

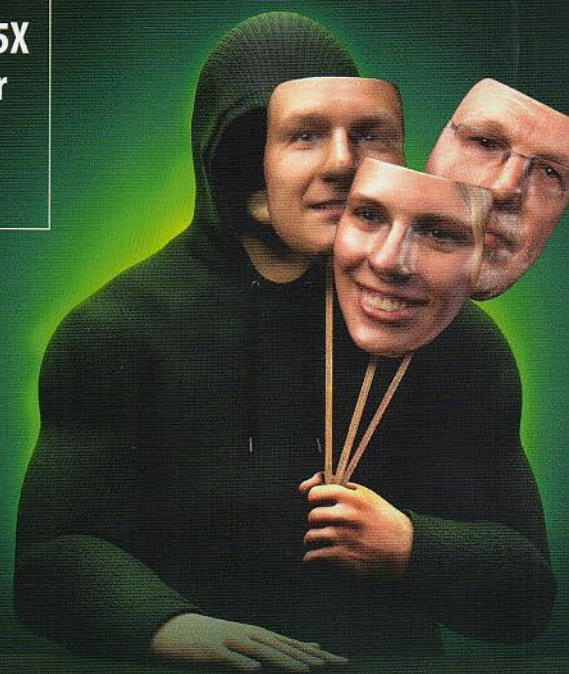
Bloßgestellt und ausgeplündert durch gekaperte Online-Konten

Identitätsklau verhindern

Angriffe entdecken • Wie Sie sich schützen • Erste Hilfe im Notfall

IM
TEST

- Übertaktbar: 28-Kerner Intel Xeon W-3175X
- Heimüberwachung: NAS als Videospeicher
- OCR-Apps zur Cloud-Dokumentenablage
- Preiswerte PC-Gehäuse mit USB-C



Günstige Gamer-Grafik

GeForce RTX 2060: Leise und schnell

KI gegen Kunden

Betrugserkennung bei Versicherungen

Fritzbox im Smarthome nutzen mit Node-Red

Docker Swarm: Container verteilen und verwalten

Raspi: DNS-Filter Pi-hole erweitern

Jetzt kaufen oder warten auf Faltdisplay und 5G?

Test der Super-Handys

7 Top-Android-Smartphones ab 400 Euro und iPhone Xs

€ 4,90
AT € 5,40 | LUX, BEL € 5,70
NL € 5,90 | IT, ES € 6,20
CHF 7,10 | DKK 54,00





The Good, the Bad and the Ugly

Die US-Geheimdienste haben es geschafft: Nach Jahren vergeblicher Warnungen überlegen nun auch die Europäer, ob sie Huawei tatsächlich weiter als Telekom-Ausrüster zulassen wollen. Der Vorwurf lautet schlicht: Der chinesische Netzzulieferer könnte durch eingebaute Hintertüren in seinen Produkten den Datenverkehr der Mobilfunknetze mitlesen (siehe Seite 16).

Auch wenn harte Belege fehlen, haltlos sind die Vorwürfe nicht: An den Skandal um den 2009 pleitegegangenen Weltkonzern Nortel erinnert man sich heute kaum noch. Der damals noch kleine Bruder Huawei hatte offenbar die Passwörter der gesamten Führungsriege Nortels ausgekundschaftet. Jahrelang ahnten die Kanadier nicht, dass Know-how von West nach Ost abfloss, bis der Erfinder der LTE-Technik weder mit Ericsson noch mit Nokia mithalten konnte - und schon gar nicht mehr mit Huawei.

Nun soll ein Sicherheitskatalog her, der Huawei einhegt. Doch das genügt nicht. Anscheinend lässt die Furcht vor Backdoors vergessen, dass es 100-prozentige Sicherheit in komplexen und noch dazu vernetzten IT-Infrastrukturen nicht geben kann. Beispielsweise kann bis heute kein Hersteller garantieren, dass seine Chips sämtliche Berechnungen korrekt ausführen. Intels FDIV-Bug im Pentium-Prozessor ist nur ein gravierendes Beispiel (massive Fehler bei manchen Gleitkommaberechnungen).

Dabei hat die Komplexität von Chips seit der Pentium-Ära stark zugenommen. Manche 5G-Bausteine müssen derart leistungsfähig gemacht werden, dass es im besten Universum, das wir kennen, gar keine Chance gibt, gegen Sicherheitslücken anzuentwickeln und zugleich den Chip in endlicher Zeit fertigzustellen - Spectre lässt grüßen. Ganz zu schweigen davon, dass in Firmware und Betriebssystemen noch mehr Hasen im Pfeffer liegen. Wer will da zwischen beabsichtigten und unbeabsichtigten Lücken unterscheiden?

Solange ein Gerät vernetzt ist, ist es aus dem Netz auch angreifbar. Genügend Manpower und Know-how vorausgesetzt, kann jede organisierte Angreifergruppe jedem Internet-Nutzer in die Unterhosen gucken. Deshalb hat die Politik keine echte Wahl, ob sie Huawei nur angeleint in die Netze lassen will oder ausschließlich deren Mitbewerber. Sie kann lediglich entscheiden, den anscheinend bösen oder vermeintlich guten Drachen zu füttern, hässlich sind sie beide.

Dan Zivadinović

Dušan Zivadinović

Trends & News

- 16 USA versus China: Huawei's zentrale Rolle
- 18 DRAM-Preise könnten steigen: USA blockieren chinesische Speicherchip-Fabrik
- 20 **Schleierfahndung mit Nummernschild-Scannern**
- 22 Bit-Rauschen: Der Handelskrieg gegen China stört die IT-Branche
- 23 Hardware: Sicherheitslücken in Mainboard-Software von Asus und Gigabyte
- 24 Embedded Systems: Raspi-Industriemodul CM3+, USB-Messmodul für 60 Euro
- 25 Server & Storage: KI-Beschleuniger, Server mit Xeon-SP Cascade Lake, Neuer Flash-Anbieter
- 26 Netze: PoE+-Switches für zu Hause, Firmen und Fahrzeuge, Access-Point mit IoT-Option
- 27 Satellitennavigation: EU macht Jagd auf GPS-Störsender
- 46 Animationstechnik: Making of ... Manou flieg flink
- 48 Musik- und CAD-Software: Ableton Live 10.1, CorelCAD 2019
- 49 Spiegellose Vollformatkamera: Panasonic Lumix S1
- 50 Apple: Unmut über FaceTime-Lücke, Ethernet-Adapter mit Lightning, Tastatur aus Glas
- 51 Forschung: Exoskelett bewegt die Hand
- 52 DNSSEC: Domains sicher umziehen mit dem Extensible Provisioning Protocol
- 53 Forschung: Seniorengerechte Hilfsroboter, Strahlenmessgerät der Uni Kiel auf dem Mond



Günstige Gamer-Grafik

Nvidias GeForce RTX 2060 hat genug 3D-Power zum Zocken in WQHD-Auflösung – und kann sogar Ray-tracing-Effekte darstellen. Sechs Grafikkarten ab 350 Euro stellen sich Nvidias Referenzkarte in puncto Leistung und Lautstärke.

- 54 Facebook: Bundeskartellamt kritisiert Marktmacht
- 55 Werbeblocker-Erweiterungen für Chrome führen zu Unmut bei Entwicklern
- 56 Linux 5.0: Ruckelfrei zocken, schnellerer Datenaustausch
- 59 Linux: Lutris importiert Spiele von GOG.com
- 60 IT in Nigeria: Start-ups werden von der Realität eingeholt
- 61 Digitaler Filmdienst UltraViolet macht dicht
- 62 E-Sport: Fußballvereine steigen in das Millionen-geschäft mit den Konsolensportlern ein
- 75 Web-Tipps: Kaffee-Wiki, Git lernen, Briefe als Zeitzeugnisse

Test & Kaufberatung

- 70 High-End-Grafikkarte AMD Radeon VII mit 16 GByte HBM2
- 72 **Übertaktbar: 28-Kerner Xeon W-3175X**
- 76 **Test der Super-Handys**
- 78 7 Top-Android-Smartphones und das iPhone Xs
- 86 Tiling Terminal Emulator: Tilix 1.8.9
- 86 Kanban-Board zum Selbsthosten: Wekan Open-Source Kanban
- 87 Bluetooth-Tastatur im Schreibmaschinen-Look: Azio Retro Classic BT
- 87 Syntaxhervorheber für Webseiten: highlight.js
- 88 Fensterputzroboter mit Akku und Sicherungsleine: Ecovacs Winbot X
- 89 Bluetooth-Audio-Dongle für Nintendo Switch: Human Things Genki
- 90 Smartes Türschloss: Nuki 2 und Keypad
- 91 Frontpanel mit Typ-C-Buchse für USB 3.1 Gen 2: Inline Frontpanel
- 91 Nutzungskontroll-App: Agooday Screen Time
- 92 Open-Source-Notensatzprogramm: MuseScore 3.0.2
- 94 Linux-Distribution mit flexiblem Desktop: Deepin 15.9
- 96 **Günstige Gamer-Grafik**
- 102 **Heimüberwachung: NAS als Videospeicher**
- 106 **Preiswerte PC-Gehäuse mit USB-C**
- 110 **OCR-Apps zur Cloud-Dokumentenablage**
- 114 Raw-Entwicklung: Acht nichtdestruktive Foto-Entwickler für schnellen Workflow
- 165 Bücher: Digitale Drogen, Printdesign



Identitätsklau verhindern

In diesem Augenblick kapern Cyber-Ganoven unzählige Online-Konten. Mit unseren Tipps verhindern Sie, dass Ihre dazugehören. Und falls es doch passiert, zeigen wir Ihnen, was zu tun ist.

Wissen

28 Identitätsklau verhindern

- 32 So erkennen Sie, welche Online-Dienste mit Ihren Zugangsdaten schludern
- 36 Wie Sie Ihre digitale Identität schützen
- 40 Sofortmaßnahmen nach einem Angriff auf Ihre digitale Identität
- 42 25 Gigabyte Passwortlisten von HaveIBeenPwned schnell lokal durchsuchen
- 64 **Versicherungen: KI gegen Kunden**
- 68 Vorsicht, Kunde: Abzocke mit Notebook-Reparaturen
- 132 Chatbots: So richtig beliebt sind sie noch nicht
- 164 Recht: Der BGH schränkt die Kosten für Abmahnungen bei Fotoklau ein
- 166 KI errät Geodaten zum Foto
- 170 So besiegte künstliche Intelligenz die Profigamer in StarCraft 2
- 180 Computermäuse: Technik und Geschichte
- 182 Drahtlose Audioübertragung zu Lautsprechern per WiSA
- 185 Bluetooth 5.1: Was es bringt, wie es funktioniert
- 186 Linux 5.0: Entwickler sperren Nvidias proprietären Grafiktreiber aus

Praxis & Tipps

- 74 Smart-TV: Samsung-TVs die Geschwätzigkeit austreiben
- 124 FAQ: Optimaler PC
- 128 Tipps & Tricks
- 134 **Fritzbox im Smarthome nutzen mit Node-Red**
- 138 Tipps zur Windows-Aufgabenplanung
- 142 **Docker Swarm: Container verteilen und verwalten**
- 150 **Raspi: DNS-Filter Pi-hole erweitern**
- 154 Messwerte und Logs speichern und automatisch zusammenfassen mit InfluxDB
- 158 WireGuard: VPN ganz einfach
- 176 F-Droid: Mit dem Repomaker eigene App-Kataloge bauen

Rubriken

- 3 Editorial: The Good, the Bad and the Ugly
- 10 Leserforum
- 15 Schlagseite
- 190 Story: Tyrus (1) von Hilga Höfkens
- 199 Stellenmarkt
- 200 Inserentenverzeichnis
- 201 Impressum
- 202 Vorschau



Test der Super-Handys

Für ein aktuelles High-End-Smartphone müssen Sie nicht mehr Ihr letztes Hemd hergeben. Trotzdem ist die Technik up to date und man braucht auf keine Spielerei zu verzichten. Sieben Top-Android-Smartphones ab 400 Euro und das iPhone Xs im Vergleich.

Leserforum

Es geht auch ohne Cloud

Editorial: Wohl und Wehe der Patientenakte,
c't 4/2019, S. 3

Vielleicht denkt mal jemand darüber nach, ob wirklich alles (inkl. Gesundheitsdaten) ins Netz gestellt werden muss. Eine verschlüsselte dezentrale Speicherung von Anamnese, Befunden, Laborwerten, Sono- und MRT-Bildern et cetera zum Beispiel auf dem USB-Stick des Patienten selbst wäre ebenso informativ, aber ohne physischen Besitz des Sticks viel weniger angreifbar. Vielleicht überrascht es Sie, dass diese Methode schon von einigen Patienten praktiziert wurde – freilich mit bescheidenem Erfolg. Warum wohl? Weil Ärzte ihre Diagnose ungern auf fremde Daten stützen und deshalb trotz Vorlage der Daten nochmals untersuchen, Blut analysieren und bildgebende Verfahren einsetzen. Und im Notfall bleibt ohnehin keine Zeit, die alten Daten sorgfältig zu sichten. Also in jedem Fall ein fragwürdiger Aufwand mit – insbesondere beim Cloud-Verfahren – inakzeptablen Risiken für den Datenschutz.

Claus P. Baumeister

Blackbox Gesundheitskarte

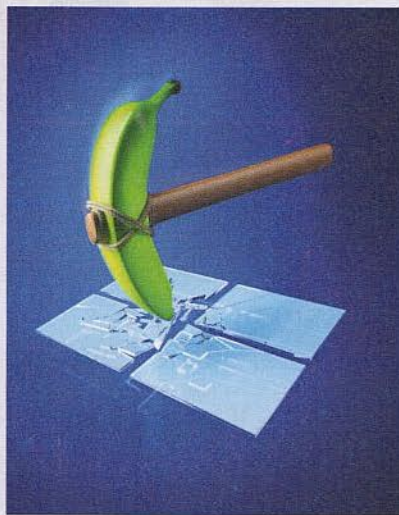
Mit der Gesundheitskarte wird es am Ende wie bei der Blackbox in Autos sein. Versicherungen werden die Herausgabe von Daten und damit eine Selbstbelastung fordern, nach dem Prinzip „wenn du nichts zu verbergen hast“. So findet mit Sicherheit ein Arbeitgeber eine gute Begründung, warum er durch unabhängige Unternehmen deinen Gesundheitsstatus prüfen lassen darf.

Ich adaptiere zunehmend die Philosophie von Herrn Weizenbaum. Wenn du deine Privatsphäre behalten willst, dann mach den verdammten Computer nicht an. Oder mit Douglas Adams: Wenn du dich vor Schlangengift schützen willst, lass dich nicht beißen.

Frank Beister

Von anderen lernen

Die Diskussion über das „Wie“ einer digitalen institutionsübergreifenden Patientenakte finde ich sehr wichtig. Ich habe



Unser Vergleich der Windows-10-Updates mit Bananen ging einigen Lesern nicht weit genug.

jedoch den Eindruck, dass man hier in Deutschland das Rad auf Biegen und Brechen neu erfinden will und damit immer weiter zurückfällt. Andere Länder sind uns bei der Digitalisierung des Gesundheitswesens zum Teil weit voraus (mit Langzeiterfahrung), ohne dabei den Datenschutz zu vernachlässigen. In Dänemark funktioniert die Datenhaltung dezentral, in Finnland kann man gar prüfen, ob Patienten nach den medizinischen Leitlinien behandelt wurden. Warum nicht im Sinne von Best Practice von den anderen Ländern lernen und damit den Rückstand endlich und vor allem patientenorientiert aufholen? Das Potenzial einer elektronischen Patientenakte ist im Einzelfall wie auf volkswirtschaftlicher Ebene hoch. Gleichzeitig ist der Rückstand in Deutschland auf nationaler wie auf Institutionsebene insgesamt gesehen enorm.

Alexander Straube

Was tun?

Windows-Update-Misere: Warum Sie reagieren sollten, c't 4/2019, S. 58

Da bekommen wir seit Jahren gebetsmühlenartig den dringenden Rat, Software-Updates zeitnah einzuspielen, um Sicherheitslücken zu schließen. Und jetzt das: sicherheitsrelevante Updates sofort ein-

spielen, von allen anderen die Finger lassen oder wenigstens verzögern, bis die Bananen gereift sind. Nach der Lektüre über Microsofts Qualitäts-Management habe ich meine Zweifel, ob diese Unterscheidung überhaupt machbar ist. Wenn der Hersteller selbst nicht weiß, was er tut, woher soll es dann der Anwender wissen?

Michael Braun

Schon vor Windows 10

Nachgereift, nachdem auf die Menschheit losgelassen, sind Windows-Versionen schon vor Windows 10. Vielleicht wurden sie damals nicht ganz so grün auf den Markt geworfen und ihnen ging nicht so schnell die Puste aus – die dreizehn (und mehr) XP-Jahre sind mittlerweile Legende und „Windows as a service“ gabs schon zuvor. Microsoft stünde es besser an, sich wieder auf das schlichte „Windows as an operating system“ zu besinnen – und zwar eins, das wenigstens fünf bis sieben Jahren unterstützt wird. Gerne auch mit telemetrischen Erhebungen, auf die der Nutzer Einfluss nehmen kann, aber möglichst ohne allen Beipack-Schrott. Ja, es ist ein Traum ...

Gustav Schrobbsdorff

Totgeglaubte Bugs

Eine Sache, die mich persönlich extrem nervt, ist, dass sogar bereinigte Fehler in

Wir freuen uns über Post

✉ redaktion@ct.de

💬 c't Forum

📘 c't magazin

🐦 @ctmagazin

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

Antworten sind kursiv gesetzt.

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

neuen Feature-Releases wieder enthalten sind. So geschehen zum Beispiel mit der Eventlog-Archivierung, die in 1709 nicht mehr funktionierte. Mit dieser Funktion kann Windows volle Eventlogs archivieren und automatisch ein neues anlegen. Der Fehler wurde im Januar-Update 2018 behoben, aber ist seit dem 1803 Release wieder zurück, und zwar auch im Server 2019. Ich habe verzweifelt versucht herauszufinden, wie man diesen Fehler an Microsoft melden kann, aber offensichtlich ist das nur über den Feedback-Hub möglich und bisher habe ich nicht den Eindruck, dass Einträge dort wirklich gelesen werden.

Holger Voges

Windows vs. Banane

Ihr Vergleich mit der Naturfrucht Musa paradisiaca (Dessertbanane) mit dem Windows-Updateprozess ist zwar auf den ersten Blick ganz überzeugend. Doch bei genauer Inaugenscheinnahme gewinnt die Natur eindeutig.

1.) Die essbare Banane ist ein Wunderwerk von Nahrungsquelle. Sie ernährt viele Millionen Menschen täglich und ist dazu äußerst gesund. Windows dagegen ernährt nur ein paar nicht ganz so gründliche Entwickler (1:0 für die Natur).

2.) Sie ist selbstreifend – ganz im Gegensatz zu Windows (2:0).

3.) Man kann sie gekühlt lange lagern und transportieren und als Großhändler gezielt mit Ethylen zur Reifung bringen. Als Reseller Windows selbst reifen lassen? Keine Chance (3:0)!

4.) Sogar der Endanwender kann sich grüne Bananen in den Vorrat legen und dann passgenau die Reifung starten – einfach, indem er einen Apfel dazulegt! Ein Apfelrechner neben dem Windows-Rechner auf den Schreibtisch hilft den Windows-Updates dagegen kein bisschen (4:0).

5.) Der Geschmack ist in der Natur immer gleich. Windows ändert sich dauernd und zwar ganz und gar nicht nach meinem Geschmack (5:0)!

6.) Nicht mal das Klonen geht so wie in der Natur. Man benötigt dazu einen speziellen Gen-Code bei Windows.

Damit ist der Endstand 6:0 für die Natur. Microsoft sollte sich davon mal eine Scheibe oder ein Stück abschneiden ...

Olaf Schilgen

Unter Wasser

Aufbruch nach Digitalien: Das smarte Leben eines smarten Bürgers, c't 4/2019, S. 32

Den Absatz „... seit 2030 Verbrennungsmotoren verboten wurden“ würde ich wie folgt ergänzen wollen: „Durch den gestiegenen Stromverbrauch zeigte sich die Schwäche der Strom-Infrastruktur. Als es wegen ausfallender Notstromaggregate in Krankenhäusern die ersten Todesfälle gab, entschied man sich, den Ausstieg aus der Braunkohle auszusetzen. Jonas kennt Venedig und die Niederlande nur als Taucherparadies. Wie fast alle seiner Mitschüler in Hannover liebt er das Fischen in der Nordsee direkt vor den Toren der Stadt.“

Andreas Oppermann

Individuelle E-Mail-Konten

Troy Hunt und der riesige Passwort-Fund „Collection #1 bis #5“, c't 4/2019, S. 16

Ein zentrales Thema ist bei den aufgetauchten Passwörtern ja auch die E-Mail-Adresse als Account-Basis-Information. Ich war mit dem Thema schon länger befasst, weil meine E-Mail-Adresse zwar nicht gehackt war, aber trotzdem auf vielen Spam-Schleudern eingetragen ist. Das war so schlimm, dass ich diese E-Mail-Adresse für 2 Jahre vom Netz genommen habe. Da es eine persönliche Domain-Adresse ist, die ich seit über 15 Jahren verwende, wollte ich sie wiederhaben. Nach 2 Jahren Fehlermeldungen für die Absender bin ich von den Spam-Schleudern befreit.

Parallel habe ich damit begonnen, meine Account-Daten zu überarbeiten, denn für zukünftige Spam-Fälle wollte ich die Quelle kennen. Mittlerweile habe ich für jeden Account neben einem Unikat-Passwort auch eine individuelle E-Mail-Adresse. So habe ich über 100 E-Mail-Adressen. Konsequenterweise betrieben ist es etwas Aufwand: anlegen, 5 Minuten warten, überprüfen und dann verwenden. Die Alias-E-Mail-Adressen werden zusammen mit den Passwort in einem Tresor verwaltet. Von vielen werde ich belächelt, wenn ich davon erzähle, aber Ihr Artikel zumindest gibt mir da recht.

Roland Kürten

Unzählige E-Mail-Konten

Es wird immer wieder empfohlen, „alle“ seine Konten zu ändern. Das ist doch ein Ding der Unmöglichkeit. Die letzten

Fragen zu Artikeln

✉ Mail-Adresse des Redakteurs am Ende des Artikels

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

20 Jahre habe ich wohl hunderte, wenn nicht tausende Kontos auf Webseiten eröffnet, von Chats über Foren, Webshops, Onlinemedien, Mail Providern und vieles mehr. Das Ändern scheitert doch genau daran, dass man keine Ahnung hat, wo man denn überall registriert ist.

Dominic Blattman

Armutszeugnis USB

Doppelte Datenrate, schnelleres Laden und höhere Sicherheit für USB-Verbindungen, c't 4/2019, S. 48

Für die IT-Branche ist die Außendarstellung von USB ein Armutszeugnis, aber leider eben auch in anderen Entwicklungen gängige und leider akzeptierte Praxis.

Mir ist durchaus bewusst, dass Normierungsgremien von verschiedenen Herstellern mit eigenen Interessen getrieben werden, dennoch sollte es gerade ITlern möglich sein, klare und eindeutige Standards zu setzen und zu definieren. Eine mit klarem Menschverstand zu verstehende Logik ist leider nicht immer zu erkennen.

Pipes

Ergänzungen & Berichtigungen

Tipfehler

Teure Telefonauskunft, Streit in der Schweiz über die hohen Kosten von Staatstrojanern und Fernmeldeüberwachung, c't 4/2019, S. 46

Der sozialdemokratische Sicherheitsdirektor im Kanton Zürich heißt nicht Mario Kehr, sondern Mario Fehr.

Telekom

Warum ein De-Mail-Konto einen Versuch wert ist, c't 4/2019, S. 72

Die Telekom ermöglicht die notwendige Identifikation für ein De-Mail-Konto auch über die ID-Funktion des Personalausweises online.



Weitere Schlagseiten auf ct.de/schlagseite

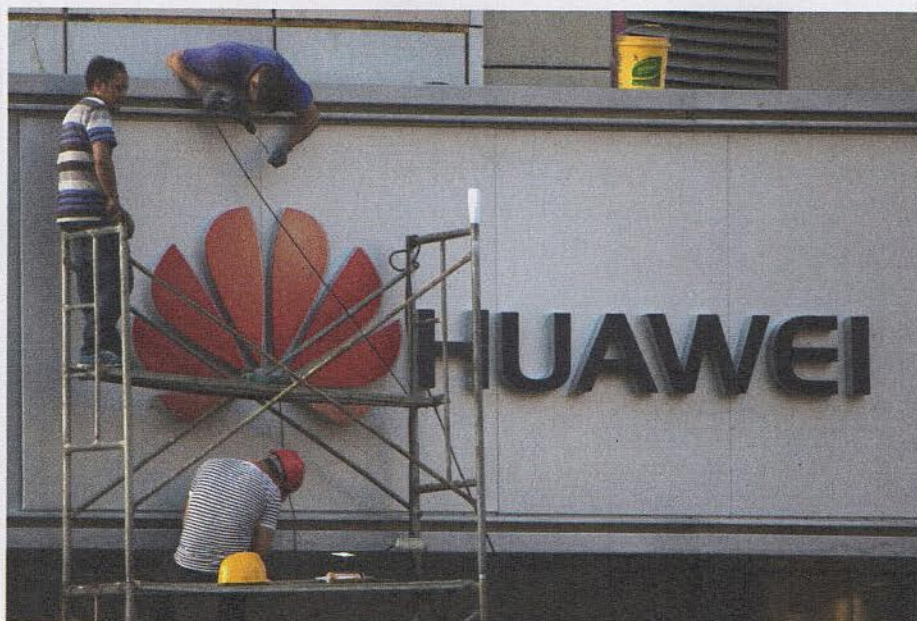


Bild: Ng Han Guan/AP/dpa

Eine Frage des Vertrauens

Welche Rolle Huawei im Handelskrieg der USA gegen China spielt

Seit Jahren warnen US-Geheimdienste vor chinesischen Telekom-Ausrüstern. Sie würden die Sicherheit der USA und deren Partner gefährden. Ohne Beweise gerät die Wahl des Netzausrüsters jedoch zur nationalen Vertrauensfrage.

Von Daniel AJ Sokolov

Seit den Snowden-Enthüllungen vor gut fünf Jahren hat man eine ungefähre Ahnung, wie die NSA über versehentliche und absichtliche Hintertüren in Cisco-Router, Dell-Server sowie Hard- und Software anderer US-Hersteller eindringt und Daten abzapft. Nun drängen die Amerikaner andere Länder wie Deutschland dazu,

auf chinesische Produkte von Huawei und ZTE zu verzichten, weil sie China Gelegenheit zur Spionage und Sabotage geben könnten.

Konkrete Beweise bleiben die Amerikaner bislang schuldig. In einem kurzen Tweet urteilte der in Japan lebende Sicherheitsexperte Hector Martin über einen Huawei-Switch. Dort fand er unter anderem selbst gestrickte Software-Elemente (Secure Shell und TCP/IP-Stack) mit Sicherheitslöchern wie in einem Schweizer Käse. Da brauche es laut Martin gar keine absichtlich eingebauten Hintertüren, wie sie die NSA im Zuge von PRISM bei großen US-Firmen einsetzte. Der chinesische Geheimdienst habe lediglich einen Zeitvorteil beim Finden und Ausnutzen der Fehler, wenn er direkten Zugriff auf den Quellcode von Huawei bekomme.

Auf Zeit spielen auch die USA. Denn für die Geheimdienste kann eine Offen-

legung von Beweisen taktische Nachteile haben: Der Gegner könnte dadurch gewarnt werden und sein Verhalten ändern. Die Frage der „nationalen Sicherheit“ ist jenseits des Atlantiks insbesondere eine Vertrauensfrage: „Die kritische Infrastruktur der USA und insbesondere ihre Telekommunikationsnetze bauen auf Vertrauen und Verlässlichkeit“. So stand es bereits 2012 in einem Bericht des Geheimdienstausschusses des Repräsentantenhauses über Huawei und ZTE. „Telekommunikationsnetze sind anfällig für böswilliges [...] Eindringen oder störende Aktivitäten. Daher muss zu jeder Zeit ein ausreichendes Niveau an Vertrauen gegenüber dem Lieferanten der Ausrüstung als auch (dem Betreiber) gegeben sein.“

Misstrauen statt Beweise

Der Parlamentsausschuss hebt die besondere Bedeutung der Telekommunikation hervor: Vom Stromnetz über das Finanzsystem, die Energie- und Wasserversorgung bis zum Transportwesen sind alle wichtigen Infrastrukturen von Datenverbindungen abhängig. Ein Problem in einem System kann eine Kettenreaktion auslösen.

Mehrfach betont der Bericht den Mangel an Vertrauen gegenüber Huawei und ZTE. „Beruhend auf verfügbaren geheimen und öffentlichen Informationen kann nicht darauf vertraut werden, dass Huawei und ZTE frei von staatlicher Einflussnahme sind, weshalb sie eine Bedrohung für die Sicherheit der USA und unserer Systeme darstellen“, heißt es in der Zusammenfassung.

Genährt wird dieser Vertrauensmangel durch die undurchsichtige Firmenkonstruktion Huaweis. Offiziell sind die in China beschäftigten Mitarbeiter auch Aktionäre des Unternehmens, wenn auch ohne Stimmrecht. Huawei wird angelastet, im Rahmen der US-Untersuchung keine konkreten Antworten gegeben zu haben. Die Firma hat zwar zugegeben, dass die kommunistische Partei Chinas einen Parteiausschuss innerhalb Huaweis betreibt. Dessen Befugnisse und seine Mitglieder blieben aber geheim.

Hinzu kommen Vorwürfe über regelmäßige Verletzungen von Patentrechten und Software-Lizenzen. Der US-Konkurrent Cisco hatte bereits 2003 geklagt, weil Huawei angeblich Quellcode kopiert hatte. Symptomatisch war, dass Huawei im Verfahren vor dem US-Kongress da-

mals Präsentationsfolien verteilte, die urheberrechtlich geschütztes Material von McKinsey enthielten. Anscheinend arbeiten auch Huaweis Anwälte nicht sorgfältiger als die Programmierer des Konzerns.

Sicherung der Wirtschaft

Der Begriff der nationalen Sicherheit umfasst in den USA wie in China wesentlich mehr als den bloßen Schutz militärischer und politischer Geheimnisse. Unter dem Begriff wird ebenso die Sicherheit der Wirtschaft, Umwelt, Energieversorgung sowie der Schutz der Informations- und Kommunikationstechnik subsumiert.

Was in den USA unter dem Begriff „Homeland Security“ läuft, regelt in China ein 2015 erlassenes Staatssicherheitsgesetz. Seit 2017 dürfen chinesische Geheimdienste jeden Bürger und jede Firma zu Auskunft und Mitarbeit verpflichten, alle Räumlichkeiten betreten, Akten einsehen, Gegenstände beschlagnahmen und Informationen sammeln. Daher sind Beteuerungen chinesischer Firmen, sich an alle Gesetze zu halten, aus US-Sicht keine Beruhigungspille.

Machtpolitisches Gerangel

Vor diesem Hintergrund ist es kein Wunder, dass sich der Konflikt der USA mit Huawei in den letzten Monaten verschärft hat: Im Dezember wurde Huaweis Finanzchefin Meng Wanzhou in Kanada verhaftet. Die USA werfen der Managerin

vor, das US-Embargo gegen den Iran unterlaufen zu haben und verlangen ihre Auslieferung. Um dies zu verhindern, reagierte China wiederum mit der Verhaftung mehrerer Kanadier.

Eine zweite US-Anklage bezichtigt Huawei der Wirtschaftsspionage. In einem Zivilprozess gab der Konzern bereits zu, dass Mitarbeiter vor rund sechs Jahren Geschäftsgeheimnisse bei T-Mobile USA ausgekundschaftet hatten. Aufgrund geheimdienstlicher Erkenntnisse gibt es nun eine erneute Anklage: Huawei soll die Wirtschaftsspionage aus seiner Firmenzentrale steuern. Es soll sogar ein Bonussystem für Mitarbeiter geben, die Geheimnisse anderer Unternehmen beschaffen.

Handelskrieg

Bei all dem Hin und Her drängt sich der Verdacht auf, die Anklagen und Warnungen seien Teil eines von Donald Trump geplanten Handelskriegs gegen China. Doch dieser Schluss würde dem aktuellen US-Präsidenten ein Maß an Koordination mit seinen Behörden und Geheimdiensten zuschreiben, das nicht zu dem Bild passt, das er seit seinem Amtsantritt abgibt.

Zudem würde die Schlussfolgerung die Chronologie ignorieren: Trump begann den Handelskrieg Anfang 2018. Der Zank mit Huawei reicht jedoch fast zwei Jahrzehnte zurück. Bereits im Jahre 2000

drangen mutmaßlich aus China stammende Hacker in das Firmennetzwerk des kanadischen Konzerns Nortel ein und zapften über Server in Shanghai jahrelang Entwicklungsberichte, Geschäftspläne und E-Mails ab. Nortel wehrte die Angriffe nur halbherzig ab und ging 2009 im Zuge der Wirtschaftskrise pleite. Huawei hatte kurz zuvor noch 400 Millionen US-Dollar für Nortel geboten. Das wurde von den Amerikanern aufgrund von Sicherheitsbedenken aber ebenso abgelehnt wie eine Übernahme des Netzwerkausrüsters 3com.

Die USA und deren enge Verbündete Australien und Neuseeland sind jedoch nicht die einzigen, die vor Huawei warnen. So stellte der indische Geheimdienst bereits 2010 klar, Ausrüstung von Huawei würde lediglich in grenzfernen Regionen Indiens gestattet. Polen hat erst kürzlich einen Huawei-Mitarbeiter unter Spionagevorwürfen verhaftet.

Alternativen in Europa

Auch in Deutschland wachsen die Widerstände. So forderte im EU-Parlament jüngst der Grünen-Abgeordnete Reinhard Bütikofer, den Einsatz von Huawei-Technik beim bevorstehenden Ausbau der 5G-Netze zu verbieten. Betroffen wäre beispielsweise die Deutsche Telekom, die aus Kostengründen weiterhin Huawei-Geräte einsetzt, obwohl deren US-Tochter T-Mobile durch Huawei-Mitarbeiter ausgespiert wurde. Dort schlägt man eine Prüfung und Zertifizierung der Netzwerkkomponenten durch ein unabhängiges Prüflabor unter staatlicher Aufsicht vor – etwa durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) – und fordert die Offenlegung der Quellcodes der Geräte.

Open Source würde zwar die anfangs erwähnten Sicherheitsprobleme durch fehlerhaften proprietären Code eindämmen. Eine absolute Sicherheit gibt es in der IT jedoch nicht (siehe Editorial auf Seite 3). Wenn man von US-Firmen wie Cisco weiß, dass der US-Geheimdienst Hintertüren nutzt, und chinesischen Firmen misstraut – dann bleiben in Europa mit Nokia und Ericsson nur wenige alternative Hersteller übrig. Siemens, einst deutscher Vorreiter bei der Netzwerktechnik, liefert inzwischen nur noch Einzelkomponenten. (hag@ct.de) **ct**

Protokolle der US-Untersuchungen:
[ct.de/y3dy](https://www.ct.de/y3dy)

Huawei in Zahlen

Huawei wurde 1987 von einem ehemaligen Telekommunikationsoffizier der chinesischen Armee gegründet und ist heute ein Vorzeigekonzerne Chinas. Der Firmenname kann salopp mit „China hat es drauf“ übersetzt werden. Huawei hat über 180.000 Mitarbeiter in drei Sparten: Endgeräte, Ausrüstung und Dienstleistungen für Telekom-Betreiber sowie Netzwerke und Datenspeicher für große Unternehmen und Behörden. 2018 hat der Jahresumsatz 108 Milliarden US-Dollar überschritten. Zum Vergleich: Google brachte es auf 136 Milliarden Dollar. Huaweis chinesischer Mitbewerber ZTE bäckt mit einem Jahresumsatz von 17 Milliarden US-Dollar (2017) wesentlich

kleinere Brötchen. Bei Smartphones lieferte sich Huawei 2018 ein Kopf-an-Kopf-Rennen mit Apple um den zweitgrößten Marktanteil hinter Samsung. Dieses Jahr möchte Huawei Samsung vom Thron stoßen. Auch bei der Netzwerktechnik (inklusive Hardware, Management und Wartung) liegt Huawei weltweit auf dem zweiten Platz hinter Cisco, noch vor Ericsson, Nokia Networks und ZTE. Praktisch alle großen Netzbetreiber haben Huawei-Ausrüstung im Einsatz. Der Erfolg wurde nicht zuletzt mit Beihilfen des chinesischen Staates ermöglicht, durch die Huawei seine Produkte oft günstiger als die Konkurrenz anbieten kann.

DRAM-Krimi

US-Behörden blockieren Betrieb einer Speicher-Chipfabrik in China

Die USA kämpfen im Handelskrieg gegen China mit harten Bandagen. Der Vorwurf der Wirtschaftsspionage gegen einen DRAM-Hersteller könnte auch bei uns die Speicherpreise in die Höhe treiben.

Von Christof Windeck

Exportverbote der USA stoppen den Betrieb der nagelneuen, mehr als 5 Milliarden US-Dollar teuren DRAM-Fabrik Fujian Jinhua Integrated Circuit (JICC) in China. Sie ist Teil der Anstrengungen Chinas, die Abhängigkeit von Importen zu verringern. Dazu gehört nicht nur die Entwicklung eigener Prozessoren wie der ShenWei-Chips für den Top-10-Supercomputer Sunway TaihuLight, sondern auch der Aufbau lokaler Halbleiterfabriken. Außer in JICC steckt die Regierung auch viel Geld in die Mobilspeicher-Fab Innotron sowie in den NAND-Flash-Fertiger Yangtze Memory Technologies (YMTC, siehe c't 18/2018, S. 16).

Doch im Herbst 2018 warf das Justizministerium der USA drei JICC-Managern Industriespionage vor. Zuvor hatte 2017 der US-Chiphersteller Micron gegen JICC geklagt. Die Vorwürfe des Ministeriums haben allerdings ein anderes Kaliber. Sie wurden nicht nur vom damaligen Justizminister Jeff Sessions vorgetragen, sondern auch von John Demers aus der National Security Division und von FBI-Direktor Christopher Wray. Sie sehen die nationale Sicherheit der USA in Gefahr, weil sich chinesische Staatsfirmen mit Dritten verschwören, um den technischen Vorsprung amerikanischer Unternehmen zu untergraben. Deshalb hat das US-Handelsministerium alle Exporte an JICC verboten.

Ohne Rohmaterialien aus den USA kann JICC nicht produzieren. Spätestens ab März wird JICC stillstehen, meldet die Financial Times. Bereits im vergangenen Oktober berichtete Bloomberg, dass Teile des großen JICC-Firmengeländes in Jinjiang in der Küstenprovinz Fujian verlassen wirkten.

Das chinesische Handelsministerium entgegnet den US-Behörden, sie trügen zu stark auf („... overgeneralize the concept of national security“). Die schweren Vorwürfe treffen auch den nach TSMC und Globalfoundries weltweit drittgrößten Auftragsfertiger für Halbleiterbauelemente, die United Microelectronics Corporation (UMC) aus Taiwan. Denn UMC verkaufte das zur DRAM-Fertigung nötige Know-how sowie einige Produktionsmaschinen an JICC und schickte den erfahrenen Manager Stephen Chen. Er wurde Chef von JICC nach einer kurzen Zwischenstation bei UMC. Zuvor leitete er Micron Memory Taiwan, die taiwanische Fertigungssparte von Micron. Nach Ansicht der US-Behörden haben Chen und zwei weitere ehemalige Micron-Taiwan-Mitarbeiter das DRAM-Wissen jedoch schlichtweg gestohlen.

Auf die Micron-Klage in den USA reagierte UMC 2018 mit einer Gegenklage in China. Bestimmte Produkte der Micron-Tochter Crucial dürfen in China nicht mehr verkauft werden, weil sie UMC-Schutzrechte verletzen. UMC entwickelt nach eigenen Angaben schon seit 1996 DRAM-Technik. Micron hingegen habe das strittige Know-how erst 2012 mit der Übernahme der seinerzeit insolventen japanischen Firma Elpida erworben. Deren DRAM-Technik kam bei der taiwanischen Elpida-Fertigungssparte Rexchip zum Einsatz, aus der später Micron Memory Tai-

wan wurde – unter der Leitung des ehemaligen Rexchip-Chefs Stephen Chen.

Chen kooperierte schon vor zehn Jahren mit UMC. Denn durch die Rezession 2008 gerieten mehrere taiwanische DRAM-Hersteller in wirtschaftliche Schieflage, außer Rexchip etwa noch Inotera, Powerchip und ProMOS. Die taiwanische Regierung wollte diese Firmen mit Subventionen retten und zum Konglomerat „Taiwan Memory Company“ (TMC) verschmelzen. Daran sollte sich auch UMC beteiligen, als TMC-Chef war Stephen Chen vorgesehen.

Druck auf UMC

Nach der Intervention der US-Behörden verkündete UMC Ende 2018, alle Aktivitäten für JICC zu stoppen. Bereits an JICC verkaufte Maschinen werden nicht von Taiwan nach China ausgeliefert, wie UMC bei der Präsentation des Jahresberichts für 2018 am 29. Januar betonte. UMC versucht anscheinend, möglichst ungeschoren aus der Sache herauszukommen: Das Unternehmen UMC ist auf Kunden aus aller Welt angewiesen, auch aus den USA.

Es ist denkbar, dass auch die taiwanische Regierung Druck auf UMC ausübt: Die USA sind die Schutzmacht Taiwans, das nur 100 Kilometer vor dem chinesischen Festland liegt. Aus dieser Perspektive mag es wiederum kein Zufall sein, dass der chinesische Präsident Xi Jinping ausgerechnet jetzt Drohungen gegen Taiwan ausspricht. Der Handelskrieg der USA, zu dem auch harte Maßnahmen gegen andere chinesische IT-Firmen wie Huawei (siehe S. 16) und ZTE gehören, sorgt für große Unsicherheit. Außer zu politischen Konflikten könnte das auch zu Lieferengpässen und Preisschwankungen führen.

(ciw@ct.de) **ct**



Die USA werfen dem chinesischen DRAM-Hersteller Fujian Jinhua Industriespionage vor.

Bild: Fujian Jinhua Integrated Circuit



Bild: Daniel Karmann/dpa

Fahndung mit dem großen Netz

Kennzeichen-Scanner der Polizei sind teilweise unzulässig

Nummernschild-Scanner erfassen alle Kennzeichen und gleichen sie mit Fahndungslisten ab. Das Bundesverfassungsgericht hat diese Schleierfahndung nun deutlich eingeschränkt. Bayern verbessert die Fahndungsergebnisse mit intensiver Handarbeit.

Von Christiane Schulzki-Haddouti

Die Polizei setzt in mehreren Bundesländern Nummernschild-Scanner ein, um die Kennzeichen passierender Fahrzeuge automatisch mit verschiedenen Datenbanken abzugleichen. Betroffen sind stets alle Fahrzeuge, die eine solche Kontrollstelle passieren, Bayern liest beispielsweise 8,5 Millionen Kennzeichen pro Monat automatisch ein.

Diese Schleierfahndung in Bayern, Baden-Württemberg und Hessen ist nach

Beschlüssen des Bundesverfassungsgerichts von Anfang Februar (1 BvR 142/15, 1 BvR 2795/09, 1 BvR 3187/10) in Teilen verfassungswidrig. Damit ändert das Gericht seine bisherige Rechtsprechung.

Ein Kfz-Kennzeichenabgleich muss „auf den Schutz von Rechtsgütern von zumindest erheblichem Gewicht“ beschränkt werden, verlangt das Gericht. Es dürfen „jeweils nur die Fahndungsbestände zum Abgleich herangezogen werden, [...] die zur Abwehr der Gefahr geeignet sind“. Das Gericht hält dabei fest: „Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, [...] und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein.“

Bis Ende des Jahres 2019 müssen die Bundesländer nun nachbessern. Sie haben zu prüfen, für welche Straftatbestände ein Abgleich erfolgen darf. Bayern darf die Kennzeichenerfassung beispielsweise für den Grenzschutz, für den die Bundespolizei zuständig ist, nicht mehr einsetzen.

Hessen und Baden-Württemberg nutzen für den Datenabgleich die Sachfahndungsdaten des Schengen-Informationssystems, womit zunächst nicht nach dem Zweck der Kennzeichenkontrolle unterschieden wird. Umstritten ist, ob nach der Entscheidung auch dauerhafte Kennzeichenkontrollen für Dieselfahrverbote rechtswidrig wären, die ein aktueller Gesetzesentwurf im Bundestag vorsieht.

Fragliche Qualität

In der Praxis wird derzeit in verschiedenen Bundesländern ein mehrstufiges Filterverfahren praktiziert, an dessen Vorgehensweise sich im Grundsatz nichts ändern wird. Für Irritationen sorgte eine angeblich extrem hohe Fehlerquote. Das Online-Magazin BuzzFeed nannte nach Durchsicht mehrerer Anfragen in den Landtagen Fehlerquoten von 93 und 98 Prozent, in Bayern sollten es gar 99,8 Prozent sein.

Die Anlagen arbeiten laut Aussage des Herstellers Vitronic zur automatisierten Kennzeichenerkennung (AKE-Anlagen) aber mit einer Treffer-Genauigkeit von mehr als 96 Prozent, also mit nur 4 Prozent Fehlerquote. Die Zuordnung eines Kennzeichens zu einem Herkunftsland erfolgt über die Syntax des Kennzeichens, nicht über das Länderkennzeichen. Die Scanner lasen drei Prozent falsch ein, und konnten weniger als ein Prozent nicht automatisch zuordnen.

Probleme mit der Erkennung gibt es noch bei bestimmten Wetterlagen wie Starkregen, Schneefall und Nebel oder wenn das Kennzeichen nicht richtig angebracht oder verschmutzt ist. Fahrzeuggeschwindigkeit oder Dunkelheit spielten jedoch keine Rolle, erklärt Jan Krüger von Vitronic, der für das Marketing der AKE-Anlagen zuständig ist. Die Kennzeichen würden erfasst und in eine Textdatei umgewandelt, die dann von der Polizei ausgewertet werde.

Filterverfahren

Bayern setzt als Bundesland mit den meisten gescannten Kennzeichen 22 stationäre Anlagen sowie 6 mobile Anlagen ein. Bundesweit sind rund dreimal so viele Geräte im Einsatz. Nach Angaben des bayerischen Innenministeriums passieren rund 8,5 Millionen Fahrzeuge pro Monat die AKE-Anlagen der Bayerischen Polizei, also rund 283.000 Fahrzeuge pro Tag. Noch vor Ort wird die weit überwiegende Zahl der vom Heck der Fahrzeuge ausgelesenen Kennzeichen in den AKE-Anlagen

vollautomatisch ausgesondert und sofort unwiederbringlich gelöscht. Diese „Nichttreffer“ machen mehr als 99 Prozent der Ablesevorgänge aus.

