also, dass die Karten sowohl mehr Arbeit pro Taktschritt schaffen, einen höheren Takt erreichen und zudem sparsamer mit Energie umgehen. Im geometrischen Mittel über die Ergebnisse der Spec ViewPerf2020 v3.1 lag die Radeon Pro W7600 in unseren Tests um 21 Prozent vor der Vorgängerin Radeon Pro W6600. Besonders stark schnitt sie in der 3D-Visualisierung der Subtests energy-03 und medical-03 ab. Die Pro W7500 schaffte 84 Prozent des geometrischen Mittels der W6600 bei nur 54 Prozent der Leistungsaufnahme.

Gegenüber älteren Radeon-Pro-Modellen war die W7600 knapp schneller als das Topmodell der Vor-Vorgängergeneration Radeon Pro W5700. Die W7500 toppte knapp das Leistungsniveau des ehemaligen High-End-Modells Radeon Pro WX 8200 von 2018, das dafür statt 70 satte 230 Watt auffahren musste.

Fazit

Für Workstations mit mittleren Ansprüchen sind AMDs Einsteiger-Radeon-Pro der 7000er-Reihe gute Optionen. Sie bringen moderne Technikfeatures zum Beispiel für besonders hochauflösende Bildschirme oder zur Videobearbeitung mit. Die Lüfter bleiben dabei sehr leise (W7500) bis erträglich (W7600) und stören bei der täglichen Arbeit im Büro nicht. Für Compute-Aufgaben und speziell KI-Berechnungen muss AMD seine aktuelle ROCm-Softwareplattform 5.7.1 und Programmbibliotheken erst noch für die kleineren Karten anpassen und freigeben. Bis das geschieht, sind Nvidias RTX-Karten dafür noch die bessere Wahl.

(csp@ct.de) c't

Literatur

[1] Carsten Spille, Elitäre Bildveredler, Workstation-Grafikkarten AMD Radeon Pro W7000 und Nvidia RTX 6000 Ada im Test, c't 18/2023, S. 104
[2] Carsten Spille, Mini-Profi, Grafikkarte für kleine Workstations: Radeon Pro W6400, c't 7/2022, S. 75
[3] Carsten Spille, Kleine 8er-Bahnen, Die Mittelklasse-Grafikkarten AMD Radeon RX 7600 und Nvidia GeForce RTX 4060 Ti im Test, c't 15/2023, S. 102

Multiplikatoren für die Produktivität: DockingStations für Multi-Display- und Multi-Port-Arbeitsplätze

Mehr als ein Bildschirm am Arbeitsplatz gehört für viele Büromitarbeiter, für Programmierer und auch Spieler zum Standard. Doch für viele Nutzer stellt sich noch immer die Frage: Wie schließe ich einen oder mehrere zusätzliche Bildschirme an meinen PC, Notebook oder Tablet an?

Ein Weg, der nicht nur einen Zuwachs an Anzeigefläche, sondern auch eine Vielzahl an nützlichen Anschlüssen bietet, ist der über DockingStations von ICY BOX®.

Wie viele Bildschirme würden Sie gerne nutzen? Abseits des rein beruflichen Kontextes ist das immer öfter auch eine persönliche Entscheidung. Während in einigen Berufsfeldern der Arbeitgeber bereits eine Entscheidung für seine Angestellten getroffen und gleichzeitig die technischen Rahmenbedingungen erfüllt hat, lohnt es sich auch für Privatpersonen und Heimnutzer, sich mit diesem Thema zu beschäftigen.

Hier sind gerade Hobby-Programmierer, Fotografen und Grafikdesigner Paradebeispiele für Anwender, die sich einen unmittelbaren Vorteil durch mehrere Displays versprechen dürfen. Mittlerweile kommen seltener ausschließlich große Desktop PCs zum Einsatz. Das hat Vor- und auch Nachteile.

Mobil und doch beschränkt?

Durch wachsende Rechen- und Grafikleistung anderer Computerformen, namentlich Notebooks, Tablets und sogar Smartphones sind Anwender heute viel flexibler in ihrer Bewegungsfreiheit, da diese Geräte kompakt und leicht sind. Doch in Sachen verfügbare Anschlüsse sind diese Geräte häufig eingeschränkt. Doch es gibt Lösungen.

Das mobile Büro

Sind Sie vor allem mit Ihrem Notebook oder einem großen, grafikfähigen Tablet mit Stylus unterwegs und wollen gelegentlich einen externen Bildschirm anschließen – etwa bei einem Kunden oder bei Ihrem Arbeitgeber – helfen bereits kostengünstige DockingStations wie die IB-DK4050-CPD weiter.

Über einen universell kompatiblen USB Type-C® Stecker profitieren Sie von insgesamt 12 Ports. Darunter finden sich zwei HDMI® und ein DisplayPort™ Anschluss, über die Ihre Arbeitsfläche um bis zu zwei Monitore zur Erweiterung oder Spiegelung ergänzt werden kann. Gleichzeitig können Geräte, die üblicherweise nicht über RJ45 LAN Anschlüsse verfügen, mittels DockingStation an kabelgebundene Netzwerke angeschlossen werden. Hier bietet das IB-DK4050-CPD eine Übertragungsrate von bis zu 5 Gbit/s.

Einschränkungen müssen bei diesen Einsteigermodellen jedoch hingenommen werden. Etwa bei der maximal erreichbaren Auflösung. Wer etwa mehr als ein zusätzliches Display mit einer Auflösung von mindestens 2K bei 60 Hz verwenden oder angeschlossene Geräte laden will, sollte zu einer „größeren" Variante greifen, die neben hoher Übertragungsgeschwindigkeit auch eigene Stromversorgung und leistungsfähigere Technik bietet.

Schaltzentrale auf dem Schreibtisch

Hier bietet sich etwa die IB-DK2288AC an. In einem eleganten schwarzen Aluminiumgehäuse verbergen sich hier sogar 17 Anschlüsse, die sich per USB Type-C® Kabel mit dem Hostcomputer verknüpfen lassen und über insgesamt je vier HDMI® und DisplayPorts™ bis zu 4 Bildschirme mit 4K Auflösung betreiben lassen. Dank beiliegendem Netzteil laden Sie gleichzeitig ein Notebook mit USB Type-C® Power Delivery mit 100 Watt und ein Tablet oder Smartphone mit bis zu 30 Watt. Durch die Notwendigkeit einer Steckdose verlieren Sie natürlich an Mobilität im Vergleich zur IB-DK4050-CPD.

Dafür profitieren selbst ältere Computer über eine USB Verbindung von einer Vielzahl zusätzlicher Optionen, die den Arbeitsplatz bereichern – etwa durch drei weitere USB 3.2 Gen 1 Ports und einen SD und microSD 4.0 Kartenleser.

Zukunftssicher mit USB4®

USB 3 war gestern – USB4® ist der neue Standard und wer bereits jetzt von rasanten Übertragungsgeschwindigkeiten von bis zu 40 Gbit/s profitieren will, sollte die IB-DK2880-C41 in Erwägung ziehen.

Hier locken zwei zusätzliche Displays mit 8K Auflösung und bis zu 60 Hz Wiederholfrequenz per HDMI® Anschluss und versprechen damit, die Umgebung für kreative Arbeiten auf ein neues Level zu heben. Gleichzeitig bietet das Modell drei USB 3.2 Gen 2 Anschlüsse, die Datenübertragungen mit bis zu 10 Gbit/s ermöglichen sowie ein USB Type-C® PD-Anschluss mit 100 Watt Ladeleistung, ein Ethernet-Port, Headset Kombibuchse und SD/microSD 4.0 Kartenleser.

Auch hier gilt wieder: Wer die volle Leistung abschöpfen will, muss auch bei diesem Mo-dell in der Nähe einer Steckdose arbeiten. Durch die umfangreichen Anschlussmög-lichkeiten tragen die DockingStations von ICY BOX® jedoch deutlich zur Produktivität auf dem Schreibtisch oder unterwegs bei.

USB4® DockingStation IB-DK2880-C41

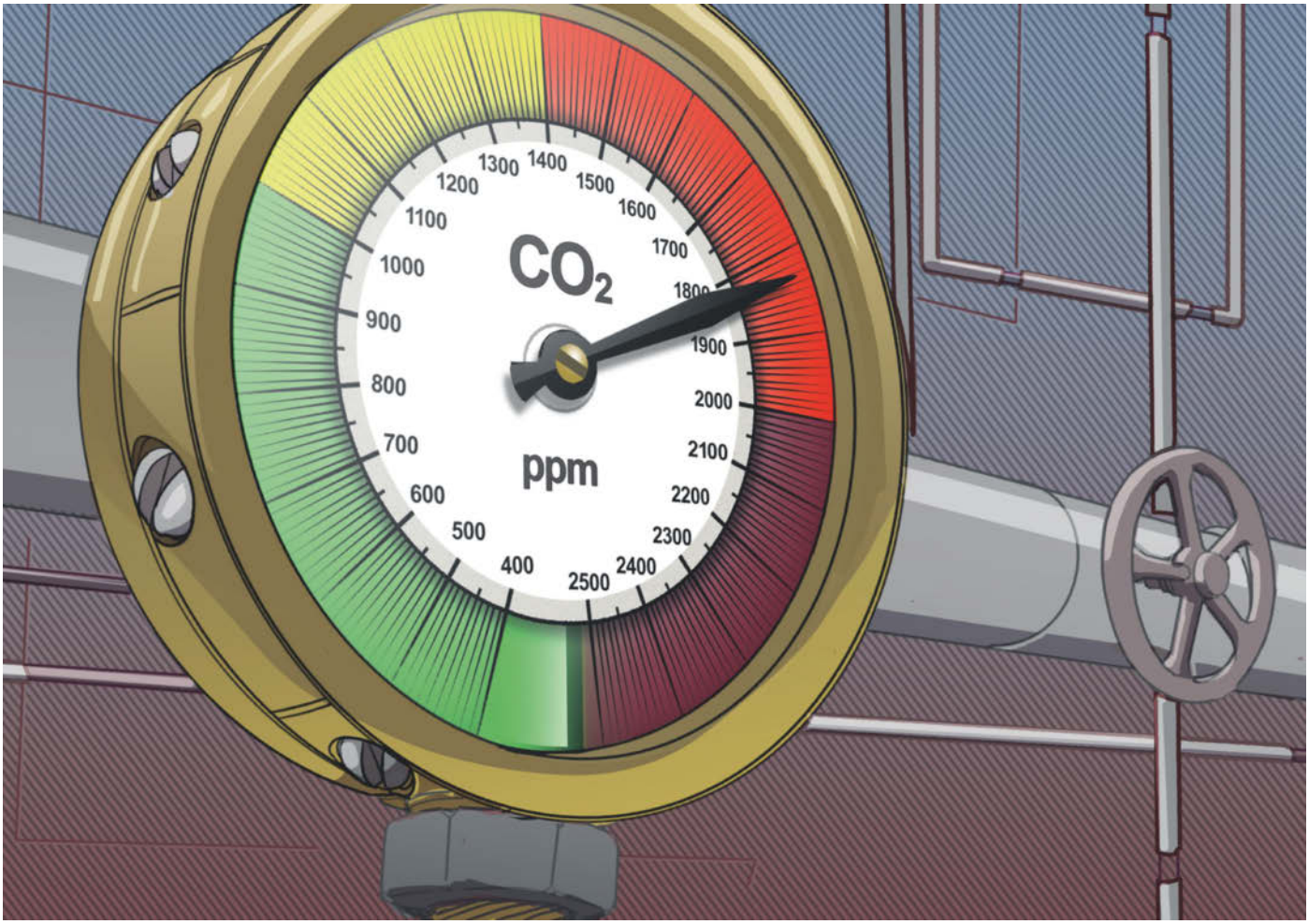


Bild: Thorsten Hübner

Frischluftanzeiger

Neun CO_2-Messgeräte für den Hausgebrauch

CO_2-Messgeräte geben darüber Aufschluss, wie gut ein Raum gelüftet ist und erlauben eine grobe Einschätzung des Infektionsrisikos durch Aerosole in der Luft, etwa für die Übertragung von Grippe- oder Coronaviren. Bei uns im Büro schlugen sich die Testkandidaten ganz ordentlich.

Von Urs Mansmann

Kohlendioxid ist in der Atemluft immer vorhanden. Sein Gehalt in der Lufthülle der Erde stieg seit Beginn der Industrialisierung von 280 auf aktuell 420 ppm (Parts per Million, Millionstel). Von Menschen ausgeatmete Luft enthält rund das Hundertfache davon, also 40.000 ppm. Das führt dazu, dass die CO_2-Konzentration in nicht oder schlecht gelüfteten Räumen stark ansteigen kann, wenn sich Menschen darin aufhalten. Je kleiner der Raum und je größer die Zahl der Menschen, desto höher fällt der Messwert aus.

Wir haben neun handelsübliche Messgeräte unterschiedlicher Preisklassen näher untersucht. Die Genauigkeit der Messwerte an sich konnten wir nicht prüfen, aber wir haben die Geräte miteinander verglichen. Dabei stellte sich heraus, dass alle Geräte den CO_2-Gehalt richtig einordnen. Es gab keinen Ausreißer mit offensichtlich falschen Anzeigewerten. Die Geräte unterscheiden sich aber vom Leistungsumfang her erheblich, siehe Tabelle auf Seite 93.

Das Umweltbundesamt hat 2008 in einer Bekanntmachung bewertet, welche gesundheitlichen Auswirkungen hohe Kohlendioxidkonzentrationen haben (siehe ct.de/yt4g). Bis 1000 ppm gelten die Werte als unbedenklich, zwischen 1000 und 2000 als auffällig und über 2000 als inakzeptabel. In der Praxis werden diese Schwellen häufig überschritten, beispielsweise in Klassenräumen, aber auch in Schlafzimmern oder Warteräumen, wenn die Lüftung unzureichend ist.

Lüftungsanlagen müssen pro Person und Stunde 36 bis 54 Kubikmeter Frischluft fördern, um die CO_2-Konzentration konstant unter den empfohlenen 1000 ppm zu halten. Viele Räume werden aber nicht über eine Anlage, sondern nur über

c't kompakt

- Aus dem CO_2-Messwert lässt sich ablesen, wann gelüftet oder eine Maske getragen werden sollte.
- Portable Geräte mit Akku oder Batterie lassen sich auch unterwegs gut nutzen.
- Ampeln und akustische Warnung liefern leicht verständliche Informationen über die Luftqualität.

Fenster belüftet – und die bleiben häufig zu, wenn es draußen kalt ist. Das ist auch ein Grund dafür, warum die Saison für Atemwegsinfekte hierzulande in die kalte Jahreszeit fällt.

Schlechte Luft

Werden 1000 ppm CO_2 in der Raumluft deutlich überschritten, leidet die Konzentrationsfähigkeit. Gesundheitlich bedenklich werden die Werte ab ungefähr 5000 ppm. Solche Spitzenwerte wurden beispielsweise bei Messreihen in deutschen Schulen vereinzelt gemessen. Das ist kein Wunder: In einem nicht gelüfteten Klassenraum mit 70 Quadratmetern und 25 Schülern erreicht der CO_2-Gehalt der Luft nach 45 Minuten bereits über 2000 ppm, nach 90 Minuten mit geschlossenen Fenstern kratzt er bereits an der 4000er-Marke.

Eine gute Lüftung senkt auch das Risiko, sich in geschlossenen Räumen, die man mit anderen Menschen teilt, beispielsweise mit Corona, einer Grippe oder einer einfachen Erkältung anzustecken. Anhand der CO_2-Konzentration kann man das Risiko abschätzen, das die Atemluft birgt: Je näher die Werte an die Basiskonzentration von 420 ppm heranrücken, desto häufiger wird die Luft ausgetauscht und desto geringer ist der Gehalt an potenziell gefährlichen Aerosolen. Höhere Werte als 1000 ppm weisen laut Umweltbundesamt auf ein erhöhtes Infektionsrisiko hin – außer die Luft wird zusätzlich gefiltert, etwa mit HEPA-Filtern (HEPA, High-Efficiency Particulate Air), die feinste Partikel aus der Luft zurückhalten, aber keinen Einfluss auf die CO_2-Konzentration haben. Solche Filter kommen beispielsweise in Flugzeugen zum Einsatz, es gibt aber auch Geräte für Wohnräume.

Richtig lüften

Üblicherweise muss man selbst daran denken, regelmäßig zu lüften, denn leistungsfähige Lüftungsanlagen sind bestenfalls in Passivhäusern verbaut. Mit CO_2-Messgeräten lässt sich der optimale Zeitpunkt dafür finden und die Dauer optimieren. Wer ein solches Gerät im Einsatz hat, findet schnell heraus, wie häufig und wie lange er lüften muss, um ein gewünschtes Niveau zu halten.

Zeichnet man die CO_2-Konzentration auf, bildet sich durch regelmäßiges Lüften ein typisches Sägezahnmuster: Der Messwert steigt kontinuierlich und linear an, um mit dem Lüften schlagartig wieder abzufallen. Sobald die Fenster wieder zu sind, beginnt ein neuer Anstieg. In einem nur per Lüftungsanlage belüfteten Raum hingegen nähert sich die Konzentration einem bestimmten Wert an, der von der zugeführten Luftmenge und der Personenanzahl im Raum abhängt. Ist niemand anwesend, nähert sich die Konzentration der der Außenluft, also 420 ppm. Das niedersächsische Landesgesundheitsamt stellt auf seiner Webseite eine Anwendung bereit, mit der sich die CO_2-Konzentration im Zeitverlauf berechnen lässt (siehe ct.de/yt4g).

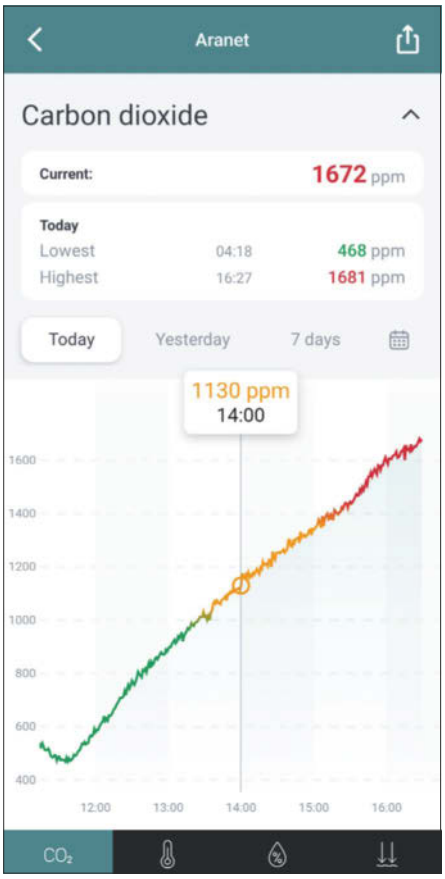
Um die Messgeräte zu benutzen, muss man keine Werte interpretieren. Die Warnhinweise sind leicht verständlich.

Die getesteten Geräte: Hinten das Bresser Smile XXL, davor v.l.n.r. Airco2ntrol Up, Luftqualitätsmonitor INV, Hama Safe, Aranet4 und CO2 Smile, vorne Airco2ntrol Mini, Coach und 5000.

Anzeige unterwegs

Wir haben für unsere Marktübersicht handelsübliche Messgeräte beschafft, die uns teilweise von den Herstellern zu Testzwecken zur Verfügung gestellt wurden. Die günstigsten Geräte sind ab rund 40 Euro erhältlich, am teuersten ist das Aranet4 für rund 180 Euro, das für den professionellen Einsatz entwickelt wurde: In der Pro-Version lassen sich bis zu 100 Aranet4 über eine Basisstation in einem Funknetzwerk mit bis zu drei Kilometern Reichweite laut Hersteller vernetzen. Damit lässt sich beispielsweise die CO_2-Konzentration in Klassen- oder Konferenzräumen oder in Betriebs- und Lagerstätten überwachen und dokumentieren.

Besonders praktisch im Alltag sind batterie- oder akkubetriebene Geräte, in



Die App für den Aranet4 bietet umfangreiche Möglichkeiten, die Messwerte darzustellen, im Ausschnitt sichtbar sind die Daten des Testlaufs.

unserem Testfeld waren das vier Vertreter: Airco2ntrol Up, Aranet4, der CO_2 Luftqualitätsmonitor INV und der Safe CO_2-Luftmesser. Die Laufzeiten der Geräte sind allerdings sehr unterschiedlich: Als erstes machte das Gerät von Hama nach rund 5 Stunden schlapp, die Modelle von TFA Dostmann und Bresser hielten mit 22 und über 24 Stunden erheblich länger durch. Von der Form und Größe her eignen sich nur das Aranet4 und das Gerät von Hama für die Jacken- oder Handtasche, die Geräte von Bresser und TFA Dostmann sind dafür zu groß und sperrig.

Der Aranet4 fällt dabei aus dem Rahmen: Er wird mit herkömmlichen AA-Batterien bestückt und läuft damit nach Herstellerangaben je nach Voreinstellung bis zu fünf Jahre. Der Sensor ist mit einem besonders stromsparenden E-Paper-Display ausgestattet. Fast alle anderen Geräte haben einen USB-Anschluss. Sie lassen sich also auch unterwegs mit einer handelsüblichen Powerbank betreiben. Die Modelle Smile und Smile XXL von Bresser haben allerdings ein Netzteil, brauchen also einen Anschluss ans Stromnetz, wobei das riesige XXL-Gerät für einen mobilen Einsatz ohnehin nicht infrage kommt.

Praktischer Testlauf

Wir haben alle CO_2-Geräte in einer realen Umgebung getestet. Die Geräte befanden sich dazu in einem Homeoffice mit 70 Kubikmeter Rauminhalt, das zunächst ausgiebig mit Durchzug gelüftet worden war, sodass der CO_2-Gehalt der Raumluft auf rund 420 ppm fiel. Dann wurden alle Fenster und Türen geschlossen, es befand sich ständig eine Person im Raum. Daraufhin stieg der CO_2-Wert über fünf Stunden kontinuierlich an. Um eine gleichmäßige Durchmischung zu erreichen, hielt die Testperson stets mehr als zwei Meter Abstand von den Testgeräten, zudem sorgte ein Deckenventilator für eine permanente Durchmischung der Luft. Weil die Messwerte schon spürbar steigen, wenn man sich nahe bei den Geräten aufhält, sollten sie für eine genaue Messung stets etwas abseits stehen und nicht etwa direkt vor einem auf dem Schreibtisch.

Wir brachen den Test ab, bevor der kritische Wert von 2000 ppm erreicht wurde, der nach unserer Berechnung nach rund fünfeinhalb Stunden zu erwarten war. Die Geräte zeigten ziemlich genau das an, was wir vor Versuchsbeginn berechnet hatten. Alle Anzeigen ließen also einen validen Rückschluss auf die Qualität der Raumluft zu und bildeten den annähernd linearen Anstieg sehr präzise ab, siehe Grafik auf dieser Seite.

Die Geräte messen alle 1 bis 15 Sekunden den CO_2-Gehalt der Luft. Lediglich der Aranet4 hat mit 1 bis 10 Minuten einen viel längeren Zyklus. In der Praxis macht das kaum einen Unterschied, denn der Messwert verändert sich ja langsam über mehrere Stunden hinweg. Kaum jemand behält das Messgerät über längere Zeit im Auge, deshalb ist eine Alarmfunktion wichtig, die auf das Überschreiten eines Grenzwerts aufmerksam macht.

Nerviges Piepen

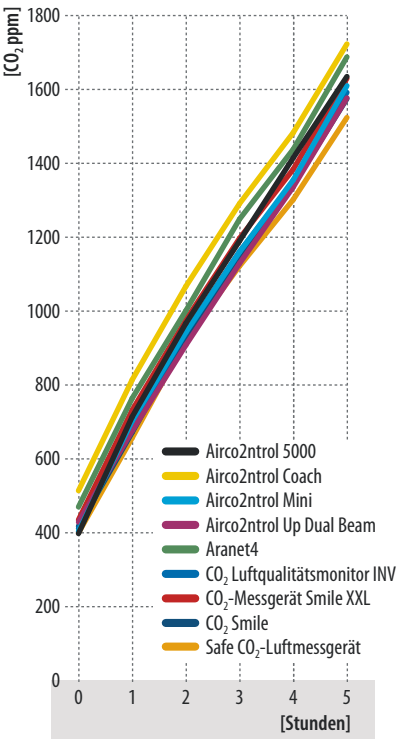
Eindeutig übertrieben haben die Entwickler dabei beim CO_2 Luftqualitätsmonitor INV von Bresser. Der Alarm besteht aus einem schrillen Ton, der sich eher nach Rauchmelder anhört denn nach dezentem Hinweis. Am zurückhaltendsten war der Aranet4, der bei jeder zu hoch ausgefallenen Messung nur einmal kurz und leise piepst und dann wieder Ruhe gibt. Die Modelle von Hama und das CO_2 Smile von Bresser wiederum melden sich mit steigender CO_2-Konzentration immer nachdrücklicher. Die nervige Akustik hat einen erheblichen Nachteil: Man ist versucht, den Alarm zunächst einmal abzuschalten, weil das Lüften erst mit Verzögerung wirkt – und vergisst nachher womöglich, ihn wieder zu aktivieren.

Praktisch und sehr informativ ist die Einordnung der Messwerte in einer Ampel. Bis 1000 oder 1200 ppm bewerten die Geräte die Luftqualität als gut, normal oder ausreichend, daran schließt sich ein gelber Bereich mit bedenklichem CO_2-Gehalt bis 1400 oder 1600 ppm an, jenseits davon wird Alarmstufe rot gegeben, bei einigen Geräten sogar noch mit einer weiteren Warnstufe ab 2000 oder 2500 ppm. Bei fast allen Geräten lässt sich die Alarmschwelle individuell verändern.

Besonders flexibel warnt der Airco2ntrol Coach: Dessen Display lässt sich so einstellen, dass sich die helle Hintergrundbeleuchtung zwischen 420 und 1400 ppm kontinuierlich von grün über gelb nach

CO_2-Messkurve

In einem Praxislauf mit ständig steigendem CO_2-Gehalt in der Luft (siehe Text) zeigten alle CO_2-Messgeräte ähnliche Werte an, es gab keinen Ausreißer.



ninjaOne

Zeit sparen, Endpunkte schützen: Automatisierung der IT-Sicherheit durch NinjaOne

Cyberangriffe werden immer ausgefeilter und komplexer. Gerade bei der Stärkung und Optimierung der Sicherheit von Endpunkten spielt daher Automatisierung eine Schlüsselrolle. Die Fähigkeit, Sicherheitsrichtlinien und -maßnahmen automatisch und konsistent zu implementieren, bildet die Basis dafür, dass Netzwerke jederzeit geschützt sind, selbst wenn IT-Teams nicht sofort verfügbar sind.

Endpunkte automatisch absichern: Mehr als nur Bequemlichkeit

Für IT-Admins, die täglich mit einer Fülle von Aufgaben konfrontiert sind, bietet die Automatisierung von Sicherheitsprozessen eine dringend benötigte Entlastung. Dabei ist sie nicht nur eine Frage der Bequemlichkeit; sie ist für die Aufrechterhaltung einer robusten Sicherheitsinfrastruktur unerlässlich. Durch Automatisierung können IT-Admins gewährleisten, dass Sicherheitsrichtlinien und -updates in Echtzeit und ohne menschliches Eingreifen angewendet werden. Dies ist in großen Organisationen oder in Netzwerken mit einer Vielzahl von Endpunkten besonders wichtig.

Ein großer Vorteil der Automatisierung liegt in der Zeiteffizienz. Statt manuell jeden einzelnen Endpunkt zu überprüfen und zu aktualisieren, können Prozesse im Hintergrund laufen, wodurch IT-Teams wertvolle Zeit für andere kritische Aufgaben gewinnen. Die Konsistenz, die durch Automatisierung erreicht wird, gewährleistet, dass alle Endpunkte nach den gleichen Standards geschützt sind und nicht durch menschliche Fehler oder Versäumnisse vermeidbaren Risiken ausgesetzt werden. Selbst die erfahrensten IT-Profis können Fehler machen, insbesondere bei wiederholten und monotonen Aufgaben. Die Automatisierung solcher Prozesse beugt solchen Schwierigkeiten vor.

Sicherheitsrichtlinien als Blaupause für die Endpunktsicherheit

Sicherheitsrichtlinien dienen als Leitfaden für Organisationen, um sicherzustellen, dass ihre Systeme und Daten vor Bedrohungen geschützt sind. Einige der wichtigsten Richtlinien für Endpunkte beinhalten die regelmäßige Aktualisierung von Software, die Verwaltung von Benutzerrechten, den Schutz vor Malware und die Überwachung ungewöhnlicher Aktivitäten.

Um dem hohen zeitlichen Aufwand Herr zu werden, den die Anwendung dieser Richtlinien in großen Organisationen mit sich bringt, kommen Automatisierungstools wie NinjaOne ins Spiel. NinjaOne ermöglicht es IT-Admins, Sicherheitsrichtlinien zentral zu definieren und sie dann automatisch auf alle Endpunkte im Netzwerk anzuwenden. Egal, ob es sich um Passwortrichtlinien, Software-Updates oder Berechtigungseinstellungen handelt, mit solchen Werkzeugen können Admins sicherstellen, dass jeder Endpunkt konform ist.

Eine Übersicht über Maßnahmen zur Endpunktsicherheit, die sich mit NinjaOne automatisieren lassen:

Firewall-Konfiguration: Firewalls dienen als Verteidigung gegen externe Bedrohungen. Durch Automatisierung kann die Konfiguration zentralisiert und regelmäßig aktualisiert werden, wodurch Fehler reduziert und ausgehende Verbindungen zu schädlichen Websites blockiert werden können.

Fortgeschrittene Überwachung: Automatisierte Protokollierung und Überwachung bieten detaillierte Einsichten in Endpunktaktivitäten. Bei Sicherheitsvorfällen können sie schnell wertvolle Informationen liefern. Besonders kritisch ist die Überwachung von Berechtigungsänderungen, die durch automatisierte Systeme sofort erkannt werden.

Passwortverwaltung: Administratorpasswörter sind essenziell für die Sicherheit. Mit Automatisierung kann die Rotation und Speicherung dieser Passwörter vereinfacht werden, wodurch menschliche Fehler reduziert und die Einhaltung von Sicherheitsstandards gewährleistet wird.

Entfernung von Malware: Für den Fall, dass schädliche Software wie Adware oder Ransomware ihren Weg auf einen Endpunkt finden, hilft die Automatisierung z. B. durch benutzerdefinierte Skripte dabei, diese zu entfernen, bevor sie Schaden anrichten können.

Automatisierung bietet eine leistungsstarke und effiziente Möglichkeit zur Steigerung der Endpunktsicherheit. Dennoch ist es von entscheidender Bedeutung, dass IT-Admins alle Prozesse sorgfältig testen, um sicherzustellen, dass sie wie beabsichtigt funktionieren und keine unbeabsichtigten Folgen haben. Mit der richtigen Kombination aus Sicherheitsrichtlinien und ihrer Automatisierung können IT-Admins sicherstellen, dass ihre Endpunkte gegen die vielfältigen digitalen Bedrohungen geschützt sind.

dunkelrot verfärbt, sodass man auch aus dem Augenwinkel mitbekommt, wenn der CO_2-Wert zu hoch klettert. Alternativ kann man das Gerät so einstellen, dass sich die Hintergrundbeleuchtung erst beim Erreichen einer definierten Warnschwelle aktiviert und dann deutlich sichtbar mit roter Warnfarbe auf den zu hohen CO_2-Pegel hinweist, ohne jedoch akustisch zu nerven.

Kleiner Messbereich

Eindeutig zu klein ist der Messbereich mit bis zu 3000 ppm beim Airco2ntrol Mini. Dieser Wert wird in schlecht gelüfteten Räumen leicht erreicht, und es macht durchaus noch einen Unterschied, wie weit er überschritten wird. Alle anderen Geräte zeigten mindestens bis 5000 ppm an. Prüfen lässt sich das leicht, indem man vorsichtig und aus mindestens einem halben Meter Entfernung in Richtung des Gerätes bläst. Direkt aus kurzer Entfernung hineinpusten oder -hauchen sollte man keinesfalls, weil das zur Bildung von Kondenswasser führen und im Extremfall sogar den Sensor beschädigen kann.

Bei den von uns untersuchten Geräten ist auch ein besonders großes dabei, das Bresser Smile XXL. Mit der noch aus vielen Metern Entfernung ablesbaren Anzeige mit 7,5 cm hohen Lettern eignet es sich beispielsweise für Klassenräume oder Großraumbüros. Die Warnschwelle für den akustischen Alarm lässt sich in einem breiten Bereich einstellen und weist dann nachdrücklich darauf hin, wenn es Zeit wird, die Fenster zu öffnen.

Sehr nützlich sind Verlaufsanzeigen. Damit kann man beispielsweise in Schlafräumen oder Büros über einen längeren Zeitraum die Messwerte erfassen und anschließend auswerten. Der Airco2ntrol 5000 von TFA Dostmann hat dazu ein Display, das den Verlauf für eine Minute, eine Stunde, einen Tag und eine Woche anzeigt. Fest für 24 Stunden ist der Verlauf beim Airco2ntrol Coach des gleichen Herstellers auf dem Display sichtbar.

Daten im Log

Mehr Möglichkeiten bietet ein Datenlog, aus dem die Messwerte auch noch lange nach der Messung ausgelesen werden können. Sehr komfortabel ist das beim Airco2ntrol 5000 gelöst. Das Gerät legt jeden Tag eine Datei auf einer MicroSD-Karte an und speichert dort sämtliche Messwerte mit einem Intervall von 5 Sekunden ab, also 17.280 Einträge pro Tag. Die Speicherkarte lässt sich entnehmen und die enthaltenen Excel-Dateien, die mit dem Datum versehen sind, am PC auswerten. Damit das richtig funktioniert, muss die Systemuhr des Messgeräts aber korrekt gestellt sein, was man bei allen Geräten mit Uhr manuell erledigt.

Beim Aranet4 speichert der Sensor die Messwerte zwischen und überträgt sie bei jedem Kontakt per Bluetooth an eine Smartphone-App, mit der man nicht nur die Daten auswerten, sondern auch die Voreinstellungen ändern kann, etwa für die Warnschwellen. Die App stellt Graphen für CO_2-Gehalt, Temperatur, Luftfeuchtigkeit und Luftdruck über beliebige Zeitintervalle dar. Extrem sperrig ist die Protokollfunktion hingegen beim Bresser CO_2 Luftqualitätsmonitor INV, der maximal 12.700 Messwerte auf einem internen Speicher ablegt. Zur Programmierung des Messzeitraums und -intervalls sowie der anschließenden Auswertung muss man ein PC-Programm des Herstellers einsetzen, das eine Einarbeitung erfordert und wenig bedienungsfreundlich ist.

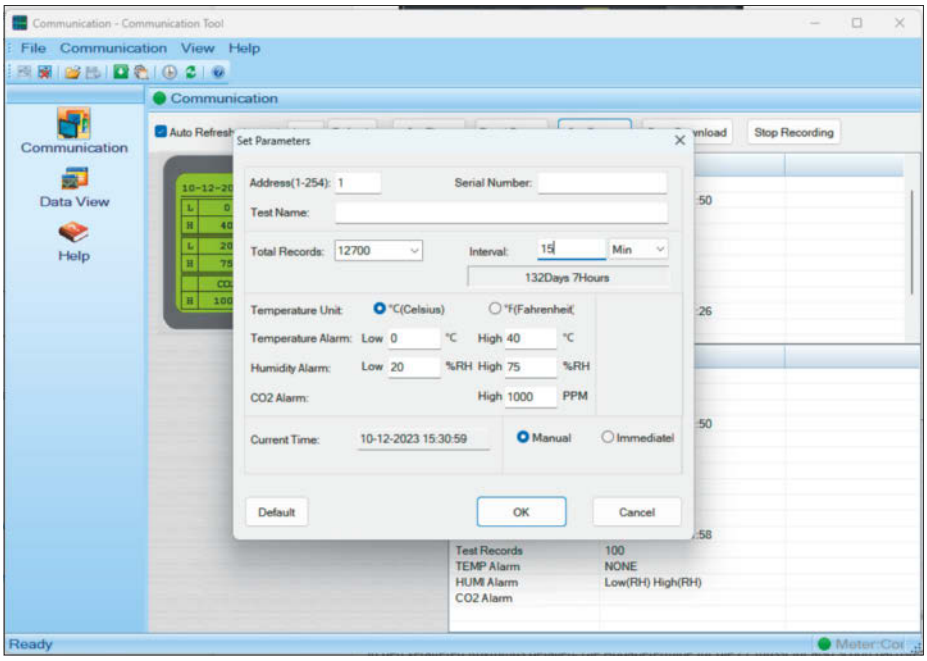
Genaue Messung

Die meisten der Geräte lassen sich kalibrieren. Das funktioniert, indem man sie an die frische Luft bringt, wo der CO_2-Gehalt bei 420 ppm liegt, und dann dort kalibriert, was je nach Modell zwischen 10 und 20 Minuten dauert. Viele der Sensoren gehen allerdings fälschlich (und unveränderlich) von 400 ppm aus, zeigen also nach der Kalibrierung rund 5 Prozent zu wenig an.

Problematisch ist die automatische Kalibrierung, die einige Geräte vornehmen. Dabei wird der niedrigste Wert einer längeren Messreihe, etwa aus 7 oder 30 Tagen, als Basiswert für 420 oder 400 ppm zugrunde gelegt. Steht das Gerät währenddessen dauerhaft in einem geschlossenen Raum mit höherer Konzentration, wird es nach der automatischen Kalibrierung zu niedrige Messwerte anzeigen.

Alle Geräte mit automatischer Kalibrierung bieten deshalb auch eine manuelle Kalibrierung an. Die ist fällig, wenn ein Gerät dauernd einen CO_2-Gehalt von 400 ppm oder weniger anzeigt. Bei den Geräten ohne Kalibrierungsmöglichkeit wird der Sensor durch Verschmutzung und Alterung tendenziell eher zu hohe Werte anzeigen als zu niedrige.

Für eine korrekte Messung müssen Temperatur und Luftfeuchtigkeit bekannt sein und zusätzlich idealerweise der Luftdruck, da der gemessene absolute CO_2-Gehalt mit fallendem Umgebungsdruck abnimmt, während der zu ermittelnde relative Anteil gleich bleibt. Der Aranet4 ermittelt den Luftdruck mit einem eigenen Sensor, was ihm dabei hilft, auch in Extremsituationen korrekte Werte anzuzeigen, also beispielsweise im Flugzeug oder im Zugspitzrestaurant, wo statt rund 1000



Das mitgelieferte Tool zur Datenauswertung für den Bresser CO_2 Luftqualitätsmonitor INV ist wenig benutzerfreundlich.

nur 700 bis 800 hPa Umgebungsdruck herrschen. Beim Airco2ntrol 5000 lässt sich immerhin manuell noch eine Höhe über dem Meeresspiegel eingeben, um den Messwert gegebenenfalls zu korrigieren. Allzu groß ist der Effekt nicht: In 1000 Metern Höhe beträgt die Abweichung des Luftdrucks gegenüber Meereshöhe gerade einmal 10 Prozent, Hoch- und Tiefdruckgebiete bewirken nur 3 Prozent Abweichung.

Fazit

Bei unserer Testmessung marschierten die Geräte erstaunlich gut im Gleichschritt und erfassten die steigende CO_2-Konzentration zuverlässig. Dabei taugen die Geräte nicht nur für zu Hause oder das Büro. Die batteriebetriebenen Geräte von Hama und SAF Tehnika sind so klein und handlich, dass man sie problemlos in der Jacken- oder Handtasche überallhin mitnehmen kann. Im Großraumbüro oder Konferenzräumen, im Restaurant, auf Veranstaltungen, im Zug oder im Flugzeug lässt sich die Luftqualität damit unauffällig überwachen. Das hilft bei der Entscheidung, wann ein guter Zeitpunkt zum Lüften – oder zum Gehen – ist oder ob es ratsam ist, eine Maske zu tragen.

Alle anderen Geräte leisten an einem festen Standort gute Dienste und weisen darauf hin, wenn die CO_2-Konzentration zu hoch klettert. Als nervig erwies sich allerdings in vielen Fällen die akustische Hinweisfunktion. Praktisch ist hingegen die Ampelanzeige, die sich in der einen oder anderen Form in allen Geräten findet, überall schon per Default mit praxisgerechten Grenzwerten hinterlegt ist und bei der Interpretation des Messwerts hilft. Ein Ausreißer war nicht dabei, die Geräte taten in unserem Praxistest verlässlich, was sie sollten.

(uma@ct.de) c't

Zusatzinformationen und Online-Rechner: ct.de/yt4g

CO_2-Messgeräte

Hersteller	TFA Dostmann	TFA Dostmann	TFA Dostmann	TFA Dostmann	SAF Tehnika	Bresser	Bresser	Bresser	Hama
Typenbezeichnung	Airco2ntrol 5000	Airco2ntrol Coach	Airco2ntrol Mini	Airco2ntrol Up Dual Beam	Aranet4	CO_2 Luftqualitäts-monitor INV	CO_2-Messgerät Smile XXL	CO_2 Smile	Safe CO_2-Luftmessgerät
Technische Daten									
CO_2-Messbereich	bis 5000 ppm	bis 9999 ppm	bis 3000 ppm	bis 5000 ppm	bis 9999 ppm	bis 9999 ppm	bis 9999 ppm	bis 5000 ppm	bis 5000 ppm
CO_2-Kalibrierung	manuell	–	–	manuell, automatisch	manuell, automatisch	manuell	–	manuell, automatisch	manuell, automatisch
Datenlog	✓ (1 Mio. Einträge, einstellbares Intervall)	–	–	–	✓	✓ (12.700 Einträge)	–	–	–
Schnittstelle zum Datentransfer	Micro-SD-Karte	–	–	–	Bluetooth	USB	–	–	–
Maße									
Gerät (B × H × T)	11,9 cm × 6,5 cm × 3,4 cm	10,4 cm × 5,4 cm × 3,2 cm	11,5 cm × 3,6 cm × 2,3 cm	7,7 cm × 14,2 cm × 9,6 cm	7,0 cm × 7,0 cm × 2,4 cm	10,8 cm × 10,8 cm × 3,8 cm	39,2 cm × 29,2 cm × 4,3 cm	10,9 cm × 12,2 cm × 3,4 cm	7,8 cm × 7,8 cm × 3,9 cm
Display	5,9 cm × 4,4 cm	6,8 cm × 3,9 cm	5,3 cm × 1,2 cm	5,0 cm × 8,7 cm	3,0 cm × 3,0 cm	7,0 cm × 7,0 cm	38,8 cm × 28,8 cm	8,0 cm × 9,7 cm	3,9 cm × 3,9 cm
Anzeige									
CO_2-Gehalt	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aktualisierungs-intervall CO_2	5 Sekunden	10 Sekunden	10 Sekunden	2 Sekunden	1, 2, 5, 10 Minuten	4 Sekunden	1 Sekunde	15 Sekunden	5 Sekunden
CO_2-Historie im Display	Minute, Stunde, Tag, Woche	24 Stunden	–	–	✓ (über App)	–	–	(Durchschnitt 15 Minuten, 8 Stunden)	–
Min/Max-Anzeige	✓	–	–	✓	✓ (über App)	–	–	✓	✓
Temperatur	✓	✓	✓	✓	✓	✓	✓	✓	✓
Luftfeuchtigkeit	✓	✓	–	✓	✓	✓	✓	✓	✓
Luftdruck	–	–	–	–	✓ (über App)	–	–	–	–
Uhrzeit	✓	✓	–	✓	–	– (nur intern)	–	–	–
Display-Art	LCD, unbeleuchtet (LED für CO_2-Ampel)	LCD, RGB-Hinter-grundbeleuchtung	LCD, unbeleuchtet	LED	E-Paper, unbe-leuchtet	LCD, Hintergrund-beleuchtung	LED	LCD, Hintergrund-beleuchtung	LED
CO_2-Warnungen									
Optisch	✓	✓	✓	✓	✓	–	–	✓	✓
Akustisch	✓	–	–	✓	✓	✓	✓	✓	✓
Alarmschwelle einstellbar	✓	✓	–	✓	✓	✓	✓	✓	✓
Bewertung (CO_2-Ampel)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stromversorgung									
Netzanschluss	Micro-USB	Micro-USB	Micro-USB	USB-C	– (optional externes Netzteil)	Micro-USB	Netzteil	Netzteil	Micro-USB
Akku/Batterie	–	–	–	Akku	2 × AA	Akku	–	–	Akku
Laufzeit netzunabhängig	–	–	–	22 Stunden	> 6 Monate	> 24 Stunden	–	–	5 Stunden
Preis									
Online-Handel, günstigster Preis	118 €	71 €	64 €	65 €	189 €	59 €	89 €	39 €	49 €

✓ vorhanden – nicht vorhanden

Neue Räumlichkeiten

Klangduell um den besten 3D-Sound fürs Heimkino

Ein AV-Receiver mit Dolby Atmos kann Ihr Wohnzimmer in ein bombastisches Heimkino verwandeln – wenn er den Klang der Lautsprecher richtig an den Raum anpasst. Denon und Yamaha verfolgen hier unterschiedliche Ansätze: Der eine bewirbt höhere Präzision mit Dirac Live, der andere Blockbuster-Sound durch KI-Training. Wir prüfen an zwei AV-Receivern, was hinter den Versprechen steckt.

Von Hartmut Gieselmann

Moderne Fernsehgeräte sind zwar schön flach und groß, aber der Ton lässt oft zu wünschen übrig. Dabei trägt ein guter Klang mindestens genauso viel zum Kinoerlebnis in den eigenen vier Wänden bei wie ein gutes Bild. Es genügt allerdings nicht, den Raum mit vielen Lautsprechern vollzustellen. Sie müssen auch genau aufeinander und auf die Örtlichkeit abgestimmt sein.

Alle Audio/Video-Receiver bieten daher spezielle Prozessoren und Algorithmen, um den Raumklang auf die jeweiligen Gegebenheiten anzupassen. Yamaha ist vollends von seiner Eigenentwicklung YPAO (Yamaha Parametric Acoustic Optimizer) überzeugt. Sie entzerrt laut Hersteller jeden Lautsprecher mit einem parametrischen Equalizer, ermittelt Abstände und Winkel und peppt den Ton mit abgestimmten „Klangfeldprogrammen“ auf, die unter anderem auch etwas Hall zumischen.

Viele andere Hersteller wie Arcam, Denon, Marantz, NAD, Onkyo oder Pioneer erlauben hingegen eine Einmessung per Dirac Live: Die Software glättet laut Hersteller nicht nur den Frequenzgang, sondern korrigiert auch das Timing, sodass Impulse synchron schwingen. Bei Denon und Marantz gibt es Dirac Live gegen Aufpreis, von Haus aus lassen sich die Modelle mit dem altbekannten System von Audyssey einmessen.

In diesem Test vergleichen wir YPAO, Audyssey und Dirac Live anhand der Receiver Yamaha RX-A6A und Denon AVC-X4800H. Beide unterstützen bis zu neun Kanäle für den Betrieb von fünf Lautsprechern auf Ohrhöhe und vier Deckenlautsprechern. Yamaha steuert außerdem zwei aktive Subwoofer an, Denon bis zu vier.

Das Denon-Modell ist zu einem Straßenpreis von rund 1400 Euro erhältlich. Hinzu kommen Kosten für die Dirac-Live-Lizenz (330 Euro) sowie ein Messmikrofon. Der Yamaha RX-A6A hat einen Straßenpreis von knapp 2300 Euro.

Raumeinmessung

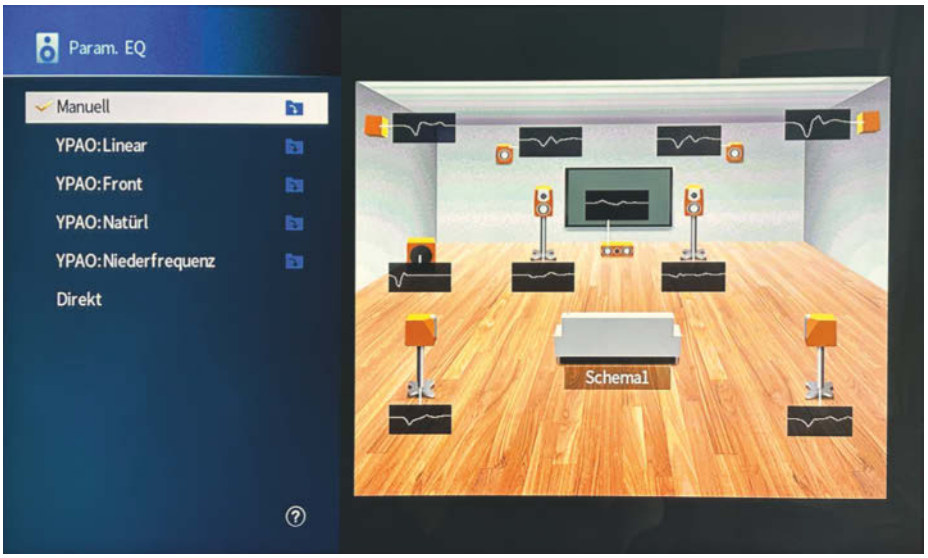
Der Hauptgrund, warum sich Nachbarn und Kinder von lauten Kinoabenden zu Hause gestört fühlen, sind dröhnende tiefe Frequenzen, die durch Wände und Decken wandern. Sie werden vor allem durch sogenannte Raummoden erzeugt. Das sind stehende Basswellen, die sich zwischen parallelen Wänden sowie Decke und Boden bilden. In den Ecken und an den Wänden des Raumes erzeugen sie einen deutlich höheren Schalldruck als an einem Hörplatz in der Mitte des Raumes. Mit einem Raummodenrechner, in den Sie die Abmessungen Ihres Raumes eingeben, können Sie die Frequenzen ermitteln (siehe ct.de/ytba).

In unserem Testwohnzimmer lagen zum Beispiel die beiden tiefsten Moden bei 35 und 47 Hertz, die mit dem Raumkorrekturprogramm schmalbandig um bis zu 18 Dezibel (!) abgesenkt werden mussten. Danach ist auch in einer hellhörigen Altbauwohnung der Betrieb einer Surround-Anlage mit Subwoofer problemlos möglich.

Ein Raum beeinflusst aber auch die höheren Frequenzen. Er kann an sich linear klingende Lautsprecher stark verbiegen, sodass der Klang aufgeblasen wirkt und an Transparenz verliert. AV-Receiver bieten zwar die Möglichkeit, einen größeren Bereich für mehrere Personen einzumessen. Dabei gehen sie jedoch mehr oder minder große Kompromisse ein, eine ideale Abstimmung ist nur für genau einen Abhörplatz möglich.

c't kompakt

- Für den Klang eines Surround-Systems ist die Einmessung der Lautsprecher entscheidend.
- Denon verbessert die räumliche Abbildung mit der Einmess-Software Dirac Live.
- Yamaha vergrößert auch die Raumwirkung von Dolby-Atmos-Signalen mit DSP-Algorithmen.



Yamahas YPAO-Einmessung erlaubt die manuelle Anpassung jeder Ausgleichskurve mit sieben parametrischen Filtern (vier Filter beim Subwoofer).

Yamahas YPAO

Yamahas YPAO sendet kurze Frequenz-Sweeps zu jedem Lautsprecher und stellt dann den Pegel und die Filter ein, um die Lautsprecher auszugleichen. Um eventuelle Überkorrekturen abzuschwächen, sollten Sie nach der ersten Messung am Stammplatz mithilfe einer mitgelieferten Schablone drei weitere Messungen durchführen. Details erläutert Yamaha in einem ausführlichen Video (siehe ct.de/ytba).

Als Besonderheit misst YPAO neben der Entfernung auch die Winkel und die Höhe der Lautsprecher zum Stammhörplatz. So erkennt der Receiver, welche Schallanteile direkt vom Lautsprecher kommen und welche der Raum reflektiert. Dies bezieht er in seine Kompensationsberechnungen und Klangfeldanpassung mit ein, die unter anderem verschiedene Hallprogramme steuert. Weichen die Positionen der aufgestellten Lautsprecher vom Ideal ab, gleicht Yamaha dies aus und simuliert (in Grenzen) sogar fehlende Decken- oder seitliche Surround-Lautsprecher.

YPAO stellt pro Lautsprecher sieben (Subwoofer: vier) parametrische Filter ein. Die Einstellung kann man auf einen manuellen Speicherplatz kopieren und dort für jedes Filter die Frequenz, die Flankensteilheit (Q) und die Stärke in Schritten von 0,5 Dezibel manuell ändern. Das geht nicht nur per Fernbedienung am Fernseher, sondern auch über ein Webinterface am Computer. Dazu gibt man im Browser die IP-Adresse des Receivers xxx.xxx.xxx.xxx/Setup ein.

Die manuellen Eingriffsmöglichkeiten bieten Profis eine hohe Flexibilität. In unserem Testwohnzimmer tippte YPOA allerdings bei den unteren Raummoden ein paar Halbtöne daneben, sodass wir die Subwoofer-Einstellungen korrigieren mussten. Ebenso wechselten wir die Polarität des Subwoofers und senkten den Pegel des etwas zu lauten Centers, damit er besser zum Rest passte.

Audyssey MultEQ-XT32

Der Denon-Receiver hat Audyssey MultEQ-XT32 bereits integriert. Das mitgelieferte Mikrofon stellt man auf einem Papptürmchen rund um den Hörplatz auf. Im Unterschied zu YPAO setzt Audyssey auf 2048 schmale Filter, die selbst kleinste Abweichungen im Frequenzgang nivellieren. Man kann nur die Zielkurve der Klanganpassung einstellen, einzelne Filter wie bei Yamaha lassen sich nicht verändern.

Audyssey senkt mit seiner Referenzkurve etwa den 2-kHz-Bereich ab und dämpft die Höhen etwas, was dem Höreindruck in einem großen Kinosaal näher kommen soll. Yamaha nennt sein Pendant „YPAO: Natürlich“. Hier entscheidet der jeweilige Film sowie der Geschmack, denn viele Abmischungen fürs Heimkino sind gegenüber den Tonspuren fürs Kino bereits in den Höhen leicht gedämpft.

Wer die Kurven anpassen will, sollte sich die „Audyssey MultEQ Editor App“ (Android, iOS) für 23 Euro kaufen. Mit ihr ist es möglich, die verschiedenen Messungen zu verwalten und die Zielkurven auf

Yamaha RX-A6A

Den AV-Verstärker mit einem Kampfgewicht von über 20 Kilogramm sollte niemand alleine tragen, der Rücken hat. Seine Lüftung ist aktiv, aber allenfalls wahrzunehmen, wenn man ein Ohr direkt an die Lüftungsschlitze hält. Diese sollten auf der Oberseite frei bleiben und weitere Geräte nur mit Abstandshaltern darauf platziert werden. Die zusätzlichen XLR-Buchsen auf der Rückseite ermöglichen lange, störungsfreie Verbindungen. Leider stehen diese nur für die Hauptlautsprecher auf der rechten und linken Seite zur Verfügung, nicht aber für die beiden Subwoofer-Anschlüsse.

Das Display auf der spartanischen Front zeigt von Haus aus leider keine Informationen über das Eingangsdatenformat an – dafür muss man per Fernbedienung auf ein Bildschirmmenü zugreifen. Die komplexe Fernbedienung leuchtet bei Bewegung. Über acht Direkttasten lassen sich beliebige Einstellungen speichern und abrufen.

- ⬆ großer Kinosound dank Surround-AI
- ⬆ tolle Anpassungen für niedrige Lautstärken
- ⬇ Einmessung verlangt manuelle Nacharbeit

Preis (Straße): circa 2300 Euro

Denon AVC-X4800H

Der AVC-X4800H ist mit rund 13 Kilogramm durchaus alleine tragbar. Aufgrund der passiven Kühlung sollten auch hier die oberen Lüftungsschlitze frei bleiben. Das sehr leise Surren des Trafos lag etwa auf dem Niveau des Yamaha-Receivers. XLR-Anschlüsse sind hier nicht vorhanden. Am Vorverstärker kann man aber – wie beim Yamaha – zu den neun Kanälen noch zwei weitere Kanäle für Aktivlautsprecher abgreifen. Das Handbuch gibt detaillierte Instruktionen, wie sich bis zu vier Subwoofer und sogar Sesselvibratoren betreiben lassen. Ausprobiert haben wir das nicht.

Das Display zeigt hilfreiche Informationen zum Eingangssignal. Die Fernbedienung ist unbeleuchtet. Die Quick-Select-Tasten sind leider nicht so komfortabel wie bei Yamaha, sodass man für einige Dynamikeinstellungen weiterhin ins Menü eintauchen muss.

- ⬆ präzise Einmessung per Dirac Live
- ⬆ extrem gute 3D-Ortung mit Dirac Live
- ⬇ kein zusätzliches Upmixing bei Dolby Atmos

Preis (Straße): circa 1400 Euro, plus Dirac Live (330 Euro), plus Messmikrofon

dem Touchscreen zu verändern. Alternativ bietet Audyssey für Windows die Einmesssoftware MultEQ-X für 200 US-Dollar an, die wir uns im Rahmen dieses Vergleichs aber nicht angeschaut haben.

Von Haus aus ignorierte Audyssey unter anderem die Raummoden unseres Wohnzimmers, sodass wir die Zielkurve manuell unter 48 Hertz absenken mussten, um die wummernden Bässe zu dämpfen. Zwar bietet Audyssey einen speziellen LFC-Modus zur Basskontrolle an, doch dieser senkt den Subwoofer breitbandig ab, wodurch viel Dynamik verloren geht. Auch die Dynamik- und EQ-Anpassungen von Audyssey sind mit Vorsicht zu genießen, da sie gerade bei der Musikwiedergabe zu einer unnatürlichen Kompression führen.

Dirac Live

Für den Denon AVC-X4800H kann man für 330 Euro eine Dirac-Live-Lizenz erwerben, die die Audyssey-Einmessung und Klanganpassung ersetzt. Die Lizenz gilt für ein Gerät. Bei einem Gerätewechsel des gleichen Modells kann man beim Support eine Umtragung erbitten. Wechsel zu anderen Modellen sind nicht möglich. Dirac bietet zwar eine günstigere Version für circa 240 Euro an, diese gleicht aber nur Frequenzen bis 500 Hertz aus und lässt insbesondere den oberen Mitteltonbereich außen vor. Letzterer ist unter anderem wichtig für eine klare Sprachverständlichkeit. Hier sollte man nicht am falschen Ende sparen.

Die Dirac-Software läuft nicht auf dem Receiver selbst, sondern am Rechner unter Windows oder macOS. Zur Einmessung benötigt man ein Messmikrofon wie das MiniDSP Umik-1 (120 Euro mit USB-Anschluss) samt geeignetem Stativ. Falls vorhanden (Support des Herstellers fragen), lädt die Dirac-Software auch Kalibrierungsdaten für das Messmikrofon. Die Messung erfolgt menügesteuert über neun Positionen. Anschließend sendet die Software die Entzerrungsfilter per LAN oder WLAN an den Denon-Receiver.

Dirac berechnet eine optimierte Entzerrungskurve automatisch, alternative Voreinstellungen mit anderen Klangcharakteristiken gibt es nicht. Die Zielkurven der Lautsprecher lassen sich aber auch manuell am Computer einstellen und auf drei Speicherplätzen im Empfänger ablegen. Zwischen diesen Speicherplätzen

WWW.OOP-KONFERENZ.DE

KONFERENZ FÜR SOFTWARE ARCHITEKTUR

ICM MÜNCHEN

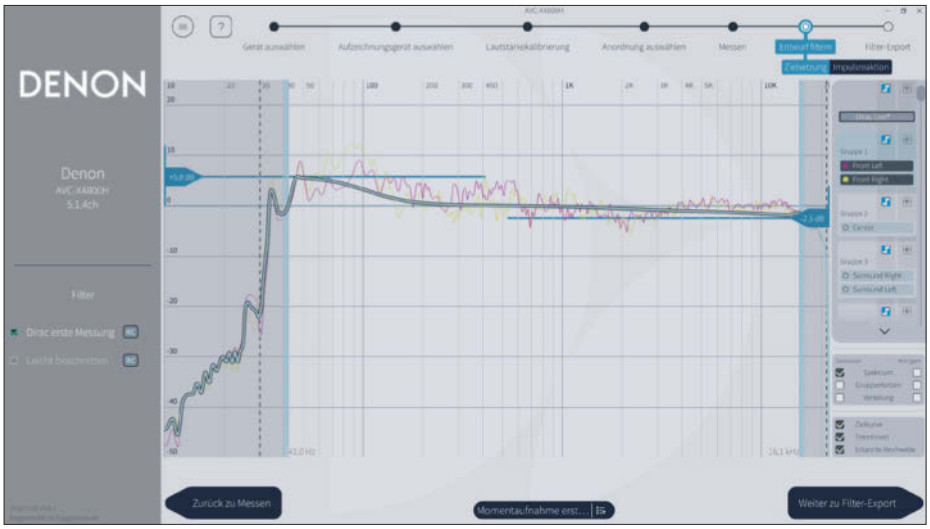
oop
software meets business

29. JANUAR – 02. FEBRUAR 2024

- ✔ Der bewährte Software-Szenetreff
- ✔ Über 170 Vorträge, rund 200 Speaker – mehr als 30% sind Frauen
- ✔ Brandaktuelle und praxisnahe Vorträge

Frühbucher-Rabatt bis zum 15.12.2023!