Die Bilder von 60.000 Kennzeichen monatlich werden zur näheren Überprüfung an die Einsatzzentralen der Bayerischen Polizei übermittelt und visuell noch einmal überprüft. Dabei bleiben monatlich rund 850 „Echttreffer“ übrig, also tatsächliche Übereinstimmungen mit dem polizeilichen InPol-Fahndungsbestand. Solche Fahrzeuge werden anschließend von Polizeibeamten gestellt. Das betrifft also nur 1,4 Prozent der an die Einsatzzentralen übermittelten Kennzeichen und etwa 0,01 Prozent der von den AKE-Anlagen insgesamt gescannten Fahrzeuge. „Die Tatsache, dass bei der AKE mehr Datensätze an die Einsatzzentralen übermittelt werden, als sich letztlich als sogenannte ‚Echttreffer‘ herauskristalisieren, ist keine Folge mangelhafter Technik“, betont ein Sprecher des bayerischen Innenministeriums. „Wir haben unsere AKE-

Anlagen bewusst so eingestellt, dass zur Fahndung ausgeschriebene Kennzeichen so sicher wie möglich detektiert werden.“

Für Fahndungszwecke reichen also die vom Hersteller gelieferten 96 Prozent noch nicht aus. Hier soll die Überprüfung möglichst vollständig erfolgen und kein Kennzeichen darf durchrutschen. Deswegen werden die Anlagen gezielt unscharf gestellt: „Das bedeutet beispielsweise, dass Umlaute, I und 1 oder O und 0 nicht unterschieden und Leerzeichen, Trennstriche sowie Sonderzeichen entfernt werden“, erklärt das bayerische Innenministerium. Je wichtiger die Polizei die Suche nimmt, desto weitmaschiger stellt sie also die Auswertung ein.

Weite Maschen für viele Treffer

Der AKE-Fahndungsbestand selbst enthält die zur Fahndung ausgeschriebenen Kennzeichen sowohl mit als auch ohne Trennstrich. Die Abfrageroutine für die erfassten Kennzeichen mit dem Fahndungsbestand

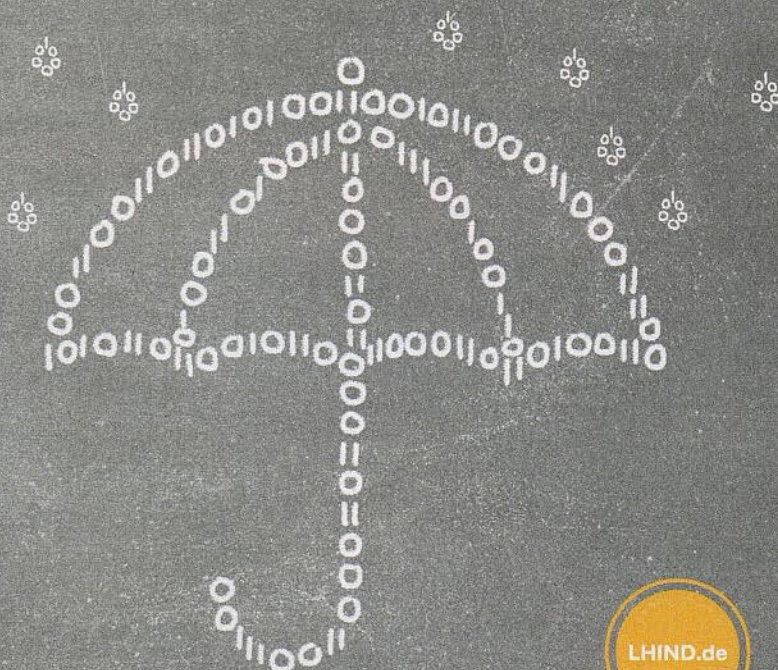
erfolgt in Bayern ohne Beachtung des Bindestrichs. „Ist beispielsweise das Augsburger Kennzeichen A-BX 000 zur Fahndung ausgeschrieben, meldet das System auch einen Treffer, wenn das Aschaffener Kennzeichen AB-X 000 erkannt wird. Gleiches gilt für ausländische Kennzeichen mit der alphanumerischen Zeichenfolge ABX000“, erklärt der Sprecher des bayerischen Innenministeriums.

Nachdem in den Einsatzzentralen das Bild des von den AKE-Anlagen erkannten Kennzeichens wie auch das tatsächlich ausgeschriebene Kennzeichen unmittelbar untereinander angezeigt werden, kann der überwiegende Anteil „unechter“ Treffer mit einem kurzen Blick als nicht relevant erkannt und sofort und unwiederbringlich gelöscht werden. Das bedeutet hohen personellen Aufwand. Diesen nimmt die Polizei aber bewusst in Kauf, damit ein zur Fahndung ausgeschriebenes Kennzeichen – beispielsweise einer Einbruchs- oder Schleuserbande – nicht unbemerkt durchschlüpfen kann. (uma@ct.de) **ct**

Sie sind
Cloud Spezialist
(m/w/divers)
und lassen Ihre
Kunden nicht im
Regen stehen?



**Lufthansa
Industry Solutions**

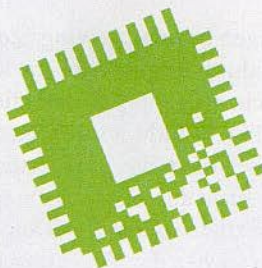


Kommen Sie an Bord:
www.lhind.de/cloud-jobs



Bit-Rauschen

Der Handelskrieg gegen China stört die IT-Branche



Apple, Intel, AMD, Nvidia, Qualcomm, TSMC, Samsung, Bosch – die Liste der IT-Firmen, deren Geschäfte unter Donald Trumps Attacken auf China leiden, wird immer länger. Und Intel hat endlich einen fast neuen Chef.

Von Christof Windeck

Viele internationale IT-Firmen haben in den vergangenen Wochen ihre (meistens guten) Ergebnisse für 2018 verkündet und dabei auch ihre (meistens bescheidenen) Prognosen für 2019 bekannt gegeben. Für die trüben Ausblicke wurden oft „schwierige makroökonomische Bedingungen“ verantwortlich gemacht. Mit diesem Euphemismus ist außer dem Brexit auch Donald Trumps Feldzug gegen China gemeint, wo die Geschäfte in der Folge immer schlechter laufen – das ist ja der Sinn der Attacke. Mal sehen, wie lange sich die Chefs der profitorientierten IT-Giganten das Gebaren der Republikaner noch zähneknirschend anschauen, bevor sie aufmucken.

Die Trump-Mannschaft steigert nicht nur mit Zöllen den Druck auf China, sondern setzt möglichst viele Daumenschrauben an. Sie sind Munition für bilaterale Verhandlungen. Der Vorwurf der (Industrie-)Spionage trifft Huawei und ZTE, aber auch weniger bekannte Namen wie die Videoüberwachungsexperten Dahua und Hikvision sowie die DRAM-Fab JICC (siehe S. 16 und 18). Als Kollateralschaden riskiert Trump Verstimmung in Taiwan – vielleicht ist es ihm ganz recht, wenn man sich dort ein bisschen vor der Schutzmacht fürchtet. Den trumpischen Ego-Feldzug dürften auch Südkorea, Singapur und Japan sorgenvoll beobachten, die sich vor Ort mit dem Giganten China arrangieren müssen.

AMD und Intel erwarten ein eher schwaches erstes Quartal, erst in der zweiten Jahreshälfte soll es aufwärts gehen. Das liegt auch an neuen Produkten, die

eben erst ab der Computex Anfang Juni zu haben sein werden: AMDs Zen-2-Prozessoren Epyc Rome und Ryzen 3000 (Matisse), Intels Xeon-SP Cascade Lake und später dann Ice Lake/Sunny Cove sowie Lakefield. AMD freut sich über 350 Millionen US-Dollar Nettogewinn im Jahr 2018, erwartet für 2019 aber nur einen Umsatzzuwachs im einstelligen Prozentbereich – nach 23 Prozent 2018.

AMD-CEO Lisa Su betonte bei der Präsentation der Ergebnisse am 29. Januar, man habe das Ziel des Epyc-Marktanteils im „mittleren einstelligen Bereich“ erreicht. Laut Mercury Research konnten die Epycs den Xeons 3,2 Prozent Marktanteil (nach Stückzahl) abnehmen.

Außerdem verkauft AMD recht viele Profi-Grafikkarten (Radeon Pro) und Rechenbeschleuniger (Radeon Instinct). Unter anderem verwendet sie Google für einen Game-Streaming-Service, von dem allerdings bisher nur ein US-Testlauf namens „Project Stream“ zu sehen war. Womöglich will Google damit Chromebooks und Android-Smartphones in preiswerte Gaming-Maschinen verwandeln, jedenfalls wenn die Netzanbindung schnell genug ist.



Intels neuer Chef Bob Swan war bis 2015 eBay-Finanzchef und davor unter anderem auch bei General Electric.

Die Epycs bescherten AMD bisher noch Verluste, unter anderem wegen der teuren Arbeiten am Zen 2 „Rome“. Doch immerhin bringen die Epycs und die Profi-GPUs schon 15 Prozent Umsatzanteil, Tendenz steigend. Wenn die 64-Kerner auf den Markt kommen, soll dann auch der Profit stimmen und die Kasse klingeln.

Neuer Intel-Chef

Seit dem 31. Januar ist Bob Swan der fast neue Intel-CEO. Er führt die Geschäfte ja schon seit Juni 2018 kommissarisch und war zuvor Finanzchef (CFO). Laut US-Wirtschaftsmedien hatte er Mitte 2018 noch nicht vor, sich als CEO zu bewerben. Doch nun will er Intel durch die Transformation vom PC-Zulieferer in eine „Data-centric Company“ führen. Prozessoren für Rechenzentren – sprich: Xeons – bringen fast die Hälfte des Gewinns ein, obwohl sie nicht einmal ein Drittel vom Umsatz ausmachen. Das Geschäft mit Rechenzentren ist also hochprofitabel und brummt, Umsatz (plus 21 Prozent) und Gewinn (plus 51 Prozent) wachsen deutlich schneller als bei den PC-Prozessoren (plus 9 respektive 10 Prozent).

Swan heuerte nach seinem betriebswirtschaftlichen Studium bei General Electric an und stieg dort in mehrere Führungspositionen auf. Nach Stationen bei Northrop Grumman und HP wurde er Finanzchef von eBay, wo er neun Jahre lang blieb. 2015 wechselte er zu einer Beteiligungsfirma und dann 2016 zu Intel. Bei technischen Entscheidungen wird er sich als Finanzexperte wohl eng mit den jeweiligen Vizepräsidenten abstimmen.

Den ersten Rang als weltweit umsatzstärkster Halbleiterhersteller hat Intel schon 2017 Jahren an Samsung abtreten müssen. Der Abstand auf die nächsten Verfolger ist dann aber groß. In der Branche setzt sich die Konzentration auf wenige Giganten immer weiter fort. Der McClean Report der Beratungsfirma IC Insights schätzt, dass 2018 die 50 größten Halbleiterfirmen 89 Prozent der gesamten Umsätze einsackten, die 514 Milliarden US-Dollar betrugen. Insgesamt wurden erstmals mehr als 1 Billion Halbleiterbauelemente verkauft. Dabei zählte IC Insights aber jede einzelne LED und jeden Schalttransistor mit. Die Stückzahlen sollen 2019 weiter steigen – fraglich ist aber, ob auch der Ertrag dann noch stimmt, wenn sich das Wirtschaftswachstum abkühlt. (ciw@ct.de) **ct**

Sicherheitslücken in Mainboard-Software

Die Hersteller von Mainboards liefern auf DVD nicht nur Treiber für Audio, Chipsatz und Netzwerk mit, sondern auch Windows-Software zum Übertakten, zum Überwachen von Lüfterdrehzahlen, Temperaturen und Spannungen sowie zum Konfigurieren von RGB-LED-Effekten. Diese Programme enthalten eigens entwickelte Treiber, weil für die genannten Funktionen ein direkter Zugriff auf die Hardware nötig ist. In den **Treibern von Asus und Gigabyte** hat der Sicherheitsforscher Diego Juarez von SecureAuth mehrere Sicherheitslücken aufgedeckt.

Die Treiber GLCKIo und Asusgio für die Asus-Software Aura Sync enthalten drei Schwachstellen (CVE-2018-18537, CVE-2018-18536, CVE-2018-18535) mit denen Angreifer höhere Rechte erlangen können. SecureAuth wies Asus erstmals im November 2017 auf die Lücken hin. Der Board-Hersteller veröffentlichte darauf im Mai 2018 eine neue Aura-Sync-Version, die jedoch nur eine der drei genannten Schwachstellen schließt. Ebenfalls betroffen

sind die Treiber GPCIDrv und GDrv der Tools Gigabyte App Center, Aorus Graphics Engine, Xtreme Gaming Engine und OC Guru II des Hardware-Herstellers Gigabyte. Diese enthalten vier Lücken (CVE-2018-19320, CVE-2018-19322, CVE-2018-19323, CVE-2018-19321), die unter anderem Zugriff auf Speicherbereiche von sicherheitskritischen Prozessen erlauben. Die Schwachstellen sind immer noch nicht behoben. (chh@ct.de)



Die RGB-LED-Software Aura Sync sorgt nicht nur für bunte Lichter, sondern bietet Angreifern auch Einfallstore.

Kurz & knapp: Hardware

Microsoft bietet einen **Windows-Patch mit aktualisierten Microcodes** für Intel-Prozessoren bis zurück zur ersten Core-i-Generation aus dem Jahr 2009 zum Download an (KB4465065). Diese schließen unter anderem CPU-Sicherheitslücken wie L1 Terminal Fault (L1TF).

Nvidia hat Version 6 der **Entwicklungsumgebung OptiX** für Raytracing-Anwendungen veröffentlicht. Sie verwendet für ausgewählte Berechnungen die RT-Kerne von Turing-Grafikchips sowie die Tensor-Kerne von Volta- und Turing-GPUs.

Für den **Grafik-Benchmark 3DMark** von UL Benchmarks gibt es ein Update. Dieses rüstet einen Funktionstest für die Kantenglättungsfunktion Deep Learning Super Sampling (DLSS) nach. Da diese die Tensor-Kerne von Turing-GPUs verwendet, funktioniert der Test derzeit nur mit Grafikkarten der Serie GeForce RTX 2000.

Microcode-Updates, OptiX 6 und 3DMark herunterladen: ct.de/yeeq

WIBU
SYSTEMS

Denken Sie an Softwareschutz?

Denken Sie an CodeMeter!

- Lizenzen in HW, SW und Cloud
- PCs, Mobile, Embedded, SPS und Mikrocontroller
- x86, ARM und PPC
- ERP, CRM und e-Commerce-Integration



30 YEARS 1989-2019
propelling your business to new heights



embeddedworld2019
Exhibition & Conference
... it's a smarter world

Treffen Sie uns: **Stand 4-360**

+49 721 931720
sales@wibu.com
www.wibu.com



**SECURITY
LICENSING**
PERFECTION IN PROTECTION

Raspberry-Pi-Industriemodul CM3+

Eine kompakte, robuste und länger lieferbare Variante des Raspberry Pi 3B+ zielt auf Embedded Systems.

Für den Einsatz beispielsweise in Steuerungsanlagen und Maschinen gibt es ab sofort das **Raspberry Pi Compute Module CM3+**. Es hat die Bauform eines Small-Outline-Speichermoduls (SO-DIMM) und passt in eine Steckfassung mit 200 Kontakten. Sämtliche Anschlüsse stellt dann das Carrier- oder I/O-Board bereit, auf dem das CM3+ steckt. Entwickler können das rund 120 Euro teure Compute Module IO Board V3 von der Raspberry Pi Foundation kaufen. Dazu gibt es billigere Alternativen wie das Waveshare Compute Module IO Board Plus für nur 50 Euro oder speziell ausgestattete I/O-Boards wie das Kontron Passepartout mit Secure Element und 24-Volt-Anschluss für Industriemaschinen. Ein fertiges Produkt mit einem Raspi-CM ist beispielsweise der Steuerungscomputer Kunbus Revolution Pi, der auf eine DIN-Hutschiene in einem Schaltschrank passt.

Im Vergleich zum Raspberry Pi 3B+ fehlt dem CM3+ Ethernet, WLAN und Bluetooth. Dafür ist – außer bei der billigeren Lite-Version – ein eMMC-Flash-Chip

mit 4, 8, 16 oder 32 GByte Kapazität aufgelötet. Das CM3+ Lite kostet unter 30 Euro, die 8-GByte-Version 32 Euro.

Die Raspberry Pi Foundation verspricht, das CM3+ bis mindestens 2026 zu liefern. Ein Zertifizierungsprogramm beim Dienstleister UL soll die Prüfung von Geräten mit CM3+ erleichtern. Diese dürfen das Logo „Powered by Raspberry Pi“ tragen, wenn sich der Hersteller dafür registriert. Die Vorgänger CM3, CM2 und CM1 sollen ab sofort nicht mehr für neue Entwicklungen eingesetzt werden, bleiben aber lieferbar. (ciw@ct.de)

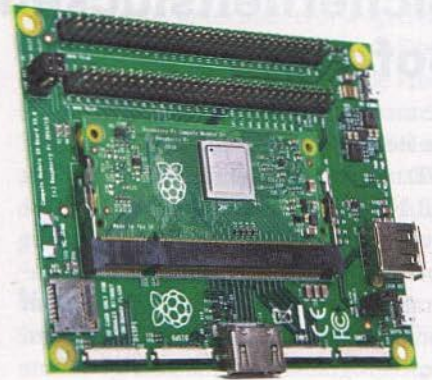


Bild: Raspberry Pi Foundation

Das Compute Module IO Board V3 macht die Anschlüsse des Raspi CM3+ nutzbar.

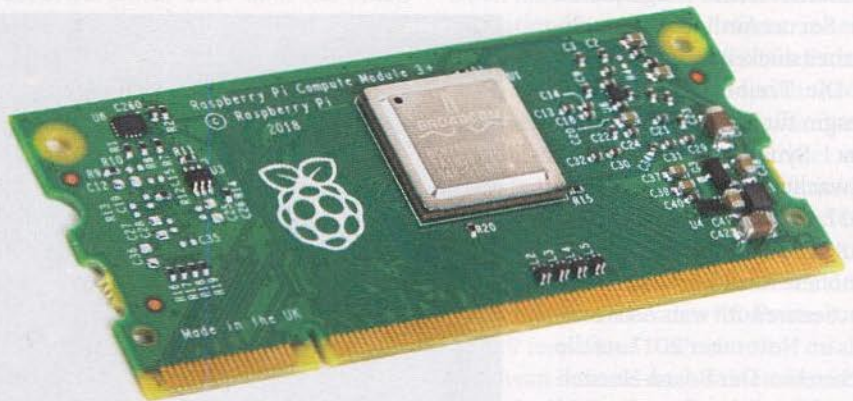


Bild: Raspberry Pi Foundation

Streifen-Raspi: Das Raspberry Pi Compute Module 3+ hat bis zu 32 GByte Flash-Speicher.

60-Euro-USB-Messmodul für Android und PC

Für Schüler und Bastler ist das Messmodul **Pocket Science Lab** mit USB-Anschluss gedacht. Es lässt sich mit einer Android-App oder mit einem Python-Programm unter anderem als Vierkanal-Oszilloskop mit bis zu 2 Megasamples/s nutzen. Außerdem arbeitet es als Spannungsmessgerät (16 Volt, 12 Bit), als Frequenzzähler, als Logikanalysator (4 Kanäle, 15 ns Auflösung), als programmierbare Spannungs- und Stromquelle sowie als Signalgenerator.

Über mehrere I²C-Schnittstellen lassen sich einfache Sensoren anschließen, auf PSLab.io finden sich Empfehlungen etwa zu einem passenden Mikrofon, einem Magnetfeld- und einem

Feuchtigkeitssensor. Außerdem ist es möglich, ein ESP8266-Modul aufzulöten, das WLAN und Bluetooth nachrüstet. (ciw@ct.de)



Bild: PSLab.io

Das Pocket Science Lab ist ein USB-Messgerät mit Android-App und Python-Software.

Embedded Systems

Die Libre Silicon Alliance (LSA) erarbeitet Werkzeuge zur Entwicklung von **Open-Source-Halbleitern**. Mit dem EDA-Entwurfswerkzeug QtFlow kann man bislang CMOS-Zellen mit 1 Mikrometer bearbeiten.

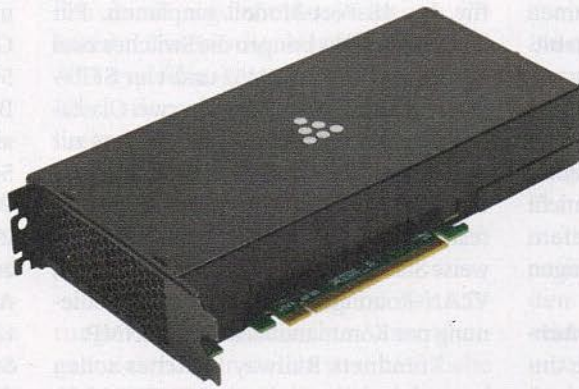
Der Hypervisor des Echtzeitbetriebssystems **PikeOS 4.2.2 ist nach Common Criteria EAL3+ zertifiziert**. Der PikeOS Separation Kernel (Microkernel) trennt Anwendungen sicher voneinander und ist für verschiedene CPU-Typen wie x86_64, ARMv7 und ARMv8 erhältlich.

Zotac kündigt robustere Varianten seiner **lüfterlosen Mini-PCs der Zbox-Reihe** an. Die Zbox-Pro-Serie startet mit fünf Varianten, drei mit Atom-Celerons und zwei mit Core-i-7000-CPU.

KI-Inferencing-Beschleuniger

Das israelische Start-up Habana Labs hat den **KI-Inferencing-Prozessor Goya HL-1000** vorgestellt. Die Beschleunigerkarte für den PCIe-Slot konkurriert mit Nvidias Tesla-Grafikkernen für Server und Intels zukünftigem Inferencing-Beschleuniger NNPL-i 1000. Der Beschleuniger erscheint mit 4, 8 und 16 GByte DDR-4-Speicher. Er soll mit ResNet-50, einem neuronalen Netz zur Bilderkennung, 15.000 Bilder pro Sekunde klassifizieren können. Dabei soll die Karte rund 100 Watt verbrauchen, die TDP gibt Habana allerdings mit 200 Watt an.

Habana liefert passend zur Karte einen Compiler namens „Synapse AI“, der ONNX versteht und Berechnungsgraphen direkt von Machine-Learning-Frameworks wie TensorFlow entgegennimmt, optimiert und auf der Karte ausführt. Die Topologie der Netzwerke



Die KI-Beschleunigerkarte Goya HL-1000 soll pro Sekunde 15.000 Bilder klassifizieren.

schränkt die Hardware laut Habana nicht ein: Goya soll sowohl Convolutional Networks als auch LSTMs beschleunigen können. Habana nennt einen Preis von etwa 2000 US-Dollar.

Im zweiten Quartal will Habana Labs auch einen fürs Training von neuronalen Netzen geeigneten Beschleuniger namens „Gaudi“ vorstellen. (pmk@ct.de)

Vorserien-Server mit Xeon-SP Cascade Lake und Optane-Speicher

Beim Hardware-Hersteller Supermicro läuft ein „Early Shipment Program“ für Server mit den kommenden „**Cascade Lake-SP**“-Xeons von Intel. Unternehmen können sich bei Supermicro bewerben, um einen solchen Server für Tests zu erhalten. Der Marktstart der neuen Xeon-SP-Baureihe wird zur Jahresmitte erwartet.

Wichtigster Vorteil der Cascade-Lake-(CLX)-Xeons ist das nichtflüchtige Optane DC

Memory, das zusammen mit normalen DRAM-DIMMs eingebaut werden kann. Damit lässt sich der Hauptspeicher etwa für In-Memory-Datenbanken auf mehrere Terabyte ausbauen. Vermutlich wird Intel auch DRAM-Module mit 16-Gbit-Chips unterstützen, um alternativ bis zu 6 TByte RAM bei Dual-Socket-Servern zu ermöglichen. Die Anzahl der CPU-Kerne wird auch bei Cascade Lake-SP nicht über 28 hinausgehen. (ciw@ct.de)

Neuer Mitspieler im Flash-Markt

Der taiwanische Produzent von NOR-Flash Macronix will in Zukunft auch **Flash-Chips auf NAND-Basis** herstellen. Laut einem Bericht von DigiTimes plant das Unternehmen Speicherchips mit 128 Gbit und 256 Gbit im 48- und 96-Layer-Design.

Laut CEO Miin Wu sollen sämtliche Ausgaben für Forschung und Entwicklung in das 3D-NAND-Projekt fließen; in diesem Jahr sollen es knapp 500 Millionen US-Dollar sein.

Macronix will die Kosten pro Bit mithilfe einer ungenannten neuartigen Architektur um rund 30 Prozent senken. Die Massenfertigung von 96-Layer-Flash soll 2021 starten, zum Zeitpunkt der 48-Layer-Fertigung gibt es noch keine Angaben. Macronix steigt jedoch zu einem eher ungünstigen Zeitpunkt in die NAND-Flash-Produktion ein: Marktforscher rechnen weiterhin mit sinkenden Preisen. (ll@ct.de)

Heiße Luft im Serverraum



Web-Thermometer von Wiesemann und Theis benachrichtigen Sie über E-Mail, wenn es im Serverraum zu warm wird.



wut.de/web-io

W&T

www.WuT.de

PoE+-Switches für zu Hause, Firmen und Fahrzeuge

Nur 60 Euro verlangt Zykel für seinen **PoE-Switch GS1005HP mit fünf Gigabit-Ports**; vier davon versorgen Netzwerkgeräte mit Energie (PoE+ mit max. 30 Watt, IEEE 802.3at). Die größere Variante GS1008HP mit acht Gigabit-PoE+-Ports kostet 90 Euro. Beide Switches sind nicht konfigurierbar (unmanaged) und liefern insgesamt maximal 60 Watt. So genügen die GS-Geräte für kleine Netze.

D-Link bietet seine **Layer-3-Switch-Serie DGS-3130** für mittlere und große Unternehmen an: Das kleinste Modell mit 24 Gigabit-Ethernet-Ports kostet rund 620 Euro, als PoE-Variante mit 370-Watt-Budget werden rund 930 Euro fällig. Wer mehr Anschlüsse benötigt, muss 1050 Euro beziehungsweise 1520 Euro mit PoE

für das 48-Port-Modell einplanen. Für schnelle Uplinks bringen die Switches zwei 10GBase-T-Ports (RJ45) und vier SFP+-Slots mit. Außerdem gehören zwei Glasfaser-Verteiler mit 24 und 48 SFP-Ports zur Serie. Zum Funktionsumfang zählt laut D-Link alles, was der Administrator von professionellen Switches erwartet, beispielsweise Stacking von maximal neun Geräten, VLAN-Routing, Spanning Tree und Bedienung per Kommandozeile oder SNMP.

Trendnets Railway Switches sollen besonders robust sein: Der TI-TPG80 ist ein **Gigabit-Ethernet-Switch mit acht PoE+-Ports**. Statt der üblichen RJ45-Raststecker nutzt der Switch M12-Schraubverbinder. Sie sollen besonders für industrielle Umgebungen mit hoher Feuchtigkeits-

und Staubbelastung geeignet sein. Das Gerät erfüllt laut Hersteller die Norm EN 50155, die elektronische Geräte für den Betrieb auf Schienenfahrzeugen zertifiziert. Der Switch arbeitet mit 24 bis 56 Volt. Am unteren Limit beträgt das PoE-Budget 100 Watt, bei 48 Volt sind es 200 Watt. Der TI-TPG80 kann Strom aus zwei unterschiedlichen Quellen beziehen. Außerdem hat er ein integriertes Relais (24 V / 1 A), das umschaltet, sobald der Strom an einer der beiden Quellen ausfällt. Der Switch kostet in den USA rund 740 Dollar. (amo@ct.de)



Die neuen Gigabit-Switches von Zykel mit fünf beziehungsweise acht Ports eignen sich für Heimnutzer oder kleine Unternehmen, die beispielsweise Access Points oder VOIP-Telefone mit Strom versorgen wollen.



Robust in der Bahn: Der TI-TPG80 von Trendnet taugt für Schienenfahrzeuge (EN 50155).

4,8 GBit/s und IoT fürs Firmen-WLAN

Ab April will Extreme Networks seine ExtremeMobility-500-Access-Points ausliefern: Sie funken über vier Antennen nach einem Entwurf für IEEE 802.11ax (Wi-Fi 6). So erreichen sie laut vorläufigem Datenblatt im 5-GHz-Band einen Summendurchsatz von bis zu 4,8 GBit/s brutto.



ExtremeMobility-Access-Points sollen dank Wi-Fi 6 auch Dinge des Internet of Things per WLAN ins Firmenetz holen.

Dafür müssen mehrere Clients parallel funken, die den **Betrieb über einen 160-MHz-Kanal und Multi-User-MIMO** beherrschen. Im 2,4-GHz-Band kommen die APs auf maximal 1,15 GBit/s brutto. Außerdem ist ein IoT-Funkmodul an Bord, das wahlweise Bluetooth 4.1 (BLE) oder LR-WPAN spricht (IEEE 802.15.4).

Die per Cloud steuerbaren APs beherrschen laut Hersteller alle bei Firmen-WLANs nötigen Funktionen inklusive der aktuellen WPA3-Verschlüsselung. Ausgerechnet drei wichtige 11ax-Erweiterungen (OFDMA, TWT und BSS Colouring/Spatial Re-use) sind im Datenblatt zum AP505i aber noch als kommende Funktion (Future) verzeichnet. Anfragen dazu und zur Verfügbarkeit hierzulande blieben bis Redaktionsschluss unbeantwortet. (ea@ct.de)

Access-Point mit IoT-Option

Lancom Systems erweitert seinen 2015 eingeführten Access-Point LN-830acn: Über den USB-Port kann man am neuen LN-830U einen Adapter für **ZigBee, Bluetooth Low Energy oder andere bei Smart Home und IoT** gebräuchliche Funksysteme betreiben. So soll der LN-830U eine langzeitstabilere Investition darstellen als APs mit integriertem IoT-Funkmodul.

Die sonstigen Daten der WLAN-Basis entsprechen denen des Vorgängers: simultaner Dualband-Betrieb mit zwei MIMO-Streams (Wi-Fi 4: IEEE 802.11n-300, Wi-Fi 5: 11ac-867), WPA2- und WPA3-Verschlüsselung (Personal/PSK und Enterprise/IEEE 802.1x), optionale Energieversorgung übers LAN-Kabel (IEEE 802.3af), optionale Steuerung über Lancom-Cloud (LMC). Der LN-830U ist ab sofort für 653 Euro erhältlich. (ea@ct.de)

Strike3: Jagd auf Navi-Störer

Ein EU-Projekt soll für mehr Störsicherheit bei GPS-/GNSS-Empfängern sorgen.

Empfänger von Satellitennavigationssystemen sind anfällig gegenüber Funkstörungen. Zweieinhalb Jahre lang hat ein internationales Projektteam mehrerer Firmen den Störsignalteppich erfasst und Wirkungen auf die Empfangsgeräte analysiert. In 23 Ländern unterhielten die Forscher 30 Mess-Stationen, und zwar an Orten, an denen es auf guten Empfang der schwachen Signale von Navigationssatelliten besonders ankommt, etwa an Flughäfen, Mautstellen, Kraftwerken und an Grenzübergängen.

Ende Januar wurde das insgesamt über drei Jahre laufende Strike3-Projekt der europäischen Satellitennavigationsagentur GSA beendet. Der Abschlussbericht der Langzeitstudie steht zwar noch aus, doch schon eine Teilauswertung vom November 2018 zeigt bereits 450.367 aufgezeichnete Störfälle, von denen rund 73.000 sogar zum Totalausfall von Satellitenempfängern führten. Die Dunkelziffer ist aufgrund der wenigen Mess-Stationen groß. Außer für die Navigation ist der korrekte Empfang auch für die Zeitsynchronisation in einigen Netzwerken wichtig, etwa beim Banking oder im Mobilfunk: Von GPS-, Galileo- oder Glonass-Daten hängen drei Viertel der kritischen Infrastrukturen ab. Schon jetzt verursachen Empfangsstörungen massiven Schaden.

59.453 aller in der Langzeitstudie beobachteten Totalausfälle wurden absicht-

lich durch sogenanntes Jamming verursacht. Die Forscher klassifizierten etwa 300 typische Jamming-Signalförmlichkeiten. Etliche der erfassten illegalen Störsender ließen sich aufgrund ihrer sehr individuellen Signalförmlichkeit trotz des arg lückenhaften Erfassungsnetzes sogar als Einzelgerät an mehreren Orten wiedererkennen.

Insgesamt überwiegen bei den Störungen aber unerwünschte Aussendungen elektrischer Geräte und natürliche Phänomene. So bewirken beispielsweise koronale Masseneruptionen auf der Sonne und Gewitter Ausfälle beim Empfang. Eine weitere Aufgabe des Strike3-Projektes lag darin, einen Teststandard für die Störsicherheit von GNSS-Empfängern zu entwickeln. Und: Mit der Daten-

sammlung sollen Geräteentwickler ihre Produkte robuster gegenüber Störsignalen machen.

Dass GNSS-Empfänger bereits jetzt unterschiedlich mit Empfangsproblemen umgehen, wurde bei exemplarischen Tests von GPS-Geräten für den Massenmarkt beziehungsweise für den professionellen Anwender deutlich. Ein Gerät für den Massenmarkt ermittelte auch bei schlechten Empfangsbedingungen noch eine Position, allerdings mit sehr großem Positionsfehler. Als Totalausfall macht sich das für den Benutzer nicht bemerkbar, solange eine Position angezeigt wird. Ein Profi-Gerät errechnete nur dann Positionen, wenn es Signale mit einem gewissen Mindeststörabstand empfing.

(mil@ct.de)



Illegale GPS-Störsender wie dieses in Autos sollen unter anderem die korrekte Erfassung von Mautstellendurchfahrten verhindern.



USB zu TCP/IP
INU-100

USB-Hub
IH-304

Seriell zu USB
SU-302

Die Systemlösung für industrieoptimierten Fernzugriff – flexibel, platzsparend, beliebig kombinierbar!

- **NEU** Isochroner USB Modus: Übertragung von Audio-Video Daten
- Fernzugriff auf USB-Geräte: virtuelle USB-Kabelverlängerung über das Netzwerk
 - In Kombination mit dem IH-304: Anzahl der anschließbaren USB-Geräte kostengünstig erweitern
 - In Kombination mit der SU-302: auch auf alle seriellen Geräte
- Störfest, robust und ausfallsicher
- bis zu 100 MB/s Datentransfer, Verbraucher via Relais schaltbar
- 5 Jahre Garantie, regelmäßige Software-Updates, technischer Support weltweit kostenlos, Made in Germany

SEH

Testprodukte anfordern!

SEH Computertechnik GmbH | Hotline: +49(0)521-94226-0 | E-Mail: info@seh.de | www.seh.de

Im Namen des anderen

Identitätsklau nimmt zu und wird raffinierter



Diebstahl und Missbrauch	Seite 28
Schutz vor Identitätsklau	Seite 32
Erste-Hilfe-Maßnahmen	Seite 36
Sicherheit der Dienste	Seite 38
Passwörter lokal checken	Seite 42

Ihre digitale Identität ist zum begehrten Angiffsziel geworden. Die Gefahr steigt, dass Fremde in Ihrem Namen auf Shopping-Tour gehen oder Ihre Daten illegal veröffentlichen. Doch wenn Sie die Methoden der Identitätsdiebe kennen, können Sie sich selber schützen.

Von Holger Bleich

Es war ein lang geplanter Urlaubstrip nach New York. Simone Peters freute sich darauf, ihren 33. Geburtstag zusammen mit ihrer besten Freundin im Big Apple zu feiern. Als sie am Flughafen ihren Pass zur Einreise überprüfen ließ, erschienen drei uniformierte Beamte: „Kommen Sie mit“, forderte einer sie auf. In einem Hinterzimmer sah sich Peters unvermittelt grimmig dreinschauenden, bewaffneten Polizisten gegenüber.

Später stellte sich heraus, dass die Bankerin ohne ihr Wissen auf einer US-Fahndungsliste gelandet war – jemand hatte ihre Identität digital dazu missbraucht, einen betrügerischen Online-Shop zu eröffnen und dort gefälschte Louis-Vuitton-Taschen zu verkaufen. Die Vorladungen gingen an eine Fake-Adresse, sodass Peters als flüchtig deklariert wurde. Erst einen Tag später hatte sich der Fall geklärt und Peters durfte einreisen.

Dies ist eine von vielen wahren Geschichten, die die Journalistin Tina Groll und der Polizist Cem Karakaya erzählen. Die beiden haben jüngst ein Buch veröffentlicht, in dem sie anhand konkreter Beispiele viele Facetten des Identitätsdiebstahls beleuchten [1]. Da geht es etwa um Stalker, die Facebook-Konten kapern, um den illegalen Handel mit ergaunerten persönlichen Daten, und vor allem um Warenbetrug, der die Opfer mitunter um viel Geld bringt.

Schwammiger Begriff

Der Klau, oder präziser gesagt: der Missbrauch von Identitätsdaten hat sich in den letzten Jahren zu einem massiven Problem entwickelt. Einer repräsentativen Befragung von PwC zufolge war bereits 2016 fast jeder Dritte in Deutschland

schon einmal Opfer eines Identitätsklaus. Je sechs Prozent berichteten, dass mit ihren Daten ein gefälschter Account angelegt wurde – etwa bei ebay oder Facebook –, oder dass die Kreditkartendaten gestohlen und missbraucht wurden. Drei von zehn der Betroffenen hatten demnach einen finanziellen Schaden erlitten (siehe Abbildung auf S. 31).

Zwar ist der Begriff Identitätsdiebstahl in aller Munde, doch was er genau beschreibt, bleibt oft schwammig. Es fehlt arglosen Konsumenten oft die Fantasie, sich vorzustellen, was böswillige Täter mit einigen wenigen privaten Informationen anfangen können – das muss nicht einmal ein Passwort sein. Deshalb ist vielen potenziellen Opfern nicht klar, welche Angriffsvektoren Täter nutzen, um an fremde Daten zu kommen.

Fiese Tricks

Der Journalist Richard Gutjahr berichtete einmal launisch in seinem Blog, wie er im Flughafen-Wartebereich genervt dem Handy-Gespräch eines Geschäftsmanns neben ihm zuhörte: „Offenbar war er gerade dabei, eine Limousine zu buchen. Irgendwann zückt er seinen Geldbeutel, beginnt damit, seine Kreditkartendaten vorzulesen. Reflexartig fahre ich die Tastatur meines iPads aus und tippe mit. Ziffer für Ziffer der Kartenummer, dann das Gültigkeitsdatum und die Prüfnummer. Warum ich das tue? Weil ich es kann.“

Gutjahr brachte es auf den Punkt: „Auf einmal wird mir klar, ich könnte jetzt weiß Gott was mit seinen Daten anstellen: einkaufen, Online-Konten bei eBay, Amazon oder Apple einrichten.“ Seinem Bericht zufolge beließ er es dabei, dem „Opfer“ seines Identitätsdiebstahls über den Druck- und Lieferservice der Deutschen Post eine Fun Card nach Hause zu schicken: „Bezahlt mit seiner Kreditkarte. Das musste sein.“

Hans-Joachim Henschel, Kriminalhauptkommissar am Landeskriminalamt (LKA) Niedersachsen, berichtete c't auf Anfrage von derzeit häufig gemeldeten Angriffsmethoden. Da wären beispielsweise die arglosen Nutzer von eBay und anderen Miet- oder Verkaufsplattformen. Von ihnen fordern Täter wahlweise als Käufer, Verkäufer oder Vermieter einen Echtheitsnachweis, etwa einen Scan des Personalausweises, eine Zulassungsbescheinigung, einen Mietvertrag oder einen Gehaltsnachweis. Diese Daten sammeln sie, um sie später selbst zu missbrauchen oder zu verkaufen.

Beliebt sei es derzeit, das Videoident-Verfahren bei Jobsuchenden zu missbrauchen. Die Täter schalten dafür gefakte Stellenangebote bekannter Unternehmen, beispielsweise Tchibo oder der Deutschen Bahn, und bauen deren Bewerbungsportale nach. Sie bringen die Jobsuchenden dazu, das Videoident-Verfahren einer Bank zu nutzen, um sich vorgeblich im Online-Bewerbungsverfahren zu authentifizieren. In Wirklichkeit bestätigen die Opfer hier der Bank, dass sie ein Konto eröffnen wollen.

Die Täter stellen sich beim Schriftverkehr zwischen Videoident-Verfahren, Bank und Jobsuchenden. Alle von der Bank benötigten Unterlagen werden über die Täter geleitet, sodass die beiden anderen Parteien nichts davon mitbekommen: „Der Jobsuchende wird dann hingehalten oder letztendlich doch nicht ‚eingestellt‘. Dass in seinem Namen ein Bankkonto existiert, bemerkt er nicht oder erst, wenn die polizeilichen Ermittlungen gegen ihn laufen. Bereits wenige Tage und Wochen reichen den Tätern, um ein Konto zum Beispiel für Geldwäsche zu missbrauchen“, beschreibt das LKA.

Geweckte Begehrlichkeiten

Je mehr Geschäfte wir online abwickeln, je mehr Prozesse aus der Offline-Welt sich über unsere digitale Identität im Internet erledigen lassen, desto begehrenswerter werden die zugehörigen Daten. Und Kriminelle entwickeln immer ausgefeiltere Methoden, um sie zu ergattern. Sicherheitsbehörden mahnen derzeit verstärkt, dieses Problem ernstzunehmen. Die European Union Agency for Network and Information Security (ENISA) etwa kategorisierte in ihrem Jahresbericht die Deliktgruppe „Identity Theft“ sowohl 2018 als auch ganz aktuell 2019 als „increasing risk“.

Das Bundeskriminalamt (BKA) spricht im aktuellen „Bundeslagebild Cybercrime“ (9/2018) von einem „gängigen und lukrativen Geschäftsmodell“. Allerdings ändern dem Bericht zufolge die Diebe offenbar zurzeit ihre Methoden, mit denen sie an Identitätsdaten von Personen kommen. Sowohl das BKA als auch Europol beobachten einen Rückgang der gemeldeten Phishing-Attacken. An deren Stelle traten vermehrt „Datenabflüsse bei großen Dienstleistern“, wie es das BKA nennt. Gemeint sind Einbrüche (Data-Breaches) bei Online-Shops, Webdiensten oder Auskunftsteilen mit dem Ziel, persönliche Informationen wie Adressen und Kreditkartennummern, vor allem aber Zugangsdaten für Nutzerkonten zu erbeuten.

Kombinationen aus Benutzernamen und Passwörtern, die sogenannten Credentials, stehen im Zentrum der Begehrlichkeiten. Eine der Kombinationen genügt Kriminellen oft als Startpunkt, um sich damit Zugang zu allen möglichen Accounts einer Person zu verschaffen und damit ihre digitale Identität komplett zu kapern [2], beispielsweise über Passwort-Recovery-Mechanismen.

Eine große Verantwortung kommt den Betreibern der Dienste zu. Sie regulieren den Einlass zu ihren Plattformen und stehen deshalb in der Pflicht, die dazu nötigen Credentials einbruchssicher zu verwalten. Ein noch so kryptisches Passwort hilft dem Nutzer wenig, wenn es im Klartext bei der Gegenstelle abgegriffen

werden kann. Und genau da liegt einiges im Argen, wie der Artikel ab Seite 38 beschreibt. Dort geben wir Hinweise darauf, wie Sie erkennen können, welchem Dienst Sie vertrauen können und welchem besser nicht.

Ab Seite 32 zeigen wir Ihnen, mit welchen Methoden Sie das Risiko Identitätsdiebstahl minimieren können. Unter anderem gilt es, sich wo immer angeboten neben dem Passwort mit einem zweiten Merkmal (Token) zu authentifizieren. Fast alle großen, wichtigen Anbieter bieten diese zusätzliche Schutzschicht mittlerweile an, die dem besonders sensiblen Online-Banking entlehnt ist. Doch auch hier gilt es, sich auf den Stand zu bringen: Je mehr sich die Zwei-

Identitätsklau rechtlich gesehen

Nicolas Maekeler

Aus juristischer Perspektive wird die digitale Identität eigentlich nicht gestohlen, denn anders als bei einem Diebstahl kann der Betroffene seine Daten normalerweise weiterhin selbst verwenden. Präziserweise müsste man daher eher von Identitätsmissbrauch reden. Im Strafgesetzbuch (StGB) findet sich – anders als im US-Recht – kein mit „Identitätsdiebstahl“ betitelter spezieller Straftatbestand.

Vielmehr können durch den Missbrauch des eigenen Namens oder anderer persönlicher Daten durch unbefugte Dritte eine Vielzahl unterschiedlicher Straftatbestände verwirklicht sein und werden. Gegen welche Gesetze ein Täter verstößt, hängt folglich davon ab, wie er sich die Daten verschafft und was er mit ihnen anstellt. Allen verschiedenen Formen des Identitätsdiebstahls mit den bestehenden Mitteln des Strafrechts beizukommen, ist deshalb schwierig.

Im Deliktbereich Computerkriminalität stellen die Paragraphen 202a bis c StGB verschiedene Formen der illegalen Beschaffung von Daten unter Strafe. Mit einer Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe muss etwa rechnen, wer sich oder einem anderen – beispielsweise mittels Key-Logging-Trojaner oder Backdoor – unbefugt Zugang zu beson-

ders gesicherten Daten verschafft. Auch das mit technischen Mitteln realisierte Abfangen von Daten aus einer nicht-öffentlichen Datenverbindung – beispielsweise mittels Sniffing-Software – ist strafbar. Auch wer solche Taten vorbereitet, indem er die benötigte Software herstellt, sich verschafft oder verkauft, verstößt gegen die Rechtsordnung.

Phishing fällt nicht in diese Kategorie, da hier die Daten vom Opfer selbst herausgegeben werden und nicht besonders gesichert sind. Werden abgegriffene Daten allerdings etwa dazu benutzt, Waren unter fremden Namen in einem Online-Shop zu bestellen und die Lieferung umzuleiten, dann liegt ohnehin ein Warenkreditbetrug, aber auch ein Computerbetrug nach Paragraph 263a StGB vor. Daneben greift in einem solchen Fall auch der Paragraph 229 StGB („Fälschung beweiserheblicher Daten“). Viele Juristen sehen diesen Straftatbestand bereits erfüllt, wenn die Anmeldung eines Accounts unter falschen Personalien erfolgt – zumindest soweit Nutzungsbedingungen akzeptiert werden müssen. In beiden Fällen sieht das Gesetz eine Freiheitsstrafe von bis zu 5 Jahren oder eine Geldstrafe vor.

Toxisches Doxing

Auch die Weitergabe, der Verkauf oder

die Veröffentlichung (Doxing) von gesammelten persönlichen Daten ist rechtswidrig. Im sogenannten Nebenstrafrecht stellt Paragraph 42 des neuen Bundesdatenschutzgesetzes (BDSG) unter anderem die gewerbsmäßige Weitergabe und das unberechtigte Veröffentlichung personenbezogener Daten mit Schädigungsabsicht unter Strafe. Diese Norm dürfte beispielsweise im Fall der massenhaften Veröffentlichung privater Informationen von Politikern und Prominenten durch den 20-jährigen Schüler aus Hessen im Dezember 2018 greifen.

Wenn in Fällen wie diesem der Täter identifiziert wurde, können Geschädigte auch zivilrechtlich gegen ihn vorgehen. So sind nicht nur Unterlassungsansprüche denkbar, sondern sie können auch Schadensersatz in Form von Schmerzensgeld verlangen – wegen der Verletzung ihres allgemeinen Persönlichkeitsrechts. So hat etwa das Landgericht Memmingen einem 12-jährigen Cybermobbing-Opfer ein Schmerzensgeld in Höhe von 1500 Euro zugesprochen (Az. 21 O 1761/13). In diesem Fall hatte der Täter unter anderem ein neues Facebook-Profil mit dem Namen des Opfers angelegt und dort gefälschte Postings platziert, welche den Schüler als homosexuell, gewalttätig und pädophil erscheinen ließen.

Faktor-Authentifizierung durchsetzt, desto intensiver werden die Bemühungen von Kriminellen, auch diese Barriere auszutricksen.

Als ein wenig löchriger Schutz gilt beispielsweise bereits heute die Authentifizierung mit einer via SMS ans Handy gesendeten PIN: Angreifer missbrauchen die Rufnummernportierung der Mobilfunk-Provider, um eine Nummer einer anderen SIM-Karte zuzuordnen. Sie rufen dazu bei dem Mobilfunkanbieter an und überzeugen den Support-Mitarbeiter, eine Portierung vorzunehmen. Dabei nutzen die Angreifer Social Engineering, spionieren also das persönliche Umfeld des Opfers aus, um dessen Identität vortäuschen zu können.

In Deutschland sind erst wenige solcher Taten bekannt. Dagegen passiert in den USA der „Port-out Scam“ (auch bekannt als SIM-Swapping) inzwischen regelmäßig. In einem besonders spektakulären Fall hat ein 20-jähriger Student aus Kalifornien fünf Millionen US-Dollar an Kryptogeld durch SIM-Swapping gestohlen und muss dafür nun für zehn Jahre ins Gefängnis. Er hatte SIM-Karten von rund 40 Opfern gekapert und dadurch Zugriff auf Accounts erlangt, um sich schließlich von dort aus Zugang zu Kryptogeldbörsen der Opfer zu verschaffen.

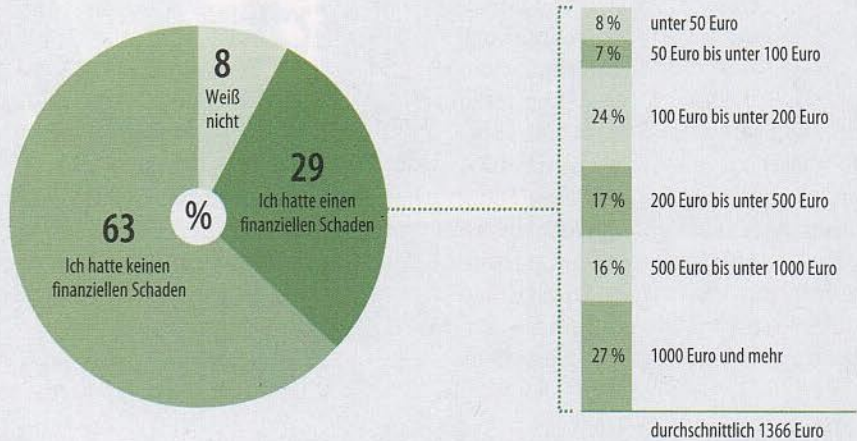
Achtung Fake-Accounts

Besonders leicht machen es Kriminellen jenen Nutzern, die allzu freizügig persönliche Daten und Identifikationsmerkmale in sozialen Medien veröffentlichen. Das Sicherheitsunternehmen Eset warnte jüngst davor, dass Social-Media-Profilen von Privatpersonen zunehmend ins Visier geraten. „Der Identitätsdiebstahl erfolgt automatisiert“, erläuterte Thomas Uhlemann von Eset: „Skripte scannen ohne menschliches Zutun die Social-Media-Plattformen nach geeigneten Profilen, um dann persönliche Bilder und Account-Informationen abzugreifen.“ Danach werden mit diesen Informationen – ebenfalls vollautomatisiert – neue Accounts auf den Plattformen angelegt.

Diese Fake-Accounts nutzen die Kriminellen, um neue Opfer anzulocken. Sie erkennen nicht, dass sie sich auf einem gefälschten Profil befinden und tappen in die Falle. So werden sie beispielsweise zu Betrugsopfern oder laden über den Klick auf einen harmlos erscheinenden Shortlink im Fake-Profil unwissentlich Schadsoftware auf ihren Rechner.

Schäden durch Identitätsklau

2016 war fast jeder dritte Bundesbürger schon einmal Opfer. 29% der Opfer erlitten überdies finanziellen Schaden.



Quelle: PwC

In Deutschland grassiert seit Längerem die „PIN-Code-Masche“: Mit einer gefakten Facebook-Identität schreibt der Täter Freunde des echten Account-Inhabers per Messenger an und bittet sie aus irgendwelchen dringenden Gründen um ihre Mobilfunknummern. Kurz darauf erhalten die Opfer eine SMS mit einem Bestätigungscode. Der „Freund“ bittet sie um den Code, der in Wirklichkeit ein Bezahl-Passwort ist, das er gleich einsetzt: Den Schaden hat das Opfer, denn es wird über seine Mobilfunkrechnung (mit Zeitverzug) abgerechnet.

Besonders perfide an dieser Masche ist, dass sie für die Opfer oft unentdeckt bleibt. „Die Geschädigten gehen oft davon aus, dass der eigene Account gehackt wurde. Oft auch, weil die Facebook-Freunde das so vermuten und dem Geschädigten so vermitteln. Dass es eine Kopie war, die inzwischen vielleicht schon wieder gelöscht wurde, wurde nicht bemerkt“, erklärt Hans-Joachim Henschel vom LKA Niedersachsen.

Wer den Verdacht hat, Opfer eines Identitätsdiebstahls zu sein, sollte unbedingt aktiv werden. Im Artikel auf Seite 36 haben wir Erste-Hilfe-Maßnahmen zusammengestellt, die eine schnelle Reaktion erleichtern. Neben technischen Eingriffen steht auch der Gang zur Polizei an. Genau wie die Kollegen vom BKA in ihrem Lagebild 2017 geht auch Henschel von einer hohen Dunkelziffer aus, weil eben viele Geschädigte – oft aus Scham – Strafanzeigen scheuen.

Dabei zeigt gerade ein aktueller, besonders spektakulärer Fund, dass längst nicht immer der Nutzer die Schuld trägt: Der Sicherheitsexperte Troy Hunt machte im Untergrund eine Sammlung an gehackten Onlinekonten mit über einer Milliarde Kombinationen aus Anmeldenamen und Passwörtern ausfindig. Kurz nach dem Fund dieser „Collection #1“ tauchten weitere Sammlungen „Collection #2 bis #5“ auf. Die fast 700 GByte großen Dateien umfassen Sammlungen von 2,2 Milliarden Onlinekonten, darunter Mail-Adressen und Passwörter [3].

Auf haveibeenpwned.com lässt sich checken, ob eigene Credentials in dem Fundus auftauchen. Alternativ kann man dort eine sortierte Liste mit Hashes von Passwörtern aus Hacks und Leaks herunterladen, um die eigenen Passwörter nicht durchs Web übertragen zu müssen. Die Kollegin Pina Merkert hat ein Python-Tool entwickelt, mit dem Sie diese Liste trotz ihrer Größe (25 GByte) in wenigen Millisekunden durchsuchen können. Eine Anleitung finden Sie auf Seite 42.

(hob@ct.de) **ct**

Literatur

- [1] Tina Groll, Cem Karakaya, Die Cyber-Profis: Lassen Sie Ihre Identität nicht unbeaufsichtigt, Ariston-Verlag, 2018
- [2] Axel Kossel, Risiko Identitätsklau, Wenn Geld und guter Ruf in Gefahr geraten, c't 24/2012, S. 132
- [3] Fabian A. Scherschel, Der Hacker-Hunter, Troy Hunt und der riesige Passwort-Fund „Collection #1 bis #5“, c't 4/2019, S. 16



Finger weg von meinen Daten!

Wie Sie Ihre digitale Identität schützen

Schützen Sie Ihre digitale Identität – sie ist ein wertvolles Gut! Mit einigen gezielten Maßnahmen und Strategien können Sie das Risiko, Opfer von Identitätsmissbrauch zu werden, deutlich reduzieren und dafür sorgen, dass sich der Schaden im Fall der Fälle in Grenzen hält.

Von Ronald Eikenberg

Es gibt zwei Arten von Menschen: Die einen wurden Opfer von Identitätsdiebstahl, die anderen werden es noch. Die gute Nachricht ist, dass Sie wenig zu befürchten haben, wenn Sie

einige grundlegende Tipps befolgen. Damit mit der Sicherheit des Hundefutter-Shops oder des Gaming-Forums nicht auch die Sicherheit Ihrer gesamten digitalen Identität steht und fällt, sollten Sie dort so wenig Daten hinterlassen, wie nur irgendwie möglich. Im Idealfall verzichten Sie auf eine Registrierung; in vielen Shops kann man schließlich auch als Gast bestellen.

Wenn eine Anmeldung verlangt wird, geben Sie ein Passwort an, das nur dort zum Einsatz kommt. Ein solches ist für einen Angreifer nämlich nahezu wertlos, nachdem er es erbeutet hat. Denn er kann damit nur etwas anfangen, wenn es auch bei anderen Diensten passt. Am besten nutzen Sie einen Passwort-Manager wie KeePass oder LastPass. Damit können Sie für jede Gelegenheit ein neues Passwort wie LXeGqzhiTg generieren. Zugegeben,

das kann man sich schwer merken – das nimmt Ihnen jedoch der Passwort-Manager ab. Wenn Sie das konsequent durchziehen und für jeden Dienst ein anderes Passwort einsetzen, dann können Sie sich bei dem nächsten Passwort-Leak entspannt zurücklehnen.

Wenn Sie Ihre Passwörter nicht einem digitalen Manager anvertrauen möchten, dann können Sie ganz altmodisch Zettel und Stift verwenden. Verwahren Sie den Zettel an einem sicheren Ort, etwa in Ihrem Portemonnaie, und legen Sie eine Kopie zu Ihren wichtigsten Unterlagen – am besten in einen feuerfesten Tresor. Wenn Sie auf Nummer sicher gehen wollen, können Sie sich ein Grundpasswort wie JRaJ6wUGTo überlegen, das Sie zum Bestandteil aller Passwörter machen – jedoch nicht mit auf den Zettel schreiben. Das ist quasi das Master-Passwort für Ihren Passwort-Manager auf Papier.

Eine beliebte Methode des Passwort-Managements kommt ganz ohne Software und Papier aus: Denken Sie sich eine Methode aus, um im Kopf aus einem Grundpasswort und dem Namen der Seite, bei der Sie sich anmelden möchten, ein Passwort zu generieren. Sie können zum Beispiel den ersten und letzten Buchstaben des Dienstes vorne und die Anzahl der Buchstaben seines Namens hinten an das Grundpasswort anhängen. Aus dem Grundpasswort JRaJ6wUGTo wird im Fall

von eBay: eyJRaJ6wUGTo4. Je individueller Ihre persönliche Methode ist, desto besser.

Passwort vergessen

Hat es ein Angreifer gezielt auf Sie abgesehen, wird er nicht lange probieren, das Passwort zu erraten. Damit kommt er bei Online-Diensten viel zu langsam voran. Zudem hat er wahrscheinlich nur eine begrenzte Anzahl an Fehlversuchen. Stattdessen sucht der Eindringling in spe nach anderen Wegen, in Ihren Account einzusteigen. Ein beliebter Weg sind Passwort-Recovery-Mechanismen. Oft ist diese Hintertür nur mit Informationen gesichert, die sich der Angreifer leicht aus sozialen Netzwerken ziehen kann – etwa dem Mädchennamen Ihrer Mutter (siehe S. 38).

Bei Passwort-Fragen gilt daher: Lügen Sie, bis sich die Balken biegen! Die einzige Einschränkung ist, dass Sie sich hinterher noch an die Lügen erinnern müssen, damit Sie im Fall der Fälle das Passwort zurücksetzen können. Machen Sie sich also am besten Notizen. Eine weitere Variante wäre, auch hier wieder einen individuellen Teil in die Antworten einfließen zu lassen: Statt in „Hannover“ wurden Sie also etwa in „eyHannover4“ geboren, wenn Sie eBay danach fragt.

Und wenn Sie schon mal in den Einstellungen Ihrer Accounts sind, sollten Sie dafür sorgen, dass überall valide Notfall-Kontaktinformationen hinterlegt sind. Falls ein Angreifer in Ihren Account eingestiegen ist, können Sie darüber mit etwas Glück die Kontrolle über Ihren Zugang zurückgewinnen.

Faktor zwei

Eine weitere wichtige Schutzbarriere für Ihre Online-Accounts ist die Zwei-Faktor-Authentifizierung (2FA). Ist sie eingeschaltet, benötigen Sie beim ersten Login auf einem Gerät neben Nutzernamen und Passwort noch einen einmalig gültigen Code. Diesen schickt Ihnen der jeweilige Dienst etwa per SMS aufs Handy. Noch sicherer sind die 2FA-Verfahren TOTP und HOTP, bei denen der Code lokal generiert wird, zum Beispiel von der Smartphone-App Google Authenticator oder einem Hardware-Token wie dem YubiKey.

2FA sorgt dafür, dass Ihr Account auch dann noch geschützt ist, wenn Ihre Zugangsdaten einem Online-Angreifer in die Hände fallen: Versucht sich ein solcher mit Ihren Daten einzuloggen, scheitert er daran, dass er den Einmalcode nicht emp-

Von HPI Identity Leak Checker <sec-checker-admin@hpi.de> Antworten · Allen antworten · Weiterleiten · Archivieren · Junk · Löschen · Mehr

Betreff: Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

An: [E-Mail-Adresse]

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse [E-Mail-Adresse] taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf. Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer
Unknown (Collection #1-5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–
Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannt								
badoo.com	Mär. 2016		122.495.418	Betroffen	Betroffen	Betroffen	–	–
Unknown (Zoosk.com)	Mär. 2013		54.103.990	Betroffen	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–

Der Identity Leak Checker verrät Ihnen, welche Ihrer persönlichen Daten bereits im Darknet kursieren.

fangen kann. Da SMS ein unsicherer Übertragungskanal ist, sollten Sie möglichst ein anderes 2FA-Verfahren wählen. Wenn Sie keine andere Wahl haben, ist die SMS-Übertragung aber immer noch besser, als ganz auf einen zweiten Faktor zu verzichten.

Die Zwei-Faktor-Authentifizierung kann Ihnen aber auch zum Verhängnis werden: wenn sich etwa Ihre Handynummer ändert oder Sie Ihr Smartphone verlieren, auf dem sich die Authenticator-App befindet. Wenn Sie keine Vorsorge-maßnahmen treffen, sind Sie dann von Ihren Accounts ausgesperrt. Falls Sie 2FA per SMS oder Anruf nutzen, müssen Sie die in den Accounts hinterlegten Rufnummern rechtzeitig ändern. Es ist eine gute Idee, mehrere 2FA-Methoden einzurichten, sofern der jeweilige Dienst dies zulässt. Dann können Sie im Fall der Fälle noch auf die zweite Methode zurückgreifen, falls die erste versagt.

Besonders große Sorgfalt sollten Sie bei der Absicherung Ihres Mail-Kontos an den Tag legen. Es ist quasi der General-schlüssel zu Ihrer digitalen Identität. Wer darauf zugreifen kann, der kann sich auch zu allen anderen Diensten weiterhangeln, die Sie mit Ihrer Mail-Adresse nutzen – ganz einfach über die Passwort-vergessen-Funktion.

Zwei-Faktor-Authentifizierung ist für den Mail-Account daher Pflicht. Wenn möglich, sollten Sie zudem von Zeit zu Zeit einen Blick auf die letzten Kontozugriffe und aktive Sitzungen werfen. Bei Google

finden Sie über ct.de/yw2w eine Übersicht. So können Sie stille Mitleser überführen, die zum Beispiel eine Browser-Sitzung auf einem anderen Rechner nutzen, die Sie nicht explizit beendet haben.

Passwörter prüfen

Um herauszufinden, ob Ihre Daten bereits im Darknet gehandelt werden, können Sie die Dienste Have I Been Pwned (HIBP) des Sicherheitsexperten Troy Hunt und den Identity Leak Checker des Hasso-Plattner-Instituts nutzen (siehe ct.de/yw2w). Beide Dienste greifen auf Datenbanken zu, in denen Milliarden gehackte Accounts gelistet sind. Wenn Sie dort eine Mail-Adresse eingeben, erfahren Sie, ob und meist auch bei welcher Gelegenheit Ihre Daten von Cyber-Ganoven abgegriffen wurden. Zudem informieren Sie die Dienste in vielen Fällen darüber, welche Art von Daten betroffen sind – also etwa, ob neben der Mail-Adresse auch ein Passwort oder gar Zahlungsdaten kopiert wurden.

HIBP zeigt Ihnen das Suchergebnis direkt im Browser an, der Identity Leak Checker verschickt seine ausführliche Auswertung per Mail. Die Dienste können zwar bestätigen, dass ein Account betroffen ist. Werden sie nicht fündig, bedeutet das jedoch nicht zwangsläufig, dass Ihre Accounts bisher von Hackern verschont wurden – die Datenbanken kennen zwar sehr viele, jedoch bei Weitem nicht alle Daten-Leaks. Bei HIBP können Sie unter „Notify me“ Ihre Mail-Adresse hinterlas-



Achtung, Achtung: Die Chrome-Erweiterung Password Checkup schlägt Alarm, wenn man kompromittierte Passwörter nutzt.

sen, um eine Alarm-Mail zu erhalten, wenn Sie von einem neuen Leak betroffen sind.

Ebenfalls von Troy Hunt wird Pwned Passwords (siehe ct.de/yw2w) betrieben. Die Seite kennt über 550 Millionen Passwörter, die im Darknet gehandelt werden. Wenn Sie dort Ihr Passwort eingeben, erfahren Sie, ob es bereits in einschlägigen Kreisen kursiert. In diesem Fall sind Sie gut damit beraten, es zu ändern. Grundsätzlich sollten Sie Ihre Kennwörter niemals auf irgendwelchen Webseiten eingeben, die nicht zu dem Dienst gehören, zu dem das Passwort passt. Pwned Passwords ist eine seltene Ausnahme, da die Site zum einen von einem renommierten Sicherheitsexperten betrieben wird und er zum anderen nachvollziehbar dokumentiert, dass die eingetippten Passwörter niemals an seine Server übertragen werden.

Hunt hat einen Verschleierungsmechanismus entwickelt, der verhindert, dass Ihr Passwort übertragen wird: Die Website hasht das Passwort lokal im Browser mit SHA-1 und schickt lediglich die ersten fünf der 40 Stellen des Hashes an den Server. Dieser liefert daraufhin die Hashes aller kursierenden Passwörter zurück, die mit diesen fünf Stellen beginnen. Schließlich überprüft ein JavaScript lokal im Browser, ob sich der Hash des eingegebenen Passworts auf der vom Server gelieferten Liste befindet. Wenn Ihnen das nicht geheuer ist, können Sie die 25 GByte große Liste der Passwort-Hashes herunterladen und selbst durchsuchen. Wir haben zu diesem Zweck ein kleines

Python-Skript entwickelt, das Sie auf Seite 42 finden.

Inzwischen befragen auch einige Passwort-Manager wie 1Password auf Wunsch die riesige Datenbank von Troy Hunt. So können Sie leicht herausfinden, ob die von Ihnen genutzten Passwörter von einem Leak betroffen sind. Unter ct.de/yw2w finden Sie zudem eine Anleitung, wie Sie die von KeePass verwalteten Kennwörter in einem Rutsch abfragen können. Ganz frisch ist die von Google angebotene Chrome-Erweiterung Password Checkup. Sie merkt sich Zugangsdaten, die Sie auf Webseiten einsetzen, und gibt Alarm, wenn sie auf ein kompromittiertes Passwort stößt. Ähnlich wie bei Pwned Passwords kommt dabei ein Verschleierungsverfahren zum Einsatz, das gewährleisten soll, dass die Sicherheit Ihrer Zugangsdaten nicht beeinträchtigt wird. In einem ersten Test zeigte die Erweiterung einen unübersehbaren Warnhinweis an, nachdem wir ein bekanntermaßen unsicheres Passwort wie „geheim“ in das Login-Formular einer Webseite eingetippt hatten.

Stalke Dich selbst

Begeben Sie sich in die Position eines Fremden, der so viel wie möglich über Sie herausfinden will. Durchforsten Sie das Netz nach Ihrem Namen mit bekannten und weniger bekannten Suchmaschinen wie Google, Bing, Qwant und DuckDuck-

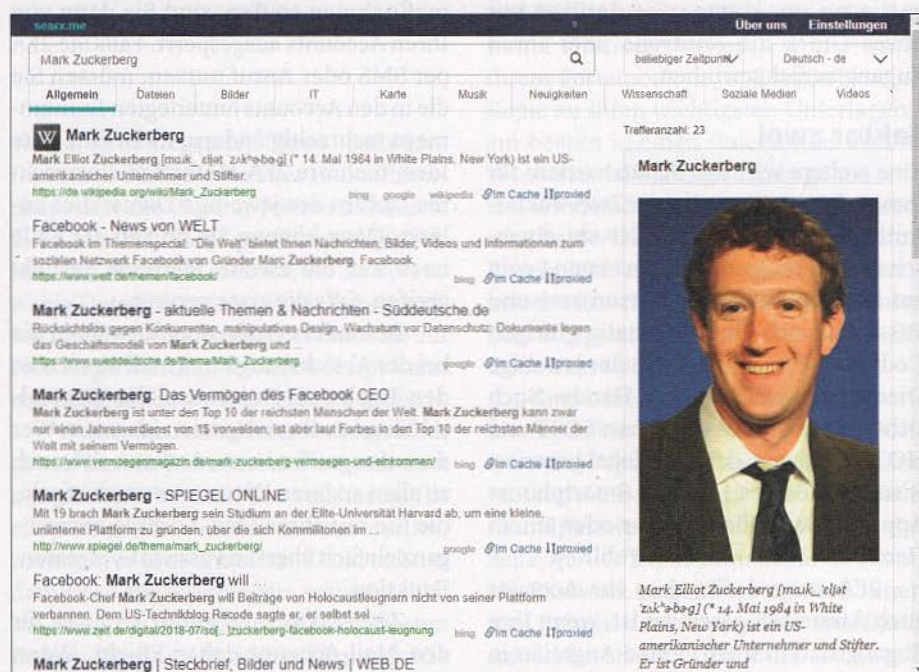
Go. Nützlich sind auch Meta-Suchdienste wie Searx.me, welche die Suchergebnisse mehrerer Lieferanten zusammenführen. Deaktivieren Sie einen etwaigen Jugendschutzfilter und experimentieren Sie mit Suchregion und -sprache. Ändern Sie die Region etwa in USA, um potenziell weitere Suchtreffer zu landen.

Auch Spezial-Suchmaschinen wie die Personensuche von DasTelefonbuch und Yasni können vergessen geglaubte Informationen über Ihre Person ans Tageslicht fördern (siehe ct.de/yw2w). Überprüfen Sie zudem, ob in sozialen Netzwerken wie Facebook und Business-Netzen wie LinkedIn oder Xing Profile auf Ihren Namen existieren. Haben Sie dort in der Vergangenheit Accounts angelegt, die Sie nicht mehr nutzen, sollten Sie diese löschen. Entdecken Sie Fake-Profilen, die andere in Ihrem Namen angelegt haben, melden Sie diese dem Betreiber.

Wer auf dem Laufenden bleiben möchte oder muss – etwa, weil er in der Öffentlichkeit steht –, kann dazu die Google Alerts nutzen (siehe ct.de/yw2w): Wenn Sie einen Alert anlegen, bekommen Sie von Google eine Mail, sobald neue Suchergebnisse zu einem bestimmten Begriff vorliegen.

Sozial abgesichert

Wenn Sie in sozialen Netzwerken wie Facebook unterwegs sind, dann sollten Sie überprüfen, welche Ihrer Daten für Freun-



Stalken Sie sich selbst, bevor es jemand anderes tut: Mit Meta-Suchmaschinen wie searx.me können Sie unerwartete Datenspuren ans Tageslicht fördern.



Über den Ratgeber Internetkriminalität informiert die Polizei Niedersachsen über aktuelle Cyber-Bedrohungen.

Hinter Identitätsdiebstahl muss nicht zwangsläufig ein Online-Krimineller stecken – auch Personen aus Ihrem persönlichen Umfeld können mit Ihren Daten viel Unheil anrichten. Sorgen Sie dafür, dass niemand ohne Weiteres auf Ihre Geräte zugreifen kann. Schützen Sie Rechner, Smartphones und Tablets mit einem Sperrbildschirm, der mindestens eine sechsstellige PIN, besser noch ein Passwort, einen Fingerabdruck oder einen Gesichtsscan einfordert. Sperren Sie Ihren Rechner, wenn Sie ihn verlassen – auch, wenn Sie sich im Büro nur einen Kaffee holen. Die Windows-Tastenkombination zum Sperren Windows+L geht schnell in Fleisch und Blut über. Sorgen Sie dafür, dass der Sperrbildschirm bei Inaktivität automatisch aktiv wird. Unter Windows können Sie dies in den Bildschirmschoner-Einstellungen festlegen („Anmeldeseite bei Reaktivierung“ einschalten).

de oder gar öffentlich einsehbar sind. Über ct.de/yw2w finden Sie die Privatsphäre-Einstellungen, mit denen Sie unter anderem festlegen, wer zukünftige Beiträge sehen darf. Sehr wichtig sind auch die Optionen im Abschnitt „Wie du gefunden und kontaktiert wirst“. Setzen Sie die Einstellung „Wer kann deine Freundesliste sehen?“ am besten auf „Nur ich“, damit niemand Einblick in Ihr Facebook-Adressbuch erhält. Diese Informationen können einem Angreifer helfen, Sie und Ihre Facebook-Freunde anzugreifen.

Über die beiden Einstellmöglichkeiten darunter legen Sie fest, ob Sie über Ihre Mail-Adresse respektive Ihre Telefonnummer bei Facebook aufgespürt werden können. Stellen Sie entweder „Freunde“ oder „Freunde von Freunden“ ein, da ansonsten jeder, der Ihre Mail-Adresse oder Telefonnummer kennt, herausfinden kann, wem sie gehört. Außerdem sollten Sie noch „Möchtest du, dass Suchmaschinen außerhalb von Facebook dein Profil anzeigen?“ auf „Nein“ stellen, damit Ihr Profil nicht von Google & Co. indexiert wird. Facebook bietet Diensten die Möglichkeit, weitreichend auf Ihren Account zuzugreifen. Kontrollieren Sie in den Einstellungen unter „Apps und Websites“, welchen Diensten Sie Zugriff auf Ihr Konto gewährt haben und sortieren Sie gründlich aus.

Ausgesperrt

Zugunsten des Komforts bleibt man bei den meisten Diensten für einen sehr lan-

gen Zeitraum eingeloggt. Oder wann haben Sie zuletzt das Login-Formular von Facebook oder Google gesehen? Viele Anbieter lassen die Sitzungen fast beliebig lange offen. Durch Session-Cookies ist man somit immer eingeloggt. Was im Alltag praktisch ist, kann jedoch in einigen Situationen auch unangenehme Konsequenzen haben: Wenn Sie „nur mal eben schnell“ bei einem Kumpel Ihre Mails checken wollen, kann dieser anschließend beliebig lange auf Ihren Posteingang zugreifen und an Ihrem digitalen Leben teilhaben. Noch unangenehmer ist die Vorstellung, dass völlig fremde Personen Zugriff erhalten, nachdem Sie sich etwa in einer Bibliothek oder am Arbeitsplatz eingeloggt haben.

Insbesondere wenn Sie fremde Rechner nutzen, sollten Sie daher immer darauf achten, sich vor dem Gehen bei den Diensten auszuloggen, wodurch Ihre Sitzung beendet wird. Darüber hinaus ist es empfehlenswert, in solchen Situationen den Inkognito-Modus des Browsers zu nutzen, um keine allzu offensichtlichen Datenspuren – etwa im Browserverlauf – zu hinterlassen. Hundertprozentige Sicherheit verschaffen Ihnen diese Maßnahmen jedoch nicht, da Sie einem fremden Rechner nie vertrauen können. Es wäre zum Beispiel denkbar, dass ein Keylogger installiert ist, der sämtliche Tastatureingaben einschließlich Ihrer Passwörter aufzeichnet. Das eigene Smartphone sollten Sie im Zweifel immer einem fremden PC vorziehen.

Kenne die Tricks

Informieren Sie sich über aktuelle Betrugsmaschen, damit Sie Ihre Daten nicht versehentlich Online-Gaunern in die Hände spielen. Einige Szenarien beschreibt der Artikel auf Seite 28, weitere wertvolle Anlaufstellen sind die zentralen Ansprechstellen Cybercrime der Polizeien sowie heise Security (siehe ct.de/yw2w). Bleiben Sie skeptisch, wenn Sie jemand aus heiterem Himmel nach Ihren persönlichen Daten oder gar einem Scan Ihres Personalausweises fragt – auch wenn diese Anfrage vermeintlich von einem Ihrer Facebook-Kontakte stammt.

Um es Angreifern nicht leichter als nötig zu machen, sollten Sie auch die üblichen Security-Basics befolgen: Halten Sie Betriebssystem und Programme auf dem aktuellen Stand, erstellen Sie regelmäßig Backups Ihrer wichtigen Dateien und stellen Sie sicher, dass ein Virenschutz mit aktuellen Signaturen läuft. Unter Windows 8 und 10 reicht der vorinstallierte Defender aus. Weitere kompakte Hinweise zur Absicherung Ihrer Geräte und Accounts liefern Ihnen unsere Sicherheits-Checklisten aus c't 20/2018 (ct.de/check2018).

Was Sie tun können, wenn das Kind bereits in den Brunnen gefallen ist und wie Sie feststellen, dass Ihre Identität missbraucht wird, erfahren Sie auf der folgenden Seite. (rei@ct.de) **ct**

Tools und Links: ct.de/yw2w



Erste Hilfe

Sofortmaßnahmen nach einem Angriff auf die eigene digitale Identität

Wenn Ihre digitale Identität missbraucht oder Ihre Accounts gehackt wurden, dann heißt es schnell sein – und retten, was zu retten ist.

Von Ronald Eikenberg

Nach einem Angriff auf Ihre digitale Identität sollten Sie zunächst einmal Ruhe bewahren. Versuchen Sie sich einen Überblick über das Ausmaß des Hacks zu verschaffen und dokumentieren Sie dabei alles mit Screenshots und Notizen. Nutzen Sie dazu einen Rechner, der garantiert virenfrei ist – wenn Sie Zweifel daran haben, dann können Sie Ihr System mit einem Live-System wie Desinfec't (siehe ct.de/ykfx) booten.

Accounts checken

Überprüfen Sie, ob Sie auf Ihre wichtigsten Accounts noch zugreifen können – allen voran der Mail-Account, aber auch Social-Media-Accounts, Konten bei Be-

zahlendiensten wie Paypal, Streamingdiensten wie Netflix und großen Online-Shops. Ihr Posteingang kann Ihnen wertvolle Hinweise darauf liefern, auf welche Accounts es der Angreifer abgesehen hatte und wie er dort eingestiegen ist. Manche Dienste melden etwa fehlgeschlagene Login-Versuche per Mail. Eine Nachricht, die Sie über eine unerwartete Änderung des Passworts oder der hinterlegten Mail-Adresse informiert, ist ein sicherer Indikator für einen Hack. Schauen Sie auch, ob sich verdächtige Mails in Ihrem Spam-Ordner befinden. Bei vielen Diensten wie Google oder Facebook können Sie in den Account-Einstellungen (siehe ct.de/ykfx) zudem überprüfen, ob es ungewöhnliche Login-Versuche gab.

Schauen Sie nach, ob Ihre Accounts als Spam-Schleuder missbraucht wurden. In diesem Fall finden Sie möglicherweise versendete Mails, private Nachrichten und öffentliche Posts vor, die nicht von Ihnen stammen. Wenn Sie sich noch einloggen können, sollten Sie überprüfen, ob die im Account hinterlegte Mail-Adresse und die Passwort-Recovery-Fragen geändert wurden. Wenn Sie nicht mehr auf den Ac-

count zugreifen können, versuchen Sie über die Passwort-vergessen-Funktion den Zugriff zurückzuerobern. Wenn dies nicht gelingt, informieren Sie den Support des betroffenen Dienstes.

Kontakte warnen

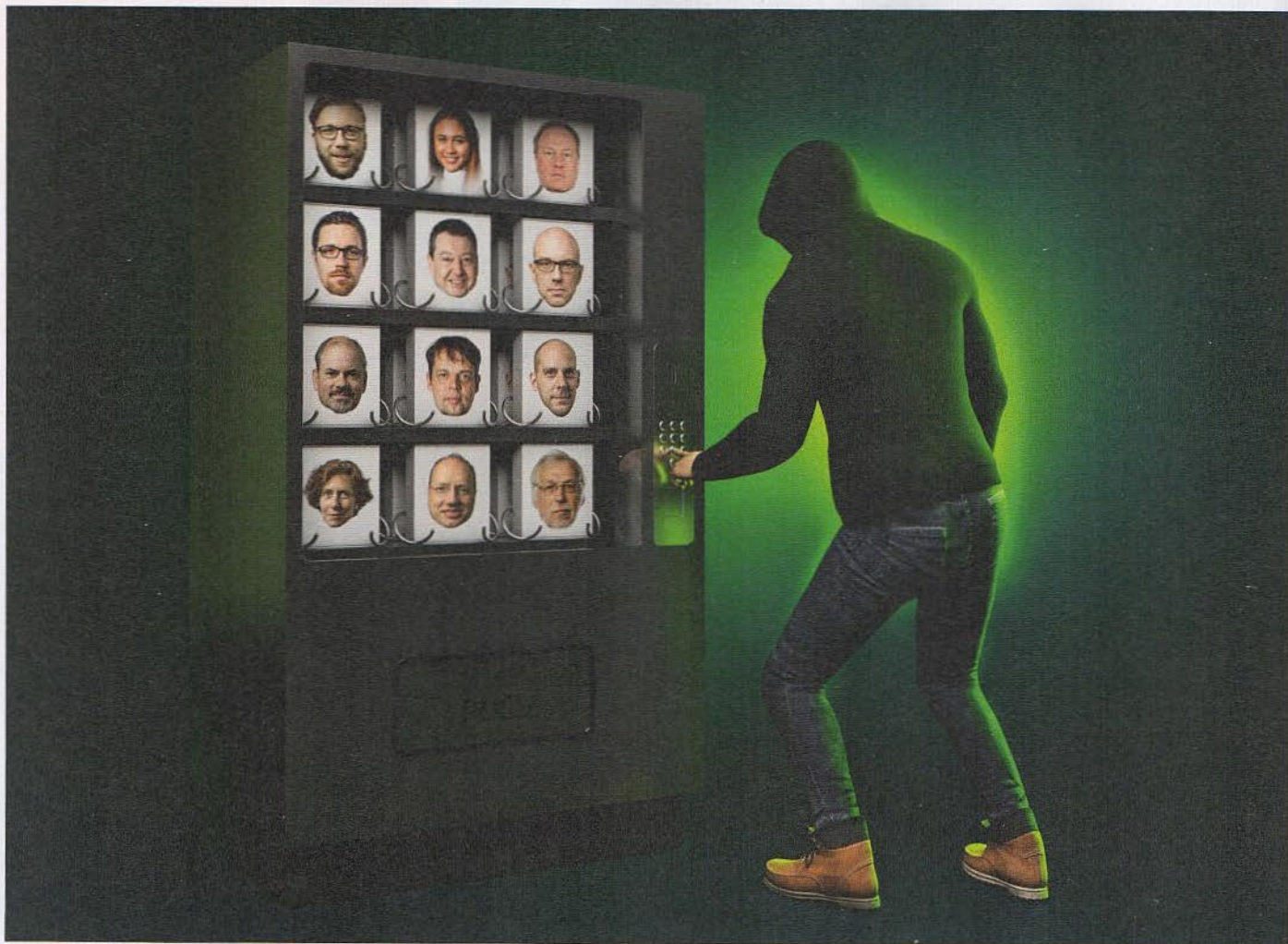
Wenn Ihre Kontakte von dem Vorfall betroffen sind – etwa durch Spam-Nachrichten oder Aufforderungen, Geld zu überweisen –, sollten Sie Ihre Freunde und Verwandte warnen. Fordern Sie Ihre Kontakte auf, auf keinen Fall auf Links oder Dateien zu klicken, die im Kontext des Vorfalls verschickt wurden. Ändern Sie die Passwörter von allen Accounts, auf welche die Täter potenziell Zugriff hatten. Behalten Sie zudem Ihre Kontoauszüge, Kreditkartenabrechnungen und Bezahl-Accounts in nächster Zeit im Blick. Fallen Ihnen Transaktionen auf, die Sie nicht zuordnen können, sollten Sie sich umgehend mit Bank, Kartenherausgeber oder Bezahl-Dienstleister in Verbindung setzen. Girocards, Kreditkarten, SIM-Karten, Online-Banking-Zugänge & Co. können Sie in vielen Fällen über den Sperr-Notruf 116 116 sperren lassen (siehe ct.de/ykfx).

Sprechen Sie auch mit anderen Personen, die Zugriff auf betroffene Zugangsdaten haben. Möglicherweise sind Sie oder eine der anderen Personen auf eine Phishing-Mail reingefallen. Unterziehen Sie Ihren Rechner einem gründlichen Virens캔, indem Sie ihn mit einem Notfall-System wie Desinfec't von DVD oder USB-Stick booten. Besteht Grund für die Annahme, dass der Rechner infiziert ist, sollten Sie Ihre wichtigen Dateien auf einen externen Datenträger sichern und das System neu aufsetzen. Falls Sie beabsichtigen, Strafanzeige zu erstatten, sollten Sie den Rechner als Beweismittel jedoch unangetastet lassen.

Anzeige erstatten

Wenn Sie den Fall zur Anzeige bringen möchten, dann wenden Sie sich am besten an Ihre örtliche Polizeidienststelle. In den meisten Bundesländern können Sie eine Strafanzeige auch über die entsprechende Online-Wache stellen. Eine Übersicht der Online-Wachen der Bundesländer sowie Hinweise zur Erstattung einer Anzeige finden Sie über ct.de/ykfx. Unternehmen richten sich am besten an die zentralen Ansprechstellen Cybercrime (ZAC) des BKA und der LKA. (rei@ct.de) **ct**

Wichtige Erste-Hilfe-Links: ct.de/ykfx



Selbstbedienungsläden

So erkennen Sie, welche Online-Dienste mit Ihren Daten schludern

Die Doxing-Angriffe auf Politiker und Milliarden geleakter Zugangsdaten machen deutlich, dass wir mehr für den Schutz der persönlichen Daten tun müssen. Doch da beginnt schon das Problem. Denn eigentlich sind nicht „wir Anwender“ das Problem, sondern die Betreiber von Diensten.

Von Jürgen Schmidt

Die meisten Kommentare und Ratsschläge zum Thema Identitätsklau legen nahe, dass jetzt die Anwender handeln müssen. Die sollten vor allem bessere Passwörter verwenden, ist die einhellige Meinung. Dabei geht das am eigentlichen Problem vorbei. Die Anwender können höchstens unmittelbar drohenden Schaden noch einschränken. An dem grundsätzlichen Problem, dass in großem Stil persönliche Daten geklaut und dann missbraucht werden, können sie fast gar nichts ändern.

Denn die Verantwortung dafür – und damit auch die Verpflichtung, jetzt etwas zu unternehmen – liegt vor allem bei den Anbietern von Internet-Diensten. Von den über zwei Milliarden Zugangsdaten

bestehend aus E-Mail-Adresse und Passwort, die aktuell im Darknet gehandelt werden, ist nicht ein einziger geklaut worden, weil deren Besitzer geschlampt hätte. Die kamen abhanden, weil die Dienste-Anbieter, denen die Daten anvertraut wurden, nicht gut genug darauf aufgepasst hatten.

Bei den Doxing-Angriffen Anfang des Jahres war das nur scheinbar anders. Da hatte tatsächlich ein geltungsbedürftiges Jüngelchen Accounts von Prominenten gekapert. Und in Einzelfällen war da vielleicht auch ein schwaches Passwort im Spiel. Doch wie es aussieht, war auch da bei der Mehrzahl der Fälle nicht die Sorglosigkeit der Opfer für den Einbruch verantwortlich, sondern unzureichende

Sicherheitsvorkehrungen beziehungsweise unsichere Prozesse bei den Betreibern der Dienste.

Wenn tatsächlich Passwörter durch Durchprobieren geknackt wurden, liegt der Verdacht nahe, dass der Betreiber keinen ordentlichen Brute-Force-Schutz implementiert hat. Mit einer sinnvollen Drosselung der Login-Versuche, die etwa nach fünf falschen Passwörtern eine zehnmünütige Pause verordnet und nach weiteren zehn Fehlversuchen den Zugang für einen Tag sperrt, lässt sich so etwas nämlich weitgehend verhindern. Nur ohne einen solchen Schutz können Angreifer mit einfachen Skripten Tausende oder gar Millionen von Passwort-Variationen durchtesten. Allerdings muss die Bremse natürlich nicht nur am zentralen Login sondern an allen Stellen umgesetzt sein, die ein Passwort kontrollieren. Also insbesondere auch beim Zugriff via Smartphone-App oder auf ein API.

Durch den Hintereingang

Wie die Einbrecher der analogen Welt nehmen nämlich auch die digitalen Identitätsräuber in aller Regel nicht den Haupteingang, um einen Account zu kapern. Viel öfter benutzen sie das Fenster oder den Hintereingang. Und darüber kommt man oft viel einfacher an die Daten als über Passwort-Knacken. Bei einem Nutzerkonto für einen Internet-Dienst ist einer dieser häufig schlecht gesicherten Hintereingänge die Funktion „Ich habe mein Passwort vergessen“. Viele der in der Vergangenheit gekaperten Promi-Accounts wurden tatsächlich über diese Hintertür übernommen.

Jede Website mit Benutzerkonten hat auch eine solche Passwort-vergessen-Funktion. Sie ist ein wichtiger Bestandteil der Benutzerverwaltung und wird auch fleißig genutzt. Bei Heise etwa rufen täglich rund 250 Nutzer diese Funktion auf, um wieder Zugang zu ihrem Konto zu erlangen – also viel zu viele, um die alle persönlich zu betreuen. Mal ganz abgesehen davon, dass dieser Service nichts kosten darf und 24 Stunden am Tag, sieben Tage die Woche bereitstehen sollte.

Banken können sich den Luxus eines aufwendigen Prozesses erlauben, der persönliche Interaktion und vor allem schwer zu fälschende Identitätsnachweise wie eine Personalausweiskopie erfordert: „Lieber mal ein paar Tage ohne Online-Banking als ausgeraubt.“ Letztlich steht dort sowohl für Betreiber als auch Nutzer

Der Passwort-Reset via E-Mail hat sich weitgehend durchgesetzt, hat aber seine Tücken.

die Sicherheit an oberster Stelle. Aber für einen Foren-Zugang, ein Konto beim Online-Shop und auch für E-Mail-Konten sieht das anders aus. Da muss der Zugang sofort wieder her – und zwar möglichst billig für den Betreiber und komfortabel für den Anwender.

Folglich muss der Passwort-Reset vollständig automatisiert ablaufen. Erschwerend kommt hinzu, dass der Dienst-Betreiber oft nur sehr wenig über den Benutzer weiß und sich deshalb der Nachweis der Zugangsberechtigung schwer gestaltet. Und da wird dann sehr häufig geschlampt. So kommt es durchaus vor, dass man für den Haupteingang – also den Login mit Benutzername und Passwort – ein mindestens achtstelliges Passwort aus Zahlen, Klein- und Großbuchstaben und sogar Sonderzeichen verwenden muss. Aber an der Hintertür „Passwort vergessen“ genügt es oft schon, das Geburts-

datum des Anwenders und den Mädchennamen seiner Mutter zu kennen.

Besser ist es, wenn der Passwort-Reset über die hinterlegte E-Mail-Adresse abgewickelt wird. An die bekommt der vergessliche Anwender einen Link zugeschickt. Beim Klick darauf öffnet sich eine Seite, auf der er ein neues Passwort eingeben kann. Das geht schnell, ist komfortabel – und für einfache Konten, etwa in Foren, bei Online-Shops oder Social Media Accounts auch aus Sicherheitssicht durchaus ausreichend. Es koppelt die Sicherheit des Accounts an die des E-Mail-Kontos. Doch auch dabei kann man vieles falsch machen.

So ist E-Mail kein wirklich sicheres Medium. Insbesondere liegen Mails oft an vielen Stellen im Klartext vor. Wenn sie dauerhaft funktionierende Passwort-Reset-Links enthalten, ist das fahrlässig. Um das damit verbundene Risiko zu

Wenn man die hinterlegte E-Mail-Adresse ohne Passwortabfrage ändern kann, ergeben sich eine Reihe von möglichen Missbrauchsszenarien.

Ist das jetzt sicher? Eigene Fragen sind ein zweischneidiges Schwert.

begrenzen, darf also der Link nur ein einziges Mal funktionieren und sollte auch nur kurze Zeit gültig sein – beispielsweise 15 Minuten bis maximal einige Stunden. Sind die abgelaufen, muss der Anwender eben einen neuen Link anfordern. Gibt es keine solchen Beschränkungen, ist das Schlamperei des Dienst-Anbieters.

Immer wieder berichten uns auch Leser davon, dass ihnen Dienste-Betreiber statt eines temporären Links ein neues Passwort im Klartext zusenden. Das ist nicht schön, lässt sich aber unter Umständen noch verschmerzen, wenn es ebenfalls nur kurzfristig gültig ist und der Anwender gezwungen wird, es sofort nach dem Login zu ändern. Auch das ist leider keineswegs selbstverständlich, wie uns Berichte von Lesern immer wieder aufzeigen.

Fatal ist es auch, wenn ein Angreifer die Passwort-Reset-Funktion einfach umleiten kann. Beim Online-Konto der Bahn etwa kann man die hinterlegte E-Mail-Adresse ändern, ohne dass man dazu das Passwort eingeben muss. Damit genügt es, dass jemand in einem unbeobachteten Moment am Rechner des Opfers diese Adresse so umstellt, dass er später via Passwort-Reset das Konto übernehmen kann.

Außerdem ließen sich diese Angriffe auch über kleine Fehler auf den Webseiten der Bahn automatisieren. Mit einer Cross-Site-Scripting- (XSS) beziehungsweise Cross-Site-Request-Forgery-Lücke (CSRF) auf bahn.de würde es genügen, dem Opfer einen passenden Link unterzuschieben, um das Konto zu kapern.

Solche Lücken sind sehr weit verbreitet und finden sich in fast jedem größeren Webangebot regelmäßig.

Wenn beim Bahn.de-Konto ein Lastschrifteinzug freigeschaltet ist, hat der Angreifer damit einen direkten Draht zum Geldbeutel des Opfers, das kaum eine Chance hat, das zu bemerken. Bestellbestätigungen gehen ja jetzt an die Adresse des Angreifers. Nicht einmal eine Informations-Mail, dass die Nachrichten zukünftig woanders landen, geht an die alte Adresse. Dieses Problem betrifft übrigens nicht nur die Bahn, sondern auch viele Shops.

Gute Fragen, schlechte Fragen

Besonders tricky ist der Passwort-Reset bei E-Mail-Konten. Da ein einfacher Passwort-Reset via E-Mail mangels Zugang zum Konto nicht funktioniert, müssen sich die Anbieter da etwas anderes einfallen lassen. Dafür gibt es kein allgemeingültiges Patentrezept. Klar ist, dass man einen zweiten Kommunikationskanal benötigt – sei das jetzt eine zweite E-Mail-Adresse oder eine Telefonnummer. Darüber hinaus ist es dabei dann mehr als wünschenswert, dass man seine Identität nachweisen muss. Vielleicht nicht unbedingt durch eine Personalausweiskopie. Aber zumindest durch das Beantworten von Sicherheitsfragen.