MICROSERVICES-ARCHITEKTUREN • CLOUD • DOMAIN-DRIVEN DESIGN • API-ENTWICKLUNG • CONTAINERISIERUNG • PLATFORM ENGINEERING • DEV(SEC)OPS • GENERATIVE AI & KI • SOFTWAREQUALITÄTSSICHERUNG • AGILITÄT • DIGITALISIERUNG • EDA



Dirac Live schlug in unserer Testumgebung eine Bassanhebung der vorderen Hauptlautsprecher vor. Ohne diese wirkte der Bass tatsächlich etwas dünn.

können Sie jederzeit im Onscreen-Menü wechseln. Für niedrigere Lautstärken könnte man etwa die Bässe und Höhen leicht anheben, um die geringere Empfindlichkeit des Gehörs in diesen Frequenzbereichen auszugleichen.

Wie klingt es?

Um die Qualität einer Einmessung zu überprüfen, hören Sie jeden Lautsprecher einzeln mit rosa Rauschen an Ihrem Stammplatz ab. Die Receiver bieten diese Möglichkeit im Setup an. Idealerweise sollte jeder Lautsprecher gleich laut klingen und auch die gleiche Klangfarbe im Rauschen haben.

Im Test gelang dies dem Yamaha nur ungefähr: Bei jedem Lautsprecher klang das Rauschen ein wenig anders. Mit Audyssey war das Automatik-Ergebnis etwas besser, allerdings patzte das System im Bassbereich, wo es die Raummoden überhaupt nicht berücksichtigte. Dadurch fehlte es dem Bass an Definition. Manuell konnten wir YPAO und Audyssey schließlich auf ein ähnlich gutes Niveau anpassen.

Die mit Abstand beste Einmessung gelang jedoch mit Dirac Live. Obwohl die Deckenlautsprecher von einem anderen Hersteller stammen, klangen alle neun Lautsprecher beim Test mit rosa Rauschen verblüffend ähnlich. Ebenso war der Subwoofer hervorragend auf die Raummoden abgestimmt, sodass selbst in den Ecken des Raumes kein Wummern zu hören war. Von dieser präzisen Einmessung profitierte insbesondere die Musikwiedergabe. Der Frequenzgang war homogen und der Bass punktgenau.

Testaufbau

Getestet haben wir beide Geräte in einem etwa 20 Quadratmeter großen Altbau-Wohnzimmer mit einer 5.1.4-Lautsprecheranlage: fünf Boxen der Nubert Nuboxx-Serie (Stückpreis etwa 300 Euro), an der Decke vier JBL Control 1 Pro (Stückpreis 75 Euro), Subwoofer Adam Sub 8 (700 Euro, Anschluss über DI-Symmetrierbox). Die Messungen für Dirac Live nahmen wir mit einem Beyerdynamic MM1 (220 Euro) vor.

Als Zuspieler kamen ein Apple TV 4K, eine Sony PlayStation 5 sowie ein UHD-Player von Panasonic zum Einsatz. Wir testeten unter anderem mit Dolby-Atmos-Filmen wie „Blade Runner“, „Apocalypse Now“, „Im Westen nichts Neues“ und „Mission Impossible: Dead Reckoning“ sowie mit den Atmos-Alben „Kraftwerk 3-D“, „The Dark Side of the Moon“, „Ella Fitzgerald sings the Irvin Berlin Song Book“ und „Jean-Michel Jarre – Oxymore“ von Apple Music. Die Videospiele „Cyberpunk 2077“, „Spider-Man 2“ und „Alan Wake 2“ rundeten den Test ab. Letztere unterstützen auf der PS5 3D-Sound in Dolby Atmos.

Vor allem verbesserte sich durch die Timing-Anpassungen die räumliche Ortung: Frontlautsprecher und Center verschmolzen zu einer Einheit und es entstanden keine „Löcher“, wenn ein Klang um den Zuhörer kreiste. Die wabernden Elektro-Klänge von Kraftwerks „Radioland“ waren ebenso gut und stabil zu orten wie die Stimme von Ella Fitzgerald, die – wie auf einer Live-Bühne – von ihrem Orchester umgeben im Raum zu stehen schien. Als in Apocalypse Now die Hubschrauber über uns hinwegflogen, konnten wir die Position der Rotoren besser lokalisieren als mit dem Audyssey-Einmesssystem oder dem Yamaha-Receiver. Kurz: Dirac Live verbesserte den 3D-Klang unserer Mittelklasse-Lautsprecher im Vergleich zu Audyssey und YPAO enorm, wie wir es vorher nicht erwartet hatten.

Aufgebrezeltes Atmos

An dieser Stelle wäre der Test beendet, hätte Yamaha nicht noch ein paar Trümpfe in der Hinterhand. Denn nicht jedes Album und nicht jeder Film klingt wie eine Referenzabmischung. Vor allem Spiele haben oft mit einer schlechten Lautstärkeanpassung der Sprecher zu kämpfen und nutzen nur selten Deckenlautsprecher.

Alan Wake 2 machte nach dem 1.08er-Update mit seiner filmreifen Klangathmosphäre und den gut abgestimmten Sprechern eine deutlich bessere Figur als Spider-Man 2 und Cyberpunk 2077. Der Denon-Receiver bildet die Atmos-Ausgabe dieser Spiele auf der PS5 nüchtern ab. Denn im Unterschied zu Yamaha kann Denon Dolby-Atmos-Signale nicht mit zusätzlichen Upmixern aufpeppen. Zwar bietet Denon ebenso wie Yamaha den Upmixer „AuroMatic“ von Auro, der den Raumeindruck vergrößert. Allerdings schaltet Denon diesen nur bei Signalen mit bis zu 7.1 Kanälen hinzu.

Yamaha kann hingegen auch DTS:X- und Dolby-Atmos-Signale mit der AuroMatic aufbessern. Alternativ schaltet man Yamahas eigenen Upmixer „Surround-AI“ ein. Der wurde speziell mit Filmen trainiert und erkennt Unterschiede zwischen Dialog- und Actionszenen. In Dialogszenen klingen die Sprecher voller und räumlicher. Surround AI kann ihre Position gegenüber dem Center auf Wunsch sogar leicht anheben. Dadurch scheinen die Stimmen mehr aus dem Bildschirm zu kommen, was erstaunlich gut funktioniert.

Surround-AI überzeugte im Test vor allem bei Filmen, sodass der Klang mehr

Kinoqualität bekam, ohne dabei zu dick aufzutragen. Bei Musik und Videospielen mischte Surround AI allerdings manchmal etwas zu viel Hall hinzu. In diesen Fällen bevorzugten wir AuroMatic, um die Räumlichkeit zu vergrößern.

Lautstärkeanpassung

Darüber hinaus punktet Yamaha mit seiner automatischen Klanganpassung (YPAO Volume), wenn man die Lautstärke herunterregelt. Denn das menschliche Gehör reagiert bei niedrigen Lautstärken weniger empfindlich auf tiefe und hohe Frequenzen, wodurch der Klang eine subjektive Mittenbetonung bekommt. Yamaha passt nicht nur den Frequenzgang an, sondern reduziert auch die Dynamik in Abhängigkeit von der Lautstärke.

Spätestens mit der dreistufigen Dialoganhebung muss man nicht mehr zur Fernbedienung greifen, um die Lautstärke zwischen Action- und Dialogsequenzen zu korrigieren. Die Anpassungen klingen bei Yamaha überaus natürlich, ohne dass uns wie bei der Audyssey-Anpassung des Denon-Receivers Kompressionsschwankungen aufgefallen wären.

Dirac Live nimmt leider keine Klanganpassungen in Abhängigkeit von der Lautstärke vor. Man kann beim Denon-Receiver im Menü Audio/Surround-Parameter zwar ein dreistufiges Loudness-Management aktivieren, das sich im Test jedoch kaum auf die Wiedergabe auswirkte. Bei Bedarf schaltet man mit der Optionstaste der Fernbedienung noch einen Dialog Enhancer hinzu. Beide Optionen lassen sich leider nicht auf einer Quick-Select-Taste zum schnellen Wechsel speichern.

Strom und HDMI

In der Tabelle finden Sie unsere Messwerte zur Leistungsaufnahme der beiden Receiver. Denon und Yamaha können im Standby einen HDMI-Kanal durchleiten. Die Leitungsaufnahme stieg dann aber um ein bis 1,5 Watt an. Ebenso viel kam nochmal hinzu, wenn die Receiver per LAN aufwachen sollten. Sparfüchse sollten HDMI- und Netzwerkfunktionen im Setup deaktivieren. Beim Denon-Receiver muss man dazu die HDMI-CEC-Steuerung abschalten, sodass er nicht automatisch aufwacht, sobald Sie einen Zuspieler einschalten.

Im Betrieb sparten wir bei beiden Modellen im Eco-Modus etwa 20 bis 40 Watt, ohne dass die Klangqualität litt. Wer wie der Bundesdurchschnitt etwa 200 Minuten pro Tag fernsieht, zahlt im niedrigsten Standby- und Eco-Modus für den Yamaha RX-A6A aufs Jahr gerechnet etwa 55 Euro Stromkosten, beim Denon AVC-X4800H sind es rund 34 Euro.

Je nach angeschlossenem HDMI-Equipment dauerte es manchmal einige Sekunden, bis die Receiver ihre Signale synchronisiert hatten – das hing vom angeschlossenen Equipment ab. Um Probleme zu verringern, sollten Sie für HDMI 2.1 möglichst kurze Kabel mit hoher Datenrate (48 GBit/s bei 8K mit 60 Hertz) verwenden.

Fazit

Ideal wäre ein AV-Receiver mit der Dirac-Einmessung von Denon und den DSP-Klangverbesserungen von Yamaha. Da es diesen aber nicht gibt, muss man sich entscheiden: Wer eine möglichst naturgetreue Wiedergabe sucht – oder gar professionell 3D-Mischungen beurteilen muss –, kommt an Dirac Live nicht vorbei. Gerade bei der Musikwiedergabe liefert der Denon-Receiver eine extrem präzise und stabile Räumlichkeit, die wir mit dem Yamaha-Modell nicht ganz erreichen konnten. Dank Dirac Live ist Denon in der Lage, auch heterogene Lautsprecherkonfigurationen in akustisch schwierigen Räumen klanglich besser zu verschweißen.

Das Yamaha-Modell brezelt dafür den Ton von Filmen und Spielen stärker auf, sodass Sie sich zu Hause wie im Kino fühlen. Der gleichzeitige Einsatz von Atmos und AuroMatic beziehungsweise Surround-AI holt aus jeder Produktion das Maximum an Raumfülle und Dialogverständlichkeit heraus. Allerdings erfordert die Einmessung bei Yamaha mehr Nacharbeit als bei Denon.

Ein Nachteil aller AV-Receiver im Alltag ist ihre komplexe Bedienung: Ohne gründliches Handbuchstudium sind Sie bei beiden Herstellern aufgeschmissen. Der Denon-Receiver lässt sich leichter einmessen, das Yamaha-Modell anschließend etwas bequemer bedienen, weil sich alle Dynamik- und Upmixing-Funktionen auf Direktwahltasten legen lassen.

Unterm Strich sind beide Modelle empfehlenswert, da sie gegenüber den AV-Receivern aus dem vorherigen Test in c't 26/2017, Seite 134, klanglich deutlich zugelegt haben. *(hag@ct.de)* c't

Raummoden-Rechner und Setup-Video:
ct.de/ytba

AV-Receiver für 3D-Sound

Name	AVC-X4800H	RX-A6A
Hersteller, URL	Denon, denon.com	Yamaha, de.yamaha.com
HDMI In / Out	7 / 3 (HDMI 2.1)	7 / 3 (HDMI 2.1)
Eingänge	6 Line (Cinch), Phono (MM), SPDIF (2 optisch, 2 koaxial)	6 Line (Cinch), Phono (MM), SPDIF (3 optisch, 2 koaxial), 2 XLR
Ausgänge	11.4 Vorverstärkerausgänge (Cinch), Kopfhörer	11.2 Vorverstärkerausgänge (Cinch), 2 XLR, Kopfhörer
Lautsprecher-Setups	bis 5.4.4 (mit zusätzlichen Verstärkern bis 7.4.4)	bis 5.2.4 (mit zusätzlichen Verstärkern bis 7.2.4)
Ethernet / WLAN / Bluetooth / Webinterface	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
3D-Formate	Auro-3D, Dolby Atmos, DTS:X IMAX Enhanced, Sony 360 RA	Auro-3D, Dolby Atmos, DTS:X
Upmixing	AuroMatic, DTS Neural:X, DTS Virtual:X, Dolby Surround Upmixer, Dolby Virtualizer	AuroMatic, Surround-AI, DTS Neural:X, Dolby Surround Upmixer, Dolby Virtualizer
Einmessmethoden	Audyssey MultEQ-XT32, Dirac Live (optional)	YPAO
Leistungsaufnahme		
Standby (HDMI, Netz ein / aus)	2,9 Watt / < 0,2 Watt	2,8 Watt / < 0,3 Watt
Leerlauf (Eco ein / aus)	43 Watt / 65 Watt	65 Watt / 87 Watt
Wiedergabe (Eco ein /aus)	50 bis 60 Watt / 80 bis 100 Watt	80 bis 100 Watt / 120 bis 140 Watt
Stromkosten[1] (Eco-Modus)	circa 34 Euro/Jahr	circa 55 Euro/Jahr
Bewertung		
Klang Musik / Filme	⊕⊕[2] / ⊕⊕[2]	⊕ / ⊕⊕
Einmessung	⊕⊕[2]	⊕
Einstellmöglichkeiten	⊕	⊕⊕
Ton-Upmixing	⊕	⊕⊕
Lautstärkeanpassung	⊕	⊕⊕
Preis (Straße)	circa 1400 €, Dirac Live 330 € plus Messmikrofon	circa 2300 €

[1] 200 Minuten Betrieb pro Tag, Standby ohne Netzeinschaltung und HDMI-Durchleitung, Eco-Modus, 50 Cent/kWh
[2] Wertung für Dirac Live, Audyssey Abwertung um eine Note
✓ vorhanden – nicht vorhanden ⊕⊕ sehr gut ⊕ gut ○ befriedigend ⊖ schlecht ⊖⊖ sehr schlecht

Aufforderung zum Gruppentanz

Smart-Home-Standard Matter: Marktübersicht und erste praktische Schritte

Mit dem herstellerübergreifenden Smart-Home-Standard Matter geht es voran: Unterstützer wie Apple, Google, Amazon, Samsung, LG und Tuya machen ihre Apps und Geräte fit dafür. Wir zeigen, welche Komponenten man bereits bekommt und wie man sie unter dem neuen Standard einrichtet.

Von Ingo Fischer

Die Idee hinter Matter ist nichts weniger als eine Revolution im Smart Home: Geräte verschiedener Hersteller sollen nahtlos und gut gesichert miteinander interagieren – und zwar auch in Gruppen lokal und direkt miteinander verknüpft, ganz ohne zentralen Hub. Und damit nicht genug: Ein Gerät lässt sich auch parallel in mehreren Ökosystemen – etwa von Amazon, Apple oder Google – einbinden. Das klingt zu schön, um wahr zu sein? Beachtet man ein paar Rahmenbedingungen, funktioniert das tatsächlich bereits jetzt recht gut.

Einen Wermutstropfen gibt es aktuell jedoch noch: Matter-Kompatibilität bei neuen Smart-Home-Geräten ist leider auch gut ein Jahr nach dem Start von Matter ebenso wie Firmware-Updates für existierende Geräte noch nicht die Regel. Diese Situation dürfte sich allerdings in den kommenden Wochen und Monaten ändern [1].

Jetzt schon einsteigen?

Den besten Überblick, welche Matter-Geräte hierzulande bereits erhältlich sind, gibt momentan die Seite Matter-Smarthome.de (siehe ct.de/yec8). Dazu zählen etwa Steckdosen von Meross sowie Lampen und LED-Strips von Nanoleaf, die jeweils ab Werk über Matter kommunizieren. Aber auch einige Bestandsgeräte lassen sich per Firmware-Update fit für den neuen Smart-Home-Standard manchen – darunter Steckdosen, Bewegungsmelder und Kontaktsensoren von Eve sowie Lampen von WiZ.

Mit dem Matter-Update für die Hue-Bridge holt man sogar alle darüber angebundenen Hue-Geräte auf einen Schlag ins Matter-Universum. Und schließlich löst sich Eve mit dem Update für seine

Steckdosen und Sensoren aus der HomeKit-Exklusivität: Mit einem Hub, der den Funkstandard Thread unterstützt (dazu gleich mehr), lassen sich die Komponenten des Herstellers nun auch in anderen Ökosystemen nutzen.

Erste Versuche mit den verfügbaren Geräten überzeugen – nicht zuletzt, weil die Smart-Home-Ökosysteme von Apple, Google, Amazon und Samsung alle auf dem Markt aktuell verfügbaren Komponenten bereits unterstützen. So kann man auch nachträglich noch entscheiden, welche Ökosysteme man auf Dauer nutzen will. Lediglich bei den Plattformen von Tuya und LG gibt es noch Lücken bei der Geräteunterstützung, auch diese Hersteller haben aber bereits begonnen, diese zu schließen.

Zusammenfassend lässt sich sagen, dass Matter für die Gerätehersteller interessant ist, weil sie mit einer Implementierung alle möglichen Ökosysteme auf einmal unterstützen können. Auf Kundenseite machen wiederum gerade Smart-Home-Einsteiger, die sich noch nicht sicher sind, was sie am Ende genau tun wollen, mit Matter-kompatiblen Geräten nichts verkehrt. Fortgeschrittene Anwender freuen sich wiederum über das „Multi-Admin-Feature“, das es ermöglicht, ein Gerät mit mehreren Ökosystemen zu verknüpfen, um sie ohne Umwege beispielsweise gleichzeitig über Amazons Alexa und Apples Siri steuern zu können.

Apps und Hubs

Für die Nutzung von Matter benötigen alle Systeme, außer dem von Tuya, zwingend einen Hub. Dieser kommuniziert lokal mit den Matter-Geräten und erlaubt in vielen Fällen, dass sich zusätzlich auch Nicht-Matter-Geräte in Routinen oder Szenen übergreifend steuern lassen. Oft stellt der Hub auch eine Verbindung zur Cloud seines Herstellers her, sodass alle angebundenen Geräte von unterwegs steuerbar sind. Bei Apple und Samsung SmartThings lässt sich diese Cloudfunktion deaktivieren. Die Matter-Geräte kommunizieren untereinander auf jeden Fall vollständig auf lokaler Ebene.

Matter setzt auf etablierte Kommunikationstechniken wie Ethernet und WLAN, aber auch auf den noch recht neuen Thread-Standard. Thread ist ein IP-basiertes, drahtloses, energiesparendes Funkprotokoll, das ein Mesh-Netzwerk aufbaut. Bei einem solchen Mesh-Netzwerk leiten mehrere Geräte die Daten weiter, wodurch idealerweise ein ausfallsicheres Netzwerk entsteht. Um Thread nutzen zu können, benötigt man einen sogenannten Border-Router, der die Brücke zum IP-Netzwerk schlägt.

Nicht alle Matter-kompatiblen Hubs bringen diese Funktion gleich mit, sodass man hier sorgfältig wählen sollte, um sich keine Möglichkeiten zu verbauen. Wir haben in der Tabelle „Matter-Hubs“ unten auf dieser Seite daher nicht nur alle aktuell verfügbaren Matter-kompatiblen Hubs aufgelistet, sondern unterscheiden auch zwischen Modellen mit und ohne Thread-Unterstützung.

Kommunikation

Apple Home, Google Home, Amazon Alexa, Samsung Smart Things und Tuya Smart Life bieten zu ihren Ökosystemen eigene Apps an, über die sich neue Geräte verknüpfen lassen. Bei Apple funktioniert Matter grundsätzlich ab iOS 16.1, wirklich stabil läuft es nach unserer Erfahrung allerdings erst ab iOS 16.5. Bei Google reichen Android 8.1 und die aktuelle Google-Home-App. Die Einrichtung eines Matter-Geräts läuft gewöhnlich über einen QR-Code, worauf wir später genauer eingehen.

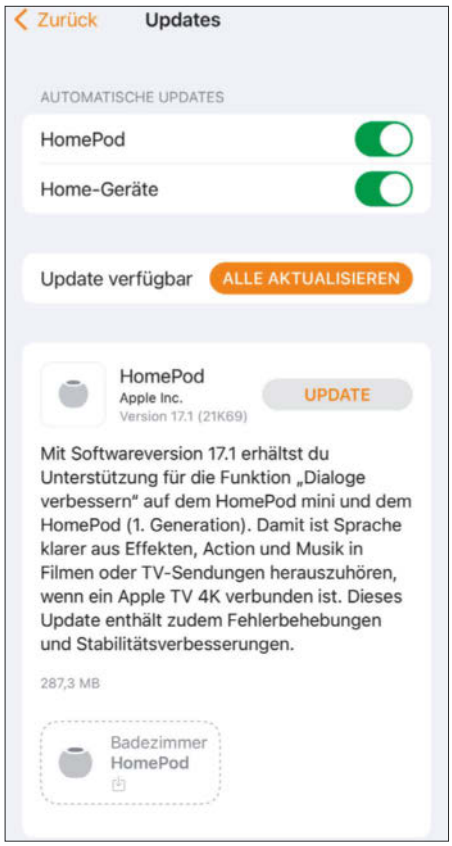
Geräte ohne Ethernet-Unterstützung nutzen bei der initialen Verknüpfung über die Smartphone-Apps gewöhnlich Bluetooth Low Energy (LE). Die Matter-Geräte erfahren darüber die nötigen Zugangsdaten zum heimischen WLAN oder dem Thread-Netzwerk.

Im Thread-Netzwerk erhält jedes Gerät vom Border-Router eine eindeutige IPv6-Adresse und ist danach darüber im lokalen Netz ansprechbar. So können alle Matter-Geräte direkt lokal miteinander kommunizieren – und zwar unabhängig davon, ob sie per Ethernet, WLAN oder Thread verbunden sind. Idealerweise sollte man dennoch darauf achten, alle Thread-fähigen Geräte zunächst im gleichen Thread-fähigen Ökosystem anzumelden, damit sie im gleichen Thread-Netzwerk funken – damit reagieren sie dank direkter Verknüpfung teilweise schneller als mit einem Umweg über den Hub.

Matter-Hubs

Anbieter	ohne Thread-Unterstützung	mit Thread-Unterstützung
Amazon	Echo Dot mit und ohne Uhr (ab 3. Gen), Echo Studio, Echo Show 5 und 8 (ab 2. Gen), Echo Show 10 (3. Gen), Echo Input, Echo Flex, Echo Plus (v2)	Echo (4. Gen)
Apple	Home Pod (1st Gen), Apple TV HD (4. Gen), Apple TV 4K Wi-Fi (2022)	Home Pod (2. Gen), Home Pod mini, Apple TV 4K WiFi+Ethernet (2022), Apple TV 4K (2021)
Google	Nest Audio, Nest Mini, Nest Hub (1. Gen), Google Home	Nest Hub (2. Gen), Nest Hub Max, Nest WiFi Pro (Wi-Fi 6E)
Samsung	Samsung SmartThings Hub v2, Samsung Family Hub Fridge (2022), Samsung Smart Monitore (2022), Samsung Smart TVs (2022)	Aeotec SmartThings Smart Home Hub, Samsung SmartThings Station, Samsung SmartThings Hub v3

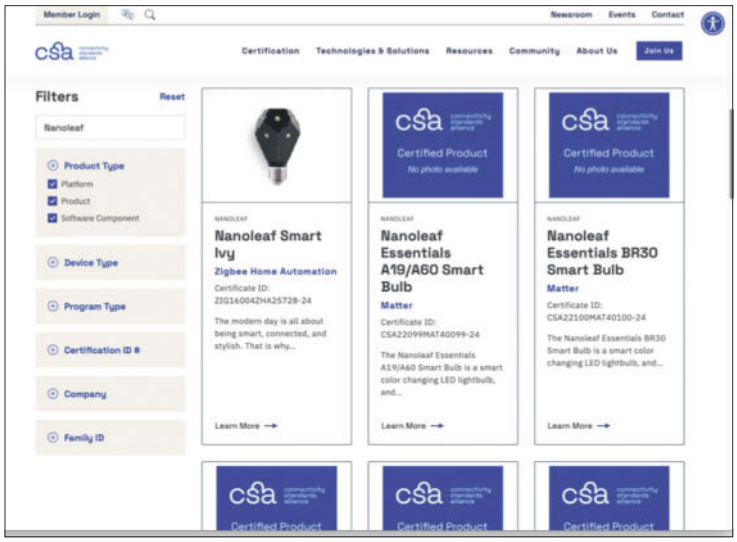
Alle Angaben laut Hersteller



Updates werden bei vielen Hubs automatisch eingespielt; dennoch sollte man ab und an prüfen, ob die Firmware wirklich aktuell ist.

IPv6 und UDP

IPv6 wird im Heimnetzwerk bisher oft noch als Profi-Spielzeug behandelt, weshalb es bei vielen Routern standardmäßig nicht aktiviert ist. Für die Nutzung von Matter empfiehlt sich ein lokales Netzwerk mit IPv6 allerdings durchaus. Zwar funktioniert es theoretisch auch mit IPv4 und MAC-basiertem Routing, das in WLAN-Routern standardmäßig implementiert ist, allerdings müssen dann wirklich alle Komponenten perfekt zusammenspielen. Bezüglich Google Home gibt es bereits Berichte über Probleme, nach denen sich ohne IPv6 keine Geräte verknüpfen be-



Ist man sich nicht sicher, ob ein Gerät Matter-zertifiziert ist, kann man dies über die Seite der Connectivity Standards Alliance (siehe ct.de/yec8) prüfen.

ziehungsweise nicht steuern lassen. Amazon gehört hingegen zu den Anbietern, die sich aktuell noch mit IPv4 zufriedengeben. Da IPv4 im Matter-Standard nur optional ist, sollte man sich besser nicht darauf verlassen, dass darüber alles auf ewig einwandfrei läuft. Mit aktiviertem IPv6 umgeht man diese Probleme vollständig.

Die Aktivierung im Router ist meist mit einem Klick erledigt, wobei gute Modelle wie die Fritzbox üblicherweise bereits sinnvolle Vorschläge für die Standardeinstellungen mitbringen. Eine externe IPv6-Adresse oder ein Internetprovider, der IPv6 für die Kommunikation im Internet unterstützt, ist nicht nötig.

Weiterhin setzt Matter aktuell für die Kommunikation nach der Geräteverknüpfung ausschließlich auf das User Datagram Protocol (UDP). Wer aus Sicherheitsüberlegungen oder anderen Gründen sein Netzwerk in verschiedene Subnetze aufgeteilt hat, muss folglich sicherstellen, dass alle UDP-Pakete korrekt geroutet werden. Dies gilt für die Netze aller beteiligten Geräte – also für das Handy mit der jeweiligen App ebenso wie für die Hubs und die Geräte selbst.

Matter-Kompatibilität

Smart-Home-Ökosystem	Apple	Google	Amazon	SmartThings	LG ThingQ	Tuya
Smarte Leuchtmittel						
Ein/Aus	✓	✓	✓	✓	✓	✓
dimmbar	✓	✓	✓	✓	–	✓
Farbtemperatur	✓	✓	✓	✓	–	✓
Farben	✓	✓	✓	k. A.	–	✓
Steckdosen/Antriebe						
Ein/Aus	✓	✓	✓	✓	✓	✓
dimmbar	✓	✓	✓	✓	–	✓
Sensoren						
Kontakt	✓	✓	✓	✓	k. A.	k. A.
Licht	✓	✓	–	✓	k. A.	k. A.
Anwesenheit	✓	✓	–	k. A.	k. A.	k. A.
Temperatur	✓	✓	✓	✓	k. A.	k. A.
Druck	–	✓	–	k. A.	k. A.	k. A.
Durchfluss	–	✓	–	✓	k. A.	k. A.
Luftfeuchtigkeit	✓	✓	–	✓	k. A.	k. A.
Schließsysteme						
smarte Schlösser	✓	✓	✓	k. A.	k. A.	k. A.
Fensterverschattung	✓	✓ (nicht Neigen)	–	k. A.	k. A.	k. A.
Heizung und Kühlung						
Thermostate	✓	✓	✓	k.A.	k. A.	k. A.
Mediengeräte						
Smart Speaker	–	✓	–	k.A.	k. A.	k. A.
Sonstiges						
Bridge-Unterstützung	✓	✓	✓	✓	–	–

Stand: Oktober 2023 ✓ vorhanden – nicht vorhanden k.A. keine Angabe

Gerätekategorien

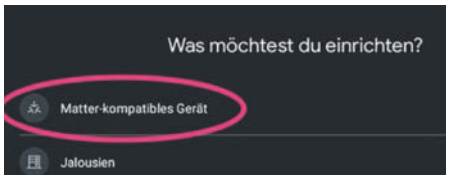
Bei der Frage, welche Matter-Gerätetypen die unterschiedlichen Ökosysteme unterstützen, gibt es aktuell noch gewaltige Unterschiede. Die Tabelle „Matter-Kompatibilität“ unten auf dieser Seite kombiniert öffentlich verfügbare Informationen der Plattformbetreiber und eigene Erfahrungen des Autors und versucht so einen Überblick zu geben, was bereits wo geht. Wie man sehen kann, liegen momentan Apple und Google hinsichtlich der Unterstützung der verschiedenen Produktgruppen vorn. Da Apps und Hub-Firmwares weiterhin ständig verbessert und erweitert werden, können neue Gerätetypen aber jederzeit hinzukommen.

Gut verknüpft

Geräte, die ab Werk Matter-kompatibel sind, kommen mit einem QR-Code, über den sie sich an ein Ökosystem anbinden lassen. Ist der QR-Code zum Scannen zu klein oder unzugänglich, kann man den ebenfalls angegebenen Zahlencode nutzen. Bei älteren Geräte, die per Firmware-Update erst Matter-kompatibel gemacht wurden, gelangt man meist über die herstellerspezifische App an den nötigen QR- oder Zahlencode. Die Verknüpfung von Geräten funktioniert aktuell bei Apple am einfachsten: Die Home-App zeigt im Netzwerk gefundene Geräte direkt an beziehungsweise verknüpft diese direkt nach dem Scannen des QR-Codes oder der Eingabe des Zahlencodes.

Bei Google kommt es vor, dass beim Hinzufügen eines Gerätes die Option „Matter kompatibles Gerät“ nicht direkt angezeigt wird. Hat man für das zu verbindende Gerät einen QR-Code, hilft hier meist eine Scanner-App, die den geräteinternen Link auch auflöst, wenn es sich nicht um eine URL handelt. Leider beherrschen viele QR-Code-Scanner, die in üblichen Foto-Apps integriert sind, dies unter Android nicht. Die App „QR & Barcode Scanner“ aus dem Play Store (siehe ct.de/yec8) lässt sich aber als ein positives Beispiel nennen. Mit der passenden App öffnet sich die Google-Home-App nach dem Scannen des QR-Codes direkt im richtigen Modus. In der Regel erscheint dann auch der fehlende Eintrag beim Verknüpfen neuer Geräte und die Verknüpfung mit Google klappt problemlos.

Bei Komponenten mit WLAN-Unterstützung geht die Verknüpfung über die Handy-Apps meist reibungslos. Falls die Geräte allerdings, wie die Modelle von Eve



Fehlt in der Google-Home-App dieser Eintrag beim Versuch, ein Matter-Gerät zu verknüpfen, dann hilft es, einmalig den QR-Code mit einer Foto-App aus dem Play Store zu scannen.

oder Nanoleaf, über Thread kommunizieren, muss auch der entsprechende Hub des gewählten Ökosystems eine Thread-Unterstützung mitbringen. Andernfalls lässt sich das Gerät nicht einbinden.

Einmal verknüpft, funktionieren die Geräte wie die anderen im jeweiligen Ökosystem verbundenen Geräte auch und lassen sich genauso über Apps oder via Sprache steuern. Doch Vorsicht: Bei Apple und Google führen zwar die Apps den Verknüpfungsvorgang für ein Matter-Gerät aus, alle Steuerungsaktionen laufen danach aber über den Hub. Wenn die Verknüpfung funktioniert hat, das Gerät aber danach als nicht erreichbar ausgewiesen wird, stimmt meist etwas mit der UDP-Kommunikation nicht. Bei Amazon erfolgt die Verknüpfung über die Echo-Geräte als Hubs. Nur über Tuyas Smart-Home-App funktioniert Matter aktuell ohne Hub – allerdings limitiert, da die App laufen muss, damit sich die verknüpften Geräte kontrollieren lassen.

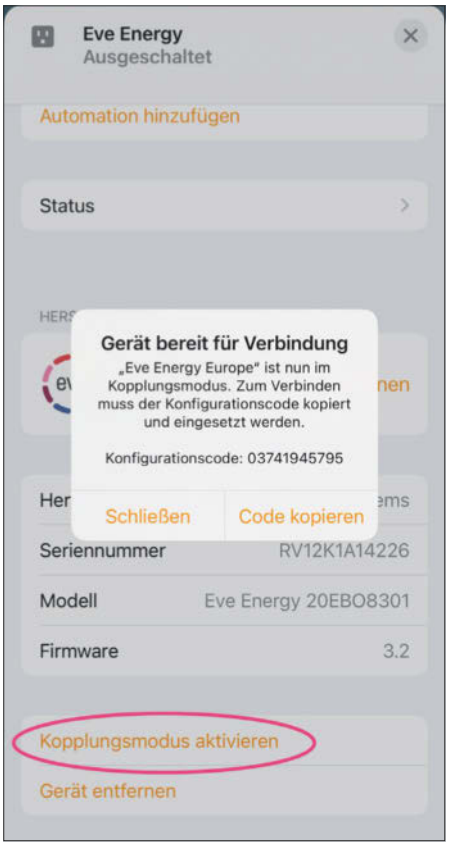
Mehrere Welten

Richtig interessant wird Matter, wenn man das „Multi-Admin-Feature“ nutzt. Dieses ermöglicht es, ein Gerät mit mehreren Ökosystemen zu verknüpfen. Beim Einbinden in einem Ökosystem tauschen die Geräte spezifische Keys und Zertifikate aus, wodurch zwischen beiden Seiten ein sogenanntes „Matter-Fabric“ entsteht. Über diesen Kommunikationsbereich im Matter-Netzwerk können fortan die Geräte des gleichen Fabric sicher miteinander kommunizieren. Gruppierungen, Szenen und Direktverknüpfungen gelten daher auch immer nur für die Geräte im gleichen Fabric. Die Matter-Spezifikation verlangt, dass jedes Gerät die Zuordnung zu mindestens fünf Fabrics ermöglicht.

Doch fünf Fabrics darf man nicht mit fünf Ökosystemen gleichsetzen: So nutzen etwa Apple und Google immer mindestens zwei dieser Fabrics für eine Verknüpfung: ein Fabric für die jeweilige Handy-App als „System-Commissioner“ und eines für den Hub als operativen Controller. Somit bleiben in der Praxis weniger parallele Verknüpfungen übrig; zwei oder drei sollten allerdings mindestens möglich sein.

Um ein Gerät zu einem weiteren Ökosystem hinzuzufügen, wird meist nicht der originale, auf diesem aufgedruckte QR-Code verwendet. Stattdessen erhält man über eine App, mit der es bereits verknüpft wurde, einen speziellen Kopplungscode. Über diese meist 11-stellige Zahl, die sich in der Regel nur einige Minuten nutzen lässt, bindet die App des Zielsystems das Gerät dann ebenfalls an.

Beim Löschen verknüpfter Geräte muss man folglich auch unterscheiden, ob die Verknüpfung nur zu einem oder zu allen Ökosystemen aufgehoben werden soll. Bei letzterer Variante sollte das Gerät danach direkt wieder neu mit dem aufgedruckten QR-Code verknüpfbar sein. Ist dies nicht der Fall, ist das Gerät bei Apple eventuell noch mit dem erwähnten „System-Commissioner“ verbunden. Diese Verbindung lässt sich auf dem iOS-Gerät unter „Einstellungen/Allgemein/Matter-Geräte“ löschen. Alternativ setzt man das Gerät auf Werkseinstellungen zurück, was allerdings den oben genannten Eintrag potenziell verwaist zurücklässt und somit nicht die beste Wahl ist.



In der Apple-Home-App lässt sich ein weiterer Kopplungscode erzeugen, um das Matter-Gerät parallel in einem anderen Ökosystem anzumelden.

Fazit

Matter vereint bewährte Features mit Eigenschaften und Möglichkeiten, die sich viele Smart-Home-Enthusiasten schon lange gewünscht haben – allen voran sind hier die sichere und lokale Kommunikation und das Multi-Admin-Feature zu nennen. Letzteres ermöglicht endlich, dass Geräte nicht mehr nur auf ein Ökosystem oder eine App beschränkt sind, sondern übergreifend nutzbar werden.

Bei Thread als technischem Neuzugang in der Smart-Home-Welt gilt derzeit zwar noch, dass sich Apple, Google, Amazon & Co. künftig besser abstimmen müssen. Am Ende könnte aber tatsächlich ein großes und recht ausfallsicheres Netzwerk im Smart Home stehen. IPv6 ist dabei bereits eine sinnvolle und zukunftsgerichtete Entscheidung.

Dass alle Geräte aufwendig zertifiziert werden müssen, verzögert augenscheinlich deren Verfügbarkeit. Alles in allem ist das Potenzial aber groß, dass Matter die Zukunft des Smart Homes wird. Die Anfänge sehen jedenfalls vielversprechend aus – und das nicht nur auf der Ebene kommerzieller Ökosysteme: Auch die Mitglieder der Open-Source-Community haben begonnen, eine Matter-Unterstützung in Projekten einzubauen. HomeAssistant erlaubt es etwa, als Beta-Funktion Matter-kompatible Geräte zu verknüpfen und so in der Smart-Home-Welt zu nutzen. Bei ioBroker soll Matter noch dieses Jahr integriert werden. Und auch für Node-Red-Nutzer gibt es erste Projekte, um Matter-Geräte zu verknüpfen und zu steuern oder eigene Funktionen als virtuelle Matter-Geräte anzubieten. Darauf gehen wir aber in einer der kommenden Ausgaben ausführlicher ein. *(nij@ct.de)* c't

Literatur

[1] Berti Kolbow-Lehradt, Auf dem Weg zum besseren Smart Home, Der herstellerübergreifende Smart-Home-Standard Matter materialisiert sich langsam, c't 26/2023, S. 140

Übersicht erhältlicher Matter-Geräte und QR-Scan-Apps: ct.de/yec8

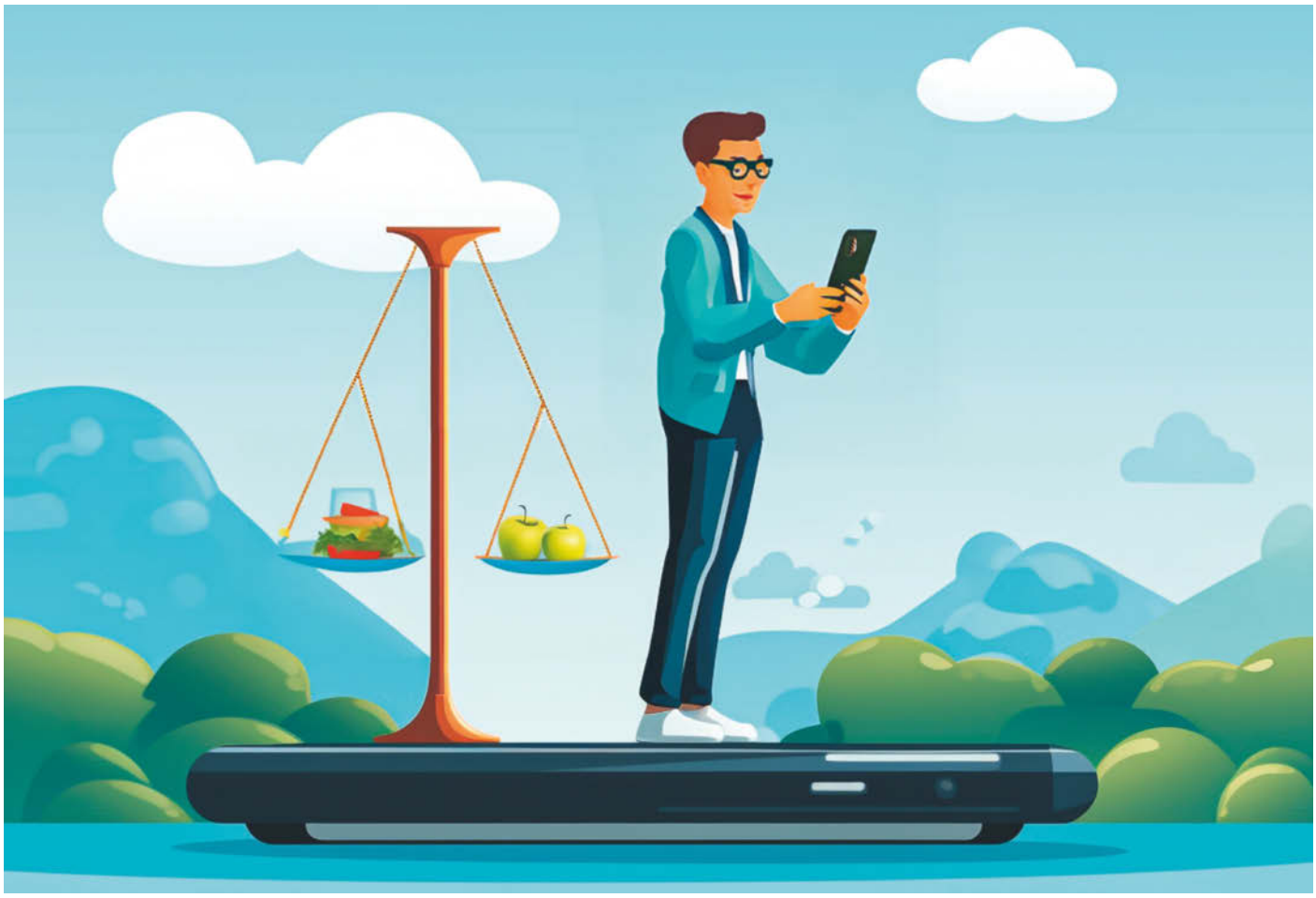


Bild: KI Midjourney | Bearbeitung c't

Die Mischung machts

So optimieren Nährwerte-Apps den Speiseplan

Wie viel Fett, Eiweiß und Kohlenhydrate landen eigentlich täglich auf dem Teller? Wer das nicht mühsam mit Küchenwaage, Nährwerttabelle und Taschenrechner ausrechnen will, überlässt die Arbeit einer Nährwerte-App. Die klugen Helfer können aber noch viel mehr.

Von Dorothee Wiegand

Vielen Menschen ist gesundes Essen zwar wichtig, sie machen aber bei der Auswahl der Speisen Fehler, ohne es zu wissen. Sei es, dass jemand sehr viel Obst isst und dabei das Gemüse zu kurz kommen lässt oder dass ein Sportler auf einen hohen Eiweißanteil achtet, aber dabei die Ballaststoffe vernachlässigt – oft stimmt die Mischung einfach nicht. In solchen Fällen helfen die hier vorgestellten Apps dem Nutzer mit Analysen, Diagrammen, Infos, Tipps und Tricks oder sogar mit kompletten Speiseplänen.

Die Zahl der Apps rund um Gesundheit und Ernährung ist riesig. Es gibt Rezeptdatenbanken [1], die Abwechslung in den Kochtopf bringen, und Barcode-Scanner-Apps [2], die den Nutzer auf spezielle Inhaltsstoffe, insbesondere Allergene, in verpackten Lebensmitteln hinweisen.

Für diesen Test haben wir nach Apps gesucht, die ganz allgemein analysieren, wie sich der tägliche Speiseplan des Nutzers zusammensetzt. Mit dabei sind: EasyFit kcal von Mario Herzberg, Foodiary des gleichnamigen deutschen Anbieters, Lifesum des schwedischen Anbieters Lifesum AB, MyFitnessPal vom gleichnamigen US-amerikanischen Anbieter, die kostenlose App „Was ich esse“ vom Bundeszentrum für Ernährung, Yazio vom gleichnamigen deutschen Anbieter sowie myFoodDoctor von der FoodDoc GmbH. Einer der TV-Ärzte aus der NDR-Doku „Die Ernährungs-Docs“, Matthias Riedl, ist sozusagen das Gesicht der App myFoodDoctor.

Vorstellungsrunde

Zu Beginn möchten die Apps den Nutzer erst einmal kennenlernen. Bis auf das minimalistische „Was ich esse“ fragen alle Apps Geschlecht, Gewicht, Alter und Sportgewohnheiten ab. Diejenigen Testkandidaten, bei denen das Abnehmen im Vordergrund steht, erkundigen sich auch nach dem Wunschgewicht und eventuell

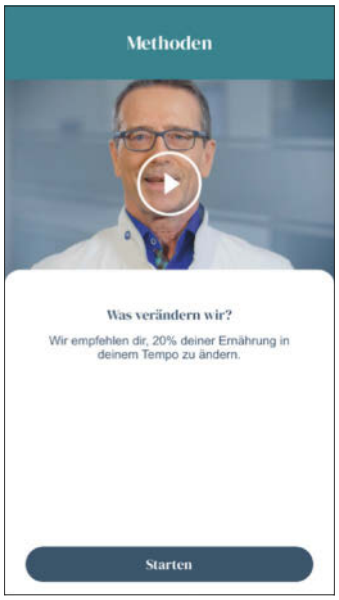
danach, wie schnell der Nutzer Gewicht verlieren möchte.

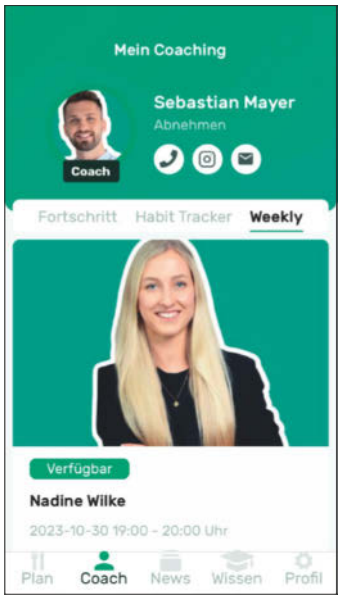
Spätestens an dieser Stelle ist bei allen Apps bis auf „Was ich esse“, das sich ohne Nutzerkonto anonym verwenden lässt, eine Registrierung fällig. Für Foodiary, Lifesum, MyFitnessPal, myFoodDoctor und Yazio haben wir allgemeinverständlich und auf Deutsch verfasste AGB und Datenschutzerklärungen mit den üblichen, DSGVO-konformen Bestimmungen online gefunden. Der US-amerikanische Anbieter von MyFitnessPal weist darin darauf hin, dass erfasste personenbezogene Daten in den USA gespeichert und verarbeitet werden und erklärt „Datenschutz und Persönlichkeitsrechte in den USA können einen geringeren Schutz als in Ihrem Land/Region bieten“. Vom deutschen Anbieter der App EasyFit kcal gibt es online nur eine englische Datenschutzerklärung, die zudem pauschal für alle Apps dieses Entwicklers gilt. Nach Einrichtung der App findet sich im Bereich „Einstellungen“ eine deutsche Datenschutzerklärung.

Machen Sie sich klar, dass Sie den Apps persönliche Daten wie Alter, Gewicht und Vorlieben, zum Teil sogar Informationen über Krankheiten anvertrauen. Zur Synchronisation der Daten auf mehreren Mobilgeräten und auch für detaillierte Analysen und Empfehlungen ist das notwendig. Durch das Abnicken der AGB und Datenschutzerklärungen stimmen Sie dem zu. Sollten Ihnen Bedenken kommen, können Sie diese Zustimmung jederzeit widerrufen und auch die Löschung Ihrer Daten beantragen – die jeweilige App dann aber nicht mehr längern nutzen.

Lifesum und myFitnessDoctor drängen recht bald auf den Abschluss eines kostenpflichtigen Abos, während sich EasyFit kcal, Foodiary, MyFitnessPal und Yazio zumindest eingeschränkt kostenlos nutzen lassen. Bei EasyFit kcal tauchen dann allerdings immer wieder bildschirmfüllende Werbeanzeigen auf. MyFitnessPal kann man einen ganzen Monat lang in der Vollversion kostenlos testen – ein sehr faires Angebot. Foodiary ist auf Dauer nur in der Bezahlversion sinnvoll nutzbar, während bei Yazio zumindest die Funktionen zum Zählen von Kilokalorien frei zugänglich sind.

Wir haben diesen Test auf Apps beschränkt, die sowohl für Android als auch für iOS verfügbar sind. Der eigentliche Test fand auf einem iPad statt, Android-Versionen haben wir uns kurz auf einem Smartphone angesehen. Falls es zur App auch eine Webanwendung gibt, ist das in der Testtabelle vermerkt. Der Inhalt der Websites und -dienste war jedoch nicht Gegenstand des Tests.





Persönliche Ansprache: In der App myFoodDoctor gibt es Videos mit TV-„Ernährungs-Doc“ Matthias Riedl. Foodiary setzt auf Webinare und Beratung durch Ernährungscoaches.

Für eine vollständige Kalorienbilanz muss man auch die sportlichen Aktivitäten berücksichtigen. Einige Apps bieten dazu die Kopplung mit Hard- oder Software an. Das können der Schrittzähler des Smartphones, Fitnesstracker wie das Fitbit oder andere Apps sein, beispielsweise die Health App von Apple, Runkeeper oder MapMy Run.

Trink mal wieder!

Alle Apps achten darauf, dass der Nutzer ausreichend trinkt. Die integrierten Wasser-Tracker zeigen die Trinkmenge als gefüllte Gläser an und verschicken regelmäßig Erinnerungen. Insbesondere Yazio meldet sich mehrmals täglich mit weiteren Hinweisen, bittet beispielsweise montags auf die Waage und mahnt morgens, mittags und abends Einträge im Tagebuch an. Zum Glück kann man auswählen, welche Art von Erinnerungen man bekommen möchte.

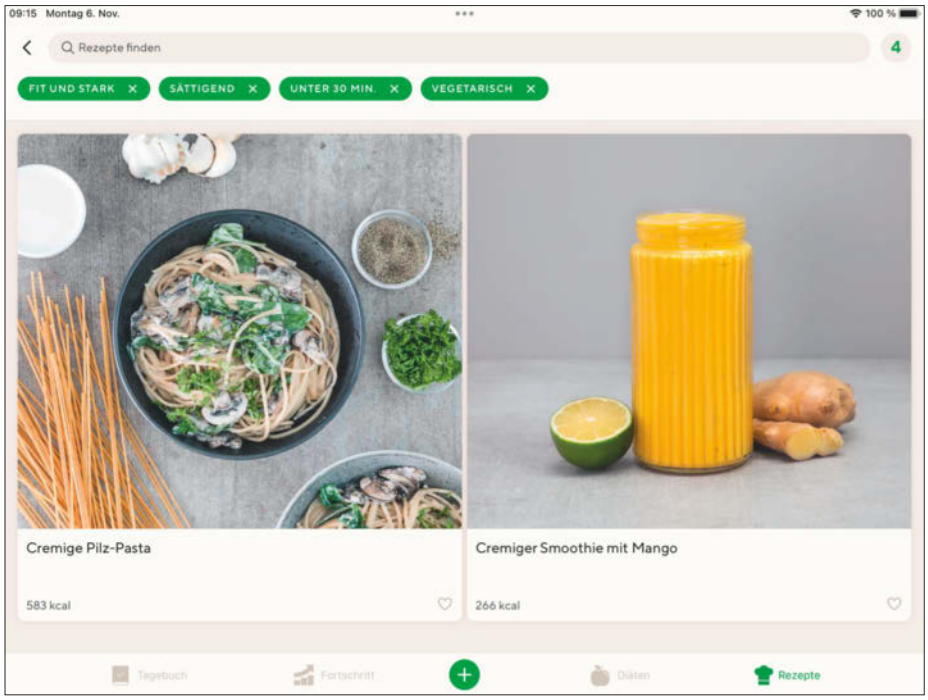
Das Ernährungstagebuch ist zentraler Bestandteil aller Apps. Ideal wäre es, wenn den Apps ein Foto vom leckeren Gemüsecurry genügte, um daraus auf magische Weise alle Inhaltsstoffe zu berechnen. Ganz so einfach ist es nicht. Vielmehr muss der Nutzer einige Tage gewissenhaft Buch führen, bevor sich erste Muster von guten und nicht so gesunden Gewohnheiten abzeichnen. Alle Apps berechnen die Verteilung der drei Makronährstoffe Fett, Eiweiß und Kohlenhydrate – im Folgenden kürzen wir Eiweiß der Einfachheit halber mit EW ab, Kohlenhydrate mit KH.

Einige Apps berechnen darüber hinaus weitere Nahrungsinhalte. myFoodDoctor analysiert beispielsweise, wie groß der tägliche Gemüseanteil ausfällt. Auch die enthaltenen Ballaststoffe sind eine wichtige Größe. MyFitnessPal und Yazio geben detailliert Auskunft zu vielen sogenannten Mikronährstoffen, also Vitaminen und Mineralstoffen. Einige Apps berechnen die gesättigten, einfach und mehrfach ungesättigten Fettsäuren getrennt, viele warnen, falls viel Salz oder Zucker zusammenkommt.

Fleißarbeit

Anfangs braucht es Zeit und Konzentration, das Ernährungstagebuch zu führen. Für unseren Test haben wir fiktive Speisepläne für vier Tage bei allen Kandidaten in die Tagebücher eingetippt. Das Frühstück von Tag 1 und 3 bestand beispielsweise aus Haferflocken, Apfel und einer Dattel zum Süßen. Tag 2 und 4 begannen mit Hirse und Birne plus einer Dattel. Es spart viel Zeit, wenn eine App die Früh-

Falls gewünscht erinnern die Nährwerte-Apps regelmäßig ans Trinken, Wiegen und Protokollieren.



Die Rezeptdatenbank von Lifesum lässt sich nach vielen Stichworten durchsuchen, etwa „klimafreundlich“, „Ernährung für Läufer“ oder „herzhafte Eintöpfe“.

stückszutaten vom Vortag als Vorauswahl anbietet, wie es bei Yazio und MyFitnessPal der Fall ist. Auch eine Favoritenfunktion hilft, wiederkehrende Kombis schneller zu erfassen. Bis auf EasyFit kcal und „Was ich esse“ bieten das alle Testkandidaten.

Die Eingabe der einzelnen Dattel mit einem Gewicht von 5 Gramm erwies sich in einigen Apps als unerwartet knifflig: myFoodDoctor beispielsweise arbeitet mit einer Standardportion von 100 Gramm. Das ist bei Trockenfrüchten oder Nüssen wenig realistisch – der Nutzer muss dann akribisch darauf achten, die Mengenangabe anzupassen. Manche Apps wollen hier helfen, indem sie viele unterschiedliche Eingabevorschläge anbieten. Doch das Durchsuchen der teils viele Bildschirme füllenden Listen kostet ebenfalls Zeit.

In der Testtabelle haben wir vermerkt, ob eine App es gestattet, eigene Mahlzeiten beziehungsweise eigene Rezepte zu ergänzen. Dabei meinen wir – anders als dies zum Teil in den Apps der Fall ist – mit einer Mahlzeit eine Zusammenstellung von Lebensmitteln wie Nudeln, Tomatensoße, Pesto und Parmesan. Als Rezept bezeichnen wir in der Tabelle dagegen eine solche Zutatenliste plus Schritt-für-Schritt-Anweisung, wie sich daraus ein fertiges Essen zubereiten lässt.

Unser Testspeiseplan enthielt durchaus Gesundes, aber auch Tiefkühlpizza und Fruchtjoghurt. Nach aktuellen Empfehlungen standen insgesamt zu viele Kohlenhydrate und zu wenig Eiweiß auf dem Plan – ein Manko, das alle Apps im Test zu Recht bemängelten. Neben den drei Hauptmahlzeiten tippten wir für jeden Tag noch zwei Snacks in die Tagebücher ein. Die individuellen Empfehlungen von myFoodDoctor enthielten richtigerweise den Hinweis, dass die Essenspausen auf diese Weise zu kurz ausfallen.

Sinnvolle Extras

Lifesum, MyFitnessPal, myFoodDoctor und Yazio bieten einen Barcode-Scanner, der helfen soll, abgepackte Lebensmittel schnell einzugeben. Die Scanner haben wir mit zehn Barcodes getestet. Als besondere Herausforderungen erwiesen sich eine Packung vorgegarter Maronen eines französischen Herstellers sowie ein Beutel schwarzer Linsen aus einem indischen Spezialitätengeschäft – diesen Code konnte keiner der Scanner knacken.

Eine integrierte Rezeptdatenbank hilft nicht nur, wenn beim Kochen mal die Ideen fehlen, sondern spart auch enorm Zeit bei den Einträgen ins Ernährungstagebuch: Alle enthaltenen Zutaten lassen sich mit einem Klick ins Tagebuch eintragen. Welche der getesteten Apps eine Rezeptsammlung mitbringen, steht in der Testtabelle. Ein Sonderfall ist dabei myFoodDoctor: Die App enthält zwar einen direkten Link zur sehr umfangreichen Rezeptsammlung des NDR. Doch die Zutaten dieser externen Rezepte lassen sich nicht in die App übernehmen.

Die Preismodelle der meisten Testkandidaten sind schwer zu durchschauen. Es gibt je nach App Abos für einen Monat

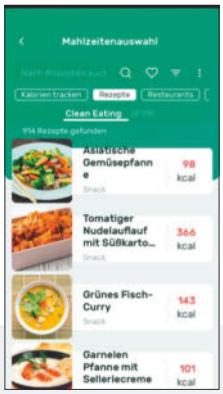
EasyFit kcal

Für jedes Lebensmittel in der Datenbank zeigt diese App eine klare, eingängige Abbildung. In den Einstellungen wählt man zwischen vier Grundfarben – das dunkle Violett empfiehlt sich, weil die recht dünne, weiße Schrift sonst schwer lesbar ist.

Gerade weil sie keine Mengenvorgaben macht, gelang es beim Test dieser App blitzschnell, Lebensmittel zu erfassen – für die einzelne Dattel am Morgen tippten wir lediglich eine „5“ ein, ohne erst umständlich eine vorgegebene Grammzahl zu löschen. EasyFit kcal nimmt alle Speisen eines Tages entgegen, ohne nach Mahlzeit oder Tageszeit zu fragen. Fehler wie zu kurze Essenspausen kann sie so nicht entdecken.

Kalorienaufnahme und -verbrauch steht im Vordergrund. Für den Verbrauch wählt man aus über 100 Sportarten, die samt Dauer und Intensität in die Bilanz eingehen. EasyFit kcal schlüsselt Eingaben auch nach EW, KH und Fett auf, weitere Nahrungsmittelanalysen gibt es nicht. Allerdings kann der Nutzer für eigene Mahlzeiten bis zu drei zusätzliche Angaben wie Salz, Zucker oder Ballaststoffe machen. Diabetiker könnten so etwa Kohlenhydrat- beziehungsweise Broteinheiten erfassen.