Leider gibt es auch kein Patentrezept für gute Sicherheitsfragen. Immerhin kann man schlechte sehr leicht erkennen. Das Geburtsdatum, das Lieblings-Urlandsland und auch der Mädchenname

Gut gemacht! Die Fehlermeldung sollte nicht verraten, ob eine bestimmte E-Mail-Adresse registriert ist.

der Mutter dürften in vielen Fällen nicht ausreichend geheim sein, um einen Missbrauch zu verhindern. Gut ist es, wenn es einen möglichst umfangreichen Fragenkatalog gibt, aus denen sich der Nutzer zwei bis drei passende aussuchen kann. Überlegen Sie dann einfach selber, wie schwer es wohl für Dritte wäre, die Antwort auf eine vorgeschlagene Frage herauszufinden.

Fragen, die sich der Anwender selbst ausdenkt, können sicher sein – oder auch nicht. Letztlich schiebt das die Verantwortung für die Fragen ganz auf den Nutzer ab. Das ist meiner Einschätzung nach zumindest dann eine schlechte Idee, wenn man einen Dienst betreibt, der sich auch an Erwin oder Lieschen Müller richtet. Man sollte diese Option zumindest mit einem Katalog vorgefertigter Fragen kombinieren.

HTTPS ist Pflicht

Die Grundvoraussetzung für eine sichere Nutzung von Internet-Diensten ist der Einsatz von Transport Layer Security (TLS), die man am Adressvorsatz „https“ erkennt. Ohne die können Dritte die übertragenen Daten mitlesen. Besonders einfach geht das etwa in öffentlichen Funknetzen. Und es genügt keineswegs, nur die Login-Seite und die mit den persönlichen Daten via HTTPS zu sichern.

Eine anonyme Wetterkarte via HTTP kann man vielleicht noch akzeptieren; Shops oder personalisierte Dienste ohne durchgehendes HTTPS sollte man hingegen grundsätzlich meiden. Da sind Ihre Daten in schlechten Händen. Und zwar

nicht nur wegen der Gefahr, die von der fehlenden Verschlüsselung ausgeht. Sondern weil der Anbieter mit dem Verzicht auf HTTPS mangelndes Sicherheitsbewusstsein demonstriert. Da kommt es dann ziemlich sicher auch an anderen Stellen zu faulen Sicherheitskompromissen – insbesondere, wenn diese von außen nicht ohne Weiteres sichtbar sind.

In aller Regel kann man als Nutzer eines Shops, eines Forums oder eines beliebigen anderen Internet-Dienstes nämlich nicht hinter dessen Kulissen schauen. Somit kann man sich selbst kein Bild davon machen, wie umfassend und vor allem wie systematisch der Anbieter die ihm anvertrauten Daten schützt.

Werden die Passwörter nach dem Stand der Technik mit einem Verfahren wie PBKDF2 oder bcrypt verschlüsselt abgelegt? Oder sind sie immer noch mit hoffnungslos veralteten Verfahren wie MD5 und SHA1 gesichert oder sogar im Klartext vorhanden? Das erfährt man häufig erst nach einem Einbruch, wenn etwa wie im Herbst 2018 1,8 Millionen Datensätze der Chat-Plattform Knuddels im Netz auftauchen – inklusive der Klartextpasswörter.

Spielt der Anbieter Sicherheits-Updates der verwendeten Software zügig ein? Schult er seine Mitarbeiter in Security-Dingen? All das entzieht sich dem Blick von außen. Und die bei heise Security im Lauf der Jahre gesammelten Erfahrungen mit Sicherheitslücken zeigen deutlich, dass auch die häufig stolz präsentierten Security-Bempel wie diverse TÜV-Prüfsiegel bei Webseiten keineswegs ein Garant für echte Sicherheit sind.

Extrem hohe Ansprüche an die Passwörter der Nutzer bedeuten übrigens auch nicht zwangsläufig, dass man es mit der Sicherheit wirklich ernst meint. Denn die Forderung nach mindestens 10 Zeichen mit gemischter Groß-/Kleinschreibung, Ziffern und Sonderzeichen kostet den Dienstebetreiber nichts. Entwickler, Software-Architekten und Administratoren mit guten Sicherheitskenntnissen hingegen schon.

Trotzdem ist man nicht allein dem guten Willen der Anbieter ausgeliefert. Denn beim etwas genaueren Hinsehen kann man zumindest einen ersten Eindruck gewinnen, wie es der Anbieter mit der Sicherheit hält. Unser Kasten „Das können Sie selber testen“ gibt Ihnen Tipps, wo Sie dabei hinschauen sollten.

(ju@ct.de) **ct**

Das können Sie selber testen

In aller Regel hat man als Benutzer keinen Einblick in die Sicherheit eines Dienstes. Ein paar Dinge kann man aber durchaus selber überprüfen, um sich ein Bild davon zu machen, wie hoch der Stellenwert der Security bei einem Angebot tatsächlich ist.

Verschlüsselung: Sind alle Web-Seiten via HTTPS gesichert? Ohne diese Transportverschlüsselung kann ein Angreifer etwa an einem WLAN-Hotspot oder im gleichen (Firmen-)Netz die übertragenen Daten mitlesen und auch den Account kapern.

Wichtige Daten: Erfordert die Anzeige oder zumindest das Ändern wichtiger Daten wie die hinterlegte E-Mail-Adresse beziehungsweise Telefonnummer die Eingabe des Passworts? Wenn nicht, genügt schon ein einfacher Fehler auf der Webseite oder ein kurzfristig ungeschützt offenes Browser-Fenster, um Ihren Account zu kapern. Werden Sie über das Ändern etwa der hinterlegten E-Mail-Adresse informiert?

Login-Bremse: Es darf nicht sein, dass ein Angreifer ungehindert Tausende oder gar Millionen von Passwörtern durchprobieren kann. Spätestens nach ein paar Dutzend fehlgeschlagenen Login-Versuchen ist klar, dass da etwas schief läuft und der Dienst sollte einschreiten. Am besten mit immer längeren Login-Sperren – etwa nach fünf Fehlern ein paar Minuten bis hin zu einem Tag nach zehn oder zwanzig. Doch Achtung beim Testen: Manche Anbieter wie GMX reagieren mit IP-Sperren auf vermeintliche Angriffe auf Passwörter. Mit etwas Pech sperren Sie mit Login-Tests also nicht nur sich, sondern auch ein paar hundert Kollegen hinter der gleichen Firewall vom GMX-Zugang aus.

Login-Tokens: Muss man sich nach dem Ändern des Passworts überall neu anmelden? Gelegentlich vergessen die Dienstebetreiber noch geöffnete Sitzungen oder Zugangs-Tokens für Smartphone-Apps zu invalidieren. Das ist dann eine tolle Hintertür, über die ein einmal kurz in das Konto eingedrungen Angreifer immer wieder Zugang erhält.

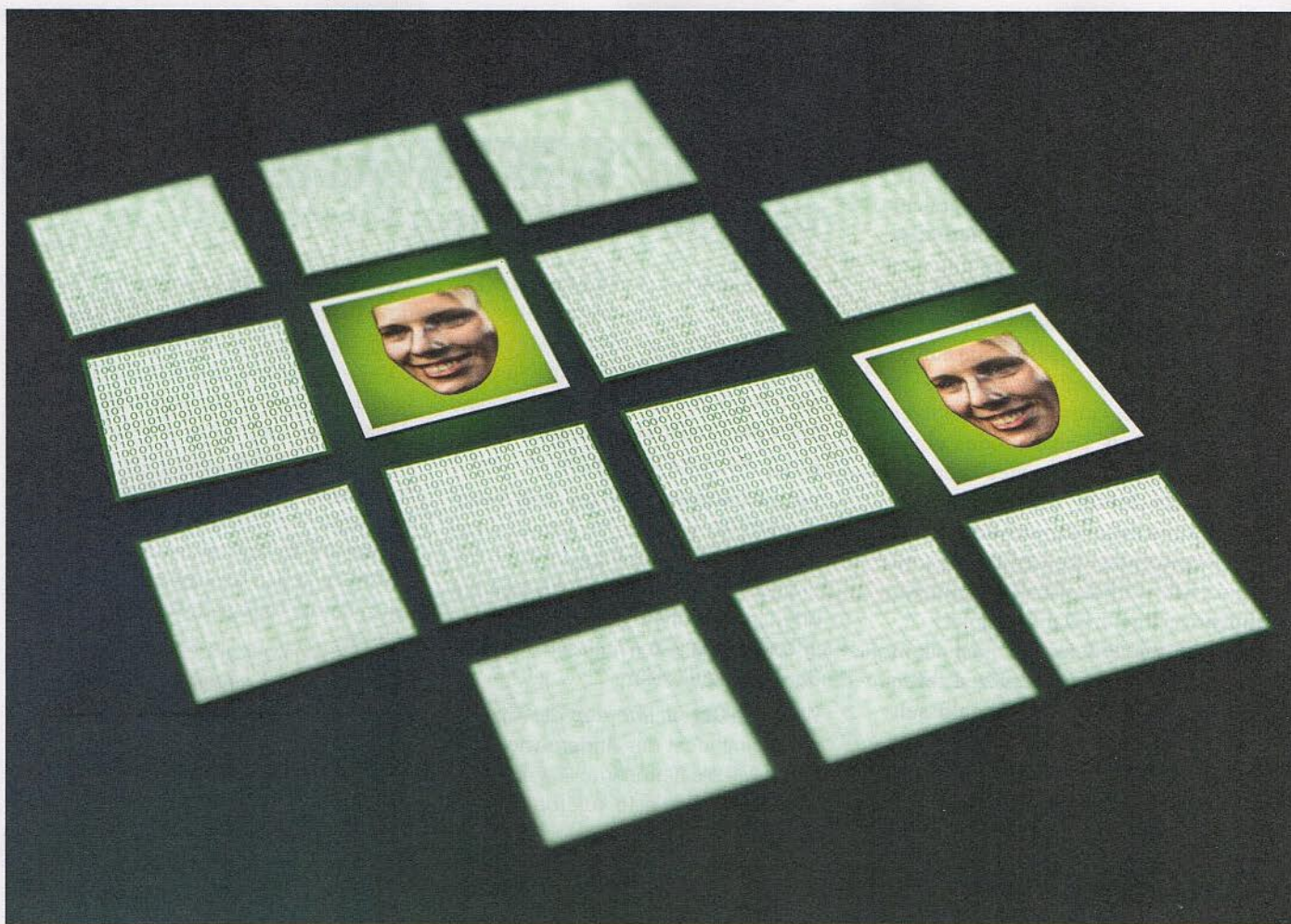
Zwei-Faktor-Authentifizierung: Zentrale Dienste, an denen die komplette Identität hängt – also insbesondere E-Mail – und solche, die direkt mit Ihrem Geldbeutel verbunden sind, sollten optional eine Zweifaktor-Authentifizierung (2FA) anbieten. Stand der Technik sind sogenannte Software-Tokens, die 2FA-Apps wie Google Authenticator erzeugen. Weniger sicher sind Codes via SMS und den höchsten Schutz bieten separate Hardware-Tokens wie ein Yubikey.

Zusätzliche Sicherheitsfragen: Sicherheitsfragen allein sind nicht ausreichend. Wenn sie aber mit dem Passwort-Reset über ein E-Mail-Konto kombiniert werden, erhöhen sie die Sicherheit. Wie man gute von schlechten Fragen unterscheidet, erklärt der Artikel bei „Gute Fragen, schlechte Fragen“.

Sinnvolle Benachrichtigungen: Gute Dienste informieren Sie über wichtige Ereignisse. Also etwa darüber, dass Sie gerade die Telefonnummer oder die E-Mail-Adresse geändert haben, über die Sie – beziehungsweise der Inhaber der neuen Adresse – Zugang zum Konto erlangen können. Dabei ist die richtige Balance wichtig. Wer ständig „Alarm“ schreit, erntet irgendwann nur noch Achselzucken.

Zweiter Kanal: Ein spezieller zweiter Kanal, der nur für die Wiederherstellung des Zugangs dient, ist insbesondere für E-Mail-Konten Pflicht. Aber auch andere Dienste profitieren von einer E-Mail-Adresse oder Telefonnummer, über die etwa der Passwort-Reset abgewickelt wird und über die man Sie unter Umständen auch über mögliche Sicherheitsprobleme mit Ihrem Account informieren kann.

Anlaufstelle für Security-Probleme: Hat der Dienst eine klar definierte Anlaufstelle, bei der man Sicherheitsprobleme melden kann? Damit wird ein Dienst zwar nicht zwangsläufig sicherer. Aber es zeigt, dass man sich des Problems der eigenen Sicherheitslücken bewusst ist und bereit, daran zu arbeiten.



Passwortsuche mit Turbo

25 Gigabyte Passwortlisten von HaveIBeenPwned schnell lokal durchsuchen

Auf haveibeenpwned.com kann man eine sortierte Liste mit Hashes von Passwörtern aus Hacks und Leaks herunterladen. Entpackt ist die knapp 25 Gigabyte groß. Mit in Python implementierter binärer Suche ist sie trotz ihrer Größe in wenigen Millisekunden durchsucht.

Von Pina Merkert

Die Webseite Haveibeenpwned.com sammelt seit Jahren Passwörter aus Leaks und Hacks. Inzwischen sind 551.509.767 Klartext-Passwörter bei dem Dienst aufgelaufen, die Nutzer auf

keinen Fall mehr benutzen sollten. Um zu prüfen, ob das eigene Passwort dabei ist, bietet der Dienst einen Webservice an. Die Webseite verschickt zwar nur auf fünf Zeichen gekürzte Hashes übers Netz, aber um sicherzugehen, dass wirklich kein Passwort im Klartext verschickt wird, müsste man vor jeder Nutzung den JavaScript-Code der Seite prüfen. Bei unserem Python-Skript können Sie sich das sparen: Es ist lokal auf Ihrer Platte gespeichert und dort vor unerwarteten Änderungen geschützt.

Es arbeitet mit einer entpackt 25 Gigabyte großen Datei mit SHA-1-Hashes der geleakten Passwörter; Sie können die Datei als 10 Gigabyte großes 7Zip-Archiv bei haveibeenpwned.com (siehe ct.de/v6rc) herunterladen.

Abgetrennt durch einen Doppelpunkt enthält jede Zeile neben dem Hash in Hex-Darstellung auch die Anzahl, in wie vielen Leaks das Passwort bereits auftaucht ist. Eine Zeile der Datei sieht beispielsweise so aus:

```
7FF579BAE8FCFE030E09;
59BC9CA6414B5C76B185A:12
```

Um in dieser Datei nach dem eigenen Passwort zu suchen, erstellt man einen SHA-1-Hash des eigenen Passworts und sucht alle Zeilen, in denen dieser auftaucht. Das geht beispielsweise auf der Linux-Konsole mit:

```
echo -n "paSsword" | sha1sum | j
↳tr [a-z] [A-Z] | cut -c1-40 | j
↳grep -f - pwned-passwords-sha1-j
↳ordered-by-hash-v4.txt
```


sha1sum erstellt einen Hash in Hex-Darstellung, nur leider mit a bis f in Kleinbuchstaben. Die konvertiert `tr [a-z] [A-Z]` in Großbuchstaben und `cut -c1-40` schneidet unnötige Zeichen hinten ab. Mit dem Ergebnis sucht `grep`, das mit der Option `-f` - den zu filternden String von `stdin` liest. Der lange Dateiname ist der Name der Datei, wie er aktuell aus dem Archiv fällt.

Sortierung nutzen

Der `grep`-Befehl durchsucht die Datei auf einem Rechner mit Core i5 mit SSD in etwas mehr als einer Minute. Er nutzt aber nicht aus, dass die Datei bereits nach Hashes sortiert ist. In einer sortierten Liste kann man per binärer Suche viel schneller suchen. Eine selbst programmierte binäre Suche in Python braucht nur wenige Zeilen Code. Wir haben daher kurzerhand ein Skript entwickelt, das die Datenmassen in Rekordzeit durchforstet (siehe ct.de/y6rc).

Damit Sie sicher sein können, dass dieser Code nichts Ungewolltes mit Ihren Passwörtern anstellt, erklären wir ihn en détail. Sie sind explizit aufgerufen, uns kritisch auf die Finger zu schauen.

Teile und herrsche

Die zentrale Idee der binären Suche besteht darin, einen Hashwert aus der Mitte der Liste herauszugreifen und mit dem Gesuchten zu vergleichen. Ist der gesuchte Hash kleiner als der herausgegriffene, muss der gesuchte Hash in der vorderen Hälfte der Liste zu finden sein. Ist er dagegen größer, kommt nur noch die hintere Hälfte der Liste infrage.

Hat man das herausgefunden, muss man nur noch eine halb so lange Liste durchsuchen, wofür man den gleichen Trick verwendet. Dieses Spiel spielt man, bis die zu durchsuchende Liste nur noch aus einem Eintrag besteht. Mit diesem vergleicht man den gesuchten Hash und erkennt daran, ob er in der Liste vorkam oder nicht.

Wir haben diese Idee mit einer rekursiven Funktion namens `search_hash()` umgesetzt. Sie nimmt neben der Datei mit der ganzen Liste auch einen über die Parameter `start` und `end` definierten Bereich entgegen. Dessen Größe halbiert sie bei jedem Aufruf und ruft sich dann selbst mit dem neuen Bereich auf. Dafür sucht sie sich zunächst die Mitte des Bereichs:

```
new_pos = start + (end - start) // 2
```

Diese Position ist aber die Position eines Bytes in der Datei. Ob an dieser Position eine Zeile anfängt oder sie in die Mitte einer Zeile verweist, weiß der Algorithmus nicht. Um den Hash zu vergleichen, muss er aber immer die ganze Zeile lesen. Das erledigt die Funktion `get_full_line()`:

```
def get_full_line(file, pos):
    file.seek(pos)
    while (pos > 0 and
           file.read(1) != "\n"):
        pos -= 1
    file.seek(pos)
    return file.readline(), pos
```

Die Methode `seek()` springt sehr schnell an eine bestimmte Position in einer Datei. Von dort aus sucht sie den Beginn der Zeile. Dafür geht sie rückwärts und liest so lange einzelne Bytes aus der Datei, bis sie einen Zeilensprung findet (`"\n"`). Von diesem Zeilenanfang ist es ein Leichtes, mit `readline()` die ganze Zeile auszulesen. Als zweiten Rückgabewert liefert die Funktion auch die Byte-Nummer des zuvor gesuchten Zeilenanfangs, da der Algorithmus den später nutzt, um den Suchbereich einzugrenzen.

Mit dieser Funktion lädt `search_hash()` die mittlere Zeile im Bereich. Die enthält neben dem Hash auch die Anzahl, was sich mit `split(':')` leicht trennen lässt. Danach gilt es zunächst zu prüfen, ob der gesuchte und gefundene Hash übereinstimmen. Ist das der Fall, gibt `search_hash()` die Anzahl zurück und der Algorithmus ist fertig.

Stimmen sie nicht überein, muss die Funktion rekursiv weitersuchen. Dafür entscheidet `search_hash()`, ob die Suche in der vorderen oder hinteren Hälfte weitergeht. Es reicht dafür, die hexadezimalen Strings der Hashes zu vergleichen. Der Vergleich prüft die Strings nämlich zeichenweise und die Buchstaben haben einen größeren Unicode als die Ziffern. Es ist daher `A > 9` und `A000 > 8AAA`:

```
def search_hash(file, my_hash,
                start, end):
    if start >= end:
        return 0
    new_pos = start + (end - start) // 2
    anddate_line, pivot=get_full_line(
                                file, new_pos)
    pwmed_hash, count = candidate_line.\
                                split(':')
    if pwmed_hash == my_hash:
        print("Password found at byte ",
              '{:11d}'.format(
                  pivot, candidate_line.strip()))
        return int(count.strip())
    if my_hash > pwmed_hash:
        return search_hash(file, my_hash,
                           file.tell(), end)
    else:
        return search_hash(file, my_hash,
                           start, pivot)
```

Um im vorderen Bereich zu suchen, hat die Funktion `get_full_line()` mit `pivot` den passenden Endwert für den Bereich geliefert. Für den hinteren Bereich ergibt es aber Sinn, hinter der gerade gesuchten Zeile zu suchen. An dieser Position steht der Dateizeiger nach `readline()`. Die Funktion `file.tell()` gibt diese Position als Zahlenwert zurück.

In beiden Fällen darf die Suche auch enden, wenn der Bereich keine Zeile mehr enthält. Das übernehmen die ersten beiden Zeilen der Funktion. Der Bereich hat nur dann eine Größe von 0, wenn der Hash nicht in der Datei steht, weshalb die Funktion dann 0 zurückgibt.

Die Unterfunktionen `get_full_line()` und `search_hash()` übernehmen die ganze Arbeit. Für die umschließende Funktion `binary_search()` reicht es daher, in einer Zeile die Rekursion mit einem Bereich von 0 bis zur Größe der Passwortdatei anzustoßen:

```
return search_hash(list_file,
                   hex_hash, 0, file_size)
```

Damit ist der Algorithmus schon fertig. Das Programm umschifft aber zusätzlich noch ein paar Alltagsprobleme, damit

```
jme@jme-ct: ~/Code/HaveIBeenPwnedOffline
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
jme@jme-ct:~/Code/HaveIBeenPwnedOffline$ time echo -n "pa55word" | sha1sum | tr [a-z] [A-Z] |
cut -c1-40 | grep -f :pwmed-passwords:sha1-ordered-by-hash-v4.txt
A710C06A86B04853180E6EBC3C760572B23AF69F:25
real    1m0.599s
user    0m14.547s
sys     0m10.425s
jme@jme-ct:~/Code/HaveIBeenPwnedOffline$
```

Die Suche mit `grep` funktioniert, dauert aber länger als eine Minute.


```
jme@jme-ct: ~/Code/HaveIBeenPwnedOffline
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
jme@jme-ct:~/Code/HaveIBeenPwnedOffline$ python binary_search.py pa$sw0rd 'Geheim HorseBatteryStaple'
Searching for hash DE547C080448C009A4077F2EC74A942356EA154B of password "pa$sw0rd".
Password found at byte 21108344308: "DE547C080448C009A4077F2EC74A942356EA154B:56"
Your password "pa$sw0rd" was in 56 leaks or hacked databases! Please change it immediately.
Searching for hash 403768760A0934828FB73FB4AAB5D0217FF88D15 of password "Geheim".
Password found at byte 7334814857: "403768760A0934828FB73FB4AAB5D0217FF88D15:897"
Your password "Geheim" was in 897 leaks or hacked databases! Please change it immediately.
Searching for hash FE69332FD868718261A186C84D4BD527F0C967D3 of password "HorseBatteryStaple".
Your password "HorseBatteryStaple" is not in the dataset. You may relax.
jme@jme-ct:~/Code/HaveIBeenPwnedOffline$
```

Zwei der gesuchten Passwörter stehen in der Datenbank. Die sollte niemand benutzen. Das dritte Passwort kam bisher in keinem Leak im Klartext vor.

man es einfach auf der Kommandozeile benutzen kann.

Encoding und Hashing

Hashfunktionen wie SHA-1 arbeiten mit Bytes statt Strings. Es spielt also eine Rolle, mit welchem Encoding die Hashes erstellt wurden. Troy Hunt, der Ersteller der Liste bei HaveIBeenPwned, erklärt in einem Kommentar zu seinem Blogpost zur Erstellung der Liste (siehe ct.de/y6rc), dass er die Passwörter in UTF-8 kodiert hat, bevor er sie gehasht hat. Daher kodiert das Python-Skript ebenfalls alle zu testenden Passwörter in UTF-8.

Den Hash berechnet die Funktion `sha1()` aus der Hashlib, die das Programm ganz zu Beginn mit `from hashlib import sha1` importiert. Die Funktion gibt ein Objekt zurück, dem man mit der Methode `hexdigest()` einen Hash in Hex-Darstellung entlockt. Da der aber Kleinbuchstaben verwendet, die Liste aber Großbuchstaben enthält, muss die String-Funktion `upper()` noch alle Klein- in Großbuchstaben umwandeln:

```
if 'decode' in dir(str):
    password = password.decode('utf-8')
    h = sha1(password.encode('utf-8'))
    .hexdigest().upper()
```

Die `if`-Anweisung in den ersten beiden Zeilen dient der Kompatibilität mit Python 2.7. Dort sind Strings nicht wie in Python 3 grundsätzlich als UTF-8 kodiert, sodass der Code sie für Python 2.7 noch dekodieren muss. Da Strings nur im alten Python eine `decode()`-Funktion besitzen, wird dieser Schritt bei Python 3 übersprungen.

Argumente parsen

Der übrige Code dient dazu, das Programm auf der Konsole leicht nutzbar zu machen. Dafür sorgt der `ArgumentParser` (`from argparse import ArgumentParser`), der Kommandozeilenargumente strukturiert entgegennimmt und automatisch

eine Hilfenachricht generiert (Aufruf mit der Option `--help`):

```
parser = ArgumentParser(description=
    'Test passwords locally.')
parser.add_argument('passwords',
    nargs='+')
parser.add_argument('--pwned-pass' +
    'words-ordered-by-hash-filename',
    required=False, default='pwned-' +
    "passwords-sha1-ordered" +
    "-by-hash-v4.txt")
args = parser.parse_args()
```

Die Methode `add_argument()` fügt jeweils einen Kommandozeilenparameter hinzu. Da der Name `passwords` nicht mit einem - beginnt, muss man für diesen Parameter beim Aufruf kein Präfix angeben. Die Option `nargs='+'` legt fest, dass es sich bei diesem Parameter um eine Liste mit mindestens einem Element handelt. Dank dieser Definition sorgt der Parser dafür, dass man mindestens ein Passwort hinter dem Dateinamen angeben muss, jedoch auch gleich mehrere per Leerzeichen getrennt angeben darf.

Das zweite Argument funktioniert nur mit Präfix. Da es aber als `required=False` erstellt wird, muss man es nicht angeben. Die Option `default` sorgt dafür, dass der Parser für das Argument auch dann einen Wert liefert, wenn es der Nutzer weggelassen hat. Ein Aufruf des Programms mit allen Argumenten sieht beispielsweise so aus:

```
python binary_search.py pa$sw0rd -j
    Geheim HorseBatteryStaple --pwned-j
    passwords-ordered-by-hash-filename -j
    pwned-passwords-sha1-ordered-by-j
    hash-v4.txt
```

Die Reihenfolge der Argumente spielt keine Rolle.

Nach dem Aufruf von `parse_args()` stehen die Parameter als Properties zur Verfügung. Das Skript nutzt sie danach, um die Passwort-Datei zu öffnen und mit `stat()` aus dem `os`-Modul (`from os import stat`) die Dateigröße auszulesen:

```
with open(args.pwned_passwords_j
    ordered_by_hash_filename,
    'r') as pwned_passwords_file:
    pwned_passwords_file_size = stat(
        args.pwned_passwords_ordered_by_j
        hash_filename).st_size
```

In der Schleife `for password in args.passwords`: sucht das Skript danach nach jedem übergebenen Passwort und gibt die Ergebnisse aus (die `print()`-Befehle haben wir hier ausgelassen).

Das ganze Skript hat nur 57 Zeilen und steht zur Begutachtung und zum Download auf GitHub (siehe ct.de/y6rc). Es macht keine Netzwerkanfragen, was Sie bereits an den Imports ganz zuoberst erkennen können. Es schreibt die eingegebenen Passwörter auch nicht auf die Festplatte, was Sie an einem `open()` mit der Option `w` erkennen würden.

Das Kommandozeilen-Interface erlaubt es Ihnen, bequem ein oder mehrere Passwörter zu prüfen. Durch die schnelle binäre Suche geht das auch mit einem Dutzend verschiedener Passwörter in wenigen Millisekunden. Falls es Ihnen unangenehm ist, Passwörter in der Bash-History wiederzufinden, müssen Sie diese deaktivieren, löschen oder die `getpass()`-Funktion aus dem `getpass`-Modul ins Skript einbauen. (pmk@ct.de) **ct**

Das Programm bei GitHub: ct.de/y6rc

```
jme@jme-ct: ~/Code/HaveIBeenPwnedOffline
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
jme@jme-ct:~/Code/HaveIBeenPwnedOffline$ time python2 binary_search.py pa$sw0rd
Searching for hash A710CD6A86B048531B0E6EBC3C760572B23AF69F of password "pa$sw0rd".
Password found at byte 15865031392: "A710CD6A86B048531B0E6EBC3C760572B23AF69F:25"
Your password "pa$sw0rd" was in 25 leaks or hacked databases! Please change it immediately.

real    0m0.027s
user    0m0.008s
sys     0m0.019s
jme@jme-ct:~/Code/HaveIBeenPwnedOffline$
```

Die binäre Suche braucht nur 0,027 Sekunden, um ein Passwort zu finden.



Bild: Luxx Film GmbH

Digitaler Möwenflug

Making of: „Manou flieg flink!“ von den Stuttgarter Luxx Studios

Am 28. Februar kommt der Animationsfilm „Manou flieg flink!“ in die deutschen Kinos. Die Luxx Studios realisierten ihn mit einem kleinen Team, viel Rechenleistung und einer Menge Herzblut.

Von André Kramer

Der Animationsfilm „Manou flieg flink!“ erzählt die Geschichte des Mauerseglers Manou, der in Nizza von den Möweneltern Yves und Blanche adoptiert wird. Die Luxx Studios produzierten den 88-minütigen Familienfilm in Kooperation mit dem Studio Ambient & Friends.

Andrea Block und Christian Haas gründeten 2006 die Luxx Studios als Dienstleister für visuelle Effekte. Luxx arbeitete über die Jahre an Einstellungen für „White House Down“, „Grand Budapest Hotel“ und „Independence Day 2“ sowie seit 2013 immer wieder an den Designs, Setbauten und einem Trailer für Manou.

„Wir wollten von Beginn an eine internationale Produktion machen“, sagt Luxx-Gründer Christian Haas im Ge-

spräch mit c’t. Nur weltweit hat der Film die Chance, die 8 Millionen Euro Produktionskosten wieder einzuspielen. Für die englische Fassung konnte die Agentur Kate Winslet und Willem Dafoe überzeugen, die Rollen der Möweneltern Blanche und Yves zu sprechen. Später wurde der Film mit deutschen Sprechern synchronisiert. Die Stimme von Yves übernahm der Satiriker und Schauspieler Oliver Kalkofe. Der Schauspieler Friedrich Mücke spricht Manou, der Komiker Dominik Kuhn synchronisiert das schwäbisch-brasilianische Perlhuhn Parzival.

Die Animation orientiert sich an der Sprachaufnahme. Die Layouts bestehen oft nur aus einer Kamerafahrt und Positionsbeschreibungen für die Vögel. Dazwischen muss die Animation eingefügt werden. Haas hatte vor Luxx Erfahrungen beim Hannoveraner Trickfilmstudio Ambient & Friends an der Arbeit für den Animationsfilm „Urmel aus dem Eis“ gesammelt. Durch diese Kontakte entstand für Manou eine Kooperation.

Inkompatible Pipelines

Ambient hat von Luxx Layout und Storyboards sowie die fertigen 3D-Modelle bekommen und erstellte anhand dieser Vor-

lagen etwas über 20 Minuten Feinanimation. Das Problem: Luxx setzt die Filmsequenzen im 3D-Animationsprogramm 3ds Max um, das sich um viele Effekte sowie Flüssigkeits- und Partikelsimulationen erweitern lässt. Ambient arbeitet mit Maya, das aber eher auf Animation ausgelegt ist. Viele für die Produktion wichtige Plug-ins sind nicht für beide Plattformen verfügbar. Für die Dauer des Projekts hat Ambient auf 3ds Max umgestellt. Selbst entwickelte Skripte und Plug-ins sollten den Filmemachern den Wechsel in die ungewohnte Arbeitsumgebung erleichtern.

Der Film besteht aus 100 Sequenzen und insgesamt 1580 einzelnen Einstellungen, die an 60 bis 70 Schauplätzen spielen. Manche der Sets im Maßstab der Vögel bestehen nur aus einem Felsvorsprung mit ein paar Möwen drauf. Das größte Modell umfasst die Stadt Nizza mit Hunderten von Häusern und Straßen.

Haufenweise Einstellungen

Jede Einstellung besteht aus mehreren Dutzend Elementen und wird etwa 15- bis 20-mal beurteilt: zunächst als Preview, dann im ersten, zweiten und dritten Compositing, schließlich mit Texturen, mit Beleuchtung, mit Korrekturen. Das kleine Studio wuchs an diesen Aufgaben. „Bei White House Down haben wir etwa 80 Shots mit insgesamt acht Minuten Länge größtenteils in Full-CG hergestellt. Bei Independence Day waren es schon über 15 Minuten Film. Der Sprung auf 1580 stellte in vielerlei Hinsicht eine neue Herausforderung dar“, erzählt Haas.

Ein fest angestellter Software-Entwickler hat für Luxx eine Projektverwaltung komplett in Python geschrieben. Dazu gehören die Luxx Toolbar, eine Dateiverwaltung, ein Datenbanksystem, das auf MySQL basiert und ein Video-Player mit Notizfunktion. Luxx nutzt außerdem einen selbst entwickelten Bildskalierer mit künstlicher Intelligenz, der ein Google-API einbindet, um gering aufgelöste Texturen auf die erforderliche Größe hochzurechnen. Hinzu kommen etliche Skripte, Tools und kleine Plug-ins für 3ds Max. Die Software läuft auf Windows-PCs und Windows-Servern mit Raid-Systemen.

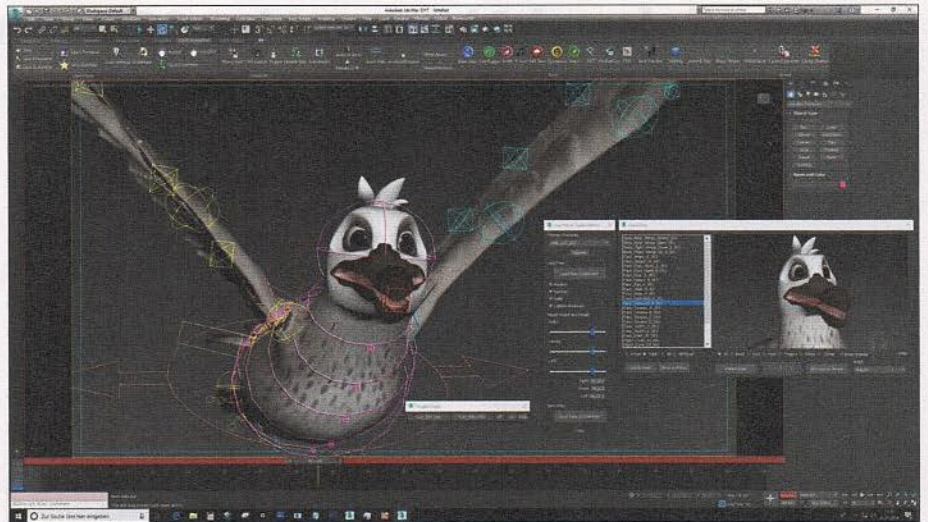
Security mit Disney-Zertifikat

Aufgrund einer Security-Zertifizierung, die Disney für die Kooperation verlangt, darf das Studio aus dem Produktionsnetzwerk heraus nicht auf das Internet zugreifen. Das gestaltete einige Aspekte des

Workflows mit Ambient schwierig. „Wir haben die Disney-Marvel-Zertifizierung, obwohl wir bisher nicht für Disney gearbeitet haben“, erzählt Haas. „Das kommt uns bei der Zusammenarbeit mit großen Filmstudios zugute, da die Disney-Zertifizierung als sehr streng gilt.“

Das Filmunternehmen verlangt die Zertifizierung, bevor es überhaupt Angebote annimmt. Die Regeln sind streng: Der Unternehmensbereich mit Internetzugang muss deutlich von dem Bereich getrennt sein, in dem mit Filmmaterial der Produktionsfirma gearbeitet wird. Das Material darf nur über ein verschlüsseltes Punkt-zu-Punkt-VPN an eine bestimmte IP-Adresse geliefert werden. Disney verlangt darüber hinaus Überwachungskameras in speziellen Bereichen, einen feuerfesten Datentresor mit einem bestimmten Mindestgewicht und Dokumentation über die An- und Abwesenheit von Mitarbeitern und Besuchern.


Im Tresor liegen stapelweise Festplatten wie Goldbarren. Bei einem 3D-Animation



Erst die Sprache, dann das Bild: Die Bewegungen von Lippen beziehungsweise Schnäbeln richten sich nach den englischsprachigen Tonaufnahmen.

tionsfilm fallen viele Daten an: 62 TByte liegen auf dem Produktionsserver, die gleiche Menge noch einmal auf einem Backup-Server. Nach den Aufräumarbei-

ten wandern 40 TByte für den Film ins Archiv und hüten all die Details der 88 Minuten, die ab Ende Februar im Kino zu sehen sind. (akr@ct.de) **ct**

Besuchen Sie uns vom 26.- 28. Feb. in Nürnberg  **embeddedworld**
Exhibition & Conference
... it's a smarter world
Erleben Sie neue Produkte auf unserem Stand 2-638 in Halle 2

AS20 Lüfterloser DIN Hutschienen-PC



- Intel® Atom E3815 2x 1,46 GHz
- 2x GB-LAN, 6x COM, 1x VGA
- 1x MiniPCIe für WiFi/BT/3G/4G
- Temp.: -20° ~ +60°C
- 5x USB 2.0, 1x USB 3.0

AE67 Lüfterlos Temp.: -20° ~ +60°C



- Pentium 4415U o. Core i5-7200U
- Intel HD Graphics 620 für 4K
- Erweiterter Temperaturbereich
- 1x HDMI, 1x DP, 1x VGA
- 4x USB 3.0, 4x USB 2.0, 6x RS232

DT340T 14" Rugged Tablet Core-i 8. Generation



- Intel® Core i5/i7 8. Gen.
- Helles Display, opt. NVIDIA Grafik
- Wasser- und Staubfest: IP65
- MIL-STD-810G, MIL-STD-461F
- Win10 IOT, Win10pro

FPZ-08 A80 8" Rugged Tablet Android 8.1



- Dünn, robust, leicht (500g)
- 8-Core CPU MSM8940
- 3GB RAM, 32GB Flash
- LTE, BT, GPS, NFC, UHF
- Temp.: -20° ~ +60°C

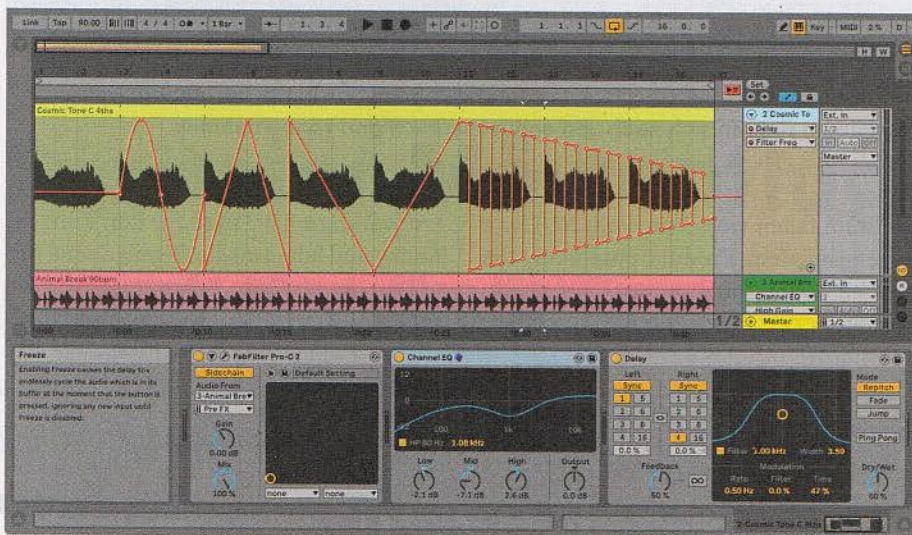
Erster Blick auf Ableton Live 10.1

Das neueste Update der Musiksoftware unterstützt unter anderem VST3-Plug-ins und vorgeformte Automationskurven.

Dank VST3 kann man in der öffentlichen Beta-Version von Ableton Live 10.1 endlich auch Sidechain-Signale direkt von jedem externen Ziel-Plug-in auswählen. Damit lässt etwa eine Kick-Drum einen

Kompressor für einen Flächenklang rhythmisch pumpen. Zudem sollen die Plug-ins besser abgeschirmt werden, damit sie bei einem Fehler nicht das ganze Live-Programm zum Absturz bringen.

Im Arrangementfenster lassen sich jetzt vorgeformte Steuerkurven wie Sinuswellen, Dreieck oder Sägezahn per Mausklick zeichnen, am Taktraster ausrichten sowie über Rampen ein- und ausblenden.



Per Sidechain lässt sich nun jedes externe Plug-in mit fremden Signalen triggern.

Das vereinfacht die Automation von Parametern, zumal man nun auch auf einem Touchpad per Pinch-Geste zoomen kann.

Die beiden neuen Effekte „Channel-EQ“ und „Delay“ haben es in sich. Der Channel-EQ ahmt einen analogen 3-Band-Equalizer nach und eignet sich für einfache Frequenzanpassungen mit weichen Übergängen. Das neue Delay kann Zeit und Frequenzspektrum seiner Echos modulieren und das Eingangssignal auf Wunsch einfrieren. Zusammen mit dem in Live 10 eingeführten „Echo“ deckt Ableton damit eine große Bandbreite ab, die viele kommerzielle Delays hinter sich lässt.

Schließlich kann der Wavetable-Synth der Live Suite nun beliebige Samples als Oszillator einsetzen. Einfach ein Sample auf das Instrument ziehen, schon generiert der Synth automatisch einen Wavetable für weitere Klangexperimente.

Live 10.1 Beta 12 lief bei uns stabil. Allerdings kann man mit Live 10.1 gespeicherte Projekte bei einem eventuellen Problem nicht in Live 10.0 laden.

Das Update ist für Besitzer von Live 10 kostenlos, es steht auf ableton.com/beta bereit. Die Vollversion ist in verschiedenen Ausbaustufen zu Preisen zwischen 79 und 599 Euro erhältlich. (hag@ct.de)

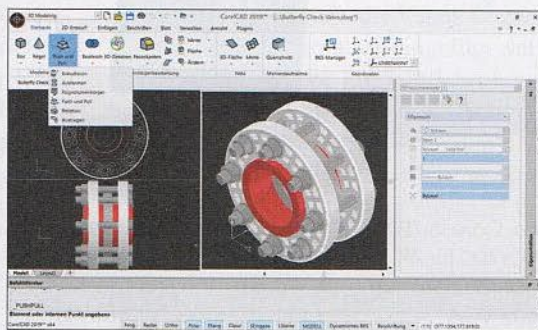
Schneller konstruieren mit CorelCAD 2019

Die 2019er Ausgabe von CorelCAD hält verbesserte Werkzeuge für **Konstruktionszeichnungen in 2D und 3D** parat. Anwender können beispielsweise per „Polyvolumenkörper“ 3D-Objekte mit polygonalen Wänden festlegen und über „Push und Pull“ einen massiven Strang aus einem 2D-Umriss wachsen lassen, als würde er mit einem Extruder ausgepresst.

Anhand von Regeln lassen sich mehrfach verwendbare 2D-Objekte definieren, die ihre Position und Größe dynamisch an die jeweilige Zeichnung anpassen – das spart Zeit bei häufig wiederkehrenden Elementen. Zum **3D-Druck und Austausch mit AutoCAD** unterstützt Corel-

CAD 2019 die Dateiformate STL und DWG. Das für macOS und Windows verfügbare Programmpaket kostet 830 Euro, ein Update ist für 300 Euro erhältlich.

(hps@ct.de)



Dank der 3D-Modeling-Funktionen lässt sich CorelCAD wie ein virtueller Extruder benutzen.

Kurz & knapp: Musik

Bitwig Studio 3 erweitert die DAW im zweiten Quartal um einen modularen Baukasten mit über 120 Synthesizermodulen. Die Beta soll in Kürze auf bitwig.com bereitstehen.

Native Instruments bietet mit dem **M32** ein besonders günstiges **Keyboard** mit kleineren Tasten und komplette-Kontrol-Integration an. Im Preis von 119 Euro ist unter anderem auch die Maschine-Software enthalten.

Korg will noch im Februar **Gadget 2** veröffentlichen. Das Update der übersichtlichen Musiksoftware läuft neben iOS und macOS nun auch unter Windows und bringt ein MIDI-Out-Modul mit.

Spiegellose Vollformatkamera von Panasonic

Panasonic hat Daten und Preise zu den Vollformat-Kameras Lumix S1 und S1R veröffentlicht. Die Modelle treten in direkte Konkurrenz zu Nikons Z- und Sonys A7-Serie.

Die Kameraserie mit Vollformat-Sensor von Panasonic soll im März erscheinen. Sie orientiert sich hinsichtlich Preis und Ausstattung eng an den Produkten von Nikon und Sony. Die Panasonic Lumix S1 soll 24 Megapixel auflösen und 2500 Euro kosten – ebenso wie die Nikon Z6 und die Sony A7 III. Die Lumix S1R liegt laut Hersteller preislich bei 3700 Euro und löst 47 Megapixel auf. Damit orientiert sie sich an der Nikon Z7 und der Sony A7R III. Beide Modelle kommen mit 5-Achsen-Bildstabilisator. Der Hybrid-Autofokus nutzt Gesichts- und Augenerkennung für Menschen, Hunde, Katzen und Vögel.

Panasonic verwendet ebenso wie Sigma das L-Bajonett von Leica. Dafür

kündigt der Hersteller zunächst drei passende Objektive an: die Festbrennweite Lumix S Pro 50mm F1.4 für 2500 Euro, das Standardzoom Lumix S 24-105mm F4 Macro O.I.S. für 1400 Euro und das Telezoom Lumix Pro S 70-200mm F4 O.I.S. für knapp 1900 Euro.

Beide Kameras bringen einen doppelten Kartenslot mit, der jeweils Platz für eine SD-Karte mit UHS-II-Unterstützung und eine XQD-Karte bietet. Das Magnesiumgehäuse soll Staub und Spritzwasser draußen halten und Kälte bis -10 °C widerstehen. Der Touchscreen auf der Rückseite misst 8,1 Zentimeter in der Diagonalen und ist um drei Achsen schwenkbar. Der OLED-Sucher löst mit 1600 × 1200 Pixeln höher auf als der von Nikon oder Sony.

Ihre Stärke spielen die Lumix-S-Kameras beim Thema Video aus: Sie zeichnen 4K-Video mit bis zu 60 Bildern pro Sekunde auf. Im 6K-Fotomodus sollen



Die S-Serie von Panasonic mit Vollformatsensor löst ebenso viel auf wie die Konkurrenz von Nikon und Sony.

die Kameras sogar etwa 30 Fotos pro Sekunde mit jeweils 18 Megapixeln schießen können.
(akr@ct.de)



Convention für digitale Transformation.

Speaker-Day am 9. April: Expert-Panel, Impulsvorträge und Praxistipps von 20 Experten auf 3 Bühnen

After-Show-Party am 9. April

Workshop-Day am 10. April: 7 ganztägige Workshops zu verschiedenen Online-Disziplinen z.B. SEO, Online-Marketing, ...

**9.–10. April 2019
Karlsruhe**

Exklusiv für c't Magazin Leser

10% Rabatt auf den Ticketpreis mit dem Aktionscode: **hallo.ct**

www.hallo.digital

Sponsoren und Partner

Sparkasse
Karlsruhe

Digital

inovex

CyberForum

DIZ
INTELLISHOP

GRENKE
Kultur- und
Kreativwirtschaft
Karlsruhe

FHS

Medienpartner

digital
phoenix

GROWTHUP

WEBSITE BOOSTING

suchradar

ct

Netzpiloten



Die Staatsanwaltschaft von New York ermittelt: Apple rutschte bei den Qualitätskontrollen ein schwerwiegender Bug in der VoIP-Anwendung FaceTime durch.

US-Politiker werfen Apple mangelnde Transparenz vor

Die FaceTime-Lücke zeige, wie iPhones zur „Spionage-Maschine“ werden können, kritisieren zwei US-Abgeordnete.

Apples Handhabung eines schweren Fehlers im VoIP-Dienst FaceTime stößt auf scharfe Kritik. Die Schwachstelle belege, dass „diese Geräte die ultimativen Spionage-Maschinen werden können.“ Das meinen der Vorsitzende des amerikanischen Energie- und Wirtschaftsausschusses, Frank Pallone, und die für Fragen des Verbraucherschutzes zuständige Abgeordnete Jan Schakowsky.

Angreifer, die ihr eigenes Konto einem FaceTime-Gruppenchat selbst hinzufügen, konnten anschließend Mikrofone von iPhones, iPads und auch Macs ohne Wissen der Nutzer aus der Ferne aktivieren.

Die beiden Abgeordneten bemängeln, dass Apple bislang den hohen Grad an Transparenz vermissen lässt, den eine derart gravierende Sicherheitslücke erfordert. Der Konzern müsse öffentlich schildern, welche Schritte er unternommen hat, um die Privatsphäre der Nutzer zu schützen.

In einem Fragenkatalog an Apple-Chef Tim Cook fordern die Politiker Antworten darauf, wann der Konzern von der Schwachstelle erfahren hat und ob es ähnliche, bislang unter Verschluss gehaltene Bugs gebe. Vor allem soll aber geklärt werden, ob Apple schon von der Schwachstelle wusste, bevor das Unternehmen kontaktiert wurde – der 14-jährige Sohn einer Familie hatte die Lücke am 19. Januar bemerkt und versucht, umgehend zu melden. Öffentlich reagierte Apple aber erst Ende Januar und schaltete die Gruppenfunktion serverseitig vorübergehend ab.

Die FaceTime-Gruppenfunktion hat die Firma mit iOS 12.1 im Oktober 2018 eingeführt. Die Politiker wollen nun wissen, welche Prüfungen die Funktion vor der Freigabe durchlaufen hat und warum die Schwachstelle nicht aufgefallen war. Außerdem soll Tim Cook beantworten, ob Apple plant, betroffene Nutzer über die Verletzung ihrer Privatsphäre zu informieren und diese zu entschädigen. **Mittlerweile klagt ein Anwalt gegen Apple**, der befürchtet, dass Dritte seine geheimen Gespräche belauscht haben. Die New Yorker Staatsanwaltschaft ermittelt. (dz@ct.de)

MacBook-Tastatur aus Glas

In einem frisch veröffentlichten Patentantrag an das US-Patent- und Markenamt (USPTO) beschreibt Apple, wie eine Glasplatte eine Tastatur ersetzen könnte. Dabei handelt es sich nicht um einen flachen Touchscreen. Stattdessen sind die Bereiche, in denen virtuelle Tasten sitzen, erhaben. Auf erkannte Eingaben soll die Tastatur per Vibration antworten und so ein **taktils Feedback** liefern.

Ein ähnliches Konzept setzt Apple seit Jahren in MacBooks um; diese simulieren Tastendrücke auf das Trackpad mit einem Vibrationsmotor (Taptic Engine). Abgesehen vom Einsparen an mechanischen Verschleißteilen hätte eine virtuelle Tastatur auch den Vorteil, dass sie sich an verschiedene Landessprachen allein per Software anpassen ließe. (dz@ct.de)

Ethernet und Strom für iPhone und iPad

Zubehörspezialist Belkin hat einen Ethernet-Adapter mit Lightning-Anschluss für Apples Smartphones und Tablets angekündigt. Er eignet sich beispielsweise für **Kassensysteme**, die auf iOS-Geräten gründen. iOS-Versionen ab 10.3.3 binden den Adapter automatisch ein.

Die Lightning-Buchse ist durchgeführt, sodass sich das iOS-Gerät während des Ethernet-Betriebs laden lässt. Das geht auch via Power-over-Ethernet (PoE). Der Adapter gibt laut Belkin bis zu zwölf Watt ab, kann so also auch ein iPad vollladen. Der maximale Durchsatz beträgt laut Belkin 480 MBit/s, was die Obergrenze des auf USB 2 basierenden Lightning-Anschlusses darstellt. In der Praxis dürfte wegen des USB-Overheads deutlich weniger herauskommen.



Lightning-Buchse durchgeführt: der Ethernet-Adapter von Belkin

Der Ethernet- und Stromadapter mit Lightning-Connector kostet 100 Euro und soll ab Anfang Februar in Apples Ladengeschäften erhältlich sein. (dz@ct.de)

Exoskelett bewegt die Hand

Mit einem neu entwickelten Hand-Exoskelett kann ein Mensch mit Lähmungen wieder greifen.

Die Konstruktion erlaubt es, die gelähmte Hand zu spreizen oder einzelne Finger zu bewegen. Das neue Hand-Exoskelett der Universität Stuttgart besteht aus einer zentralen Montageeinheit und beweglichen Fingermodulen. Motor und Elektronik wiegen etwa 400 Gramm, das gesamte Exoskelett etwas weniger als ein Pfund. Patienten mit einer gesunden Hand können die Apparatur selbstständig anlegen.

Das am Unterarm befestigte Gerät ist mit Elektromyografie-(EMG-)Sensoren ausgestattet. Diese Elektroden messen selbst schwache Muskelaktivitäten am Unterarm, deren Signale dann die Motoren des Exoskeletts steuern; ein Verfahren, das aber bei vielen Varianten der Lähmung nicht anwendbar ist. Für die Zukunft planen Projektpartner der Uniklinik Tübingen,

Das leichte Exoskelett steuert jeden Finger der Hand einzeln.

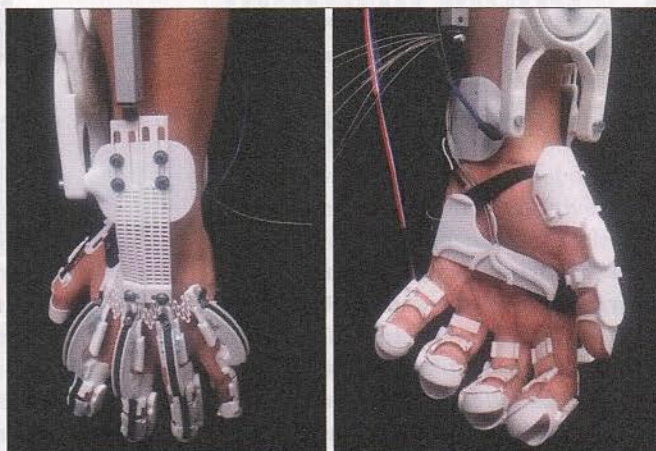


Bild: Uni Stuttgart

gen, die Handfunktionen direkt mit Hirnströmen steuern zu lassen, beispielsweise in Verbindung mit Augenbewegungen.

Eine zusätzliche Funktion soll in Zukunft mit verschiedenen Greiftechniken auf unterschiedliche Alltagsobjekte eingehen und damit das Greifen sicherer

machen. Mit einer kamerabasierten 3D-Objekterkennung versuchen Wissenschaftler der Hochschule Reutlingen, Gegenstände schon früh zu identifizieren und einzuschätzen, um dann den dafür passenden Griffmodus voreinzustellen.

(agr@ct.de)

Köln. KOMED,
1.-3. April 2019

building **IoT**

Die Softwareentwicklerkonferenz zu Internet of Things und Industrie 4.0

Treff für IoT-Gestalter

AUS DEN VORTRÄGEN

- IoT-Projekte in großen Organisationen
- Wie man 50.000 Geräte gegen ihren Willen vernetzt
- IoT-Sensorik 2.0: Machine Learning im Sensor
- Hardware in the Docks – Container in der Embedded-Welt
- Secure Smart Home Development

Programm online!

WORKSHOPS

- MQTT Deep Dive
- Continuous Deployment im Embedded-Umfeld
- Datenanalyse und ML skalieren mit PySpark
- Embedded- und ML-Modelle mit TensorFlow Lite und uTensor

Goldsponsoren:

adesso | business people technology

BOSCH
Technik fürs Leben

HIVEMQ

codecentric

com2m
connecting software solutions

tarent

Bronzesponsoren:

ASQF®
Das Expertennetzwerk

CONTACT
Software

Veranstalter:

Developer

dpunkt.verlag

www.buildingiot.de

Haben wir schon immer so gemacht

Alte Nameserver-Technik bedroht die öffentliche Hand

DNSSEC bringt Sicherheit bei der Abfrage von IP-Adressen. Man sollte erwarten, dass Internet-Provider der Politik mit gutem Beispiel den Weg dorthin weisen. Die Wirklichkeit sieht anders aus.

Von Marcus Fauré

Eigentlich waren die Weichen richtig gestellt: Als das Land Nordrhein-Westfalen .nrw-Domains für Städte und Kommunen reservierte, war DNSSEC von Anfang an dabei. Doch als einige Städte ihre Domains zu eigenen Providern brachten, wollten sich die neuen Verwalter anscheinend nicht mit dem Thema befassen. Bei der Hälfte wurde die Sicherheitstechnik abgeschaltet. Die andere Hälfte erwischte es schlimmer: DNSSEC blieb aktiviert, war aber auf den Nameservern nicht konfiguriert, sodass mehrere hundert Domains un erreichbar wurden.

Dabei ließen sich solche Störungen technisch verhindern, wenn das zur Domainverwaltung meist eingesetzte Extensible Provisioning Protocol bei einem Nameserver-Wechsel Schlüsselmateriale automatisch entfernen würde, falls der Admin kein neues konfiguriert. Bei .de-Domains ist das schon so – die zuständige Denic setzt auf ein eigenes Protokoll. Derzeit fordert aber niemand eine solche Erweiterung für EPP. Immerhin sind alle Registrare vertraglich verpflichtet, DNSSEC zu unterstützen.

Dass es trotzdem so schlecht klappt, liegt kaum am Aufwand. DNS-Server werden moderat mehrbelastet; sie beantworten weniger Anfragen mit dem schlanken UDP, aber mehr mit dem aufwendigeren TCP. DNSSEC-Signaturen berechnen gängige DNS-Server auf Knopfdruck. Ganz ohne Mühe geht es zwar nicht, weil Registrare den öffentlichen Teil des Key Signing Key (KSK) einer Domain an die Registry melden müssen. Aber schon ab rund 1000 Domains stellt eine Infrastruktur, die das erledigt, für Registrare keinen nennens-

werten Aufwand mehr dar. Schwieriger ist die Schulung von Supportmitarbeitern. DNSSEC bringt kein Geld ein und Vorteile sind für Websitekunden nicht so greifbar wie etwa mehr Speicherplatz. Domaintransfers werden jedoch komplizierter. Das macht die Rechnung für knapp kalkulierende Anbieter einfach: Sie ignorieren DNSSEC weitgehend.

Das BSI fordert DNSSEC schon länger. Aus gutem Grund, denn es sind schon Angriffe auf die Namensauflösung bekannt geworden (siehe ct.de/ykb6): Nutzer der Webseite MyEtherWallet verloren Kryptogeld durch einen DNS-Hack. Die Türkei leitete twitter.com nach regierungskritischen Meldungen auf eine eigene Webseite um. Die TLD .io hätte leicht Opfer einer Nameserver-Übernahme werden können.

Wie es klappen kann

Die Situation wird sich vor allem dann bessern, wenn Nutzer DNSSEC gezielt anfragen. Öffentliche Einrichtungen sollten in ihren Ausschreibungen konkret Sicherheit einfordern und die Umsetzung sicherstellen. Ein ähnliches Potenzial haben auf DNSSEC aufbauende Techniken mit sicht-

barem Mehrwert. Der Grundstein dazu ist schon gelegt. Fingerabdrücke von SSL-Zertifikaten lassen sich bereits DNSSEC-gesichert im Nameservice hinterlegen (DANE, DNS-based Authentication of Named Entities). Würden Webbrowser DANE nutzen, wäre das fehlerträchtige, aber teure System mit Zertifizierungsstellen größtenteils überflüssig. Mailserver nutzen den Mechanismus bereits.

Eine verpasste Gelegenheit war der DNS Flag Day vom 1. Februar. Er konzentrierte sich auf die Protokollerweiterung EDNS und klammerte fragwürdige SOA-Records oder DNSSEC aus. So bewertet der zugehörige EDNS-Test die für Prüfungen absichtlich fehlerkonfigurierte Domain dnsec-failed.org irreführenderweise positiv. Die Aufmerksamkeit für die Aktion hätte größeren Nutzen erzielen können.

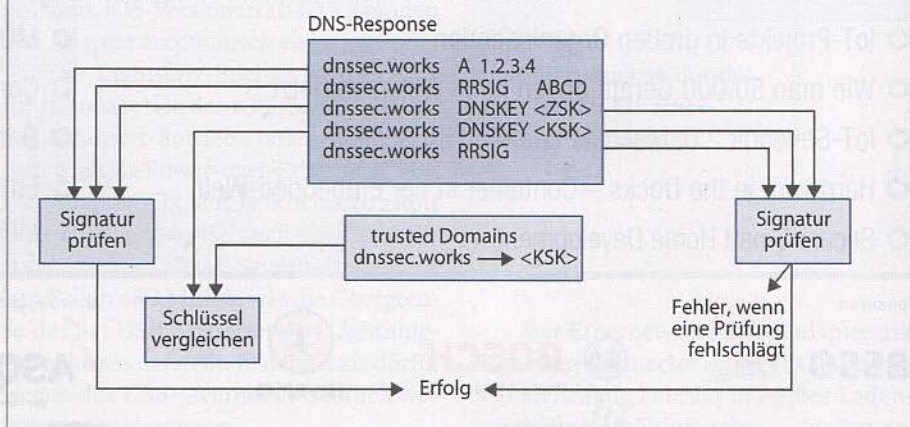
Wie man DNSSEC etablieren kann, zeigen etwa die Niederlande oder Tschechien. Durch konsequente Lobbyarbeit bei den eigenen Registraren haben diese Länder eine DNSSEC-Verbreitung von über 50 Prozent erreicht, Tendenz steigend. Der Betreiber der Top-Level-Domain .eu fördert die Technik mit Rabatten bei den Domaingebühren. Und Institute, die die Top-Level-Domain .bank nutzen wollen, sind verpflichtet, DNSSEC einzusetzen – hier sind 100 Prozent der Domains signiert. (dz@ct.de) **ct**

DNS-Attacken und Gegenmaßnahmen
ct.de/ykb6

Marcus Fauré ist Gründer und Geschäftsführer des Providers Global Village.

Sicherheitsgewinn durch DNSSEC

Der Empfänger einer signierten DNS-Antwort kann anhand zweier Schlüssel prüfen, ob die Nachricht unverfälscht ist und ob der Sender der Nachricht vertrauenswürdig ist.



Omas Roboter hat Geduld

Roboterhilfe bietet eine Chance, im Alter selbstbestimmt zu leben. Aber wie sollte der **seniorengerechte Roboter** aussehen und sich verhalten? Forscher der Uni Siegen haben Senioren befragt und mit ihnen Situationen nachgestellt. Ihr Roboter Sympartner fährt selbstständig, ist etwa 1,50 Meter groß, bietet eine Ablagefläche und trägt vorn einen Tablet-PC, der verschiedene Funktionen anbieten kann. Das Wichtigste ist seine soziale Aufgabe: Der Senior soll sich nicht einsam fühlen. Darf der Roboter zum Wecken ins Schlafzimmer kommen? Für viele Ältere ist das ein No-Go. Sympartner bleibt also zur Weckzeit draußen, tut geschäftig und fährt auf und ab.

Psychologen rieten dazu, den Serviceroboter nicht menschenähnlich zu gestalten. Die Stärke des Roboters liegt gerade darin, dass er kein Mensch ist. Die Maschine ist unendlich geduldig, wiederholt Sätze beliebig oft, kann auch sehr langsam fah-



Sympartner als täglicher Begleiter: Manche Senioren sahen den Testroboter als Ding, andere als Freund.

ren. „Maschinen nehmen Menschen so, wie sie sind, sie beurteilen sie nicht“, betont Professor Marc Hassenzahl. Niemand muss ihnen danken und keiner muss ein schlechtes Gewissen haben, dass er einem Roboter zur Last fällt. (agr@ct.de)

Uni Kiel hinterm Mond

Als erste Sonde überhaupt ist die chinesische Chang'e-4 auf der Rückseite des Mondes gelandet. Mit an Bord ist ein **Strahlenmessgerät** aus den Laboren der Kieler Christian-Albrechts-Universität. Zuvor kamen Instrumente der Kieler bereits bei Missionen der amerikanischen NASA und der europäischen ESA zum Einsatz. Das Besondere am neuen Lunar Lander Neutron and Dosimetry (LND) ist, dass das kompakte Gerät neben elektrisch geladener Strahlung auch elektrisch neutrale Neutronen und Gamma-Strahlung messen kann. Diese Strahlungen könnten Astronauten und Mondkolonisten gefährlich werden, da sie tief im Körper Krebs auslösen können. Außerdem ist das LND in der Lage, durch den Nachweis einer bestimmten Neutronen-Strahlung Wasser im Mondboden aufzuspüren.

(agr@ct.de)

HE Minds Mastering Machines

14.-16. MAI 2019

CONGRESS CENTER ROSENGARTEN,
MANNHEIM

DIE KONFERENZ FÜR MACHINE LEARNING UND KÜNSTLICHE INTELLIGENZ

PROGRAMM ONLINE!
Frühbucher bis 22. März 2019

In den Vorträgen und Workshops geht es u.a. um:

- Grundlagen von Machine Learning, Deep Learning und Reinforcement Learning
- Anwendungen, z.B. in Text- und Sprachverarbeitung, Bilderkennung oder Prediction
- Herausforderungen wie Interpretierbarkeit, Small Data, Operationalisierung
- Tools wie Keras, TensorFlow, PyTorch und Model-Management-Frameworks
- Fortgeschrittene Themen: Neural Embeddings, Wahrscheinlichkeitsmodelle, Security
- Praxisbeispiele aus dem Flugzeugbau und der Werkstoffbearbeitung
- DSGVO und andere rechtliche Aspekte beim Einsatz von ML und KI

WWW.M3-KONFERENZ.DE

Goldsponsor

 **NOVATEC**

Veranstalter





heise **Developer**



dpunkt.verlag

Datenausbeutung

Das Bundeskartellamt legt sich mit Facebook an

In einem Aufsehen erregenden Beschluss attestiert die deutsche Wettbewerbsbehörde Facebook eine marktbeherrschende Stellung. Der Konzern soll seine Datensammelpraxis einschränken, ansonsten drohen hohe Geldstrafen.

Von Holger Bleich

Die angefasste Reaktion von Facebook zeigte, dass das Bundeskartellamt am 7. Februar mit Verve in ein Wespennest gestochen hatte. Die Behörde hat den US-Konzern auf einem seiner Kernmärkte – nämlich Deutschland – scharf angegriffen. Sie hat Facebooks gängige Praxis, massenhaft Nutzerdaten zu sammeln, zu aggregieren und auszuwerten, in Teilen verboten – zumindest dann, wenn keine informierte Einwilligung des Nutzers vorliegt.

Fast drei Jahre lang hatte das Bundeskartellamt die Wettbewerbssituation der am deutschen Markt präsenten Social-Media-Plattformen und das konkrete Gebaren von Facebook durchleuchtet. Dies sei in enger Kooperation mit den Datenschutzbehörden geschehen, betonte das Kartellamt. In diesem Verfahren betrat es nämlich Neuland: Erstmals musste es den potenziellen Missbrauch von Big-Data-Praktiken einordnen – und dabei die seit Mai 2018 neue europäische Rechtslage (EU-Datenschutz-Grundverordnung, DSGVO) berücksichtigen.

Ausbeutungsmissbrauch

In einem ersten Schritt hat die Behörde ermittelt, dass ihrer Ansicht nach Facebook auf dem deutschen Markt für soziale Netzwerke marktbeherrschend ist und somit der kartellrechtlichen Missbrauchskontrolle unterliegt. Google+ sei ausgeschlossen, LinkedIn und Xing seien nicht in direktem Wettbewerb, Snapchat, Twitter, YouTube, Instagram oder Pinterest deckten andere Bedarfe ab als Facebook und seien damit ebenfalls außen vor. Lock-in-, Skalen- und Netzwerk-Effekte würden dafür sorgen, dass zusätzliche

„Hürden für Wechsel zum Wettbewerb“ vorhanden sind.

Diese marktbeherrschende Position, so die Argumentation des Bundeskartellamts, nutze Facebook widerrechtlich aus, indem es sich über bestehendes europäisches Datenschutzrecht hinwegsetzt. Der Konzern beute seine Nutzer aus. Das vorgeworfene Delikt heißt tatsächlich „Ausbeutungsmissbrauch“ oder juristischer „Konditionenmissbrauch“.

Konkret geht es um die gängige Praxis, über die Plattform hinaus Nutzer im Web bei jeder sich bietenden Gelegenheit zu beobachten. Das betrifft sowohl die zum Konzern gehörenden Dienste Instagram und WhatsApp als auch die Social-Plug-ins auf Websites, den Log-in-Service und Facebook Analytics.

Das Bundeskartellamt hat Facebook nun untersagt, Nutzerdaten aus diesen Quellen zusammenzuführen, solange keine ausdrückliche Einwilligung des Kunden vorliegt. Diese Einwilligung darf nicht an die Nutzung gekoppelt sein, sprich: Die Dienste müssen dem Kunden auch zugänglich sein, wenn er die Einwilligung verweigert.

Fehlt die Einwilligung, muss Facebook die Datensammelei einschränken oder die Daten anonymisieren. Der Kon-

zern hat nun vier Monate Zeit zu erklären, wie er das technisch löst. Die Vorschläge will die Behörde dann genau prüfen. Das Kartellamt droht mit einem Bußgeld, insbesondere aber mit der ihm zustehenden Möglichkeit, fortlaufende Zwangsgelder zu verhängen. Es sei beispielsweise möglich, zehn Millionen Euro pro Monat zu verlangen, falls Facebook sich nicht an die Vorgaben hält.

Andreas Mundt, Präsident des Bundeskartellamts, gab sich bei der Erläuterung der Entscheidung selbstbewusst: „Wir nehmen bei Facebook für die Zukunft eine Art innere Entflechtung bei den Daten vor.“ Mundt sparte nicht mit Kritik am Geschäftsmodell von Facebook: „Diese Unternehmen überziehen uns mit einer neuen wirtschaftlichen Ordnung“, begründete der Behördenchef seinen derzeitigen Fokus auf Internetunternehmen.

Beleidigte Reaktion

Facebook reagierte regelrecht beleidigt auf die Entscheidung: „Wir haben über fast drei Jahre mit dem Bundeskartellamt kooperiert und werden unseren Dialog mit der Behörde fortsetzen. Ungeachtet dessen lehnen wir die Auffassung des Bundeskartellamts entschieden ab.“ Man sei keineswegs marktbeherrschend: „Wir haben in Deutschland einen harten Wettbewerb mit anderen Diensten, doch das Bundeskartellamt hält es für irrelevant, dass unsere Apps mit YouTube, Snapchat, Twitter und vielen anderen Wettbewerbern um die Aufmerksamkeit der Nutzer konkurrieren.“ Außerdem habe Facebook alle DSGVO-Vorgaben umgesetzt. Die Daten „dienstübergreifend zu nutzen hilft uns auch dabei, die Sicherheit der Menschen zu verbessern.“ Der Konzern hat bereits angekündigt, Beschwerde gegen den Beschluss am zuständigen Oberlandesgericht Düsseldorf einzulegen.

Mit seiner Kritik steht Facebook nicht allein da. Die Entscheidung des Bundeskartellamts beruhe auf einer „ebenso eigenwilligen wie fragwürdigen Interpretation des neuen europäischen Datenschutzrechts“, kommentierte etwa der Datenschutzexperte Professor Nico Härting. Ohnehin sei die Durchsetzung der DSGVO Aufgabe der Datenschutzbehörden: „Schützenhilfe durch nationale Wettbewerbsbehörden ist weder nötig noch vorgesehen. Auf dem Weg zu einem einheitlichen europäischen Datenschutzrecht sind Querschüsse nationaler Behörden kontraproduktiv.“ (hob@ct.de) **ct**



Andreas Mundt, Präsident des Bundeskartellamts: „Wir nehmen bei Facebook für die Zukunft eine Art innere Entflechtung bei den Daten vor.“

Bild: Torsten Klein

Sorgen um Werbeblocker-Erweiterungen für Chrome

Mit dem Plan, die Erweiterungsschnittstelle von Chrome zu ändern, haben die Chrome-Entwickler massive Kritik auf sich gezogen. Die Änderung soll die bisher sehr weitgehenden Rechte von Erweiterungen einschränken.

Für Kontroversen sorgt das declarativeNetRequest-API (siehe ct.de/yr2r). Es regelt das Blockieren der von einer Webseite angeforderten Inhalte – also das zentrale Feature vieler populärer Erweiterungen wie Werbeblocker und Sicherheits-Add-ons. Die Entwickler wollen so Sicherheitsprobleme mit Erweiterungen verhindern. Probleme dieser Art, etwa das Ausspähen privater Daten, waren in der Vergangenheit häufig aufgetreten.

Während Erweiterungen bisher frei entscheiden können, ob bestimmte Ressourcen geblockt werden oder nicht, macht das neue API klare Vorgaben. Ähnlich wie in den von Adblock Plus verwendeten Listen bestehen sie aus Suchmustern wie „abc*d“. Allerdings wollen die Chrome-Entwickler die Blocklisten auf 30.000 Einträge beschränken – weniger als die Hälfte der beliebten „EasyList“.

Erweiterungen wie uBlock Origin oder uMatrix wären völlig aus dem Spiel, klagten deren Entwickler: Beide durchsuchen nicht einfach Listen, sondern

arbeiten komplexere Regeln ab. Für Adblock Plus sähe es kaum besser aus. Und auch Antiviren- oder Kinderschutzprogramme wären mit dem neuen API passé. Entwickler so unterschiedlicher Software wie Privacy Badger, F-Secure oder AdGuard waren sich in ihrer Kritik an declarativeNetRequest einig.

So berechtigt die Sicherheitsanliegen der Chrome-Entwickler auch sind, steht ein Verdacht im Raum: Will sich das weitgehend werbefinanzierte Unternehmen Google, das vor einem Jahr selbst einen eher schwachen Werbefilter in Chrome eingebaut hat, unliebsame Erweiterungen vom Hals schaffen, die dem eigenen Geschäft schaden?

Das Chrome-Team bemüht sich derzeit um Deeskalation: Es gehe nicht darum, Werbeblocker aus dem Browser

hinauszudrängen, sondern sie im Gegenteil schneller und sicherer zu machen – und im Übrigen werde sich der Entwurf noch ändern, schrieb ein Chromium-Entwickler.

Die Diskussion fokussiert sich zwar auf die neue Block-Schnittstelle, doch auch andere Vorschläge stehen in der Kritik. Geplant ist unter anderem, Erweiterungen das Nachladen externen Codes zu verbieten, die Zugriffsrechte auf offene Seiten einzuschränken und als Hintergrundprozesse nur noch ServiceWorker zuzulassen. Vieles davon ist sinnvoll, würde aber für Erweiterungsentwickler eine Menge Arbeit bedeuten. Allein die Umstellung auf ServiceWorker dürfte Tausende von Erweiterungen unbrauchbar machen.

(jo@ct.de)

declarativeNetRequest-API: ct.de/yr2r

urlFilter	Matches	Does not match
"abc"	https://abcd.com https://example.com/abcd	http://ab.com
"abc*d"	https://abcd.com https://example.com/abcxyzd	http://abc.com
"[a.example.com]"	https://a.example.com/ https://b.a.example.com/xyz	http://example.com/
"[https]"	https://example.com	http://example.com/ http://https.com
"example^123 "	https://example.com/123 http://abc.com/example?123	https://example.com/1234 https://abc.com/example0123

Das neue API beherrscht nur simple Regeln – für viele Werbeblocker reicht das nicht aus.

TDT® | Wenn Sicherheit zählt

Bundesamt
für Sicherheit in der
Informationstechnik

ISO 27001 Zertifikat
auf der Basis von IT-Grundschutz

Zertifikat Nummer:
BSI-IGZ-0294-2017
gültig bis: 06.09.2020

- BERATUNG & PLANUNG
- NETZWERKMANAGEMENT
- SUPPORT - BIS ZU 24/7/365
- SECURITY MADE IN GERMANY
- FIRMWAREANPASSUNGEN
- NETZWERKMONITORING
- CUSTOM ROUTER DESIGN



Kernel-Log

Linux 5.0: Ruckelfrei zocken, schnellerer Datenaustausch

Der nächste Linux-Kernel macht einen Teil des Performance-Verlusts wieder wett, den die Spectre-Gegenmaßnahmen kosten. Der endgültige Umstieg auf die modernere Block-Layer-Infrastruktur zwingt Storage-Admins zum Umdenken. Gamer dürfen sich über Support für AMDs Freesync freuen.

Von Thorsten Leemhuis

Eine der meist diskutierten Neuerungen des nächsten Linux-Kernels ist nur eine kosmetische: Der am 25. Februar erwartete Nachfolger von Linux 4.20 trägt nicht die Versionsnummer 4.21, sondern die 5.0. Zu sagen hat der Sprung nichts: Die Änderungen sind nicht zahlreicher oder bedeutender als sonst; auch wurden nicht mehr alte Zöpfe abgeschnitten als üblich. Denn wie schon bei ähnlichen Sprüngen zuvor erfolgte auch der jetzige nur, weil Torvalds die zweite Zahl der Versionsnummer zu groß wurde. Oder wie er sagte: „Mir gehen die Finger und Zehen zum Zählen aus.“

Zurückerobern!

Zu den wichtigsten Neuerungen zählen Optimierungen, durch die Linux 5.0 beim Versenden von UDP-Paketen und Einsatz des Netzwerk-Schnellverarbeitungswegs XDP wieder nahezu die Performance erreichen soll, die Linux Ende 2017 erzielt hat. Das ist einigen Änderungen am DMA- und Netzwerkcode zu verdanken, die den Overhead von Retpoline erheblich reduzieren, das vor der Anfang 2018 bekannt gewordenen Prozessor-Sicherheitslücke Spectre v2 schützt. Die Linux-Entwickler diskutieren derweil mit „Static Calls“ und „Optpolines“ zwei weitere Ansätze, um die Einbußen von Retpoline generell zu reduzieren; noch ist allerdings ungewiss, ob sie die Praxisreife erreichen.

Für viel Aufsehen sorgten bei Linux 5.0 vorgenommene Aufräumarbeiten, die ZFS On Linux (ZOL) kaputt gemacht haben, weil es eine bislang genutzte Funktion aufgrund einer Lizenzkennzeichnung und -Durchsetzungstechnik nicht mehr verwenden kann. Die ZOL-Entwickler haben das Problem in ihrem Hauptentwicklungszweig mittlerweile umschifft, wie der Artikel auf Seite 186 erläutert. Der beschäftigt sich auch mit weiteren Anpassungen des neuen Kernels, die proprietären Treibern gezielt Knüppel zwischen die Beine werfen. Damit wollen einige Linux-Entwickler vor allem Nvidia treffen.

Ruckelfrei spielen

Der für AMDs moderne Grafikchips zuständige Kernel-Treiber Amdgpu beherrscht jetzt Freesync, das Bildstörungen wie Tearing oder Ruckler vermeiden hilft. Das gelingt durch dynamische Anpassung der Bildwiederholrate, daher wird die auf VESA Adaptive Sync aufbauende Technik auch Variable Refresh Rate (VRR) genannt. Zum Freesync-Einsatz ist neben dem neuen Linux-Kernel auch das für Februar angesetzte Mesa 19.0 nötig, denn erst der darin enthaltene OpenGL-Treiber von AMD bringt alles Nötige mit; ferner muss auch der Treiber für den X-Server die Technik unterstützen, sofern man einen solchen einsetzt. AMDs proprietäres Treiberpaket beherrscht Freesync schon länger.

Die erstmals beiliegende Schriftart „Terminus 16x32“ verhilft der Textkonsole auf HiDPI-Displays zu einer adäquaten Größe. Das ist vor allem für Bootprozess und Embedded-Systeme interessant, denn eine zu hochauflösenden Bildschirmen passende Schrift kann man schließlich auch zur Laufzeit einstellen (siehe Tipps & Tricks der c't 4/19, S. 157).

NSA ausbooten

Linux unterstützt jetzt die Stromchiffren XChaCha12 und XChaCha20. Auf ihnen baut der ebenfalls neue Verschlüsselungsalgorithmus Adiantum auf, den Dm-

Crypt/Cryptsetup/LUKS und das von Ext4 und F2FS verwendete Fscrypt jetzt nutzen können, um Daten zu ver- und entschlüsseln. Adiantum stammt von Google und wurde für leistungsschwache Android-Geräte entwickelt, denen Kryptobeschleuniger für das üblicherweise bei der Datenträgerverschlüsselung verwendete AES fehlen. Ursprünglich hatte das Unternehmen geplant, das von der National Security Agency (NSA) entwickelte und daher viel kritisierte Speck zu nutzen. Kaum dass Mitarbeiter von Google den Speck-Support in den Linux-Kernel integriert hatten, verkündete das Unternehmen allerdings eine Kehrtwende und stellte wenig später HPolyC vor, aus dem Adiantum hervorging. Letzteres soll sogar schneller als Speck sein, das wieder entfernt wurde, weil niemand sonst Interesse daran vorbrachte.

Apropos NSA: Linux unterstützt nun auch den in RFC 6986 definierten Hash-Algorithmus Streebog, der zu den russischen Standardalgorithmen für Kryptografie („GOST Algorithmen“) zählt. Er wurde vom russischen Inlandsgeheimdienst FSB als Alternative zu SHA-3 mitentwickelt. Genau wie bei der von der NSA beigesteuerten und schon lange in Linux enthaltenen Sicherheitstechnik SELinux sind solche Ursprünge aber kein Ablehnungsgrund, solange die Implementierung sauber scheint.

Moderner speichern

Die Kernelentwickler haben den älteren der beiden Block-Layer-Ansätze rausgeworfen; damit verschwinden auch I/O-Scheduler wie Deadline und CFQ, die viele Admins vom Performance-Tuning kennen. Wer Datenträgerzugriffe optimieren will, muss sich daher mit dem neueren, seit Linux 3.13 im Kernel enthaltenen Ansatz auseinandersetzen – dem Multi-Queue Block IO Queueing Mechanism (Blk-Mq), der mit mehreren Warteschlangen arbeitet und nun die Basis der gängigen Storage-Treiber bildet. Der zugehöri-



The numbering change is not indicative of anything special. If you want to have an official reason, it's that **I ran out of fingers and toes to count on, so 4.21 became 5.0**. There's no nice git object numerology this time (we're about 6.5M objects in the git repo), and there isn't any major particular feature that made for the release numbering either. Of course, depending on your particular interests, some people might well find a feature **they** like so much that they think it can do as a reason for incrementing the major number.

So go wild. Make up your own reason for why it's 5.0.

Der Sprung von 4.x auf 5.0 erfolgte, weil Linus Torvalds die „Finger und Zehen zum Zählen ausgehen“.

ge Scheduler Mq-Deadline arbeitet ähnlich wie der entfernte Namensverwandte und ist daher recht simpel und vorhersehbar. Komplexer ist der im weiteren Sinne aus CFQ hervorgegangene BFQ, der die anstehenden I/O-Aufgaben eher mal umsortiert oder wartet, um Reaktionsgeschwindigkeit oder Durchsatz zu steigern.

Auf Btrfs-Dateisystemen lassen sich jetzt Auslagerungsdateien ablegen. Das ist für Distributionen wie Ubuntu interessant, die standardmäßig mit Auslagerungsdateien arbeiten. Das Ganze klappt aber nur unter bestimmten Bedingungen, daher darf das Btrfs-Volume etwa nur aus einer Partition bestehen.

Der neben Virtio-SCSI vielfach beim Virtualisieren eingesetzte Storagetreiber Virtio-Blk kann den Host nun per Discard darüber informieren, wenn Speicherbereiche virtueller Datenträger keine Daten mehr enthalten, weil dort liegende Dateien gelöscht wurden. Das kann Performance und Lebensdauer von SSDs verlängern, wenn der Host das per Trim-Befehl an die SSD weitergibt. Außerdem ist das Ganze interessant, um Image-Dateien virtueller Maschinen (VMs) zu schrumpfen.

Schneller netzwerken

Linux bringt jetzt einen Client (auch Initiator oder Host genannt) und einen Server (Target) mit, um über TCP-Verbindungen auf NVMe-Datenträger zuzugreifen (NVMe over Fabrics). Außerdem kann der Kernel per UDP eingehende Pakete jetzt sammeln und in größeren Bündeln an die Zielapplikation übergeben, was den Durchsatz steigert und zugleich den Prozessor entlastet. Durch dieses „Generic Receive Offload (GRO) für Plain UDP Sockets“ legte der Durchsatz bei einem Test des Entwicklers von 1079 auf 1466 MByte/s zu.

Im Speicherbereich von Programmen liegende Daten kann Linux jetzt via UDP versenden, ohne sie zuerst im Arbeitsspeicher duplizieren zu müssen. Dieser Zero-

copy-Ansatz reduziert den Overhead und verspricht, die Performance zu steigern; TCP unterstützt Ähnliches bereits seit Linux 4.14.

Die Sicherheitsfunktion Seccomp (Secure Computing) kann jetzt ein Userspace-Programm zurate ziehen, um zu entscheiden, ob eine Tätigkeit eines anderen Programms erlaubt oder verboten wird. Container-Managementprogramme sollen diese Funktion nutzen können, um Containern etwa das Anlegen grundlegender und ungefährlicher Gerätedateien (etwa /dev/zero oder /dev/null) zu erlauben, das Erstellen anderer jedoch zu unterbinden. So ein Managementprogramm könnte auch Kernel-Module auf dem Host nachladen, wenn Software in Containern diese anfordert. Dabei geht es somit um Regeln, die sich mit einem Userspace-Programm einfacher und flexibler programmieren lassen als im Kernel.

Steuern, was wo läuft

Über die modernere Variante der Control Groups (Cgroups v2) lässt sich jetzt steuern, welche Prozessorkerne oder Speicherbereiche die zugeordneten Prozesse nutzen; das ist etwa für besonders leistungsstarke NUMA-Systeme interessant, damit die Prozesse (und somit auch Container oder VMs) wenn möglich lokalen Arbeitsspeicher verwenden.

Intels Ablaufverfolgungs- und Performance-Monitoring-Technik Processor Trace (PT) lässt sich jetzt auch in VMs nutzen. Außerdem hat KVM eine neue Betriebsart gelernt, um Gastsysteme ohne BIOS zu booten und so den Start zu beschleunigen.

Linux 5.0 unterstützt Nvidias als Tegra194 oder Xavier bekannte ARM-Prozessoren. Ebenfalls neu ist Basissupport für die von Freescale Semiconductor/NXP gefertigten Prozessoren der i.MX8-Familie. Zu der gehört auch der SoC, den Purism beim Linux-Smartphone Librem 5 einsetzen will; Support für dessen Ent-

wicklerboard oder das Smartphone selbst enthält Linux 5.0 aber nicht.

Linux unterstützt jetzt das Bussystem MIPI I3C, das auch als SenseWire bekannt ist; es soll das weit verbreitete I2C beerben, um Sensoren oder andere Prozessoren anzubinden.

Viele neue Treiber

Die Entwickler haben ferner den Hardware-Support wieder signifikant erweitert, denn sie haben Dutzende neuer Treiber integriert und Hunderte existierende verbessert. Alles aufzulisten würde mehrere c't-Seiten füllen, daher folgen nur einige Beispiele.

Der neue Kernel unterstützt die Touch-Funktion des 7-Zoll-Touch-Displays für den Raspberry Pi, das raspberry.pi.org vertreibt. Neu dabei ist auch ein Treiber für das Cougar 700K Gaming Keyboard. Ferner haben die Entwickler den Support für Mäuse mit hochauflösendem Scrollrad verbessert. Die neue Kernelversion kann bereits die Temperatur der zweiten Generation von AMDs Zen-Prozessoren auslesen. Linux 5.0 unterstützt zudem die Audio-Einheit einiger neuer Ryzen-G-Prozessoren besser und weiß weitere Varianten der VEGA-Grafikchipfamilie von AMD anzusprechen. Der Kernel bringt ferner Basis-Support für GPUs aus Nvidias Turing-Reihe, die bei der GeForce-RTX-2000-Serie zum Einsatz kommt. Neu dabei ist auch ein Treiber für einen AQtion 2.5/5-Gbit-USB-Ethernet-Adapter von Aquantia.

Das neue Energy Aware Scheduling (EAS) soll helfen, den Energieverbrauch bei Prozessoren mit ARMs big.LITTLE zu senken, in denen unterschiedliche energiehungrige CPU-Kerne stecken. Durch EAS kann der Scheduler bekanntermaßen simple und kurzlebige Prozesse an schwache und sparsame Kerne senden, während er rechenintensive gleich stärkeren zuteilt. Ohne eine Lösung wie EAS verbrauchen solche SoCs mehr Strom als nötig und spielen zugleich ihr Performance-Potenzial nicht aus. Mit solchen SoCs bestückte Android-Geräte bringen daher meist einen der vielen Vorläufer von EAS mit, die in den vergangenen sieben Jahren entstanden. Keiner davon konnte allerdings die Ansprüche der Entwickler des Prozess-Schedulers erfüllen. EAS hat das jetzt geschafft – ist aber auch bewusst simpel gehalten, daher bietet es noch viel Raum für Verbesserungen, an denen bereits gearbeitet wird.

(thl@ct.de) **ct**

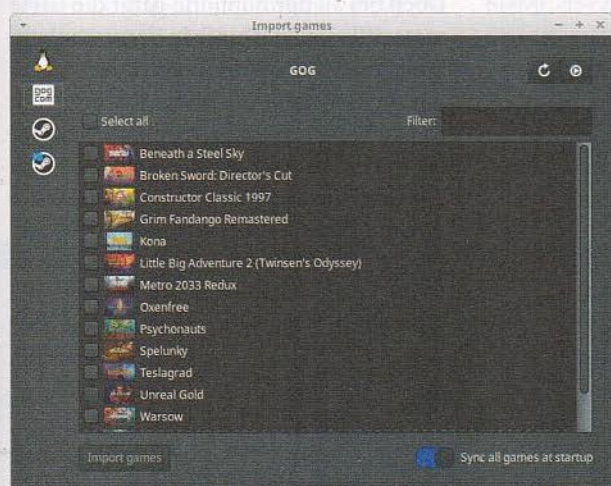
Lutris importiert Spiele von GOG.com & Co.

Die Linux-Software Lutris vereint sämtliche Spiele auf einer **grafischen Oberfläche**, egal ob sie über die Paketverwaltung, über Steam oder auf anderem Weg eingerichtet wurden. Selbst alte Retro-Schätzchen für C64, Atari & Co. bindet die Software ein und installiert den passenden Emulator.

Die neue Version 0.5 kann erstmals direkt Spiele von der Online-Plattform GOG.com importieren. Windows-Spiele, die nur mit der Hilfe von Wine oder der Windows-Version von Steam laufen, kann das Programm ebenfalls einrichten. Dabei verwaltet das Open-Source-Tool verschie-

dene Wine-Versionen und übernimmt die Installation des Windows-Steam-Clients. Lutris beherrscht nun auch die Installation von CAB-Komponenten, die Unterstützung für die Windows Media Foundation liefern.

Bereits installierte Spiele lassen sich in Lutris einfach importieren. Weitererichtet man mithilfe von Community-Skripten von der Projekt-Website ein. Die dazu praktische Suchfunktion wurde mittlerweile ins Programm integriert. Lutris 0.5 steht auf der Projekt-Website zum Download bereit. Für einige Distributionen gibt es Paketquellen. (lmd@ct.de)



Mit wenigen
Mausklicks importiert
Lutris unter Linux
zahlreiche Spiele
von verschiedenen
Anbietern.

Kurz & knapp: Linux

Das Debian-Projekt hat die siebte Aktualisierung seiner stabilen Linux-Distribution **Debian GNU/Linux 9 Stretch** veröffentlicht. Das Point-Release 9.7 korrigiert einen Fehler im Paketmanager apt, der eine gravierende Sicherheitslücke darstellt.

Die neueste Version 0.14.0 der **Desktop-Umgebung LXQt** stattet den Dateimanager PCManFM mit einer zweigeteilten Ansicht aus. Jetzt lassen sich Icons für Computer, Netzwerk, Home-Verzeichnis und Mülleimer auf dem Desktop ablegen.

Die **Free Software Foundation Europe** (FSFE) hat eine Broschüre mit dem Titel „Public Money? Public Code!“ veröffentlicht, die als kostenloser Download zur Verfügung steht (siehe ct.de/yh3s). Die Publikation untersucht den Einsatz freier Software zur Modernisierung der öffentlichen Infrastruktur.

Die neue Version der Linux-Distribution **Slax 9.7.0** ist jetzt noch kleiner. Neu dabei ist usb-modeswitch für USB-Geräte sowie das Kommando slax activate, das Module in den RAM kopiert.

Download der Broschüre: ct.de/yh3s

Ihr Erste-Hilfe-Set: Das Notfall-System für den Ernstfall

Jetzt für 12,90 € bestellen.

Desinfec't
Das Notfall-System für den Ernstfall

Windows-PCs untersuchen und säubern
Trojaner und Viren beseitigen
Daten retten und sofort wiederherstellen

Auf DVD & als Download
für USB-Sticks

NEUE VERSION 2018/19

Die DVD für die Virenjagd

- Mit 4 Scanmodi: Auto, Fast, 1-Secur, Synchro
- Kein Root-Laufwerk nötig
- ISO zum Download
- Auf USB-Stick installierbar

JETZT NEU! c't wissen Desinfec't 2018/2019

Dank Desinfec't 2018/2019 analysieren Sie Ihr bedrohtes Windows-System aus mehreren Blickwinkeln: Viren aufspüren, Hardware untersuchen, Daten sichern. Vier Viren-Scanner und TeamViewer helfen Ihnen auch bei der Fernwartung.

Auch als Download erhältlich.
shop.heise.de/desinfec2018-19

12,90 € >

shop.heise.de/desinfec2018-19 service@shop.heise.de

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 15 €.

Auch auf USB-Stick erhältlich!

heise shop
shop.heise.de/desinfec2018-19 >



Bild: Sunday Alamba/dpa

Afrikas Start-up-Träume

Nigerias IT-Pläne landen in der harten Realität

Mit Blick auf die Wahlen in Nigeria hoffen IT-Investoren auf eine glorreiche Cyber-Zukunft. Doch die realen Probleme holen sie ein.

Von Andreas Schuchardt

Nigeria hat sich in der virtuellen Welt bislang vor allem durch die sogenannte „Nigeria Connection“ einen Namen gemacht. Per Mail wurden Menschen in Deutschland und Europa überraschende Erbschaften von erheblicher Höhe in Aussicht gestellt. Für deren Empfang seien allerdings Vorabzahlungen von mehreren tausend Euro fällig. Mal für angebliche Anwalts- und Ausfuhrgebühren, mal zur aufwendigen chemischen Reinigung stark verschmutzter Geldscheine. Naiven Zeitgenossen wurden so Millionen aus der Tasche gezogen, während sich die versprochenen Reichtümer in Luft auflösten.

Das soll nun Vergangenheit sein. Heute verweist Westafrikas Regionalmacht stolz auf eine eigene, kleine legale IT-Hochburg namens „Yabacon Valley“. Im Stadtviertel Yaba der Metropole Lagos residieren viele neu entstandene Unternehmen der noch jungen Tech-Szene.