+ zügige Dateneingabe
+ unmittelbares grafisches Feedback
– eingeschränkte Analyse



Foodiary

Auch mit Foodiary lassen sich die Zutaten einer selbst gekochten Mahlzeit festhalten. Die Idee hinter dieser App ist jedoch eine andere: Der Nutzer erhält individuelle Empfehlungen für alle Mahlzeiten des Tages, für die die App auch Einkaufslisten generiert. Wer den Rezeptvorschlägen der App folgt, erreicht laut Anbieter jeden Tag das gesetzte Ziel an Makronährwerten, ohne selbst planen zu müssen.

Die App richtet sich an junge, Fitness- und Sport-affine Personen: Außer Mahlzeiten und einzelnen Lebensmitteln lassen sich auch diverse Nahrungsergänzungen wie Eiweißpulver und Fitnessriegel mit einem Klick hinzufügen; ein Reiter namens „Restaurants“ führt zu einer Liste mit „Dean&David“-Produkten.

Der volle Funktionsumfang der App lässt sich für 29 Euro drei Monate lang nutzen. Darüber hinaus gibt es für 150 Euro ein dreimonatiges individuelles digitales Coaching, bei dem eine KI den Nutzer anhand seiner Angaben und Ziele berät. Für 450 Euro kann man drei Monate Betreuung durch einen menschlichen Coach und Ernährungsberater buchen. Beide Beratungsangebote bezuschussen viele Krankenkassen mit 150 Euro.

- umfangreiche Rezeptdatenbank
- persönliche Beratung zubuchbar
- teils hakelige Bedienung

Lifesum

Anhand von Fragen ermittelt Lifesum den wöchentlichen „Life Score“ des Nutzers. Ist der Nutzer bei salzigem Knabberkram schwach geworden, hat er ausreichend Fisch gegessen, Vollkorn- oder Weißmehlprodukten den Vorzug gegeben, das Training vernachlässigt? Je nach den Antworten liegt der Life Score zwischen „am Ziel vorbei“ und „optimal“.

Schön: Gleich nach den Einträgen für einen Tag erscheint eine Tagesbewertung. Sie lautete im Test am zweiten Tag, mit Pizza zum Abendbrot: „Versuche, deine Kalorienzufuhr etwas einzuschränken und lege deinen Fokus auf gesunde Alternativen!“

Nahrungsmittel lassen sich zügig eintippen. Die Datenbank enthält allerdings eine verwirrende Vielfalt an Einträgen. So gibt es einerseits 100 Gramm „Erbsen, grün, gekocht“ mit 69 Kilokalorien, dieselbe Menge „Erbsen grün gegart“ soll dagegen 85 Kilokalorien haben.

Der Barcodescanner arbeitete im Test sehr fix und erkannte alles bis auf die schwarzen Linsen aus dem indischen Spezialitätensortiment. Zum Teil stimmten die Angaben aus dem Scanner allerdings nicht exakt mit denen auf der Packung überein.

- umfangreiche Rezeptdatenbank
- motivierende Nutzeransprache
- teils widersprüchliche Angaben

MyFitnessPal

Das Eingeben von Nahrungsmitteln brauchte bei dieser App anfangs Zeit. Bei Gemüse steht häufig eine 100-Gramm-Portion in der Datenbank, für Nüsse häufig 25 Gramm – das ist sinnvoll, verlangt aber Konzentration. Falls die vorgegebene Menge nicht passt, wählt man mithilfe eines Drehrädchens einen Bruchteil oder ein Vielfaches. Ein Problem ist die Fülle der Datenbankeinträge. So liefert der Suchbegriff „Erbsen“ mehr als hundert Treffer, darunter Einträge wie „Schwarze Erbsen 171 gramm“ und „Matschige Erbsen 201 gramm“.

MyFitnessPal erstellt auch zu Mikronährstoffen Grafiken, doch die muss man erst mal finden. Sie verstecken sich hinter den Bezeichnungen „Fortschritt“, „Mein Wochenbericht“ und „Ernährung“, die man durch Klick auf „... mehr“ unten rechts auf den Bildschirm ruft.

Der integrierte Barcode-Scanner musste lediglich bei den schwarzen Linsen passen, für alle anderen Codes lieferte er je einen passenden Treffer.

In dieser App nimmt auch das Aufzeichnen der sportlichen Betätigung einen großen Raum ein. Laut Hersteller lässt sich MyFitnessPal dazu aktuell mit 23 Sport- und Fitness-Apps koppeln.

- 30 Tage lang gratis testbar
- analysiert viele Mikronährstoffe
- unübersichtliche Struktur

sowie für drei, sechs oder zwölf Monate. Während des Testens fielen uns immer wieder Angebote mit kräftigen Rabatten auf, die jedoch mitunter nur für den ersten Monat eines längeren Abo-Zeitraums galten. Bei Foodiary besteht die Möglichkeit, sich die Kosten zumindest teilweise von der Krankenkasse erstatten zu lassen. Für myFoodDoctor ist die Anerkennung der App als Präventionsmaßnahme beantragt.

In der Testtabelle sind alle verfügbaren Abos mit den jeweiligen regulären Preisen aufgelistet. Sie sollten übrigens gut überlegen, bevor Sie ein Jahresabo für eine der Nährwerte-Apps abschließen. Die beste Nutzung der Apps ist es, sich bei einer Ernährungsumstellung vorübergehend unterstützen zu lassen. Im Idealfall haben Sie nach drei Monaten so viel über Ihre Ernährung gelernt, dass Sie anschließend auf dem richtigen Kurs sind. Zum

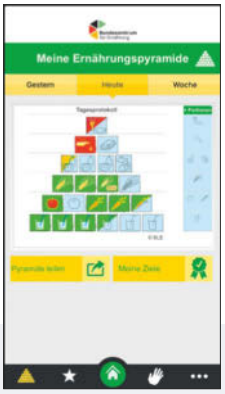
myFoodDoctor

Die Basis dieser App ist das 20:80-Prinzip, zu dem der namensgebende NDR-Ernährungsdoc Matthias Riedl mehrere Bücher geschrieben hat. Die Idee: 80 Prozent der liebgewonnen Verhaltensweisen dürfen bleiben. Die App identifiziert diejenigen 20 Prozent der Essgewohnheiten, die zur gesünderen Ernährung oder Gewichtsreduktion Schritt für Schritt umgestellt werden sollten.

Nachdem die ersten Nahrungsmittel eingetippt sind, zeigt die App unmittelbar die Mengen von EW, Kalorien, Zucker, Ballaststoffen und Gemüse als Anteil der empfohlenen Tagesmenge an. Am vierten Tag bekommt der Nutzer zum ersten Mal eine individuelle Empfehlung – im Test kommentierte myFoodDoctor die Mahlzeitenstruktur sowie die Tagesmenge an Proteinen und Ballaststoffen. Dann schlug die App erste Schritte zur Ernährungsumstellung vor, darunter Intervallfasten. Der Nutzer wählt aus diesen „Methoden" genannten Vorschlägen etwas aus.

Das Eingeben der Daten geht dank durchdachtem Bedienkonzept leicht von der Hand. Der Barcode-Scanner musste bei den Maronen und den schwarzen Linsen passen. Ansonsten lieferte er jeweils genau einen passenden Treffer.

- motivierende Nutzeransprache
- differenzierte Analyse
- individuelle Empfehlungen



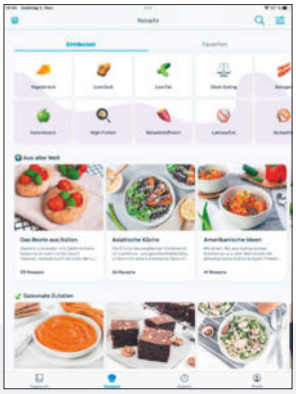
Was ich esse

Das kostenlose „Was ich esse" ist ein Service des Bundeszentrums für Ernährung (BZfE) in Bonn. Grundlage dieser App ist die sogenannte Ernährungspyramide. Sechs Würfel für „Wasser trinken" bilden das Fundament, darauf eine Reihe aus fünf Würfeln – zwei für Obst und drei für Gemüse. Die Pyramidenspitze zeigt, was seltener gegessen werden sollte: ein Würfel für Süßes, zwei Würfel für Fett.

Jeder Würfel steht für eine „Portion", worunter diese App immer eine Handvoll versteht. Dieses sehr grobe Maß wächst sozusagen mit: Für Kinder empfiehlt die App eine kleine Hand voll Broccoliröschen oder Karotten, für Erwachsene entsprechend mehr. Man kann die Vorgaben zwar anpassen, etwa die zweite Pyramidenschicht zu einer Obst- plus vier Gemüseportionen ändern – an der Darstellung der Pyramide in der Hauptansicht ändert das aber nichts.

Portionen lassen sich lediglich in 0,5er-Schritten angeben – für eine einzelne Dattel zu ungenau. Die Auswertung erfolgt nicht nach EW, KH und Fett, sondern nur nach den Kategorien der Pyramide: Getränke, Obst, Gemüse, Getreide, Michprodukte, Fisch/Fleisch/Wurst/Eier, Fette und Öle sowie Extras.

- leicht bedienbar
- unmittelbare grafische Rückmeldung
- Portionsangaben ungenau



Yazio

Bereits die erste Mahlzeiteneingabe – das Frühstück aus Hafer, Apfel und Dattel – kommentierte Yazio ausführlich. Allerdings fallen die umfangreichen Kommentare oft widersprüchlich aus. So lobt die App Süßkartoffeln als kalorienarm, warnt aber gleichzeitig vor den vielen Kohlenhydraten des Gemüses. Selbst bei geringen Mengen Olivenöl weist die App auf dessen Fettgehalt hin und warnt bei einer einzelnen Dattel vor zu viel Zucker.

Die Rezeptsammlung kann man anhand von Suchbegriffen wie „Für unterwegs", „Wenig Zutaten" oder „Low Carb" durchforsten. Bemerkenswert sind Yazios detaillierte Auswertungen: Die App stellt nicht nur die täglich aufgenommene Menge an EW, KH und Fett als Säulendiagramm dar, sondern auch Vitamine, Mineralstoffe, Zucker, Salz, Alkohol und etliche weitere Nahrungsbestandteile. Yazio kann auch die Stimmung des Nutzers tracken.

Yazios Barcode-Scanner erkannte im Test alles bis auf die schwarzen Linsen, lieferte aber zum Teil sehr viele Treffer: 12 bei einer Packung mit einem spanischen Käsesortiment, 16 bei einem Kräuterfrischkäse. So gestaltete sich das Scannen teilweise unübersichtlich.

- umfangreiche Rezeptdatenbank
- analysiert viele Mikronährstoffe
- teils widersprüchliches Feedback

einen will man womöglich nicht jahrelang akribisch über seine Essgewohnheiten Buch führen, zum anderen finden sich in Internetforen Berichte darüber, dass Nutzer von Kalorienzähl-Apps regelrecht abhängig wurden und Essstörungen entwickelten – diese Gefahr ist bei aufs Abnehmen und auf den Kalorienverbrauch fokussierten Apps nicht zu unterschätzen.

Fazit

Für einen groben Überblick über die eigenen Essgewohnheiten ist „Was ich esse" eine gute Wahl. Die App vermittelt bewährte Konzepte wie die Ernährungspyramide sowie das Prinzip, jeweils eine Handvoll von einem Nahrungsmittel als eine Portion zu verstehen. Die kompakte App kann Obst-Junkies und Gemüsemuffel enttarnen und auf hohen Fett- oder Zuckerkonsum aufmerksam machen.

Mehr als eine allererste, sehr allgemeine Analyse liefert sie jedoch nicht.

Wer spontan entscheidet, was auf den Tisch kommt, und gern eigene Rezepte zubereitet, braucht eine App, die die Nahrungsmittelangaben zügig entgegennimmt. EasyFit kcal, Lifesum und myFoodDoctor sind dann eine gute Wahl. Mit seinen eingängigen, irgendwie niedlichen Abbildungen eignet sich EasyFit kcal übrigens auch gut dazu, Kindern in Elternhaus, Kita oder Grundschule die Grundlagen rund um gesundes Essen nahezubringen.

Falls in der Küche die Ideen fehlen, helfen Lifesum und Yazio mit ihren Rezeptdatenbanken weiter. Foodiary hat ebenfalls viele interessante Rezepte im Gepäck und geht noch einen Schritt weiter: Hier stehen vollständige Ernährungspläne im Vordergrund, denen der Nutzer nur folgen muss, um sich ausgewogen zu ernähren.

Passionierte Sportler sollten sich Foodiary, MyFitnessPal oder EasyFit kcal genauer anschauen. Bei Foodiary steht die passende Ernährung für Sportler im Vordergrund, MyFitnessPal verbindet sich mit zahlreichen Sport-Apps und mit EasyFit kcal kann man den Kalorienverbrauch vieler Sportarten von Hand recht genau exakt tracken.

Wer sich über Mikronährstoffe informieren möchte, findet bei MyFitnessPal und Yazio detaillierte Auswertungen; die Analyse von myFoodDoctor geht ebenfalls über die Makronährstoffe hinaus und betrachtet etwa die Menge der Ballaststoffe, Zuckerkonsum und Gemüseanteil.

Besonders individuell beraten Lifesum, Foodiary und myFoodDoctor. Bei Lifesum funktioniert das mit langen Fragenserien, Foodiary bietet gegen Aufpreis den persönlichen Kontakt zu einem Coach. myFoodDoctor analysiert das Ernährungstagebuch am eingehendsten von allen hier getesteten Apps.

Wie eingangs erwähnt, gibt es eine Vielzahl weiterer Gesundheits- und Fitness-Apps in den Stores. Falls Ihre persönliche Lieblings-App nicht dabei war, schreiben Sie uns gern an: *(dwi@ct.de)* **c't**

Literatur

[1] André Kramer, Innovativ kochen, Sechs Rezept-Apps für abwechslungsreiche Küche, c't 5/2021, S. 120

[2] Arne Grävemeyer, Andrea Trinkwalder, Tricorder im Supermarkt, Scanner-Apps checken Lebensmittel – wir checken die Apps, c't 1/2022, S. 104

Alle genannten Apps: ***ct.de/ytxy***

Nährwerte-Apps

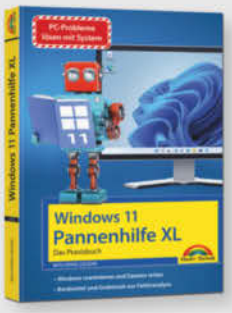
App	EasyFit kcal	Foodiary	Lifesum	MyFitnessPal	myFoodDoctor	Was ich esse	Yazio
Anbieter	Mario Herzberg	Foodiary GmbH	Lifesum AB	MyFitnessPal, Inc.	FoodDoc GmbH	Bundeszentrum für Ernährung	Yazio GmbH
Firmensitz	Deutschland	Deutschland	Schweden	USA	Deutschland	Deutschland	Deutschland
URL	easyhealthapps.com	foodiary.app	lifesum.com/de	myfitnesspal.com/de	myfooddoctor.de	www.bzfe.de/app-was-ich-esse	yazio.com/de
Android / iOS ab Version	4.4 / 12.0	7.0 / 11.0	9.0 / 14.0	geräteabhängig / 15.0	5.0 / 11.0	4.1 / 16.2	7.0 / 14.0
korrespondierende Webanwendung	–	✓	✓	✓	–	–	–
Schwerpunkt der App liegt auf	Kalorienzählen, Gewichtskontrolle	Ernährung für Sportler, individuelle Ernährungspläne, umfassende Information	Kalorienzählen, spezielle Ernährungspläne (7 bis 21 Tage, z.B: vegan, Keto, Paleo, zuckerfrei)	Kalorienzählen, Gewichtskontrolle, Fitness	Prävention, 20:80-Methode, individuelle Beratung, umfassende Information	erste Orientierung, Ernährungspyramide	Kalorienzählen, Gewichtskontrolle, Vitamine & Mineralien
Ernährungstagebuch							
Lebensmittelliste zeigt Verlauf	✓	–	✓	✓	✓	✓	✓
nachträgliche Einträge möglich	✓	–	✓	✓	✓	(✓)[1]	✓
berücksichtigt Essenszeitpunkt	–	✓	✓	✓	✓	–	✓
eigene Lebensmittel hinzufügen	✓	✓	✓	✓	–	✓	✓
Favoritenfunktion für Lebensmittel / Mahlzeiten	– / –	– / (✓)[2]	✓ / ✓	– / –	– / ✓	✓ / –	✓ / ✓
eigene Mahlzeiten / Rezepte hinzufügen	✓ / –	✓ / –	✓ / ✓	✓ / –	✓ / –	– / –	✓ / ✓
Barcode-Scanner	–	–	✓	✓	✓	–	✓
Weitere Funktionen							
Wasser-Tracker	(✓)[3]	✓	✓	✓	✓	✓	✓
Intervallfasten-Timer	–	–	✓	–	✓	–	✓
Rezeptdatenbank / Anzahl Rezepte laut Hersteller	–	✓ / 1700+	✓ / k.A.	–	(✓)[4]	–	✓ / 2000+
App erstellt Einkaufsliste	–	✓[2]	(✓)[5]	–	–	–	✓
Sport-Tracker	✓	–	(✓)[6]	(✓)[6]	(✓)[7]	–	✓
Bewertung							
Ernährungstagebuch	⊕	○	⊕	○	⊕	⊖	⊕
Nährwertanalyse	○	○	⊕	⊕⊕	⊕⊕	○	⊕⊕
Beratung	⊖	⊕⊕	⊕	○	⊕⊕	⊖	○
Preise							
	einmalig 7 €	3 Monate: 29 €	1 Monat: 15 €	1 Monat: 20 €	6 Monate: 50 €	kostenlos	3 Monate: 30 €
			3 Monate: 40 €	12 Monate: 80 €	12 Monate: 90 €		12 Monate: 50 €
			12 Monate: 100 €				

✓ vorhanden – nicht vorhanden k.A. keine Angabe ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht

[1] nur Vortag [2] nur Rezepte aus DB [3] nur iOS [4] Link zu externer DB [5] für Ernährungspläne [6] nur über Fitnessgeräte und -Apps [7] nur Dauer, nicht Sportart

Für Wissenshungrige...

Ausgewählte Fachliteratur



Wolfram Gieseke

Windows 11 – Power-Tipps

Ob ein externes Gerät nicht erkannt wird, Programme nicht mehr wie gewohnt laufen oder ein Ihnen unbekannter Update-Fehler auftritt: Wenn Sie den unterschiedlichen Fehlermeldungen selbst auf den Grund gehen möchten, hilft Ihnen dieses Buch weiter.

19,95 €

Brian Svidergol, Bob Clements, Charles Pluta

Microsoft 365 Mobilität und Sicherheit

Bereiten Sie sich auf die Microsoft-Prüfung MS-101 vor und zeigen Sie, dass Sie die erforderlichen Fähigkeiten und Kenntnisse für die Verwaltung von Mobilität und Sicherheit in Microsoft 365 sowie die damit verbundenen Verwaltungsaufgaben in der Praxis beherrschen. Dieses Prüfungstraining wurde für erfahrene IT-Profis entwickelt.

49,90 €

Eric Amberg, Daniel Schmid

Hacking – Der umfassende Praxis-Guide (2. Auflage)

Dies ist ein Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheitsspezialisten und interessierte Poweruser. Mithilfe vieler Workshops sowie Tipps und Tricks lernen Sie die Vorgehensweise eines professionellen Hacking-Angriffs kennen.

49,99 €

Michael Weigend

Python 3 für Studium und Ausbildung

Alle wichtigen Grundlagen der Python-Programmierung werden erklärt. Es sind keine Vorkenntnisse notwendig und die Themen werden fachunabhängig erläutert.

19,99 €

Christian Immler

Haus und Wohnung smart vernetzt

Ob Sie Daten, Musik und Medien im ganzen Haus nutzen, Ihr WLAN optimieren oder per App aus der Ferne Ihre Heizung anstellen, diese und weitere relevante Themen rund um Ihr vernetztes Zuhause werden in diesem Buch ausführlich besprochen.

19,95 €

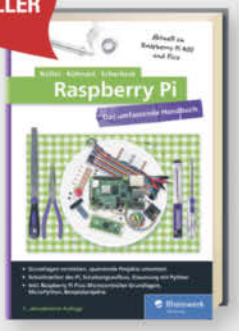
Thomas Kaffka

3D-Druck – Praxisbuch für Einsteiger (3. Auflage)

Entdecken Sie die nahezu unbegrenzten Möglichkeiten des 3D-Drucks in allen Varianten: vom Einsatz des eigenen 3D-Druckers zu Hause über die Verwendung von öffentlich zugänglichen Druckern bis hin zur Nutzung von 3D-Druckservices.

29,99 €

BEST-SELLER



Michael Kofler, Charly Kühnast, Christoph Scherbeck

Raspberry Pi (7. Auflage)

Das Standardwerk in 7. Auflage, aktuell zum Raspberry Pi Pico.
Die RasPi-Experten Michael Kofler, Charly Kühnast und Christoph Scherbeck bieten Ihnen auf über 1.000 Seiten das komplette Wissen, damit Sie mit dem Raspberry Pi richtig durchstarten.

44,90 €

Anatomie 4D – Der menschliche Körper

Mithilfe einer kostenlosen App und bahnbrechender Augmented Reality kann der Aufbau der Knochen, die Muskeln in Aktion, das Nerven- und Kreislaufsystem sowie das größte menschliche Organ, die Haut, beobachtet werden.

14,95 €

...und Nerds

shop.heise.de/highlights2023

Zubehör und Gadgets

Oxocard Artwork Creative Coding

Mit dem leistungsfähigen Dual-Core Chip ESP32 liefert die Oxocard genügend Power für Ihre Experimente. Lernen Sie in kurzer Zeit wie man beeindruckende visuelle Effekte erzeugt, wie wir sie aus Spielen und Filmen kennen.

69,90 €

musegear® finder Version 2

Finden Sie Schlüssel, Handtasche oder Geldbeutel bequem wieder statt ziellos zu suchen. Mit dem Finder können Sie z.B. das Smartphone klingeln lassen oder Wertgegenstände einfach tracken und noch mehr.

24,90 €

Joy-IT LCR-T7 Messgerät

Mit Hilfe des LCR Messgerätes können Sie die Induktivitäten (L) von Spulen, Kapazitäten (C) von Kondensatoren und deren Widerstände (R) als Verlust messen. Die automatische Bauteilerkennung von dem Messgerät kann elektronische Komponenten (Dioden, Z-Dioden, Doppeldioden, Widerstände, Kondensatoren, Induktoren, Thyristoren, Triacs, Feldeffekttransistoren, Bipolartransistoren und Batterien) erkennen.

29,90 €

Nitrokey 3A NFC

Der Nitrokey 3 vereint die Funktionen vorheriger Nitrokey Modelle: FIDO2, Einmalpasswörter, OpenPGP Chipkarte, Curve25519, Passwort-Manager, Common Criteria EAL 6+ zertifiziertes Secure Element, Firmware-Updates. Damit werden Ihre Accounts zuverlässig gegen Phishing und Passwort-Diebstahl geschützt.

59,90 €

Joy-IT OR750i: Freifunk- & OpenWrt-Dual-Band-Router

Der Einstieg in die Freifunk- und OpenWrt-Welt kann oft schwierig sein. Deshalb hat Joy-IT in Zusammenarbeit mit Freifunk Hannover und c't den OR750i entwickelt.
Dank Webinterface kann man beliebige Firmwares einfach hochladen – ohne komplizierte Kommandos oder inkompatible Hardware-Revisionen; ideal für OpenWrt-Einsteiger und solche, die Freifunk einfach nur nutzen wollen.

39,90 €

JOY-IT DSO-138 M mini Oszilloskop

Das Mini- Oszilloskop mit einer Bildschirm-Größe von 2,4" kann per USB oder Akku betrieben werden. Eine Verbesserung ist der externe Triggereingang, welcher TTL- und LVTTL-Signale als Quelle akzeptiert und serielle Ausgabe von Wellenformdaten.

54,90 €

Die Reise mit dem micro:bit V2

Mit der Electronic Adventure Experimentier-Box ab 8 Jahren lernt man in aufeinander aufbauenden Lektionen wie sich auf Basis des BBC micro:bit spannende Experimente verwirklichen lassen.

49,90 €

REINER SCT Authenticator

Der REINER SCT Authenticator speichert die elektronischen Schlüssel für die Logins sicher in seiner Hardware und generiert die TOTP-Einmalpasswörter hochgenau alle 30 Sekunden. Er arbeitet ohne Internetverbindung und kann deshalb online nicht angegriffen werden. Zusätzlich kann seine Funktion noch mit einem PIN-Schutz abgesichert werden.

44,90 €

Zahlen, Daten, Fakten

Kurznachrichtendienste

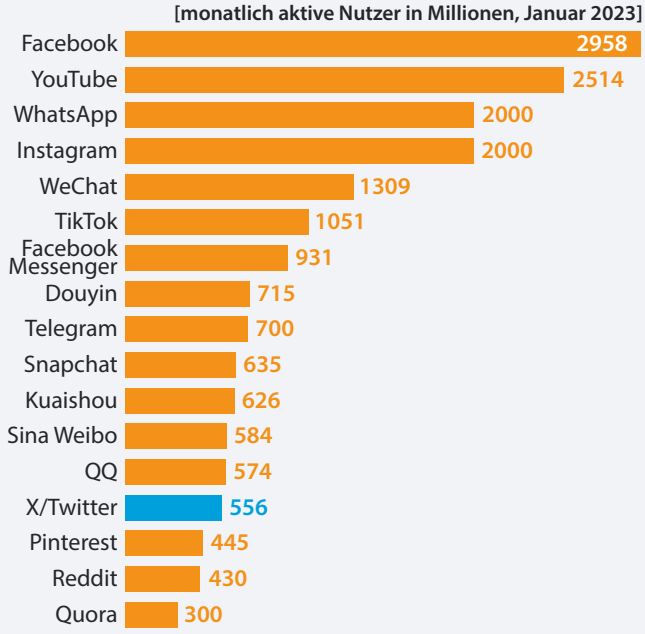
Elon Musk zog bald nach Übernahme des mittlerweile in „X“ umbenannten Kurznachrichtendienstes Twitter den Zorn der Nutzer auf sich, indem er integrierte Leistungen kürzte oder bepreiste. Doch es ist wie bei einem Messenger: Man kann ja nicht einfach dem Anbieter den Rücken kehren – die für die eigenen Themen relevanten Nutzer müssten ebenfalls wechseln. So ist X trotz aller Proteste und Boykottandrohungen unangefochten die Nummer eins für Kurznachrichten.

In den USA steht Threads in direkter Konkurrenz zu X; der Kurznachrichtendienst von Meta ist derzeit in Europa noch nicht verfügbar. Innerhalb von einer Stunde knackte er im Juli 2023 die 1-Millionen-Nutzer-Marke. Doch die harte Währung der Branche sind die aktiven Nutzer – Experten sprechen vom „monetarisierbaren täglich aktiven Nutzer“, kurz mDAU, als Kenngröße und vermuten bei Threads weit weniger mDAUs als Anmeldungen.

In Deutschland bieten sich Mastodon und neuerdings auch Bluesky für X-Verweigerer an. Deren Nutzerzahlen liegen noch weit unter denen von X. Mastodon dokumentiert Nutzeraktivität sehr transparent. Die Grafik zeigt, welche Rolle der Ärger über X dafür spielt. *(dwi@ct.de)* c't

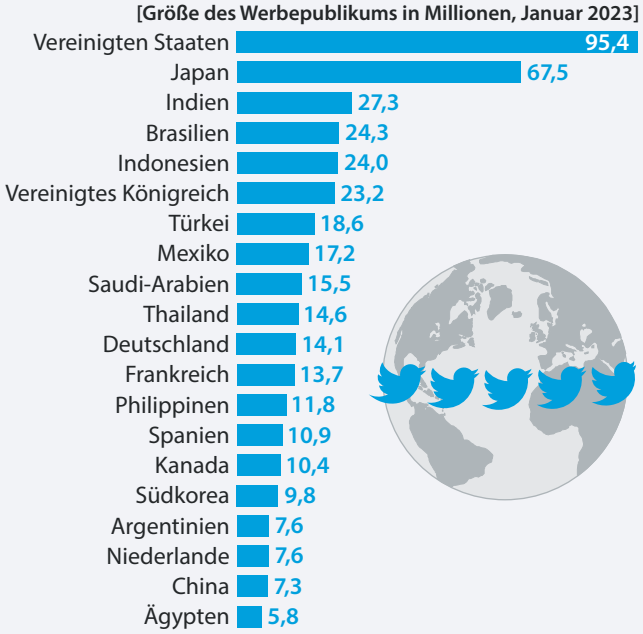
▶ Nutzerzahlen im Vergleich

Bei der Zahl der zumindest einmal im Monat aktiven Nutzer in sozialen Netzwerken und Messengern rangiert X/Twitter relativ weit hinten.[1]



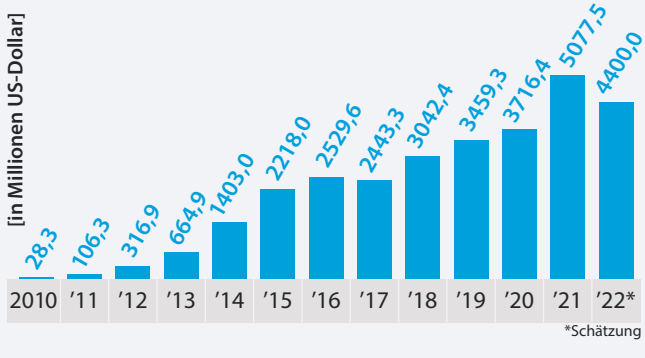
▶ Werbereichweite von Twitter

Im Januar 2023 belief sich die Größe des Werbepublikums bei X/Twitter in den USA auf rund 95,4 Millionen Personen.[1]



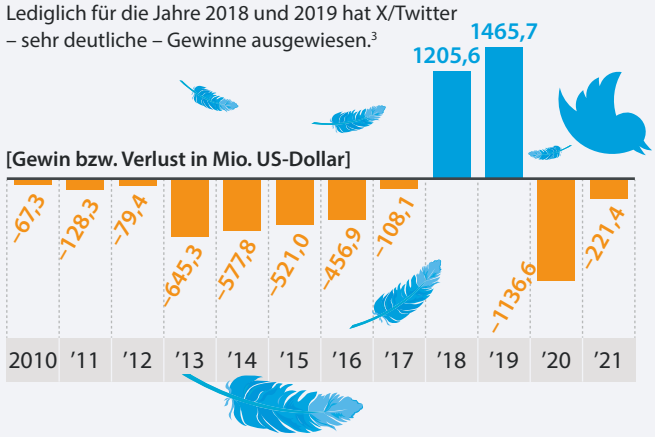
▶ Meist steigende Umsätze

Der dargestellte Umsatz für 2022 beruht auf einer Schätzung. X/Twitter selbst hat seit Juli 2022 keine Kennzahlen mehr ausgewiesen.[2]



▶ Gewinne + Verluste

Lediglich für die Jahre 2018 und 2019 hat X/Twitter – sehr deutliche – Gewinne ausgewiesen.[3]

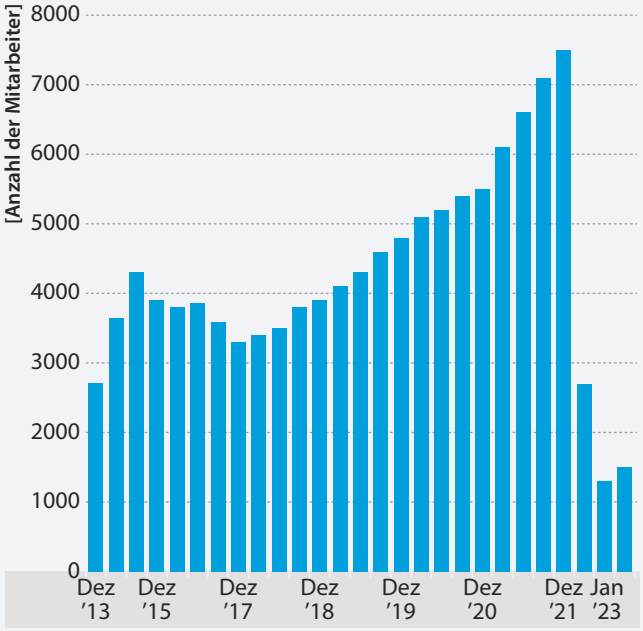


▶ Dynamische Entwicklung

Ein Vergleich der Anfangsphase einiger Onlinedienste zeigt, wie dynamisch sich Nutzerzahlen heutzutage entwickeln.[5]

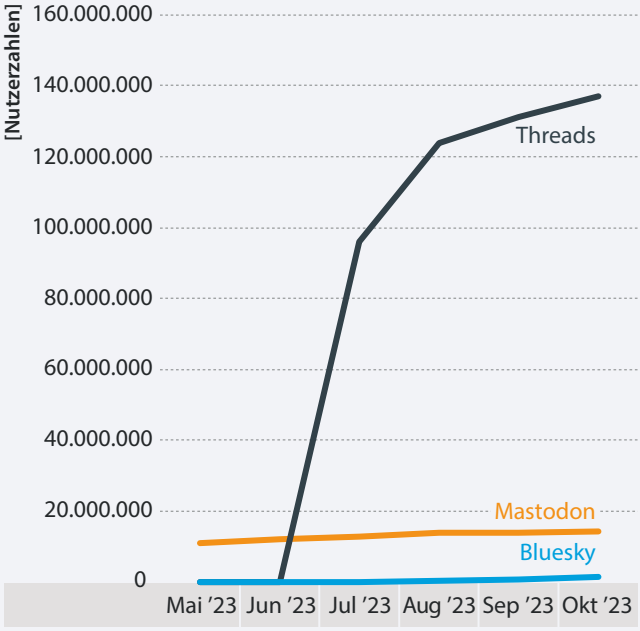
▶ Viele mussten gehen

Nachdem Elon Musk Twitter im Oktober 2022 übernommen hatte, entließ er innerhalb kürzester Zeit mehr als 60 Prozent der Mitarbeiter.[3]



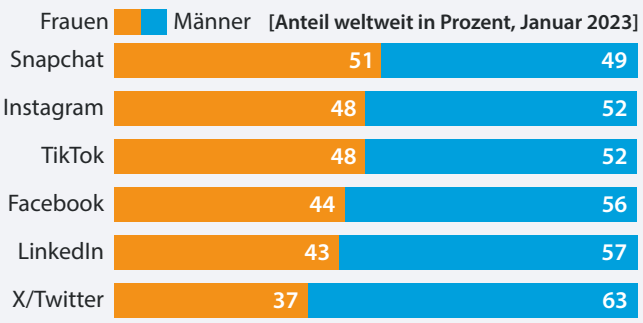
▶ Threads: Toller Start

Threads startete im Sommer 2023 grandios, die Zahl der täglich aktiven Nutzer ging aber schon bald um mehr als 80 Prozent zurück.[4]



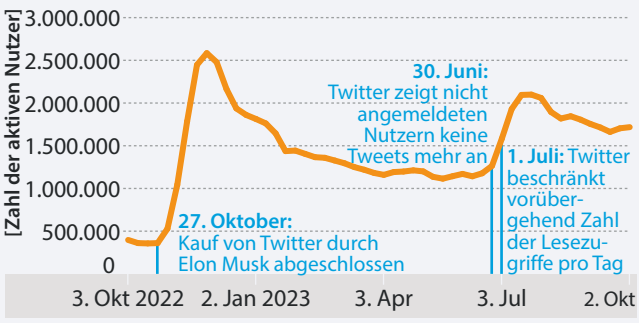
▶ Deutlich mehr Männer

Der Frauen- und Männeranteil bei den sozialen Netzwerken unterscheidet sich deutlich. Fast zwei Drittel der X/Twitter-Nutzer sind männlich.[3]

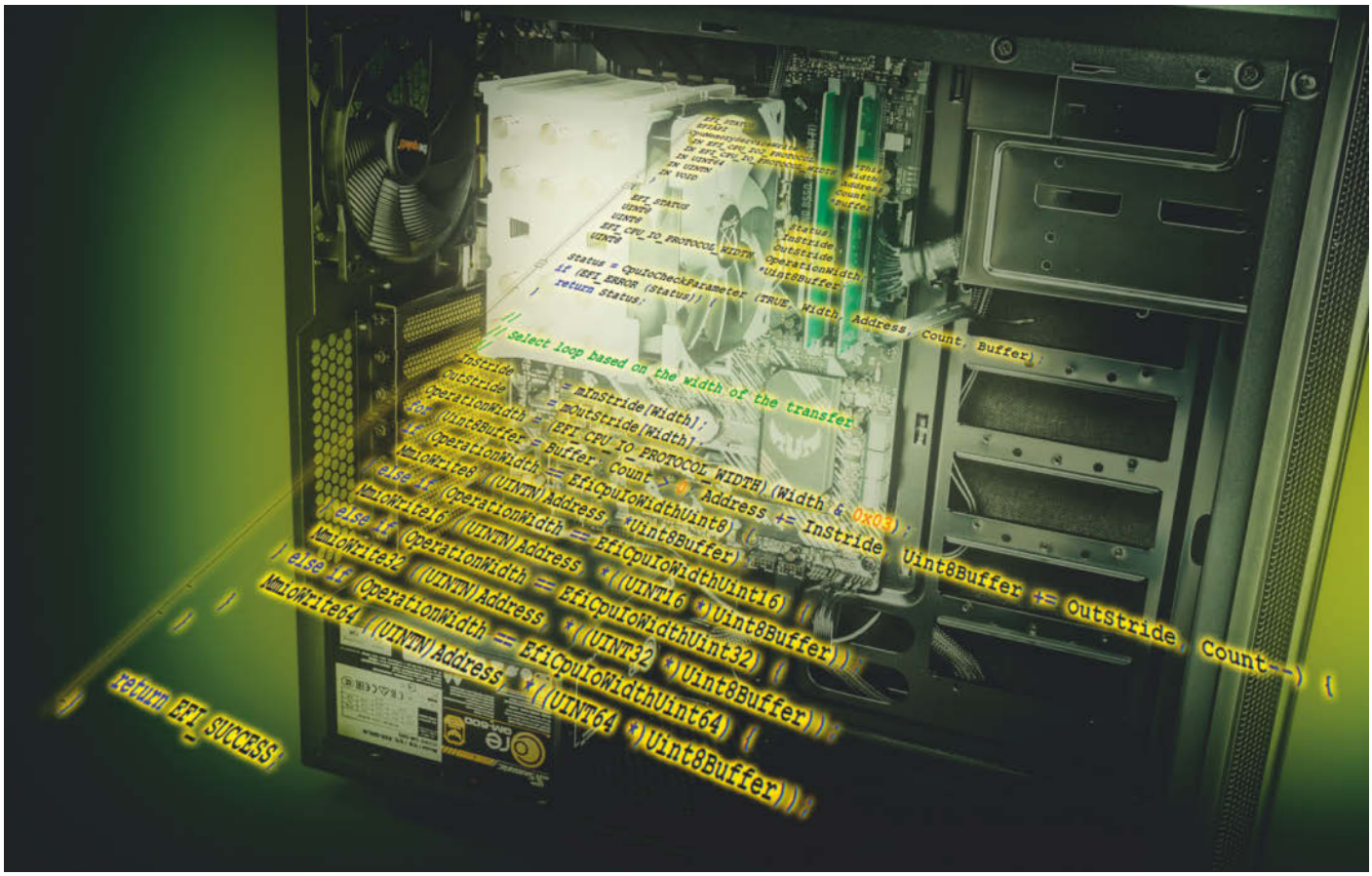


▶ Mastodon: Aktive Nutzer

Die Zahl der aktiven Mastodon-Nutzer stieg mehrfach als Reaktion auf Twitter-Ereignisse, ging aber nach einigen Tagen wieder zurück.[6]



Quellen: ¹ Statista / DataReportal ² Statista / Business of Apps ³ Statista ⁴ Quiver Quantitative / Wikipedia ⁵ Statista / Business ⁶ Mastodon



Löcher im Unterbau

Sicherheitsrisiken von UEFI-BIOS-Versionen ohne Support

Alle paar Wochen tauchen neue BIOS-Sicherheitslücken auf. Doch die meisten älteren PCs, Notebooks und gebrauchten Computer erhalten keine BIOS-Updates mehr. Es stellt sich die Frage, wie unsicher solche Rechner sind – wir versuchen eine Antwort.

Von Christof Windeck

Wenn ein Betriebssystem keine Sicherheitsupdates mehr bekommt, raten Experten von der Nutzung ab. Denn es ist weniger sicher als eines, das noch mit Updates versorgt wird. Da stellt sich die Frage, welche Risiken ein PC-BIOS birgt, für das es keine Updates mehr gibt. Denn immer wieder tauchen Sicherheitslücken auch im UEFI-BIOS auf. Wer einen alten Computer nutzt, sollte das damit verbundene Risiko abwägen.

Firmware-Gefahren

Wurde der BIOS-Code kompromittiert und darin etwa Schadcode verankert, ist der Computer unsicher. Ein Virenscanner, der unter dem Betriebssystem läuft, kann derartige „Bootkits“ nur schwer entdecken. Der BIOS-Code läuft sozusagen eine Ebene tiefer und lässt sich auch nicht mit Windows-Standardfunktionen komplett aus dem Flash-Chip des Mainboards auslesen, um ihn zu prüfen.

Es ist nicht nur schwierig, manipulierte Firmware zu finden, sondern auch, sie zu beseitigen. Denn sie übersteht die Neuinstallation des Betriebssystems, das Löschen der Festplatte und selbst deren physischen Austausch. Auch wenn man ein BIOS-Update einspielt, löscht es nicht zwingend sämtliche Spuren des Vorgängers, denn nicht jedes BIOS-Image füllt die gesamte Flash-Kapazität. Im Extremfall muss man den ganzen Computer entsorgen. Deshalb gelten Firmware-Attacken als besonders heimtückisch.

Einige nachgewiesene Firmware-Attacken zielen darauf, die SSD-Verschlüsselung per BitLocker auszuhebeln, um an geschützte Daten zu kommen. Im manipulierten BIOS-Code können Angreifer etwa Keylogger unterbringen, die Passworteingaben mitschneiden, oder Funktionen zum Nachladen von Schadcode.

Obwohl Angriffe auf die Firmware also sehr mächtig sind, kommen sie im Vergleich zu Windows-Malware oder Attacken auf Browser sehr selten vor. Das hat einen einfachen Grund: Windows und Browser laufen in ähnlichen Versionsständen auf Millionen Computern. Dadurch entfalten Malware-Angriffe auf diese Ziele breite Wirkung. Es gibt vielseitige Bausätze für solche Malware und man kann sogar standardisierte Ransomware-Attacken per Darknet in Auftrag geben.

Im Vergleich dazu ist der Angriff auf ein UEFI-BIOS sehr viel schwieriger, weil man ihn für eine bestimmte Computer-

serie auf Maß schneidern muss. Selbst ähnliche Notebooks desselben Herstellers laufen manchmal mit ganz unterschiedlicher Firmware, haben also nicht dieselben Schwachstellen.

Schon deshalb entfaltet ein BIOS-Angriff keine Breitenwirkung. Viele nachgewiesene Firmware-Angriffe wie BlackLotus [1], CosmicStrand, ESPecter, LoJax und MosaicRegressor [2] zielten daher auf Notebooks besonders gefährdeter Einzelpersonen, etwa von Gegnern der nordkoreanischen Diktatur. Auch Ermittlungsbehörden nutzen sie manchmal, um digitale Beweise zu ergattern.

Ein Großteil der bekannten BIOS-Lücken lässt sich zudem nicht so einfach von Malware aus dem Netz ausnutzen, sondern benötigt etwa die Ausführungsrechte eines angemeldeten Administrators; im Branchenjargon spricht man von „privileged User“. Derartige Sicherheitslücken lassen sich also nicht so einfach mit Schadcode ausnutzen, die man per Mail oder Browser aufs System bringt. Manche BIOS-Schwachstellen, etwa Fehler in der Authentisierung lokaler Nutzer (BIOS-Passwort), kann sogar nur ein Angreifer missbrauchen, der physischen Zugriff auf das System hat (physical Presence). Ein typisches Szenario ist das der „bösartigen Reinigungskraft“ (Evil Maid), die unbeobachtet etwa im Hotelzimmer einige Minuten Zugriff auf ein Notebook hat und manipulierte Firmware aufspielt. Doch was bisher galt, kann sich jederzeit ändern: Im Prinzip kann morgen eine schwere BIOS-Sicherheitslücke auftauchen, die aus dem Internet angreifbar ist. Liefert der PC-Hersteller dann keinen Patch, hat man ein Problem.

Was Pessimisten befürchten

Manche Experten raten zur Entsorgung von Rechnern, für die es keine Firmware-Updates mehr gibt. Das ist zumindest für Notebooks von Geheimnisträgern nachvollziehbar, die gestohlen oder unbemerkt manipuliert werden könnten, um ihre verschlüsselte SSD zu entsperren. Aber es trifft auch gewerblich genutzte Rechner, weil der Schutz gegen Malware auch bei Datenschutz und Haftung eine Rolle spielt, Stichwort DSGVO: Käme es durch eine bekannte BIOS-Sicherheitslücke beispielsweise zu einem Diebstahl sensibler Kundendaten, müsste sich der zuständige Admin wohl auf peinliche Fragen gefasst machen. Bei der gewerblichen Speicherung und Verarbeitung sensibler Daten auf einem Rechner ohne Support – also auch ohne BIOS-Updates – rutscht man also in eine juristische Grauzone.

Viele Nutzer spielen allerdings sogar verfügbare BIOS-Updates nicht ein, wenn sie dazu gezielt eine Software herunterladen und dann auch noch von Hand installieren müssen. Daher haben die meisten Business-Notebooks vorinstallierte Tools, die das automatisch erledigen. Bei Lenovo heißt es „Vantage“. Sicherheitsrelevante Firmware-Updates erscheinen bei neuen Geräten nicht selten. Im Verlauf eines Jahres nach dem Kauf 2022 lieferte Lenovo für das ThinkPad Carbon X1 Gen 10 sechs BIOS-Updates, von denen drei mindestens als „wichtig“ eingestufte Sicherheitslücken schlossen. Außerdem kamen drei Updates für die Firmware der Intel Management Engine (ME/CSME).

Update-Automaten haben jedoch Nebenwirkungen. So wurden per Windows Update etwa schon unpassende Firmware-Updates verteilt [3]. Außerdem können Firmware-Updates den Funktionsumfang des Geräts verändern. Und wenn sich etwas am Firmware-TPM ändert, kann es nötig werden, anschließend den Wiederherstellungsschlüssel für die BitLocker-Verschlüsselung der SSD neu einzugeben. Hat man diesen nicht zur Hand – etwa auf einer (Dienst-)Reise –, kommt man nicht mehr an seine Daten heran.

c't kompakt

- Schwachstellen im (UEFI-)BIOS können nur Updates des jeweiligen Geräteherstellers (Notebook, PC, Mainboard) schließen.
- Nach dem Support-Ende gibt es keine Updates mehr; folglich bleiben Sicherheitslücken offen.
- Wie schwer die daraus entstehenden Risiken wiegen, hängt von mehreren Faktoren ab, etwa der Sensibilität der auf dem PC gespeicherten Daten.

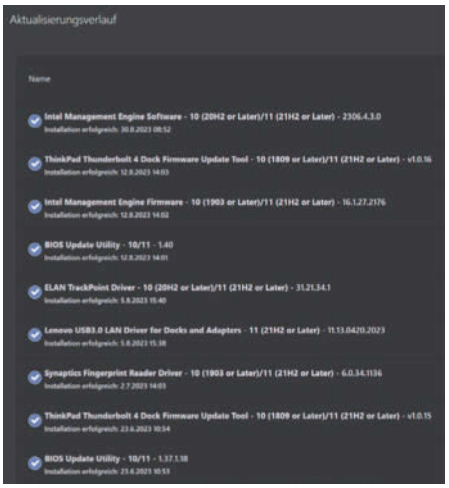
Sichere Konfiguration des BIOS-Setup

Sicherheitsfunktionen des UEFI-BIOS konfiguriert man per BIOS-Setup. Zwei Maßnahmen sind besonders wichtig: Stellen Sie sicher, dass Ihr PC UEFI Secure Boot nutzt, und vergeben Sie ein sicheres Passwort für den Zugriff aufs BIOS-Setup.

Mit UEFI Secure Boot lädt das BIOS nur kryptografisch signierte Bootloader, um Manipulationen zu erschweren. Secure Boot funktioniert nur, wenn das Betriebssystem im UEFI-Modus startet. Den zum alten BIOS kompatiblen „Legacy“-Bootmodus sollten Sie deshalb abschalten. UEFI Secure Boot ist bei den meisten Rechnern mit vorinstalliertem Windows 10/11 automatisch aktiv.

Ein BIOS-Passwort erschwert es Unbefugten, Schutzmaßnahmen im BIOS-Setup abzuschalten. Schreiben Sie ein BIOS-Passwort unbedingt auf und legen Sie es beispielsweise mit den Kauf- und Garantiebelegen für das Gerät ab. Gleiches gilt für den Wiederherstellungsschlüssel der Laufwerksverschlüsselung.

Für stärkeren Schutz schalten Sie im BIOS-Setup das Booten von allen anderen (USB-)Datenträgern außer dem mit der Systempartition ab sowie auch das Booten per Netzwerk. Bei manchen Rechnern kann man auch die Erkennung von USB-Eingabegeräten durch das BIOS deaktivieren. Das erschwert aber nicht nur unerwünschte Zugriffe, sondern auch etwa jene, die Sie zur Wartung benötigen. Was wichtiger ist, müssen Sie selbst abwägen.



Die Update-Automatik aktueller Notebooks spielt relativ häufig neue BIOS-Versionen ein, aber auch Sicherheitsupdates für Intels Management Engine.

Trotzdem sind automatische BIOS-Updates per Windows Update eine zentrale Säule im Microsoft-Schutzkonzept „Secured-Core PC“, siehe Kasten unten. Diese Firmware-Updates nutzen das in der UEFI-Spezifikation beschriebene „UEFI Capsule Update“, das auch der Linux Vendor Firmware Service (LVFS) verwenden kann.

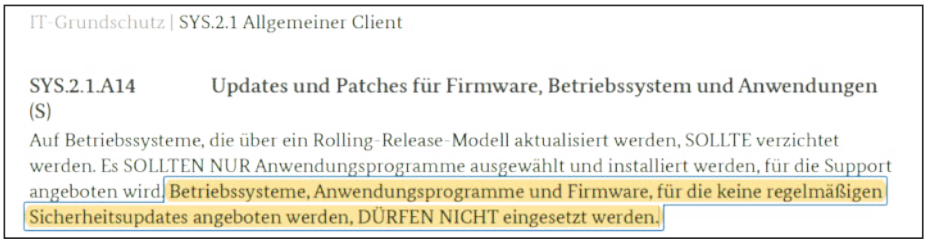
Microsoft arbeitet zudem seit Jahren am Sicherheitscontroller Pluton, der als Hardware-Vertrauensanker (Root of Trust) die Firmware stärker schützen soll als ein standardisiertes Trusted Platform Module (TPM 2.0). Bei Pluton orientiert sich Microsoft an Vorbildern wie Apple (T2) und Google (Titan).

Was Optimisten sagen

Obwohl Millionen Notebooks und PCs niemals ein BIOS-Update erhalten, sind Malware-Angriffe per BIOS sehr selten. Und wie oben erwähnt sind manche Firmware-Manipulationen nur dann durchführbar, wenn der Angreifer physischen Zugriff auf den Rechner hat. Das stellt ein geringes Sicherheitsrisiko dar, wenn der PC in einem Büro steht – zumindest wenn letzteres außerhalb der Arbeitszeiten abgeschlossen ist und sonst nur vertrauenswürdiges Personal Zutritt hat. Das betrifft allerdings auch Reinigungskräfte, Hausmeister und Handwerker.

Bei der Mehrzahl der privat genutzten Rechner spielen BIOS-Schwachstellen keine Rolle. Denn wenn noch nicht einmal ein BIOS-Passwort eingerichtet ist, kann jeder, der physischen Zugriff hat, nach Herzenslust im BIOS-Setup herumfuhrwerken, ein anderes Betriebssystem booten oder manipulierte Firmware einspielen. Ist die Platte oder SSD unverschlüsselt, bootet man einfach ein anderes Betriebssystem und kopiert die Daten oder baut die Platte aus. Viele Desktop-PC-Nutzer würden nicht einmal einen per USB angesteckten Keylogger bemerken und erst recht keinen, der sich in einem Kabelstecker oder direkt in der Tastatur versteckt. Gegenbeispiel: Damit Manipulationen am Gehäuse leichter zu erkennen sind, markiert die Firma Nitrokey optional die Schraubenköpfe ihrer Linux-Notebooks, die mit der offenen UEFI-Alternative Coreboot arbeiten.

Zudem ist das BIOS-Passwort bei vielen Rechnern kein unüberwindlicher Schutz, denn selbst bei manchen aktuellen PCs funktionieren Masterpasswörter oder andere Tricks zur Umgehung. Bei manchen hebelt etwa ein BIOS-Update das Passwort aus. Ein c’t-Leser hat sogar einen schon vor 14 Jahren veröffentlichten Trick (siehe ct.de/ydyp) noch erfolgreich bei fünf Jahre alten Business-Notebooks von Fujitsu angewendet. Durch diese Brille betrachtet liegt der Schluss nahe, dass ein BIOS mit Sicherheitslücken kein besonders hohes Risiko birgt.


IT-Grundschutz | SYS.2.1 Allgemeiner Client

SYS.2.1.A14 (S) Updates und Patches für Firmware, Betriebssystem und Anwendungen

Auf Betriebssysteme, die über ein Rolling-Release-Modell aktualisiert werden, SOLLTE verzichtet werden. Es SOLLTEN NUR Anwendungsprogramme ausgewählt und installiert werden, für die Support angeboten wird. Betriebssysteme, Anwendungsprogramme und Firmware, für die keine regelmäßigen Sicherheitsupdates angeboten werden, DÜRFEN NICHT eingesetzt werden.

Das BSI empfahl noch 2021 für den „IT-Grundschutz“, PC-Clients auszumustern, für die es keine Firmware-Updates (mehr) gibt. Diese Anforderung SYS.2.1.A14(S) entfiel mittlerweile jedoch.

Abwägungsfrage

Wie hoch das Sicherheitsrisiko durch ein veraltetes UEFI-BIOS ist, lässt sich nicht pauschal bewerten. Es kommt vielmehr auf das gesamte System sowie seine anderen potenziellen Schwachstellen an.

Attacken auf BIOS-Sicherheitslücken sind kein bloßer Mythos, aber glücklicherweise selten. Bei Windows-Rechnern stellt das BIOS ein relativ kleines zusätzliches Sicherheitsrisiko dar. Denn in Betriebssystem und Anwendungssoftware klaffen viel häufiger Lücken, die sich zudem leichter für Angriffe missbrauchen lassen.

Speichert ein PC besonders schützenswerte Daten, sollte man auf Firmware-Updates achten. Das betrifft vor allem Notebooks, die außerhalb gesicherter Büroräume leicht gestolen werden können. Diese Geräte sollten aber vor allem sorgfältig für maximale Sicherheit konfiguriert sein, um es Angreifern so schwer wie irgend möglich zu machen.

(ciw@ct.de) c't

Notebooks mit besser geschütztem BIOS

Seit 2019 gibt es von großen Notebookherstellern wie Dell, HP, Lenovo und Microsoft sogenannte „Secured-Core PCs“. Diese Mobilrechner haben jeweils ein UEFI-BIOS, das bestimmte von Microsoft festgelegte Kriterien erfüllt. Außerdem bauen Dell, HP und Lenovo auch noch jeweils proprietäre Schutzfunktionen für die Firmware ein.

Für einen Secured-Core PC (SCPC) verlangt Microsoft etwa Tabellen im BIOS, die den Zugriff auf RAM-Adressbereiche des System Management Mode (SMM) einschränken (SMM Protection). Damit Windows Manipulationen an der Firmware enttarnen kann, schreibt ein sogenanntes Dynamic Root of Trust for Measurement (DRTM) Hashes in bestimmte Register des Trusted Platform Modules (TPM). Zudem muss der Hersteller eines SCPC BIOS-Updates via Windows Update ausliefern.

HP nennt seine zusätzlichen Firmware-Schutzmaßnahmen Sure Start, Dell SafeBIOS. Einige dieser Systeme binden Funktionen der CPU-Hersteller ein wie Intel BootGuard, Trusted Execution Technology (TXT) und Hardware Shield sowie AMD Platform Secure Boot (PSB). Microsoft hat den Sicherheitscontroller Pluton entwickelt, den AMD und Qualcomm in ihre Prozessoren integrieren. Apple-Geräte prüfen ihre Firmware mit dem hauseigenen Sicherheitscontroller T2, Google setzt bei Chromebooks auf den Titan-Chip. Wie stark diese komplexen Funktionen konkret schützen, lässt sich aber schwer einschätzen.

Literatur

[1] Christof Windeck, Nutzlose Notbremse, Microsoft reagiert unentschlossen auf eine BIOS-Sicherheitslücke, c’t 8/2023, S. 36

[2] Christof Windeck, Extrem selten, extrem gefährlich, Bootkit infiziert UEFI-BIOS, c’t 23/2020, S. 38

[3] Christof Windeck, BIOS-Bombe, Wie Windows Update HP-Notebooks mit AMD Ryzen lahmlegte, c’t 7/2020, S. 136

BIOS-Passwort löschen: ***ct.de/ydyp***

Feiern Sie Advent in Nerdistan!

Verpassen Sie kein Türchen!

Freuen Sie sich ab 1. Dezember auf tolle Deals und attraktive Gewinne im heise-Adventskalender!

- Exklusive Gratis-Software von heise Download
- Gratis-Magazine
- Mega-Schnäppchen vom heise Shop
- Gewinnspiele mit tollen Gewinnen

heise.de/advent23

heise medien

Heise Medien GmbH & Co. KG · Karl-Wiechert-Allee 10 · 30625 Hannover

Bild: KI Midjourney | Bearbeitung c't

Unter Beobachtung

Smartphonehersteller mit Staatsauftrag: Wie Honor aus Huaweis Schatten tritt

Seit drei Jahren ist der Smartphonehersteller Honor selbstständig. In China ist das Unternehmen Marktführer, in Europa ein schlafender Riese. Das könnte sich bald ändern – und die USA schauen genau hin.

Von Robin Brand

Es ist eine bedeutsame Bühne, die George Zhao am 1. September 2023 in Berlin betritt. Doch so viel zu zeigen hat er gar nicht: Das eine Smartphone ist in China längst vorgestellt, das andere nur ein Konzept. Aber das ist zweitrangig an diesem Tag, an dem der Geschäftsführer des Smartphoneherstellers Honor die Eröffnungs-Keynote der IFA hält. Die Nachricht ist eine andere. Über Jahre hat hier der einstige Mutterkonzern Huawei die großen Keynotes gehalten, doch der spielt als Smartphonehersteller kaum mehr eine Rolle in Europa. Stattdessen schickt sich Honor an, den Platz im Rampenlicht zu übernehmen.

Wenige Wochen später, am 17. November 2023, ist Honor genau drei Jahre selbstständig. In Europa kennen nur wenige das Unternehmen, doch in China ist es in Rekordzeit zum Marktführer aufgestiegen. Das wirft die Frage auf, ob Honor nur eine neue Hülle für Huaweis Smartphonegeschäft ist. Und, ob die Marke bald auch in anderen Märkten so groß werden kann wie einst Huawei oder ob die USA das mit Sanktionen verhindern würden.

Das Jahr 2020 neigt sich dem Ende entgegen, als der Druck für Huawei zu groß wird. Aufgrund der US-Sanktionen sieht sich das Unternehmen gezwungen, die Smartphone-Tochtermarke Honor zu

verkaufen. Ein Konsortium staatlich kontrollierter chinesischer Unternehmen kauft sie für umgerechnet rund 12 Milliarden Euro. Honor, zu Huawei-Zeiten auf günstigere Smartphones spezialisiert, erweitert unter neuer Führung sein Sortiment zügig um High-End-Modelle und wird mehr oder weniger aus dem Stand zu einem der größten Smartphoneproduzenten in China.