„Nachdem wir erst vor ein paar Jahren Basis-Telefonie ins Hinterland gebracht haben, sprechen wir nun über die Anwendung künstlicher Intelligenz und maschinellen Lernens“, verkündete Sunday Dare, Manager der Nigerian Communications Commission (NCC) vor Industriellen in Lagos. Per Datengewinnung und Cloud-Entwicklung werde die Dienstleistungsbranche ein neues Niveau erreichen. Die dazu nötigen Weichen sollen bei den Parlaments- und Präsidentschaftswahlen am 16. Februar 2019 gestellt werden. Beobachter erwarten ein enges Rennen zwischen dem greisen Amtsinhaber Muhammadu Buhari und seinem auf Privatisierung und freie Märkte setzenden Herausforderer Atiku Abubakar.

Programmierer für 290 Euro

Der Ausgang der Wahl wird von Investoren weltweit mit Spannung erwartet. Allein von Januar bis September 2018 sammelten nigerianische Start-ups fast 120 Millionen Dollar an Investitionen ein. Der Großteil der knapp hundert Firmen ist in der Finanz- und Medienbranche aktiv.

Weitere 100 Millionen Dollar konnte das Unternehmen Andela Anfang 2019 einstreichen. Zu den Geldgebern gehören

neben Facebook-Gründer Mark Zuckerberg auch das von Al Gore gegründete Generation Investment Management. Die Arbeitsbedingungen in Nigeria versprechen ihnen hohe Gewinne. Andela beschäftigt 1100 Software-Entwickler zu deutlich niedrigeren Gehältern, als in den USA und Europa üblich sind: In den ersten Jahren verdienen die afrikanischen Entwickler umgerechnet nur 290 Euro im Monat. Zu den Kunden von Andela zählen unter anderem Google und Microsoft.

Für den zuständigen Minister Dr. Adebayo Shittu ist denn auch die IT- und Telekom-Industrie der „Schlüssel zum Wirtschaftswachstum“. Nigeria sei mit seiner durchschnittlich sehr jungen Bevölkerung eine „Konsumenten-Nation“.

Andere Sorgen

Doch bei all der Euphorie gerät die harte materielle Realität rasch in Vergessenheit. So kämpfen Armee und Polizei seit zehn Jahren gegen die islamistische Guerillatruppe Boko Haram – ein Bürgerkrieg, der bis heute 27.000 Tote forderte, zwei Millionen Menschen zu Flüchtlingen machte und die Infrastruktur schwer schädigte.

Die Energieversorgung ist ein Dauerproblem. 60 Millionen Einwohner müssen ihren Strom mit Dieselgeneratoren selbst erzeugen. Unterschlagungen und Korruption in großem Stil gehören zum Alltag. Nach UN-Berechnungen entgingen dem Land allein 2018 aufgrund von Straftaten im Bereich der Erdölförderung Einnahmen von rund 2,5 Milliarden Euro.

Bei einem just auf magere 65 Euro pro Monat angehobenen Mindestlohn ist es ein sehr weiter Weg zur herbeigewünschten Konsumgesellschaft: Die Inflation liegt bei 12 Prozent, die Arbeitslosenquote bei 23. Mehr als die Hälfte der Nigerianer lebt unter der Armutsgrenze. „Die Angehörigen der Mittelschicht haben kein Geld, deswegen gibt es keine Kunden“, zitierte die „Financial Times“ Geschäftsleute in Lagos.

Angesichts dieser Lage können die meisten Nigerianer vom erhofften Internet-Boom allenfalls träumen: Nur knapp ein Drittel der 190 Millionen Einwohner kann per Mobilfunk im Web surfen, Zugang zu einem Festnetzanschluss haben weniger als ein Prozent. Wer immer auch die Wahlen gewinnt: Auf ihn warten große Herausforderungen. Nigeria wird kaum über Nacht so blühen, wie es die Spam-Mails der Märchenonkel einst versprochen.

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

Digitaler Filmdienst UltraViolet macht dicht

Diverse Blu-ray-Filme bringen Gutscheine für digitale Kopien auf UltraViolet mit. Ende Juli wird der Dienst nun eingestellt.

Wer bislang Filme oder TV-Serien auf Blu-ray Discs oder UHD kaufte, fand mitunter Gutscheine mit Download-Codes für UltraViolet in der Verpackung. Mit diesen Codes konnte man eine digitale Filmkopie der Blu-ray auf dem Smartphone, Tablet oder im Browser streamen. Alternativ lässt sich eine DRM-geschützte Kopie in eine Player-App laden, ohne den Kopierschutz der Disc knacken zu müssen.

Am 31. Juli 2019 schließt UltraViolet seine Pforten. Digitale Kopien der Filme stehen dort dann nicht mehr zur Verfügung. Höchste Zeit, die eigene Blu-ray-Sammlung nach Codes zu durchforsten.

Doch was passiert mit einer DRM-geschützten Filmsammlung, wenn der Anbieter dicht macht? Im Fall von UltraViolet

könnte man die Filme auf Festplatte laden und im UltraViolet-Player offline ansehen. Das geht solange gut, bis die Festplatte abbraucht oder die nicht mehr aktualisierte Player-App nicht mehr startet.

Praktischer ist da schon die Möglichkeit, seine UltraViolet-Sammlung auf einen anderen Anbieter zu übertragen. In Deutschland klappt das am besten bei Flixter. Der von Warner betriebene Service erlaubt es, weiterhin sämtliche UV-Filme per Flixter zu streamen und herunterzuladen. Die dazu nötige Verknüpfung der Nutzerkonten sollte man unbedingt bis zum 31. Juli auf www.myuv.com/retailers einrichten.

Flixter ist hierzulande der einzige Anbieter, der das volle UltraViolet-Angebot übernimmt und dessen Code-Einlösungen weiterhin akzeptiert. Das muss in Zukunft jedoch nicht so bleiben. In den Geschäftsbedingungen stellt der Mutterkonzern Warner klar, dass Filme und Serien



Um digitale Filme von UltraViolet zu behalten, müssen Kunden ihre Sammlung zu Flixter umziehen.

anderer Studios irgendwann einmal nicht mehr oder nur noch gegen eine Gebühr per Flixter abgerufen werden könnten. Man würde Kunden jedoch rechtzeitig darauf hinweisen und Gelegenheit geben, wegfallende Titel herunterzuladen.

Doch wie auch immer ein solcher Übergang aussieht: Das Vertrauen von Filmfans in digitale Sammlungen nimmt dadurch schweren Schaden. (hag@ct.de)

heise
MacDev

3.– 5. Dezember 2019
Karlsruhe, Haus der Wirtschaft

Die neue Entwicklerkonferenz von Mac & i

Die **heise MacDev** ist die erste Entwicklerkonferenz von Mac & i, dem Apple-Magazin der c't. Sie beschäftigt sich mit allen Aspekten der Softwareentwicklung für Apple-Geräte, also Mac, iPhone, iPad, aber auch Apple Watch und Apple TV.

Um unser Programm optimal auf die Teilnehmer zuzuschneiden, würden wir uns freuen, wenn Sie uns etwas über Ihre Interessen und Tätigkeitsschwerpunkte mitteilen.

Bitte geben Sie Ihre Interessen und Wünsche unter: <https://heise-macdev.de/> ein.

Call for Papers startet
am 15. März 2019

www.heise-macdev.de



Bild: FC Schalke 04 e.V.

Lukrative Hassliebe

E-Sport und Fußballvereine suchen kommerzielle Synergien

Die Bundesregierung hat die Gleichstellung des E-Sports versprochen, doch die Sportverbände treten auf die Bremse. Gleichzeitig steigen Fußballbundesligisten in das Millionengeschäft mit den Konsolensportlern ein.

Von Torsten Kleinz

Der Deutsche Olympische Sportbund erkennt die Bedeutung von E-Gaming als Teil einer modernen Jugend- und Alltagskultur an, nicht jedoch als eigenständige sportliche Aktivität. Mit dieser Positionierung hat der Deutsche Olympische Sportbund Ende 2018 den olympischen Träumen des organisierten E-Sports eine Absage erteilt: E-Sport-Vereine haben kurzfristig keine Chancen, in Deutschland den Status der Gemeinnützigkeit mit der gleichen Leichtigkeit zu erlangen wie ein Fußball- oder Schwimmverein.

Die Hoffnungen, als quasi normale Sportart anerkannt zu werden, waren in

der E-Sport-Branche groß – gerade dank des politischen Rückenwindes, den sie zuvor erfahren hatte. Mit ihrem Auftritt bei der Eröffnung der Gamescom 2017 hatte Bundeskanzlerin Angela Merkel eine politische Trendwende eingeleitet. Statt insbesondere vor „Killerspielen“ zu warnen, erkennen führende Politiker Spiele nun als aufstrebenden Wirtschaftszweig und wertvollen Teil der Jugendkultur an. Im Koalitionsvertrag steht dies sogar als explizites Versprechen: „Wir [...] werden E-Sport künftig vollständig als eigene Sportart mit Vereins- und Verbandsrecht anerkennen und bei der Schaffung einer olympischen Perspektive unterstützen“, heißt es in dem Dokument von SPD und CDU.

Aufpoliertes Image

Für die etablierten Sportverbände in Deutschland war dies jedoch ein Affront. „Ob E-Sport in die Welt des deutschen Sportes passt, entscheiden wir – und ob der E-Sport olympisch wird, bestimmt das Internationale Olympische Komitee“, betonte DOSB-Vorstandsvorsitzende Veronika Rücker auf der Sportrechte-Konferenz SPOBIS in Düsseldorf.

Insbesondere mit gewalthaltigen Titeln wie etwa Counter-Strike wollen die Sportfunktionäre nichts zu tun haben. Deshalb hat der Dachverband eine Trennlinie gezogen: So seien „elektronische Sportartensimulationen“ – wie etwa FIFA – ein zukunftssträchtiges Betätigungsfeld der bestehenden Sportvereine. Der Rest des abfällig „E-Gaming“ getauften E-Sports soll jedoch in den etablierten Strukturen keinen Platz finden.

Ähnlich hatte sich auch der Chef des Internationalen Olympischen Komitees Thomas Bach geäußert und ausgeschlossen, dass E-Sport kurzfristig zur olympischen Disziplin werden könne. Dabei sind die Spiele selbst für E-Sportler kaum attraktiv, da der Veranstaltungszyklus viel zu lange ist für die schnelllebige Branche. Doch wäre E-Sport olympisch, würde ein Automatismus in Gang gesetzt, der den E-Sport-Mannschaften von Steuerfreiheit bis zur staatlichen Nachwuchsförderung viele Vorteile verschaffen würde.

Konsumorientierte Fans

Auch dies sorgt für die Ablehnung durch die Sportverbände. Denn längst sind die Newcomer zu Konkurrenten aufgestiegen. Wenn die Jugendlichen lieber an der Konsole als auf dem Trainingsplatz ihre Runde ziehen, droht den klassischen Sportarten ein Nachwuchsproblem. Und auch auf der Einnahmenseite macht sich die Konkurrenz bereits bemerkbar. Denn inzwischen verteilen immer mehr Sportsponsoren wie Versicherer oder Autohersteller ihre Etats auch auf Konsolenspieler.

Die E-Sport-Industrie verspricht den großen Weltmarken ein junges, begeistertes Publikum, das über klassische Werbung zunehmend schwerer zu erreichen ist. Auf der SPOBIS zeigte Christine Schröder-Schönberg, die die Sponsorengelder des Transportkonzerns DHL betreut, wie das Publikum eines von DHL mitfinanzierten E-Sport-Turniers den Konzern mit Sprechchören begrüßte – auf den Rängen eines Fußballstadions kaum vorstellbar.

Ein weiterer Grund für die Ablehnung der Verbände ist die Furcht, an die Seite gedrängt zu werden. So können Spielehersteller ohne jede Mitwirkung der Vereine oder Verbände zentrale Regeln verändern und den Sport ihren eigenen Interessen unterordnen. In Düsseldorf verbalisierte Brandon Snow, Chief Revenue Officer der Activision Blizzard Esports Leagues, die Horrorvision der Funktio-

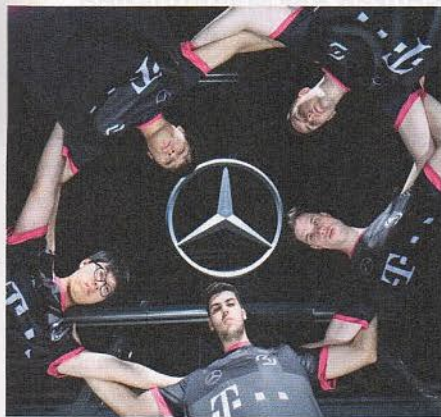
näre: „Uns gehört nicht nur der Ball oder das Stadion, uns gehört die gesamte Liga.“ Sich mit einem kompletten Verbandssystem mit widerstrebenden Interessen auseinanderzusetzen erscheint angesichts dieser Machtfülle unnötig.

Millioneneinsätze

Für die Spielehersteller ist der E-Sport eine attraktive Option. Wer einen Titel als E-Sport etabliert, kann sich zum einen über jahrelange Nachfrage in einem sehr schnelllebigen Geschäft freuen. Gleichzeitig eröffnet der E-Sport neue Monetarisierungsmöglichkeiten. Wo Millionen an Sponsorgeldern fließen, müssen Hersteller nicht auf umstrittene Methoden wie Loot-Boxen oder Pay-to-Win-Modelle zurückgreifen, um Umsätze jenseits des Verkaufspreises zu erzielen. Zudem bemühen sich die Hersteller, zunehmend ins Geschäft mit Fanartikeln einzusteigen.

Für den E-Sport öffnet sich damit auch das Geschäft mit den Übertragungsrechten. So startete der deutsche Anbieter Sport1 im Januar einen eigenen E-Sport-Kanal, der unter anderem in den kostenpflichtigen Sport-Paketen der Pay-TV-Anbieter ausgestrahlt wird.

Wie viel Geld bereits im E-Sport steckt, zeigt Hersteller Riot Games, der die Europa-Liga für seinen Titel League Of Legends Ende 2018 auf ein Franchise-System umgestellt hat. Zehn Bieter konnten die exklusiven Lizenzen erwerben. Der Kostenpunkt lag dabei jeweils zwischen 8 und 10,5 Millionen Euro. Für das Geld erwarben die Franchise-Nehmer nicht nur einen dauerhaft sicheren Antrittsplatz, sondern auch einen Anteil an den zentralen Einnahmen der Liga durch Sponsoring und Fanartikel.



Sponsoren wie Daimler zielen auf ein junges, konsumfreudiges Publikum.

Bild: Daimler

Einer der Lizenznehmer ist einer der etabliertesten Namen des deutschen Sports: Der FC Schalke 04 engagiert sich seit 2016 im E-Sport und hat neben FIFA und Pro Evolution Soccer auch League Of Legends ins Portfolio aufgenommen. Obwohl die Anfangsinvestitionen beträchtlich waren, spricht der Club mittlerweile von einem funktionierenden Geschäftsmodell, das neue Millioneninvestition rechtfertigt. So schauten laut Angaben von Riot Games 99,6 Millionen Zuschauer das Finalspiel zwischen Invictus Gaming und Fnatic an.

Obwohl prominente Fußballfunktionäre wie Uli Hoenes sich immer wieder verächtlich über den E-Sport äußern, stimmt die Liga mit den Füßen ab: So nehmen bereits 22 Teams aus der 1. und 2. Fußballbundesliga an der „VBL Club Championship“ teil – auch bekannt als die „virtuelle Bundesliga“. Gespielt wird dort FIFA 19.

Kommerz statt Breitensport

Die Allianz zwischen Fußball und E-Sport kommt nicht von ungefähr. Bundesligavereine sind schon lange Unterhaltungskonzerne mit eigenen Mediensparten und damit ebenso streng kommerziell ausgerichtet wie die E-Sport-Szene. Zwar findet man auch im E-Sport mitgliedergetriebene Vereine, allerdings spielen sie hierzulande nur eine untergeordnete Rolle. Grund dafür ist eben auch, dass sie nicht die Steuerprivilegien und die gesellschaftliche Akzeptanz herkömmlicher Sportvereine genießen.

Für kommerzielle Vereine sind die Bundesligisten als Kooperationspartner attraktiv, weil diese das Geschäft mit Sponsoren und der Nachwuchsgewinnung in Jahrzehnten perfektioniert haben. Symptomatisch ist ein Deal, der Anfang Januar verkündet wurde. So übernahmen beim seit 1997 existierende E-Sport-Vorreiter SK Gaming zwei neue Partner das Ruder: der 1. FC Köln und Mercedes. Neben Investitionen in ungeannter Höhe bringen beide ihre Kompetenzen ein: Während der FC Köln den sportlichen Teil des Geschäfts verstärkt, kann der Autohersteller dafür sorgen, dass das Image des E-Sports weiterhin konsumentenfreundlich bleibt. „Ich bin sicher, dass wir gegenseitig voneinander viel lernen und profitieren werden“, erklärte SK-Gaming-Gründer Alexander Müller bei der Verkündung der neuen Partnerschaft. (hag@ct.de) **ct**

DER DATEN-MANAGER

FÜR STARKE FILESERVER

Datenbestand optimieren
In großen Umgebungen

Data Retention einführen
Ad hoc und regelbasiert

IT entlasten durch Prozesse
Mit Data Ownern und Fachabteilungen



Nutzbarkeit der
Daten optimieren
mit migRaven
Data Retention

« Data Retention macht die wichtigen Daten sichtbar, indem es den Rest verschwinden lässt »

secIT by Heise
HANNOVER 2019

Besuchen Sie uns auf der secIT 2019
www.aikux.com/secIT



Betrüger gesucht

Tools decken manipulierte Versicherungsfälle auf

Überteuerte Versicherungsfälle und manipulierte Fotos lassen sich heute automatisiert entlarven. Fake-Schadensberichte fallen in einer Autorenprüfung auf, für die als Testmaterial Beiträge von c't-Redakteuren dienen.

Von Arne Grävemeyer

Eine einfache, leicht durchzuführende Bildmanipulation kann einen Lackkratzer länger oder einen Brandfleck größer erscheinen lassen. Den Text einer unverdächtigen Schadensmitteilung kann man sich aus dem Internet ziehen. Diese Masche ist rechtlich dunkler als grau,

denn veränderte Fotos oder fremde Schadensberichte schildern abweichende Sachverhalte und überhöhte Schadenersatzansprüche. Es lockt die Chance auf schnelles Geld von der Versicherung. Aber Vorsicht, mit verschiedenen Software-Tools und künstlicher Intelligenz fischen erste Versicherer bereits automatisiert Manipulationen aus der Masse der Schadensmeldungen heraus.

Am Fraunhofer Institut für Sichere Informationstechnologie (SIT) ist in Zusammenarbeit mit einigen Kooperationspartnern ein ganzer Satz an Werkzeugen entstanden, die Bildmanipulationen aufdecken, falsche Rechnungsbeträge erkennen oder Berichte aus fremder Feder entlarven. Als Plug-ins wurden diese Tools in ein Demo-Schadenbearbeitungssystem des Fraunhofer Instituts für Arbeitswis-

senschaft und Organisation integriert. Ebenso probiert Arvato Financial Solutions die neuen Werkzeuge aus.

Spuren der Manipulation

„Bei der Bildmanipulation kann mit unserem Baukasten letztlich jeder Eingriff aufgedeckt werden“, erklärt Professor Martin Steinebach, Abteilungsleiter am Fraunhofer SIT. Sein Team hat in den vergangenen Monaten für jede erdenkliche Fotobearbeitung ein Plug-in entwickelt, das die entsprechende Änderung nachweist. Wenn beispielsweise ein Bildausschnitt skaliert wird, etwa weil ein Schaden größer erscheinen soll, dann entstehen dabei Pixellücken, die aufgefüllt werden müssen. Jede dafür eingesetzte Bearbeitungsmethode lässt sich anhand ihrer Interpolationen auf Pixelebene nachweisen.

Letztlich sind sechs Plug-ins entstanden, mit denen Versicherer schon heute in automatischen Durchläufen die Fotos eingehender Schadensmeldungen auf verschiedenste Bildmanipulationen prüfen können. Darunter ein sogenannter Duplicate Detector, der untersucht, ob Bildbereiche mehrfach verwendet worden sind. Der Duplicate Detector deckt Copy-and-Move-Aktionen auf, das vorherrschende Verfahren beim Retuschieren.

Da die am Projekt beteiligten Versicherungen ihre Teilnahme nicht öffentlich machen, zeigt Christian Winter, wissenschaftlicher Mitarbeiter am SIT, als Beispiel ein Fake-News-Foto aus den internationalen Nachrichten. Beim Test eines Abwehrraketen systems der iranischen Revolutionsgarde stiegen 2008 lediglich drei von vier Raketen hoch, eine nicht. Auf dem veröffentlichten Bild des Militärs starten aber alle vier Raketen. „Unser Plug-in zerlegte das Bild in seine Elemente und erkannte untypisch ähnliche Bereiche“, erklärt Winter. Der Algorithmus geht nicht pixelweise vor, denn das wäre zu aufwendig. Stattdessen bildet er zu einzelnen Bildsegmenten eine Art Hashwert und vergleicht zunächst diese. Erst bei einem Treffer ermittelt der Duplicate Detector den ganzen Umfang der Retusche, markiert die als kopiert erkannten Bereiche farbig und gibt Alarm.

Fremdbilder fallen auf

Weitere Tools mit Prüffunktionen sind der Camera Model Verifier, der die Metadaten zum Bild zu Rate zieht und prüft, ob diese zum Foto passen. Sogenanntes Image Splicing, also das Kopieren und Einfügen von Bildbereichen aus anderen Fotos, erkennt der Splicing Detector. Der Double JPEG Detector alarmiert, falls das JPEG-Verfahren mehrfach zur Komprimierung angewendet worden ist, beispielsweise beim Speichern nach Bearbeitungen. Falschen Verdächtigungen entgeht der gutwillige Versicherte daher, wenn er keine Änderungen an Fotos vornimmt, also nicht einmal den Kontrast erhöht, nicht komprimiert und auch keine Kreismarkierungen oder Pfeile ins Bild einfügt.

Schließlich gibt es noch zwei Plug-ins, die eingereichte Fremdbilder entdecken sollen. Das eine greift auf eine interne Datenbank mit bereits bekannten Fotos zu, und mit dem zweiten können gleiche Fotos im Internet aufgestöbert werden. „Im Grunde ist es sehr einfach, die Google-Suche einzubinden. Allerdings gibt es

in vielen Fällen rechtliche Bedenken, ob Kundenfotos bei Google hochgeladen werden dürfen“, schildert Winter. Als Alternative verwenden die Forscher die Bildersuchmaschine TinEye (www.tineye.com) eines kanadischen Entwicklerteams.

Während die Bildforensik vor allem vereinzelte Betrugsversuche aufdecken soll, für die sich eine aufwendige manuelle Recherche kaum lohnt, sucht die Ziffernanalyse nach auffälligen Abrechnungen im großen Stil. So lassen sich bei den Rechnungen einer betrügerischen Kfz-Werkstatt Besonderheiten erkennen, wenn Zahlbeträge über mehrere Quartale untersucht werden. Sehr einfach zu entlarvende Fälle wären wiederkehrende Zahlenfolgen oder Summen, die bemerkenswert häufig knapp unter einer Bagatellgrenze, etwa unter 1000 Euro, bleiben.

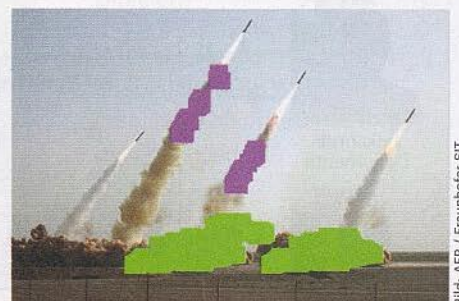
Komplexere statistische Kontrollverfahren ziehen unter anderem die Benford-Analyse heran. Dabei werden Gesetzmäßigkeiten berücksichtigt, nach denen Ziffernmuster empirisch auftreten sollten. Beispielsweise steht in Zahlensystemen,

die hierarchisch aufeinander aufbauen, bei Beträgen mit gleicher Stellenzahl die „1“ am Anfang wesentlich häufiger als die „9“. Auch hier würden also viele Rechnungen über 900 bis 999 Euro gegenüber wenigen mit Beträgen von 100 bis 199 Euro auffallen und einen Alarm auslösen.

Textforensik

In der Textforensik eröffnet die Autorschaftsanalyse überraschende Perspektiven. Wenn beispielsweise unter verschiedenen Identitäten massenhaft fingierte Fälle eingereicht werden, kommen erfahrungsgemäß vorformulierte Schadensmeldungen zum Einsatz. Ein automatisiertes Verfahren könnte nun die auffälligen Texte mit hoher Sicherheit einem Autor zuordnen. Schlägt dieses System Alarm, können weitere Prüfungen folgen.

Für das Training ihrer Tools nutzten Oren Halvani und seine Kollegen am SIT die Texte von 50 c't-Autoren. Mit hoher Sicherheit konnten sie dann auch unbekannte Texte dieser Autoren sicher zuordnen. In der c't-Redaktion stieß diese Ankündi-



Aufgedeckter Fake: Ein per Copy-Move-Retusche verändertes Foto wird anhand der kopierten Bildbereiche automatisiert entdeckt.

Bild: AFP / Fraunhofer SIT

gung zunächst auf Skepsis. Aber ein Test gab dem Forscherteam recht. Wir sendeten drei am Institut unbekannte Texte ein, die auch noch aus einem anderen Jahr als die Trainingstexte stammten. Einen Beitrag konnten die Forscher zweifelsfrei dem richtigen Autor zuordnen, bei einem weiteren schwankten sie zwischen zwei Autoren, einer davon war der richtige. Den Autor des dritten relativ kurzen Beitrags konnten die Wissenschaftler nicht bestimmen. Wenn man allerdings die Abläufe in der c't-Redaktion kennt und weiß, wie viele Augen jeden Text durchgehen und wie viele Gegenlese-Schleifen durchlaufen werden, dann wundert man sich schon, dass der Autorenstil immer noch in zwei von drei Fällen deutlich erkannt werden konnte.

Vergleich der Schreibstile

„Wir suchen nach Ähnlichkeiten im Schreibstil“, berichtet Halvani. Als entscheidend dafür habe sich die Analyse vor allem der Redundanzen und Funktionswörter erwiesen, im Gegensatz zu den Inhaltswörtern, die eine eigene lexikalische Bedeutung tragen. Im Deutschen rechnet man etwa 700 Wörter zu den Funktionswörtern, darunter die Artikel, Konjunktionen, Pronomen und Präpositionen. Schon eine einfache Vektoranalyse, die schlicht das Vorkommen der jeweiligen Funktionswörter zählt und deren Zahlenverhältnis wiedergibt, erlaubt Zuordnungserfolge beim Vergleich unterschiedlicher Texte. Allein mit diesem Verfahren haben die Forscher bereits Autorenstile identifizieren und voneinander unterscheiden können, wie Halvani berichtet.

Für die Autorschaftsanalyse werden verschiedene am SIT entwickelte Tools genutzt, von der Vektoranalyse bis zu neuronalen Netzen. Die schärfste Waffe ist laut Halvani allerdings ein Kompressionsverfahren, das beim Vergleich von Texten die schnellste und treffsicherste Klassifizierung zwischen „derselbe Autor“ und „unterschiedliche Autoren“ erlaubt. Dabei nutzen die Forscher Prediction by Partial Matching (PPM), einen statistischen Textkompressionsalgorithmus, der in den 80er-Jahren entwickelt worden ist, aber wegen seines Arbeitsspeicherhungers lange Zeit kaum eingesetzt wurde.

Insbesondere die hier eingesetzte Variante PPMd hat die Besonderheit, dass sie Texte durcharbeitet und dabei Wahrscheinlichkeiten jeweils für das nächste Zeichen, das nächste Wort, die nächste Formulierung im Kontext errechnet. Dieses Vorgehen spricht stark auf Schreibstil und quantifizierbare Stilmerkmale an und erzeugt im Hintergrund eine Wahrscheinlichkeitstabelle, die bis zur vollständigen Bearbeitung des Textes stetig optimiert wird. Für sich genommen stellt schon diese Tabelle eine Art Sprachmodell zum Autor dar. In der Kompressionsphase werden dann die Prognosen kodiert, die Kompressionsrate sagt daher zusätzlich etwas über den Schreibstil des Autors aus.

Am SIT zeigte der Vergleich von Autorentexten mittels PPMd-Kompressionsverfahren nicht nur die höchsten Trefferaten. Zudem erwies sich dieses Verfahren als das mit Abstand schnellste [1]. Während aufwendige Architekturen wie zum Beispiel rückgekoppelte neuronale Netze

zum Teil über 20 Stunden für Training und Analyse beanspruchen, erzeugt das Kompressionsverfahren seine Einschätzungen in wenigen Sekunden. Halvani bezeichnet in diesem Fall den Einsatz von neuronalen Netzen als „Zeit- und Stromfresser“. Auf der anderen Seite erlauben neuronale Netze mittels unterschiedlicher Verfahren eine Rückverfolgung, welche Stilmerkmale letztlich den wichtigsten Ausschlag für ein Klassifizierungsergebnis gaben. Mit kompressionsbasierten Lernmodellen ist dies nur schwer umzusetzen.

Auf einen Autor fokussiert

Ein weiterer Ansatz nutzt sogenannte Autoencoder, relativ einfache neuronale Netze. Autoencoder besitzen nur einen Hidden Layer und dieser weist weniger Neuronen auf als Eingangs- und Ausgangslayer. Solche Netze erzeugen also fast automatisch Verluste zwischen Textein- und -ausgabe, da der Hidden Layer die Eingabe nicht vollständig repräsentieren kann. Wird ein Autoencoder auf die Texte eines Autors trainiert, so erzeugt er bei diesem Autor in der Regel einen kleineren Kompressionsfehler als bei Texten anderer Autoren. Bis heute ist für die Autorschaftsanalyse am SIT ein Werkzeugkasten mit fast 30 Tools entstanden, deren Ergebnisse sich gegenseitig bestärken oder widersprechen können. Einzelausschläge werden damit relativiert, sichere Autorenerkennung mehrfach bestätigt.

Die Tools, die ursprünglich mit Blick auf die Versicherungsbranche entstanden sind, werden inzwischen auch für andere Zwecke genutzt. Insbesondere die Bildforensik steht im Zentrum eines neuen Projektes zur Fake-News-Erkennung.

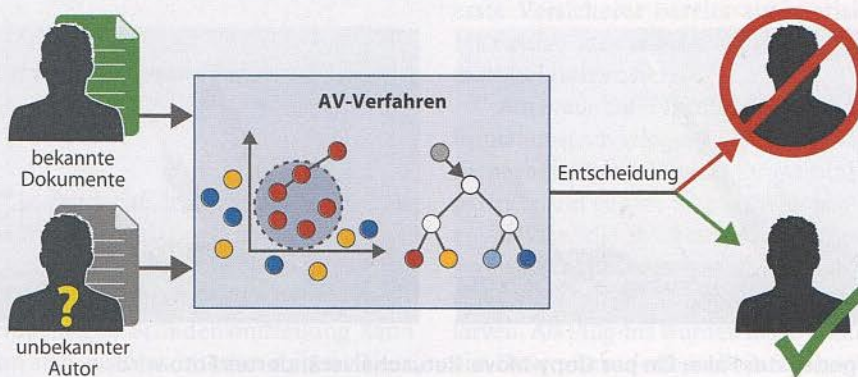
Mit der Textforensik eröffnet sich ein noch weiteres Feld. So versuchen die Forscher mit ihren Tools inzwischen auch, Hate Speech sowie extremistische Äußerungen zu erkennen. Ein weiteres Projekt dient dem Autoren-Profilung: Die verwendete Sprache kann beispielsweise einen Erwachsenen in einem Kinderforum verraten. Ganz naheliegend ist es, per Autorschaftsanalyse etwa Ghostwriter von Bachelor-, Master- oder Doktorarbeiten zu entlarven; auch auf diesem Feld konnten die Forscher schon klare Manipulationen nachweisen. (agr@ct.de) **ct**

Literatur

- [1] Oren Halvani, Christian Winter, Lukas Graner, Authorship Verification based on Compression-Models: <https://arxiv.org/abs/1706.00516>

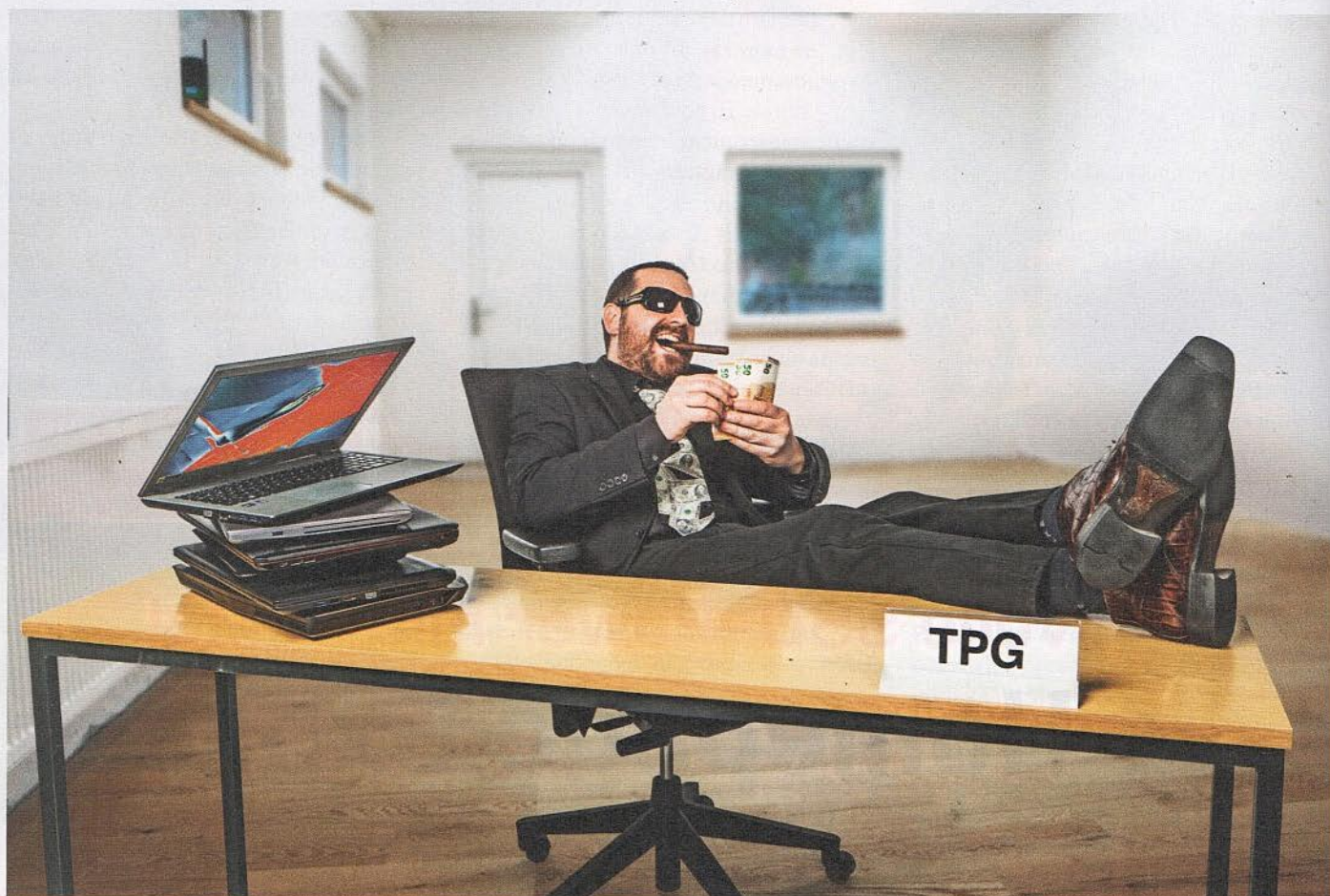
KI erkennt Autorenstil

Die Autorschaftsanalyse erfolgt am Fraunhofer SIT mittels verschiedener KI-Systeme, die Stilmerkmale eines Autors quantifizieren und mit einem bereits analysierten Schreibstil vergleichen. Im Training mit Texten von insgesamt fünfzig c't-Autoren gelang die Autorenverifikation (AV) mit hoher Sicherheit.



Reparatur-Falle

Abzocke mit Notebook-Reparaturen



Wenn ein teures Notebook den Geist aufgibt, hofft man sehr, eine günstige Reparaturmöglichkeit zu finden. Doch dabei kann man auch auf Betrüger hereinfliegen.

Von Tim Gerber

Als Florian H. im vergangenen Sommer von einem Bekannten ein defektes Lenovo Yoga Tab 2 Pro angeboten wurde, schlug der IT-Experte für 50 Euro zu. Das Tablet hatte neu stolze 1100 Euro gekostet und war erst etwa zweieinhalb Jahre alt. Vielleicht ließe es sich ja noch günstig reparieren, dann wäre es ein echtes Schnäppchen.

Also erwarb er am 30. August 2018 zum Pauschalpreis von 130 Euro unter pcspezialist-regensburg-notebookservice.de den Austausch des Mainboards an dem Yoga Tab. Mit etwas Verzögerung aufgrund der Urlaubszeit ging der Tablet-PC beim „Service Center Süd“ im öster-

reichischen Klagenfurt am Wörthersee ein. Der Service bestätigte dies per E-Mail, die durchschnittliche Bearbeitungszeit sollte demnach 10 Tage sein. Noch am selben Tag erhielt Florian H. einen Anruf vom „PC Spezialisten“, in dem ihm mitgeteilt wurde, außer dem Mainboard seien auch noch die Platine mit der Spannungsversorgung sowie ein Verbindungskabel defekt.

Mit den weiteren Teilen sollte die Reparatur 259,43 Euro kosten, die per Vorkasse bezahlt werden müssten. Da das immer noch günstig schien, überwies Florian H. den Betrag umgehend auf das ihm genannte Konto.

Nun passierte erst einmal nichts. Am 16. Oktober fragte Florian H. per E-Mail nach dem Stand der Reparatur, erhielt aber keine Antwort. Eine Woche später, am 24. Oktober, fragte er abermals vergeblich nach dem Stand der Angelegenheit.

Am 29. Oktober rief Florian H. in der Berliner Niederlassung des „Service Center Süd“ an, die unter pcspezialist-berlin-notebookservice.de angegeben ist. Die Dame am Telefon sagte ihm, sie müsse sich erst über seinen Fall erkundigen. Er erhielt dann am selben Tag eine Benachrichtigung per E-Mail. Es fehle noch ein Verbindungskabel, damit die Reparatur seines Notebooks abgeschlossen werden könne, hieß es. Dieses solle aber „in den nächsten Tagen“ im Service-Center eintreffen.

Weiter hörte Florian H. von der Firma nichts. Auf eine Nachfrage per E-Mail vom 27. November reagierte die Firma ebenso wenig wie auf eine weitere E-Mail vom 10. Dezember, in welcher der Kunde eine Frist bis zum 21. Dezember für die Rückgabe des Tablets setzte – in welchem Zustand auch immer es sich bis dahin befinden möge. Und da sich auch daraufhin nichts tat, forderte Florian H. die Firma nochmals per Einschreiben an ihre Adresse in Berlin-Neukölln auf, das Gerät zurückzugeben und den gezahlten Betrag für die nicht ausgeführte Reparatur zu erstatten. Zeitgleich wandte er sich an die Redaktion der c't.

Alter Bekannter

Der Fall erinnerte sofort an den von Hubert S., über den wir in c't 20/2018, Seite 58, berichtet hatten. Er hatte eine Reparatur beim „PC-Spezialisten für Regensburg“ an seinem Lenovo-Notebook in Auftrag gegeben, die sich auf dieselbe Weise zuerst verteuert und dann schier endlos in die Länge gezogen hatte. Er hatte es im Zuge der damaligen Recherchen von der Firma in defektem Zustand zurückerhalten. Auch von seinem Notebook fehlt ab dem 6. September, dem erneuten Eingang bei TPG, jede Spur. Nachfragen beantwortete ihm das Unternehmen nicht.

Wir fragten zunächst am 28. Januar per E-Mail und Fax bei der TPG Scheidl GmbH in Klagenfurt nach dem Tablet von Florian H. Die TPG steckt sowohl hinter dem „Service Center Süd“ mit Adresse in

Berlin-Neukölln als auch hinter der Regensburger Internetadresse. Wir wollten nun wissen, wie der Stand der Reparatur an dem Tablet von Florian H. ist.

Am 31. Januar erhielten wir ein Fax der Firma, unterzeichnet von Klaus Petscharnig. Mit „erheblichen Anstrengungen und größter Mühe“ sei es nun gelungen, das nötige Ersatzteil „aus Übersee“ zu bekommen. Man habe den Kunden bereits telefonisch informiert, dass man ihm sein Tablet „in den nächsten zwei Tagen“ repariert werde zukommen lassen. Da das Tablet von Florian H. aber am 4. Februar noch immer nicht bei ihm eingetroffen war, fragten wir in Klagenfurt nach.

Per Fax teilte uns Klaus Petscharnig am 4. Februar mit, das Tablet von Florian H. sei am 31. Januar versendet worden, und nannte uns eine Tracking-Nummer für die Sendungsverfolgung. Der zu Folge wurde tatsächlich eine Sendung am 1. Februar in einem Paketzentrum nahe Klagenfurt eingeliefert. Von dort hat sie sich aber nicht weiterbewegt. Laut Auskunft des Paketdienstleisters wurde das Porto für mehrere Sendungen der TPG nicht entrichtet und das Paket deshalb gepfändet.

Bezüglich des Notebooks von Hubert S., das sich seit September bei TPG befindet, sei „bedauerlicher Weise keine Lösung geplant“. Die „ungerechtfertigte Berichterstattung“ der c't beschäftige derzeit seine Rechtsabteilung, ließ uns Petscharnig wissen. Dass eine solche Rechtsabteilung existiert, ist allerdings fraglich. Denn Klaus Petscharnig, der laut Registertrag der Firma TPG Scheidl (FN 267566f) mit Vornamen Nikolaus heißt, ist am Vormittag des 4. Februar zu einer Verhandlung gegen ihn im Landesgericht Klagenfurt ohne jeden rechtlichen Beistand erschienen.

Verurteilt

Eine Gerichtssprecherin bestätigte uns den Bericht der Kronen-Zeitung (Ausgabe für Kärnten vom 5. Februar 2019, S. 30). Demzufolge wurde Petscharnig aufgrund einer gefakten E-Mail wegen schweren Betruges verurteilt. Der Richter bezeichnete die Fälschung in der Verhandlung als „ziemlich plump“ und verurteilte ihn zu 5 Monaten Haft, die zur Bewährung ausgesetzt wurden. Außerdem muss er eine Geldstrafe von 220 Tagessätzen à 5 Euro berappen. Das Urteil ist freilich noch nicht

rechtskräftig und darauf angesprochen kündigte Petscharnig an, in Berufung gehen zu wollen.

Bei der Kärntner Justiz sind er und seine Geschäftspartnerin Sonja Scheidl keine Unbekannten. Bereits am 6. April 2017 wurden die beiden vom Landesgericht wegen Betrügerischer Krida (Konkursbetrug) im Zusammenhang mit einem Konkursverfahren der TPG verurteilt (Aktenzeichen 80 Hv 1/17). Die Berufung gegen das Urteil hat das Oberlandesgericht Graz mit Urteil vom 23. August 2017 abgewiesen, die Verurteilung ist damit rechtskräftig.

Und aufgrund der Recherchen der c't ermittelt die Staatsanwaltschaft Klagenfurt nun auch wegen des Verdachts des Betruges mit den angeblichen Notebookreparaturen weiter gegen die beiden. Florian H. und Hubert S. haben jedenfalls Anzeige erstattet. Eventuellen weiteren Geschädigten der TPG Scheidl GmbH ist zu raten, sich direkt an die Staatsanwaltschaft Klagenfurt zu wenden.

Auch beim Generalstaatsanwalt von Berlin, wo die TPG ja eine Anschrift hat, scheint Petscharnig kein Unbekannter zu sein. Weshalb dort genau gegen ihn ermittelt wird, konnte die Behörde bis Redaktionsschluss allerdings nicht mitteilen.

Warnsignale

Dass die beiden Kunden jemals ihre Geräte oder gar ihr Geld wiedersehen, scheint angesichts der Sachlage äußerst unwahrscheinlich. Zu erkennen war die fragliche Seriosität der Firma anhand deren Webseiten für juristische Laien nur schwer, zumal sie gezielt gängige Begriffe wie „PC Spezialist“ verwenden. Diesen nutzt auch ein zur Synaxon AG gehörender Händlerverband, der nichts mit der TPG aus Klagenfurt zu tun hat. Markenrechtlich zu schützen sei der Begriff leider nicht, ließen uns die Synaxon-Juristen wissen.

Wie man solche Spreu wie die TPG vom Weizen seriöser Reparaturbetriebe im Internet zuverlässig trennen kann, ist schwer zu sagen. Stutzig machen sollten besonders günstige Preise und Vorkasse. Von der verlockenden Aussicht, mit einer günstigen Reparatur ein teures, aber defektes IT-Schätzchen retten zu können, sollte man sich nicht ködern lassen.

(tig@ct.de) **ct**

Verwendete Webseiten der TPG:
ct.de/ykp2

**VOR
SICHT
KUNDE!**



Mit (fast) allen Registern

Spielergrafikkarte Radeon VII mit 16 GByte HBM2

AMD zündet für die High-End-Grafikkarte Radeon VII ein kleines Technikfeuerwerk, um die alternde GCN-Architektur fit für die nächste Runde zu machen.

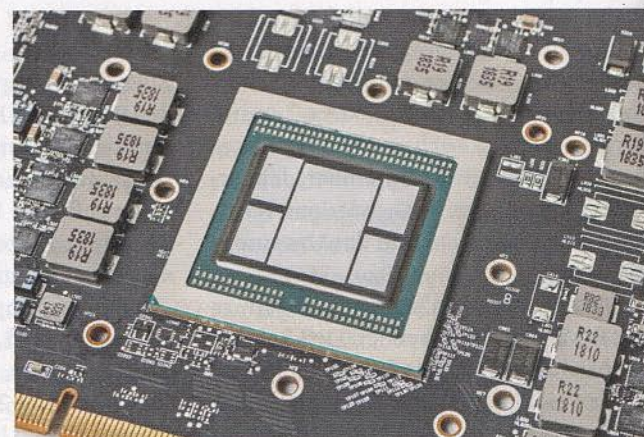
Von Carsten Spille

Mit der rund 730 Euro teuren Radeon VII will AMD wieder in der von Nvidia dominierten Highend-Klasse mitmischen. Der Hersteller zielt damit auf die GeForce RTX 2080 als Gegner. AMD verspricht dreistellige Bildraten in vielen aktuellen Spielertiteln in WQHD-Auflösung und meist auch noch flüssige Darstellung in Ultra HD. Doch die Radeon VII kann noch mehr – zum Beispiel ihre Rechenkraft von 13,8 Billionen Rechenschritten pro Sekunde als OpenCL-Rechenbeschleuniger zur Verfügung stellen. Man-

che Videobearbeitungsprogramme wie Adobe Premiere nehmen diese Leistung gern mit. Auch beim Grafikspeicher protzt AMD und stattet die Radeon VII mit 16 GByte des rasend schnellen High Bandwidth Memory 2 (HBM2) aus.