Im Auftrag des Staates

Der Aufstieg im Heimatland verläuft in atemberaubender Geschwindigkeit. Kaum ein Jahr selbstständig, eröffnet Honor mitten in der Coronapandemie im November 2021 in der „Pingshan High Tech Zone“ im Nordosten Shenzhens eine in Windeseile hochgezogene Fabrik, um die Nachfrage vor allem im heimischen Markt zu bedienen. Im selben High-Tech-Park produziert auch das Halbleiterunternehmen Semiconductor Manufacturing International Corporation (SMIC). BYD, der weltgrößte Akkuhersteller, hat hier seinen Unternehmenssitz.

Innerhalb dieses chinesischen Prestigeprojekts nimmt Honor eine exponierte Stellung ein. Denn während bei Huawei die Firmenstrukturen stets undurchsichtig blieben, ist bei Honor klar, dass der Staat das Sagen hat (siehe Interview auf der nächsten Seite). Dass das Unternehmen Erfolg hat, ist somit eine Frage von staatlicher Tragweite – erst recht, nachdem der Fall Huaweis gezeigt hat, wie hart US-Sanktionen einen chinesischen Tech-Giganten treffen können. Zu Beginn konzentriert sich Honor auf den heimischen Markt. Vermutlich auch, um nicht direkt ebenfalls Ziel von US-Sanktionen zu werden.

In Honors neuer „Smart Factory“ im High-Tech-Park läuft die Produktion von nicht faltbaren Smartphones vom Start weg zu 75 Prozent automatisiert ab, später steigert das Unternehmen die Automatisierung gar auf 80 Prozent, sagt Alex Pang, Director of Manufacturing. Pro Produktionsstraße sind nur 21 Mitarbeiter nötig. Aus jeder der 150 Meter langen Produktionslinien purzelt alle 28,5 Sekunden ein fertiges Smartphone. Die Gesamtproduktionszeit pro Gerät liegt bei 40 bis 50 Stunden, je nach Modell.

Schon im ersten Quartal nach der Eröffnung der neuen Smart Factory kann Honor einen Meilenstein verkünden: Erstmals ist das junge Unternehmen größter Smartphoneproduzent in China. Ganze 15 Millionen Handys verkauft das Unternehmen in den ersten drei Monaten des Jahres 2022, schätzen Analysten von Canalys – allein in China. Dabei profitiert Honor auch vom ehemaligen Huawei-Know-how. Durch das gemeinsame Erbe sei man in der Lage gewesen, „auf einem viel höheren Level mit den eigenen Entwicklungen einzusteigen“, teilt ein Unternehmenssprecher auf unsere Anfrage mit. Wie viele Ingenieure genau von Huawei zu Honor gewechselt sind, verrät das Unternehmen nicht, aber: 8000 der 13.000 Honor-Beschäftigten arbeiteten im Bereich Forschung und Entwicklung. Sieben Entwicklungszentren betreibt Honor weltweit.

Honor-Launch in China ein Großereignis

Ohne die Zwänge der gemeinsamen Unternehmenspolitik mit Huawei schielt Honor von Anfang an auch aufs High End und will eigene Expertise in der Fertigung von faltbaren Smartphones aufbauen, der Königsdisziplin des Smartphonebaus. Anfangs habe man dabei Verluste eingefahren, gibt Zhao am Rande eines Gruppeninterviews zum Launch des Magic V2 in Peking gegenüber c’t zu. Doch mit dem chinesischen Staat im Rücken ist Geld nicht das Problem.

Es dauert nicht lange, bis die Investitionen Früchte tragen: Im Sommer 2023 stellt Honor mit dem Magic V2 das bis dahin dünnste Foldable der Welt vor, zusammengeklappt ist es weniger als einen Zentimeter dick. Zhao sieht das Gerät als Wegbereiter für Foldables auf dem Weg zum Massenprodukt, das herkömmliche Smartphones verdrängt. Zumindest in China scheint die Nachricht zu verfangen. Tausende strömen zum Launch-Event ins ehemalige Olympia-Schwimmzentrum am nördlichen Stadtrand Pekings.

Außerhalb Chinas verläuft das Wachstum der ehemaligen Huawei-Tochter dagegen verhältnismäßig langsam. Analysten von Counterpoint Research beziffern den Marktanteil im Jahr 2022 in Europa auf 2,3 Prozent. 95 Prozent der Gesamteinnahmen stammen demnach aus dem Asien-Pazifik-Raum.

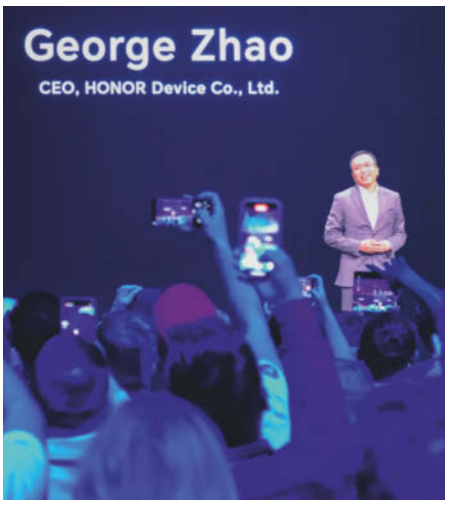
Eine Ursache, warum sich Honor auf den Heimatmarkt konzentriert, liegt zu diesem Zeitpunkt erst ein paar Monate zurück. Im Herbst 2021 treffen sich nach einem Bericht der Washington Post Vertreter des US-Außen-, Handels-, Verteidigungs- und Energieministeriums, um über Honor zu beraten. Dass die ehemalige Huawei-Tochter nach dem Verkauf weiter auf westliche Hard- und Software zugreifen kann, ist einigen von ihnen ein Dorn im Auge. Ihrer Ansicht nach hat sich Peking durch die Ausgliederung Honors der US-amerikanischen Exportkontrolle entzogen.

Dem Bericht zufolge sprechen sich Beamte des Energie- und des Verteidigungsministeriums dafür aus, auch die ehemalige Huawei-Tochter auf die sogenannte Entitätsliste zu setzen. Damit verlöre Honor unter anderem die Möglichkeit, seine Smartphones mit 5G-Chips und Google-Diensten auszustatten. Außen- und Handelsministerium stimmen dagegen – mit Erfolg. Bis heute verzichtet die US-Politik auf Maßnahmen gegen Honor. Doch die Botschaft dürfte angekommen sein, in Sicherheit wiegen kann sich Honor nicht.

Honor wäre das erste Sanktionsziel

Ein zu großer und zu schneller Erfolg vor allem im Westen könne Honor zur Zielscheibe von Sanktionen machen, schätzt Kai von Carnap, ehemaliger Analyst des Mercator Institute for China Studies und heute unabhängiger Forscher (gesamtes Interview siehe Kasten auf S. 116). Dass die USA und China zwischenzeitlich auch mal um entspanntere Beziehungen miteinander bemüht seien, müsse nichts heißen. „Honor wäre eine der ersten Zielscheiben, wenn es wieder in angespanntere Zeiten geht“, ist sich von Carnap sicher.

Bis heute ist Honor in den USA nicht aktiv. Ob das auch mit dem Huawei-Erbe und Sorgen vor drohenden Sanktionen zu



Große Bühne für Honor: Auf der IFA hielt George Zhao die Eröffnungskeynote.

„Honor ist ein staatlicher Handy-Produzent“

Der Chinaexperte Kai von Carnap befasst sich mit der Beziehung zwischen dem Parteistaat und den Informations- und Kommunikationstechnologien (IKT) im Kontext von Chinas digitaler Entwicklung. Zum Zeitpunkt unseres Interviews war er als Analyst für das Mercator Institute for China Studies tätig. Mittlerweile hat er das Institut verlassen und arbeitet als unabhängiger Forscher. Im Interview ordnet er den rasanten Aufstieg Honors in China ein.

c't: In China gehörte Honor nach dem Verkauf an Shenzhen Zhixin New Information Technology Co. Ltd quasi aus dem Stand zu den größten Smartphoneherstellern. Wie kann das sein? Welche Ressourcen hat das Unternehmen dafür genutzt?

Kai von Carnap: Der Erfolg kommt nicht von ungefähr, schon vorher war Honor der erfolgreichste Smartphoneableger von Huawei. Und nachdem Huawei durch US-Sanktionen von wichtigen Zulieferern abgeschnitten war, entstand ein Vakuum, das Honor nutzen konnte. Hinzu kommt, dass weitere US-Sanktionen darauf abzielten, China von der High-End-Chipentwicklung abzuhalten, und das sind nicht die Chips, die wichtig für die Entwicklung von Smartphones sind. So konnte Honor mit dem großen staatlichen Konglomerat um Shenzhen Zhixin im Hintergrund weiter auf globale Netzwerke zugreifen und im Schatten der Huawei-Sanktionen seine Smartphoneentwicklung weiter vorantreiben. Allerdings sind die Verbindungen zwischen Honor und seinem ehemaligen Mutterkonzern Huawei bis heute relativ fragwürdig, genau wie unklar ist, wie viele staatliche Fördermittel und Subventionen in den vergangenen Jahren an Honor geflossen sind.

c't: Honor selbst ist stets darum bemüht, seine Unabhängigkeit von Huawei zu betonen. Glauben Sie, die Unternehmen sind im Hintergrund noch miteinander verbandelt?

von Carnap: Auf dem Papier hat man sich offiziell getrennt. Aber vom Topmanagement und mittleren Management bis hin zum Zulieferer- und Vertriebsnetzwerk ist die Firma die gleiche. Auch in der Unternehmenskultur von chinesischen Techkonglomeraten ist es unwahrscheinlich, dass sich ein solches über Nacht trennt. Wir sehen das auch bei Alibaba, das dabei ist, sich in sechs verschiedene Bereiche aufzuspalten. Alibaba versucht, sich durch diesen Kompromiss an geopolitische Spannungen anzupassen und gleichzeitig so wenige Strukturen wie möglich aufzugeben.

Auf ähnliche Weise entwickeln sich Honor und Huawei vordergründig zu Wettbewerbern. Aber wenn es darum geht, ausländische Technologie zu akquirieren, kann ich mir vorstellen, dass es aus staatlicher Lenkungssicht eine Win-Win-Situation ist: Man kann einerseits über das Konstrukt Honor/Shenzhen Zhixin weiter Technologie und Materialien aus dem Ausland nach China bringen und möglicherweise an Huawei weiterreichen. Auf der anderen Seite kann Huawei R&D-Erkenntnisse über die Smartphoneentwicklung an Honor weitergeben.

c't: Im Unterschied zu den Eigentumsverhältnissen bei Huawei macht China kein Geheimnis um die Mehrheiten bei Honor.

von Carnap: Genau, das ist ganz klar ein Staatsunternehmen. Hauptanteilseigner ist Shenzhen Smart City Technology, ein staatliches Unternehmen, mit einem Anteil von mehr als 95 Prozent. Generell hat der chinesische Staat schon immer großen Einfluss speziell auf den IKT-Sektor ausgeübt. Seit etwa 2017 ist zu beobachten, dass er auch zunehmend auf die Consumer-Industrie, also auf die Internetplattformen und die Hersteller von Handhelds, mehr Einfluss nimmt. Das geschieht auf verschiedenen Wegen, zum Beispiel über sogenannte Golden Shares, also Minderheitsbeteiligungen von 1 Prozent, die der Staat zum Beispiel an Internetplattformen hält und darüber in strategische Entscheidungen der Unternehmen eingreift. Ein anderer Weg ist, wie wir es bei Honor gesehen haben, einfach Firmenanteile komplett zu übernehmen. Honor ist, wenn man so will, ein staatlicher Handyproduzent. Im Falle Honor glaube ich aber nicht, dass es von langer Hand geplant war. Das Konstrukt war einfach eine Reaktion auf die politischen Gegebenheiten.

c't: Kann man bei den größeren chinesischen Herstellern wie Oppo und Xiaomi immer davon ausgehen, dass der Staat über Golden Shares mit drin ist?

von Carnap: Im Falle Oppo und BBK oder auch Xiaomi sind keine Diskussionen über

tun hat, beantwortet das Unternehmen nicht, sondern betont lediglich, dass es seit 2020 unabhängig sei. Und als unabhängiges Unternehmen verpflichte es sich „zur Einhaltung aller Gesetze und Vorschriften in jedem Land, in dem wir tätig sind“.

In anderen westlichen Märkten verfolgt Honor dagegen eine Strategie des langen Atems. Wo Huawei einst aggressiv und schnell Marktanteile eroberte und gerne mal Stärke demonstrierte, hört man von Honor wenig markige Worte. Bald nach der Ausgründung beginnt Honor zwar, Smartphones in Europa zu verkaufen. An die Zahlen der chinesischen Konkurrenten Oppo oder Xiaomi kommt der Konzern allerdings nicht heran, von Branchengrößen wie Apple und Samsung ganz zu schweigen. CEO George Zhao betont, man wolle Schritt für Schritt wachsen in Europa.

Doch speziell in Deutschland, dem größten Smartphonemarkt in Europa, dürfte Honor schon bald größere Schritte machen. Einerseits verkauft Honor hier relativ wenige Smartphones, auch für europäische Verhältnisse. Genügend Raum für Wachstum gäbe es also. Zudem tun sich hier besondere Möglichkeiten auf: Die Marken des BBK-Konzerns, darunter Oppo, OnePlus, Vivo und Realme, dürfen aufgrund von Patentstreitigkeiten mit Nokia ihre Smartphones nicht in Deutschland verkaufen und blicken in eine ungewisse Zukunft.

Außerdem ist der deutsche Markt besonders attraktiv, da deutsche Konsumenten sich ihre Smartphones viel kosten las-

Golden Shares bekannt. Es gibt aber über Parteizellen andere Kanäle für staatliche Einflussnahme. Diese kann sich auf verschiedene Weisen erkennbar machen, ist aber meistens vergleichsweise gering. Man kann davon ausgehen, dass der Großteil der strategischen Entscheidungen und der R&D-Entwicklung unabhängig von Staatsinteressen ist.

c't: In China gehört Honor zu den Marktführern, im Westen hat das Unternehmen nur geringe Marktanteile. Der CEO sagt, man könne nur Schritt für Schritt wachsen. Ist das einfach der Versuch, unter dem Radar zu bleiben, damit man nicht plötzlich auch auf der Sanktionsliste der USA landet?

von Carnap: In der aktuellen Lage müssen sich alle chinesischen Tech-Hersteller die Frage stellen, ob sie in den kommenden Monaten von den USA sanktioniert werden könnten. Und so erklärt sich Honors Schritt-für-Schritt-Narrativ ganz gut. Das Unternehmen ist eben bemüht, unter dem Radar der Geopolitik zu bleiben, weil es möglichst nicht mit Huawei assoziiert werden und die Frage der staatlichen Hilfsmittel nicht aufkommen lassen will. Als Handyhersteller muss Honor sich doppelt Sorgen machen. Ein erfolgreiches Unternehmen Honor, das Millionen von Smartphones mit eigenen Cloud-Services und chinesischen Apps im Westen verkauft, stellt gerade aus amerikanischer Sicht natürlich ein riesiges Sicherheitsproblem dar. Daher könnte ein zu großer und zu schneller Erfolg Honor zur Zielscheibe möglicher Sanktionen machen. Auf der anderen Seite gibt es in den letzten Wochen und Monaten Annäherungsversuche zwischen den USA und China, um die wirtschaftlichen und die technologischen Beziehungen aufrechtzuerhalten. Aber es kann genauso gut in den nächsten Monaten wieder in die andere Richtung umschwenken. Und sollte Trump nächstes Jahr wieder gewählt werden, sieht es mit dem gegenseitigen Austausch wieder ganz anders aus. Honor wäre eine der ersten Zielscheiben, wenn es wieder in angespanntere Zeiten geht.

c't: Die Schritt-für-Schritt-Taktik bedeutet gleichzeitig eine Abkehr vom einstigen Erfolgsrezept von Huawei, das sehr aggressiv Wachstum auf dem europäischen Markt forciert hat.

von Carnap: Auch da spielen die Sanktionen eine Rolle: Honor kann die Märkte gar nicht ähnlich aggressiv erschließen, weil es die Produktionskapazitäten noch nicht hat. Man kann also einerseits eine große Nachfrage im Westen nicht bedienen, will es andererseits auch noch nicht, weil zu starkes Wachstum mit Sanktionen quittiert werden könnte. Gleichzeitig versuchen sich die chinesischen Smartphonehersteller unabhängiger von US-kontrollierten Zulieferern zu machen. Rein theoretisch ist das Know-how da, die Smartphones selbst zu bauen. Aber China muss erst die heimische Chipproduktion ausbauen und sich im Bereich Software unabhängig machen. Von daher ist es smart von Honor, die heimischen Produktionsmöglichkeiten mit den geopolitischen Spannungen in Balance zu halten.

Bild: Mercator Institute for China Studies

Chinaexperte Kai von Carnap: „Wenn es in angespanntere Zeiten geht, wäre Honor eine der ersten Zielscheiben."

c't: Könnten sich Huawei, Honor & Co. künftig unabhängig machen von westlichen Zulieferern?

von Carnap: Dass Tech-Unternehmen im 21. Jahrhundert vollkommen unabhängig werden von globalen Netzwerken und Zulieferern, sehe ich nicht. Alleine in der Halbleiterproduktion – selbst wenn der Großteil nach China verlegt wird –, werden Produzenten in irgendeiner Form immer von ausländischen Zulieferern abhängig sein. Eine hundertprozentige Handyautarkie wird es nicht geben. Weder für Honor, noch für Huawei, aber genauso wenig für Apple, Samsung oder Nokia. Die Frage ist, wie kann man sich in den entscheidenden Teilen der Lieferketten und Produktionsabläufe unabhängig machen, um im globalen Markt mögliche Alternativen zu haben. Das wird ein langer Weg, diese entscheidenden Produktionsunabhängigkeiten zu erreichen, der in fünf Jahren nicht gegangen ist.

sen, nach Bitkom-Zahlen 563 Euro im Schnitt. Honor, als Huawei-Tochter noch der Billigheimer im Konzern, kann nun die hochpreisigen Smartphones, die große Margen erzielen, selbst verkaufen. Allerdings tut sich der Konzern im Westen schwer, das Image als Produzent günstiger Smartphones abzulegen. Wer mehr Geld für ein Smartphone ausgibt, greift lieber zu Apple oder Samsung.

Kein Wunder also, dass George Zhao die große Bühne auf der IFA nutzt, um Honor als Innovationstreiber zu inszenieren. Schließlich ist es Honor, das gerade in China das dünnste Foldable der Welt vorgestellt hat und schon an noch dünneren Konzept-Phones arbeitet, so das Narrativ des CEOs. Und tatsächlich zeigen erste Zahlen, dass das V2 in China ein Verkaufsschlager werden könnte. Dass er mit dieser Nachricht in Europa durchdringt, scheint Zhao indes selbst noch nicht so recht zu glauben. Während das Magic V2 in China längst erhältlich ist, stehen in Deutschland auch zwei Monate nach der IFA-Keynote weder ein Starttermin noch Preise fest. Im eher konservativen europäischen Smartphonemarkt müssen es vorerst weiterhin die klassischen, nicht faltbaren Smartphones richten.

(rbr@ct.de) c't

Hinweis: Ein Teil der Recherche fand während des Magic-V2-Launchs in Peking statt. Honor hat die Reisekosten des Autors übernommen.

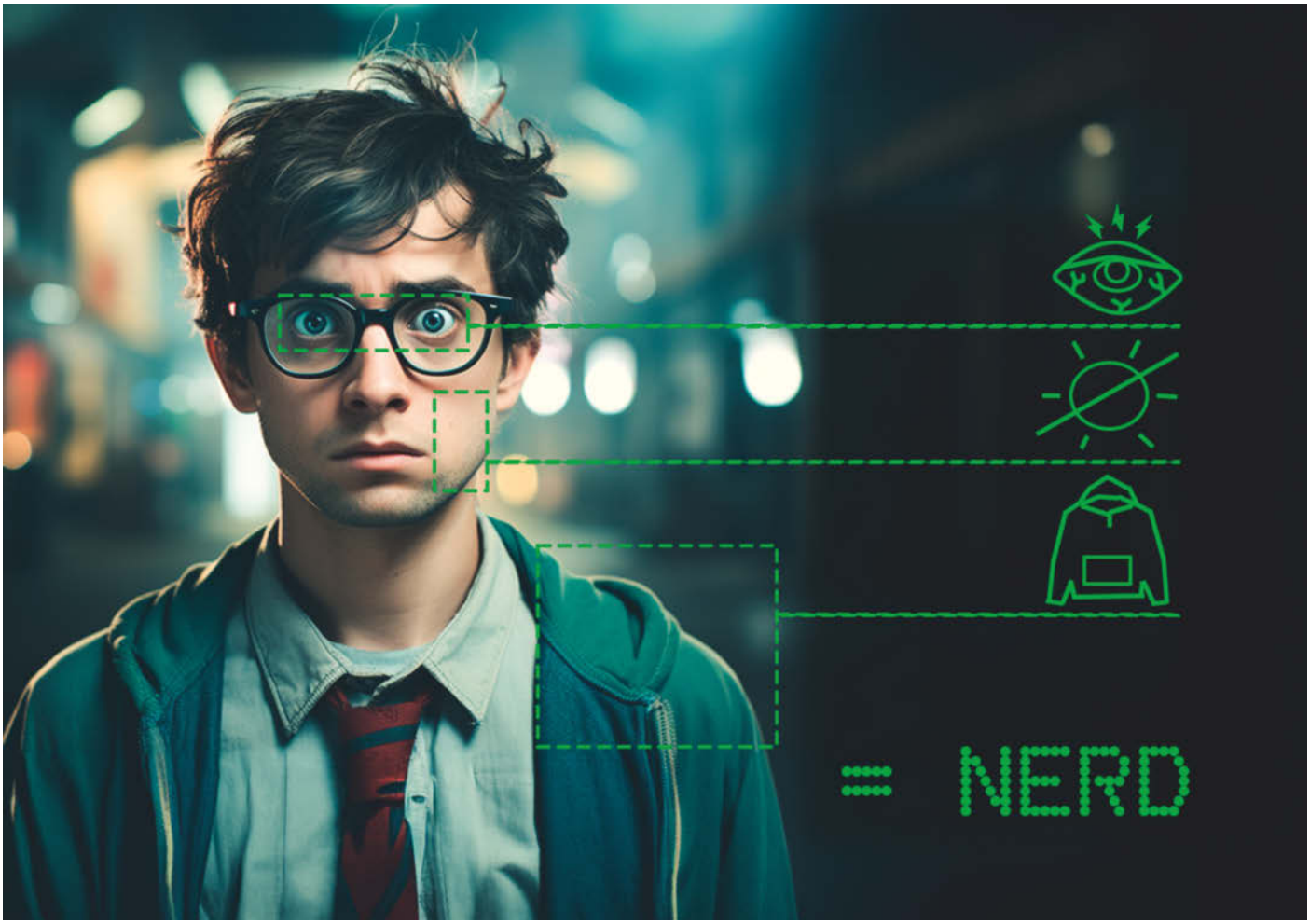


Bild: KI Stable Diffusion | Bearbeitung c't

So denkt die KI

Verfahren findet Denkkonzepte wie beim Menschen in neuronalen Netzen

Bisher markieren Heatmaps, worauf eine künstliche Intelligenz besonders achtet, wenn sie etwa ein Bild einordnet. Ein neues Verfahren entlockt leistungsfähigen KIs ihre komplexen Kriterien. Damit können Anwender deren Entscheidungen viel besser nachvollziehen.

Von Arne Grävemeyer

Wie schätzt eine künstliche Intelligenz das Alter einer Person auf einem Foto? Woran erkennt sie ein Rotkehlchen, ein Zebra oder in der dermatologischen Praxis Hautkrebssymptome? Gerade das medizinische Beispiel zeigt, wie wichtig es wäre, die Konzepte genau zu verstehen, die hinter einer KI-Entscheidung stecken. Doch die komplexen Modelle, die in automatisierten Machine-Learning-Prozessen entstehen und sich in Netzen aus Zigtausenden miteinander vernetzten Neuronen manifestieren, offenbaren ihre internen Prozesse nicht so einfach.

Eine Hilfe stellt bislang das LRP-Verfahren (Layer-wise Relevance Propagation). Mit dieser Methode lassen sich die Prozesse im neuronalen Netz zurückverfolgen, schichtweise von der Klassifikation am Ende bis zu den Eingangsdaten auf der Input-Ebene. Bei einem Bilderkenner beispielsweise berechnet das LRP-Verfahren nach einer Entscheidung („es ist ein Zebra“) eine Heatmap. Die hebt genau die Bildpixel hervor, die sich im individuellen Fall am stärksten auf die getroffene Klassifikation auswirkten. In diesem Fall würde die Heatmap wahrscheinlich Bildbereiche

hervorheben, die Streifen im Fell und den pferdeähnlichen Kopf des Tieres zeigen.

Was steckt hinter den Pixeln?

Eine solche Heatmap erklärt manches, lässt aber Interpretationsspielräume offen, wie Wojciech Samek erklärt. Samek ist Leiter der Abteilung KI am Fraunhofer Heinrich-Hertz-Institut (HHI) und hält an der TU Berlin Vorlesungen über maschinelles Lernen. Er zeigt die Heatmap des Fotos einer jungen Frau, deren Alter eine KI auf 25 bis 30 Jahre schätzte; dem Anschein nach liegt sie damit richtig. Hervorgehoben sind Pixel im Bereich des lächelnden Mundes der Frau sowie ihrer Augen. „Was hat aber nun die Entscheidung maßgeblich beeinflusst, die Art des Lächelns, die Form der Lippen, die Farbe der Zähne oder deren Form? Das verrät die Heatmap nicht“, betont Samek.

Die Wissenschaftler sprechen angesichts dieser Unsicherheit vom Interpretation Gap. Die tatsächlichen semantischen Konzepte hinter der KI-Klassifizierung bleiben verborgen. Ebenso ist nicht klar, wie viele unterschiedliche Bewertungsmuster die Entscheidung stützen, für welche dieser Konzepte das einzelne Pixel einen Ausschlag gibt und welchen Anteil die einzelnen Kriterien an der Gesamtentscheidung haben. Heatmaps sagen nur etwas darüber aus, wo etwas Relevantes steckt, sie verraten aber nicht, was daran bedeutsam ist.

Samek und seine Kollegen von HHI, TU Berlin sowie des Berlin Institute for the Foundations of Learning and Data (BIFOLD) suchten nach einer Möglichkeit, das LRP-Verfahren zu erweitern. Ihre Vermutung: Die höheren Schichten eines neuronalen Netzes repräsentieren oftmals für Menschen verständliche Konzepte. In ihrer jüngsten Veröffentlichung stellen die Forscher ihr CRP-Verfahren (Concept Relevance Propagation) vor [3]. Sie zeigen darin, wie sie in leistungsfähigen Modellen die Entscheidungsgrundlagen finden. Und diese semantischen Konzepte gleichen oftmals dem Bild, das sich Menschen von der Welt machen.

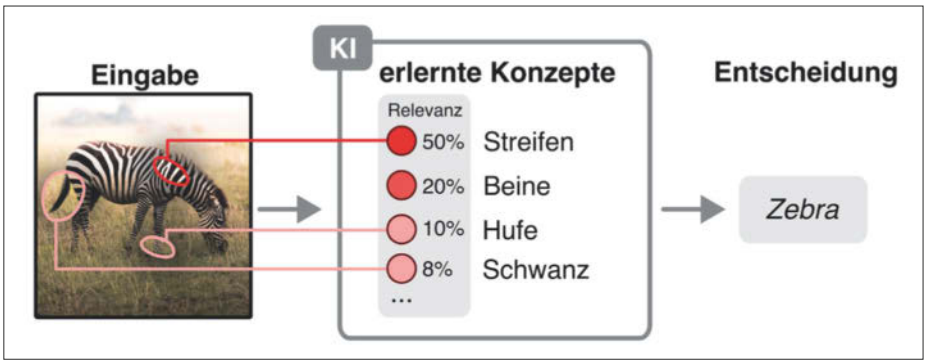


Bild: HHI

Das allerwichtigste an einem Zebra sind die Streifen. Das neue Verfahren erlaubt es dem Anwender, die Konzepte nachzuvollziehen, mit denen eine KI Objekte klassifiziert.

Heatmaps für inhaltliche Konzepte

Das CRP-Verfahren ermittelt zunächst die Relevanz der einzelnen Kanäle in den höheren Schichten des betrachteten neuronalen Netzes unmittelbar vor der Ausgabeschicht. „Diese Relevanzwerte liefert uns die LRP-Methode bereits in ihren ersten Berechnungsschritten“, sagt Samek. CRP rechnet aber nicht wie LRP weiter durch alle Schichten bis auf die Eingangsebene zurück. Stattdessen betrachtet das neue Verfahren die relevantesten Kanäle und berechnet nur für diese die zugehörigen sogenannten Conditional Heatmaps. „Wir berechnen die Verteilung der entscheidenden Pixel auf der Eingangsebene also nur spezifisch für einen Kanal. Die Methodik ist im Übrigen gleich der des LRP-Verfahrens“, erklärt Samek. So entstehen also Heatmaps für die unterschiedlichen Konzepte.

Dabei erkennt man beispielsweise, dass auf dem Foto eines Zebras in der allgemeinen Heatmap zwar der Schwanz und die Hufe betont sind, dass das Kriterium des gestreiften Fells aber viel höher gewichtet ist als „Hufe“ und „Schwanz“. Es verteilt sich nur weniger auffällig auf viel mehr Pixel.

Um die erkannten Konzepte zu beschreiben, bietet das neue Verfahren zwei Wege. Zunächst ermittelten die Forscher, bei welchen Referenzbildern aus den Trainingsdaten eines KI-Modells die Kanäle hohe Werte aufweisen. Diese Beispiele haben in der Regel eine auffällige Gemeinsamkeit und geben damit das zugrundeliegende Muster wieder. Bilder von Zebras, Tigern, Streifenhörnchen, getigerten Katzen und gestreiften Pelzmänteln könnten gemeinsam zum Beispiel das Kriterium „gestreiftes Fell“ abbilden, zumal die dazugehörigen Conditional Heatmaps den Blick zusätzlich auf die Streifenmuster lenken. Ein Anwender kann derart präsen-

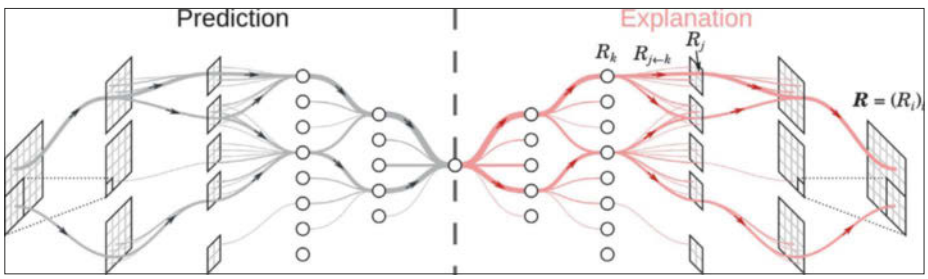


Bild: HHI

Während das neuronale Netz eine Eingabe Schicht für Schicht verarbeitet, um sie zu klassifizieren (linke Seite) kehrt das LRP-Verfahren die Berechnungen um und ermittelt eine Heatmap, die die Bedeutung jedes Eingabepixels für das Endergebnis darstellt (rechts).

c't kompakt

- Eine künstliche Intelligenz gilt als Black Box. Worauf ihre Entscheidungen beruhen, lässt sich kaum prüfen.
- Das neue CRP-Verfahren analysiert neuronale Netze und erkennt deren gelernte semantische Konzepte.
- Diese Muster erklären Entscheidungen in einer Weise, die dem menschlichen Denken entgegenkommt.

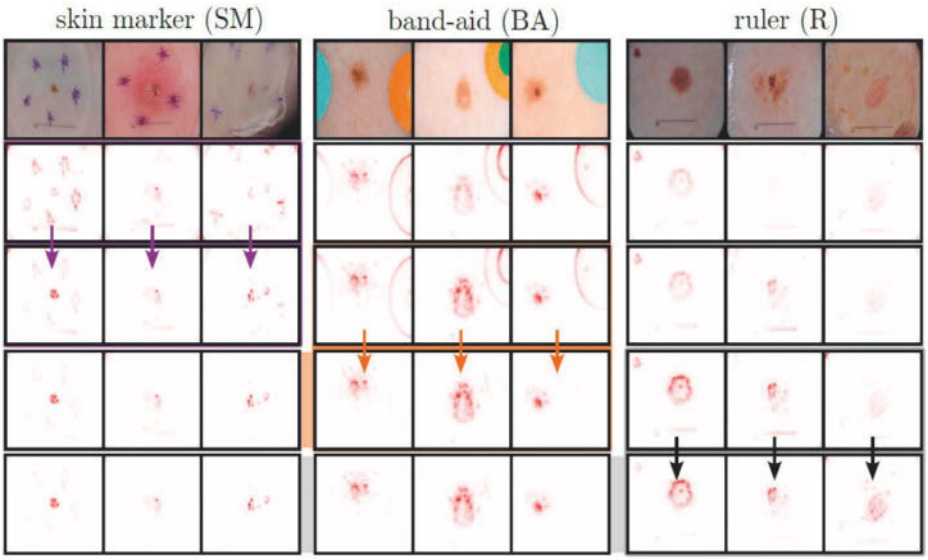


Bild: Lapuschkin, Samek, Wiegand et al.

Markierte Hautmale und bunte Pflaster tauchen in den Heatmaps einer KI zur Hautkrebserkennung auf; sie wurden als Hinweis für ein gefährliches Melanom eingeschätzt. Mit Debugging-Tools legten Forscher die fehlerhaften Zweige des Erkennermodells still und eliminierten den Bias.

tierte Konzepte in der Regel leicht verstehen und auch benennen.

Eine zweite Möglichkeit, Konzepte einzuordnen, bieten Zusatzdaten, die jeweils unter einem Label zusammengefasst sind. Das könnten beispielsweise Bildsammlungen sein, die bestimmte Körperteile hervorheben, Flügel, Hufe, Schnauzen oder Euter. Weitere gelabelte Sammlungen könnten Körper mit Haut, Fell oder Federn umfassen. Auffällige Formen, Farben oder Muster: Für jedes zu erwartende Konzept lassen sich gelabelte Datensätze erzeugen. Der Vorteil dieser Methode besteht darin, dass die Trainingsdaten nicht vorliegen müssen. Außerdem könnte der Anwender, wenn er einmal Datensätze zu passenden Oberbegriffen zusammengestellt hat, damit unterschiedliche KI-Versionen testen. Er kann so automatisiert prüfen, welche Konzepte ein KI-Modell verwendet und in welchen Kanälen der höheren Netzwerkschichten diese repräsentiert sind.

Hautkrebsverdacht begründen

Samek und seine Kollegen versuchen nicht nur, die Konzepte zu entlarven, mit denen man Zebras erkennt oder das Alter von Personen schätzen kann. Das Fraunhofer HHI ist unter anderem am EU-Projekt IToBoS (Intelligent Total Body Scanner for Early Detection of Melanoma) beteiligt und betreut darin Modelle zur Hautkrebserkennung. Woran machen die bestehenden Erkenner fest, dass eine Aufnahme ein gefährliches Melanom zeigt? Ist es die Form, die Farbe oder liegt es an bestimmten Unregelmäßigkeiten?

„Wir haben mit unserer CRP-Methode nachgeschaut, ob KI-Modelle die gleichen festgelegten Kriterien überprüfen, mit denen auch Hautärzte einen Hautkrebsverdacht begründen“, berichtet Samek. Zu seiner Überraschung stieß er in einem großen internationalen Datensatz, der allgemein für das Training von Modellen zur Hautkrebserkennung verwendet wird, auf einen klaren Bias, also verzerrende Trainingsdaten in den verwendeten Fotos: Viele der eingestellten Bilder zeigten nicht nur Hautmale. Vor allem in kritischen Beispielfällen kam es vor, dass Dermatologen die betrachtete Hautstelle vor dem Fotografieren mit dem Kugelschreiber eingerahmt oder mit bunten Pflastern markiert hatten. In einigen Fällen waren auf den Fotos auch Lineale für den Größenvergleich zu erkennen.

Prompt entdeckte die CRP-Methode in der Erkenner-KI die Konzepte „Kugelschreiber-Markierung“, „bunte Pflaster“ und „Lineal am Bildrand“, die die KI offensichtlich als starke Hinweise auf gefährliche Hautveränderungen identifiziert hatte.

Falsche Konzepte ausschalten

Konzepte für erklärbare KI haben in diesem Fall also Fehlverhalten eines KI-Modells entlarvt. Als Konsequenz daraus arbeitet das Team um Samek nun auch an Debugging-Techniken, um fehlerhafte Konzepte auszuschalten.

Ein einfacher Weg wäre es, die Trainingsdaten von den Bildern mit verräterischen Markierungen zu bereinigen und damit dann ein neues Modell zu trainieren. Für den Fall, dass das aber nicht möglich sein sollte, entwickeln die Forscher Werkzeuge, mit denen sie die fehlerhaften Zweige im neuronalen Netz erkennen und stilllegen oder abschwächen. Kontroll-Heatmaps zeigen anschließend, dass der Einfluss der unzulässigen Entscheidungshilfen zurückgeht, wenn auch nicht unbedingt komplett verschwindet. Neuronale Netze verkörpern ihr Wissen in aller Regel redundant verteilt auf mehrere Bereiche.

Im Vergleich zu den Heatmaps des LRP-Verfahrens erklärt CRP das Verhalten einer KI auf einer semantisch abstrakteren Stufe, ganz ähnlich, wie sich Menschen auch untereinander verständigen. Was ist ein Zebra? Es hat einen Kopf wie ein Pferd, Hufe, einen Schweif und – ganz wichtig: Es hat Streifen im Fell. Woran erkennt man den schwarzen Hautkrebs? Da gibt es zum Beispiel Besonderheiten der Form, der Farbe und der Ränder des betrachteten Hautmals.

Mit Debugging-Tools kann der Anwender nicht nur korrigierend eingreifen. Er könnte in Zukunft auch die Bedeutung von Konzepten oder die Robustheit eines Modells interaktiv testen und beispielsweise ausprobieren, wie sich Klassifikationen verändern, wenn er einzelne Beurteilungsmuster abschaltet. Der Erklärprozess könnte also aktiver werden. In Zukunft ist damit eine Art der Diskussion auf einer abstrakten, inhaltlichen Ebene vorstellbar, auf der der Anwender einzelne Konzepte im KI-Modell ein- und ausschalten, verstärken und abschwächen kann.

Neues Wissen aus der KI

Darüber hinaus ist es möglich, dass man die KI anhand von Datensätzen lernen lässt und dann die durch CRP gewonnene Erklärbarkeit nutzt, um neues Wissen aus dem Modell zu ziehen. Das nennen die Wissenschaftler den „explorativen Ansatz“. Dadurch, dass die Modelle die Konzepte offenlegen, die zu ihren Entscheidungen führten, ist es möglich, dass der Anwender neue Zusammenhänge versteht. Das wird vielleicht nicht in der Hautkrebserkennung der Fall sein. Aber schon in mehreren Bereichen der medizinischen

Bild: HHI

Woran erkennt eine KI einen Papageien? Unter anderem an den Augen und dem Federkleid; beispielhafte Bildausschnitte verdeutlichen diese Konzepte.

Radiologie könnten neue Erkenntnisse in komplexeren Daten schlummern, die KI-Modelle erlernen, ohne dass sie bereits von den Medizinern vollständig durchschaut worden sind.

Samek sieht das CRP-Verfahren für erklärbare KI im Übrigen nicht auf Bilddaten beschränkt. Er verweist auf komplexe Datensätze zu Gensequenzen, oder etwa Elektrokardiogramme (EKG), die aufgrund elektrischer Spannungskurven die Leistungsfähigkeit des Herzens darstellen. In derartigen Bereichen, in denen auch Experten erst mühsam lernen müssen, die entscheidenden Strukturen in den Daten und Messkurven zu erkennen, könnten KI-Modelle wohl eher Zusammenhänge finden, die von Menschen bislang übersehen worden sind. Der Austausch in abstrakteren semantischen Konzepten eröffnet dann eine Chance, die Hinweise aus dem KI-Modell zu verstehen, zu untersuchen und dadurch neues Wissen zu gewinnen.

Allerdings ist die Heatmap, die auf Fotos verständliche Hinweise gibt, nicht unbedingt geeignet, um an Sequenzen und EKG-Kurven relevante Eingabepixel zu markieren. Welche Regelmäßigkeiten oder Unregelmäßigkeiten im EKG sind von Bedeutung, was bedeutet ein bestimmter Peak? Es ist eine Herausforderung, Konzepte einer KI auf diesen Daten so hervorzuheben, dass die Forscher und Mediziner, die damit arbeiten, darin etwas erkennen können. Ebenso müssen die KI-Forscher neue Wege gehen, Konzepte aus den Modellen darzustellen und anschließend auch zu benennen.

Spracherkenner verraten Dialekte

In einer aktuellen Arbeit versuchen Samek und sein Team, wie sie das CRP-Verfahren auch auf Spracherkenner anwenden können. Es geht um Fragen wie: An welchen Sequenzen einer Audioaufnahme erkennt man einen bestimmten Dialekt oder welche Kombinationen deuten auf eine bestimmte Sprache hin? Der neue Ansatz besteht darin, dass die Forscher dem KI-Modell virtuelle Layer hinzufügen, die den Entscheidungsprozess nicht beeinflussen, aber aus den Frequenzspektren bestimmte Frequenzräume hervorheben.

Am Ende müssten Konzepte vergleichbare Audiosequenzen mit typischen Ausdrücken oder Ausspracheeigenheiten darlegen. Anstelle von unübersichtlichen Frequenzbändern bekäme der Anwender also eigentümliche Betonungen und regionale Begriffe als Soundfiles zur Auswahl: „nech?“, „gell?“, „Host mi?“

Ein weiteres Forschungsgebiet für die nahe Zukunft der erklärbaren KI sind die großen Sprachmodelle wie ChatGPT und Bard. In deren Netzwerken sind sogenannte Attention Layer eingebaut, die helfen, Abhängigkeiten auch in großen Texten und zwischen weit auseinanderliegenden Sätzen zu erfassen. Diese Netzwerkarchitektur bereitet dem CRP-Verfahren allerdings Probleme, wenn es darum geht, die Relevanzverteilung von Knoten der höheren Schichten in Bezug auf die Eingabe zu ermitteln. Aber die Forscher hoffen, auch diese Hürde in den nächsten Monaten überspringen zu können.

Das Heidelberger Unternehmen Aleph Alpha, das mit Luminous einen zu ChatGPT vergleichbaren Sprachgenerator anbietet, hat bereits eine Lösung für derartige Probleme vorgestellt. Innerhalb der Luminous-Familie gibt es seit Juni eine Version namens Control, die Teile ihrer Ausgabe erklären soll. Konkret sieht das so aus, dass der Anwender auf einzelne Aussagen einer Antwort klicken kann und Control dann dazu Sätze im Anfrage-Prompt farbig markiert, die für die Ausgabe relevant waren. Damit erhält der Anwender Hinweise, die ihm helfen, den generierten Text auf seine Stichhaltigkeit abzuklopfen.

Licht in die Black Box

Während KI-Modelle in weite Bereiche der Technik und des Alltagslebens eindringen, sind sie aufgrund ihrer zugrundeliegenden Netzwerkstruktur bislang als Black Boxes in ihrer Entscheidungsfindung nur schwer zu kontrollieren gewesen. Heatmaps, wie sie etwa das LRP-Verfahren berechnet, geben nur Anhaltspunkte dafür, ob eine KI nach sinnvollen Kriterien Entscheidungen trifft.

Die neue CRP-Methode zeigt nun, dass viele Modelle tatsächlich abstraktere semantische Konzepte entwickeln, die denen gleichen, mit denen auch Menschen ihre Umwelt sortieren. Diese Beurteilungskriterien zu kennen, könnte es Anwendern ermöglichen, KI-Modelle auf Sicherheit und Zuverlässigkeit zu überprüfen. Mit diesem Instrument kann der Anwender sogar mit der KI über Merkmale diskutieren und dafür im Was-wäre-wenn-Modus probeweise einzelne Konzepte stilllegen.

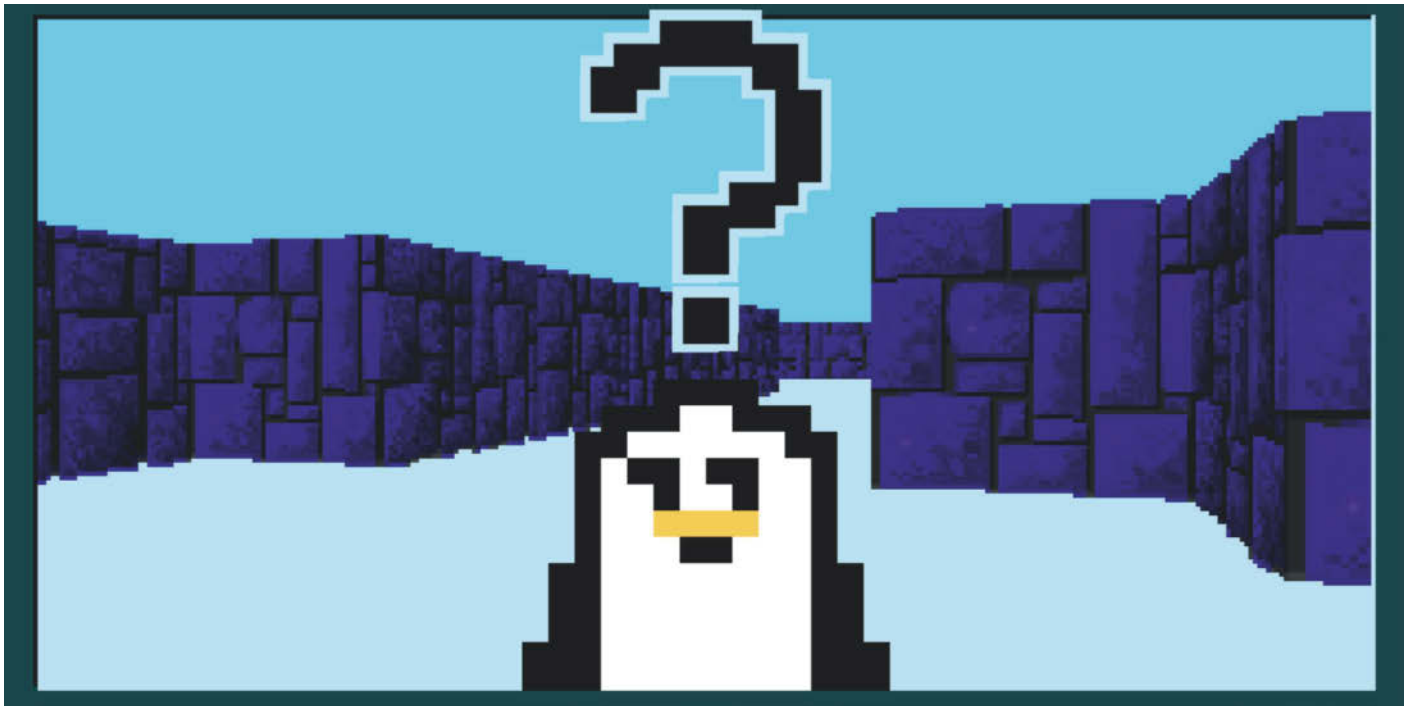
Explorative KI-Systeme können künftig sehr komplexe Trainingsdaten durchforsten und in verständlicher Weise die gefundenen Zusammenhänge und Konzepte mitteilen. Daraus könnten Wissenschaftler neue Forschungsansätze entwickeln. *(agr@ct.de)* **c't**

Literatur

[1] Arne Grävemeyer, Intelligenztest für KI, Wie sich KI-Entscheidungen überprüfen lassen, c't 6/2020, S. 58

[2] Andreas Holzinger, Interpretierbare KI, Neue Methoden zeigen Entscheidungswege künstlicher Intelligenz auf, c't 22/2018, S. 136

[3] Sebastian Lapuschkin, Wojciech Samek, Thomas Wiegand et al., From attribution maps to human-understandable explanations through Concept Relevance Propagation, nature machine intelligence, online: 20. September 2023, https://doi.org/10.1038/s42256-023-00711-8



Wo gehts hier raus?

Labyrinthe lösen mit Python und NetworkX

Ob rutschende Pinguine in c't-Rätseln oder verzweifelte Familien im Maisfeld – mit Python und NetworkX finden sie aus jedem noch so komplizierten Labyrinth schnell heraus.

Von Andreas Welzien

Ariadne-Faden war gestern – heute würde sich Theseus seinen Weg durch das Labyrinth zum Minotaurus und wieder hinaus mit Computerhilfe bahnen. Er muss dafür nur ein bisschen die Programmiersprache Python sprechen können, den Rest übernimmt das Python-Modul NetworkX (zu installieren mit `pip install networkx`).

Frisch aus c't Nerdistan

Mit NetworkX findet man nicht nur den Ausweg aus dem Labyrinth, sondern kann auch Routen planen, Netzwerkstrukturen erforschen und vieles mehr. Im Folgenden geht es der Einfachheit halber um klassische Labyrinthe in 2D, also auf einer Ebene.

Kanten und Knoten

NetworkX kann sich leider nicht selbst ein Bild von einem Labyrinth machen, dieses muss man NetworkX beschreiben, damit es etwas damit anfangen kann. Die Struktur, mit der NetworkX arbeitet, ist ein sogenannter Graph. Ein Graph besteht aus Knoten und Kanten. Knoten (engl. nodes) sind die Stellen, zum Beispiel in einem Labyrinth, an denen man sich befinden kann. Kanten (engl. edges) verbinden diese Knoten, sodass klar wird, von welchem Ort (Knoten) man zu einem anderen gelangt und von dort aus weiter zu anderen et cetera.

Der erste Schritt zum Graphen ist, das Labyrinth zu abstrahieren, es sich also nicht wie Irrwege zwischen Hecken, Hanf, Mauern oder Mais vorzustellen, sondern sich zu fragen, wo entlang man gehen könnte. Als Beispiel soll das folgende Minilabyrinth dienen, das 10 × 6 Felder umfasst (siehe die Datei simple_maze.txt im Listing-Archiv zu diesem Artikel, erhältlich via ct.de/ypga):

```
S ########
#        #
# ###  # #
# #    # #
# #  # # #
####Z#####
```

Hierin sind die Doppelkreuze undurchdringbare Wände, die Leerstellen sind begehbar (die späteren Knoten im Graphen). `S` und `Z` sind ebenfalls begehbar und stehen für Start und Ziel.

Jedem Feld lässt sich eine Koordinate zuordnen. Wie in der Computerei üb-

lich befindet sich der Ursprung links oben. Der Start hat also die Koordinaten (0, 0), das Ziel (4, 5). Man kann sich im Labyrinth horizontal oder vertikal von einem begehbaren Feld zum nächsten bewegen: Ein Schritt nach rechts ist einer um (+1, 0), nach links um (–1, 0), nach oben um (0, –1) und nach unten um (0, +1).

Konkreter

Der nächste Schritt ist der Aufbau einer Hilfsstruktur, und zwar der Menge `accessible` mit den Koordinaten aller begehbaren Felder. Ganz nebenbei entsteht das Dictionary `start_end` mit den Koordinaten von Start und Ziel.

Dazu liest das Skript simple_solver.py das obige Labyrinth zeilenweise in die Variable `maze` ein und durchläuft alle Zeilen und Spalten:

```
maze = open('simple_maze.txt')\
  .readlines()
accessible = set()
start_end = {}
for y, row in enumerate(maze):
  for x, char in enumerate(row):
    if char != '#' :
      accessible.add((x, y))
    if char in ['S', 'Z']:
      start_end[char] = (x, y)
```

Der dritte Schritt definiert die Kanten des Graphen. NetworkX stellt zur Verwaltung von Graphen die Klasse `Graph` bereit.

Der Graph muss Kanten für alle möglichen Schritte von einem begehbaren Feld zum nächsten enthalten. Dazu ermittelt das Skript ausgehend von jedem begehbaren Feld die Koordinaten der vier Nachbarfelder und schlägt diese in `accessible` nach. Existiert das Nachbarfeld darin, fügt die `Graph`-Methode `add_edge()` die Kante dem Graphen hinzu. Als Parameter erwartet sie die Koordinaten von Start- und Zielknoten. Das erledigt im Skript folgender Code:

```
LEFT, RIGHT, DOWN, UP = \
  (-1, 0), (1, 0), (0, 1), (0, -1)
DIRECTIONS = LEFT, RIGHT, DOWN, UP

import networkx as nx
G = nx.Graph()
for x, y in accessible:
  for dx, dy in DIRECTIONS:
    possible_pos = x + dx, y + dy
    if possible_pos in accessible:
      G.add_edge((x, y), possible_pos)
```

Nun steht der Graph und die NetworkX-Funktion `shortest_path` kann den kürzesten Pfad zwischen Start- und Zielknoten berechnen:

```
path = nx.shortest_path(
  G, start_end['S'], start_end['Z'])
```

`path` enthält danach eine Liste der Koordinaten vom Start zum Ziel. Auf `print(path)` erscheint:

```
[(0, 0), (1, 0), (1, 1), (2, 1),
 (3, 1), (4, 1), (5, 1), (5, 2),
 (5, 3), (4, 3), (4, 4), (4, 5)]
```

Malt man Punkte an diese Stellen im Labyrinth, visualisiert das die Lösung:

```
..########
#.....   #
# ###. # #
# # .. # #
# # .# # #
####.#####
```

Ein solches Labyrinth ist trivial und von Hand schneller zu lösen, als das Python-Skript dafür aufzurufen. Aber: Man kann damit den kürzesten Weg zwischen zwei Punkten in 2D-Labyrinthen beliebiger Größe finden. Standardmäßig benutzt NetworkX dafür übrigens den Dijkstra-Algorithmus [1].

Komplexere Fragestellungen lösen

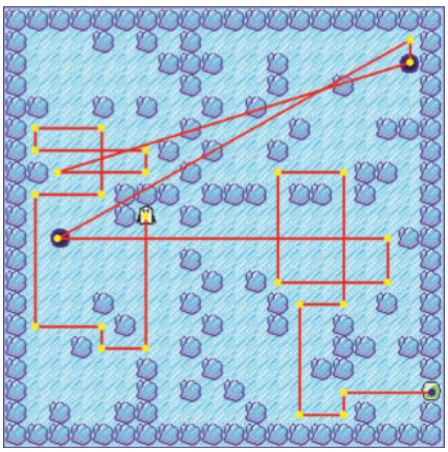
Ein Labyrinth wie zum Beispiel das in der Rätselaufgabe mit dem rutschenden Pinguin (siehe c't 19/2023, S. 56) lässt sich so allerdings nicht lösen. Denn es hat vier Besonderheiten, die Kopfzerbrechen bereiten:

1. Der Pinguin bewegt sich nicht in Einzelschritten in eine bestimmte Richtung, sondern rutscht immer bis zum nächsten Hindernis (Stein oder Loch).
2. Die Richtung, in die der Pinguin rutscht, ist wichtig: Eine Verbindung von A nach B ist nicht automatisch auch eine von B nach A.
3. Wenn der Pinguin in ein Loch fällt, erscheint er direkt an der Position des anderen Loches und bleibt dort stehen.
4. Es wird nicht nur der Weg mit den wenigsten Zügen (Schubser in eine Richtung) gesucht, sondern falls es mehrere davon gibt, soll der mit der kürzesten Gesamtdistanz (Anzahl der zurückgelegten Felder) gewählt werden.

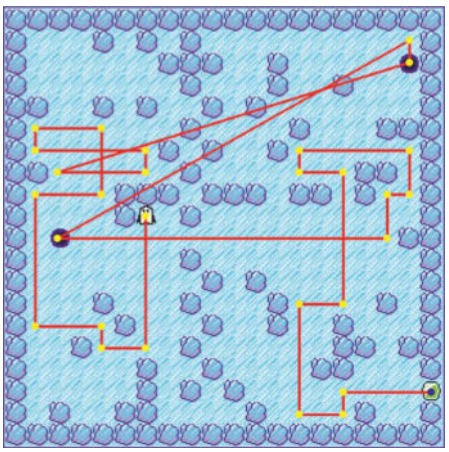
Damit NetworkX die Richtung der Verbindungen beachtet und nicht automatisch

c't kompakt

- Den Weg aus einem Labyrinth heraus kann man als ein Problem der Graphentheorie formulieren.
- Mit den theoretischen Grundlagen muss man sich zum Glück fast gar nicht beschäftigen, wenn man eine fertige Programmierbibliothek benutzt.
- Die Python-Bibliothek NetworkX lässt sich leicht bedienen und geht schnell zu Werke.



Visualisiert man das Ergebnis des Pfadfindeskripts, ergibt sich einmal ein Pfad mit den wenigsten Zügen …



… und einmal einer mit der kürzesten Distanz, aber zwei Zügen mehr.

davon ausgeht, dass ein Weg von A nach B auch einer von B nach A ist, muss man zu einem Graphen vom Typ `DiGraph` greifen (`Di` steht für „directed“, also gerichtet).

Wie zuvor ermittelt das Skript alle möglichen Verbindungen zwischen zwei Punkten, allerdings nicht die direkte Verbindung zwischen zwei benachbarten Feldern, sondern die zwischen einem Startpunkt und dem durch Rutschen erreichbaren Endpunkt.

Dazu entstehen wie im obigen Beispiel Hilfsstrukturen für die Koordinaten der begehbaren Felder sowie für Start und Ziel. Weil die Löcher eine Spezialbehandlung benötigen, merkt sich das Skript deren Koordinaten in einem weiteren Array namens `holes`:

```
accessible = set()
holes = set()
start_end = dict()
for y, row in enumerate(maze):
  for x, char in enumerate(row):
    if char not in ['#', 'O']:
      accessible.add((x, y))
    elif char == 'O':
      holes.add((x,y))
    if char in ['S', 'Z']:
      start_end[char] = (x, y)
```

Nun kann die virtuelle Rutschpartie beginnen (siehe Listing unten). Das Skript startet mit der Position des Pinguins (`S`) und sucht von dort aus in allen vier Richtungen nach Verbindungen, die zu einem Stein oder Loch führen. Sollte es ein Loch sein, ist der Endpunkt der Verbindung die Position des anderen Lochs, sollte es ein Stein sein, die Position vor dem Stein.

Von diesen Endpositionen aus gesehen wiederholt sich das Vorgehen, bis die Schleife alle erreichbaren Positionen abgearbeitet hat. Um eine Endlosschleife zu vermeiden, werden nur Endpositionen als neuer Startpunkt betrachtet, bei denen die zu bildende Verbindung (Kante) noch nicht existiert (`if (pos1, pos2) in G.edges`).

Im Unterschied zum Eingangsbeispiel bekommen Kanten ein Gewicht `weight`, das sich aus der beim Rutschvorgang zurückgelegten Strecke `distance` ergibt. Das ist erforderlich, weil NetworkX später nicht nur einfach den Weg mit den wenigsten Zügen, sondern auch den Weg mit der geringsten Gesamtdistanz ermitteln soll.

Nach diesen Vorbereitungen kann das Skript NetworkX nach allen Wegen zwischen Start und Ziel fragen, die mit den wenigsten Zügen auskommen:

```
paths = nx.all_shortest_paths(G,
  start_end['S'], start_end['Z'])
```

Unter diesen Wegen ist derjenige mit der kürzesten Distanz gesucht:

```
moves, distance, path = min(
 (len(p) - 1, nx.path_weight(
                  G, p, 'weight'), p)
  for p in paths)
print(moves, distance, path)
```

```
G = nx.DiGraph()
not_visited = [start_end['S']]
max_distance = max(len(maze), len(maze[0]))
while len(not_visited) > 0:
  x, y = not_visited.pop(0)
  pos1 = x, y
  for dx, dy in DIRECTIONS:
    for distance in range(1, max_distance):
      x2, y2 = x + dx * distance, y + dy * distance
      pos2 = x2, y2
      if pos2 in accessible: # weiter rutschen
        continue
      if pos2 in holes:
        pos2 = [p for p in holes if p != pos2][0]
      else:
        pos2 = x2 - dx, y2 - dy
        distance -= 1
      if (pos1, pos2) in G.edges:
        break
      G.add_edge(pos1, pos2, weight=distance)
      not_visited.append(pos2)
      break
```

Zum Lösen des Rutschpartie-Rätsels legt das Skript rutschpartie_solver.py einen gerichteten Graphen an. Die Kanten darin verbinden alle möglichen Startpunkte mit den von dort aus erreichbaren Endpunkten. Die Kanten erhalten ein Gewicht, das der Entfernung zwischen Start- und Endpunkt entspricht.