Die Vega-20-GPU ist das Herzstück der Radeon VII und der erste Grafikchip

Neben dem Grafikchip sind links und rechts jeweils zwei Stapel HBM2-Speicher auf dem Trägersubstrat vorhanden.



mit 7 nm feinen Strukturen. Das ermöglicht mehr Schaltkreise, höhere Taktraten oder niedrigere Leistungsaufnahme. Für die Radeon VII hat AMD sich entschieden, den Fokus auf eine Verkleinerung und hohe Taktraten zu legen. Mit bis zu 1800 MHz Spitze und 1750 MHz längerfristigem Boost liegt die Radeon VII trotz Luftkühlung deutlich vor der RX Vega 64.

Von der Theorie ...

Den Vorteil der von 14 auf 7 Nanometer verkleinerten Fertigung hat AMD hauptsächlich genutzt, um den aus der Radeon RX Vega bekannten Chip von 495 auf 331 mm² zu verkleinern – um ein rundes Drittel also. Die maximale Anzahl an Rechen-einheiten ist mit 4096 – von denen die Radeon VII anders als die Vega 64 nur 3840 nutzt – zwar nicht höher als beim Vorgänger, aber einzelne Bestandteile sind deutlich mächtiger als zuvor. Wissenschaftliche Berechnungen mit doppelter Genauigkeit etwa beackerte die Radeon VII im Test mit knapp 3,5 TFLOPS Durchsatz, was verglichen mit dem Vorgänger eine Steigerung um Faktor 4 bedeutet. Verglichen mit der GeForce RTX 2080 ist die Radeon VII bei dieser Rechenart um Faktor 9,4 schneller.

Durch die Verkleinerung der GPU ist nun genügend Platz für vier HBM2-Stapel – beim Vorgänger passten nur zwei. Auch die Anzahl der Datenleitungen verdoppelte AMD. Damit überträgt der Speicher der Radeon VII ein saftiges Terabyte pro Sekunde und ist damit gut doppelt so schnell wie der des Vorgängers und knapp 2,3 mal so schnell wie der der GeForce RTX 2080.

... in die Praxis

In den meisten Anwendungen wird lediglich einfache Genauigkeit (FP32) genutzt. Der Vega-20-Vorteil ist dann deutlich ge-

ringer, von ihrer hohen Speichertransfer-rate profitiert die Radeon VII jedoch auch hier. In der einfachen Luxmark-Szene Luxball HDR ist sie zwei Drittel schneller als ihre Vorgängerin RX Vega 64 und auch als die GeForce RTX 2080.

In Spielen zeigt sich allerdings wieder einmal, dass Rechenkraft nicht alles ist. Auch die festverdrahteten Textureinheiten, Rasterisierer und Rasterendstufen spielen hier eine wichtige Rolle und die wurden im Vergleich zur Vega 64 kaum verbessert. Deshalb müssen sie hauptsächlich durch den höheren Takt und die verdoppelte Speichertransfertrate zulegen. Im 3DMark Firestrike Extreme und Timespy ist die Radeon VII gut 20 Prozent schneller als die Vega 64. Im Firestrike Extreme kommt sie etwa auf das Niveau der GeForce RTX 2080, fällt im DX12-Test Timespy jedoch zurück.

In Spielen erreicht die Radeon VII knapp das Leistungsniveau der GeForce RTX 2080 und schafft im Far-Cry-5-Benchmark auch in Ultra HD mit HD-Texturpack flüssige 61 fps. In Shadow of the Tomb Raider sind es in derselben Auflösung 45 fps, in GTA V, welches den Radeon-Karten traditionell schlecht liegt, ebenfalls. Dort ist die Radeon VII auch nur noch auf RTX-2070-Niveau. In WQHD-Auflösung ist die Radeon oft etwas langsamer als die RTX 2080, stemmt aber nichtsdestotrotz geschmeidige Bildraten im Bereich von 75 fps und aufwärts.

Sparsam nur im Leerlauf

Die drei Lüfter der Radeon VII drehen im Leerlauf sehr langsam und stören nicht. Ihre 0,1 Sone sind an der Untergrenze unserer Messgenauigkeit – sehr gut! Dabei bleibt die Karte mit 13 Watt für ihre Leistungsklasse angemessen sparsam. Erfreulicherweise änderte sich das auch kaum, als wir UHD-Displays oder bis zu vier Monitore anschlossen – dann lag die Leistungsaufnahme bei immer noch guten 15 Watt.

Unter Dauerlast jedoch drehen die Lüfter nach wenigen Minuten mit knapp 3000 U/min und erzeugen einen störenden Lärmpegel von 3,3 Sone – im reinen Compute-Betrieb blieb es allerdings bei 2,0 Sone. Im 3DMark Firestrike schluckt die Karte 254 Watt mit kurzzeitigen Spitzenwerten bis 312 Watt. Im Furmark arbeitet sie dauerhaft an ihrer 300-Watt-Grenze, wobei einzelne Spitzenausschläge bis 408 Watt gehen.

Fazit

AMD betreibt die Radeon VII nah am Limit, um mit Nvidias GeForce RTX 2080 mitzuhalten. Das schlägt sich speziell in der hohen Lautstärke und Leistungsaufnahme unter Last nieder. Mit 730 Euro ist sie teurer als die billigsten GeForce RTX 2080, erreicht in 4K-Auflösung manchmal aber höhere Bildraten. Bei reinen Rechen-

aufgaben spielt sie ihre hohe Rechenleistung und Transferrate aus und deklassiert die Nvidia-Karte in einigen Disziplinen. Dank 16 GByte Grafikspeicher bremsen auch größere Workloads die GPU nicht aus. Spieler mit einer Radeon VII schlafen dank des dicken Speicherpolsters im Hinblick auf künftige Hi-Res-Texturpakete etwas ruhiger. (csp@ct.de) ct

Radeon VII: Spezifikationen

Grafikkarte	GeForce RTX 2080 FE	Radeon Vega VII	Radeon RX Vega 64
GPU / Größe	TU104 / 545 mm²	Vega 20 / 331 mm²	Vega 10 / 495 mm²
Fertigung / Transistoren	12 nm / 13,6 Mrd.	7 nm / 13,2 Mrd.	14 nm / 12,5 Mrd.
PCIe-Generation / TDP	3.0 / 225 Watt	3.0 / 300 Watt	3.0 / 295 Watt
Rechenblöcke / Shader-Kerne	46 / 2944	60 / 3840	64 / 4096
GPU- / Turbo-Takt	1515 / 1800 MHz	1400 / 1750 (1800)² MHz	1274 / 1546 MHz
Rechenleistung (HP / SP / DP)¹	21,2 / 10,6 / 0,33 TFlops	27,6 / 13,8 / 3,46 TFlops	25,4 / 12,7 / 0,79 TFlops
Zeit Blender 2.79b „Classroom“	208 Sek. (tile size = 16)	183 Sek. (tile size = 256)	212 Sek. (tile size = 256)
Speicher / Transferrate	8 GByte GDDR6 / 448 GByte/s	16 GByte HBM2 / 1 TByte/s	8 GByte HBM2 / 484 GByte/s
Display-Anschlüsse	3 × DP 1.4, HDMI 2.0b, USB-C	3 × DP 1.4, HDMI 2.0b	3 × DP 1.4, HDMI 2.0b
Preis (bei Launch)	650 (850) €	729 €	410 (499) €

¹ HP: Half Precision (FP16), SP: Single Precision (FP32), DP: Double Precision (FP64) ² kurzzeitiger Spitzenwert bei Teillast

Spieleleistung

Grafikkarte	GTA V (DX11) Maximum, 4xMSAA [fps]	Far Cry 5 (DX11) Ultra, SMAA, HD-Texturen [fps]	Shadow o. t. Tomb Raider (DX12) Maximum, SMAA, 16x AF [fps]
	besser ▶	besser ▶	besser ▶
Full HD	1920 × 1080	1920 × 1080	1920 × 1080
Gigabyte GeForce RTX 2080 T Gaming OC	108	132	153
AMD Radeon VII	96	118	118
Gainward GeForce Phoenix GS RTX 2080	106	126	124
MSI GeForce RTX 2070 Gaming Z	100	122	103
Asus ROG Strix Geforce GTX 1070 Ti	93	106	85
Sapphire Nitro+ Radeon RX Vega 64	82	116	95
Powercolor Radeon RX Vega 56 Red Dragon	73	108	85
MSI GeForce GTX 1060 Gaming X 6 GB	71	74	56
WQHD	2560 × 1440	2560 × 1440	2560 × 1440
Gigabyte GeForce RTX 2080 T Gaming OC	104	121	105
AMD Radeon VII	76	105	82
Gainward GeForce Phoenix GS RTX 2080	95	109	86
MSI GeForce RTX 2070 Gaming Z	86	94	70
Asus ROG Strix Geforce GTX 1070 Ti	71	76	58
Sapphire Nitro+ Radeon RX Vega 64	60	87	63
Powercolor Radeon RX Vega 56 Red Dragon	54	77	56
MSI GeForce GTX 1060 Gaming X 6 GB	46	49	36
4K (UHD)	3840 × 2160	3840 × 2160	3840 × 2160
Gigabyte GeForce RTX 2080 T Gaming OC	71	75	59
AMD Radeon VII	46	60	45
Gainward GeForce Phoenix GS RTX 2080	56	60	46
MSI GeForce RTX 2070 Gaming Z	48	50	37
Asus ROG Strix Geforce GTX 1070 Ti	37	40	30
Sapphire Nitro+ Radeon RX Vega 64	34	47	33
Powercolor Radeon RX Vega 56 Red Dragon	30	41	29
MSI GeForce GTX 1060 Gaming X 6 GB	25	24	18

Testsystem: Core i7-8700K (OC 4,7 GHz), 32 GByte RAM, Radeon Adrenalin Ed 2019 18.9.1 / Press, GeForce 417.71, Windows 10 1809 x64

Verspäteter Konter

Übertaktbarer 28-Kern-Prozessor Xeon W-3175X



Um die Performancekrone von AMD zurückzuerobern und Hardware-Enthusiasten glücklich zu machen, ist Intel jedes Mittel recht. Im Xeon W-3175X für 3000 Euro steckt ein hochgetakteter Serverprozessor mit 28 Kernen.

Von Christian Hirsch

Der Threadripper-Schock sitzt immer noch tief bei Intel. Um dem im August vergangenen Jahres vorgestellten 32-Kern-Prozessor Ryzen Threadripper 2990WX etwas entgegenzusetzen, hatte Intel bis Jahresende 2018 eine Workstation-CPU mit 28 Kernen versprochen. Die selbstgesetzte Frist verfehlte Intel zwar um einen Monat, doch nun gibt es den Xeon W-3175X mit 28 Kernen, 56 Threads und 255 Watt Thermal Design Power endlich.

Da bei der High-End-Desktop-Plattform LGA2066 für Core-X-Prozessoren bei 18 Kernen Schluss ist, hat Intel für den Xeon W-3175X das Server-Ökosystem der Xeon-SP-Prozessoren in Workstations umgetopft. Die Herkunft merkt man der CPU deutlich an: Jedem der 28 Kerne steht jeweils 1 MByte Level-2-Cache zur Verfügung und alle teilen sich 38,5 MByte L3-Cache. Der Xeon W-3175X hält allein durch den Anpressdruck des Kühlers in

der riesigen Fassung LGA3647 und steuert sechs DDR4-Speicherkanäle an. Für Erweiterungskarten und Zusatzchips auf dem Mainboard stellt der Prozessor 44 PCIe-3.0-Lanes bereit, weitere 20 liefert der zugehörige (Server-)Chipsatz C621.

Bei der Zielgruppe der 3000-Euro-CPU kann sich Intel nicht so recht entscheiden. Zum einen hebt der Chip-Hersteller die Fähigkeit hervor, dass die CPU auch mit Registered-ECC-Speicher umgehen kann. Das ist für professionelle und wissenschaftliche Workstation-Anwendungen wichtig, bei denen fehlerfreie Rechenergebnisse gefordert sind. Zum anderen möchte Intel sogenannte „Ultimate Enthusiasts“ erreichen und gibt deshalb im Unterschied zu den übrigen Xeons das Übertakten per Multiplikator frei.

Lauter Riese

Dieser Spagat fiel auch beim Testsystem auf, das uns Intel zur Verfügung gestellt hat: Zur Ausstattung zählten außer sechs 8-GB-Byte-ECC-RDIMMs eine Gaming-Grafikkarte vom Typ GeForce GTX 1080 sowie eine Optane-SSD mit 480 GByte Kapazität und U.2-Anschluss. Als wir den wassergekühlten Rechner mit 14 Lüftern das erste Mal einschalteten, schlossen die Kollegen wegen 12 Sone Lautheit im gegenüberliegenden Büro prompt die Tür. Verursacher waren die kräftigen Lüfter auf dem Wärmetauscher der Asetek-Wasserkühlung. Warum Intel nicht von vorn-

herein die zusätzlich mitgelieferte Wasserkühlung von EKWB installiert hat, wundert uns. Diese war deutlich leiser und kühlte obendrein besser. Das Kabel für die Pumpe mussten wir auf einen anderen Anschluss umstecken, weil sie sonst nicht immer anlief und die CPU ihren Takt auf rund 1 GHz drosselte.

Nachdem diese Hürden überwunden waren, konnte der Xeon W-3175X endlich seine Stärken zeigen. Im Rendering-Benchmark Cinebench R15 schlägt er ohne Übertaktung einen ebenfalls wassergekühlten Threadripper 2990WX mit 3 Prozent Vorsprung. Hier muss man allerdings beachten, dass der Cinebench vollständig in der mit 32 Sekunden sehr großzügig bemessenen Turbophase abläuft, in der der Xeon seine TDP von 255 Watt deutlich überschreitet. Der Xeon W-3175X rechnet – trotz vier Kernen weniger – schneller als der 2990WX, weil er dabei mit 3,8 GHz läuft. Der AMD-Prozessor hält hingegen seine 250 Watt TDP ein und taktet deshalb bei Last auf allen 32 Kernen 500 MHz langsamer. Im länger andauernden Blender-Benchmark musste der Xeon hingegen mit 3 Prozent Rückstand dem Threadripper den Vortritt lassen.

Eindeutiger ist das Bild bei der Singlethread-Wertung mit 11 Prozent Vorsprung für den Xeon sowie bei der Paradeisziplin aktueller Intel-Prozessoren, sobald hochoptimierter Code zum Einsatz kommt: Der Xeon W-3175X hat pro Kern

Vergleich Xeon W-3175X und Ryzen Threadripper 2990WX

Prozessor	Kerne	Takt (nom. / Turbo)	Cinebench R15 Singlethread	Cinebench R15 Multithread	Blender 2.79 BMW [s]	Handbrake Fast-1080p30 [fps]	Handbrake Production Max [fps]	Flops 64 Bit [GFLOPs]	Leistungsaufnahme Leerlauf / Volllast
			besser ►	besser ►	◀ besser	besser ►	besser ►	besser ►	◀ besser
Xeon W-3175X	28+HT	3,1 / 4,3 GHz	189	5379	95	92	57	2516	111/407
Threadripper 2990WX	32+SMT	3,0 / 4,2 GHz	170	5203	93	54	43	876	73/477

gemessen jeweils mit GeForce GT 1030 und SSD, Xeon W-3175X: 48 GByte DDR4-2666, Threadripper 2990WX: 32 GByte DDR4-2666

zwei AVX512-Einheiten, während der Threadripper 2990WX pro Taktzyklus und Kern lediglich eine 256 Bit breite FMA-Instruktion (fused multiply and add) verarbeiten kann. In dieser Disziplin kommt der Xeon mit 2,5 TFLOPs bei doppelter Genauigkeit (64 Bit) fast auf die dreifache Rohleistung des Threadripper.

Gitter schlägt Multichip

Beim Videokodieren mit Handbrake zeigen sich anhand der Messwerte weitere Unterschiede im Aufbau der beiden CPUs. Abhängig von der Komplexität des Video-codecs hat der Xeon mit 30 bis 70 Prozent Abstand die Nase vorn. Wie bei den Xeon SP sitzen die 28 Kerne in einem 6x6-Raster im monolithischen Halbleiter-Die. Auf den acht verbleibenden Positionen sitzen die zwei Speicher-Controller mit je drei DDR4-Kanälen sowie die PCIe-Root-Hubs und die beim Xeon W-3175X ungenutzten UPI-Links (Ultra Path Interconnect) für Multisocket-Systeme. Untereinander kommunizieren die Kerne und

die RAM-Controller über ein Mesh, wodurch die durchschnittliche Speicherlatenz rund 80 Nanosekunden beträgt. Beim Threadripper 2990WX verteilen sich die 32 Kerne auf vier Octa-Core-Dies, wobei zwei davon keinen lokalen Speicher anbinden und stattdessen über das Infinity-Fabric auf das RAM eines anderen Dies zugreifen müssen. Die Latenz beträgt deshalb entweder 60 oder 100 Nanosekunden. Die heterogene NUMA-Architektur der Threadripper-Prozessoren wird vom Scheduler von Windows 10 noch nicht optimal unterstützt, was bei Anwendungen wie Handbrake die Performance schmälert.

Unter Volllast mit Prime95 schluckte das Testsystem mit dem Xeon W-3175X maximal 540 Watt. Die Package Power betrug dabei bis zu 360 Watt. Bei Dauerlast nach der 32-sekündigen Turbophase hielt der Xeon seine TDP mit 254 Watt exakt ein. Die Gesamtleistungsaufnahme lag dann bei 407 Watt. Das Threadripper-System benötigte 477 Watt, bei einer CPU Package Power von 249 Watt (TDP: 250

Watt). Beim Übertakten des Xeon erreichten wir 4,6 GHz und 6516 Cinebench-Punkte. Mit Prime95 lief das System dann aber nicht mehr stabil. Bei 4,5 GHz konsumierte der Rechner mit Prime95 1018 Watt, wovon allein 540 Watt auf die CPU entfielen.

Fazit

Intel kann sich mit dem Xeon W-3175X die Performance-Krone bei Desktop- und Workstation-Prozessoren zurückholen. PC-Bastler haben zwar die Auswahl zwischen den beiden Mainboards Asus ROG Dominus Extreme und Gigabyte AIX-C621, bei einem Prozessorpreis von 3000 Euro und mutmaßlichen Stückzahlen im niedrigen vierstelligen Bereich wird der Xeon W-3175X aber wohl hauptsächlich werbewirksamen Demosystemen vorbehalten sein. Im High-End-Desktop-Segment liefert AMD mit dem Ryzen Threadripper 2990WX für 1800 Euro weiterhin das bessere Preis/Leistungsverhältnis.

(chh@ct.de) **ct**

Darmstadt, darmstadtium
4.-6. Juni 2019

DevOps Essentials 2019

Deep-Dive-Trainings zu Continuous Delivery, DevOps und Containerisierung

THEMEN

- ✱ DevOps-Kultur im Unternehmen schaffen
- ✱ Softwareentwicklung mit Continuous Delivery
- ✱ Vorteile und Anwendungszwecke von Microservices-Architekturen
- ✱ Docker für Fortgeschrittene
- ✱ Container-Orchestrierung mit Kubernetes – für Einsteiger und Fortgeschrittene
- ✱ Service Meshes mit Istio und Co.
- ✱ Site Reliability Engineering
- ✱ Testen und Qualitätssicherung

PROGRAMM ONLINE!
Early Bird bis 12. April 2019



Veranstalter



heise Developer

dpunkt.verlag

www.devops-essentials.de

Trau, schau, Smart-TV

Geschwätzige Samsung-TVs datensparsam betreiben

Bei unserem letzten Test von Smart-TVs stach Samsungs Gerät hervor, weil es vergleichsweise viele Daten ins Netz übertragen hat. Anders als damals beschrieben kann man die Datenflut eindämmen – Samsung hat den Bedienkniff dafür nur gut versteckt.

Von Peter Siering

Für c't 25/2018 haben wir Smart-TVs getestet und dabei geprüft, was die schlauen Fernseher in die Welt hinausposaunen: zum TV-Hersteller, zu den Sendern und zu den App-Anbietern [1]. Das Testgerät von Samsung erwies sich dabei als besonders geschwätzig; ein etwas älteres Gerät des gleichen Herstellers aus einem vorherigen Test (UE43MU6179U in [2]) plauderte ebenso munter drauflos. So fiel unser Fazit zu den Geräten entsprechend deutlich aus. Ein längerer Austausch mit Samsung brachte Klarheit: Die Bedienführung des Geräts bei der Erstinstallation hatte uns genarrt.

Im zweiten Schritt bei der Ersteinrichtung fragt ein Assistent nach der Zu-

stimmung zu den Geschäftsbedingungen und Datenschutzrichtlinien. Man kann einzelnen Punkten zustimmen oder global seine Zustimmung erteilen. Anschließend fährt man mit dem Druck auf OK fort. Wir hatten uns gewundert, dass der Assistent in den nächsten Einrichtungsschritt weiterspringt, egal ob wir zustimmten oder nicht. Unterschiede hinsichtlich des Netzwerkverkehrs fanden wir nicht (siehe [1]).

Samsungs Erklärung

Samsung wies darauf hin, dass in diesem Installationsschritt statt einer Zustimmung auch das Überspringen möglich sei. In der Tat ist das der Fall: In der oberen Bildschirmcke steht bei allen Geräten „Überspringen“. Wenn man auf der Fernbedienung den Knopf „Rechts“ betätigt, dann erscheint ein Dialog, der erklärt, dass man den Smart Hub erst nach der Zustimmung nutzen kann – an dieser Stelle kann man die Zustimmung dann überspringen.

Wir haben für diese Bedienweise anhand des Samsung-TV-Geräts aus [2] die Pakete gezählt und dann liegt es hinsichtlich der Paketmengen in ähnlichen Regio-

nen wie andere Smart-TVs aus dem Testfeld. Der Preis, den man dafür bezahlt, ist der gleiche hier wie dort: Da die Apps deaktiviert sind, kann man unter anderem kein Netflix schauen, erreicht das Prime-Angebot nicht und hat auch keinen Web-Browser zur Verfügung.

Schmalspurbetrieb

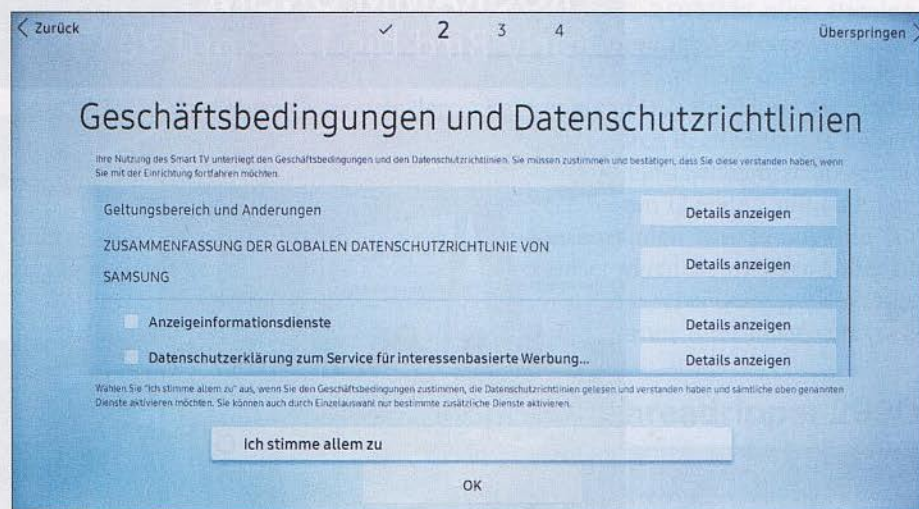
Was in dieser Schmalspurbetriebsart mit den Samsung-TV-Geräten überhaupt funktioniert: Fernsehen, Dateien von einem DNLA-Gerät abspielen und beim Fernsehen die HbbTV-Angebote abrufen. Außerdem arbeitet die Update-Funktion des Geräts trotz fehlender Zustimmung für Smart-Allergiker mag das fast schon zu viel sein. Fraglos reduziert es den Netzwerkverkehr erheblich und hält dem Nutzer auch die lästige Samsung-Werbung vom Hals, die die Geräte sonst im Smart Hub einblenden.

Unterm Strich ist die Bedienführung an der Stelle, an der Samsung die Zustimmung des Käufers einholen möchte, wenig gelungen. Samsung hat uns Bilder geschickt, die im Kleingedruckten einen Hinweis auf die Option zum Überspringen enthalten. Unser Altgerät aus [2] zeigt keinen solchen Hinweis trotz aktueller Firmware. Das rund ein Jahr jüngere Testgerät aus [1] konnten wir bis Redaktionsschluss nicht mehr prüfen.

Aus unserer Sicht ist das nicht die einzige Stelle, an der Samsung Käufer im Dunklen lässt: Im Einrichtungsmenü findet sich eine Funktion zum Zurücksetzen des Smart Hub. Wenn man die aufruft, verhält sich das TV-Gerät wieder so, als hätte man während der Einrichtung die Zustimmung verweigert. Die Apps verschwinden. Eine passende Bezeichnung wäre wohl „Zustimmung widerrufen“.

Wer ein bereits eingerichtetes Samsung-Gerät in den Schmalspurbetrieb versetzen will, braucht es nicht vollständig neu zu konfigurieren, sondern kommt mit dem Zurücksetzen des Smart Hub aus und muss dann mit den beschriebenen Funktionseinschränkungen leben.

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



Denkste: Wer keine Häkchen setzt und „OK“ drückt, stimmt trotzdem zu. Nur das unscheinbare „Überspringen“ oben rechts heißt „Lass mich in Ruhe“. Hinweise darauf finden sich bei vielen Geräten nicht mal im Kleingedruckten.

Literatur

- [1] Peter Siering, Clever oder tumb?, Was Smart-TVs ins Internet übermitteln und wie leicht sie sich hacken lassen, c't 25/2018, S. 74
- [2] Ulrike Kuhlmann, Rudi Opitz, TV-Tuning, HDR-fähige 4K-Displays von 43 bis 55 Zoll als Fernseher, Monitor und Gaming-Display im Test, c't 25/2017, S. 136

Weitere Bilder: ct.de/y934

Kaffee-Knowhow

www.kaffeewiki.de

Das **KaffeeWiki** informiert zu Herstellung und Genuss von Espresso & Co. Im „Einstieg in die Welt des Espresso“ finden angehende Kaffeekenner Antworten auf grundlegende Fragen zu Mahlgrad, Brühvorgang und Crema. Ein anderer Abschnitt beschäftigt sich mit diversen Kaffeespezialitäten von Espresso Corretto bis Latte Macchiato – der lustigerweise als „Mega-Milch-Mode-Mix zum Beeindrucken weiblicher Gäste“ beschrieben wird.

Das KaffeeWiki ist aber nicht nur ein Nachschlagewerk für die Kaffe Zubereitung, sondern beschreibt auch im Detail die

Zweikreisler:

- Auch ein Zweikreisler muss vor dem ersten Bezug ordentlich durchheizen, in der Regel länger als jeder Einkreisler (min. 30 Minuten)
- Das Vorgehen gleicht größtenteils dem beim Einkreisler, jedoch muss man vor dem Espresso-Bezug erst einen Leerbezug durchführen, weil das Wasser im Wärmetauscher mit der Zeit die Temperatur des Kessels annimmt. Dieses überhitzte Wasser muss erst abgelassen werden, weil es sonst den Kaffee verbrennen würde. Wie viel Wasser abgelassen werden muss, hängt von der Maschine und dem eingestellten Kesseldruck ab, die Menge muss jeder für seine Maschine selbst herausfinden. Mit dem Leerbezug kann man auch gleich die Tassen aufwärmen.
- Jetzt spannt man wie gewohnt den Siebträger ein und brüht den Espresso.
- Mit etwas Geschick oder einer Dosierautomatik kann man beim Zweikreisler schon mit dem Milchschaumen beginnen, wenn der Espresso noch läuft.
- Weitere Unterschiede in der Bedienung gibt es nicht, abgesehen vom separaten Heißwasserhahn. Bei einigen Maschinen muss man noch selbst den Kesselfüllstand regulieren, neuere Modelle haben zu großen Teilen eine automatische Kesselfüllung.
- Wenn der Espresso immer zu bitter oder vor allem zu sauer ist, kann das an einem ungeeigneten Kesseldruck liegen. Dieser wird am Prestostat in der Innenseite der Maschine verstellt. Bei fast allen Zweikreislern lässt sich über das Bypass- oder Expansionsventil auch der Brühdruck einstellen.

Verheißes Espressohehl



Gesamtes und poliertes Mehl



Fertiger Espresso

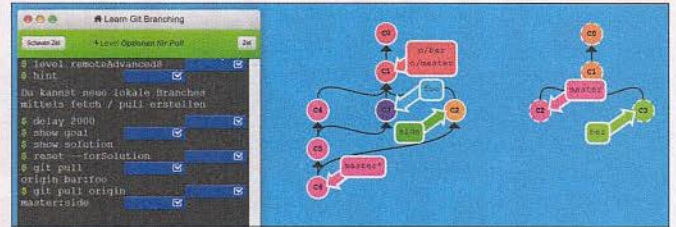
Funktionsweise unterschiedlicher Maschinenarten. Es erklärt, wozu das Entlüftungsventil dient und wie sich Vibrations- von Rotationspumpen unterscheiden. Schließlich hat das Wiki unzählige Tipps zur Wartung, Pflege und Reparatur verbreiteter Fabrikate parat. Hat man die eigene Maschine in der alphabetischen Liste gefunden, kann man etwa nachlesen, wie man deren Siebträger fachgerecht zerlegt und reinigt. (dwi@ct.de)

Git verstehen

<https://learngitbranching.js.org>

Git ist ein Versionsverwaltungssystem, das in vielen Open-Source-Projekten für Ordnung sorgt. Aber auch Entwickler kommerzieller Software arbeiten damit. So verwendet Microsoft seit 2017 Git zur Verwaltung der Windows-Versionen. Zentrale Bestandteile der Arbeit mit Git sind das Branching und Merging – das Erstellen neuer Entwicklungszweige und das Verschmelzen solcher Zweige. **Learn Git Branching** vermittelt die Regeln dafür in Form eines Spiels.

Standardmäßig befindet sich das Spiel im Erklärmodus. Dann beginnt jedes Level mit Hinweisen zu einem oder mehreren Kommandos; auch die Aufgabe des Levels wird Schritt für Schritt erläutert. Anschließend erwartet eine Konsole vom Spieler Eingaben, beispielsweise `git checkout bugFix` oder `git rebase master`. Rechts daneben werden Commits und Zweige



grafisch angezeigt. Bunte Kreise stehen hier für die Programmversionen, Linien verbinden diese zu einer Baumstruktur. Nach jeder Eingabe ändert sich die Struktur entsprechend der verwendeten Kommandos. Mit `show goal` kann der Spieler zwischen dem gewünschten Zielzustand des Baums einblenden.

Das Git-Spiel umfasst 33 Level. Fortgeschrittene können mit `build level` weitere Level bauen oder mit `import level` Aufgaben von Freunden ausprobieren. (dwi@ct.de)

Briefe als Zeitzeugnisse

www.briefsammlungen.de

Die 1995 gegründete „Museumsstiftung Post und Telekommunikation“ unterhält Museen in Berlin, Frankfurt/Main und Nürnberg. Die Stiftung besitzt die weltweit umfangreichste Sammlung deutscher Feldpost. Die ältesten dieser Briefe wurden im frühen 18. Jahrhundert geschrieben. Der größte Teil der insgesamt 120.000 Zeitzeugnisse stammt aus dem Ersten und Zweiten Weltkrieg. Die **Briefsammlungen der Museumsstiftung Post und Telekommunikation** kann man in Berlin in einer Dauerausstellung ansehen, ein großer Teil davon steht aber auch online zur Verfügung. Außer drei Feldpost-Sammlungen gibt es noch „Post von drüben“ mit rund 6000 Briefen, die zwischen 1949 und 1990 zwischen DDR und BRD verschickt wurden; 600 dieser Dokumente sind aktuell online einsehbar.

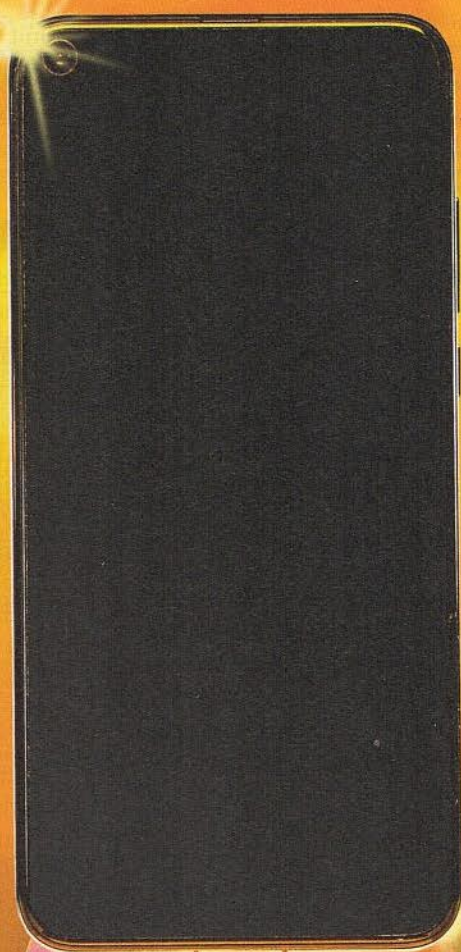
Die Briefsammlungen sind hervorragend für die Online-Recherche aufbereitet. Sie lassen sich per Volltextsuche oder nach bestimmten Orten, Themen oder Zeiträumen durchsuchen. Einerseits stehen JPG-Dateien sämtlicher Briefseiten zur Verfügung. Andererseits liegen alle Inhalte auch in Textform vor, was beispielsweise bei Briefen, die in Sütterlin geschrieben wurden, das Lesen sehr erleichtert. Viele der Originaldateien werden durch eine kurze biografische Skizze des Verfassers ergänzt. (dwi@ct.de)



Diese Seite mit klickbaren Links: ct.de/yeqx

Biegen ohne brechen

Wie sich Smartphones 2019 verändern werden



**Technik-Trends
bei Smartphones Seite 76
Vergleichstest
High-End-Smartphones Seite 78**

Flexible Displays, 5G und künstliche Intelligenz: Zukünftige Smartphones sollen endlich wieder echte Innovationen bieten. Die diesjährige Generation kommt dagegen vergleichsweise langweilig daher.

Von Hannes A. Czerulla

Bei den Smartphones steht dieses Jahr die wahrscheinlich größte Design-Evolution seit dem kapazitiven Touchscreen an: Endlich sind biegsame Displays marktreif. Es gibt sogar schon die ersten Geräte mit der Technik zu kaufen.

Am weitesten in der Entwicklung scheint die Firma Royole. Nie gehört? Wir auch nicht, bevor wir deren erstes marktreifes biegsames Smartphone FlexPai auf der CES in die Hand nehmen konnten. Doch auch die populäreren Hersteller stehen mit solchen Geräten in den Startlöchern. Mit hoher Wahrscheinlichkeit werden viele von ihnen ihre flexiblen Smartphones zur Mobilfunkmesse MWC enthüllen. Ganz vorne mit dabei sein wird voraussichtlich Samsung mit seiner Infinity Flex Display genannten Technik. Doch auch Konkurrenten wie Xiaomi haben konkrete Produkte angekündigt.

Abgesehen davon, dass die neuen Displays unheimlich schick und ungewöhnlich aussehen und neue Smartphone-Bauformen zulassen, haben sie auch noch einen praktischen Nutzen. Denn sie stellen ähnlich viel Bildschirmfläche zur Verfügung wie deutlich sperrigere Tablets, sind zusammengeklappt aber nicht viel größer als heutige Smartphones.

Vorerst werden die faltbaren Smartphones aber noch ein Nischendasein führen – einfach deshalb, weil die futuristische Produktkategorie teuer ist. So kostet das FlexPai mit 256 GByte Flash-Speicher in Royoles Webshop sage und schreibe 1539 Euro.

Auch auf Seiten der Netzbetreiber steht eine große Entwicklung an: Der LTE-Nachfolger 5G steht vor der Tür. Und noch keines der aktuellen Smartphone-Modelle ist darauf vorbereitet. Der Mobilfunkstandard verspricht bis zu 100-fach höhere Download-Geschwindigkeiten als im LTE-Netz und minimale Signallaufzeiten.

Vor allem Letzteres eröffnet neue Möglichkeiten im Bereich Cloud-Gaming

oder Cloud-Computing – also die Auslagerung der Rechenkapazität auf Server. Doch bis unsere Smartphones hierzulande im 5G-Netz mit all seinen Vorteilen surfen, ist es noch ein weiter Weg. Zwar könnten die ersten Telefone dieses Jahr zu kaufen sein, doch wird es noch dauern, bis die Provider Verträge mit erschwinglichen Konditionen anbieten. Da greift man lieber zu einem aktuellen High-End-Modell mit LTE Cat15 oder höher und schöpft zumindest die Maximalgeschwindigkeit der hiesigen LTE-Netze aus.

Intelligente Assistenten

KI, KI, KI ... hört man die Werbeslogans der Smartphone-Hersteller, fragt man sich, wie das derzeitige Smartphone überhaupt noch ohne künstliche Intelligenz funktionieren kann. Firmen wie LG, Huawei und Samsung preisen kaum ein Feature so stark an wie die KI, die angeblich in ihren Geräten steckt. LG lässt die eigenen Technik ThinQ sogar in die Modellnamen einfließen, wie zum Beispiel beim G7 ThinQ.

Wird man also technisch abgehängt, wenn man sich ein aktuelles, noch weniger intelligentes Telefon zulegt? Dazu muss man die Funktionen näher anschauen, die angeblich so sehr von der KI profitieren.

Nach aktuellem Stand handelt es sich größtenteils um einfache Automatisierungen wie beispielsweise eine Voraussage, welche App der Nutzer als Nächstes öffnen möchte. Etwas weiter gehen die KI-Funktionen der Kameras. So erkennt beispielsweise Huawei Knipse immer mehr Objekte und Szenen von selbst und passt die Einstellungen an, um beispielsweise Porträtaufnahmen mit einem passenden Bokeh zu versehen, den Sonnenaufgang mit einer Langzeitbelichtung in prächtigen Farben erstrahlen zu lassen oder die Auslösezeit herabzusetzen, weil die Hauskatze sonst wieder aus dem Arrangement huscht.

Mit echter, autonom lernender Intelligenz hat das wenig zu tun und das wird sich in der kommenden Gerätegeneration auch noch nicht grundlegend ändern. Außerdem besteht bei den aktuellen High-End-Modellen eine gute Chance, dass sie neue Funktionen per Software nachgeliefert bekommen.

Kamera

Die Chance auf spätere Verbesserungen per Update besteht auch bei den Kameras. Sie haben in den letzten Jahren qualitativ spürbar zugelegt und schießen beispielsweise deutlich bessere Fotos bei Dunkelheit. Dabei haben sich Chips und Optiken nur in überschaubarem Maß weiterentwickelt. Der Großteil der Fortschritte ist der kontinuierlich verbesserten Software zuzuschreiben. Das sieht man unter anderem daran, dass in einem Großteil der Geräte die gleichen Sony-Sensoren eingebaut sind und man dennoch deutliche Unterschiede bei den Bildern erkennen kann. Einzig bei der Brennweite wünscht man sich mehr Auswahl. (hcz@ct.de) **ct**

Für über 1500 Euro kann man bei Royole ein Stück Zukunft kaufen. Erschwingliche Preise für faltbare Smartphones darf man in diesem Jahr aber nicht erwarten.





Superphones

High-End-Smartphones mit Dual-SIM und Mehrfachkameras im Vergleich

Ein guter Zeitpunkt, um sich ein Spitzen-Smartphone zuzulegen: Aktuelle Geräte sind bereits ein paar Monate erhältlich, sodass man nicht mehr die von Herstellern anfangs aufgerufenen Mondpreise bezahlen muss. Die Technik ist dennoch up to date und man braucht auf keine Spielerei zu verzichten.

**Von Robin Brand
und Hannes A. Czerulla**

Sie suchen nach einem Smartphone mit bester Ausstattung und allen aktuellen Funktionen, das nicht schon nächstes Jahr völlig veraltet ist? Dann ist jetzt ein guter Zeitpunkt, zuzuschlagen und sich ein High-End-Modell zu gönnen.

Zwar werden die Hersteller im Frühling jede Menge neue Modelle auf die Kunden loslassen, aber weltbewegende Innovationen wie faltbare Displays oder 5G-Unterstützung bleiben vorerst Prototypen oder teuren Exoten vorbehalten. Auch steht zunächst keine Entwicklung

an, die das Smartphone im Alltag spürbar verbessert. Vielmehr liegt der Vorteil aktueller Geräte darin, dass sie ausgereifte Technik beherbergen: Die Akkus halten lang, die Prozessoren sind schnell, die Kameras schießen gute Bilder und die Software läuft dank Updates stabil auf dem aktuellen Stand.

Testfeld

Der Einzelgänger im Testfeld ist das Apple iPhone Xs Max. Denn alle anderen Testkandidaten laufen mit Android. Es handelt sich dabei um die etwas größere Ver-

sion des Xs. Doch bis auf Display-Größe und Akku unterscheiden sich die beiden Apples nicht voneinander.

Das iPhone tritt gegen die Elite der Android-Telefone an. Was für Apple das iPhone Xs Max, ist in der Android-Welt das Pixel 3 XL, das direkt vom Android-Paten Google stammt. Hier findet man ein unverbasteltes Betriebssystem und kann darauf zählen, die aktuelle Android-Version früher als andere auf dem Gerät zu haben.

Huawei hat seinem Spitzenmodell Mate 20 Pro gleich drei Kameras für die Rückseite spendiert. Das Honor View 20 Pro aus gleichem Haus machte wegen seines Display-Notch von sich reden – beziehungsweise deswegen, weil es keinen hat. Stattdessen ist es eins der ersten Telefone mit einem Loch im Display, durch das die Kameralinse schaut.

Das Samsung Galaxy Note 9 setzt sich wie seine Vorgänger durch den namensgebenden Bedienstift von der Masse ab. Typisch für LG ist der Preis des G7 ThinQ seit dem Marktstart deutlich gefallen, und somit kostet es nur 400 Euro – halb so viel wie manch anderer Kandidat, ohne bei der Ausstattung abgehängt zu werden. Sony hat bei dem Xperia XZ3 das erste Mal ein OLED in sein Topmodell eingebaut. OnePlus vertreibt sein 6T weiterhin direkt über die eigene Webseite und spart damit Kosten, die es in Form niedrigerer Preise an den Kunden weitergibt. Mittlerweile gibt es auch einen offiziellen deutschsprachigen Webshop.

Display

Unterscheidungsmerkmal Nummer 1 ist bei den meisten Geräten im Test das Display – kein Wunder, bestehen die Smartphones augenscheinlich aus kaum etwas anderem mehr. Weiterhin existieren die Lager OLED und LCD. Wobei Letzteres

Das Huawei Mate 20 Pro hält für fast jede Situation die passende Kamera und Brennweite bereit.



zunehmend an Anhängern verliert; nur das Honor View 20 und das LG G7 ThinQ haben noch ein LCD beziehungsweise IPS-Screen eingebaut.

Alle anderen Geräte nutzen ein OLED und es gibt kaum noch einen Grund, das nicht zu tun. Sie zeigen im Vergleich zu LCDs einen deutlich höheren Kontrast und kräftigere Farben. Wobei die Hersteller die Anzeigen mittlerweile konservativer kalibrieren und kein Display mehr Farben so bonbonbunt darstellt wie zu Anfangszeiten der OLEDs.

Die hellsten Anzeigen haben das Samsung Galaxy Note 9, das Sony Xperia XZ3 und das LG G7 mit jeweils über 700 cd/m² – mehr gibts auch bei Smartphones außerhalb des Testfelds nicht. Es folgen das Apple iPhone Xs Max und das Huawei Mate 20 Pro mit rund 650 cd/m². Der Unterschied zu den drei Top-Displays ist kaum sichtbar und Bildschirme mit mehr als 600 cd/m² kann man auch noch bei viel Lichteinfall gut ablesen. Schlusslicht bildet das Honor View 20 mit fast 350 cd/m² – scheint beispielsweise die Sonne direkt auf den Bildschirm, erkennt man das Bild deutlich schlechter als auf den helleren Anzeigen.

Der hohe Wert des G7 ist mit Vorsicht zu genießen, denn LG trickst ein wenig: Zusätzlich zu den üblichen roten, grünen und blauen Subpixeln hat der Hersteller weiße Pixel eingebaut. Dadurch steigt die Helligkeit weißer Flächen oder Farben mit hohem Weißanteil. Aber umso kräftiger die Farben sind, umso geringer ist der Vorteil dieser speziellen Subpixelmatrix.

Gerne werben die Hersteller momentan mit HDR10 oder Dolby Vision, wie es auch bei Fernsehern üblich ist. Viel Aufmerksamkeit sollte man den Labels nicht schenken, denn die Auflagen für Mobilgeräte sind bei Weitem nicht die gleichen wie für TVs und sehr viel weicher definiert. So muss ein Smartphone beispielsweise nur eine Helligkeit von 550 cd/m² erreichen für HDR10; für Dolby Vision gilt gar keine Vorgabe.

Die Auflösung liegt fast bei allen Geräten jenseits von Full-HD. Eine Rolle spielt das kaum noch, da alle Anzeigen scharf sind. Unterschiede zwischen den Bildschirmen in Bezug auf die Schärfe sind nur mit der Lupe festzustellen. Geräte wie das Note 9 mit höherer Auflösung

Laufzeiten

Modell	Video (200 cd/m²) [h]	3D-Spiel (200 cd/m²) [h]	WLAN-Surfen (200 cd/m²) [h]	Video-Streaming (200 cd/m²) [h]	Ladezeit auf 50 % / 100 %
	besser ▶	besser ▶	besser ▶	besser ▶	
Apple iPhone Xs Max	11,9	9,9	8,8	13,4	88 min / 144 min
Google Pixel 3 XL	12,8	8,8	9,8	11,5	34 min / 108 min
Honor View 20	10	7,2	11,4	9,9	25 min / 84 min
Huawei Mate 20 Pro	14,8	8,8	12,6	13,1	22 min / 66 min
LG G7 ThinQ	9,7	5,7	9	8,9	36 min / 106 min
OnePlus 6T	18,5	9,7	14	15,2	31 min / 80 min
Samsung Galaxy Note 9	17,5	8,4	14,9	13,1	39 min / 106 min
Sony Xperia XZ3	11,2	8,2	11,4	10,3	52 min / 166 min
Spiel: Asphalt 8, Surfen: Abruf einer einfachen Webseite alle 30 s					



Loch statt Notch:
Honor hat ins Display
des View 20 ein Loch
für die Frontkamera
gebohrt.

regeln sogar per Software herunter, um Strom zu sparen.

Notch

Seit den ersten Smartphone-Displays mit schmalem Rand stellt sich die Frage: Wohin mit der Frontkamera? Apple, Google und LG fanden für sich die Antwort in Form eines Notch, also einer länglichen Einkerbung im Display. So richtig schön ist diese Lösung nicht. Da sowohl iOS als auch aktuelle Android-Versionen die Darstellung an die Einkerbung anpassen, gibt es aber keine praktischen Nachteile.

Die Notches des Xs Max, Mate 20 Pro, Pixel 3 XL und G7 sind deswegen so breit, weil sie nicht nur die Frontkamera beherbergen, sondern auch den Lichtsensor und den Telefonlautsprecher. OnePlus hat es beim 6T geschafft, den Lautsprecher in die Gehäusekante zu verfrachten, sodass im Notch nur die Kamera sitzt. Dadurch ist die Einkerbung des 6T nur etwa ein Viertel so groß wie bei den anderen Geräten und man hat mehr Bildschirmfläche zum Nutzen. Einen Schritt weiter geht Honor und stanzt kurzerhand ein kleines Loch ins Display, durch das die Kamera den Nutzer anlinst. Nach etwas Gewöhnung fällt das Loch kaum noch auf und es verdeckt keine Schaltflächen oder Ähnliches.