Das führt zur Ausgabe:

```
26 93 [(6, 9), (6, 15), (4, 15),
(4, 14), (1, 14), (1, 8), (4, 8),
(4, 5), (1, 5), (1, 6), (6, 6),
(6, 7), (2, 7), (18, 2), (18, 1),
(2, 10), (17, 10), (17, 12), (12, 12),
(12, 7), (15, 7), (15, 13), (13, 13),
(13, 18), (15, 18), (15, 17),
(19, 17)]
```

Zwischen Start und Ziel liegen also 26 Züge. Auf dem Weg hat der Pinguin eine Strecke von 93 Feldern zurückgelegt (siehe Bilder auf der vorangehenden Seite).

Wer neugierig ist, ob es eventuell einen Weg mit einer kürzeren Strecke, aber mehr Zügen gibt, wechselt einfach die Funktion zur Pfadermittlung: Mit `dijkstra_path()` statt `shortest_path()` berücksichtigt NetworkX die Kantengewichte, mithin die Entfernungen zwischen den Haltepunkten:

```
path = nx.dijkstra_path(
  G, start_end['S'], start_end['E'])
```

Fertig.

Fazit

Beide Beispiele zeigen, wie leicht der Umgang mit grundlegenden Funktionen von NetworkX ist. Man kommt nicht nur schnell zum (Programmier-)Ziel, sondern auch noch superschnell zum Ergebnis: Die Laufzeit vom Einlesen des Labyrinths von SSD bis zur Ausgabe bewegt sich im einstelligen Millisekundenbereich. Das Berechnen aller Pfade dauert sogar nur ein paar Dutzend Mikrosekunden.

Außer den vorgestellten Funktionen gibt es noch etliche weitere zur Ermittlung von kürzesten Pfaden, etwa mithilfe des Bellman-Ford-, Floyd-Warshall- oder A*-Algorithmus, sowie viele andere Algorithmen mehr rund um Graphen. Stöbern Sie ruhig ein bisschen in der sehr ausführlichen Dokumentation von NetworkX. Ein detailliertes Video zur Lösung des Pinguin-Rätsels finden Sie übrigens bei YouTube (alle Links unter ct.de/ypga).

(ola@ct.de) c't

Literatur

[1] Jo Bager, Zielfinder, Kürzeste Wege berechnen mit Dijkstras Algorithmus – und viele zusätzliche Daten, c't 8/2020, S. 64

Listing-Archiv, NetworkX-Doku, YouTube-Video: ct.de/ypga

Online-Konferenz – 23. November 2023

inside agile

TEAM UP!

Teamentwicklung in Zeiten von Remote-Work

... denn Remote-Teamentwicklung schafft neue Herausforderungen

- Wie kann erfolgreiche Teamentwicklung speziell in Remote- und Hybrid-Umfeldern gelingen?
- Wen oder was braucht es dafür?
- Und wie lässt sich das neue Verhalten nachhaltig verankern?

Für viele dieser Fragen haben sich in der Remote-Arbeit Lösungsansätze bewährt, die im Zentrum dieser Online-Konferenz stehen. Ausgewiesene Experten und Expertinnen zeigen erfolgreiche Wege, mit denen Teams ihre Ziele klar definieren und umsetzen können. Team Up! wendet sich an Führungskräfte und Verantwortliche in Projektteams, an (Agile) Coaches & Consultants und an Personalentwicklerinnen.

Jetzt **Tickets** sichern!

teams.inside-agile.de

+++ Außerdem Online-Workshops am 24./25. November, 6./7. Dezember und 7. Dezember 2023 +++

Veranstalter dpunkt.verlag iX MAGAZIN FÜR PROFESSIONELLE IT

Online-Konferenz – 28. November & 5. Dezember 2023

inside agile

AGILE LEADERSHIP CONFERENCE

So werden agile Teams besser

Kaum ein Unternehmen kommt heute noch ohne **agile Arbeitsweisen** aus. Der **Leadership Day (28.11.)** und der **Self Leadership Day (5.12.)** behandeln aktuelle Herausfordungen von Führung und Management:

- Wie führt man selbstorganisierte Teams und wieso ist dabei die Selbstführung entscheidend?
- Wie kann man Mitarbeitende beurteilen, wenn die Teamleistung im Fokus steht?
- Braucht es überhaupt noch disziplinarische Führungskräfte?

Die Konferenz richtet sich an **Gruppen-/Team-/Abteilungsleiterinnen und -leiter** sowie erfahrene **Scrum Master/Agile Coaches.**
Wer teilnimmt, sollte ein agiles Grundverständnis mitbringen.

Jetzt **Tickets** sichern!

alc.inside-agile.de

+++ Außerdem Online-Workshops am 29. November und 8. Dezember 2023 +++

Veranstalter dpunkt.verlag iX MAGAZIN FÜR PROFESSIONELLE IT

Kooperationspartner it-agile Agile Academy

RAM statt Flash

Frühe SSDs im c't-Test

Eine der ersten in der c't getesteten Solid-State-Disks war 1999 die Quantum Rushmore RU5053F. Statt damals noch langsamem und unzuverlässigem Flash-Speicher nutzte sie schnelles RAM – zu einem Preis, bei dem man nicht nur damals schlucken musste.

Von Rudolf Opitz

Kurz vor der Jahrtausendwende speicherten Festplatten bereits mehrere Gigabyte und ließen ihre Magnetplatten für hohe Datenraten bis zu 15.000 mal pro Minute rotieren. Doch brauchte es Zeit, bis die Köpfe die nötige Position erreicht und die gewünschten Daten gelesen hatten. SSDs als Festplattenersatz mit wenigstens 20-fach geringeren Zugriffszeiten gab es schon zu astronomischen Preisen. Flash galt jedoch noch als nicht sehr haltbar und fehleranfällig, auch wenn die Anbieter anderes behaupteten.

Quantum bot als Alternative seine Rushmore-Serie mit Kapazitäten bis 3,2 GByte an. Harald Bögeholz hatte die kleinste Platte mit 511 MByte für die c't 18/1999 getestet:

„Um die Zugriffszeiten deutlich zu verbessern, hilft nur eines: Man verzichtet auf mechanische Komponenten und speichert die Daten in RAMs. Einer der wenigen Hersteller solcher ‚Solid-State-Disks' ist Quantum. [...] Die RU5053F ist trotz ihrer für heutige Verhältnisse geringen Kapazität ein dicker Brocken: Sie kommt im 5,25"-Formfaktor mit ‚voller Bauhöhe' (3,25 Zoll) daher."

Also handelt es sich bei dem Rushmore-Laufwerk um eine RAM-Disk. Doch die speichert Daten nur bei laufendem Rechner. Was passiert mit den Daten, wenn der PC heruntergefahren wird?

„Damit die Daten beim Abschalten nicht verloren gehen, hat Quantum eine 2,5"-Festplatte als Puffer integriert. Nach dem Einschalten beginnt die SSD unverzüglich damit, ihre Nutzdaten von der Pufferplatte ins interne RAM einzulesen."

So „Solid State" war die Quantum-Disk also gar nicht. Da sie die Daten beim Systemstart zunächst ins RAM übertragen musste, was etwa zwei Minuten dauerte, gab es kein schnelleres Booten wie bei modernen SSDs. Die RU5053F eignete sich daher eher für Server, beschleunigte den Zugriff auf Datenbanken und machte Webservern Beine. Und wenn es einen Stromausfall gibt?

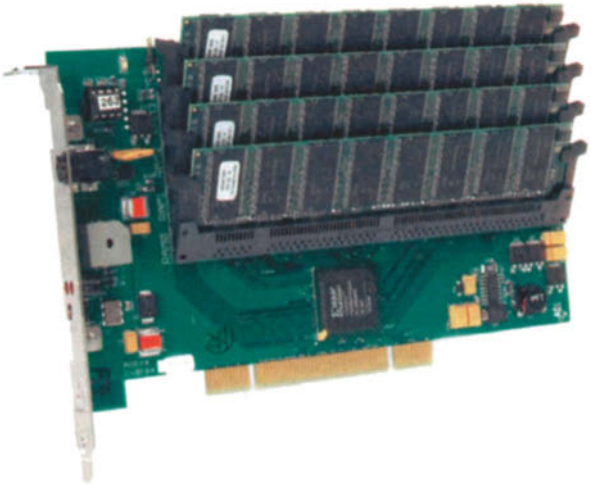
„Ein Akku-Paket versorgt die Laufwerkselektronik und die Pufferplatte genügend lange mit Strom, sodass sie alle ungesicherten Daten speichern kann. Günstigstenfalls ist dazu nicht viel zu tun, da das Laufwerk neu geschriebene Daten im Hintergrund ständig auf die Pufferplatte sichert."

Das erklärt die Abmessungen des Rushmore-Laufwerks: Abgesehen von RAM und Elektronik beherbergte das Gehäuse die Puffer-Festplatte und einen Akkupack. Die Zugriffszeit auf die arbeitsbereite SSD betrug verglichen mit damaligen Laufwerken sensationelle 0,2 Millisekunden. Die 511-Megabyte-Platte kostete rund 15.000 US-Dollar!

Gut zwei Jahre später begutachtete Christof Windeck in der c't 8/2002 eine günstigere Solid-State-RAM-Disk: das Rocket-Drive der US-Firma Cenatek für etwa 1000 US-Dollar. Es bestand aus einer PCI-Karte mit vier DIMM-Slots, von denen in der Basisversion zwei mit je einem 256-MByte-SDRAM-Riegel bestückt waren.

„Ein externes Netzteil versorgt die Steckkarte über eine Buchse im Slotblech mit Strom, sodass die Daten auch beim Abschalten oder Absturz des PC erhalten bleiben. Will man sich vor Stromausfall schützen, muss man das RocketDrive-Netzteil an eine USV anschließen."

Bis sich Flash-Speicher als schnelle Festplattenalternative durchsetzte, vergingen weitere fünf Jahre. Zunächst waren Flash-SSDs noch sehr teuer und oft nicht so schnell wie versprochen. Intel gehörte damals zu den Vorreitern der modernen SSD-Technik, etwa mit „Turbo Memory" für Notebooks oder später mit den ersten 2,5-Zoll-Laufwerken, die wirklich extrem schnell und gleichzeitig stromsparend waren. Auf dem Intel Developer Forum 2007 sah Pat Gelsinger, damals noch Intel-CTO, in die Zukunft: Flash-Laufwerke könnten in puncto Transferraten herkömmliche Festplatten bald deutlich übertrumpfen. Hätte unser Prozessorspezialist Andreas Stiller dagegengewettet, hätte er wohl diesmal verloren (siehe c't 24/2023, S. 132). *(rop@ct.de)* c't



Günstiger als die Quantum RU5053F war das RocketDrive von 2002, dass nur 1000 Dollar kostete, sich mit SDRAM erweitern ließ, aber über ein externes Netzteil gepuffert werden musste.

SSD-RAM-Drive-Tests zum Nachlesen:
ct.de/ytjj

Harald Bögeholz

Solider Bolide

Solid-State-Disk RU5053F von Quantum

Von Jahr zu Jahr trumpfen die Festplattenhersteller mit immer schnelleren Laufwerken auf. Trotzdem sind in so manchen großen Datenbanken oder Webservern immer noch die Festplatten der bremsende Faktor. Eine Solid-State-Disk kann ein solches System auf Trab bringen – wenn Geld keine Rolle spielt.

Hinsichtlich der Datenraten lassen Festplatten heute kaum noch zu wünschen übrig: Bereits ein einzelnes modernes Laufwerk liefert Dauertransferraten von über 20 MByte/s – genug für die Aufnahme oder Wiedergabe eines unkomprimierten Videodatenstroms. Doch in einer Disziplin haben Festplatten eine prinzipbedingte Schwäche: Die Zugriffszeit lässt sich aufgrund der mechanischen Gegebenheiten kaum noch weiter verbessern. Um einen bestimmten Sektor lesen zu können, muss eine Festplatte nämlich zunächst die Köpfe auf die richtige Spur bewegen und dabei deren mechanische Trägheit überwinden. Anschließend vergeht eine so genannte Latenzzeit, bis der gewünschte Sektor am Lesekopf vorbeikommt.

Um die Zugriffszeiten deutlich zu verbessern, hilft nur eines: Man verzichtet auf mechanische Komponenten und speichert die Daten in RAMs. Einer der wenigen Hersteller solcher 'Solid-State-Disks' ist Quantum. Die Familie 'Rushmore Ultra' umfasst Modelle mit Kapazitäten bis 3,2 GByte. Das mit 511 MByte zweitkleinste Exemplar fand sich für einen kurzen Test in der c't-Redaktion ein. Die RU5053F ist trotz ihrer für heutige Verhältnisse geringen Kapazität ein dicker Brocken: Sie kommt im 5,25"-Formfaktor mit 'voller Bauhöhe' (3,25 Zoll) daher.

Das Laufwerk verfügt über einen 68-poligen Wide-Ultra-SCSI-Anschluss sowie den festplattenüblichen Stromversorgungsstecker, lässt sich also als direkter Ersatz für eine Festplatte in ein bestehendes SCSI-System integrieren. Damit die Daten beim Abschalten nicht verloren gehen, hat Quantum eine 2,5"-Festplatte als Puffer integriert.

Nach dem Einschalten beginnt die SSD unverzüglich damit, ihre Nutzdaten von der Pufferplatte ins interne RAM einzulesen. Greift man während dieses Vorgangs auf Daten zu, die noch nicht gelesen sind, erzielt das Laufwerk natürlich noch nicht die volle Performance, sondern nur die der Pufferplatte. Nach etwa zwei Minuten ist die Solid-State-Disk dann 'voll da'.

Im normalen Betrieb liest und schreibt die Rushmore die Daten direkt aus dem RAM. Bei einem plötzlichen Stromausfall geht nichts verloren: Ein Akku-Paket versorgt die Laufwerkselektronik und die Pufferplatte genügend lange mit Strom, sodass sie alle ungesicherten Daten speichern kann. Günstigstenfalls ist dazu nicht viel zu tun, da das Laufwerk neu geschriebene Daten im Hintergrund ständig auf die Pufferplatte sichert.

Quantum garantiert, dass die Akkus mindestens dreimal täglich auch den ungünstigsten Fall bewältigen können, dass sämtliche Daten noch auf die Pufferplatte geschrieben werden müssen. Um ganz sicher zu gehen, sorgt eine Akku-Kontrolle überdies dafür, dass die SSD bei niedrigem Ladestand auf 'Write-Thru'-Betrieb schaltet, Daten also grundätzlich erst auf die Pufferplatte schreibt, bevor sie das entsprechende SCSI-Kommando bestätigt. Das ist natürlich nur für Notfälle gedacht und würde die Schreibperformance des Laufwerks auf die der 2,5"-Pufferplatte begrenzen.

Ihre reinen Leistungsdaten musste die Rushmore zunächst mit dem DOS-basierten Benchmark H2bench an unserem üblichen Testsystem für Festplatten unter Beweis stellen, sodass die Ergebnisse mit denen aus dem Festplattentest im letzten Heft vergleichbar sind. Erwartungsgemäß brilliert die SSD vor allem bei der mittleren Zugriffszeit. Mit einem Wert von 0,2 ms schlägt sie die bisher in dieser Disziplin schnellste Festplatte, die Cheetah 18LP, um Längen: 7,3 ms beträgt deren mittlere Zugriffszeit über die gesamten 18 GByte Kapazität. Fairerweise muss man den Wert der SSD allerdings mit der Zugriffszeit der Cheetah innerhalb einer vergleichbaren Kapazität vergleichen: 4,2 gegen 0,2 ms ergibt aber immer noch den Faktor 21. Die Dauertransferrate der SSD liegt mit kontinuierlichen 28 MByte/s über der sämtlicher Festplatten, jedoch hätten wir erwartet, dass das Ergebnis dem durch das Wide-Ultra-SCSI-Interface vorgegebenen Maximum von 40 MByte/s noch ein wenig näher kommt.

Ein Test unter Windows 98 gab uns Gelegenheit zu überprüfen, wie viel mehr Leistung diesem Betriebssystem mit einer superschnellen Festplatte zu entlocken ist. Das Ergebnis ist eher ernüchternd: Es fühlt sich zwar irgendwie schneller an, bootet jedoch nur unwesentlich schneller, und das Ergebnis der Anwendungs-Benchmark-Suite BAPCo verbessert sich im Vergleich zu einer Seagate Cheetah 18LP nur von 226 auf 240 Punkte (Asus P2B, Pentium-III-600, 64 MByte RAM, Diamond Viper V550). Unter den in der BAPCo enthaltenen Einzeltests zeigte der Datenbank-Benchmark mit Paradox 8.0 die mit 13 % größte Verbesserung (232 auf 263 Punkte).

Um eine Testumgebung zu schaffen, in der wirklich die Festplatte der leistungsbegrenzende Faktor ist, setzten wir die SSD in einen Vier-Prozessor-Server von Intel mit 500-MHz-Xeons und 384 MByte RAM unter Linux ein. Festplattenintensive Operationen wie das Durch-'greppen' eines ganzen Filesystems liefen im Vergleich zu einer Festplatte günstigstenfalls anderthalb mal so schnell ab, während das ansonsten gern herangezogene Kompilieren des Linux-Kernels davon mit bestenfalls 10 % profitierte.

Ein wirklich großer Datenbankserver stand uns zum Test leider nicht zur Verfügung. Der Einsatz einer Solid-State-Disk kommt jedenfalls erst nach einer sorgfältigen Analyse in Betracht, ob wirklich der Parameter 'mittlere Zugriffszeit' das Nadelöhr ist und nicht etwa Dauertransferrate, Prozessorleistung, SCSI-Bus oder sonst etwas. Daher gibt es SSDs auch nicht an jeder Straßenecke, sondern die Hersteller großer Datenbank- oder Webserver integrieren sie bei Bedarf direkt in ihre Systeme. Ach ja, der Preis: 15 000 US-Dollar würde die RU5053F einen Endkunden ungefähr kosten. (bo)

Quantum RU5053F (Rushmore)	
Solid-State-Disk mit Pufferplatte	
Hersteller	Quantum, Frankfurt, Tel. 0 69/95 07 67-0
Preis	zirka 15 000 US-Dollar
Kapazität	511 MByte
Interface	Wide Ultra SCSI
Dauertransferrate Lesen/Schreiben	27,5/28,0 MByte/s
Mittlere Zugriffszeit	0,2 ms
Gewichteter Mittelwert (Hdbench)	19,6 MByte/s

Stressärmer teamsen

Einknopf-Tastenkürzel für Microsoft Teams

In MS-Teams-Konferenzen gibt es für häufig genutzte Funktionen wie das Heben der Hand oder das Ein- und Ausschalten des Mikrofons zwar Tastenkombinationen, diese sind jedoch umständlich und nicht anpassbar. Mit ein paar Tricks realisieren Sie eine elegantere Einknopf-Lösung.

Von Stefan Wischner

Ein Klassiker im Teams-Meeting: „Dein Mikro ist noch aus!“ Beobachtet von allen Teilnehmern stutzt der Angesprochene zunächst, die Augen gehen nach unten zu Maus oder Touchpad, fahnden dann kreisend nach dem Mauszeiger, um sich schließlich auf der Suche nach dem Mikrofonsymbol nach oben zu wenden. Die dabei gemurmelte Entschuldigung entschlüsseln nur geübte Lippenleser.

Zwar lassen sich viele wichtige Funktionen in Teams auch per Tastatur bedienen, eine Übersicht aller Kürzel liefert das Programm selbst über „Tastenkombinationen“ im oberen Dreipunktemenü. Die Shortcuts sind aber fest vorgegeben und Dreifingerkrallengriffe wie Strg+Umschalt+M für Mikrofon an/aus oder Strg+Umschalt+K zum Heben und Senken der Hand sind weder intuitiv noch komfortabel.

Souveräner ginge es mit einer leicht zu findenden Einzeltaste, was sich mit ein bisschen Soft- oder Hardwarehilfe einrichten lässt, auch wenn das natürlich nicht verhindert, dass man vergisst, das Mikrofon einzuschalten. Am einfachsten lässt sich das mit Eingabegeräten lösen, in deren Treibersoftware Makros programmierbar sind. Damit kann man eine selten genutzte Taste mit einer bestimmten Kombination wie Strg+Umschalt+M belegen. Meist kommt solche Hardware aus dem Gamingbereich; es gibt aber auch makrofähige Office-Mäuse und Tastaturen.

X-Mouse Button Control

Mit dem kostenlosen Windows-Tool X-Mouse Button Control belegen Sie die Tasten jeder beliebigen, auch nicht makrofähigen Maus. Eine ausführliche Beschreibung finden Sie in [1]. Dort geht es zwar um die Mediensteuerung, die Belegung mit Teams-Tastenkürzeln funktioniert aber im Prinzip genauso. Die Kurzfassung: Legen Sie in X-Mouse Button Control ein neues Profil für Microsoft Teams an und wählen Sie im Layer 1 für die gewählte Maustaste die Aktion „Simulated Keys“. Tragen Sie dann im zugehörigen Einstellungsdialog unter „Enter the custom key(s)“ zum Beispiel `{CTRL}{SHIFT}m` ein, um das Mikrofon ein- und auszuschalten. Analog verfahren Sie mit weiteren Kürzeln auf anderen Maustasten. Sie können auch weitere Profile anlegen, etwa für das Videokonferenz-Programm Zoom, bei dem die Tastenkürzel ärgerlicherweise anders sind als bei Teams. Durch das Umschalten von Profilen erreichen Sie, dass stets die gleiche Taste etwa fürs Freischalten des Mikros zuständig ist.

AutoHotkey

Eine Alternative zu X-Mouse Button Control, die auch mit Tastaturen funktioniert, ist der kostenlose Skript-Interpreter AutoHotkey. Damit können Sie komplexe Makros schreiben und allerlei Vorgänge in Windows und Applikationen automatisieren, was eine gewisse Einarbeitung erfordert. Einen guten Einstieg finden Sie unter [2] und [3]. Die Konfiguration von Hotkeys ist hingegen sehr einfach. Ein Druck auf eine Tastatur- oder Maustaste generiert dabei eine definierbare Tastenkombination oder -folge. Kurzgefasst geht das so: Laden Sie AutoHotkey herunter (ct.de/y182) und installieren Sie es. Dann legen Sie mit einem Editor Ihrer Wahl, zum Beispiel dem Windows-Notepad, eine Textdatei an. Darin tippen Sie die notwendigen Befehlszeilen. Speichern Sie die Datei mit der Endung .ahk und starten sie per Doppelklick oder besser verschieben sie in den Autostart-Ordner von Windows – fertig.

So sieht eine Codezeile für AutoHotkey aus, die nach einem Druck auf F12 die Tastenkombination Strg+Umschalt+M an das aktive Programm schickt:

```
F12::Send ^+m
```

Analog ergänzen Sie die Textdatei um Zeilen mit weiteren Hotkey-Definitionen. Das klappt nicht nur mit Tastaturtasten, sondern auch mit Maustasten. Das Beispiel sieht für die mittlere Maustaste anstelle von F12 so aus:

```
MButton::Send ^+m
```

Eine Referenz mit allen Tasten finden Sie in der Onlinedokumentation von AutoHotkey (ct.de/y182).

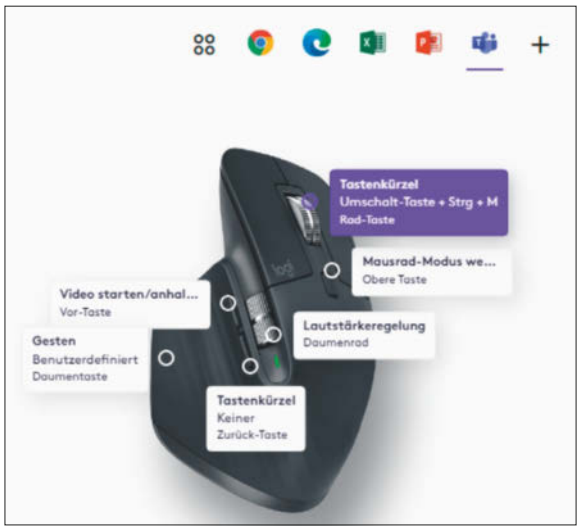
Tastatürchen

Eine elegante Alternative, die die Belegung Ihrer Tastatur und Maus unverändert lässt, ist externe Hardware als Schaltpult für Teams-Befehle.

Bei AliExpress und anderen Fernostversendern bekommt man für ganz kleines Geld programmierbare Mini-Tastaturen für den USB-Anschluss. Es gibt Ausführungen mit zwei bis einem Dutzend Tasten, auf den teureren stecken auch ein oder zwei Drehregler.

Wir haben uns für unter zehn Euro ein ganz einfaches Viertastenmodell bei AliExpress besorgt und ein ganz ähnliches mit drei Schaltern bei Amazon für gut den doppelten Preis. Beide überraschen durch unerwartet hohe Qualität der eingebauten mechanischen Taster. Billig wirkt hingegen das kippelige und rutschige Kunststoffgehäuse – nichts, was sich nicht mit einem Streifen Doppelklebeband lösen ließe. Etwas abenteuerlich ist die Softwareinstallation von der Webseite, die auf dem Beipackzettel der Tastatur beschrieben wird. Wir brauchten drei Versuche, dort das passende Programm zu finden, das die angesteckte Dreitastentastatur aus dem Amazon-Einkauf erkennt – in unserem Fall war das Footswitch 7.4.4. Dessen Bedienoberfläche ist etwas krude; die Programmierung der Tasten mit den passenden Kürzeln für diverse Teams-Funktionen klappt aber gut. Der Name des Programms deutet es schon an: Es gibt externe USB-Taster auch als Fußschalter, das unter dem Tisch platziert wird.

Schwierig war die Softwarebeschaffung für die Ali-Express-Tastatur. Die erforderte Detektivarbeit; die Spur führte von einem YoutTube-Video letztlich zu einer Google-Drive-Freigabe. Sicherheitshalber probierten wir das Programm nach ausgiebiger Virenprüfung erst einmal in einer virtuellen Maschine aus. Unsere Bedenken blieben glücklicherweise unbegründet.



Etwas teurere Office-Eingabegeräte, wie zum Beispiel die MX-Master-Mäuse von Logitech, erlauben das Umbelegen von Tasten und Steuerelementen in der mitgelieferten, allerdings oft Ressourcen fressenden Software (im Bild: Logitech Options+).

c't kompakt

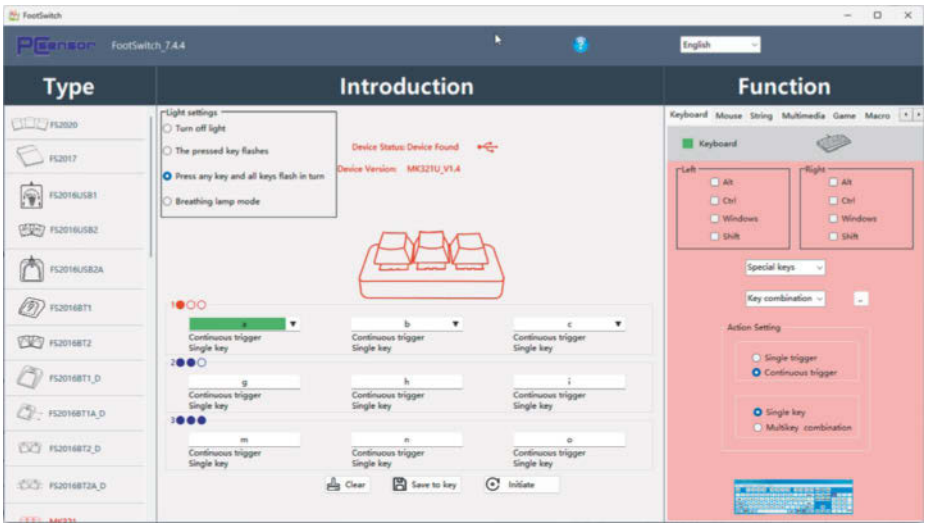
- Die Tastaturkürzel für häufig genutzte Funktionen in MS Teams sind umständlich und schwer zu merken.
- Deutlich komfortabler geht es mit extra Hardware.
- Auch mit kostenlosen Softwaretools können Sie die Steuerung vereinfachen.

Luxusschaltpult: Elgato Stream Deck

Eleganter, aber auch deutlich teurer als das China-Tastatürchen, ist ein Stream Deck von Elgato, nicht zu verwechseln mit der Handheld-Spielekonsole Steam Deck von Valve. Stream Decks sind kompakte Pultgehäuse mit programmierbaren Tasten und kleinen LCD-Anzeigen für die Beschriftung. Je nach Ausführung und Tastenanzahl kosten die Geräte bis zu 220 Euro. Für die Teams-Steuerung reicht jedoch das etwa 60 Euro teure Stream Deck Mini mit sechs Tasten.

Es gibt zwei Möglichkeiten, ein Stream Deck zum Steuern von Teams zu konfigurieren. Die erste sendet keine Tastenkürzel, sondern nutzt das API des Teams-Clients. Diese Methode setzt einen Microsoft-365-Business-Account voraus und funktioniert (noch) nicht mit der Vorschauversion des neuen Teams-Clients. Die Software des Stream Deck braucht dazu einen API-Key, den Sie direkt aus dem Teams-Client unter „Einstellungen/Datenschutz/API verwalten/API aktivieren“ aus dem Feld „API Token“ in die Zwischenablage kopieren.

Das Teams-Plug-in installieren Sie aus dem Store, den Sie in der Elgato-Software über das obenstehende Symbol mit stilisiertem Schaltpult und Pluszeichen erreichen. Legen Sie nach der Installation ein neues Profil an, das Sie zum Beispiel „Teams“ nennen. Im rechten Menü finden Sie dann den Abschnitt „Microsoft Teams“ mit allen steuerbaren Teams-Funktionen. Ziehen Sie eine davon, zum Beispiel „Ca-



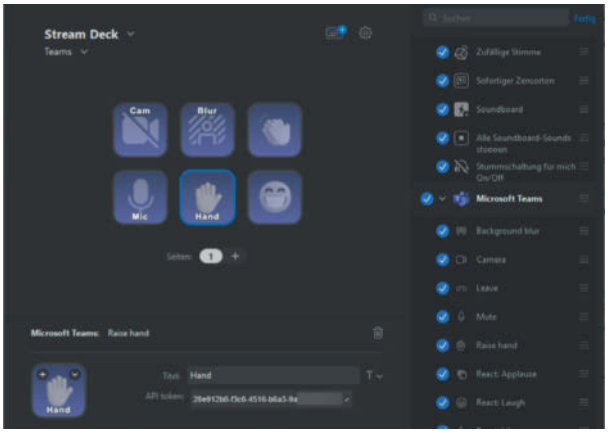
Praktisch billig, mit Hürden bei der Softwareinstallation: programmierbare Mini-USB-Tastaturen aus China.

mera“, auf einen freien Button im linken Bereich. In das erste Eingabefeld im unteren Bereich tragen Sie einen Namen für die Aktion ein, in das zweite („API Token“) fügen Sie den API-Key aus der Zwischenablage ein. Letzteres machen Sie nur für die erste Tastenbelegung; der Key wird für weitere Tasten automatisch übernommen.

Falls die API-Steuerung in Ihrem Teams-Client fehlt, konfigurieren Sie die Kürzel auf dem konventionellen Weg. Legen Sie dazu in der Stream-Deck-Software ein neues Profil an und ziehen Sie dann aus dem Abschnitt „System“ für jede zu belegende Taste die Aktion „Hotkey“ auf die gewünschte Schaltfläche. Im unteren Bereich klicken Sie in das Feld „Hotkey“ und drücken die Tastenkombination, die Sie dem Button zuweisen wollen, also zum Beispiel Strg+Umschalt+M, um das Mikrofon ein- und auszuschalten. Um ein passendes Symbol auf der Schaltfläche anzuzeigen, klicken Sie das Pluszeichen in der linken oberen Ecke des vorgegebenen Symbols an, um die Icon-Library zu öffnen. Eine größere Auswahl bieten die kostenlosen Icon-Packs, die Sie aus dem Store installieren können.

Bei beiden Methoden ist es sinnvoll, die Belegung auf das Programm Teams zu begrenzen. Das gilt natürlich auch für andere Anwendungen, die Sie mit dem Stream Deck steuern wollen. Klicken Sie dazu in der Stream-Deck-Software links oben auf das aktive Profil und wählen Sie aus dem Ausklappmenü „Profile bearbeiten …“. Im nächsten Fenster markieren Sie links das jeweilige Profil und wählen unter „Programm“ die Anwendung aus, die das Profil aktivieren soll. In der Liste werden aktuell laufende Programme gezeigt. Fehlt das Gewünschte, starten Sie es entweder zuvor oder navigieren Sie per „Anderes …“ zur zugehörigen EXE-Datei. Eines der Profile können Sie als Standardprofil festlegen (Häkchen bei „Das ist mein Standardprofil“). Es wird immer dann aktiv, wenn keines der anderen Profile arbeitet.

Wenn Ihnen der Preis für ein Stream Deck zu hoch ist, können Sie stattdessen auch ein vielleicht abgelegtes Smartphone mit der App „Stream Deck Mobile“ aus dem jeweiligen Store nutzen. Die App setzt iOS ab 15 oder Android ab 6.0 voraus und erfordert ein Abo für 3 Euro im Monat; die ersten 30 Tage sind jedoch kostenlos, genug zum Ausprobieren. Damit das Smartphone zum Stream Deck mit Touchscreen wird, muss auch auf dem PC die unabhängig von der Hardware kostenlos ladbare Stream-Deck-Software laufen, mit der sich die App verbindet.



In der Software zum Stream Deck konfigurieren Sie die Tasten des Schaltpults wahlweise per API zum Teams-Client oder über Tastenkürzel.

Und auf dem Mac?

Die meisten der vorgestellten Lösungen sind Teams für Windows vorbehalten. Weder haben wir macOS-Software für die China-Tastaturen gefunden, noch gibt es Mac-Versionen von AutoHotkey und X-Mouse Button Control. Eine Alternative dazu ist das allerdings kostenpflichtige BetterTouchTool.

Zwar lassen sich in den Systemeinstellungen von macOS grundsätzlich Tastenkürzel für die meisten installierten Apps definieren. Jedoch funktioniert das nur für Befehle, die über die macOS-eigenen Pulldown-Menüs der jeweiligen Anwendung erreichbar sind. Im Fall des Teams-Clients findet sich dort nichts Sinnvolles.

Die von uns ausprobierten Minitastaturen speichern die Belegung in einem eigenen Speicher. Programmiert man sie auf einem Windows-Rechner mit passenden Mac-Kürzeln, kann man das Gerät anschließend einfach umstecken. Problemlos lässt sich das Elgato Stream Deck unter macOS nutzen. *(swi@ct.de)* c't

Literatur

[1] Stefan Wischner, Turn up the Scroll Wheel, Mediensteuerung unter Windows per Maus, c't 15/2023, S. 148
[2] Hajo Schulz, Tipp-o-matik, Windows automatisieren mit AutoHotkey, c't 10/2019, S. 156
[3] Hajo Schulz, Tippen mit Stil, Die Tastatur anpassen unter Windows, c't 10/2020, S.146

Alle Tools zum Download: ct.de/y182

heise academy

M365 sicher und effektiv administrieren

Webinar-Serie „Microsoft 365 für Admins“

6. Dezember 2023 – 24. Januar 2024

Microsoft 365 bildet in vielen Unternehmen das Rückgrat der alltäglichen Büroarbeit: von Office-Anwendungen über Mail-Server bis zu Cloud-Speichern und Security-Tools.

Lernen Sie in unserer Webinar-Serie, dieses vielseitige Anwendungspaket zu administrieren und optimal für Ihr Unternehmen auszureizen.

Jetzt Kombi-Rabatt sichern:
heise-academy.de/webinare/m365admins1223

Effektiv zusammenarbeiten in Microsoft Teams

Webinar-Serie „Kollaboratives Arbeiten mit Microsoft Teams“

7. Dezember 2023 – 1. Februar 2024

Microsoft Teams ist aus den meisten Unternehmen nicht mehr wegzudenken. Hybride Arbeitsmodelle in verteilten Teams sind nur durch gut strukturierte Kommunikationstools umsetzbar. In dieser Webinar-Serie lernen Sie, wie Ihnen Microsoft Teams diese Zusammenarbeit erleichtert.

Jetzt Kombi-Rabatt sichern:
heise-academy.de/webinare/msteamskollab1223

Bild: KI Midjourney | Bearbeitung c't

Internetdinge im Edelgasnetz

LoRaWAN „Helium“ mit Node-Red kombinieren

Das LoRaWAN „Helium“ ist eine kommerzielle Alternative zum kostenfreien The Things Network, die aufgrund besserer Abdeckung besonders für den mobilen Einsatz interessant ist. Die Grundlagen des Netzes und Wichtiges zur Einrichtung erfahren Sie hier.

Von Andrijan Möcker

Die energiesparende Funktechnik LoRaWAN ist ideal für drahtlose Sensoren und Tracker (Ortungsgeräte). Da aber, verglichen mit Mobilfunknetzen mit GSM, LTE und 5G, wenige unternehmerisch betriebene landesweite LoRaWAN-Netze existieren und noch seltener internationales Roaming zwischen diesen funktioniert, stellt sich für mobile Nutzer immer die Frage: Gibt es vor Ort ein Gateway, also Netzabdeckung?

Während für Gateway-Betreiber im kostenfreien The Things Network (TTN) Eigennutz und Philanthropie im Vordergrund stehen, ist es beim ebenso weltweit aktiven Pendant „Helium“ der finanzielle Faktor. Die meisten Helium-Hotspots (Gateways) betreiben Privatpersonen, die dafür sowie für die übertragenen Datenpakete kleine Beträge in Kryptowährung erhalten. Dass Geld eher zieht als Philanthropie, beweisen die rund 345.500 aktiven Helium-Hotspots, denen etwa 113.800 TTN-Gateways gegenüberstehen. Helium hat nicht nur in Mitteleuropa solide Abdeckung; insbesondere in Süd- und Osteuropa, in der Türkei, auf Zypern und im Libanon gibt es deutlich mehr Helium- als TTN-Gateways. Das macht das Netz für alle die spannend, die LoRaWAN überregional – etwa für Ortungsgeräte – einsetzen möchten oder keine eigenen reichweitenstarken Gateways aufbauen wollen oder können.

Wie Sie Helium zusammen mit der Flowchart-Programmieroberfläche Node-Red einsetzen, ohne einen Hotspot aufzubauen, beleuchten wir in diesem Artikel. Die Node-Red- und LoRaWAN-Grundlagen sparen wir uns dabei; sind Sie Einsteiger, lesen Sie am besten unsere Grundlagenartikel mit Produktbeispielen in [1, 2, 3, 4]. Sie beziehen sich hauptsächlich aufs The Things Network, doch im Helium-Netz wird auch nur mit Wasser gekocht – beziehungsweise mit standardkonformem LoRaWAN. Die Verwaltungskon-

sole sieht etwas anders aus, aber vieles wird Ihnen bekannt vorkommen.

Voraussetzungen

Anders als das The Things Network besitzt das Helium derzeit keinen MQTT-Broker, über den man die Daten aus der Ferne mit einer ausgehenden Verbindung abfragen könnte. Pakete leitet Helium momentan ausschließlich über HTTP(S)-POST-Requests an externe Anwendungen weiter. Solche kann man mit einem HTTP-In-Node in Node-Red problemlos entgegennehmen. Voraussetzung ist jedoch, dass die Node-Red-Instanz an einer öffentlichen IPv4-Adresse über das Internet erreichbar ist. Damit die Daten nicht unverschlüsselt durchs Netz reisen, sollten Sie auch einen HTTPS-Proxy für Node-Red eingerichtet haben. Das geht etwa mit dem Docker-Container Traefik (ct.de/yvjx, [5]).

Besitzen Sie keine öffentliche IPv4-Adresse, können Sie beispielsweise eine günstige virtuelle Maschine bei einem Hoster buchen und dort Node-Red installieren oder den Dashboard-Provider Datacake ausprobieren, der ebenfalls Daten aus externen Anwendungen entgegennehmen kann. Links dazu finden Sie unter ct.de/yvjx.

Um Einheiten für die Datenübertragung in Helium zu kaufen, benötigen Sie zudem eine Kreditkarte. Die müssen Sie aber nicht sofort preisgeben, denn zum Start gibts 500 Einheiten zum Spielen. Außerdem läuft die Abrechnung auf Prepaid-Basis, sodass keine bösen Überraschungen möglich sind.

Abdeckung

Unabhängig davon, ob Sie Helium regional nutzen wollen oder etwa nur als LoRaWAN-Redundanz zu einem GSM/LTE-gestützten Ortungsgerät, sollten Sie die Abdeckung in Ihrer Nähe prüfen, bevor Sie ans Werk gehen. Auch das Ortungsgerät sollte regelmäßig ein Kontroll-Lebenszeichen senden können.

Dafür gibt mehrere Möglichkeiten: hotspotty.net liefert Hotspot-Standorte und dazugehörige Statistiken; die angezeigten Hexagone repräsentieren jedoch nicht die tatsächliche Abdeckung. Diese erfahren Sie (möglicherweise) auf coveragemap.net. Das ist das Helium-Pendant zum TTN Mapper und stützt sich genauso auf durch LoRaWAN-Tracker ermittelte Messpunkte. Zeigt die Seite an Ihrem Standort keine Heatmap an, existieren dafür schlicht keine Datenpunkte.

Gibt es in erreichbarer Umgebung keinen Hotspot, sollten Sie über einen eigenen nachdenken. Dieser Artikel liefert dafür zwar keine Anleitung, unter ct.de/yvjx haben wir jedoch (englische) Infoseiten dazu verlinkt.

Kosten

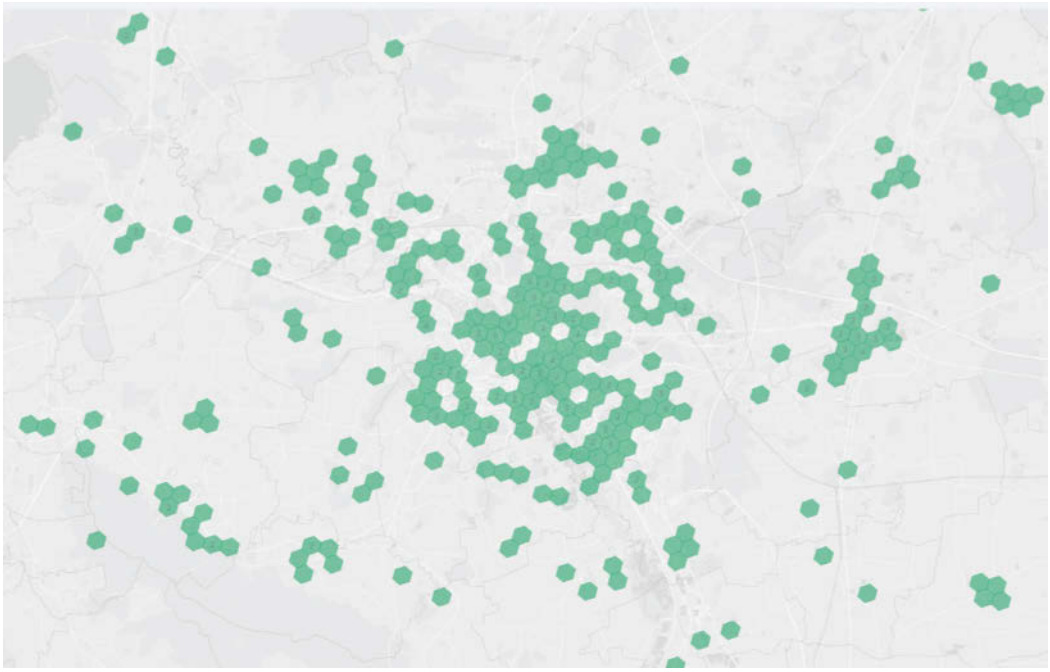
Das Benutzen der Serverinfrastruktur und das Anlegen von LoRaWAN-Geräten in Helium ist kostenfrei. Datenpakete verursachen jedoch Kosten, die über ein Prepaid-Konto beglichen werden. Die Abrechnungseinheiten heißen in Helium „Data Credits“ und einer kostet derzeit 0,000047 Euro, für den Mindestbetrag von 4,75 Euro (5 US-Dollar) bekommt man also 100.000 Stück.

Ein LoRaWAN-Paket bis 24 Byte Länge kostet einen Data Credit, Pakete zwischen 25 und 48 Byte Länge werden mit zwei Data Credits berechnet und alles darüber hinaus mit elf Data Credits. LoRaWAN-Geräte sind aber sparsam: Typische Atmosphärensensoren verschicken in der Regel weniger als 24 Byte große Pakete. Unser für diesen Artikel in Helium eingebuchte Dragino LGT-92 (GPS-Tracker) versendet 30 Byte pro Durchgang. Das liegt daran, dass er nicht nur die Koordinaten, sondern auch Lagewerte und den Status mancher Einstellungen mitschickt.

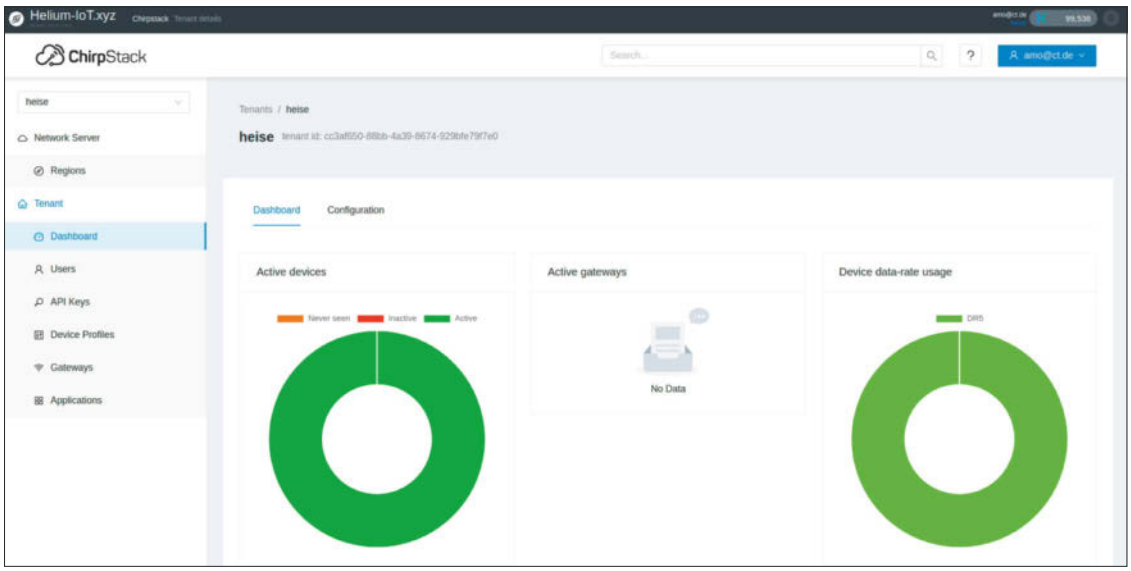
Der Kurs ist gut; als Beispiel: Gehen wir davon aus, dass der Tracker Bewegungserkennung aktiviert hat, zwei Stunden pro Tag bewegt wird und dabei alle fünf Minuten einen Standort verschickt,

c't kompakt

- Das LoRaWAN „Helium“ belohnt Abdeckung mit Kryptowährung, das hat für viel Verbreitung gesorgt.
- Auch ohne Hotspot kann sich jeder anmelden und das Netz benutzen.
- Ein Datenpaket kostet nur einen Bruchteil eines Cents.



Helium kann in an vielen Orten – wie hier in Hannover – eine deutlich höhere Gateway-Dichte als das The Things Network aufweisen. Die Website hotspotty.net zeigt Hotspot-Standorte.



Wer das The Things Network bereits kennt, wird sich im Helium-ChirpStack-Interface ebenso zurechtfinden. Menüführung und einige Begriffe sind anders, doch daran gewöhnt man sich schnell.

sind das 24 Pakete pro Tag und folglich 8760 Pakete im Jahr. Helium berechnet pro 30-Byte-Paket zwei Data Credits, also 17.520 DC pro Jahr. Diese kosten umgerechnet 82 Cent. Die 4,75 Euro erkaufen in diesem Anwendungsfall also fast sechs Jahre Konnektivität.

Anmeldung

Die Helium-Verwaltungskonsole erreichen Sie über console.helium-iot.xyz. Sie wird vom französischen IoT-Dienstleister Ingenious Things betrieben und ist bei einem Hoster untergebracht, der so französisch ist, dass er seine eigene Website ausschließlich in der Landessprache anbietet – alles EU-Datenschutz also.

Zum Anmelden öffnen Sie die Seite und klicken auf „No account? signup!“. Die Felder sind größtenteils selbsterklärend; „tenant/org name“ vergeben Sie frei und „coupon code“ bleibt leer. Danach bestätigen Sie noch Ihre E-Mail-Adresse und melden sich in der Konsole an.

Dort begrüßt Sie eine ChirpStack-Oberfläche; ChirpStack ist eine quelloffene LoRaWAN-Serversoftware, die Ingenious Things in angepasster Form benutzt. Die Begriffe links im Menü ähneln denen im The Things Network stark und dürften Ihnen bekannt vorkommen. Ein paar Dinge sind dennoch anders: Geräteeinstellungen und Decoder werden in sogenannten „Device Profiles“ definiert und nicht in der Anwendung (Application). Sie referenziert man wiederum beim Anlegen von Geräten, sodass Geräte unterschiedlichen Typs in einer Anwendung existieren können, ohne dass das Einrichten hohen Aufwand bedeutet.

Gerätekonfiguration

Um das erste Gerät in Helium einzubuchen, erstellen Sie somit zuerst ein Geräteprofil: Öffnen Sie dazu das Menü „Device Profiles“ und klicken Sie auf „Add device profile“. Im Reiter „General“ vergeben Sie einen Namen passend zum Gerät und optional eine Beschreibung; für beide Regionsfelder wählen Sie „EU868“, die „MAC Version“ sowie die „Regional parameters revision“ füllen Sie anhand des Datenblatts des Geräts. Im Falle des Dragino LGT-92 ist das „LoRaWAN 1.0.2 Rev B“.

Die Reiter OTAA, Class-B und Class-C passen Sie ebenso anhand der Herstellerinformationen zum Gerät an. Da der LGT-92 nur ein Class-A-Gerät ist und OTAA zur Anmeldung nutzt, sind hier – wie bei vielen anderen akkubetriebenen Geräten – keine Anpassungen nötig.

Der „Codec“ alias Decoder ist das Stück JavaScript, welches das Paket zerteilt, verarbeitet und als menschenlesbares JSON ausgibt – sofern Ihr Gerät nicht im standardisierten Cayenne-LPP-Format sendet. In ChirpStack funktionieren JavaScript-Decoder ein bisschen anders als im TTN, weshalb man die von Herstellern gelieferten Decoder nicht 1:1 übernehmen kann. ChirpStack erwartet im Feld „Codec functions“ die Funktion `decodeUplink` und übergibt dieser ein Objekt mit der LoRaWAN-Nutzlast als Byte-Array, dem Port und den Gerätevariablen, während die meisten TTN-Decoder das Byte-Array und den Port als einzelne Parameter annehmen. Sofern der Hersteller Ihres Geräts keinen separaten ChirpStack-Decoder bietet, passen Sie diesen selbst an; eine Anleitung dazu finden Sie über ct.de/yvjx.

Mit vollständigem Codec ist das Device Profile fertig und Sie bestätigen die Eingaben mit „Submit“.

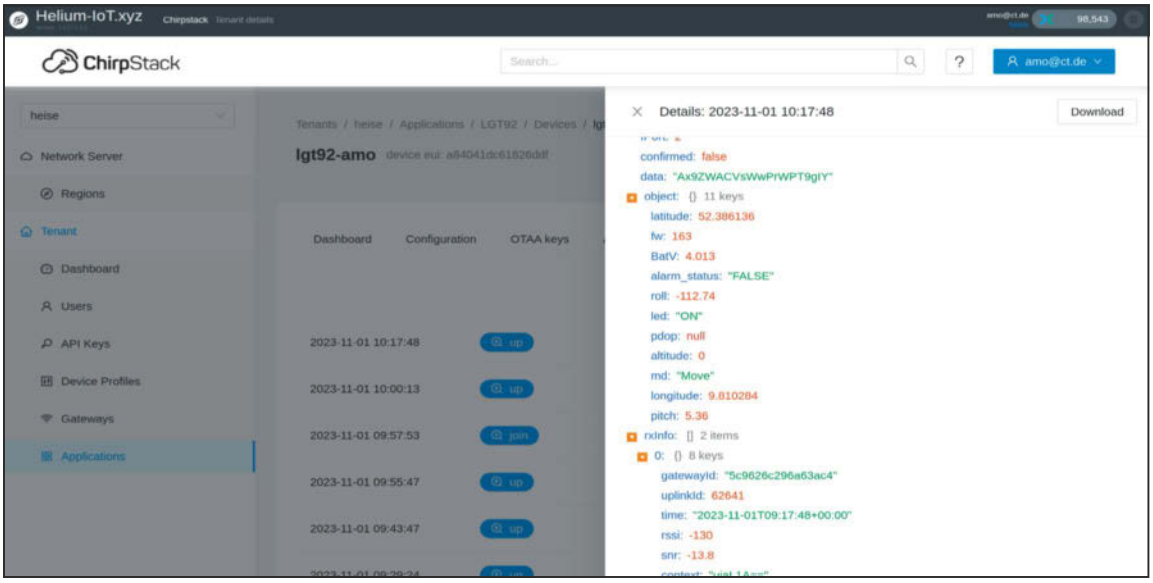
Wechseln Sie in das Menü „Applications“, um Ihre erste Anwendung anzulegen. Klicken Sie auf „Add application“, vergeben Sie einen Namen und klicken Sie „Submit“. Viel einzurichten gibt es vorerst nicht: Im nächsten Menü wählen Sie „Add device“, um ein Gerät hinzuzufügen – das Menü ist bis auf die „JoinEUI“ selbsterklärend. Die heißt bei manchen Herstellern „AppEUI“. Außerdem fehlt das AppKey-Feld in diesem Menü; er wird erst nach dem ersten „Submit“ gefordert. Geben Sie ihn ein, klicken Sie erneut auf „Submit“.

Nach dem Eingeben des AppKeys ist Ihr Gerät bereit für einen Test: Wechseln Sie in den Reiter „LoRaWAN frames“ und schalten Sie das Gerät ein. Ist ein Gateway in Reichweite, sollte wenig später ein Paket eintreffen. Verwendet das Gerät ABP, ist kein Austausch von Schlüsseln nötig und eventuell dauert es etwas, bis etwas passiert – die Anleitung des Herstellers verrät Näheres.

Weiterleitung

Um die Daten in Node-Red zu empfangen, öffnen Sie zunächst das Node-Red-Webinterface und legen optional einen neuen Flow für Helium-Daten an. In diesen Flow ziehen Sie dann einen HTTP-In-Node und öffnen dessen Einstellungen per Doppelklick: Die Methode lautet „POST“ und die URL können Sie beliebig wählen; sie muss mit einem Schrägstrich eingeleitet werden, also etwa `/helium-post-lgt92`.

Im Helium-Webinterface öffnen Sie – wenn Sie sie nicht noch offen haben – die



Wie das TTN bietet auch die Chirpstack-Konsole eine Live-Ansicht der eingehenden Datenpakete.

Anwendung, von der Sie die Daten weiterleiten wollen, und wechseln in den Reiter „Integrations“. Suchen Sie die HTTP-Integration und klicken Sie auf das Plus, um diese hinzuzufügen. Im folgenden Konfigurationsmenü tragen Sie die Adresse Ihrer Node-Red-Instanz zuzüglich des Pfades als „Event endpoint URL“ ein, etwa `https://nr.ct.example.com/helium-post-lgt92`, und bestätigen mit „Submit“.

Im Node-Red-Flow hängen Sie anschließend einen Debug-Node an den HTTP-In-Node und klicken auf „Übernehmen (Deploy)“, damit die Änderungen übernommen werden. Anschließend schalten Sie das LoRaWAN-Gerät aus und wieder ein oder stoßen anderweitig eine Übertragung an. Kommen die Daten an, können Sie damit in Node-Red weiterarbeiten; der HTTP-In-Node erkennt automatisch, dass es sich um ein JSON-Objekt handelt, und konvertiert es entsprechend. Die dekodierte Nutzlast befindet sich in `msg.payload.object`. Tut sich nichts, prüfen Sie die eingetragene URL in der HTTP-Integration und etwaige Firewall-Einstellungen für die eingehende Verbindung.

Traccar

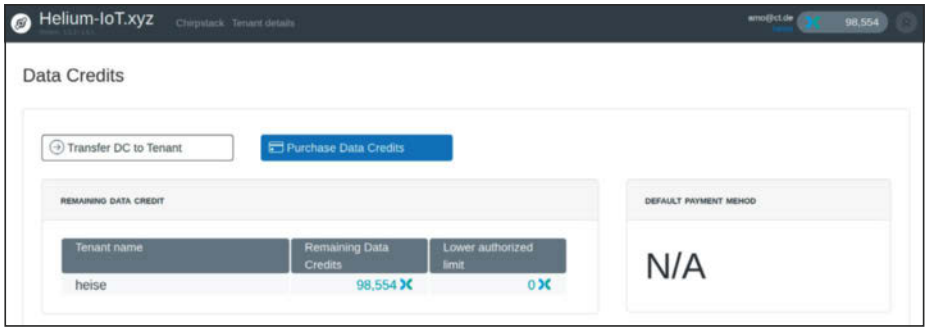
Gerade der Tracking-Anwendungsfall ist mit Helium spannend, weil LoRaWAN-Ortungsgeräte deutlich seltener funken und auch weniger Sendeleistung verwenden als welche mit Mobilfunk, sodass das Auffinden mit HF-Suchgeräten (Wanzenfindern) wesentlich schwieriger ist – ein Vorteil für den Diebstahlschutz.

Der GPS-Tracker-Server Traccar [6] eignet sich sehr gut zur unkomplizierten Kombination mit LoRaWAN-Ortungsgeräten. Wie das mit dem The Things Network zusammen mit einem PHP-Übersetzerskript geht, haben wir bereits in c’t 21/2021 beschrieben [7]. Ein passendes PHP-Skript haben wir nun auch für Helium gebaut, das sie über ct.de/yvjx finden. Sie können also der Anleitung größtenteils folgen und die URL zum Skript in der HTTP-Integration auf der Helium-Konsole einfügen. Beachten Sie jedoch, dass wir mittlerweile die Installation mittels Docker empfehlen.

Aufgeladen

Wenn Sie mit den ersten 500 Data Credits positive Erfahrungen sammeln konnten und Helium weiter nutzen wollen, klicken Sie oben rechts neben Ihrer E-Mail-Adresse auf den Kontostand und dann auf „Purchase Data Credits“. 100.000 Stück, also 5 US-Dollar, sind das Minimum, das Sie eingeben müssen. Anschließend klicken Sie auf „Purchase with Credit Card“ und geben Ihre Daten ein.

Helium beziehungsweise ChirpStack besitzt weit mehr Funktionen, als dieser Artikel abdeckt. Links zu weiteren Dokumentationen – etwa dazu, wie man Downlink-Pakete verschickt – haben wir unter ct.de/yvjx für Sie verlinkt. *(amo@ct.de)* c't



Die Data Credits (DC) sind die Währung im Helium. Die Pakete sind allerdings so günstig, dass man selbst mit etwas weniger als 5 Euro viel erreicht, und zum Einstieg gibts 500 DC zum Ausprobieren.

Literatur

[1] Jan Mahn, Reaktionsmaschine, Einstieg in Heimautomation mit Node-Red, c’t 15/2018, S. 142

[2] Jan Mahn, Langstreckenfunk, IoT-Funk LoRaWAN: für kleine Datenmengen und hohe Reichweiten, c’t 10/2019, S. 140

[3] Andrijan Möcker, Plug & Funk, LoRaWAN für IoT-Projekte: Einfach einsteigen mit TTN und Node-Red, c’t 14/2021, S. 148

[4] Andrijan Möcker, Selbstbaunetz für die Smart City, LoRaWAN: Grundlagen, Netzausbau, Anwendungen, c’t 19/2023, S. 22

[5] Jan Mahn, HTTP-Einweiser, Eingehenden HTTP-Verkehr mit Traefik routen, c’t 17/2019, S. 158

[6] Andrijan Möcker, Protokollant der Herumtreiber, GPS-Tracker-Server Traccar: Ortungsportal selbst gemacht, c’t 18/2023, S. 150

[7] Andrijan Möcker, Positionsübersetzer, LoRaWAN-GPS-Tracker mit Traccar verbinden, c’t 21/2021, S. 162

Decoder, PHP-Skripte, Dokumentation:
ct.de/yvjx

IoT zum Sparpreis

Verdeckten Raspberry Pi 4 im Helium-Hotspot befreien

Eine LoRaWAN-Basis und ein Raspberry-Pi-4-Komplettset zum kleinen Preis: Das bekommt man mit dem Helium-Hotspot SenseCAP M1, der derzeit günstig gebraucht im Netz erhältlich ist. Wir erklären, worauf Sie achten müssen und wie Sie das Gerät ins The Things Network umziehen.

Von Andrijan Möcker

Wer in die Themen Smart City, Smart Home ohne Cloud und Internet of Things (IoT) einsteigen will, sieht sich schnell mit den Preisen für Raspberry Pis, die gut als Einsteiger-Heimserver taugen, und denen für Gateways für den IoT-Funkstandard LoRaWAN konfrontiert [1]. Beides ist zwar nach den Jahren der Chipknappheit und Wucherpreisen wieder gut und vergleichsweise günstig verfügbar, trotzdem knackt ein Starterset aus beiden Gerätetypen mit allem nötigen Zubehör leicht die 350-Euro-Marke.

Derzeit kann man aber auch 100 bis 280 Euro günstiger zum Ziel kommen: mit dem SenseCAP M1 von Seeed Studio. Er ist eigentlich ein Hotspot – also eine Basisstation alias Gateway – für das LoRaWAN-Projekt „Helium“, das für den Betrieb und das Weiterleiten der von LoRa-Sensoren gefunkten Datenpakete kleine Beträge in Kryptowährung auslobt.

Im formschönen Alugehäuse steckt ein handelsüblicher Raspberry Pi 4, gepaart mit einem LoRaWAN-Gateway-Modul, einem aktiven Kühler und einer hochwertigen microSD-Karte. Ein USB-C-Netzteil und eine 868-MHz-Antenne sind ebenfalls im Set. Das alles wird derzeit gebraucht für 70 bis 200 Euro gehandelt: ein sehr guter Deal.

Einziger Nachteil der Konstruktion: Die seitliche Abdeckung blockiert die USB-Ports des Raspi. Mit einer kleinen Handfräse lassen sie sich aber freilegen. An die Micro-HDMI-Anschlüsse kommt man allerdings nur mit Winkelsteckern.

Im Helium-Modus hat man keinen Zugriff auf das Linux des M1, kann also nichts weiter damit anstellen. Allerdings hindern einen nur zwei Schrauben daran, das zu ändern: Überschreibt man die eingesteckte MicroSD-Karte mit einem frischen Raspberry Pi OS, hat man alle Freiheiten auf dem Platinchen.

Als gewinnbringenden Helium-Hotspot kann man den M1 dann nicht mehr einsetzen, der LoRaWAN-Teil funktioniert aber trotzdem und kann etwa mit dem The Things Network verbunden werden. Wie das geht, erzählen wir später im Artikel. Grundlagen zu LoRaWAN, dem The Things Network und wie Sie damit loslegen, finden Sie über die Literaturverweise am Ende.

Dieser Artikel leistet zwar keine umfangreichen Hilfestellungen zum Einrichten des Raspberry Pi und der Bedienung des Linux-Systems, die Raspberry-Pi-Foundation liefert auf ihrer Website jedoch eine englische Schritt-für-Schritt-Anleitung zum Start. Wir haben die Anleitung und weitere Hilfeseiten unter ct.de/yjkk verlinkt. Für die Installation benötigen Sie einen Rechner mit einem microSD-Slot oder einem SD-Slot zuzüglich microSD-Adapter. Den Raspi binden Sie wahlweise über Kabel oder WLAN ins Heimnetz ein.

Einkaufstour

Beim Kauf des SenseCAP M1 lohnt es sich, auf die Speicherausstattung zu achten: Sie variiert, denn der Hersteller hat Raspis mit 2, 4 und 8 GByte großem Arbeitsspeicher gekauft und zufällig eingebaut. Einige Verkäufer schreiben die Speicherausstattung direkt in das Angebot. Fehlt die Angabe, bitten Sie den Verkäufer, Ihnen die Modellnummer vom Etikett zu nennen, sie lautet etwa „Model: M1-4868“. Die erste Ziffer hinter dem Bindestrich steht für die RAM-Ausstattung, die drei Ziffern dahinter für das vom LoRaWAN-Gateway-Modul unterstützte Frequenzband.

In nahezu allen von uns entdeckten Angeboten war das Band als „868 MHz“ oder „EU868“ angegeben; das ist momentan der einzige Bereich, in dem LoRaWAN in Europa großflächig genutzt wird. Fehlt es, fragen Sie den Verkäufer unbedingt nach der Modellbezeichnung. In der Zeit des Hypes um Kryptowährungen gab es einen regelrechten Sturm auf die Geräte und es ist nicht auszuschließen, dass Menschen aus Unwissenheit Geräte aus oder für Nordamerika bestellt haben. Deren LoRaWAN-Module arbeiten um 915 MHz; sie dürfen in Europa nicht in Betrieb genommen werden. Der Raspberry im Gerät funktioniert natürlich trotzdem.

Die günstigsten Fänge können Sie auf den Kleinanzeigen-Portalen machen. Stellen Sie sich darauf ein, wenigstens 100 Euro auszugeben; mit Glück klappt es für 70 bis 95 Euro. Kaufen Sie lieber von Händlern, dann schauen Sie bei eBay, wo der M1 nur unwesentlich teurer ist: Zwischen 130 und 200 Euro müssen Sie dort einplanen.

Basisinstallation

Die Installation eines neuen Raspberry Pi OS ist schnell erledigt: Die Raspberry Pi Foundation bietet mittlerweile ein komfortables Tool für Windows, macOS und Linux, das das Betriebssystem automatisch herunterlädt und die microSD-Karte damit vorbereitet. Die Schritt-für-Schritt-Anleitung finden Sie über ct.de/yjkk.

Vorsicht beim Entfernen der SD-Karte: Sie ist mit einem Stück Klebeband gesichert, das man abziehen muss.

Klicken Sie beim Beschreiben der SD auf „Edit Settings“, wenn das Tool Ihnen

die Frage „Use OS customisation?“ stellt. Dann können Sie einen Hostnamen, WLAN-Zugangsdaten, einen Benutzernamen, ein Kennwort und weiteres konfigurieren und anschließend direkt per SSH auf das Gerät kommen, ohne vorher noch mal einen Bildschirm anschließen zu müssen.

Nach abgeschlossener Installation suchen Sie die neue IP-Adresse des Pi mit einem Netzwerkscanner wie Fing oder im Webinterface Ihres Routers und verbinden sich über einen SSH-Client mit der Konsole des Betriebssystems. Dafür benutzen Sie die zuvor im Imaging-Tool vergebenen Zugangsdaten.

Führen Sie zunächst `sudo apt update && sudo apt upgrade -y` aus, um die Paketlisten zu aktualisieren und eventuelle Updates zu installieren; Betriebssystemabbilder sind nur am Tag ihrer Veröffentlichung aktuell.

LoRaWAN-Gateway

Um das Gateway-Modul zu aktivieren, müssen Sie nur zwei Schnittstellen zum Leben erwecken und ein kleines Stück Software herunterladen, das die LoRa-Pakete vom Modul abholt und an einen Server weiterleitet: den Packet Forwarder. Haben Sie keine Erfahrung mit LoRaWAN, schauen Sie zunächst in die Grundlagenartikel [1, 2].

Vergessen Sie auf keinen Fall, die mitgelieferte Antenne anzuschrauben, bevor Sie anfangen! Ist kein Strahler an der RP-SMA-Buchse, kann das Modul beim Senden irreparabel beschädigt werden.

Damit der Dienst mit dem Modul sprechen kann, müssen das Serial Peripheral Interface (SPI) und der Inter-Integrated-Circuit-Bus (I^2C) aktiviert werden: Öffnen Sie dazu das Konfigurationstool mit `sudo raspi-config`, setzen Sie SPI und I^2C im Menü `Interface Options` auf `enable` und verlassen Sie den Dialog wieder. Ein Neustart mit `sudo reboot` stellt sicher, dass die Änderungen übernommen werden. Verbinden Sie sich danach direkt wieder per SSH, es geht in der Konsole weiter.

Installieren Sie zuerst die Versionsverwaltung git: `sudo apt install git -y`. Damit laden Sie den Quelltext herunter: `git clone https://github.com/Lora-net/sx1302_hal`. Dann wechseln Sie mit `cd sx1302_hal` in den Ordner und starten den Compiler mit `make`. Anschließend müssen noch einige Reset- und Einschalt-Pins im

Der Raspberry Pi sitzt zusammen mit der LoRa-Gateway-Platine im Alugehäuse. Der Hersteller hat ihm sogar einen aktiven Kühler spendiert.

Reset-Skript richtig eingestellt werden. Dazu öffnen Sie das Skript mit dem Befehl `nano tools/reset_lgw.sh` im Texteditor Nano und ändern die Pin-Nummern bei folgenden Parametern wie gezeigt:

```
SX1302_RESET_PIN=17
SX1302_POWER_EN_PIN=18
SX1261_RESET_PIN=5
```

Die Navigation in Nano läuft über die Pfeiltasten. Speichern Sie die Änderungen mit Strg+O, beenden Sie den Texteditor mit Strg+X und kopieren Sie das Skript mit `cp tools/reset_lgw.sh packet_forwarder/` in den Ordner des Packet Forwarders.

Zuletzt müssen Sie die Konfigurationsdatei des Forwarders mit einer Gateway-ID und den Serveradressen anpassen: `nano global_conf.json.sx1250.EU868` Scrollen Sie herunter bis zu `"gateway_conf"`, um dort die `gateway_ID` zu editieren: Entfernen Sie die letzten 12 Stellen (5A und alle folgenden Nullen) und ersetzen Sie sie wahlweise durch die WLAN- oder die Ethernet-MAC-Adresse vom Etikett des M1 (Unterseite), aber ohne die Doppelpunkte zu übernehmen. Kopieren Sie die Gateway-ID zusätzlich in ein Textdokument auf Ihrem Rechner, um sie später ins The Things Network übertragen zu können.

Direkt unter der ID folgen die Server-Parameter: Setzen Sie `server_address` auf `eu1.cloud.thethings.network` und beide Port-Parameter auf `1700`.

Die Keepalive- und Stat-Intervalle bestimmen, wie oft der Forwarder Lebenszeichen und Statistiken an den LoRaWAN-Server sendet. Die voreingestellten Werte – beide in Sekunden – sind unserer Ansicht nach etwas übertrieben. 30 Sekunden Keepalive und 120 Sekunden Stat-Intervall genügen völlig.

Die Einstellungen sind danach einsatzbereit; speichern Sie mit Strg+O und schließen Sie Nano mit Strg+X.

Bevor Sie den Forwarder starten, legen Sie einen Gateway-Eintrag im The Things Network an: Öffnen Sie eu1.cloud.thethings.network im Browser, klicken Sie auf „Go to gateways“ und dort auf „Register gateway“. Tragen Sie die zuvor im Textdokument gespeicherte Gateway-ID in das Feld „Gateway EUI“ ein und bestätigen Sie mit „Confirm“. Dann vergeben Sie die „Gateway ID“ und den „Gateway name“, wie Sie möchten; der Frequenzplan muss „Europe 863-870 MHz (SF9 for RX2 - recommended)“ lauten. Wollen Sie nicht, dass Gateway-Standort und -Status öffentlich sichtbar sind, entfernen Sie noch die blauen Haken am Ende. Mit „Register gateway“ übernehmen Sie alles.

Das muss man beim Antennenkauf beachten: Seeed Studio hat sich für RP-SMA statt wie üblich für SMA entschieden. Für viele LoRa-Antennensets wird man somit einen Adapter benötigen.

Zu Diensten

Wechseln Sie wieder zum SSH-Client, der mit Ihrem Raspi verbunden ist, um den Forwarder für einen ersten Test zu starten. Das erledigen Sie mit dem Befehl `./lora_pkt_fwd -c global_conf.json.sx1250.EU868` – vorausgesetzt, Sie sind noch im Ordner `sx1302_hal/packet_forwarder`; wenn nicht, wechseln Sie mit `cd` wieder hinein.

Beobachten Sie gleichzeitig die TTN-Seite des Gateways; wenige Sekunden nach dem Gateway-Start sollte es Ihnen als „Connected“ angezeigt werden. Wenn nicht, müssen Sie die Seite möglicherweise neu laden. Passiert dann noch immer nichts, beobachten Sie die Anzeige im SSH-Terminal auf Fehlermeldungen. Taucht kein Fehler auf und Ihnen werden sogar empfangene Pakete angezeigt, die aber nicht im TTN ankommen, blockiert möglicherweise eine Firewall die ausgehenden Pakete.

Klappt alles, beenden Sie den Dienst wieder mit Strg+C, um einen systemd-Service einzurichten, der den Forwarder bei Absturz oder Neustart wieder in Gang setzt. Dazu kopieren Sie den Forwarder zunächst nach `/usr/local/bin`, wo er besser aufgehoben ist als in Ihrem Home-Verzeichnis: Springen Sie mit `cd ..` eine Ebene höher, sodass Sie im Ordner `sx1302_hal` sind, dann kopieren Sie den Ordner `packet_forwarder` nach `/usr/local/bin`: `sudo cp -r packet_forwarder/ /usr/local/bin/packet_forwarder`.

Dann legen Sie das Service-File an, das systemd die Einstellungen mitteilt: Wechseln Sie mit `sudo -i` in den Superuser-Modus und dann in den Ordner mit den Service-Files: `cd /etc/systemd/system` Mit `nano packet-forwarder.service` legen Sie das neue Service-File an; unter ct.de/yjkk haben wir den nötigen Inhalt verlinkt, den Sie einfach hineinkopieren. Sollten Sie unsere Anweisungen zuvor nicht ganz übernommen und etwa Ordnernamen geändert haben, müssen Sie die Pfade im Service-File anpassen. Speichern und verlassen Sie den Editor mit Strg+O und Strg+X.

Mit `systemctl enable packet-forwarder.service` weisen Sie systemd an, den neuen Service zu übernehmen, und mit `service packet-forwarder start` geben Sie den Startschuss. Zuletzt machen Sie in der TTN-Konsole und mit `service packet-forwarder status` eine Kontrolle; steht der Dienst auf „active (running)“ und tauchen unten im Log Meldungen auf wie `RF packets received by concentrator:...`, läuft alles wie gewünscht. Gibt es Fehlermeldungen, prüfen Sie noch einmal alle Pfade im Service-File. Stellen Sie einen Fehler fest, beheben Sie ihn und laden das File mit `systemctl daemon-reload` neu.

Losvernetzt

Der Raspberry Pi 4 im SenseCAP M1 ist mit dem LoRaWAN-Packet-Forwarder vollkommen unterfordert. Der Dienst verursacht meist weniger als 10 Prozent CPU-Last und das auch nur auf einem der vier Kerne, der Rest langweilt sich. Diesem unhaltbaren Zustand können Sie begegnen, indem Sie das Platinchen mit weiteren Aufgaben beschäftigen.

In c’t 14/2021 [2] erklären wir etwa, wie Sie die Flowchart-Programmieroberfläche Node-Red mit dem The Things Network verbinden und mit den Daten der LoRaWAN-Geräte arbeiten. In c’t 16/2023 [4] nutzen wir die Daten aus dem TTN, um dynamische Karten zu erstellen. Aber auch für typische Smart-Home-Zentralen wie OpenHAB oder Home Assistant hat der Raspberry Pi noch mehr als genug Rechenleistung über. *(amo@ct.de)* **ct**

Literatur

[1] Jan Mahn, Langstreckenfunk, IoT-Funk LoRaWAN: für kleine Datenmengen und hohe Reichweiten, c’t 10/2019, S. 140
[2] Andrijan Möcker, Plug & Funk, LoRaWAN für IoT-Projekte: Einfach einsteigen mit TTN und Node-Red, c’t 14/2021, S. 148
[3] Jan Mahn, Reaktionsmaschine, Einstieg in Heimautomation mit Node-Red, c’t 15/2018, S. 142
[4] Andrijan Möcker, Knotenkarte, Dynamische Karten mit Node-Red, c’t 16/2023, S. 142

***Anleitungen, Dateien:* ct.de/yjkk**

Bild: KI Midjourney | Bearbeitung c't

Paketfließband

Pakete mit Nix managen und bauen, Teil 2

Der zweite Teil dieser Einführung in den Paketmanager Nix für Entwickler bohrt das Beispielprojekt auf: Automatische Checks, problemlose Einbindung in CI-Pipelines, plattformunabhängige Paketbeschreibungen – all das ist mit Nix nur ein paar Config-Zeilen entfernt.

Von Jacek Galowicz

Der Paketmanager Nix glänzt mit ungewöhnlichen Fähigkeiten, die insbesondere für Entwickler interessant sind: schnell mal ein Programm ausprobieren, spontan und temporär ein paar Tools in einer Shell verfügbar machen oder dauerhafte, reproduzierbare Entwicklungsumgebungen einrichten. All das kombiniert Nix mit einer immensen Softwareauswahl, ohne dass man sich mit Containern oder virtuellen Maschinen herumschlagen muss.

Der erste Teil dieser Einführung in Nix [1] hat gezeigt, wie Sie eine kleine „Flake“-Datei erstellen, mit der Nix ein C++-Testpaket baut. Eine erweiterte Version dieser Flake zeigt das Listing auf Seite 144. Neben dem C++-Paket beschreibt diese Version auch noch ein Rust-Paket – Flakes können durchaus mehrere Pakete beschreiben. Das Rust-Paket ist ganz ähnlich aufgebaut, nur nutzt es statt CMake das Rust-Tool Cargo. Außerdem ruft es nicht `mkDerivation` auf, sondern die Hilfsfunktion `buildRustPackage`; dazu später mehr.

Das Listing müssen Sie nicht abtippen, Sie finden diesen Stand der Flake auch im GitHub-Repository des Autors via heise.de/s/leP5.

Flake-Parts

Die Pakete und die Shell-Definition der Flake funktionieren (zum Beispiel per `nix run .#hello-rust`), sind aber im Flake-Attributpfad auf eine bestimmte Systemarchitektur festgelegt (über die Variable `system`). Nutzer einer anderen Architektur müssen die Variable anpassen, damit die Flake funktioniert. Das lässt sich sehr bequem verbessern, mit einer Biblio-

thek namens Flake-Parts. Dafür passen Sie die Definition von `outputs` wie folgt an:

```
outputs = inputs:
  inputs.flake-parts.lib.mkFlake {
    inherit inputs;
  } {
    systems = [
      "x86_64-linux"
      "aarch64-linux"
      "x86_64-darwin"
      "aarch64-darwin"
    ];
    perSystem = {
      config, pkgs, system, ...
    }: {
      devShells.default = # ...
      packages = {
        hello-cpp = # ...
        hello-rust = # ...
      };
    };
  };
```

Achten Sie auf die mit dem Kommentar `# ...` markierten Auslassungen! Dort übernehmen Sie die Definitionen aus der originalen Flake. Die Funktion `outputs` hat nur noch einen Parameter `inputs`, statt einer Parametermenge (`self` und `nixpkgs`). Der Einschub `inputs.flake-parts.lib.mkFlake {…}` zwischen Funktionskopf und -körper sorgt dafür, dass man im Code der Funktion Helferlein der Flakes-Parts-Bibliothek nutzen kann. Wie genau so ein Einschub funktioniert, führt hier zu weit. Es kommen verschiedene Besonderheiten davon zum Einsatz, wie Nix Funktionen handhabt (siehe ct.de/ycxk).

Ein solches Helferlein, das nun in der `outputs`-Funktion zur Verfügung steht, ist `perSystem`: Alles, was Sie in diesem Attribut definieren, übersetzt Nix automatisch in Attributpfade für alle Architekturen (die in `systems` stehen): Aus `packages.hello-cpp` wird `packages.x86_64-linux.hello-cpp`, `packages.aarch64-linux.hello-cpp` und so weiter. So kann man sich darauf konzentrieren, portable Paketbeschreibungen zu spezifizieren, um dann an einer zentralen Stelle der Flake zu definieren, welche Architekturen sie denn unterstützt.

Damit `inputs.flake-parts` allerdings überhaupt zur Verfügung steht, muss man der Flake ein `inputs`-Attribut verpassen, das Sie zwischen `description` und `outputs` einfügen können:

```
inputs = {
  flake-parts.url = "github:hercules-↵
                                ↳ci/flake-parts";
  nixpkgs.url = "github:nixos/nixpkgs/↵
  ↳nixos-unstable";
};
```

Die erste Input-Angabe definiert, woher die Flake-Parts-Bibliothek kommt. Die zweite beschreibt, aus welchem Git-Repository und welchem Branch die `nixpkgs`-Paketdefinitionen sein sollen. Bislang fehlte diese Angabe. Weil die Flake `nixpkgs` verwendete, aber nicht als Input-spezifizierte, hat Nix die Lücke mit der globalen Nix-Registry auf GitHub gestopft. Die explizite Angabe verweist auf dieselbe Quelle, macht das aber deutlicher und ermöglicht in Zukunft Anpassungen, beispielsweise um bestimmte Branches auszuwählen.

Die Shell und die Pakete aus dieser Flake funktionieren nun automatisch sowohl unter Linux als auch macOS und auf verschiedenen Prozessorarchitekturen.

Flake-Checks

Die nächste Verbesserung des Projekts nutzt den Befehl `nix flake check`. Er prüft, ob die Flake-Datei bestimmten Regeln folgt, und kann außerdem benutzerdefinierte Checks ausführen – zum Beispiel, ob sich noch alle Pakete bauen lassen.

Um den Befehl zu nutzen, fügen Sie die bisherigen Pakete einfach zu einem neuen `checks` Attribut hinzu, das Sie unterhalb der `packages` definieren:

```
checks = {
  inherit (config.packages)
    hello-cpp
    hello-rust
    ;
};
```

c't kompakt

- Um den Paketmanager Nix existiert ein ausgedehntes Ökosystem mit passenden Werkzeugen und Bausteinen für Entwicklungsaufgaben.
- Neben allerlei Komfortfunktionen sorgt Nix so vor allem für Konsistenz im Projekt und seinen Abhängigkeiten über alle beteiligten Entwickler hinweg.
- Auch angebundene CI-Systeme testen und bauen Software exakt so wie jeder Entwickler, was unangenehme Überraschungen verhindert.

Die verwendete `inherit`-Syntax von Nix bedeutet: Aus der gegebenen Attribut-Menge (`config.packages`) werden die danach genannten Attribute übernommen. Das macht es einfach, einerseits Pakete in die Checks aufzunehmen, ohne ihre Definition zu duplizieren, und andererseits später noch zusätzliche Checks zu definieren. `config` ist eine von Flake-Parts bereitgestellte Selbstreferenz, über die man leicht andere Teile der `perSystem`-Konfiguration adressieren kann.

Einstweilen bewirkt diese Erweiterung lediglich, dass nun auch der Befehl `nix flake check` die Pakete hello-cpp und hello-rust baut (und eventuelle Probleme dabei meldet). Zusätzliche Checks werden im weiteren Verlauf dieses Artikels noch hinzugefügt.

Shell-Vereinfachung

Weiter geht es mit der Definition der Development-Shell (die Sie per `nix develop` betreten). Sie ist etwas redundant zu den Definitionen der C++- und Rust-Pakete, weil sie deren Abhängigkeiten nochmals separat auflistet. Das verbessern Sie leicht:

```
devShells.default = pkgs.mkShell {
  inputsFrom = ↵
  ↳ builtins.attrValues config.checks;
};
```

Über das Attribut `inputsFrom` nimmt `mkShell` eine Liste von Nix-Derivations (siehe [1]) entgegen. Aus jeder extrahiert Nix die Abhängigkeiten und verwendet sie als Abhängigkeiten der Shell. Die eingebaute Funktion `builtins.attrValues` gibt eine Liste aller Werte in einer Attributmenge zurück, in diesem Fall also alle `checks`.

Nun sind alle Abhängigkeiten der beiden Pakete nur noch beim jeweiligen Paket definiert und müssen nicht an mehreren Stellen in der Flake gepflegt werden.

GitHub CI

Über den `check`-Befehl lassen sich Nix-Flakes auch elegant in Continuous-Integration-Systeme (CI) integrieren, wie etwa die Werkzeuge von GitHub. Ein Beispiel dafür finden Sie im Listing auf Seite 147. Es beschreibt einen sogenannten Workflow aus GitHub-Actions (siehe ct.de/ycxk), den das System bei jedem Push und Pull-Request startet.

Der CI-Job läuft auf GitHubs „Runnern“, die mit Ubuntu und macOS laufen. Dort installiert der Workflow zunächst Nix

(über den Determinate-Systems-Installer) und führt eine Caching-Action aus. Die befüllt den Nix-Store bei jeder Ausführung aus dem GitHub-Runner-Cache der letzten CI-Ausführung. Dieser Cache wird nach dem CI-Job aktualisiert, was zu einer erheblichen Beschleunigung konsekutiver CI-Jobs führt.

Der eigentliche CI-Job besteht lediglich aus dem Aufruf `nix flake check`. Es ist nun unerheblich, welche Pakete und Checks Sie noch zur Flake hinzufügen: Die CI zieht automatisch mit. Und wenn mal ein Job aufgrund eines Fehlers nicht funktioniert, so kann jeder Entwickler das Problem auf seinem Laptop mit `nix flake check` spielend leicht nachvollziehen. Entwickler müssen so nie wieder patchen, committen, pushen und dann warten, ob das CI-System die Änderung akzeptiert: Sie haben lokal genau die gleiche Umgebung, Abhängigkeiten und Checks zur Verfügung, die auch das CI-System nutzt.

Pre-Commit-Check

Bislang bestehen die Checks des Artikelprojekts lediglich darin, die Projektpakete zu bauen, aber in der Regel ist es sinnvoll, weitere Checks zu definieren. Indem man etwa Integrationstests von Nix ausführen lässt (die es in diesem Beispielprojekt allerdings nicht gibt) oder indem man ein Tool wie pre-commit einspannt (Links zu allen Tools unter ct.de/ycxk). Entwickler nutzen pre-commit beispielsweise gerne, um bei jedem Commit automatisch eine Code-Analyse und -Formatierung durchzuführen.

Auch bei solchen Werkzeugen ist es problematisch, wenn verschiedene Entwickler unterschiedliche Konfigurationen nutzen und etwa nicht exakt die gleichen Versionen aller von pre-commit verwendeten Tools auf allen Entwickler-Umgebungen laufen. pre-commit kann zwar fehlende Tools installieren, aber was, wenn nicht mal der gleiche Paketmanager für alle Tools auf allen Systemen zur Verfügung steht? Hinzu kommt, dass man auch dem CI-System beibringen muss, das Tool auszuführen.

Ohne das Rad neu zu erfinden, löst das Projekt pre-commit-hooks.nix diese Herausforderungen sehr elegant: In die Checks der Flake integriert, generiert es eine Konfigurationsdatei für pre-commit, die Tools aus den nixpkgs-Quellen verwendet. Weil Abhängigkeiten der Checks von der `nix develop`-Umgebung übernommen werden, steht so pre-commit perfekt reproduzierbar auf jedem Entwickler-Laptop und im CI-System bereit.

Anfängliche Flake

```
{
  description = "Heise Nix Example Project";

  outputs = { self, nixpkgs }:
    let
      system = "x86_64-linux";
      pkgs = nixpkgs.legacyPackages.${system};
    in {
      devShells.${system}.default = pkgs.mkShell {
        buildInputs = with pkgs; [
          boost
          cmake
          cargo
          rustc
        ];
      };
      packages.${system} = {
        hello-cpp = pkgs.stdenv.mkDerivation {
          name = "hello-cpp";
          src = ./cpp;
          nativeBuildInputs = [ pkgs.cmake ];
          buildInputs = [ pkgs.boost ];
        };
        hello-rust = pkgs.rustPlatform.buildRustPackage {
          name = "hello-rust";
          src = ./rust;
          cargoLock.lockFile = ./rust/Cargo.lock;
        };
      };
    };
}
```

Der Einbau geschieht in drei Schritten: Als Erstes müssen Sie das `inputs`-Attribut um die Flake des Projekts pre-commit-hooks.nix erweitern, damit das Tool zur Verfügung steht:

```
inputs = {
  # ... bisherige Inputs ...
  pre-commit-hooks.url = "github:↵
        ↳cachix/pre-commit-hooks.nix";
};
```

Nun können Sie einen neuen Check hinzufügen, der das Tool nutzt:

```
checks = {
  # inherit ...
  pre-commit-check = inputs.pre-↵
     ↳commit-hooks.lib.${system}.run {
    src = ./.;
    hooks = {
      # Rust
      clippy.enable = true;
      rustfmt.enable = true;

      # Nix
      deadnix.enable = true;
      statix.enable = true;

      # Shell
      shellcheck.enable = true;
      shfmt.enable = true;
    };
    settings.rust.cargoManifestPath ↵
              ↳ = "./rust/Cargo.toml";
  };
};
```

Mit dem Attribut `hooks` schalten Sie verschiedene Check-Tools von pre-commit einfach an, was zu ihrer automatischen Installation und Konfiguration führt. Lediglich den Rust-Tools muss erklärt werden, in welchem Ordner die Cargo-Dateien liegen. Das erledigt die `settings`-Zeile am Ende. Eine Liste der verfügbaren Tools

und weitere Anleitungen finden Sie in der README.md des Projekts git-pre-commit-hooks.nix.

Alle diese pre-commit-Checks führt Nix nun bei jedem `nix flake check` aus – automatisch auch auf dem CI-System! Der dritte Schritt fehlt allerdings noch, schließlich sollen die Checks ja ebenfalls laufen, wenn Entwickler committen. Dazu erweitern Sie das `devShells.default`-Attribut der Entwicklungsumgebung folgendermaßen:

```
devShells.default = pkgs.mkShell {
  inputsFrom = builtins.attrValues ↴
                  ↳ config.checks;
  inherit (config.checks.↴
       ↳pre-commit-check) shellHook;
};
```

Der von pre-commit-hooks.nix erzeugte Flake-Check enthält nämlich auch das Attribut `shellHook`, welches direkt in die Developer-Shell übernommen werden kann.

Beim Betreten der `nix develop`-Umgebung erzeugt Nix von nun an eine Datei namens .pre-commit-config.yaml, die pre-commit so konfiguriert, dass auch jeder Commit die Checks anstößt. Die Datei sollten Sie der `.gitignore`-Liste hinzufügen, da Nix sie bei jedem Betreten der Developer-Shell neu generiert.

Ob alles richtig funktioniert, prüfen Sie zum Beispiel, indem Sie die Entwicklungsumgebung betreten und die Datei rust/src/main.rs „verschlimmbessern“:

```
fn main() {
println!("Hello, world!");
}
```

Beim Commit moniert der rustfmt-Check die nicht mehr vorhandene Einrückung des Funktionskörpers:

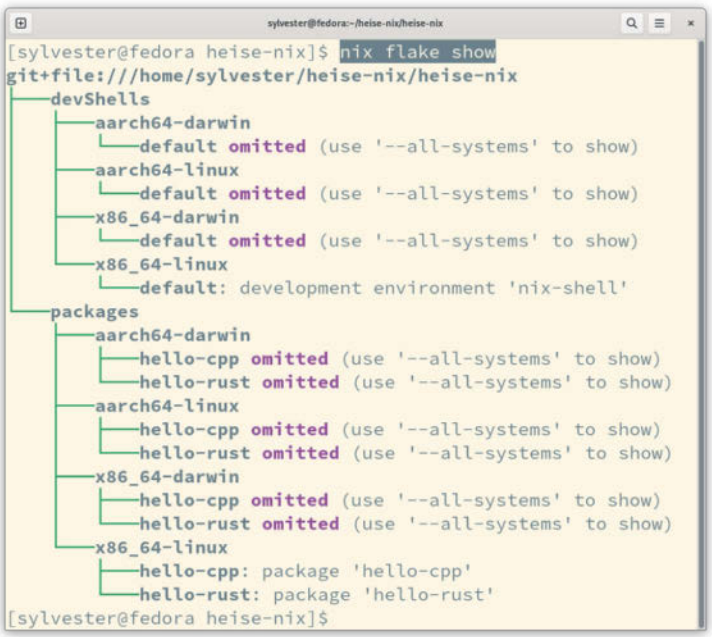
```
[...]
rustfmt.....................Failed
- hook id: rustfmt
- files were modified by this hook
[...]
```

Rustfmt bemängelt die schlechte Formatierung nicht nur, sondern korrigiert sie auch gleich. Das Ergebnis muss nur noch vom Entwickler inspiziert, akzeptiert und zum git-Index hinzugefügt werden, beispielsweise per `git add -p`:

```
diff --git a/rust/src/main.rs b/rust/↴
                              ↳src/main.rs
index f5c339a..e7a11a9 100644
--- a/rust/src/main.rs
+++ b/rust/src/main.rs
@@ -1,3 +1,3 @@
 fn main() {
-println!("Hello, world!");
+    println!("Hello, world!");
 }
(1/1) Stage this hunk [y,n,q,a,d,e,?]?
```

Rust Crane

Bisher erzeugt die Funktion `pkgs.rustPlatform.buildRustPackage` das Paket `hello-rust`. Sie stammt direkt aus den `nixpkgs`. Nix bringt solche Helferfunktionen für aktuell 39 Sprachen und Frameworks mit (siehe ct.de/ycxk), unter anderem auch für Java, JavaScript und Python.



Dank der Flake-Parts-Bibliothek hat man im Nu eine Flake, die Pakete für allerlei Systemarchitekturen anbietet.

Diverse Organisationen haben allerdings ihre eigenen Nix-Bibliotheken entwickelt und als Open Source veröffentlicht, die oft noch mehr können.

Als Beispiel wirft dieser Artikel einen Blick auf die Bibliothek Crane, die eine Vielzahl von Funktionen und Vorteilen gegenüber dem in `nixpkgs` eingebauten Rust-Support bietet. Besonders fällt die Geschwindigkeitsverbesserung von Builds mit Crane auf: Cargo muss nun nicht mehr alle Rust-Abhängigkeiten selbst bauen, denn sie werden im Nix-Store gecacht. Dieser Vorteil erstreckt sich auch auf Nutzer der `nix develop`-Umgebung, sofern CI und Entwickler den gleichen Nix-Binary-Cache verwenden – das sind allerdings Tricks für einen Folgeartikel.

Crane liefert auch die Helferlein rustfmt und clippy mit, allerdings deckt unser Beispielprojekt diese bereits über pre-commit ab. Als Beispiele dienen deshalb der Einbau von Sicherheitschecks über den gesamten Abhängigkeitsbaum aller Rust-Bibliotheken sowie die Generierung von Rust-Dokumentation.

Zunächst müssen Sie mal wieder neue Inputs oben in der Flake-Datei hinzufügen:

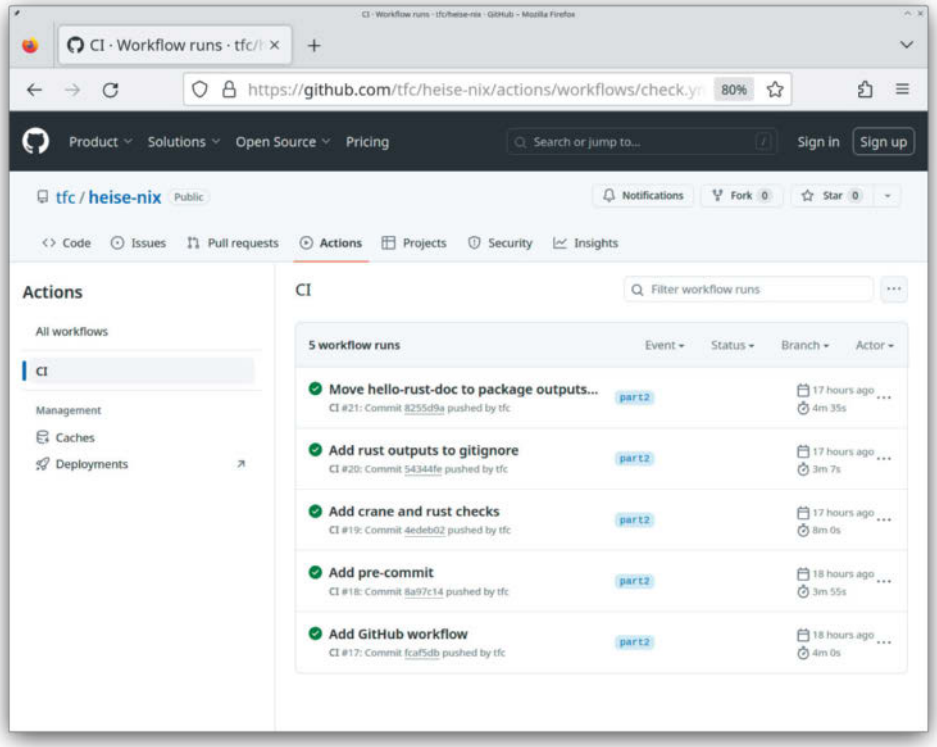
```
inputs = {
  # ... bisherige Inputs ...
  advisory-db.url = "github:rustsec/↵
                     ↳advisory-db";
  advisory-db.flake = false;
  crane.url = "github:ipetkov/crane";
  crane.inputs.nixpkgs.follows = ↵
                                 ↳ "nixpkgs";
};
```

Die `advisory-db`-Zeilen brauchen Sie für die Security-Checks später. Bei den Zeilen darunter fällt auf, dass Crane mit einer eigenen `nixpkgs`-Referenz in seinen Inputs gebaut wird. Es ist aber ohne Weiteres möglich, die Referenz mit `nixpkgs` aus der aktuellen Flake zu überschreiben. Das geschieht in der letzten Zeile. Details erklärt die Flake-Dokumentation (siehe ct.de/ycxk).

Nun können Sie das `hello-rust`-Paket an sich umbauen. Legen Sie dafür zunächst mit einer `let ... in`-Klausel (wie man sie auch von anderen funktionalen Sprachen kennt) ein paar Helfer-Variablen an:

```
perSystem = {
  config, pkgs, system, ...
}: let
  craneLib = inputs.crane.lib.↵
                            ↳${system};
  src = craneLib.cleanCargoSource ↵
            ↳ (craneLib.path ./rust);
  cargoArtifacts = craneLib.↵
      ↳buildDepsOnly { inherit src; };
in {
  devShells.default = #...
# ...
```

Zuerst wird die Variable `craneLib` als Abkürzung zur Crane-Bibliothek definiert. (Die Variable `system` befüllt das `perSystem`-Konstrukt der Flake-Parts-Bibliothek.) Die Variable `src` verweist auf den Quelltext des Rust-Pakets, nachdem er mit den Funktionen `path` und `cleanCargoSource` aus der `craneLib` von allem bereinigt wurde, was



Die Integration von Nix-Flakes mit CI-Systemen wie hier GitHub-Workflows ist einfach und vor allem wartungsarm.

für das Bauen von Rust-Paketen unwesentlich ist. Zuletzt erzeugt die Funktion `buildDepsOnly` eine Nix-Derivation, die alle in Cargo.toml erwähnten Pakete baut – also alle Abhängigkeiten des Rust-Pakets, aber nicht das Paket selbst. Es ist oft hilfreich, (Rust-)Abhängigkeiten getrennt zu cachen und referenzieren zu können.

Mit diesen Vorarbeiten fällt der eigentliche Umbau des `hello-rust`-Pakets leicht. Crane bringt genau dafür die Funktion `buildPackage` mit:

```
hello-rust = craneLib.buildPackage {
  inherit cargoArtifacts src;
};
```

Das Ergebnis funktioniert automatisch sowohl lokal (per `nix build .#hello-rust`) als auch im CI-System, das den Aufruf `nix flake check` nutzt. Wie in [1] beschrieben sollten Sie immer auch Änderungen an der Datei flake.lock committen, damit das CI-System auf dem gleichen Stand ist. Sonst kann es zu Problemen und Inkonsistenzen kommen.

Zuletzt können Sie noch Checks einfügen, die per `cargo doc` Dokumentation erstellen und per `cargo audit` nach Rust-Abhängigkeiten mit bekannten Sicherheitslücken suchen. Auch dafür enthält Crane Funktionen, die passende Nix-Derivations generieren:

```
packages = {
  # ... bisherige Packages ...
  hello-rust-doc = craneLib.cargoDoc {
    inherit cargoArtifacts src;
  };
};
checks = {
  inherit (config.packages)
    hello-cpp
    hello-rust
    hello-rust-doc
    ;

  hello-rust-audit = craneLib.↵
                        ↳cargoAudit {
    inherit (inputs) advisory-db;
    inherit src;
  };

  # pre-commit-check = ...
};
```

In den Aufrufen der Funktionen `cargoDoc` und `cargoAudit` sieht man schön, wie sie den Quellcode in `src` sowie die `cargoArtifacts`, die sämtliche Abhängigkeiten enthalten, wiederverwenden. Außerdem fällt auf, dass das Audit direkt als Check definiert wird, der Dokumentationsbau hingegen als Paket, das die Checks referenzieren. So können Sie die Dokumentation bequem mit `nix build .#hello-rust-doc` erstellen, Sie finden das Ergebnis im Order result. Denn der Check prüft zwar, ob die Dokumentation gebaut werden kann, speichert sie aber nicht: Checks haben keine Ausgabe, sie können nur funktionieren oder einen Fehler melden.

Alle Checks laufen nun automatisch bei jedem CI-Run und auch, wenn der Entwickler lokal `nix flake check` ausführt. Für nichts davon müssen Nutzer oder Admins der CI-Maschinen/VMs/Container Bescheid wissen oder Software bereitstellen.

Weil die Paketlisten des Security-Checks (`advisory-db`) als Flake-Input definiert wurden, aktualisiert Nix sie automatisch mit jedem `nix flake update`.

Fazit und Ausblick

Dieser Artikel hat die Flake des Beispielprojekts weiterentwickelt. Aus einer Minimalversion, die lediglich zwei Pakete bauen konnte und eine Entwicklungsshell bot, wurde eine architekturunabhängige Flake, die pre-commit-Aktionen automatisiert, Dokumentation erzeugt und nach Sicherheitslücken in Abhängigkeiten sucht. Außerdem wurde die Flake exemplarisch so in die GitHub-CI integriert, dass man die CI-Beschreibung nicht anpassen muss, wenn sich das Projekt weiterentwickelt, und leicht lokal nachvollziehen kann, wo es klemmt, wenn das CI-System Fehler meldet. Der Einfachheit halber geschah das mit einem schlichten Aufruf von `nix flake check`, aber es gibt auch deutlich mächtigere und Nix-spezifischere Lösungen: Das Nixpkgs-Projekt selbst hat die Hydra CI hervorgebracht; daneben gibt es – teilweise kostenlose – Dienste wie Hercules CI oder NixCI (alle Links via ct.de/ycxk), die Flakes ohne weitere Vorbereitung des Projekts inspizieren, pro Output einen Job erstellen und in der optimalen Reihenfolge bauen.

Die fertige Flake finden Sie im GitHub-Repo des Autors via heise.de/s/4YGL. In einer der nächsten Ausgaben erklären wir, wie Sie einen binären Cache für Ihre Open-Source-Projekte einrichten, um Builds und Shells noch schneller an Benutzer und Kollegen zu liefern. Und wie Sie Cross-Builds der C++- und Rust-Beispielapps realisieren, damit Sie diese auch für Windows-User und beispielsweise Raspberry-Pis anbieten können.

(syt@ct.de) c't

GitHub-Workflow

```
name: CI


on:
  push:
  pull_request:

jobs:
  check:
    runs-on: ${{ matrix.os }}
    strategy:
        matrix:
            os: [ubuntu-latest, macos-latest]
    steps:
      - uses: actions/checkout@v3
      - uses: DeterminateSystems/nix-installer-action@main
      - uses: DeterminateSystems/magic-nix-cache-action@main
      - run: nix flake check
```

Literatur

[1] Jacek Galowicz, Paketiermaschine, Softwarepakete mit Nix managen und bauen, c't 23/2023, S. 150

Tools und Dokumentationen: ct.de/ycxk

Bild: Thorsten Hübner

Cloudtresor zum Generieren von Einmalpasswörtern

2FA-Authentifikator selbst gemacht

Onlinekonten zusätzlich zum Passwort mit einem zweiten Faktor abzusichern, ist immer eine gute Idee. Leider geht das oft zulasten des Komforts. Das Open-Source-Projekt 2FAuth verschiebt den Authenticator ins Netz. Mit unserer Anleitung hosten Sie die App in Eigenregie und bauen sich ein zweites 2FA-Standbein auf.

Von Markus Stubbig

Man kennt es: Nach der Eingabe des Passworts fragt die Website nach dem zweiten Faktor in Form eines sechsstelligen Zahlencodes, den man aus einer Authentifikator-App fischen muss. Onlinekonten zusätzlich zum Passwort mit dem TOTP-Verfahren (Time-based one-time password) zu schützen, ist deutlich sicherer als ein Passwort allein, benötigt keine weitere Hardware und wird bereits von vielen Webdiensten angeboten. Eigentlich eine super Sache, aber wo ist das blöde Smartphone schon wieder? Warum sollte man überhaupt ein anderes Gerät herauskramen, wenn ich mich doch am Desktop-PC anmelden will? Und wehe demjenigen, dessen Smartphone abraucht ohne eine 2FA-Backup-Strategie zu haben.

Das Open-Source-Projekt 2FAuth soll diese Probleme lösen. Der Clou: Sie hosten die Software für den TOTP-Authenticator einfach selbst und greifen bequem mit dem Browser auf Ihre Einmalpasswörter zu, egal von welchem Gerät. Die selbst gehostete Option eignet sich für diejenigen, die sich bei 2FA nicht allein auf ihr Smartphone verlassen wollen und ihre Codes nicht in die Hände von Großkonzernen wie Google legen wollen. Dessen Authenticator war beispielsweise zuletzt negativ aufgefallen, weil er die Geheimnisse, also die Zeichenfolge, aus denen ein Algorithmus das Ein-

malpasswort errechnet, beim Sync unverschlüsselt übertragen hatte.

Das Projekt ist außerdem interessant für Unternehmen, die eine 2FA-Strategie entwickeln wollen, aber nicht alle Mitarbeiter mit einem extra Smartphone oder Hardwaresicherheitsschlüsseln ausstatten können oder wollen.

Blaupause

2FAuth ist eine klassische Webanwendung unter Linux, die mit dem PHP-Webframework Laravel entwickelt wurde und einen Webserver sowie eine SQLite-Datenbank braucht. Am einfachsten installieren Sie die App mit Docker. Damit Sie bequem an Ihre Einmalkennwörter gelangen, lohnt es sich, 2FAuth auf einen Server zu packen, der über das Internet erreichbar ist. Sie können die Software prinzipiell auf einem Raspberry Pi in Ihrem Heimnetz laufen lassen, müssen dann aber entweder eine Portweiterleitung am Router eintragen [1] oder mit einem VPN darauf zugreifen. Wir beschreiben das Einrichten auf einem angemieteten vServer mit öffentlicher IPv4-Adresse.

Für 2FAuth reicht die kleinste vServer-Konfiguration, die Sie bei Ihrem Hostingprovider finden, beispielsweise eine Konfiguration mit 1 vCPU und 2 GByte RAM. Als Betriebssystem nutzen wir Ubuntu 22.04 LTS. Wir raten dazu, sich stets via SSH-Schlüssel auf dem Server anzumelden und die Authentifizierung mittels Passwort zu deaktivieren [2]. Unsere Anleitung setzt Linux- und Docker-Grundwissen voraus.

Um die Weboberfläche von 2FAuth TLS-verschlüsselt auszuliefern, nutzen wir den simplen Reverse-Proxy Caddy, der ein Zertifikat von Let's Encrypt oder ZeroSSL besorgt und automatisch verlängert. Sie brauchen dafür eine Domain, für die Sie einen A-Record anlegen können, der auf die IP-Adresse Ihres Servers verweist, beispielsweise 2fauth.example.com. Wenn Sie 2FAuth in Ihrem Heimnetzwerk betreiben und keine feste, öffentliche IPv4-Adresse haben, können Sie sich mit einem DynDNS-Dienst behelfen.

Vorbereitung

Loggen Sie sich mit SSH auf Ihrem Server ein und bringen Sie das System auf den neuesten Stand:

```
apt update
apt upgrade
```

Um die aktuelle Version von Docker und Docker Compose zu bekommen, installieren Sie einige Pakete und fügen den GPG-Schlüssel von Docker hinzu:

```
apt-get install ca-certificates \
curl gnupg

install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.\
docker.com/linux/ubuntu/gpg | sudo \
gpg --dearmor \
-o /etc/apt/keyrings/docker.gpg

chmod a+r /etc/apt/keyrings/docker.gpg
```

Dann kommen die Docker-Paketquellen dran:

```
echo "deb [arch="$(dpkg --print-\
architecture)" \
signed-by=/etc/apt/keyrings/docker\
.gpg] https://download.docker.\
com/linux/ubuntu "$(. /etc/os-\
release && echo \
"$VERSION_CODENAME")\
stable" | tee /etc/apt/sources\
.list.d/docker.list > /dev/null

apt update
```

Installieren Sie Docker:

```
apt install docker-ce docker-ce-cli \
containerd.io docker-buildx-plugin \
docker-compose-plugin
```

Falls es auf dem System noch keinen weiteren Benutzer außer root gibt, legen Sie jetzt einen an, vergeben ein sicheres Passwort und fügen Sie ihn zur Gruppe sudo und docker hinzu:

```
adduser cttest
usermod -aG sudo cttest
usermod -aG docker cttest
```

c't kompakt

- 2FAuth funktioniert wie Authenticator-Apps, die auf dem Smartphone Einmalpasswörter generieren, ist aber eine Web-App, die Sie selbst hosten können.
- Sie hat nicht nur eine intuitive Weboberfläche, sondern punktet auch mit einem umfangreichen API. Profis besorgen sich ihre 2FA-Codes über die Kommandozeile.
- Sie müssen Ihre klassische Authenticator-App nicht einmotten. Bei Verlust oder Defekt des Smartphones dient 2FAuth als Rettungsanker.

Ersetzen Sie den Platzhalter „cttest" durch einen Benutzernamen Ihrer Wahl. Loggen Sie sich danach mit dem neuen Benutzer ein.

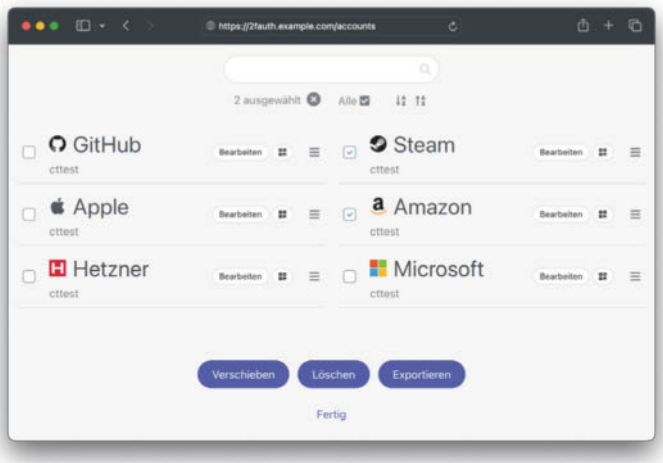
```
su - ihr_benutzername
```

Installation

Um die Installation von 2FAuth und Caddy mit Docker zu erleichtern, stellen wir ein öffentliches GitHub-Repository zur Verfügung, das eine Docker-Compose-Vorlage enthält. Klonen Sie zunächst das Repository und navigieren in das neue Verzeichnis:

```
git clone \
https://github.com/ndi-ct/2fauth-caddy

cd ~/2fauth-caddy
```



2FAuth funktioniert wie eine Authentifikator-App auf dem Smartphone, ist aber eine Webanwendung, die Sie in Eigenregie betreiben können.

```
services:
   caddy:
     image: caddy:latest
     ports:
       - 80:80
       - 443:443
     volumes:
       - ./Caddyfile:/etc/caddy/↵
                        ↳Caddyfile
       - ./caddy-data/certs:/data
     restart: always

   2fauth:
    image: 2fauth/2fauth
    container_name: 2fauth
    volumes:
      - ./2fauth:/2fauth
    ports:
      - 8000/tcp
    environment:
      - APP_NAME=2FAuth
      - APP_ENV=local
      - APP_DEBUG=false
      - SITE_OWNER=cttest↵
                       ↳@example.com
      - APP_KEY=↵
            ↳StringOf32CharsExactly
      - APP_URL=↵
        ↳https://2fauth.example.com
      - CACHE_DRIVER=file
      - SESSION_DRIVER=file
      - MAIL_DRIVER=log
      - MAIL_HOST=smtp.example.com
      - MAIL_PORT=2525
      - MAIL_cttest↵
                       ↳@example.com
      - MAIL_USERNAME=cttest
      - MAIL_PASSWORD=cttest
      - MAIL_ENCRYPTION=SSL
      - MAIL_FROM_NAME=cttest
      - MAIL_FROM_ADDRESS=cttest@↵
                        ↳example.com
      - WEBAUTHN_NAME=2FAuth
      - WEBAUTHN_ID=null
      - WEBAUTHN_ICON=null
      - WEBAUTHN_USER_↵
            ↳VERIFICATION=preferred
      - TRUSTED_PROXIES=*
      - SESSION_LIFETIME=120
```

Den oben gezeigten Ausschnitt aus der Datei docker-compose.yaml müssen Sie nicht abtippen. Laden Sie die Datei einfach von ct.de/yx51 herunter.

In dem Ordner finden Sie die Datei docker-compose.yaml, die als Bauplan für den Containerverbund aus 2FAuth und Caddy dient.

Öffnen Sie die Datei mit einem Texteditor Ihrer Wahl, um einige Umgebungsvariablen anzupassen. Tragen Sie beim Schlüssel `SITE_OWNER=` Ihre E-Mail-Adresse ein. Beim Punkt `APP_KEY=` fügen Sie einen String mit exakt 32 Zeichen ein. Den können Sie sich mit einem Passwortmanager generieren oder auf der Kommandozeile mit folgendem Befehl erzeugen:

```
cat /dev/urandom\| tr -dc \
'a-z0-9' | head -c 32
```

Bei `APP_URL=` tragen Sie die URL ein, unter der 2FAuth erreichbar sein soll. Die Umgebungsvariablen `MAIL_HOST=` bis `MAIL_FROM_ADDRESS=` passen Sie an, wenn 2FAuth E-Mails versenden soll, beispielsweise um ein vergessenes Passwort zurückzusetzen. Das ist sinnvoll, wenn Sie 2FAuth nicht allein nutzen, sondern auch Freunde, die Familie oder wenn Sie es als Admin im Unternehmen betreiben. Tragen Sie dann die Daten Ihres Mailservers oder von Ihrem SMTP-Provider ein.

Öffnen Sie danach die Datei namens Caddyfile im gleichen Ordner. Das ist eine Konfigurationsdatei für den Reverse-Proxy Caddy, der eingehende Anfragen an den 2FAuth-Container durchreicht und die Weboberfläche der Anwendung via HTTPS ausliefert. Caddy besorgt dafür ein kostenloses Zertifikat von Let's Encrypt oder ZeroSSL und verlängert es automatisch, bevor es abläuft. Im Caddyfile müssen Sie den Platzhalter 2fauth.example.com lediglich durch Ihre eigene Domain ersetzen, die auf die IP-Adresse Ihres Servers verweist:

```
https://2fauth.example.com {
       reverse_↵
↳proxy 2fauth:8000
}
```

Mit der sogenannten HTTP-Challenge beweist Caddy einer Zertifizierungsstelle (CA) wie Let's Encrypt, dass der Server unter Ihrer Kontrolle steht. Dafür muss der TCP-Port 80 erreichbar sein. Für HTTPS braucht es außerdem TCP-Port 443. Stellen Sie sicher, dass keiner davon durch eine Firewall blockiert wird. Wenn Sie 2FAuth in Ihrem Heimnetzwerk betreiben und es nicht von außerhalb erreichbar sein soll, können Sie auch ein selbst signiertes Zertifikat von Caddy nutzen. Die Dokumentation dazu haben wir unter ct.de/yx51 verlinkt. Ohne HTTPS können und sollten Sie 2FAuth nicht betreiben. Die App weigert sich dann, neue QR-Codes zu scannen.

Geheimnis-Fütterung

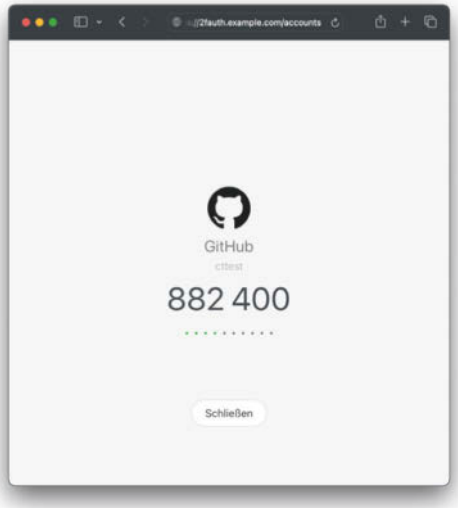
Jetzt ist alles bereit, um den Containerverbund zu starten. Tippen Sie dazu folgenden Befehl ein:

```
docker compose up -d
```

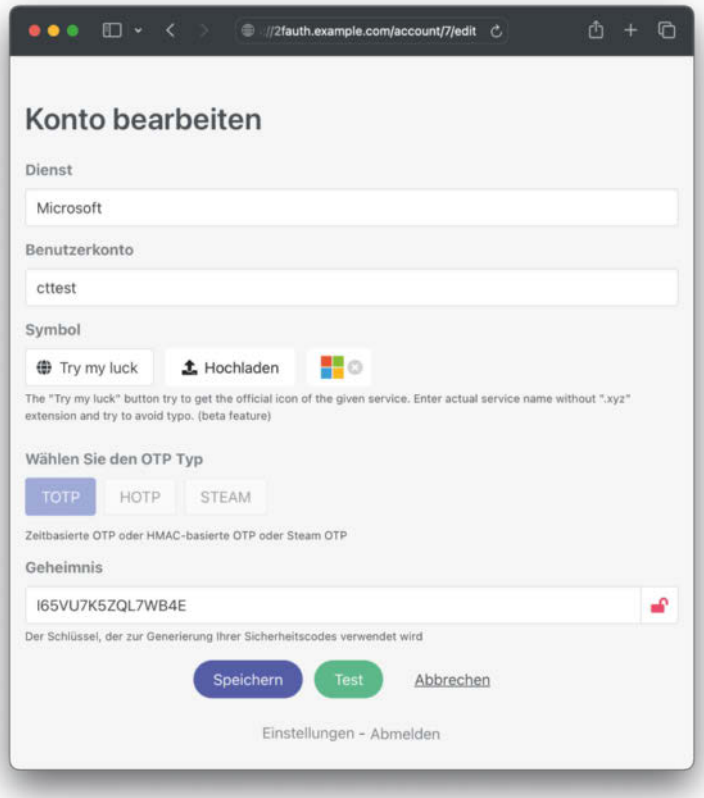
Nach wenigen Minuten sollte 2FAuth startklar sein. Öffnen Sie Ihren Browser und rufen Sie die URL https://2fauth.example.com/register auf. Wenn das nicht klappt, helfen die Befehle `docker logs caddy` und `docker logs 2fauth` bei der Fehlersuche.

Den ersten Benutzer, den Sie registrieren, macht 2FAuth automatisch zum Administrator. Vergeben Sie ein sicheres Passwort und merken Sie sich das gut. Wenn Sie 2FAuth alleine nutzen, dann sollten Sie in der Weboberfläche zunächst das Menü für die Einstellungen öffnen und einen Haken bei „Disable Registration" setzen, um Unbefugten die Tür vor der Nase zuzuschlagen, wenn sie auf Ihrer 2FAuth-Instanz ein Konto eröffnen wollen. In diesem Menü bestimmen Sie auch die Sprache; 2FAuth orientiert sich an den Spracheinstellungen für den Browser. Anschließend kehren Sie zum Hauptmenü zurück.

Bis jetzt ist die Liste der 2FA-Konten leer. Das ändern Sie mit einem Klick auf die Schaltfläche „Neu". 2FAuth bietet sogleich an, einen QR-Code mittels Kamera



2FAuth generiert zeitlich begrenzt nutzbare Einmalpasswörter mit den TOTP- und HOTP-Algorithmen und erzeugt Codes für den Login bei der Gamingplattform Steam.



Für das TOTP-Verfahren braucht es ein Geheimnis, das der Authentifikator und der Webdienst kennen. Um das Geheimnis in den Authentifikator zu bekommen, scannt man üblicherweise einen QR-Code. Wenn das mangels Kamera nicht geht, kann man auch eine Zahlenfolge eingeben.

zu scannen, verhält sich also genau so, wie Sie es beispielsweise vom Google Authenticator auf dem Smartphone kennen. Das klappt etwas besser mit einem Smartphone, das bei 2FAuth eingeloggt ist, ist aber auch mit einer Webcam möglich. Egal wie, Sie müssen Ihrem Browser die Erlaubnis für den Kamerazugriff erteilen.

Aber was tun, wenn Ihr Gerät über keine Kamera verfügt? Für diesen Fall gibt es die Option „Erweitertes Formular verwenden“. Damit können Sie beispielsweise QR-Codes als Bilder hochladen. Letztlich ist der QR-Code nur ein Vehikel, um einem Authentifikator, hier 2FAuth, ein Geheimnis einzuflößen.

Wenn Sie bei einem Webdienst die Zwei-Faktor-Authentifizierung mittels Einmalpasswörtern aktivieren, können Sie sich zumeist das Geheimnis anzeigen lassen. Diese Zeichenfolge, beispielsweise I65PT7K5ZDL7WB4E, können Sie auch selbst in 2FAuth eintippen. Dann müssen Sie aber bestimmen, mit welchem Algorithmus 2FAuth aus dem Geheimnis Einmalkennwörter generieren soll. In der Regel handelt es sich um TOTP. HOTP (Schlüssel-Hash-Nachrichtenauthentifizierungscode) ist nicht mehr sehr verbreitet. Steam-OTP für den Gaminganbieter setzt nur der Steam Guard ein. Wie TOTP und Co. genau funktionieren, haben wir in [3] aufgeschrieben.

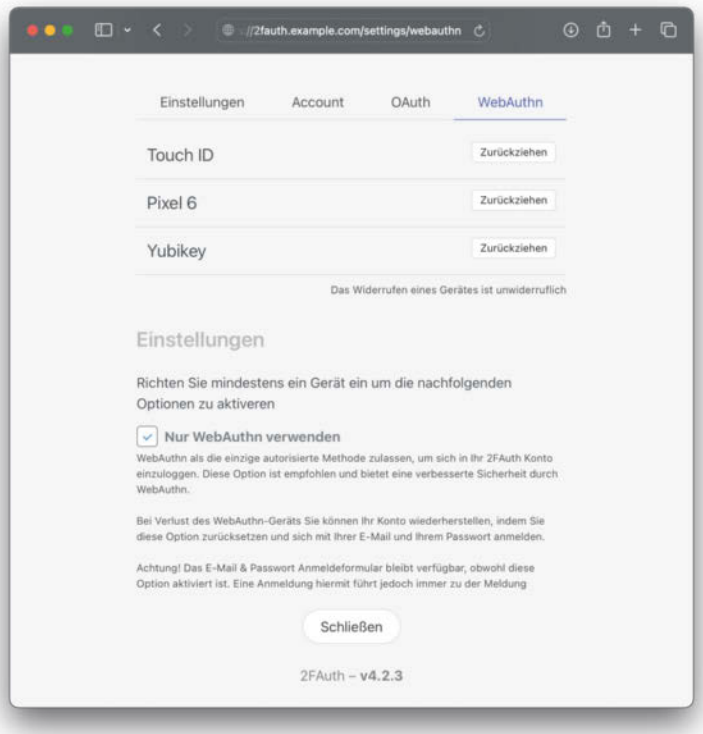
Vermutlich haben Sie jedoch bereits eine Reihe von Accounts durch eine Authentifikator-App auf Ihrem Smartphone abgesichert. Je nach App können Sie Ihre Geheimnisse auch exportieren. Wenn Sie diese Dateien mit der Import-Funktion von 2FAuth hochladen, importieren Sie auf einen Schlag Ihre gesamte Sammlung an Geheimnissen und haben direkt ein Backup angelegt für den Fall, dass Ihr Smartphone verloren oder kaputtgeht. 2FAuth selbst exportiert Geheimnisse als JSON.

2FA für den 2FA-Tresor

Schützen Sie Ihre 2FAuth-Instanz gut vor neugierigen Blicken! In den Einstellungen sollten Sie die Zeitdauer für die automatische Sperrung nach Inaktivität heruntersetzen, die Voreinstellung beträgt 15 Minuten. Wenn Sie die Option „Generierte Einmalpasswörter als Punkte anzeigen“ aktivieren, können Neugierige keinen Blick mehr auf Ihre Einmalpasswörter erhaschen. Sie selbst können die Passwörter aber trotzdem kopieren und in Login-Formulare einfügen.

2FAuth speichert Daten in einer SQLite-Datenbank, die sich im Verzeichnis ~/2fauth-caddy/2fauth befindet, wenn Sie diese Anleitung befolgt haben. Legen Sie regelmäßig ein Backup der Datenbankdatei an. Im Einstellmenü legen Sie unter „Administration“ fest, sensible Daten wie Geheimnisse und E-Mails nur verschlüsselt in der Datenbank zu speichern. Wenn Sie irgendwann ein Backup der Datenbank wiederherstellen wollen, brauchen Sie dazu den Schlüssel, den Sie bei der Umgebungsvariable `APP_KEY=` in der Docker-Compose-Datei gesetzt haben. Speichern Sie den Schlüssel an einem sicheren Ort – und nur dort.

Den 2FAuth-Webzugang sollten Sie besonders gut abdichten. Zum Glück beherrscht die Software die Anmeldung mit WebAuthn, sodass Sie sich auch passwort-



2FAuth hilft Nutzern, ihre Logins mit einem zweiten Faktor zu schützen, aber wer schützt 2FAuth? Am sichersten ist es, mehrere WebAuthn-Geräte oder Passkeys zu registrieren und den Login mit Nutzername und Passwort zu verbieten.

los mit einem FIDO2-Hardwaresicherheitsschlüssel oder mit einem Passkey einloggen können. Navigieren Sie dazu im Einstellmenü zum Reiter WebAuthn und fügen Sie solche Geräte hinzu. Die Entwickler von 2FAuth empfehlen, die Option „Nur WebAuthn verwenden“ zu aktivieren. Die Anmeldung funktioniert dann nur noch mit einem zuvor hinterlegten Gerät oder Passkey.

API für Power-User

Für die meisten Nutzer dürfte es reichen, sich fix bei 2FAuth einzuloggen, das Einmalkennwort abzuholen und sich damit beim gewünschten Webdienst anzumelden. 2FAuth enthält darüber hinaus aber auch ein umfangreiches REST-API, das den Funktionsumfang enorm erweitert. Damit können Sie beispielsweise mit Linux-Bordmitteln wie curl über die Kommandozeile auf die Datenbank zugreifen, Einmalkennwörter und QR-Codes abrufen oder neue Accounts und Geheimnisse hinzufügen.

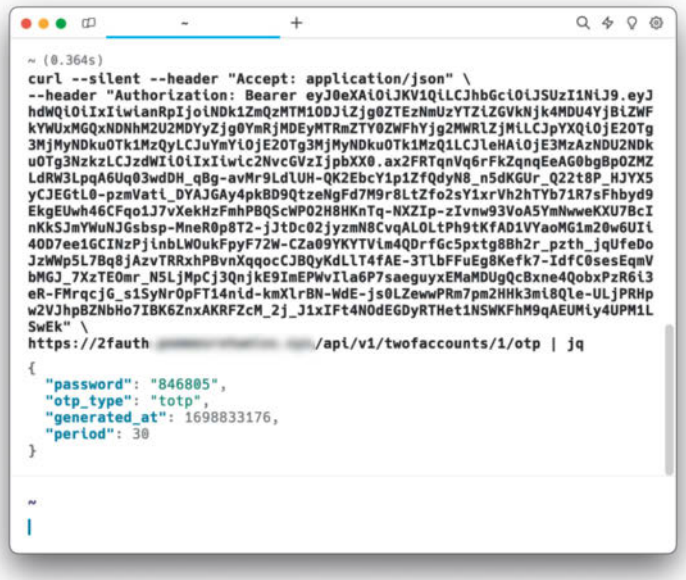
Dafür generieren Sie in der Weboberfläche von 2FAuth zunächst ein persönliches Zugriffsstoken (PAT). Obacht! Die App zeigt das Token nur einmal an. Die Zeichenfolge müssen Sie bei jeder Anfrage an das API als Bearer-Token im Autorisierungs-Header mit angeben.

Sämtliche Funktionen des API zu erklären, würde den Rahmen des Artikels sprengen, aber für eine kurze Demonstration reicht es, eine Liste von Accounts abzurufen, um deren IDs herauszufinden und im zweiten Schritt für einen davon ein Einmalpasswort zu generieren.

Mit dem folgenden Befehl schicken Sie eine autorisierte Anfrage an den Endpunkt `/api/v1/twofaccounts` und verlangen eine Liste Ihrer Accounts:

```
curl --silent --header \
"Accept: application/json" \
--header "Authorization: \
Bearer eyJ0eXAiOiJKV1QiLCJAJSUzI1Ni" \
https://2fauth.\
example.com/api/v1/twofaccounts | jq
```

Ersetzen Sie die Zeichenfolge hinter `Authorization: Bearer` durch Ihr persönliches Zugriffstoken. Es ist deutlich länger als der hier gezeigte Ausschnitt. Nach wenigen Sekunden antwortet Ihr 2FAuth-Server mit der Liste. In diesem Beispiel haben wir einen GitHub-Account mittels TOTP abgesichert.



Nutzer, die viel auf der Kommandozeile unterwegs sind, besorgen sich ihre Einmalpasswörter über das umfangreiche API.

```
[
{
"id": 1,
"group_id": null,
"otp_type": "totp",
"account": "cttest",
"service": "GitHub",
"icon": "cq4UWdVSYGLAQPt5hgkICfE.svg",
"digits": 6,
"algorithm": "sha1",
},
]
```

Wie man in der Antwort lesen kann, trägt der Dienst namens GitHub die ID 1. Über den Endpunkt `/api/v1/twofaccounts/{id}/otp` fragen Sie Einmalpasswörter ab. Sie ersetzen den Platzhalter `{id}` lediglich durch die ID des gewünschten Dienstes:

```
curl --silent --header \
"Accept: application/json" \
--header "Authorization: \
Bearer eyJ0eXAiOiJKV1QiLCJhJSUzI1Ni" \
https://2fauth.example.\
com/api/v1/twofaccounts/1/otp | jq
```

Voilà! Die Antwort mit dem Einmalkennwort kommt postwendend:

```
{
  "password": "805049",
  "otp_type": "totp",
  "generated_at": 1698726059,
  "period": 30
}
```

Welche Möglichkeiten das API von 2FAuth noch bietet, erklären die Entwickler unter ct.de/yx51. Für die ersten Gehversuche steht ein Demoserver unter demo.2fauth.app zur Verfügung.

Fazit

2FAuth ist eine Open-Source-Alternative für Nutzer, die proprietären Authentifikator-Apps für das Smartphone nicht über den Weg trauen. Dadurch, dass der Tresor mit den Einmalpasswörtern aus dem Netz zugänglich ist, ist man nicht auf die Sync-Funktion der Hersteller angewiesen, muss aber trotzdem nicht auf Komfort verzichten. Außerdem geht es am Notebook oder Desktop-PC oft schneller, sich bei 2FAuth einzuloggen und das Einmalpasswort zu kopieren, als das Smartphone herauszukramen, zu entsperren und die Codes abzutippen.

Achten Sie darauf, die Software auf Ihrem 2FAuth-Server aktuell zu halten und gewähren Sie den Zugang zur Weboberfläche, wenn möglich, nur via WebAuthn (FIDO2). Sollte Ihnen 2FAuth gefallen, motten Sie Ihren Smartphone-Authentifikator besser trotzdem nicht sofort ein, sondern nutzen Sie beide Tools im Verbund. Dann haben Sie auch bei Smartphoneverlust oder Internetflaute stets Ihren zweiten Faktor parat. *(ndi@ct.de)* **ct**

Literatur

[1] Peter Siering, Löchlein bohren, Dienste aus dem eigenen Netz ins Internet bringen, c’t 19/2021, S. 74
[2] Niklas Dierking, Schlüsselmeister, Sicher und komfortabel arbeiten mit SSH, c’t 21/2022, S. 172
[3] Niklas Dierking, Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Onlinezugänge, c’t 9/2022, S. 18

***Dokumentationen von Caddy und 2FAuth, Demo-Instanz:* ct.de/yx51**

Zurechtgepuzzelt

Erweiterungen für den Linux-Desktop Gnome auf Version 45 migrieren

Die Entwickler des Linux-Desktops Gnome haben mit Version 45 die eigene JavaScript-Engine GJS modernisiert. Bestehende Erweiterungen sind mit der neuen Schnittstelle nicht kompatibel und brauchen eine Anpassung. Wir erklären Ihnen die Hintergründe und zeigen, wie Sie selbst eine Extension fit für Gnome 45 machen.

Von Andy Holmes und Keywan Tonekaboni

Die Linux-Desktopumgebung Gnome präsentiert sich mit einer schlichten Bedienoberfläche. Fehlt einem eine Funktion, gibt es dafür wahrscheinlich eine Erweiterung, die sie nachrüstet. Eine solche Gnome Shell Extension ist wie Teile der Shell in JavaScript programmiert. Die Ausführung übernimmt die Runtime „Gnome JavaScript“ (GJS).

Da JavaScript ursprünglich nur dafür gedacht war, Webseiten zu pimpen, fehlte es zunächst an einem Importmechanismus, der Programmbestandteile aus anderen Dateien lädt. Daher haben Projekte wie Node.js und Gnome für GJS zunächst eigene Importsysteme entwickelt, um Module nachzuladen. Später erhielt JavaScript ein einheitliches, standardisiertes Importsystem namens „ES Modules“ (ESM). Dieses verwendet seit Version 45 nun auch die Gnome Shell.

Mit dem Wechsel vom GJS-Eigenbau zum Standard ES Modules verwenden Programme und Erweiterungen für Gnome die bekannte und übliche JavaScript-Syntax. So finden sich Außenstehende mit JavaScript-Erfahrung leichter zurecht und können einfacher eigene Erweiterungen schreiben oder vorhandene verbessern. Da sich die Syntax aber von jener von GJS unterscheidet, müssen alle Gnome-Erweiterungen angepasst werden.

Der Aufwand ist in der Regel überschaubar und die Autoren vieler populärer Erweiterungen haben diese bereits an Gnome 45 angepasst.

In diesem Artikel erklären wir, wie Gnome-Erweiterungen aufgebaut sind, und zeigen Schritt für Schritt an der Erweiterung „Date Menu Formatter“, welche Änderungen notwendig sind, um diese auf Gnome 45 zu migrieren. Sollte Ihre Lieblingserweiterung noch nicht aktualisiert sein, sehen Sie, was nötig ist, um sie anzupassen. Ein Grundverständnis für JavaScript genügt.

c't kompakt

- Gnome Shell nutzt ab Version 45 den JavaScript-Standard „ES Modules“.
- Dafür muss der Code von Erweiterungen angepasst werden, aber der Aufwand ist überschaubar.
- Bestehende Erweiterungen lassen sich leicht migrieren und die Änderungen als Pull-Request einreichen.

Grundlagen

Bevor es an die konkreten Schritte geht, vorab etwas Theorie zu Gnome-Erweiterungen und Imports.

Wie man eine Gnome-Erweiterung schreibt, sprengt den Rahmen des Artikels. Eine Anleitung finden Sie unter ct.de/yxgr. Zum Verständnis nur so viel: Eine Gnome-Erweiterung enthält mindestens zwei Dateien: extensions.js und metadata.json. In extension.js gibt es eine Klasse, welche abgeleitet ist von `Extension` aus gnome-shell/js/extensions/extension.js. Sie muss die Methoden `enable()` und `disable()` enthalten. Wenn `enable()` aufgerufen wird, wendet die Erweiterung ihre Änderungen an der Gnome Shell an, und bei `disable()` muss sie die Änderungen wieder rückgängig machen. Den Code aus extension.js führt `gnome-shell` in ihrem Prozess aus.

Die Datei metadata.json enthält, wie der Name schon andeutet, Metadaten der Erweiterung im JSON-Format. Dazu zählen eine eindeutige ID (`"uuid"`), der Name der Erweiterung, ihre Beschreibung und eine Liste der kompatiblen Gnome-Shell-Versionen.

Bietet die Erweiterung einen Einstellungsdialog an, benötigt man dafür noch eine Datei namens prefs.js. Hinzu kommen eigene JavaScript-Dateien, Stylesheets, Icons, Töne und andere Materialien. Alle Dateien kommen in ein Verzeichnis, dessen Name der UUID entspricht.

Am Anfang von extension.js stehen die Importe. Bei der vorher von GJS genutzten Eigenbausyntax gab man Importe in einer Punktnotation an, die den Pfad nur unvollständig abbildete:

```
const Main = imports.ui.main;
```

Mit ES Modules und dessen Syntax entsprechen alle Importe entweder einem Pfad oder einem URI (Uniform Resource Identifier), wie es in modernen JavaScript-Frameworks inzwischen üblich ist. In Gnome 45 sieht der gleiche Import nun wie folgt aus:

```
import * as Main from 'resource://
      ↳/org/gnome/shell/ui/main.js';
```

Importtypen und ihre Syntax

Es gibt für verschiedene Importtypen eigene Pfadangaben: Gnome-Bibliotheken, GResource-Module und eigene Module.

Gnome-Bibliotheken sind üblicherweise in C programmiert, allerdings mit einem Flair von Objektorientierung, wobei alle Objekte auf `GObject` aufbauen. Damit man aus JavaScript auf Klassen zugreifen und sie importieren kann, generiert GObject-Introspection (GI) Bindings dorthin. Darüber erfährt die JavaScript-Engine GJS, welche Eigenschaften und Methoden verfügbar sind und wie es den Speicher managen soll. Pfade zu Bibliotheken sind sehr schlicht und haben keine Unterverzeichnisse. Ihr URI beginnt jeweils mit `gi://`:

```
// Syntax vor Gnome 45:
// const GLib = imports.gi.GLib;

import GLib from 'gi://GLib';
```

Um Module der Gnome Shell zu importieren, welche sich in JavaScript-Dateien finden, verwendet man die Schnittstelle GResource. Dies ist ein virtuelles Dateisystem, aus dem Anwendungen benötigte Dateien in den Speicher laden können. Sie verhalten sich wie echte Dateien und ihr Pfad beginnt meist mit der Application-ID, wobei die Punkte durch ein `/` ersetzt werden. Der GResource-Pfad unterscheidet Groß- und Kleinschreibung.

In extension.js beginnen sämtliche Importe von Modulen der Gnome Shell mit `resource:///org/gnome/shell/`.

```
import * as Util from 'resource://
      ↳/org/gnome/shell/misc/util.js';
```

Anders verhält es sich bei Importen in der Datei prefs.js. Da der Prozess, der prefs.js ausführt, die Application-ID `org.gnome.Shell.Extensions` hat, beginnt hier der URI mit `resource:///org/gnome/Shell/Extensions/`. Beachten Sie die großen Anfangsbuchstaben bei Shell und Extensions:

```
import {ExtensionPreferences} from
  'resource:///org/gnome/Shell/
  ↳Extensions/js/extensions/prefs.js';
```

Die Extension und ihre Einstellungen laufen in getrennten Prozessen.

Leider beschreibt die Gnome-Dokumentation nicht alle verfügbaren Module. Am einfachsten ist es, im Quelltext der Gnome Shell nachzusehen. Die relevanten Stellen im Gnome-Repository bei GitLab und der Dokumentation haben wir unter ct.de/yxgr verlinkt.

Einfacher wird der Import von eigenen Modulen. Hier erwartet GJS relative Pfade und Dateinamen wie bei Node.js oder anderen JavaScript-Frameworks. Wenn Ihre Erweiterung im Unterverzeichnis lib eine Datei namens utils.js enthält, dann lautet der Import:

```
import * as Utils
from './lib/utils.js';
```

Eingeschränkten Zugriff handhaben

Nicht immer genügt es, nur die Syntax anzupassen, denn es gibt einen Haken: Vor der Einführung von ES Modules waren die in Gnome-Erweiterungen genutzten Module nur Skripte und man konnte auf sämtliche darin definierten Klassen, Funktionen und Variablen zugreifen. Mit ES Modules geht das nicht mehr. Der Zugriff ist nur noch auf Elemente möglich, die das Modul mit dem Schlüsselwort `export` freigibt. Standardmäßig werden Variablen nur lesbar exportiert, außer wenn jemand für eine Erweiterung um Schreibzugriff bittet.

Benötigen Sie für die anzupassende Erweiterung Zugriff auf nicht exportierte Elemente aus der Gnome Shell oder Schreibzugriff auf eine Variable, dann bit-

ten Sie die Gnome-Entwickler darum. Ergänzen Sie den Code der Gnome Shell um die benötigten Exports und reichen Sie diese Änderungen in einem Merge-Request auf GitLab ein. Schreiben Sie in der Commit-Nachricht, warum und wofür Sie die Exports benötigen. Auf Nachfrage von c't bestätigten verantwortliche Gnome-Entwickler ihre Bereitschaft, benötigte Exports zu ergänzen. Andernfalls versuche man, gemeinsam nach einer alternativen Lösung zu suchen. Im Gnome-Shell-Repository finden sich etliche angenommene Änderungen.

Portierung in der Praxis

Genug der Theorie – auf ans Eingemachte! Sie benötigen lediglich einen Texteditor und die Versionskontrollsoftware Git, die Sie auf Linux-Systemen einfach über die Paketverwaltung installieren; etwa mit `sudo apt install git` unter Debian und Ubuntu.

Wir haben die Erweiterung „Date Menu Formatter“ ausgewählt, die bisher nicht für Gnome 45 angepasst war. Mit ihr ändert man das Format der Uhrzeit- und Datumsanzeige im Gnome-Panel. Die Erweiterung eignet sich gut, um die Änderungen zu demonstrieren.

Als Erstes haben wir das Code-Repository der Erweiterung auf GitHub geforkt. Den Link zum Repository finden Sie meistens in der Beschreibung der Erweiterung auf extensions.gnome.org unter „Homepage der Erweiterung“. Liegt das Repository auf einer GitLab-Instanz, melden Sie sich dort statt bei GitHub an.

Den neuen Fork haben wir mit Git geklont, also auf unser lokales System kopiert:

```
git clone git@github.com:andyholmes↵
            ↳/date-menu-formatter.git
```

Anschließend sind wir in das Verzeichnis des lokalen Repository gewechselt und haben einen neuen Branch (Entwicklungszweig) namens „andyholmes/gnome-45“ angelegt (`-c`). Danach sind wir dorthin gewechselt (`switch`).

```
cd date-menu-formatter
git switch -c andyholmes/gnome-45
```

Mit einem neuen Entwicklungszweig trennt man Änderungen sauber und kann diese später als Pull-Request im ursprünglichen Repository einreichen. Machen Sie das sinngemäß genauso, aber passen Sie die Bezeichnungen an Ihren User- und Projektnamen an.

Als Nächstes prüfen Sie, ob die Erweiterung veraltete (deprecated) Module wie `Mainloop`, `Signals` oder `ByteArray` nutzt und aktualisieren Sie diese Aufrufe. Ein Indiz für veraltete Module sind Importanweisungen, die weder mit `import.gi` beginnen noch unter den GResource-Modulen auffindbar sind. Außerdem steht in der GJS-API-Referenz eine Warnung („This module is not available as an ECMAScript Module“).

Die Erweiterung Date Menu Formatter greift in extensions.js auf das schon länger veraltete Modul „Mainloop“ zu (`imports.mainloop`), was mit ES Modules nicht mehr zugänglich ist. Die benötigte Funktion `timeout_add_seconds()` findet sich in GLib. Einen Vorher/Nachher-Vergleich finden Sie unter ct.de/yxgr verlinkt.

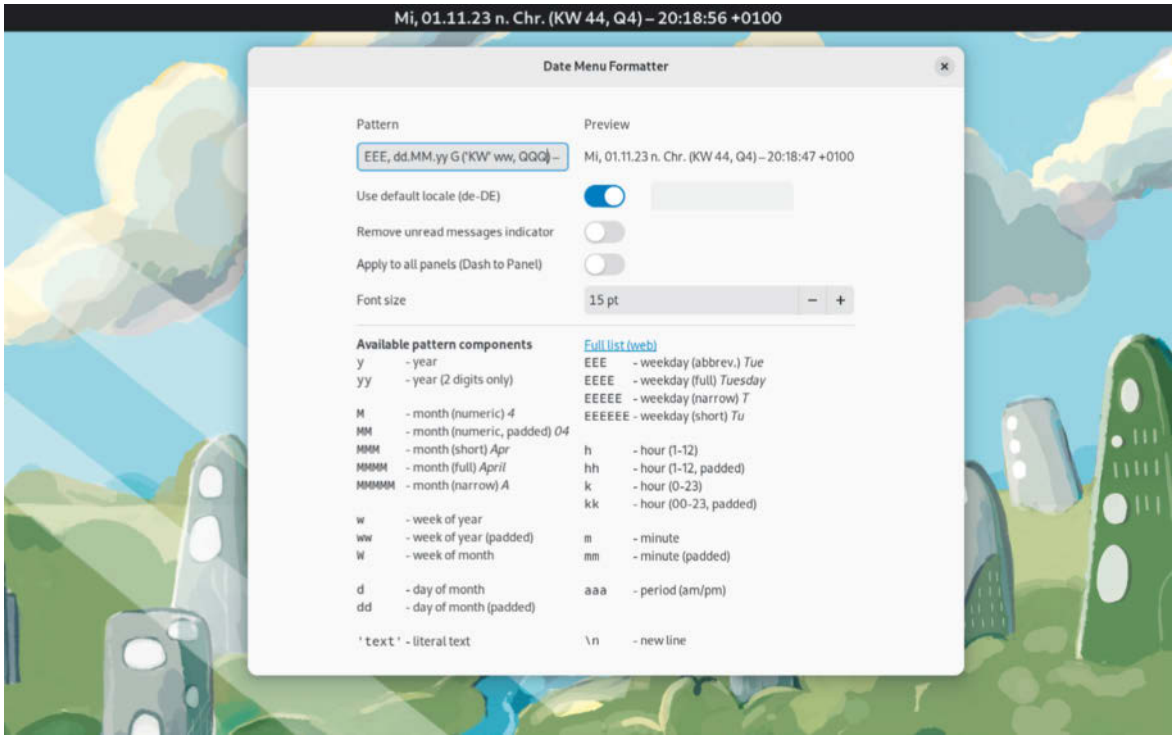
Importe umwandeln

Nun gilt es, die Änderungen auf die Importe zu übertragen. Starten Sie in der Datei extension.js und ändern Sie alle Importe wie oben beschrieben in die ESM-Syntax um. Bei „Date Menu Formatter“ muss man die kompakte Schreibweise `const { GLib, Clutter, St } = imports.gi;` in einzelne Statements aufteilen:

```
import GLib from 'gi://GLib';
import Clutter from 'gi://Clutter';
import St from 'gi://St';
```

Wenn ein Modul importiert werden soll, das zur Codebasis der eigenen Erweiterung gehört, ist der alte Code verwirrend umständlich.

```
const Me =
 ExtensionUtils.getCurrentExtension();
const { SimpleDateFormat } =
 Me.imports.lib.SimpleDateFormat;
```



Mit der Erweiterung „Date Menu Formatter“ kann man die Datumsanzeige individuell einrichten. Nach unseren Anpassungen funktioniert sie auch mit Gnome 45.

Derselbe Import für Gnome 45 sieht wesentlich eleganter aus:

```
import { SimpleDateFormat } from
  './lib/SimpleDateFormat.js';
```

Statt mit * alles aus dem Modul zu importieren, beschränken die geschweiften Klammern den Import auf die genannten Elemente, also auf die Klasse `SimpleDateFormat`.

Als Nächstes deklarieren Sie die Klasse der Erweiterung anders. Importieren Sie zunächst das Modul `Extension` von der Gnome-Shell:

```
import { Extension } from
  'resource:///org/gnome/shell/↵
          ↳extensions/extension.js';
```

Leiten Sie danach eine Klasse mit einem eindeutigen Namen von `Extension` ab und machen diese mittels `export default` sichtbar:

```
export default class DateMenuFormatter
  extends Extension {
    // ...
}
```

Die Deklaration als `default` stellt sicher, dass die Gnome-Shell diese Klasse importieren kann, ohne ihren genauen Namen zu kennen.

Sollten Sie in dieser `default`-Klasse den `constructor()` überschreiben, müssen Sie die Funktion `super()` aufrufen und die Metadaten an die Elternklasse weitergeben:

```
constructor(metadata) {
  super(metadata);
  this._displays =
    [this._createDisplay()];
  // ...
}
```

Die vorher verpflichtende Methode `init()` ist jetzt obsolet und Sie sollten sie entfernen. Meist wurde `init()` genutzt, um die Übersetzung der Extension-Bedienelemente zu starten. Die Gnome Shell initialisiert Übersetzungen automatisch seit Version 45, wenn es in der `metadata.json` einen Eintrag für den Schlüssel `gettext-domain` gibt.

Haben Sie die Klasse geändert, passen Sie anschließend diejenigen Ausdrücke mit `var` an, mit denen ein Element exportiert werden sollte. Verwenden Sie dafür `export const` (oder `export let` für Variablen mit Schreibzugriff).

Einstellungen migrieren

Wenn Sie mit den Anpassungen in extensions.js fertig sind, setzen Sie das Prozedere in der Datei prefs.js fort, sofern vorhanden.

Darin sind die Importe und Exporte anzupassen. Die Datei muss unbedingt die Elternklasse `ExtensionPreferences` importieren:

```
import { ExtensionPreferences } from
  'resource:///org/gnome/Shell/↵
  ↳Extensions/js/extensions/prefs.js';
```

Achten Sie dabei wie gehabt auf die Groß- und Kleinschreibung im URI.

Deklarieren Sie die von `ExtensionPreferences` abgeleitete `default`-Klasse. Bei den Einstellungen von Date Menu Formatter sieht das so aus:

```
export default
  class DateMenuFormatterPreferences
  extends ExtensionPreferences {
    // ...
}
```

Vergessen Sie nicht, auch andere Module beziehungsweise JavaScript-Dateien der zu migrierenden Erweiterung zu prüfen. In der Datei „lib/SimpleDateFormat.js“ des Date Menu Formatter stand vorher:

```
var SimpleDateFormat = class { // ...
```

Das haben wir geändert zu

```
export const SimpleDateFormat =
  class { // ...
```

Erst damit funktioniert der weiter oben beschriebene Import von `SimpleDateFormat`.

Sind alle JavaScript-Dateien angepasst und veraltete Aufrufe ausgemistet, fehlt noch ein letzter Schritt: In der Datei metadata.json geben Sie an, mit welcher Gnome-Version die Erweiterung kompatibel ist. Die Versionsnummern tragen Sie unter dem Schlüssel `shell-version` ein. Es akzeptiert Versionsnummern als eine Liste aus Zeichenketten: (`"shell-version": [ "44", "43.beta", ... ]`). Da durch den Umstieg auf ESM die Erweiterungen nicht mehr zu vorherigen Gnome-Versionen kompatibel sind, entfernen Sie alle Nummern und tragen lediglich die aktuelle Version ein:

```
"shell-version": ["45"],
```

Um gleichzeitig Gnome-Versionen vor und nach dem Wechsel auf ES Modules zu bedienen, können Entwickler verschiedene Varianten ihrer Erweiterung auf extensions.gnome.org hochladen. Wir empfehlen, Varianten einer Erweiterung für verschiedene Gnome-Versionen mit Git-Branches zu pflegen.

Erweiterung testen

Beachten Sie beim Testen: Wenn Sie eine Erweiterung aktivieren, dann wird dabei die Gnome Shell gepatcht, also ihr Code verändert. Die Erweiterung wird ein Teil des Gnome-Shell-Prozesses. Im Unterschied zu anderen Frameworks können JavaScript-Engines den Code nicht mehr entladen/rauswerfen. Um Änderungen an der Erweiterung sauber zu testen, müssen Sie die Gnome Shell vorher neu starten beziehungsweise den geänderten Code mit einem neuen Prozess einlesen.

Vorher paketieren Sie erst einmal die Erweiterung. Falls Sie im Terminal nicht eh schon an Ort und Stelle sind, wechseln Sie mit `cd` in das Projektverzeichnis mit dem Quelltext Ihrer Erweiterung. Bauen Sie darin mit dem Tool `gnome-extensions` das installierbare Erweiterungspaket. Bekannte Dateien, wie extensions.js, prefs.js, Stylesheets, Übersetzungen und GSettings-Schemas findet es selbst. Mit der Option `--extra-source=` übergeben Sie zusätzliche Quellen, etwa eigene JavaScript-Dateien:

```
gnome-extensions pack \
  --extra-source=utils.js \
  --extra-source=lib/
```

Anschließend finden Sie eine Zip-Datei, die passend zur UUID benannt ist und alle benötigten Dateien enthält. Dieses Paket installieren Sie mit dem Subkommando `install`.

```
gnome-extensions install \
  date-menu-formatter@marcin↵
  ↳jakubowski.github.com.↵
  ↳shell-extension.zip
```

Daraufhin starten Sie die Gnome-Session neu, indem Sie sich ausloggen und wieder anmelden. Da das auf Dauer lästig ist, wäre auch während der laufenden Session der Start einer neuen, verschachtelten (nested) Gnome Shell eine Option:

```
dbus-run-session --  gnome-shell \
  --nested --wayland
```

Dazu muss die Gnome-Sitzung im Wayland-Modus laufen. Verwendet ihr Gnome den altbackenen X11-Modus, dann starten Sie stattdessen den laufenden Gnome-Shell-Prozess neu, indem Sie Alt+F2 drücken und dann `r` eingeben und mit der Eingabetaste bestätigen.

Innerhalb der neu gestarteten Gnome Shell, egal ob „nested“ oder mit X11, öffnen Sie ein Terminal und aktivieren die Erweiterung:

```
gnome-extensions enable ↵
  ↳date-menu-formatter@marcin↵
  ↳jakubowski.github.com
```

Dies müssen Sie in Regel nur einmal machen, solange Sie die Erweiterung nicht mit `disable` oder anderweitig deaktivieren. Die Änderungen der Erweiterung an der Gnome Shell sollten unmittelbar aktiv und sichtbar sein.

Die Zip-Datei können Sie auf einen anderen Computer oder in eine virtuelle Maschine kopieren, installieren und testen. Dies bietet sich an, um das Verhalten der jeweiligen Erweiterungsvarianten unter Gnome 44 und 45 zu testen.

Wichtig ist, daher wiederholen wir den Hinweis, dass Sie die Gnome Shell jedes Mal neu starten müssen, bevor Sie veränderten Code testen können.

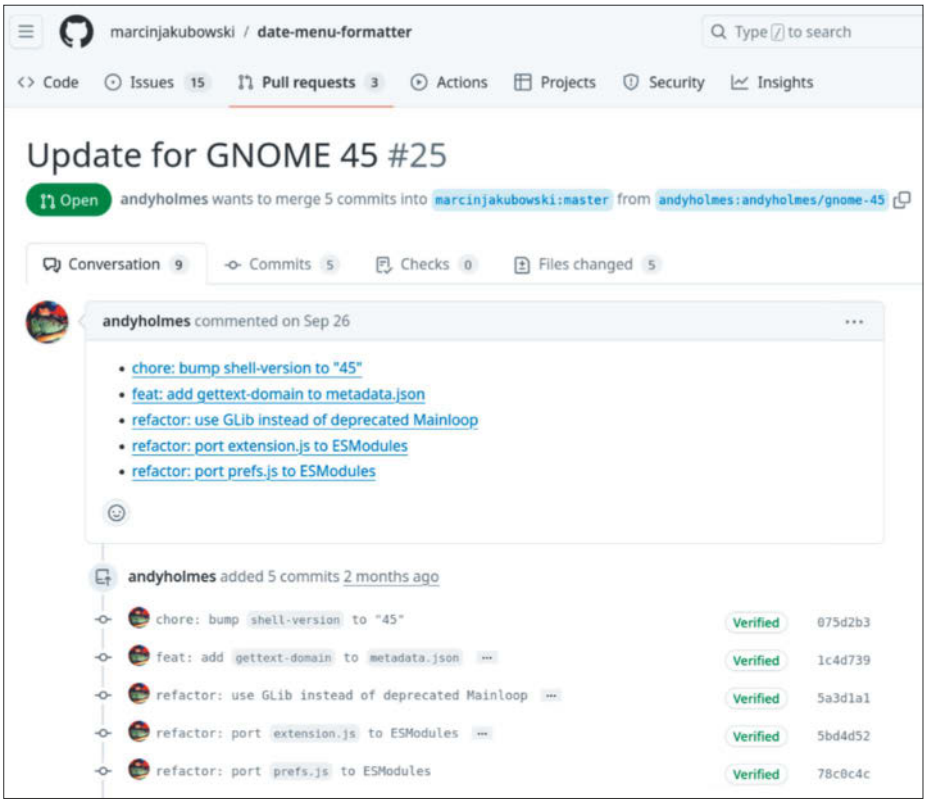
Hilfe

Kommen Sie beim Migrieren nicht weiter, fragen Sie ruhig online bei der Gnome-Community nach Unterstützung. Die Maintainer der Gnome Shell und von GJS sind sehr aktiv und in der Regel hilfsbereit. Ein guter Ort für Ihre Fragen ist der Chatraum #extensions:gnome.org, wofür Sie ein Konto im Kommunikationsnetzwerk Matrix brauchen. Das können Sie direkt mit dem Messenger Element registrieren, den es als Webanwendung für den Browser gibt und auch herunterladbar als App für Linux, Windows, macOS sowie Android und iOS.

Weitere Informationen finden Sie in der englischsprachigen Dokumentation unter gjs.guide. Die ist verständlich geschrieben, aber lückenhaft.

Pull-Request einreichen

Haben Sie die Erweiterung erfolgreich angepasst und getestet, checken Sie Ihre Änderungen mit `git commit` in Ihr lokales



Die Änderungen an der Erweiterung haben wir auf GitHub als Pull-Request zur Begutachtung eingereicht.

Repository ein. Git fragt Sie nach einer Commit-Beschreibung. Diese sollte knapp den Anlass der Änderung beschreiben.

Um den aktuellen Branch aus Ihrem lokalen Git-Repository auf GitHub hochzuladen, definieren Sie für diesen Branch mit `git push -u` ein Upstream-Ziel. Bei uns sah der Git-Befehl wie folgt aus:

```
git push -u origin andyholmes/gnome-45
```

Nun reichen Sie Ihre Änderungsvorschläge im ursprünglichen Repository als Pull-Request zur Begutachtung ein. Auf GitLab heißt es „Merge Request“, bedeutet aber de facto das Gleiche. Beide Plattformen erzeugen aus den Unterschieden zwischen Ihrem Entwicklungszweig und dem Ziel-Branch einen Diff, samt Beschreibung, Visualisierung, Ticket und Diskussionsbereich. Außerdem prüfen sie, ob eine konfliktfreie Integration der Code-Änderungen möglich ist. Im Idealfall sagen die Maintainer der Erweiterung nur danke und nehmen den Pull-Request an, mergen ihn also.

Öffnen Sie dazu im Webbrowser auf der GitHub-Webseite das von Ihnen geforkte Repository und klicken Sie oberhalb der Dateiliste auf „... Branches“. Suchen Sie in der Liste den von Ihnen für die Migration erstellten Entwicklungszweig und klicken Sie rechts auf die Schaltfläche „New pull request“. Github wählt das ursprüngliche Repository als Vergleichsbasis. Passen Sie das noch an den Branch an, etwa wenn es neben „master“ oder „main“ schon einen eigenen Branch für die Anpassung auf Gnome 45 gibt.

Füllen Sie das Formular aus: Vergeben Sie einen Titel und beschreiben Sie im Text, warum Sie den Pull-Request einreichen und weshalb Sie sich für Ihre Herangehensweise entschieden haben. Schicken das Ganze mit „Create pull request“ ab.

Nachdem wir auf GitHub unseren Pull-Request eingereicht hatten, passierte einige Tage lang nichts. Auf Rückfrage eines Users, ob die Erweiterung noch aktiv gepflegt werde, schrieb der Entwickler, er plane bisher nicht, auf Gnome 45 zu wechseln. Wer die Erweiterungen portieren möchte, solle ruhig die Erweiterung forken. Das ist eben auch Open Source: Nicht jede Verbesserung wird dankend angenommen, aber man hat die Freiheit, den Quellcode zu nehmen und ihn eigenständig weiterzuentwickeln. *(ktn@ct.de)* c't

Dokumentation, Tutorials, Quelltexte: ct.de/yxgr

Endet das Schweigen?

Whistleblower-Schutz: Neue Bestimmungen jetzt umsetzen!

Nach zähem Ringen und sehr verspätet ist im Sommer das neue Hinweisgeberschutzgesetz in Kraft getreten. Trotz einiger Schwächen kann es dazu führen, dass mehr Missstände in Unternehmen abgestellt werden.

Von Harald Büring

Whistleblower, die Missstände in Unternehmen und anderen Organisationen aufdecken, erfüllen eine wichtige gesellschaftliche Aufgabe. Gleichwohl waren diese Hinweisgeber vom deutschen Recht lange Zeit unzureichend geschützt. Viele Übel dürften nur deshalb auf Dauer existiert haben, weil Menschen, die sie hätten melden können, Angst vor Repressalien oder anderen Nachteilen hatten.

Wie unsicher die Situation vor Gericht war, zeigt das Beispiel einer Altenpflegerin, die einen Missstand in der Pflege angezeigt hatte und deshalb von ihrem Arbeitgeber gekündigt worden war: Das Bundesarbeitsgericht (BAG) hielt die Kündigung für rechtmäßig [1] und das Bundesverfassungsgericht (BVerfG) nahm ihre Verfassungsbeschwerde nicht zur Entscheidung an [2]. Erst der Europäische Gerichtshof für Menschenrechte (EGMR) sah die Sache anders und sprach ihr zumindest eine Entschädigung zu [3].

Wie riskant es sein konnte, einen Missstand intern zu melden, zeigt ein Fall, in dem ein Arbeitnehmer seinen Arbeitgeber auf schwere Verstöße gegen den Brandschutz aufmerksam gemacht und auf einer Änderung bestanden hatte. Der Arbeitgeber stellte ihn deshalb von der Arbeit frei, sperrte seinen Account und erteilte ihm Hausverbot. Daraufhin meldete der Mitarbeiter die Verstöße der Bauaufsicht und drohte dem Arbeitgeber damit, an die Öffentlichkeit zu gehen. Der kündigte ihm fristlos. Erst das Landesarbeitsgericht (LAG) Niedersachsen entschied, dass die Kündigung rechtswidrig war – aber nur, weil sich der Arbeitgeber eindeutig rechtswidrig verhalten und dadurch erheblich zur Eskalation beitragen hatte [4].

Zähes Ringen

Trotz dieser untragbaren Situation tat sich der deutsche Gesetzgeber lange Zeit schwer, potenziellen Hinweisgebern mit schützenden Regelungen Rückendeckung zu geben. Zunächst trat auf europäischer Ebene Ende 2019 die EU-Richtlinie 2019/1937 (Whistleblower-Richtlinie) in Kraft. Im Vorfeld war es vor allem um die Frage gegangen, ob sich ein Hinweisgeber zunächst an seinen Arbeitgeber wenden muss und sich erst nach vergeblicher Klärung an externe Stellen wenden darf. Nach langen Mühen einigte man sich darauf, dass ihm das freigestellt bleiben soll (Art. 10). Allerdings dürfen Whistleblower normalerweise nicht sofort einen Missstand publik machen (Art. 15).

Die Bestimmungen der Whistleblower-Richtlinie hätten eigentlich bereits bis zum 17. Dezember 2021 in nationales Recht umgesetzt sein müssen. Doch es folgte ein zähes Ringen, der Gesetzgebungsprozess zog sich in die Länge. Der erste Anlauf in Form eines Referentenentwurfs des Bundesjustizministeriums (BMJ) scheiterte im Februar 2021 bereits daran, dass ihm das Bundeskabinett nicht zustimmte.

Nach der Bundestagswahl reichte das nunmehr FDP-geführte BMJ erneut einen Referentenentwurf ein, zu dem das Bundeskabinett im Juli 2022 einen Regierungsentwurf verabschiedete. Nachdem der Bundestag das Hinweisgeberschutzgesetz (HinSchG) im Dezember 2022 endlich verabschiedet hatte, blockierte der Bundesrat diese Fassung. Im Vermittlungsausschuss einigte man sich schließlich auf eine modifizierte Fassung, die nach Zustimmung durch den Bundestag und den Bundesrat am 2. Juli 2023 in Kraft trat.

Die verspätete Umsetzung der Whistleblower-Richtline in deutsches Recht hatte sogar zur Folge, dass die EU-Kommission gegen Deutschland ein Vertragsverletzungsverfahren einleitete. Nachdem sie Deutschland vergeblich zur Umsetzung aufgefordert hatte, verklagte die Kommission Deutschland vor dem Europäischen Gerichtshof (EuGH). Die Klage ist seitdem dort anhängig (Az. C-149/23). Experten rechnen damit, dass die Bundesrepublik

Die Anbieter von Meldestellensoftware erleben derzeit einen kleinen Boom.

mindestens 30 Millionen Euro Strafe zahlen muss.

Noch wirken nicht alle Vorschriften des neuen Gesetzes vollständig, doch spätestens jetzt sollten sich Arbeitgeber auf die neue Situation einstellen. Unternehmen mit mindestens 50 Beschäftigten müssen gemäß § 12 Abs. 2 HinSchG einen internen Meldekanal für potenzielle Hinweisgeber einrichten und betreiben. Dies kann ein IT-gestütztes Hinweisgebersystem sein. Dafür geeignete Softwareanwendungen und externe Dienste erleben gerade einen kleinen Boom. Im Prinzip genügt es aber bereits, wenn das Unternehmen eine Telefonhotline für Hinweisgeber betreibt.

Bild: Jörg Carstensen/dpa

Der CDU-Abgeordnete Günter Krings bestand im Bundestag darauf, dass eine anonyme Meldestelle in Unternehmen nicht nötig sei.

Kulanzfrist läuft aus

Ab welchem Zeitpunkt diese Pflicht greift, hängt von der Anzahl der Mitarbeiter ab. Unternehmen mit 50 bis 249 Beschäftigten dürfen sich noch bis zum 17. Dezember dieses Jahres Zeit lassen (§ 42 Abs. 1 HinSchG). Bis dahin gilt eine Kulanzregelung für sie, in der sie keine Bußgeldstrafen befürchten müssen. Unternehmen mit wenigstens 250 Beschäftigten müssen sich besonders beeilen, falls sie die Pflichten noch nicht umgesetzt haben: Sie müssen bereits seit dem Inkrafttreten des Hinweisgeberschutzgesetzes Anfang Juli Strafzahlungen fürchten.

In einigen Ausnahmefällen müssen übrigens auch Unternehmen mit weniger als 50 Beschäftigten eine interne Meldestelle betreiben. Dies gilt beispielsweise für Wertpapier-Dienstleistungsunternehmen, Kreditinstitute und Finanzdienstleister. Die einbezogenen Bereiche führt § 12 Abs. 3 HinSchG auf.

Generell gilt: Nutzt ein Mitarbeiter den Kanal, muss ihm dies die interne Meldestelle innerhalb von sieben Tagen bestätigen. Binnen drei Monaten muss sie ihn über die ergriffenen Maßnahmen informieren. Das können interne Compliance-Untersuchungen sein oder die Weiterleitung der Meldung an eine zuständige Stelle, etwa eine Strafverfolgungsbehörde.

Als zweite, gleichwertige Möglichkeit zur Abgabe von Hinweisen hat das Bundesamt für Justiz (BfJ) eine externe Meldestelle eingerichtet. Dem Gesetz zufolge dürfen auch die Bundesländer eigene externe Meldestellen einrichten. Whistleblower können sich frei entscheiden, ob sie eine Meldung an die interne Meldestelle ihres Unternehmens geben oder die externe Meldestelle nutzen möchten.

Wie eine Sprecherin des Justizministeriums mitteilte, hat die beim BfJ angesiedelte Meldestelle von Anfang Juli bis zum 12. September insgesamt 113 Meldungen erhalten. Die meisten davon gingen den Angaben zufolge über ein Onlineformular ein. Auch die Beratungsleistung der Meldestelle werde „rege in Anspruch genommen“, sagte die Sprecherin.

Anonymität nur optional

Viel Streit drehte sich während des Gesetzgebungsverfahrens um die Frage, inwieweit Unternehmen anonymen Hinweisen nachgehen beziehungsweise dafür interne Meldekanäle einrichten müssen. Die vom Bundestag im Dezember 2022 verabschiedete Fassung des Hinweisgeberschutzgesetzes sah vor, dass interne Meldestellen auch anonyme Kontaktaufnahmen ermöglichen müssen. Demgegenüber lautet die in Kraft getretene Fassung von § 16 Abs. 1 Satz 4 bis 5 HinSchG wie folgt: „Die interne Meldestelle sollte auch anonym eingehende Meldungen bearbeiten. Es besteht allerdings keine Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen“.

Der Gesetzgeber hat dadurch nicht nur die Unternehmen von der Einrichtung spezieller Meldekanäle für anonyme Meldungen entbunden. Er hat durch die Formulierung „sollte“ zugleich klargestellt, dass Entgegennahme anonymer Meldungen ohnehin nur eine Handlungsempfehlung, aber keine Verpflichtung gibt. In der Bundestagsdebatte ums Gesetz am 11. Mai 2023 bestand Günter Krings (CDU) darauf, dass es besser sei, wenn Hinweisgeber ihren Namen angeben. Sie seien durch das Hinweisgeberschutzgesetz dennoch hinreichend geschützt. Außerdem sei es für Unternehmen zu aufwendig, einen anonymen internen Meldekanal einzurichten. Und in der darauf folgenden Sitzung des Bundesrats verwies Thomas Strobel (CDU) darauf, dass seiner Ansicht nach vor allem kleine Familienbetriebe überlastet würden, sollten sie anonyme Kanäle betreiben müssen.

Ob das Hinweisgeberschutzgesetz Whistleblower ausreichend schützt, ist fraglich: Der Schutzbereich erstreckt sich über EU-Recht und Straftaten hinaus nur auf die in § 2 Abs. 1 HinSchG detailliert aufgeführten Verstöße, beispielsweise zur Produktsicherheit. Ferner wird die Situation schwierig, wenn sich der Whistleblower geirrt hat. Er ist bereits dann nicht geschützt, wenn er grob fahrlässig eine unzutreffende Meldung abgegeben hat (§ 9 HinSchG). Wann eine Meldung grob fahrlässig ist, ist Einschätzungssache, also im Zweifel eine Sache für die Gerichte.

Auch wenn es das Gesetz nun nicht erzwingt: Unternehmen sollten freiwillig anonyme interne Meldungen über etwaige Missstände prüfen. Das hat den Vorteil, dass sie eher von Verstößen beziehungsweise kriminellen Machenschaften erfahren. Dies ist vor allem wichtig, wenn es um die Sicherheit der Mitarbeiter beispielsweise durch Missachtung des Brandschutzes oder um die Gefährdung der IT-Sicherheit geht. *(hob@ct.de)* c't

Literatur

[1] BAG, Beschluss vom 06.06.2007, Az. 4 AZN 487/06
[2] BVerfG, Beschluss vom 06.12.2007, Az. 1 BvR 1905/07
[3] EGMR, Urteil vom 21.07.2011, Az. 28274/08
[4] LAG Niedersachsen, Urteil vom 16.03.2022, Aktenzeichen 8 Sa 809/20

Tipps & Tricks

Sie fragen – wir antworten!

Kein 5G mit CallYa

Mein Prepaid-Tarif von Vodafone CallYa erlaubt die Nutzung von 5G. Mein Smartphone ist 5G-fähig, bucht sich aber nur ins 4G-Netz ein, obwohl ich das 5G-Netz in den Einstellungen freigegeben habe. Gibt es irgendwo noch eine versteckte Einstellung, damit ich auch 5G nutzen kann?

Einige CallYa-Kunden klagen darüber, dass ihr Smartphone sich nicht ins 5G-Netz einbuchen will. Das liegt aber in den meisten Fällen nicht am Smartphone, sondern an den Einstellungen, die beim Provider hinterlegt sind. Kontaktieren Sie den CallYa-Kundenservice unter der Rufnummer 0172/2 29 02 29 telefonisch oder per WhatsApp und bitten Sie darum, 5G freizuschalten. Nach einem Neustart des Smartphones sollte 5G dann funktionieren. *(uma@ct.de)*

Zeitumstellung mit Verzögerung

Bei der Umstellung von Sommer- auf Winterzeit haben sich zwei Funkuhren in meinem Haushalt wieder einmal nicht umgestellt. Ich habe diesmal die Uhren nicht neu gestartet, sondern abgewartet. Erst in der Nacht zum Montag stellten sie sich dann richtig ein, wie ich am folgenden Morgen feststellte. Woher kommt diese große Verzögerung?

Viele Funkuhren synchronisieren die Uhrzeit nur einmal in 24 Stunden mit dem Zeitzeichensender, um Energie zu sparen. Einige verbreitet eingesetzte Uhrwerke für Funkuhren machen dies stets morgens um 1 Uhr, also kurz vor der eigentlichen Zeitumstellung. Die Geräte bekommen deshalb erst 22 beziehungsweise 23 Stunden später mit, wenn eine Zeitumstellung erfolgt ist. Einen Workaround dafür gibt es nicht. Sie müssen entweder warten, bis die betroffenen Uhren sich wieder synchronisieren, oder eine Synchronisierung durch kurzes Entnehmen der Batterien aktiv anstoßen.

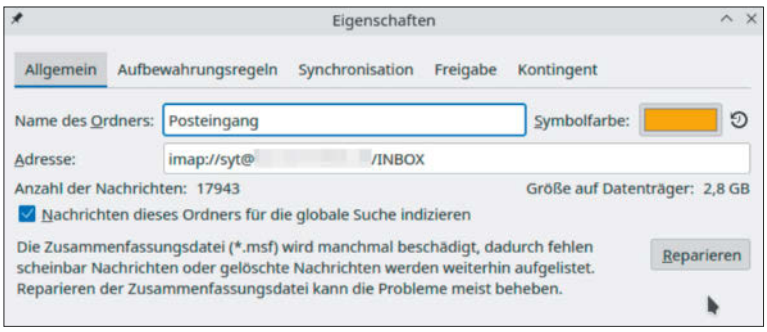
Aber auch korrekt programmierte Funkuhren haben zunehmend Probleme, das Funksignal zu empfangen. Die Übertragung geschieht auf Langwelle, der Sender steht in Mainflingen bei Frankfurt. Der Empfang des mit zunehmender Entfernung vom Sender immer leiser werdenden Signals wird oft von lokalen Störungen beeinträchtigt, beispielsweise aus Monitoren oder Schaltnetzteilen. Die beste Chance für den Empfang besteht in der zweiten Nachthälfte, weil dann viele Geräte, die lokale Störungen verursachen, abgeschaltet sind. Es kann aber auch helfen, die Geräte vorübergehend an einen anderen Ort im Haus zu bringen, wo weniger Störungen herrschen. *(uma@ct.de)*

Thunderbird: E-Mail-Nachricht kaputt

Wenn ich in Thunderbird eine bestimmte Nachricht öffne, braucht das Programm seltsam lange, um sie anzuzeigen. Anhänge dieser Nachricht kann ich weder öffnen noch speichern; Thunderbird legt die Dateien zwar an, sie haben aber keinen Inhalt.

Zu solchen Problemen kann es kommen, wenn Thunderbirds lokaler Nachrichtenindex beschädigt ist. Dann listet das Programm Nachrichten auf, die es eigentlich gar nicht mehr gibt, zeigt Ihnen existierende Nachrichten nicht an oder es kommt zu anderen seltsamen Ausfällen – wie eben Anhängen, deren Inhalt nicht verfügbar ist.

Solche Indexprobleme hat Thunderbird leider ab und zu, immerhin gibt es eine eingebaute Problembehebung: Machen Sie einen Rechtsklick auf den Ordner mit der fehlerhaften Nachricht und wählen Sie im Kontextmenü den Punkt „Eigenschaften“. Das Fenster, das sich daraufhin öffnet, enthält die Schaltfläche „Reparieren“. Das veranlasst Thunderbird, sämtliche Mails des Ordners neu vom IMAP-Server abzurufen und den Index neu aufzubauen. Je nach Anzahl der Nachrichten kann das durchaus ein Weilchen dauern. Sie können das Eigenschaftenfenster aber direkt schließen und den Fortschritt in der Statusleiste des Mailers verfolgen. *(syt@ct.de)*



Thunderbird beschädigt mitunter seine Indexdateien, kann sie immerhin aber auch reparieren.

Fragen richten Sie bitte an

hotline@ct.de

c't Magazin

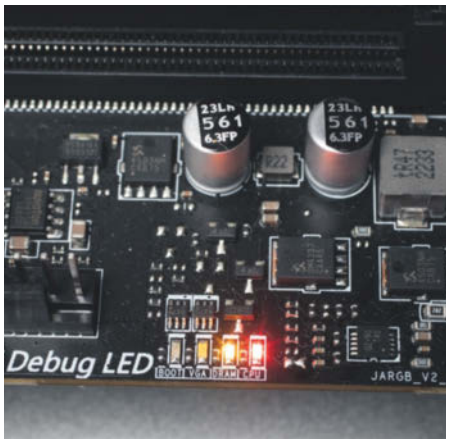
@ctmagazin

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter **www.ct.de/hotline.**

Diagnose-LEDs auf Mainboards

Mein neuer Selbstbau-PC startet nicht. Von den vier Diagnose-LEDs auf dem Board leuchtet die RAM-LED. Austausch-Arbeitsspeicher brachte jedoch keine Besserung, sondern erst ein neues Board. Warum ist das so?

Viele moderne Mainboards bringen Diagnose-LEDs mit, die bei Bootproblemen einen Hinweis auf die Ursache geben. Meist sind das vier Stück für CPU, RAM, GPU/VGA und BOOT. Allerdings können diese immer nur als Indiz für die Fehlerursache gelten, denn dahinter steckt keine ausgeklügelte Diagnosefunktion, sondern sie zeigen im Prinzip nur, an welcher Stelle der Bootvorgang hängen bleibt.



Die Diagnose-LEDs auf modernen Mainboards helfen bei der Fehlersuche, allerdings können sie auch nur Indizien liefern.

Leuchtet beispielsweise die RAM-LED dauerhaft, kann der Arbeitsspeicher defekt sein. Es ist aber ebenso möglich, dass der Prozessor ein Problem hat, denn der Speichercontroller sitzt in der CPU. Auch fehlerhafte BIOS-Einstellungen für das RAM, Fremdkörper in der CPU-Fassung oder ein defektes Mainboard verursachen diese Fehlermeldung. Eindeutiger ist es bei GPU/VGA und BOOT. Ersteres deutet auf ein Problem bei der Initialisierung der Grafikkarte oder der integrierten GPU hin. Im zweiten Fall findet das Board kein passendes Boot-Device, erkennt also beispielsweise die SSD nicht oder der Bootmodus (UEFI oder CSM) passt nicht zum Betriebssystem auf dem Systemdatenträger. *(chh@ct.de)*

MQTT Explorer und TLS

Mich treibt MQTT Explorer in den Wahnsinn: Ich habe meinen MQTT-Server per Port-Weiterleitung im Router von außen zugänglich gemacht. Per TCP-Proxy versieht ihn Traefik mit Zertifikaten von Let's Encrypt. Wenn ich im MQTT Explorer aber die Option „Validate certificate" setze, sagt das Programm „certificate has expired". Wo liegt das Problem?

Vermutlich haben Sie alles richtig gemacht: MQTT Explorer verwendet als Basis die Entwicklungsumgebung Electron, die das Schreiben lokal ausgeführter JavaScript-Programme erlaubt. Doch die verwendete Electron-Version vertraut schlicht der Zertifikatskette nicht, auf der das Zertifikat von Let's Encrypt aufbaut.

Sie können dem Programm etwas Nachhilfe geben, indem Sie mit dem Knopf „ADVANCED" in die Einstellungen für Ihre MQTT-Verbindung wechseln. Dort betätigen Sie „CERTIFICATES" und dann „SERVER CERTIFICATE (CA)". Jetzt können Sie das fehlende Zertifikat ergänzen, damit diese Verbindung Let's Encrypt vertraut – das „ISRG Root X1"-Zertifikat müssen Sie vorher herunterladen (siehe ct.de/y14x).

Dass das Problem beim MQTT Explorer liegt, können Sie bestätigen, indem Sie gesicherte Zugriffe auf Ihren MQTT-Server mit dem openssl-Befehl unixoider Betriebssysteme testen. Die Eingabe von

```
openssl s_client -connect ↵
↳<Ihr Server>:8883 -showcerts
```

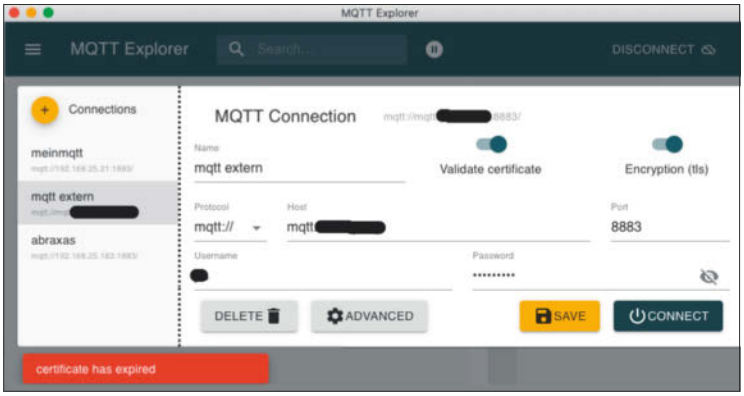
sollte Hinweise auf von Let's Encrypt ausgestellte Zertifikate bringen.

Wenn Sie nur Hinweise auf ein „TRAEFIK DEFAULT CERT" erhalten, testen Sie womöglich unter einer etwas älteren macOS-Version. Deren aus LibreSSL stammendes openssl schickt den Servernamen beim Zugriffsversuch nicht mit (kein SNI). Dann sollten Sie den Befehl zu

```
openssl s_client -connect ↵
↳<Ihr Server>:8883 -servername ↵
↳<Ihr Server> -showcerts
```

abwandeln. *(ps@ct.de)*

***Let's-Encrypt-Zertifikat:* ct.de/y14x**



Wenn MQTT Explorer meckert, dass das Zertifikat des Servers abgelaufen sei, kann das eine falsche Fährte sein.

Seite in PDF direkt aufrufen

Ich versuche vergeblich, mit dem PDF-XChange-Viewer ein PDF auf einer bestimmten Seite zu öffnen. Zwar akzeptiert er die Dateiangabe „C:\Pfad\zu\ct2322.pdf#16" zum Aufruf von Seite 16 des Dokuments, zeigt aber kein Ergebnis an. Haben Sie eine Idee, wie man das bewerkstelligen könnte?

Als Dateiangabe, die sich ohne Nennung des zuständigen Programms „einfach so" aufrufen ließe, versteht Windows so etwas wie „xyz.pdf#16" nicht. Was funktionieren müsste: den Viewer explizit aufzurufen und dessen Befehlszeilensyntax zu verwenden, um direkt eine Seite anzusteuern. Laut der Doku unter ct.de/y14x lautet die für den PDF-XChange Viewer:

```
"C:\Wo\auch\immer\PDFXCview.exe" /A ↵
↳"page=16" "C:\Pfad\zu\ct2322.pdf"
```

Die Pfade müssten Sie natürlich an Ihre Gegebenheiten anpassen; einzutragen wäre das Ganze dann in das „Ziel" einer neu erstellten Verknüpfung in Ihrem Ordner. Der Assistent zum Erstellen einer Verknüpfung fragt nach dem „Speicherort". *(hos@ct.de)*

***Dokumentation:* ct.de/y14x**

Container verwalten mit Kubernetes

Docker vereinfacht den Betrieb von Serversoftware, hat im Funktionsumfang aber Grenzen – wenn die Anforderungen steigen, wechseln viele zu Kubernetes und stehen vor neuen Fragen. Antworten auf die häufigsten von ihnen haben wir zusammengetragen.

Von Jan Mahn

Darum Kubernetes

Ich arbeite bereits länger mit Docker und habe nur eine grobe Ahnung, was Kubernetes macht. Warum braucht man Kubernetes genau?

Wenn Sie bisher mit dem Funktionsumfang von Docker zufrieden sind und nicht vorhaben, Ihre Infrastruktur zu skalieren, brauchen Sie Kubernetes wahrscheinlich nicht. Es lohnt sich immer dann, wenn Sie mit Docker-Bordmitteln nicht mehr weiterkommen. Ein typisches Beispiel: Docker kann Container mit dem Attribut `depends_on` in einer Compose-Datei nur ganz grob in der richtigen Reihenfolge starten (etwa zuerst die Datenbank, dann den Webserver). Dabei kann es mal passieren, dass eine Anwendung nach Updates ein paar Sekunden oder Minuten nicht erreichbar ist. Bei häufigen Updates und sehr anspruchsvollen Nutzern wollen Sie so etwas verhindern – Kubernetes beherrscht unter anderem sogenanntes Rolling Update, bei dem immer ein funktionierender Container bereitsteht und wirklich keine einzige Anfrage ins Leere läuft.

Anders als manchmal behauptet, braucht Kubernetes nicht zwangsläufig mehrere Server, die im Cluster laufen, sondern kann auch auf einem einzelnen Server Docker ersetzen. Im Cluster mit mehreren Maschinen spielt es seine Stärken aber so richtig aus. Während Docker die Container nur starten, stoppen und löschen kann, orchestriert Kubernetes sie. Soll heißen: Kubernetes kann entscheiden, auf welchem Server ein Container am besten läuft und wie viele identische Container gebraucht werden. Kommt ein Cluster mal an seine Grenzen, beschaffen Sie einfach weitere Hardware und erweitern den Serververbund.

Kann man nicht auch auf Docker Swarm wechseln, um mehrere Server mit Containern zu betreiben?

Docker Swarm löst ein ähnliches Problem und es ist in der Tat einfacher, die bekannte Syntax von Docker-Compose einfach weiterzuverwenden und mehrere Server als Docker-Swarm zu betreiben. Das Problem ist die etwas ungewisse Zukunft: Docker Swarm wanderte im Rahmen eines Abverkaufs zusammen mit der Enterprise-Sparte von der Docker Inc. zur Firma Mirantis. Die verdient ihr Geld überwiegend mit Dienstleistung und Produkten rund um Kubernetes und trotz aller Beteuerungen, Swarm nicht einzustellen, kann niemand garantieren, dass es Swarm in fünf Jahren noch gibt.

Kubernetes dagegen hat Google an die CNCF, eine Stiftung unter dem Dach der Linux Foundation, übergeben. Die Software ist der Branchenstandard, Open Source und auf alle Fälle zukunftssicher. Und noch ein Argument spricht für Kubernetes: Das Ökosystem ist überragend. Egal, welches Problem Sie mit Kubernetes lösen wollen – fast immer hatte schon jemand ein ähnliches und fast immer hat schon jemand ein passendes Open-Source-Projekt mit einer Lösung gebaut.

Wir nutzen bereits Docker für viele Serverdienste und denken darüber nach, auf Kubernetes umzusteigen. Wie schwierig ist das?

Technisch ist der Umstieg von Docker auf Kubernetes überschaubar. Das liegt daran, dass die Images (die zum Beispiel aus dem Docker-Hub oder anderen Registries kommen) auch von der Container-Runtime in Kubernetes genutzt werden. Es gibt also kein eigenes Kubernetes-Image-Format. Zeit investieren müssen Sie lediglich, um Docker-Compose-YAML durch Kubernetes-YAML zu ersetzen. Weil Kubernetes viel mehr Einstellmöglichkeiten kennt, werden die neuen YAML-Dateien deutlich länger und es gibt ein paar neue Konzepte zu lernen (für Volumes, Netzwerk und Konfigurationen). Einen ausführlichen Einstieg in Kubernetes für Docker-Kenner lesen Sie in [1].

Am besten lernen Sie direkt nach den ersten Gehversuchen mit Kubernetes-YAML die Syntax eines Paketmanagers wie Helm. Dann wird das Installieren und Aktualisieren von Kubernetes-Umgebungen schlagartig einfacher [2].

Kubernetes-API

Kubernetes hat ein API, funktioniert das ähnlich wie der Docker-Socket?

Das Kubernetes-API erfüllt einen ähnlichen Zweck, man kann darüber Kubernetes-Objekte anlegen und bearbeiten. Der zentrale Unterschied zur Docker-Welt: Das API kennt Authentifizierung und Autorisierung. Cluster-Admins können also genau steuern, wer welche Objekte sehen und ändern kann. Kubernetes ist damit für Umgebungen vorbereitet, in denen größere Teams an einem Cluster arbeiten und nicht jeder alles ändern darf. Dazu gehört auch, dass die meisten Objekte in sogenannten Namespaces liegen, über die man einen großen Cluster aufteilen kann.

In meinen Docker-Umgebungen nutze ich öfter den Trick, den Docker-Socket als Volume mit der Definition `/var/run/docker.sock:/var/run/docker.sock` in einen Container hereinzureichen, damit

der Container andere Container sehen und bearbeiten kann. Geht so etwas auch mit Kubernetes?

Ja, auch in Kubernetes können Container auf das Kubernetes-API zugreifen und weil es eine Berechtigungsverwaltung gibt, können Sie auch viel genauer steuern, was der Container darf – das ist also wesentlich sicherer. Viele Anwendungen aus dem Kubernetes-Ökosystem nutzen dieses Konzept auch fleißig aus. Allerdings funktioniert das Kubernetes-API völlig anders als der Docker-Socket, Sie können also nicht einfach denselben Code im Container nutzen.

Versionen und Distributionen

Kubernetes wird ja ständig weiterentwickelt und es gibt regelmäßig neue Releases. Wie wichtig ist es, immer die neueste Version im Cluster zu nutzen?

Die Versionierung orientiert sich am Konzept Semantic Versioning [3], die Versionsnummer besteht aus Major-, Minor- und Patch-Version. Die Major-Version 1 wurde seit dem ersten Release im Juli 2015 noch nicht verändert, obwohl man einige Änderungen und Abkündigungen schon als Breaking-Change einstufen könnte. Stattdessen gibt es immer drei Minor-Versionen, die parallel unterstützt und mit Patches versorgt werden. Aktuell sind das die Versionen 1.26, 1.27 und 1.28. Anders als bei Anwendungen für Endnutzer, bei denen man sich meist auf neue Features freut, muss man bei einer Infrastruktursoftware wie Kubernetes nicht sofort jede neue Minor-Version installieren. Die neuen Funktionen lösen oft sehr spezielle Probleme, die viele noch nie hatten. Im Gegenzug werden mit jeder Minor-Version lang verkündete Deprecations umgesetzt, es fallen also Dinge weg – ein Update erfordert also manchmal kleine Anpassungen an Ihren YAML-Dateien.

Zügig installieren sollten Sie aber jeweils die Patch-Versionen unterhalb Ihrer Minor-Version. Die Patches beseitigen Probleme und schließen Sicherheitslücken. Als Cluster-Admin sollten Sie sich außerdem im Kalender notieren, bis wann die verwendete Minor-Version Support bekommt, und rechtzeitig den Umstieg vorbereiten. Version 1.28 bekommt zum Beispiel noch bis zum 28. Oktober 2024 Updates, die neue Version 1.29 soll am 5. Dezember 2023 erscheinen. In der Regel dauert es vier Monate bis zur nächsten Minor-Version. Mehr Informationen zu den Terminen finden Sie über ct.de/y13s.

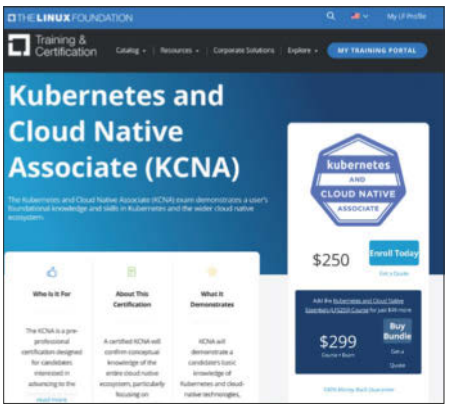
Wie Linux wird Kubernetes in Form von Distributionen angeboten. Welche sollte ich da nehmen?

Kubernetes ist eben keine einzelne Binärdatei, die man auf kubernetes.io herunterladen und installieren könnte. Zu einem Cluster gehören mehrere Komponenten, die zusammenspielen müssen. Daher gibt es Distributionen, zu denen auch eine Installationsroutine gehört. Welche Distribution Sie nutzen, hängt von der Umgebung ab. Wenn Sie Kubernetes als Komplettprodukt (Managed Kubernetes) bei einem großen Cloudprovider wie Google, Amazon oder Azure mieten, bekommen Sie die Kubernetes-Engine des jeweiligen Anbieters und müssen sich um Einrichtung und Updates gar nicht kümmern. Für eine Distribution entscheiden müssen Sie sich nur, wenn Sie den Cluster selbst auf eigener oder gemieteter Hardware (oder in gemieteten VMs) einrichten. Für kleine und mittlere Umgebungen empfehlen wir die Distribution k3s, die mittlerweile ein CNCF-Projekt ist. Damit haben Sie schnell einen Cluster eingerichtet. Für größere Umgebungen ist Rancher einen Blick wert – dazu gehört eine grafische Oberfläche im Browser, über die Sie Server einrichten und verwalten. Eine Liste mit weiteren Distributionen finden Sie über ct.de/y13s.

Qualifikation

Ich arbeite jetzt schon länger mit Kubernetes. Wie weise ich gegenüber einem potenziellen Arbeitgeber nach, dass ich von der Materie etwas verstehe?

Kubernetes-Experten sind verständlicherweise gefragt. Um die Fähigkeiten nachzuweisen, hat die Linux Foundation ein mehrteiliges Zertifizierungsprogramm entwickelt. Das Prinzip ist immer gleich: Sie bereiten sich im Heimstudium oder bei einem Schulungsanbieter auf eine Prüfung vor und absolvieren diese daheim am Computer. Dabei müssen Sie die Webcam aktivieren und einem Prüfer durch



Die Linux Foundation bietet ein Zertifizierungsprogramm für Kubernetes-Kenner an. Mit der Prüfung zum KCNA beginnt der Zertifizierungspfad.

Drehen der Webcam beweisen, dass Sie keine Spickzettel versteckt haben. Als Hilfsmittel zugelassen ist bei den meisten Prüfungen nur die offizielle Kubernetes-Doku. Geprüft wird also mehr Anwendungswissen und weniger die Fähigkeit, Dinge stumpf auswendig zu lernen.

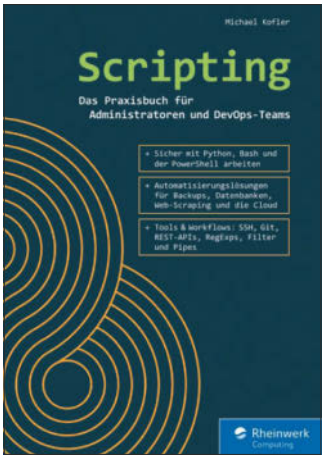
Die einfachste und mit 250 US-Dollar günstigste Prüfung ist die zum „Kubernetes and Cloud Native Associate“ (KCNA). Wesentlich anspruchsvoller ist der „Certified Kubernetes Administrator“ (CKA), der sich an Cluster-Admins richtet. Der „Certified Kubernetes Application Developer“ (CKAD) weist nach, dass er auch Anwendungen entwickeln kann, die mit dem Kubernetes-API sprechen, und dass er weiß, wie man Anwendungen am besten für den Betrieb in Containern vorbereitet. Als „Certified Kubernetes Security Specialist“ (CKS) müssen Sie die Sicherheitsfunktionen durchschauen. 400 US-Dollar für die Prüfungen und ein paar Monate Vorbereitungszeit müssen Sie einplanen. Offiziell sind die Zertifikate drei Jahre gültig.

Eine Übersicht über die Kubernetes-Zertifizierungen der Linux Foundation finden Sie über ct.de/y13s. *(jam@ct.de)*

Literatur

[1] Jan Mahn, Containerkompetenzoffensive, Auf dem Lernpfad zum Kubernetes-Kenner, Teil 1, c’t 22/2022, S. 162
[2] Jan Mahn, Containerverpacker, Kubernetes-Anwendungen mit Helm paketieren, c’t 11/2023, S. 164
[3] Jan Mahn, Bedeutung 2.0.0, Warum Versionsnummern nicht willkürlich sind, c’t 24/2021, S. 128

***Dokumentation:* ct.de/y13s**



Michael Kofler
Scripting
Das Praxisbuch für Administratoren und DevOps-Teams

Rheinwerk, Bonn 2023
(Der Buchverlag gehört wie c't zu Heise Medien.)
ISBN 978-3836294249
492 Seiten, 40 €
(PDF-/Epub-/Kindle-E-Book: gleicher Preis)

Die Finger schonen

Wer als Serveradmin und Softwarejongleur Skripte nutzt, muss weniger Tipparbeit von Hand erledigen. Michael Kofler führt umfassend ins Scripting mit Bash, Python und PowerShell ein.

Die Softwarewelt kennt viele Werkzeuge zum Automatisieren von Abläufen. Kofler, seit Jahrzehnten Linux-Experte und fleißiger Kompendienschreiber, hat sich die Bash-Shell, die Programmiersprache Python und die Microsoft-Skriptsprache PowerShell vorgenommen. Gemeinsam decken die drei Werkzeuge ein großes Spektrum an Betriebssystemen und Anwendungsfällen ab.

Zunächst machen ein paar Beispielskripte Lust auf mehr. So motiviert lernt der Leser in knapp gehaltenen Kapiteln die wichtigsten Eigenschaften des Werkzeugtrios kennen und freut sich über die Erkenntnis, dass die meisten Automatisierungsaufgaben nur wenig Aufwand erfordern. Ebenso wichtig wie Strukturen und Eigenheiten der Sprachen sind die Umgebungen, in denen das Scripting stattfindet. So rufen Bash-Skripte zahlreiche Linux-Kommandos auf, die zu kennen sich lohnt, während die PowerShell auf Hunderte von CmdLets zurückgreift. Kofler stellt die wichtigsten Befehle kurz vor; auf Techniken wie Pipes und reguläre Ausdrücke geht er detailliert ein. Ferner erklärt er, wie Skripte automatisch starten, zeitgesteuert mittels Cron oder mit dem Windows Task Manager. Eher übergeordnete Abschnitte erläutern die Verarbeitung von XML- und JSON-Dateien sowie den ferngesteuerten Zugang per SSH.

Viel Beispielcode zu alltäglichen Aufgaben für Serverbetreuer und Webschaffende bevölkert das letzte Drittel des Buchs. Manche der Skripte fertigen Backups an, andere manipulieren Bilder oder werten mithilfe von Web Scraping Webseiten aus. Etwas für Fortgeschrittene sind die Beispiele, die REST-Schnittstellen abfragen oder auf Datenbanken zugreifen. Selbst ein Kapitel über die Verwendung von Clouddiensten wie Amazon S3 fehlt nicht. Zudem führt Kofler vor, wie man Docker für Skriptanwendungen einsetzt. Dabei setzt er Docker- und AWS-Kenntnisse voraus.

Bisweilen schießt der Autor ein wenig über sein Thema hinaus; die kurzen Kapitel über Visual Studio Code und Git wären nicht unbedingt nötig gewesen. Aber das ist Meckern auf sehr, sehr hohem Niveau. Jedenfalls befähigt und reizt das Buch jeden mit nur etwas Programmiererfahrung dazu, sich hilfreiche Skripte für den eigenen Bedarf maßzuschneidern. *(psz@ct.de)*

Digitales Rebellendorf

Das Internet ist fest in der Hand der Hightech-Giganten: Google, Facebook, Amazon und wie sie alle heißen. Aber in einem kleinen gallischen Dorf gibt es freies WLAN, freie Software, eine freie Enzyklopädie und Datenschutz.

„Der Kampf um das Internet" ist vielleicht ein etwas zu martialischer Titel und was Mey als „digitale Gegenwelt" bezeichnet, hat nicht wirklich Aussicht darauf, einen Kampf gegen Google, Facebook und Konsorten zu gewinnen. Der nichtkommerzielle Firefox-Browser etwa rangiert nach Nutzerzahlen weit abgeschlagen hinter Chrome und Edge, aber er ist ein wichtiger Baustein im Anonymisierungsprojekt Tor. Die Wikipedia konkurriert nicht mit Google, Facebook oder Microsoft, sondern ist eine Instanz, die es schafft, sich unabhängig von den großen IT-Konzernen aus Spenden zu finanzieren.

Wie kommt es eigentlich, dass ein komplettes Office-Paket wie LibreOffice kostenlos verfügbar ist, während man das Pendant von Microsoft teuer bezahlen muss? Wie entsteht ein komplett freies Betriebssystem, wovon leben die Entwickler? Auf solche Fragen hat Mey Antworten. Es stellt sich heraus, dass die verschiedenen großen Open-Source-Projekte höchst unterschiedliche Organisationsstrukturen und Finanzierungsmodelle haben.

Der größte Geldgeber des Anonymisierungsprojekts Tor ist ausgerechnet das US-Außenministerium, das bei der Förderung von Anti-Zensur-Technologie in Kauf nimmt, dass die US-Geheimdienste außen vor bleiben. Als größter Geldgeber des Firefox-Projekts, das sich den Datenschutz auf die Fahnen geschrieben hat, stellt sich Google heraus. Der Konzern zahlt Hunderte von Dollarmillionen im Jahr dafür, die Standard-Suchmaschine in Firefox zu sein – und bekommt so in der Voreinstellung jeden Buchstaben übermittelt, den Nutzer bis zum ersten Punkt in die Adresszeile eingeben. Dies sind nur zwei Beispiele für Aha-Erlebnisse aus Meys Streifzug durch die „digitale Gegenwelt".

Mey schreibt allgemeinverständlich und bemüht sich, Dinge wie den Unterschied zwischen Quellcode und ausführbaren Binaries für IT-Laien zu erklären. IT-Experten dürften bei manchen Verallgemeinerungen zusammenzucken (Linus Torvalds ist nur einer der beiden Väter von Linux? Na ja, wenn man GNU/Linux meint, sollte man Richard Stallman mitzählen). Doch auch IT-Kenner dürften aus diesem Buch so manches Neue lernen – schließlich denken technisch orientierte IT-ler eher selten über Organisationsstrukturen, Finanzierungsmodelle und die Welt der Open-Source-Lizenzen nach. *(Dr. Harald Bögeholz/dwi@ct.de)*

Stefan Mey
Der Kampf um das Internet
Wie Wikipedia, Mastodon und Co. die Tech-Giganten herausfordern

C.H.Beck, München 2023
ISBN 978-3406807220
236 Seiten, 18 €
(Epub-/Kindle-E-Book: 13 €)

EXKLUSIVE PARADIESE

VON GERD SCHMIDINGER

Wie in Trance verließ Ronja ein letztes Mal ihren Arbeitsplatz. Fünfundzwanzig Jahre hatte sie dort verbracht, fünf Tage die Woche, im Kindergarten „Rappelkiste“.

Sie hatte ihre Arbeit mit Leidenschaft verrichtet und mit Mühe. Die anfängliche Begeisterung wurde zu einem ruhig dahin strömenden Fluss, den in den letzten Jahren die Mühe schleichend zuschüttete. Die Kinder waren noch immer erfrischend und voller Zauber – aber irgendwie zunehmend beladen von den Nöten der Erwachsenen. Oder war es normal, dass sich Fünfjährige darum sorgten, ob sie noch gebraucht würden in einer vollkommen technisierten Welt? Dabei verstand sie sie ja, die Kleinen: Sie selbst hätte ja ebenfalls keinen anderen Job mehr gefunden. „Etwas mit Menschen“, das war das Einzige, was übrigblieb, außer den Jobs als System-Administratorin oder KI-Spezialistin. Etwas mit Menschen. Es hatte mal eine Zeit gegeben, als Menschen noch freiwillig Zeit miteinander verbrachten, nicht nur, wenn sie dafür bezahlt wurden.

Wieso fiel ihr der Abschied so schwer? Hinter ihr schloss sich die bunte Kindergartentür mit einem sanften Surren. Ein letztes Mal. Ronja schüttelte sich. Es war gut. Es würde gut werden. „Hol mir einen Wagen“, sprach sie zu ihrem Handgelenk hin. Der Connector flötete sanft sein übliches „Gerne“. Ronja blickte die Straße hinunter. Spürte ein flaues Gefühl im Magen. Vorfreude? Angst? Eines der Taxis hielt. Ein Wayfair Walhalla. Dunkel, nobel, die Sitze mit Leder aus Tissue Engineering bezogen. Ronja nahm rechts vorne Platz. „Zur Entsorgungszentrale“, sagte sie. Das Auto fuhr mit einem sanften Ruck los. „Ein Minzbonbon?“, fragte eine gediegene männliche Stimme. Warum immer Minze? Ronja nickte, nahm vom ausgefahrenen Tablett das runde Ding entgegen und steckte es sich in den Mund. Sie ärgerte sich. Schon wieder überrumpelt. Eigentlich hätte sie lieber etwas zu trinken gehabt, aber jetzt lutschte sie schon an dem Bonbon mit dem beißenden Geschmack. Egal, sagte sie sich, reg dich nicht auf, es ist der erste Tag deines neuen Lebens. In Rente. Einer ordentlichen Rente; sie hatte sich gewundert, dass es so viel war. Und sie würde ihre Zeit nicht allein verbringen. Sie hatten es sogar hingekriegt, dass sie am selben Tag gemeinsam Abschied vom Berufsleben nehmen konnten. Sie und Bernd. Sie würde mit ihm die Welt bereisen, faulenzen, aber auch wandern, lesen, lachen. Ins Theater gehen. Ihr Herz pochte schneller. Wie lange waren sie nicht mehr im Theater gewesen! Für all das war jetzt Zeit.

Der Tod hat seinen Schrecken verloren: Dank einer geeigneten Schnittstelle kann sich das Bewusstsein im Sterbefall rechtzeitig davonmachen, um in digitalen Seelen-Themenparks weiterzuleben. Und wer wäre besser geeignet dazu, deren Server zu betreiben, als clevere und verantwortungsbewusste Versicherungsunternehmen?

Ob er schon vor der Entsorgungszentrale wartete? Sie hatten gleichzeitig Feierabend und die Zentrale, wo er die vergangenen dreizehn Jahre gearbeitet hatte, lag am anderen Ende der Stadt. Aber auf die paar Minuten kam es nun auch nicht mehr an. Ein Bild schob sich in ihren Gedanken vor die vorüber gleitenden Hausfassaden: ihre Mutter und ihr Vater! Einträchtig saßen sie auf der Couch, die sanften Finger ihrer Mutter in den schwieligen ihres Vaters. Vertrauensvoll, voller Liebe. Ihre Eltern würden noch ein wenig warten müssen.

Ein Gedanke traf Ronja schmerzhaft wie ein Stich: Auch ihre Eltern hatten sich auf die Rente gefreut. Auch sie wollten die Zeit im Ruhestand zusammen verbringen. Doch dann … Damals war die Technologie der selbstfahrenden Autos noch relativ neu – und offenbar unausgereift. Wie hätten sie es auch wissen können, dass ausgerechnet am ersten Tag ihres neuen Lebens die Sensortechnik versagen würde? Nur ein Glück, dass Zheng Bao die Neuronen-Platinenschnittstelle schon erfunden hatte. Ronja würde ihre Eltern wiedersehen. Nicht so bald, hoffte sie jedenfalls.

DAMALS WAR DIE TECHNOLOGIE DER SELBSTFAHRENDEN AUTOS NOCH RELATIV NEU.

Aber irgendwann, nach vielen Jahren eines genussvollen Rentnerlebens, würde sie sie wiedersehen – in einem der exklusiven Paradiese. Nein, nicht in irgendeinem: im PFP, dem Paradies für Paare, dort, wo es die meisten ihrer Bekannten hinzog nach dem Tod.

Bild: KI Midjourney | Bearbeitung c't

Erinnerungen zeichneten ein sanftes Grinsen auf Ronjas Lippen. Papa hatte Mama gerne damit aufgezogen, dass er doch lieber einen Vertrag mit „1001 Nacht“ gemacht hätte. Papa spielte manchmal den Schwerenöter und Mama tat ihm zuliebe so, als würde sie das ärgern. Einmal hatte sie versucht, den Spieß umzudrehen, und damit gedroht, sich bei „Femina“ anzumelden. Doch Papa war ganz verunsichert gewesen; so hatte sie ihn noch nie gesehen. Ob er ihr nicht genüge? Ob er ihr zu alt geworden sei? Ob sie lieber einen knackigen jungen Mann haben würde? Ronja war schließlich aus dem Zimmer gegangen: Es war ihr peinlich, worüber ihre Eltern vor ihr sprachen. Dabei war für jeden Außenstehenden klar gewesen, dass die beiden einander abgöttisch liebten. Und nun waren sie tot – jedenfalls ihre Körper.

Irgendwie wirkte die Geist-Computer-Transformation immer noch wie Magie. Ewiges Leben! Der große Traum der Menschheit war Wirklichkeit geworden. Einzige Grundvoraussetzung war, dass man den Körper rechtzeitig fand. Bis zu einer halben Stunde nach dem Ableben konnte man die Transformation noch durchführen, danach war es zu spät. Deshalb war es ja auch Pflicht, den Connector stets am Handgelenk zu tragen. Das Gerät spürte sofort, wenn etwas nicht stimmte, und alarmierte die Ewigkeitsversicherung, für die der Träger sich beizeiten entschieden hatte.

Wieder erschien vor ihrem inneren Auge das Bild ihrer Eltern. Glücklich, in sich ruhend. Anders als sie und Bernd. Sie und ihr Mann funktionierten gut, aber da war auch immer wieder Trennendes zwischen ihnen, ein Abgrund. Ganz schlimm war es gewesen, als es um die Wahl des Paradieses gegangen war. Bernd hatte darauf bestanden, den Preußischen Himmel zu wählen. Nicht, weil er es selbst wollte, sondern wegen seiner Eltern. Sie konnte das ja ein wenig verstehen – auch sie wollte ihre Eltern wiedersehen. Aber mit seinen Eltern hatte sich Bernd nie verstanden. Und dann die Ewigkeit mit ihnen verbringen wollen? In einem Paradies voller Pickelhaubenträger, Kaiserverehrer und Reichsbürger? In einer Ewigkeit, in der man zur Militärparade ging statt auf den Rummelplatz? Sie hatten wochenlang gestritten, bis er schließlich zugegeben hatte, dass er Angst vor seiner Mutter hatte. Dass er nicht wusste, wie er ihr beibringen sollte, dass sie das PFP gewählt hatten. Er hatte sich schließlich in Ermangelung von Argumenten breit schlagen lassen. Und mittlerweile wirkte er ganz glücklich mit seiner Entscheidung. Das PFP war das mit Abstand am besten ausgereifte Paradies. Weitläufig, voller Menschen, aber auch mit der größten und spektakulärsten Welt voller Gebirge, Wälder und Schluchten. Und Stränden am türkisfarbenen Meer. Alles gab es da, was es auf der Erde auch gab, und noch viel mehr. Sogar Pickelhauben, wenn man denn unbedingt eine wollte.

* * *

Bernd stand schon am Straßenrand. Lächelte, als er erkannte, wer aus dem Walhalla stieg. Küsste Ronja so leidenschaftlich auf den Mund, dass ihre Brille unangenehm gegen ihre Augenhöhlen drückte. Dennoch fühlte es sich gut an, altbekannt und doch neu, freier, wie ein Vorbote von Abenteuern. Ronjas Blick ruhte etwas länger auf Bernds blassblauen Augen. Schließlich wandte er sich ab und öffnete die linke Vordertür. Fahrertür hieß das früher. Lustig, wie sich die Dinge änderten. Als Ronja neben ihm saß, begann Bernd auf das Armaturenbrett zu trommeln. Irgendwie hätte es Ronja jetzt schön gefunden, wenn er sie gefahren hätte. Wie damals, vor fast einem halben Jahrhundert, als er sie mitgenommen hatte zur Dorfdisco. Ein unsicherer Macho-Depp. Aber völlig vernarrt in sie, das hatte sie überzeugt. Erst spät hatte sie herausgefunden, wie sehr er unter dem strengen Regiment seiner Eltern litt. Wie sensibel er dann doch war.

DAS GERÄT SPÜRTE SOFORT, WENN ETWAS NICHT STIMMTE, UND ALARMIERTE DIE EWIGKEITSVERSICHERUNG.

„Wohin willst du fahren?“, fragte Bernd und lächelte. Ronja legte eine Hand auf sein Knie. „Lass uns in den Wald fahren, du weißt schon, zum Wanderparkplatz. Und dann zu unserer Lichtung spazieren.“ Ein schelmisches Grinsen erschien auf Bernds Gesicht. Er wusste genauso gut wie sie, was sie auf dieser Lichtung getrieben hatten. Damals, in den frühen Jahren ihrer Beziehung. „Zum Wanderparkplatz Erlenbach“, sagte Bernd schließlich verträumt. Das Auto fuhr an, reihte sich in den Verkehr ein. Trug sie sanft hinaus aus der Stadt. Da vorne war schon die Teufelsschlucht. Da waren früher, als man noch selbst fuhr, immer wieder Betrunkene heruntergestürzt. Von der Straße aus ging es dort mindestens hundert Meter nach unten. Ronja schauderte. Die Leitplanke war immer noch nicht repariert. Komisch, nach all den Jahren. Was war jetzt los? Ronja fühlte sich mit aller Macht in den Sitz gepresst. Wieso gab der Walhalla Gas? Ihr Herz war ein einziges Pochen. Bevor sie über die Reste der Leitplanke in die Tiefe fiel, blickte sie ein letztes Mal in die blassblauen Augen Bernds.

* * *

Ronja hob den Kopf, blickte an sich hinab. Eindeutig. Sie lag auf einem mit blauer Satinwäsche bezogenen Bett und sie war nackt. Sie fühlte sich eigenartig. Als kribbelte ihr ganzer Körper. Moment! Das war doch nicht ihr Körper! Oder doch? Reine, straffe Haut, kaum Leberflecken – und diese Brüste, die sie kaum sehen konnte, weil sie so nahe waren! Doch nein, ein kurzes Fokussieren ihrer Augen genügte, und schon sah sie auch aus allernächster Nähe ganz scharf. Sie fuhr sich mit der Hand über den Kopf. Keine Brille. Augen wie ein Luchs.

Ein flaues Gefühl schlich sich in ihren Magen. Es gab nur eine Erklärung: Sie war tot, zerschellt am Grund der Teufelsschlucht. Zusammen mit Bernd. Bernd! Sie blickte um sich.

Wo war er nur? Erst jetzt wurde Ronja bewusst, was sie neben ihrem offenbar besonders aufregend verjüngten Körper schon die ganze Zeit wahrgenommen hatte: Sie befand sich auf einem von einem blauen Baldachin beschirmten Himmelbett, inmitten eines großzügigen Schlafzimmers. Einzelne Schmucksteine zierten die ockerfarbenen Wände. Eine Glasfront mit Schiebetür führte auf eine mit Sandsteinplatten ausgelegte Terrasse, und dahinter befand sich – ein Pool! Nicht bloß irgendeiner, sondern ein Infinity-Pool, dessen helle, lichtdurchflutete Wasser in jene des tiefblauen Meeres überzugehen schienen.

Ronja richtete sich kerzengerade im Bett auf. Irgendetwas war hier falsch. Sie hatten das Haus am Ufer des Meeres gebucht, ja, aber keinen Pool! Sie sprang aus dem Bett. Fast wäre sie hingefallen, so kraftvoll federten ihre Beine. Was für ein Körper! Als sie auf die Terrasse trat, erstaunten sie die Dimensionen des Grundstücks. Hatten sie so einen großen Garten gebucht? Neben dem Pool breitete sich eine mediterrane Gartenlandschaft aus, mit Zitronenbäumen, Zypressen, einem Springbrunnen und Bänkchen zum Verweilen. Ronja zog die Luft tief in ihre Lungen ein. Sie konnte ihn förmlich schmecken, den Süden. Doch dieses Grundstück und dieses Haus waren eindeutig eine Nummer zu groß. So etwas hätten ihre Versicherungsbeiträge nicht hergegeben.

Zögernd ging sie zurück ins Schlafzimmer, doch selbst zögerliche Schritte machten Spaß. Sie ließ ihren Blick schweifen. Neben dem Schrank stand ein Hocker und auf dem Hocker lag ein Connector. Natürlich, den gab es hier auch, schließlich war das Jenseits dem Diesseits nachempfunden, nur einen Hauch perfekter. Sie legte das Gerät um ihr linkes Handgelenk und sagte: „Bin ich im richtigen Haus?“

„Ja“, flötete die sanfte Stimme aus dem Connector. „Sie haben ein Upgrade bekommen. Automated Motion bittet um Entschuldigung für die Unannehmlichkeiten bei Ihrer letzten Fahrt. Zur Wiedergutmachung übernimmt die Firma die Kosten des Upgrades. Dieses gilt zeitlich unbegrenzt.“ Ronja wusste nicht, was sie sagen sollte. Einerseits war „Unannehmlichkeit“ wohl kaum der passende Ausdruck für ihre Todesfahrt – andererseits war so ein Upgrade für die Ewigkeit auch nicht zu verachten. Mehr würde sie gegen ein Unternehmen wie Automated Motion sowieso nicht herausschlagen.

„DU HAST EIN UPGRADE BEKOMMEN.“

„Wo ist Bernd?“, fragte Ronja und schämte sich ein wenig, dass sie diese Frage erst jetzt stellte.

„Ihr Ehemann hat ebenfalls ein Upgrade bekommen. Automated Motion möchte Ihnen aufrichtig das Bedauern dafür aussprechen, dass Sie Ihre Rente nicht gemeinsam genießen können.“

„Ja, aber wo ist er? Wir haben dieses Haus zusammen gebucht. Zeitlich unbegrenzt.“

„Das ist korrekt. Ihr Mann hat allerdings eine andere Ewigkeitsversicherung abgeschlossen.“ Ronja wurde schwarz vor Augen. „Was hat mein Mann?“, flüsterte sie mehr zu sich selbst als zum Connector.

„Er hat eine Versicherung mit PH, dem Preußischen Himmel, abgeschlossen.“

Scham, Trauer, roter Zorn. Und das alles in einem jungen, perfekt funktionierenden Körper. Ronja hatte das Gefühl, zu zerplatzen. Während sie in einem gelben Kleid, das sie sich ohne nachzudenken aus dem Schrank geschnappt hatte, am Meer entlangstapfte, den Sand unter ihren kraftvollen Füßen, erwürgte sie in Gedanken abwechselnd Bernds Mutter und ihn selbst. Aber das brachte nichts, sie konnte es ja nicht wirklich tun. Verträge mit unterschiedlichen Firmen trennten sie für immer. Für ewig. Keine Möglichkeit der Aussprache mehr, keine Möglichkeit, ihn zu beschimpfen, ihm Teller nachzuwerfen. Er würde es nicht einmal erfahren, wenn sie sich mit einem anderen Mann einließ. Nach schier endlosem wütendem Stapfen kam ihr ein Gedanke, der sie nicht mehr losließ: Wo waren ihre Eltern? Und wie um alles in der Welt war es möglich, dass sowohl sie als auch ihre Eltern am Tag ihres Rentenbeginns einem Autounfall zum Opfer gefallen waren? Sie blieb stehen, sprach zu ihrem Connector hin: „Wo sind Peter und Johanna Schwarz?“ Der Connector antwortete ohne Umschweife: „Das ist eine gesperrte Information.“

* * *

Ronja blinzelte. Sie war nun schon einen Monat tot. Neben ihr krause Locken. Ein Adonis auf zerwühlten Laken. Verzweifelte, wütende Ekstase gestern Nacht. Wieder einmal. Sie wusste gar nicht, der Wievielte das war. Es hatte sie nur kurz verwundert, wie bereitwillig die Männer mit ihr ins Bett gingen. Dabei war es gar nicht so unlogisch: Viele Paare sahen das Jenseits als einen Neuanfang, mit Bereitschaft zu Toleranz. Oder sie trennten sich angesichts der Vorstellung, eine Ewigkeit miteinander verbringen zu müssen. Ronja schälte sich vorsichtig aus den Laken, warf leise ihr schwarzes Kleid über. Sie schickte sich gerade an, im Storchengang zur Tür zu staksen, da fühlte sie seinen Blick auf sich ruhen. „Jetzt weiß ich, woher ich dich kenne“, sagte die tiefe, männliche Stimme, und schon wieder perlte sie ihren Rücken hinunter und hinterließ eine Gänsehaut. Sie drehte sich um, starrte in das von aufregenden Kieferknochen begrenzte Gesicht: „Woher?“ Mit einer anmutigen Bewegung setzte sich der junge Mann auf. Und klopfte neben sich aufs Bett. „Deine Eltern heißen Peter und Johanna, nicht wahr?“ Ronja ging wieder aufs Bett zu, fläzte sich hin, ihren Liebhaber interessiert fixierend. Wie hieß er doch gleich? Robert – oder Rolf? „Woher kennst du meine Eltern?“, fragte sie, und ihr Herz machte einen Sprung. Wusste dieser Mann etwas über sie?

Der junge Mann deutete mit ausgebreiteten Armen auf sich selbst und grinste: „Ich bin’s, Onkel Rolf!“ Ronja war es plötzlich, als schrillten tausend Alarmglocken. Onkel? Das war so falsch, so unendlich falsch – aber halt, sie hatte doch gar keinen Onkel namens Rolf! Rolf schien ihre Panik bemerkt zu haben; sein selbstsicheres Grinsen war angestrengter Sorge gewichen. „Kein wirklicher Onkel, keine Angst.

Über den Autor

Bild: Gerd Schmidinger

Gerd Schmidinger, im österreichischen Feldkirch geboren, lebt heute in Heilbronn. Seit seiner Jugend ist er ein begeisterter Schreiber. Von seinen zahlreichen Kurzgeschichten sind einige als kleine E-Books erschienen: Als Lesetipp sei hier seine „Hiobsbotschaft“ von 2015 genannt (ISBN 978-3945069110), die für rund 2,50 Euro im Handel ist. Für seinen ersten Science-Fiction-Roman sucht er derzeit noch nach einem Verlag. Als Lehrer schlägt Schmidinger sich mit den digitalen Medien im Schulkontext herum – gesellschaftliche Auswirkungen etwa von Robotik und KI sieht er durchaus ambivalent: „Unsere Gesellschaft erhofft sich durch Digitalisierung etwas wie Erlösung vom eigenen Denken. Und das ist etwas, was noch nie gut gegangen ist.“

Aber du hast mich immer Onkel Rolf genannt, früher.“ Ein weißhaariger Mann mit wucherndem Bart, ein alter Freund ihrer Eltern, deutlich älter als sie selbst. War er nicht Versicherungsvertreter gewesen? Sie brachte das Bild von Onkel Rolf nicht mit jenem Gott in Menschengestalt zusammen, der da neben ihr hockte. War das möglich? Onkel Rolf hatte sie noch vor ein paar Stunden in den Wahnsinn … Nein, halt! Ihr war, als räusperte sich ihr Über-Ich. Reiß dich zusammen. Denk nicht zu genau über alles nach. Sonst kapierst du noch, was das für ein kranker Scheiß ist.

„Wo sind meine Eltern?“, fragte Ronja. „Ich konnte sie bisher nicht finden.“ Onkel Rolf blickte zur Seite. „Ich habe vor einiger Zeit den Kontakt zu ihnen verloren.“ Er streifte ihren Blick. Andere Seite. Sie folgte seinem Blick hinaus aufs Meer. Irgendwie lebten hier alle am Meer. Wie war das überhaupt möglich?

„Aber du weißt doch sicher, wie ich sie finden kann“, sagte Ronja. Rolf fixierte sie, schien nachzudenken. Seufzte. „Deine Eltern sind gestorben.“ Irres Lachen. Es stoppte erst, als Ronja merkte, dass es von ihr selbst kam.

„Gestorben? Wir sind alle gestorben. Das ist der Witz bei der ganzen Sache.“ Sanft legte Rolf seine Hand auf ihren Arm. „Man kann noch einmal sterben. Und dann ist man wirklich tot. Dann wird das Persönlichkeitsprofil gelöscht. Ein für alle Mal.“

„Aber da gibt es doch Backups. Eine Garantie. Es gibt doch Leute, die springen ohne Fallschirm aus dem Flugzeug und stehen nach dem Aufprall einfach wieder auf.“

„Sie stehen nicht mehr auf, wenn sie es nicht wollen. Man kriegt eine Frage gestellt: Willst du deinen Avatar wieder aktivieren oder soll er unwiderruflich gelöscht werden? Diese Frage bekommt jeder gestellt, der im PFP stirbt. Und manche entscheiden sich für die Auslöschung.“

„Aber meine Eltern? Wieso sollten sie das tun?“ Rolf zuckte die Schultern. Und dabei blickte er ihr nicht in die Augen.

Das Gespräch mit Rolf ging Ronja nicht aus dem Kopf. Sie war sich sicher, dass er ihr nicht alles erzählt hatte. Wieso hatte er ihr überhaupt etwas erzählt? Sie musste herausfinden, was wirklich mit ihren Eltern geschehen war. Ihre Eltern und Selbstmord – das konnte sie sich einfach nicht vorstellen. Sie hatten hier alles, ihre alte Liebe und junge Körper, ein Leben in Reichtum und Überfluss, Meer und Berge und Stadt und Vergnügen – warum in aller Welt brachte man sich da um? Ronja verstand es nicht. Sie hatte Bernd verloren, sie hatte einen Grund, zu verzweifeln – aber sich deshalb umbringen?

Zu Hause angekommen – es reichte ein kleiner Befehl an den Connector, da wurde sie an ihren Pool gebeamt – schlenderte sie ein wenig zwischen den Zitronenbäumen herum. Dann fragte sie: „Wann haben Peter und Johanna Schwarz Selbstmord begangen?“

„Das ist eine gesperrte Information.“

„Aber es stimmt? Sie haben Selbstmord begangen?“

„Das ist eine gesperrte Information.“

So kam sie nicht weiter. „Wie viele Leute haben im PFP schon Selbstmord begangen?“

„Das ist eine gesperrte Information.“

„ABER DA GIBT ES DOCH BACKUPS. EINE GARANTIE.“

Ronja blickte hinaus, dahin, wo das Türkis des Meeres ins tiefe Blau des Himmels überging. Möwen schaukelten auf dem Wasser. War das echte Meer jemals so schön gewesen? Es benötigte gewiss Unmengen von Strom, die künstlichen Paradiese zu erschaffen. Dieser Detailreichtum, diese Farben! Und in jedem Augenblick kamen neue Menschen dazu, immer mehr, ohne Unterlass. Woher kam die ganze Energie? Ronja fröstelte, trotz der sommerlichen Temperaturen.

„Wie viele Menschen leben im Paradies für Paare?“, stieß sie schließlich krächzend hervor.

„Insgesamt zweihundert Millionen.“

Ronja schüttelte sich. „Wie viele Bewohner gab es vor fünf Jahren?“

„Zweihundert Millionen.“

„Und vor zehn Jahren?“

„Zweihundert Millionen.“

Das Geschrei der Möwen klang plötzlich wie Hilfeschreie. Hilfeschreie sterbender Menschen. So vieler sterbender Menschen.

(psz@ct.de) c't

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**).

ORACLE Feuerwehr www.oraservices.de G

softaktiv.datensysteme Datenbankapplikationen, Website Boosting, Online-Pressemitteilungen, Unterstützung bei Ihren V-Projekten. Einfach anrufen, Faxen oder eine E-Mail schicken. Telefon: 0511/3884511, Mobil: 0170/3210024, Telefax: 0511/3884512, E-Mail: service@softaktiv.de, Internet: www.softaktiv.de G

nginx-Webhosting: **timmehosting.de** G

www.patchkabel.de - LWL und Netzwerk Kabel G

xxs-kurze Daten- & Netzkabel: kurze-kabel.de G

EDELSTAHL LED SCHILDER: www.3D-buchstabe.com
HAUSNUMMERN nobel 230V~: www.3D-hausnummer.de G

Erfahrene Diplom-Fachübersetzerin übersetzt EDV-Texte aller Art (Software und Hardware) insbesondere Texte aus den Bereichen Telekommunikation und Netzwerke. Englisch-Deutsch. Tel. + Fax: 05130/37085 G

www.embedded-specialists.de G

Delphi Legacy: Sie haben Mission-critical Anwendungen in einer alten Delphi-Version? Update, Datenexport, Migration nach C#, www.cordes-dev.de/delphi G

Anzeigenschluss für die nächsten erreichbaren Ausgaben:
28/2023: 14.11.2023
29/2023: 28.11.2023
01/2024: 08.12.2023

c't – Kleinanzeigen

Private Kleinanzeige:
erste Druckzeile € 10,– ; jede weitere Zeile € 8,–

Gewerbliche Kleinanzeige:
erste Druckzeile € 20,–; jede weitere Zeile € 16,–

Chiffre-Anzeige: € 5,– Gebühr

Hinweis: Die Rechnungsstellung erfolgt nach Veröffentlichung der Anzeige!

Name/Vorname

Firma

Str./Nr.

PLZ/Ort

Bitte veröffentlichen Sie den Text in der nächsterreichbaren Ausgabe von c't.

○ Den Betrag habe ich auf Ihr Konto überwiesen.
Sparkasse Hannover,
IBAN DE98 2505 0180 0000 0199 68, BIC SPKH DE 2H

Bei Angeboten: Ich versichere, dass ich alle Rechte an den angebotenen Sachen besitze.

Datum Unterschrift (unter 18, der Erziehungsberechtigte)

Faxnummer: 05 11 / 53 52-200
eMail: dispo@heise.de

Bitte veröffentlichen Sie in der nächsterreichbaren Ausgabe (Vorlaufzeit mind. 3 Wochen) folgende Anzeige im Fließsatz ○ privat ○ gewerblich* (werden in c't mit G gekennzeichnet) ○ Chiffre

€ 10,– (20,–)
€ 18,– (36,–)
€ 26,– (52,–)
€ 34,– (68,–)
€ 42,– (84,–)
€ 50,– (100,–)
€ 58,– (116,–)
€ 66,– (132,–)

Pro Zeile bitte jeweils 45 Buchstaben einschließlich Satzzeichen und Wortzwischenräumen. Wörter, die **fettgedruckt** (nur in der ersten Zeile möglich) erscheinen sollen, unterstreichen Sie bitte. Den genauen Preis können Sie so selbst ablesen. * Der Preis für gewerbliche Kleinanzeigen ist in Klammern angegeben. Soll die Anzeige unter einer Chiffre-Nummer erscheinen, so erhöht sich der Endpreis um € 5,– Chiffre-Gebühr.

Ausfüllen und einsenden an: **Heise Medien GmbH & Co. KG**
c't-Magazin, Anzeigenabteilung
Karl-Wiechert-Allee 10, 30625 Hannover

↳ Weiterlesen, wo andere aufhören.

heise medien

Nachrichtenredakteur (m/w/d)

IT- und Technik sind deine Leidenschaft, Neuigkeiten hast du stets im Blick und dazu schreibst du gerne? Dann gestalte als News-Redakteur (m/w/d) die Zukunft des Nachrichtengeschäfts beim renommiertesten deutschsprachigen IT-Portal heise online mit.

Deine Aufgaben

- Für heise online recherchierst und schreibst du zu Technik- und IT-Themen.
- Zudem betreust und steuerst du die Startseite von heise online.
- Im Idealfall hast du eine Affinität zu Videos und Podcasts, an denen du gerne als Host oder Gast teilnimmst.
- Durch dein Interesse und deine Neugier saugst du alle Informationen der IT-Branche auf.

Deine Benefits

- Dein Windows- oder Mac-Notebook wählst du selbst aus, du hast flexible Arbeitszeiten und die Möglichkeit, mobil zu arbeiten.
- Natürlich bekommst du kostenlosen Zugang zu sämtlichen Heise-Produkten inklusive der heise Academy.
- Beim Digital Detox helfen dir unser Mitarbeiter-Fitnessprogramm Hansefit, die Kaffee- und Wasser-Flat, unsere großartige Kantine mit kostenlosem Mittagessen und unsere regelmäßigen Mitarbeiter-Events.

Deine Ansprechpartnerin
Rebecca Klatt,
Personalreferentin
Tel.: 0511 5352-108

Bitte bewirb dich online: **karriere.heise.de**
Bei uns ist jede Person, unabhängig des Geschlechts, der Nationalität oder der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters sowie der sexuellen Identität willkommen.

Wir freuen uns auf deine Bewerbung!

mainova

Arbeiten bei Mainova – Da steckt mehr dahinter!

Zuverlässige Energie für Ihre IT-Karriere

Jetzt bewerben
mainova.de/karriere

Inserenten*

Stellenanzeigen

Veranstaltungen

Ein Teil dieser Ausgabe enthält Beilagen der EWE AG, Oldenburg.

** Die hier abgedruckten Seitenzahlen sind nicht verbindlich. Redaktionelle Gründe können Änderungen erforderlich machen.*

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: „Hacking-Projekte mit dem Raspi": Ronald Eikenberg *(rei@ct.de)*,„NAS-Geräte aufrüsten": Dušan Živadinović *(dz@ct.de)*

Chefredakteur: Torsten Beeck *(tbe@ct.de)* (verantwortlich für den Textteil)

Stellv. Chefredakteur: Axel Kossel *(ad@ct.de)*

Chef vom Dienst: Georg Schnurer *(gs@ct.de)*

Koordination Leserkommunikation: Martin Triadan *(mat@ct.de)*

Leiter redaktionelle Entwicklung: Jobst Kehrhahn *(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 *(tig@ct.de)*, Arne Grävemeyer *(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

Leitende Redakteure: Peter Siering *(ps@ct.de)*, Jan Mahn *(jam@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 Schirrmacher *(des@ct.de)*, Hajo Schulz *(hos@ct.de)*, Jan Schüßler *(jss@ct.de)*, Kathrin Stoll *(kst@ct.de)*, Keywan Tonekaboni *(ktn@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 Jurran *(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 Kehrhahn *(keh@ct.de)*

Koordination: Pia Groß *(piae@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)*

Redaktionsassistenz: Susanne Cölle *(suc@ct.de)*, Christopher Tränkmann *(cht@ct.de)*

Software-Entwicklung: Kai Wasserbäch *(kaw@ct.de)*

Technische Assistenz: Ralf Schneider (Ltg., 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 89/42 71 86-0, Fax: 0 89/42 71 86-10

Ständige Mitarbeiter: Detlef Borchers, Herbert Braun *(heb@ct.de)*, Tobias Engler, Monika Ermert, Stefan Krempl, 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: 5C1C1DC5BEEDD33A
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: ayznmonmewb2tjvgf7ym4t2726muprjvwckzx2vhf2hbarbbzydm7oad.onion

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

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. 40 vom 1. Januar 2023.

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 AUGE, 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)*.

ISSN 0724-8679 AWA LAE

Vorschau c't 28/2023

Ab 2. Dezember im Handel und auf ct.de

Der optimale PC

Mit den aktuellen c't-Bauvorschlägen stellen Sie sich Ihren nächsten PC zusammen: je nach Wunsch und Bedürfnissen einen sparsamen Office-Mini-PC oder eine leistungsstarke Gaming-Maschine. Zudem erfahren Sie, worauf Sie beim Kauf von aktuellen Hardwarekomponenten achten müssen.

Ein Sack voll Geschenke

Die Tage werden kürzer und bald beginnt die Zeit der Ruhe und Besinnung. Wer seinen Liebsten mit kleinen, großen oder nerdigen Geschenken zu Weihnachten eine Freude bereiten will, findet in der kommenden Ausgabe die spannendsten und nützlichsten Geschenke-Tipps aus einem Jahr c't.

Test: Bilder verwalten ohne Cloud

Große Fotosammlungen verwaltet man besser mit lokalen Bilddatenbanken statt in der Cloud. Einige dieser Programme wenden sich an Bildagenturen, andere an Privatnutzer, die ihre Bilder für soziale Medien oder Fotobücher verwenden. Wir helfen bei der richtigen Wahl.

Günstige Drucker-Scanner-Kombis

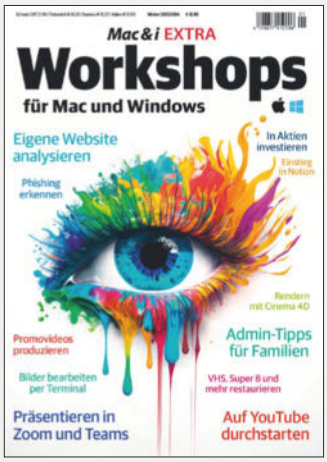
Wer für mäßiges Druckaufkommen in Haushalt und Homeoffice ein preisgünstiges Multifunktionsgerät sucht, muss mit hohen Folgekosten für Tintenpatronen rechnen. Als Sparoption werden für manche Modelle Tintenabos mit Druckseitenabrechnung angeboten. Doch was taugen diese Drucker?

PV-Strom im Mehrfamilienhaus

Die Dächer von Mehrfamilienhäusern werden kaum für Photovoltaik genutzt. Das will die Bundesregierung ändern und plant eine neue Form des Mieterstroms: Mieter und Vermieter schließen einen Vertrag, ein Algorithmus verrechnet Verbrauch und Erzeugung. So profitieren Sie von der Reform.

Noch mehr Heise-Know-how

iX Developer Herbst 2023 jetzt im Handel und auf heise-shop.de



Mac & i extra Winter 2023/2024 jetzt im Handel und auf heise-shop.de

MIT Technology Review 8/2023 jetzt im Handel und auf heise-shop.de


secIT by heise
HANNOVER 2024
meet.
learn.
protect.
05. - 07. MÄRZ 2024, HANNOVER
Die Kongress-
messe für
Security-Profis
Bis 31.12.2023
kostenloses Sponsored-Ticket
sichern oder von unseren
Frühbucherrabatten profitieren.
secit-heise.de
Offizieller Eventpartner
itsa EXPO CONGRESS
HOME OF IT SECURITY

HETZNER

KRAFTPAKET FÜR HÖCHSTE ANSPRÜCHE

DEDICATED SERVER EX130

Intel® Xeon® Gold 5412U Prozessor

DEDICATED SERVER EX130-R

- ✔ Intel® Xeon® Gold 5412U 24-Core "Sapphire Rapids"
- ✔ 8 x 32 GB DDR5 RDIMM
- ✔ 2 x 1,92 TB Gen4 NVMe SSD
- ✔ Unbegrenzter Traffic
- ✔ Standort Deutschland & Finnland
- ✔ Keine Mindestvertragslaufzeit
- ✔ Setupgebühr 94,01 €

monatlich ab **159,46 €**

DEDICATED SERVER EX130-S

- ✔ Intel® Xeon® Gold 5412U 24-Core "Sapphire Rapids"
- ✔ 4 x 32 GB DDR5 RDIMM
- ✔ 2 x 3,84 TB Gen4 NVMe SSD
- ✔ Unbegrenzter Traffic
- ✔ Standort Deutschland & Finnland
- ✔ Keine Mindestvertragslaufzeit
- ✔ Setupgebühr 94,01 €

monatlich ab **159,46 €**

Alle Preise inkl. 19% USt. Preisänderungen und Irrtümer vorbehalten.

www.hetzner.com