Sony und Samsung gehen den klassischen Weg und lassen den oberen Bildschirmrand über die gesamte Display-Breite laufen.

Entsperrmethoden

Weiterhin ist der Fingerabdruckscan die bevorzugte Authentifizierungsmethode der Hersteller. Bis auf das iPhone haben alle Telefone einen entsprechenden Sensor, meist auf der Rückseite eingebaut. Beim OnePlus 6T und Huawei Mate 20 Pro ist er unsichtbar hinterm Display versteckt. Die Stelle, auf die man den Finger zum Entsperren legen muss, zeigt der Bildschirm an. Der Vorteil liegt darin, dass man das Telefon nicht erst aufheben muss, um zu entsperren. Alle Sensoren funktionieren zuverlässig und schnell, die im Display brauchen ein klein wenig länger.

Apple setzt beim iPhone Xs Max voll und ganz auf die Gesichtserkennung Face ID. Ein Fingerabdrucksensor ist nicht eingebaut. Stattdessen projiziert eine auf der Vorderseite eingebaute Infrarot-LED 30.000 Messpunkte aufs Nutzergesicht, von dem die Kamera dann ein dreidimensionales Bild macht. Die Technik erkennt sogar, ob der Nutzer das Gerät anschaut und entsperrt nur, wenn die Augen aufs iPhone gerichtet sind. Vorteil der Methode

ist, dass man nicht erst den Fingerabdrucksensor ertasten oder das Gerät aufheben muss. Die Erkennung funktioniert kaum langsamer als der Scan eines Fingerabdrucks. Allerdings ist die Fehlerquote höher und immer mal wieder muss man einen zweiten Versuch starten. Ein reproduzierbares Bild des Nutzers wird nicht gespeichert, sondern nur Hash-Werte.

Zwar bieten auch die Android-Geräte eine Entsperrung durch Gesichtserkennung an, doch sie erfassen nur ein zweidimensionales Bild und sind daher einfacher auszutricksen.

Kameras

Es scheint, als hätten die Smartphone-Hersteller eine universelle Antwort auf alle Kameraprobleme gefunden: mehr Kameras. Nur noch das Sony Xperia XZ3 und das Google Pixel 3 XL kommen mit einer einzelnen Kamera auf der Rückseite aus. OnePlus und Honor nutzen eine zweite Kamera für künstliche Tiefenunschärfe (Bokeh) auf Porträtaufnahmen. Wobei die Single-Kameras das dank spezieller Software genauso gut beherrschen, die besten Bokeh-Aufnahmen machte das Pixel 3. Das iPhone und das Note 9 nutzen die Zweitkamera ebenfalls für solche Zwecke; man kann sie aber auch direkt ansteuern. Es handelt sich dabei um Zweifach-Telekameras. Unserer Meinung nach ist ein Tele nützlicher im Smartphone als eine weitere weitwinkeligere Kamera wie im LG G7. Beim 6T und View 20 kommt der Nutzer nicht an die Fotos der Zweitkamera heran. Auf die Spitze treibt es Huawei und baut drei Kameras ins Mate 20 Pro ein: eine normale Kamera, eine mit Superweitwinkel und eine mit dreifachem Tele. Das lässt Freiraum für Kreativität und tut auch der Fotoqualität gut. Videos gefielen uns ebenfalls sehr gut, doch in bestimmten Situationen zeigten sich leichte Ver-

Benchmarks

Modell	Coremark Multi-Core [Punkte]	GFXBench 3.1 Manhattan offscreen [Punkte]	GFXBench 3.1 Manhattan onscreen [Punkte]	3DMark Ice Storm Unlimited [Punkte]	3DMark Slingshot Extreme [Punkte]
	besser ▶	besser ▶	besser ▶	besser ▶	besser ▶
Apple iPhone Xs Max	-	139	60	77250	k. A.
Google Pixel 3 XL	75844	60	34	60996	5554
Honor View 20	74205	54	51	37242	3626
Huawei Mate 20 Pro	81208	53	49	34684	3547
LG G7 ThinQ	71683	60	31	58520	4391
OnePlus 6T	76280	61	54	65767	4734
Samsung Galaxy Note 9	58013	45	24	42372	3349
Sony Xperia XZ3	75536	54	30	66531	4527

zeichnungen der Linsen oder unauffällige Pumpbewegungen des Autofokus.

Alle Geräte im Test machen grundsätzlich sehr gute Bilder, die man ohne Bearbeitung auf dem nächsten Familientreffen präsentieren kann. Die Auflösung spielt eine Nebenrolle, solange man später keine Bildausschnitte nutzen möchte. Die Spreu vom Weizen trennt sich nur in besonders herausfordernden Situationen, vor allem mit wenig Licht. In dieser Situation zeigt sich unter anderem, wie gut die Software auf die Bedingungen reagiert und ob die Automatik die richtigen Einstellungen wählt.

Wurde es dämmrig, war das Google Pixel 3 XL im Fototest nicht mehr zu schlagen. Denn dann kann der „Nachtsichtmodus“ seine volle Stärke ausspielen und auf Wunsch die Nacht so weit aufhellen, dass Dinge auf den Fotos zu erkennen sind, die selbst das menschliche Auge in der Dunkelheit nicht mehr sieht. Der Nachtsichtmodus verwendet dafür mehrere Fotos gleichzeitig, ähnlich wie bei HDR-Bildern.

Das iPhone platziert sich im Mittelfeld und stellt Farben recht kühl dar. Da die Bilder etwas aufgehellt werden, fehlt es ihnen im Vergleich mit dem Pixel 3 XL etwas an Kontrast. Merkwürdigerweise ist es bei Videos genau umgekehrt. Dort sind die Aufnahmen des Pixel etwas zu hell und lassen an Kontrast und Farbstärke vermissen. Das iPhone punktet bei den Videoaufnahmen auf ganzer Linie, zeigt realistische Kontraste und Plastizität. Der optische Bildstabilisator funktioniert so zuverlässig, dass man manchmal meinen könnte, das Video wurde mithilfe eines Gimbals gedreht. Selbst Schwenks funktionieren geschmeidig.

Dual-SIM

Auf Dual-SIM-Funktion haben viele Smartphone-Nutzer jahrelang gewartet, doch auf Druck der Netzbetreiber fand man die praktische Technik fast immer nur in Low-End-Geräten. Glücklicherweise sind diese Zeiten vorbei und ein Großteil der High-End-Smartphones unterstützt mittlerweile eine zweite SIM-Karte.

Eine Selbstverständlichkeit ist das aber auch in diesem Testfeld nicht. Denn das Apple iPhone Xs Max, das Google Pixel 3 XL und das LG G7 ThinQ nehmen nur eine physische SIM-Karte auf. Die ersten beiden sind die einzigen Geräte im Test, die mit einer eSIM-Karte betrieben werden können. Nutzt man diese Mög-



Apple iPhone Xs Max

Unter High-End-Smartphones hat das Apple-Handy immer einen Sonderstatus: Es kommt nicht aus der Android-Welt. Ein homogenes, flüssiges Betriebssystem und eine Update-Versorgung, von der Android-Nutzer nur träumen können, gehören zu den Vorzügen von iOS. Doch es greift zu kurz, das aktuelle Topmodell iPhone Xs Max auf die Software zu reduzieren. Als teuerstes iPhone aller Zeiten auf den Markt gekommen, nimmt das brillante Display fast die gesamte Vorderseite ein. So schafft es Apple, ein riesiges Panel mit einer noch recht kompakten Form zu kombinieren. Die Kamera fotografiert auf hohem Niveau – wie beim Vorgänger iPhone X kommen eine Weitwinkel- und eine Zweifach-Telekamera zum Einsatz. Ähnlich wie die konkurrierenden Android-Smartphones kombiniert das iPhone beispielsweise in der Dunkelheit mehrere Fotos, um Bildrauschen zu reduzieren und Kontrast zu erhöhen. Anders als bei Androiden kann der Nutzer aber kaum selbst eingreifen. Die Resultate unterscheiden sich von der Konkurrenz vor allem in Details.

Insgesamt überzeugt das iPhone Xs Max im Vergleich zum Vorgänger mit verbesserter Kamera, schnellerem Prozessor und längeren Laufzeiten – das rechtfertigt für iPhone-X-Besitzer aber kaum eine 1000-Euro-Investition. Wer hingegen von älteren iPhone-Modellen umsteigt, wird deutliche Verbesserungen feststellen können. Geladen wird via proprietärem Lightning-Stecker.

- 👉 Spitzendisplay
 - 👉 schnellster Prozessor
 - 👉 sehr teuer
- Preis: 1150 Euro



Google Pixel 3 XL

Auch mit der dritten Generation der Pixel-Reihe versucht sich Google im High-End-Segment. Die Smartphones punkten mit exklusiven Android-Features und häufigen Updates – und das drei Jahre lang sofort zum Veröffentlichungstermin, nicht erst Monate später. Wer ein unverbasteltes Android-System möchte, ohne nervige, herstellereigene Apps, kommt am Pixel nicht vorbei. Kein Wunder, denn kein Smartphone-Hersteller definiert sich so sehr über die Software wie Google.

Da kann es schon mal passieren, dass der Kamera per Update das Sehen im Dunkeln beigebracht wird. Zuletzt erhielten die Pixel-Telefone – auch frühere Generationen – den Nachtsichtmodus, der die Handys bessere Fotos in der Dunkelheit schießen lässt. Während der Algorithmus tatsächlich beeindruckend funktioniert, lässt sich mit Software nicht jedes Problem lösen. Die Weitwinkellinsen mancher Konkurrenten mit Dual- oder Triplekamera kann das Pixel mit einem Objektiv nicht imitieren, Zoom nur berechnen. Dennoch gehört die Kamera zu den besten auf dem Markt.

Der lange Support für die Pixel-Telefone macht den Vorgänger Pixel 2 zur schärfsten Konkurrenz. Das deutlich günstigere Gerät profitiert von den Software-Neuerungen gleichermaßen. Die Hardware des aktuellen Pixel ist auf der Höhe der Zeit – aber ohne das gewisse Etwas. Der Speicher lässt sich leider nicht erweitern. Dual-SIM-fähig ist es nur über eine eSIM.

- 👉 Updates kommen zeitnah
 - 👉 sauberes Android
 - 👉 beste Low-Light-Performance
- Preis: 700 Euro



Honor View 20

Jetzt also ein Loch im Display: Während viele Hersteller die Aussparung für die Kamera im Display, den Notch, immer weiter verkleinern, platziert Honor beim View 20 die Frontkamera einfach direkt im LCD-Panel. Mit dieser Neuerung kommt die Huawei-Tochter der Konkurrenz zuvor. Keinen halben Zentimeter misst die runde Aussparung für die Frontkamera. Der beeindruckende Effekt: Auf der Vorderseite besteht das View 20 fast ausschließlich aus Display. Nach kurzer Nutzung fällt das Kameraloch kaum mehr ins Auge.

Abseits der Lochkamera spendiert Honor dem View 20 erstaunlich viel Technik für den Preis – wahlweise bis zu 256 GByte Flash- und 8 GByte Hauptspeicher. Im Inneren werkelt der gleiche schnelle Prozessor wie im Mate 20 Pro. Die Kamera schießt bis zu 48 Megapixel und holt im AI Ultra-Clarity-Modus viele Details aus den recht blassen, kühl abgestimmten Motiven, wenn der Fotograf das Handy stillhält. Da die Dateien so bis zu 20 MByte groß sind, löst die Automatik standardmäßig 12 Megapixel auf und neigt dann zum Glatteichnen von Details. Verzichtern müssen Nutzer auf einen zertifizierten Schutz vor Wasser und Staub ebenso wie auf die Möglichkeit, das Handy drahtlos zu laden. Dafür hat das Handy eine Kopfhörerbuchse.

- 👍 gute Performance
 - 👍 riesiges Display, ...
 - 👎 ... das heller sein könnte
- Preis: 570 Euro



Huawei Mate 20 Pro

Viel hilft viel: Zumindest auf das Topmodell von Huawei trifft das zu. Mit dem Mate 20 Pro zeigt der Hersteller, dass es auch mal mehr als zwei Linsen sein dürfen. Denn mit der Triple-Kamera müssen Smartphone-Nutzer kaum Abstriche machen. Das optische Dreifach-Tele ist im Test den Zweifach-Teles überlegen und die Weitwinkelkamera mehr als eine Spielerei – zumindest bei guten Lichtverhältnissen. Die Hauptkamera lässt sich auch bei Dunkelheit nicht so schnell aus dem Konzept bringen. So flexibel wie mit dem Mate 20 Pro fotografiert sich mit keinem anderen High-End-Telefon. Kurzum: Die Triple-Kamera des Mate 20 Pro gehört zu den besten Smartphone-Kameras auf dem Markt.

Auch der hauseigene Kirin-Prozessor ist auf Augenhöhe mit den Wettbewerbern von Qualcomm und Samsung. Einzig den Apple-Prozessoren muss er sich geschlagen geben. Das große OLED-Display leuchtet hell und kontraststark. Es ist an den Flanken leicht nach hinten gebogen. Wem das nicht reicht, der schließt das Handy per USB-C an einen Monitor an. So wechselt das Huawei in einen komfortablen Desktopmodus. Für lange Laufzeiten sorgt ein großer Akku mit 4200 mAh Kapazität, der außerdem erfreulich schnell lädt – in 66 Minuten ist er voll. Nervig sind dagegen die vielen haus-eigenen Apps, die einen penetrant zu einer Huawei-ID überreden wollen. Der Speicher lässt sich zwar erweitern, aber nur mittels Huawei-eigener Nano-Memory-Karte.

- 👍 großartige Kamera
 - 👍 lange Laufzeiten
 - 👎 eigenes Speicherkartenformat
- Preis: 800 Euro



LG G7 ThinQ

Vorhersehbarkeit kann man der G-Serie von LG wahrlich nicht vorwerfen. Mal versuchte es LG mit geschwungenem Body, dann mit einem der ersten 1440p-Panels, dann mit einem Leder-rücken und später sogar mit einem modulareren Handy. Nachdem sich LG mit dem G6 komplett vom modularen Konzept verabschiedet hat, ist das G7 ThinQ für G-Verhältnisse eine behutsame Weiterentwicklung. Im Unterschied zum 6er kommt das G7 ThinQ mit einem aktuellen Top-Prozessor. Neu ist auch eine Aussparung im sehr hell leuchtenden LC-Display, der Notch. Passé ist der mit dem Fingerabdrucksensor kombinierte Powerbutton. Das Einschaltknöpfchen ist an den Rand des Geräts gewandert. Dort sitzt auch eine Taste, die eigens dafür gedacht ist, den Google Assistant zu wecken.

Dem Trend, die Kopfhörerbuchse einzusparen, folgt LG glücklicherweise nicht. Im Gegenteil: Wie das LG V30 hat das G7 gleich vier Audiowandler, die genug Leistung für Kopfhörer mit hoher Impedanz mitbringen. Einen Mehrwert in manchen Situationen liefert der Weitwinkel der Dual-Kamera. Aber leider sind die Aufnahmen an den Rändern verzerrt. Insgesamt reicht die Fotoqualität nicht an die der Konkurrenz heran – da hilft auch die KI nicht, die Objekte, die sie erkennt, fleißig vorschlagwortet und die Einstellungen der Situation entsprechend anpasst. Wer nicht die beste Smartphone-Kamera auf dem Markt braucht, könnte mit dem G7 ThinQ dennoch glücklich werden, zumal bei einem Preis um 400 Euro.

- 👍 helles Display
 - 👎 veraltetes Android
 - 👎 Kamera mäßig
- Preis: 400 Euro



OnePlus 6T

Die Konkurrenz für den einstigen selbsternannten „Flaggschiff-Killer“ wird größer. Mit Xiaomi oder Honor drängen weitere Player in den Markt der günstigeren High-End-Geräte. Mit dem 6T verfolgt OnePlus eine simple Strategie, um den Angriff abzuwehren: weiterhin gute Handys bauen. Der Hersteller, der seine Geräte im Halbjahrestakt auf den Markt wirft, packt alles ins 6T, was unter High-End-Verdacht steht. Die Performance ist auf Augenhöhe mit der von teuren Premium-Handys, die Akkulaufzeiten gehören zu den besten überhaupt. Wem ein langer Support wichtig ist, macht mit dem OnePlus nichts falsch. Selbst das OnePlus 3, einst mit Android 6 auf den Markt gekommen, erhält Android 9. Das Betriebssystem ist zudem angenehm unverbastelt.

Obwohl der Verkaufspreis von 550 Euro für das Einstiegsgerät mit 128 GByte Flash und 6 GByte RAM deutlich unter der hochpreisigen Konkurrenz liegt, wartet OnePlus beim 6T mit Extravaganzen wie einem Fingerabdruckscanner im Display auf. Eine Kopfhörerbuchse oder nach IP-Standard zertifizierter Schutz gegen Staub und Nässe fehlen dagegen, der Speicher ist nicht erweiterbar. Bei der Kamera schwächelte OnePlus zudem ein wenig – gemessen an High-End-Ansprüchen. Daran hat der Hersteller gearbeitet. Speziell in Situationen mit wenig Licht übertrifft das 6T seine Vorgänger sichtbar. An die Gesamtleistung der Konkurrenz-Knipser von Samsung, Huawei oder Google reicht es aber nicht heran.

- 👍 lange Laufzeiten
 - 👍 unverbasteltes Android
 - 👎 Kamera nicht high-end
- Preis: 550 Euro



Samsung Note 9

Gute Kameras und schnelle Prozessoren haben alle High-End-Smartphones. Einen Stift hat nur Samsungs Galaxy Note 9. Beim jüngsten Spross der Note-Familie wird dieser wahlweise auch zur Fernbedienung. Per Bluetooth lässt sich zum Beispiel die Kamera auslösen oder die Präsentation der Fotos steuern; ein Gimmick, das sich im Test als überraschend nützlich erwiesen hat. Allerdings ist der Spaß kurzlebiger Natur. Nur für eine halbe Stunde reicht der Akku im Stift. Wie gewohnt zum Schreiben und Zeichnen lässt sich der Stift auch bei leerem Akku benutzen. Praktisch: Nimmt man bei ausgeschaltetem Display den Stift heraus, öffnet sich eine Notiz-Soforteingabe, die Geschriebenes beim Wiedereinstecken des Stifts automatisch speichert.

Während Stift-Fans kaum Alternativen zum Note finden werden, liefert das Smartphone auch allen anderen High-End-Liebhabern jede Menge Kaufargumente. Eine tolle Kamera, ein Spitzen-Display und ein ausdauernder Akku gehören dazu. Ob Kopfhörerbuchse, erweiterbarer Speicher, Dual-SIM, USB-C-Desktopmodus oder IP68-Zertifizierung: Der Ausstattungsliste fehlt es an nichts. Einen Haken hat das Ganze allerdings, nämlich das Preisschild, das Samsung seinem Tophandy umgehängt hat. Zum Marktstart kostete es rund 1000 Euro, um etwa 800 Euro erleichtert es seine Käufer derzeit. Da das Note 9 im Vergleich zum Vorgänger vor allem im Detail verbessert ist, lohnt sich der Vergleich vor dem Kauf. Das Note 8 kostet nur knapp die Hälfte.

- 👍 helles OLED
 - 👍 Spitzenkamera
 - 👍 Stifteingabe
- Preis: 800 Euro



Sony Xperia XZ3

Die Tophandys von Sony sehen immer ein wenig aus wie die Neuheiten aus dem Vorjahr. Da macht das Xperia XZ3 mit seinen breiten Displayrändern keine Ausnahme. Auch sonst ist das Gerät ein typisches Sony-Smartphone: Die Verarbeitung ist tadellos, der Support stimmt. Der Januar-Sicherheitspatch war Mitte des Monats da. Neu ist dagegen das OLED-Display. Dieses löst beim XZ3 die ohnehin schon nicht schlechten LCD-Panels der Vorgänger ab. Das OLED glänzt mit größerem Farbraum, höheren Kontrasten und ist mit 750 cd/m² eines der hellsten Displays auf dem Markt. Für Nutzer, die viele Videos auf dem Handy schauen, ist es einen Blick wert.

Trotz seiner Größe liegt das XZ3 dank schmalen Displayrand und abgerundeten Kanten gut in der Hand. Auf dem Tisch platziert, ist es nicht mehr so wackelig wie der Vorgänger XZ2. Mit einer eigenen Hardware-Taste für die Kamera positioniert Sony sein High-End-Gerät als Kamera-Smartphone – mit nur einer Linse. Bei guten Lichtverhältnissen schießt sie gute, etwas dunkle Fotos mit vielen Details. Manchmal reagiert die Kamera-App etwas träge. Nett ist die Super-Zeitlupe mit bis zu 960 fps. Ohne Teleobjektiv und Weitwinkel ist die Fotografie mit dem Sony-Smartphone aber nicht so flexibel wie bei der Konkurrenz. Dennoch: Wirkliche Schwächen leistet sich das XZ3 nicht.

- 👍 helles OLED
 - 👍 Verarbeitung
 - 👎 Kamera träge
- Preis: 700 Euro

lichkeit, kann man den frei gewordenen SIM-Karten-Slot für einen zweiten Mobilfunkvertrag nutzen.

Die eSIM, also eine virtuelle SIM-Karte, die nur als Software vorliegt, hat theoretisch den Vorteil, dass Tarifwechsel einfacher und schneller vonstatten gehen und man beispielsweise nicht erst auf den Versand der Karte warten muss. In der Realität dürften aber die wenigsten Nutzer regelmäßig wechseln. Außerdem ist Dual-SIM per eSIM nur ein kleiner Trost für den fehlenden zweiten SIM-Karten-Slot. Denn bislang bieten nur Vodafone und die Telekom passende (teils recht teure) Tarife mit eSIM an. Tarife im O2-Netz und die zahlreichen deutlich günstigeren Angebote von Dritt-Providern kann man nicht nutzen.

Bis auf das LG G7 liefen alle Geräte mit dem aktuellen Android 9 und Sicherheitspatches von Dezember oder Januar. Eine solch positive Bilanz konnten wir bislang selten in einem Vergleichstest ziehen.

Zwar arbeiten unterschiedliche Prozessoren in den Geräten, die in Benchmarks unterschiedliche Ergebnisse lieferten, doch geraten die SoC in den High-End-Smartphones immer mehr zur Nebensache. So liefen alle Geräte im Test vollkommen flüssig und stellten auch die grafisch anspruchsvollsten Spiele ruckelfrei dar.

Fazit

Ein Test ohne Ausfall: Wer bereits eines der Testgeräte besitzt, hat nichts falsch gemacht und sich eines der besten Smartphones zugelegt.

Bewegt man sich bereits im iOS-Universum und will nicht zu Android wechseln, kauft man sich ein iPhone Xs. Ist das Display zu klein, nimmt man das Xs Max. Falsch macht man mit dem Gerät nichts. Es hat den schnellsten Prozessor, der Akku hält bis zu zwei Tage lang. Die Kamera ist zwar nicht die beste, aber dennoch sehr gut. Das einzige, was am iPhone Xs wirklich schmerzt, sind Apples horrenden Preise. Alternativ gibt es das billigere iPhone XR, bei dem man aber deutliche Ausstattungsabstriche machen muss.

Möchte man immer die aktuelle Android-Version auf dem Gerät haben und kein vom Hersteller verbasteltes Betriebssystem, ist das Google Pixel 3 XL die erste Wahl. Zudem bekommt man die beste (Einzel-)Kamera und ein rundum gut ausgestattetes Gerät. Ein Speicherkarten-Slot, echtes Dual-SIM oder ein spannenderes Design sind das einzige, was man

vermissen könnte. Eine um 150 Euro günstigere Alternative mit ebenso sauberem System ist das OnePlus 6T. Die Kamera ist nicht so gut wie beim Pixel 3, dafür sind die Laufzeiten etwas länger. In derselben Preisklasse wirbt das Honor View 20 um Kunden – dank „Lochkamera“ mit extravaganter Optik, aber mit nicht

ganz so brilliantem Display und kürzeren Laufzeiten. In Sachen Kamera nehmen sich das Honor und das OnePlus nichts.

Mit nicht ganz so guter Software, aber dafür mit All-Inclusive-Hardware-Paket kommt das Samsung Galaxy Note 9. Abgesehen von Samsungs (dezentem) Android-Anstrich ist es uneingeschränkt für

High-End-Smartphones

Modell	Apple iPhone Xs Max	Google Pixel 3 XL	Honor View 20
Ausstattung			
Betriebssystem / Bedienoberfläche	iOS 12.1.3 / –	Android 9.0 / –	Android 9.0 / Magic 2.0.1
Android-Sicherheitspatch-Ebene	–	Jan 19	Jan 19
Prozessor / Kerne	Apple A12 Bionic / 2 × 2,5 GHz, 4 × 1,59 MHz	Qualcomm Snapdragon 845 / 4 × 2,8 GHz, 4 × 1,8 GHz	Huawei Kirin 980 / 2 × 2,6 GHz, 2 × 1,9 GHz, 4 × 1,8 GHz
Grafik	Apple A12 Bionic	Qualcomm Adreno 630	ARM Mali-G76
Arbeitsspeicher / Flash-Speicher (frei)	4 GByte / 64 GByte (52 GByte)	4 GByte / 64 GByte (53 GByte)	8 GByte / 256 GByte (238,2 GByte)
Wechselspeicher	–	–	–
WLAN / Dual-Band	WiFi 5 / ✓	WiFi 5 / ✓	WiFi 5 / ✓
Bluetooth / NFC / Standortbestimmung	5.0 / nur Apple Pay / GPS, Glonass, Galileo	5.0 / ✓ / GPS, Glonass, Beidou, Galileo	5.0 (aptX HD) / ✓ / GPS, Glonass, Beidou, Galileo
Fingerabdrucksensor	–	✓	✓
Kopfhörerbuchse	–	–	✓
mobile Datenverbindung ¹	LTE Cat. 16 / 13 (1000 MBit/s Down, 150 MBit/s Up), HSPA	LTE Cat. 16 (1000 MBit/s Down, 75 MBit/s Up), HSPA	LTE Cat. 13 (400 MBit/s Down, 150 MBit/s up), HSPA
Dual-SIM / Hybrid-Slot / e-SIM-fähig	– / – / ✓	– / – / ✓	✓ / – / –
Akku / austauschbar / drahtlos ladbar	3174 mAh / – / ✓	3430 mAh / – / ✓	4000 mAh / – / –
USB-Anschluss / OTG / DisplayPort	Lightning / – / –	Typ-C (USB 3.1) / ✓ / –	USB Typ-C (3.1) / ✓ / ✓ (USB-C)
Schnellladetechnik	proprietär ²	✓	✓
Abmessungen (H × B × T)	13,5 cm × 6,5 cm × 1,2 cm	15,8 cm × 7,7 cm × 0,8 cm	15,7 cm × 7,5 cm × 0,9 cm
Gewicht	208 g	184 g	185 g
Schutzart	IP68	IP68	–
Farbvarianten	Silber, Grau, Gold	Weiß, Schwarz, Rosa	Blau, Schwarz, Rot
Kamera-Tests			
Hauptkamera Auflösung / Blende / OIS	12,2 MP / f/1,8 / ✓	12,2 MP / f/1,8 / ✓	48 MP / f/1,8 / –
Hauptkamera Videos 4K / Full-HD	60 fps / 60 fps	30 fps / 30 fps	30 fps / 60 fps
Zweitkamera Auflösung / Blende / OIS	12,2 MP / f/2,4 / ✓ (Zweifachtele)	–	k. A.
Frontkamera Auflösung Fotos / Video	7,2 MP / FullHD	8 MP / FullHD	24,8 MP / FullHD+
Display-Messungen			
Technik	OLED (AMOLED)	OLED (AMOLED)	LCD (IPS)
Diagonale / Größe	6,5 Zoll / 14,9 cm × 6,9 cm	6,3 Zoll / 14,4 cm × 7 cm	6,4 Zoll / 14,7 cm × 6,9 cm
Auflösung (Pixeldichte)	2688 × 1242 Pixel (458 dpi)	2960 × 1440 Pixel (522 dpi)	2310 × 1080 Pixel (399 dpi)
Helligkeitsregelbereich / Ausleuchtung	4 ... 648 cd/m² / 92 %	2 ... 388 cd/m² / 94 %	0,9 ... 348 cd/m² / 93 %
Kontrast / Farbraum	> 10.000:1 / DCI-P3	> 10.000:1 / AdobeRGB	1039:1 / über sRGB
Bewertung			
Bedienung / Performance	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕
Ausstattung Software / Hardware	⊕⊕ / ⊕	⊕⊕ / ⊕	⊕ / ⊕
Display	⊕⊕	⊕	○
Laufzeit	⊕	⊕	⊕
Kamera Fotos / Videos	⊕ / ⊕⊕	⊕⊕ / ⊕	⊕ / ○
Preis	1150 € (64 GByte), 1300 € (256 GByte), 1500 € (512 GByte)	700 € (64 GByte), 900 € (128 GByte)	570 € (6 / 128 GByte), 650 € (8 / 256 GByte)

¹ Herstellerangaben ² Schnellladeteil nicht im Lieferumfang ³ Drittkamera mit Ultra-Weitwinkel 20 MP / f/2,2
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht

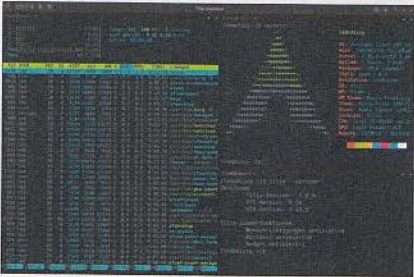
fast jeden zu empfehlen. Der S-Pen ist ein weiterer Pluspunkt, der einem schnell ans Herz wächst. Wer die passende Kamera für jede Situation immer dabei haben möchte, trifft mit dem Huawei Mate 20 Pro die beste Wahl. So vielseitig wie mit der Triple-Kamera mit Weitwinkel und und Dreifachtele ist die Fotografie mit kei-

nem anderen High-End-Smartphone. Es stört vor allem die penetrante Anbietung von Huawei-Clouddiensten. Ein Alleinstellungsmerkmal wie Kamera oder Software fehlt dem Sony Xperia XZ3, doch grundsätzlich ist es ein gutes Gerät. Soll es möglichst preiswert werden, ist das LG G7 ThinQ die erste Wahl. Für unter

400 Euro bekommt man hier Hardware, die mit den anderen Kandidaten zumindest mithalten kann. Einige Kompromisse muss man eingehen: LCD statt OLED, nicht die beste Kamera und vom Hersteller verändertes Android. Aber: Für den Preis einiger Konkurrenten kann man sich gleich zwei G7 zulegen. (hcz@ct.de) **ct**

Huawei Mate 20 Pro	LG G7 ThinQ	OnePlus 6T	Samsung Galaxy Note 9	Sony Xperia XZ3
Android 9.0 / EMUI 9.0	Android 8.0 / LG UX	Android 9.0 / Oxygen OS	Android 9.0 / One UI	Android 9.0 / Sony
Dez 18	Nov 18	Dez 18	Jan 19	Jan 19
Huawei Kirin 980 / 2 × 2,6 GHz, 2 × 1,9 GHz, 4 × 1,8 GHz	Qualcomm Snapdragon 845 / 4 × 2,8 GHz, 4 × 1,8 GHz	Qualcomm Snapdragon 845 / 4 × 2,8 GHz, 4 × 1,8 GHz	Samsung Exynos 9 Octa / 4 × 2,7 GHz, 4 × 1,8 GHz	Qualcomm Snapdragon 845 / 4 × 2,8 GHz, 4 × 1,8 GHz
ARM Mali-G76	Qualcomm Adreno 630	Qualcomm Adreno 630	ARM Mali-G72	Qualcomm Adreno 630
6 GByte / 128 GByte (103,7 GByte)	4 GByte / 64 GByte (47,8 GByte)	8 GByte / 128 GByte (108 GByte)	8 GByte / 128 GByte (108 GByte)	4 GByte / 64 GByte (41 GByte)
NM-Card	MicroSDXC	—	MicroSDXC	MicroSDXC
WiFi 5 / ✓	WiFi 5 / ✓	WiFi 5 / ✓	WiFi 5 / ✓	WiFi 5 / ✓
5.0 (aptX HD) / GPS, Glonass, Beidou, Galileo	5.0 (aptX HD) / ✓ / GPS, Glonass, Beidou, Galileo	5.0 (aptX HD) / ✓ / GPS, Glonass, Beidou, Galileo	5.0 / ✓ / GPS, Glonass, Beidou	5.0 (aptX) / ✓ / GPS, Glonass, Beidou, Galileo
✓	✓	✓	✓	✓
—	✓	—	✓	—
LTE Cat. 21 (1400 MBit/s Down, 200 MBit/s Up), HSPA	LTE Cat 18/13 (1200 MBit/s Down / 150 MBit/s Up), HSPA	LTE Cat. 16/13 (1000 MBit/s Down, 150 MBit/s Up), HSPA	LTE Cat. 18 (1200 MBit/s Down, 150 MBit/s Up), HSPA	LTE Cat. 18 (1200 MBit/s Down, 150 MBit/s Up), HSPA
✓ / ✓ / —	— / — / —	✓ / — / —	✓ / ✓ / —	✓ / ✓ / —
4200 mAh / — / ✓	3000 mAh / — / ✓	3700 mAh / — / —	4000 mAh / — / ✓	3330 mAh / — / ✓
Typ-C (USB 3.1) / ✓ / ✓ (USB-C)	Typ-C (USB 2.0) / ✓ / —	Typ-C (USB 2.0) / ✓ / —	Typ-C (USB 3.1) / ✓ / ✓ (USB-C)	Typ-C (USB 3.1) / ✓ / —
✓	✓	✓	✓	✓
15,7 cm × 7,2 cm × 0,9 cm	15,2 cm × 7,1 cm × 0,9 cm	15,8 cm × 7,5 cm × 0,8 cm	16,2 cm × 7,6 cm × 0,9 cm	15,8 cm × 7,4 cm × 0,9 cm
190 g	160 g	183 g	200 g	194 g
IP68	IP68	—	IP68	IP65/68
Schwarz, Blau, Grün, Violett	Schwarz, Grau	Mattschwarz, Glänzenschwarz	Schwarz, Blau, Rosa, Kupfer	Rot, Grün, Weiß, Schwarz
39,9 MP / f/1,8 / ✓	16,3 MP / f/1,6 / ✓	15,9 MP / f/1,7 / ✓	12,2 MP / f/1,5 + 2,4 / ✓	19,2 MP / f/2 / —
30 fps / 60 fps	60 fps / 60 fps	60 fps / 60 fps	60 fps / 60 fps	30 fps / 60 fps
10 MP / f/2,4 / — (Dreifachtele) ³	16,3 MP / f/1,9 / — (Weitwinkel)	20 MP / f/1,7 / —	12,2 MP / f/2,4 / (Zweifachtele)	—
23,8 MP / FullHD+	8 MP / FullHD	15,9 MP / FullHD	8 MP / 2K	13 MP / FullHD
OLED (AMOLED)	LCD (IPS)	OLED (AMOLED)	OLED (AMOLED)	OLED (AMOLED)
6,3 Zoll / 14,7 cm × 6,7 cm	6,1 Zoll / 14 cm × 6,5 cm	6,4 Zoll / 14,7 cm × 6,8 cm	6,4 Zoll / 14,6 cm × 7,1 cm	6 Zoll / 13,6 cm × 6,8 cm
3120 × 1440 Pixel (541 dpi)	3120 × 1440 Pixel (566 dpi)	2340 × 1080 Pixel (404 dpi)	2960 × 1440 Pixel (516 dpi)	2880 × 1440 Pixel (538 dpi)
1,7 ... 676 cd/m² / 93 %	3,8 ... 708 cd/m² / 88 %	1,7 ... 445 cd/m² / 89 %	2 ... 712 cd/m² / 96 %	2 ... 750 cd/m² / 100 %
> 10.000:1 / AdobeRGB	2472:1 / über sRGB	> 10.000:1 / AdobeRGB	> 10.000:1 / AdobeRGB	> 10.000:1 / AdobeRGB
⊕ ⊕ / ⊕ ⊕	⊕ ⊕ / ⊕ ⊕	⊕ ⊕ / ⊕ ⊕	⊕ ⊕ / ⊕ ⊕	⊕ ⊕ / ⊕ ⊕
⊕ / ⊕ ⊕	○ / ⊕	⊕ ⊕ / ⊕	⊕ / ⊕ ⊕	⊕ / ⊕
⊕ ⊕	⊕	⊕	⊕ ⊕	⊕ ⊕
⊕ ⊕	○	⊕ ⊕	⊕ ⊕	⊕
⊕ ⊕ / ⊕	○ / ○	⊕ / ⊕	⊕ ⊕ / ⊕	⊕ / ⊕
800 €	400 €	549 € (6 / 128 GByte), 579 € (8 / 128 GByte), 629 € (8 / 256 GByte)	800 €	700 €

✓ vorhanden — nicht vorhanden k. A. keine Angabe



Konsolen-kacheln

Das Linux-Programm Tilix erleichtert die Arbeit mit vielen parallel geöffneten Terminals, indem es sie in einem Fenster ganz nach Wunsch anordnet.

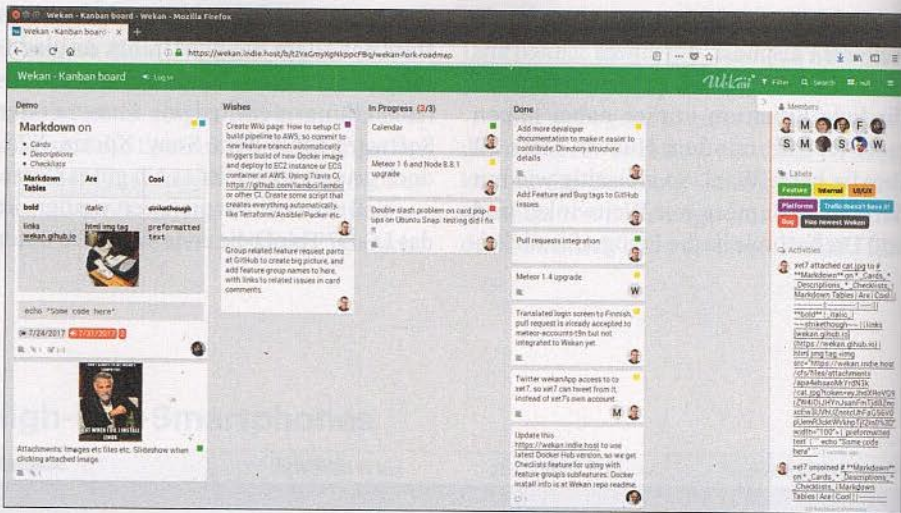
Das Tilix-Programmfenster nimmt beliebig viele Terminals auf – per Tastendruck oder Klick fügt man horizontal oder vertikal weitere ein. Wird das Fenster zu voll, legt man eine neue Session an, die Tilix in einer ausklappbaren Seitenleiste verwaltet. Per Drag & Drop lassen sich Terminals beliebig anordnen.

Den Titel eines Terminals legt man mit Platzhaltern und Text selbst fest. Auch Schrift, Transparenz, Hintergrundbild und einiges mehr lassen sich anpassen und in einem Profil speichern. Tilix kann anhand definierter Bedingungen automatisch zu einem anderen Profil wechseln. So können andere Farben signalisieren, dass man als root arbeitet – und entsprechend Vorsicht walten lassen sollte. Die Fensteraufteilung kann als JSON-Datei gesichert und bei Bedarf wieder geladen werden.

Den aus dem gleichnamigen Spiel bekannten Quake-Modus beherrscht Tilix ebenfalls. Per Tastendruck klappt dann eine Konsole vom Fensterrand aus auf. Dazu legt man den Aufruf von `tilix --quake` auf ein Tastenkürzel. Sollen in zwei Terminals dieselben Eingaben vorgenommen werden, kann Tilix die Eingabe synchronisieren. Für häufig verwendete Verzeichnisse lassen sich Lesezeichen anlegen. (lmd@ct.de)

Tilix 1.8.9

Tiling Terminal Emulator	
Hersteller	Gerald Nunn, https://gnunn1.github.io/tilix-web/
Systemanf.	Linux
Preis	kostenlos



Online-Pinnwand

Kanban-Boards sind ein beliebtes Werkzeug, um die Arbeit von kleinen und mittleren Teams zu organisieren. Mit Wekan kann man ein solches Board selbst betreiben.

Klassische Kanban-Boards bestehen aus einer Wand, an der man Notizzettel mit Klebestreifen befestigt. Je nach Projekt gruppiert man diese in Spalten wie „in Bearbeitung“, „dringend“ oder „erledigt“. Arbeitet das Team nicht ständig im gleichen Raum, gibt es digitale Kanban-Boards, die das Grundprinzip der Klebezettel nachbilden und um nützliche Funktionen erweitern: Benachrichtigungen per Mail, Ablaufdaten und Kommentarfunktionen. Der Markt für solche Cloud-basierten Angebote ist groß.

Wer die Geheimnisse des Projekts nicht einem Cloud-Anbieter anvertrauen und pro Benutzer bezahlen möchte, kann auf das Open-Source-Programm Wekan setzen. Die Webanwendung ist auf dem eigenen Linux-Server schnell installiert oder noch bequemer als Docker-Container gestartet und bietet viele Funktionen, die man anderswo nur in teuren Paketen bekommt. Benutzer können private Boards anlegen, Boards mit anderen teilen, Verantwortliche hinzufügen und Anhänge an Aufgaben anhängen.

Für jede Aufgabe kann man Teilaufgaben in Form eines weiteren Kanban-Boards erzeugen. Wer mit Start-, End- und Fälligkeitsdaten arbeitet, kann in eine Kalenderansicht umschalten und Wekan für die Terminplanung im Team

nutzen. Bisher noch nicht implementiert, aber in Planung, ist eine Anbindung an andere Kalendersysteme oder ein Export als CSV-Datei.

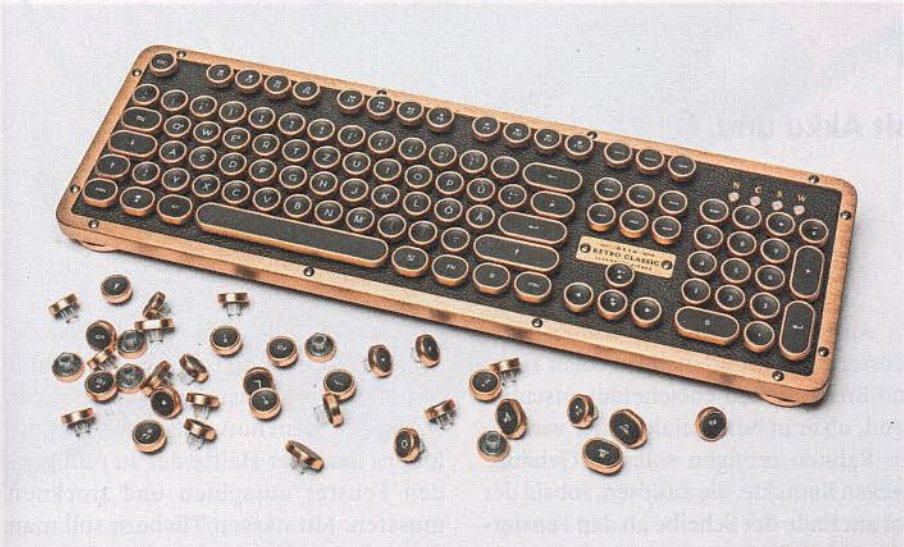
Admins können ein Plug-in nachrüsten und einen LDAP-Server mit Wekan verbinden, um die Benutzeranmeldung zu übernehmen. Auch eine Anbindung an andere Anwendungen über OAuth2 ist möglich. Nutzt man das Board mit mehreren Kollegen, sollte man einen Mailserver angeben, damit Wekan sich per E-Mail melden kann.

Die Oberfläche auf einem großen Bildschirm ist größtenteils selbsterklärend, übersichtlich und auch auf Deutsch übersetzt. Verschiebt ein anderer Benutzer ein Kärtchen, wird die Änderung ohne Reload in Sekunden bei allen anderen übernommen. Etwas fummelig ist die Arbeit auf mobilen Geräten – die Wekan-Entwickler haben die nötigen Optimierungen der Oberfläche schon als Aufgabe auf dem eigenen Kanban-Board.

Wekan ist vor allem interessant für Teams, die in die Arbeit mit Kanban-Boards einsteigen und Wert darauf legen, Kontrolle über die Daten zu behalten. Wer von einer kommerziellen Lösung wie Trello wechselt, wird sicherlich an der einen oder anderen Stelle ein langweiliges Feature vermissen. (jam@ct.de)

Wekan Open-Source Kanban

Kanban-Board zum Selbsthosten	
Anbieter	wekan.github.io
Docker-Image	wekan/wekan
Preis	kostenlos, MIT License



Tippen wie früher

Die Retro Classic von Azio ist eine Bluetooth-Tastatur, die Schreibmaschinen-Gefühl bieten will. Das Gehäuse aus Metall und Leder verleiht ihr einen edlen Look, der aber nur leidlich von einigen Mankos ablenkt.

Ob sie ein Klassiker ist oder – weil alte Schreibmaschinen doch etwas anders aussahen – zum Steampunk zählt, bleibt akademisch, interessierte Blicke zieht die Tastatur allemal auf sich. Es gibt sie in drei Farbvarianten mit Metallrahmen und Lederüberzug; eine Variante mit Holz statt Leder ist derzeit nur mit US-Layout erhältlich. Für 30 Euro weniger gibts ein Modell ohne Bluetooth. Eine kompakte Variante ohne Ziffern- und Cursorblock ist beim Hersteller im US-Layout bestellbar, ebenso eine Maus in ähnlichem Design.

Auch die getestete deutsche Version kann ihre US-Herkunft nicht leugnen, so ist die Enter-Taste quer angeordnet mit darüber liegender Taste für ,/#. Die unterschiedliche Belegung für Windows und macOS löst Azio ungewöhnlich: Ein Satz Austausch-Tastenkappen mit entsprechendem Aufdruck liegt bei, die Kap-

pen zieht man ohne Werkzeug einfach ab. Mit einem Schalter an der Rückseite schaltet man um; ein weiterer Schalter wechselt zwischen USB- und Bluetooth-Verbindung. Für erstere liegt ein USB-C-Kabel bei, über das man auch den Akku lädt. Im Test verschluckte die Bluetooth-Verbindung manchmal kurz ein paar Buchstaben, der Reconnect funktionierte nicht immer zuverlässig.

Die Tastenkappen samt metallfarbener Umrandung sind aus Plastik gefertigt. Sie wirken daher nicht so hochwertig wie der Body; zudem waren bei uns die Fn- und die Leertaste nicht sauber entgratet. Aufgrund der runden Form mit Rahmen und großen Abständen tippt es sich gewöhnungsbedürftig und anfangs fehlerträchtig, auch weil die mittig aufgehängten, hohen Tasten wackeln. Die Kappen – vor allem die breiten – nehmen schnell Fingerfett an, lassen sich aber auch einfach abnehmen und reinigen.

Die Schalter des chinesischen Herstellers Kailh haben einen deutlichen, angenehmen Anschlag und klicken vernehmlich – klingen aber auch nicht mehr nach Schreibmaschine die anderer Tastaturen. Die Beleuchtung ist auch ohne Treiberinstallation einstellbar; sie scheint weiß durch den hohlen Tastenhals, was Streulicht vermeidet.

Die Standfüße halten die fast 1,5 kg schwere Tastatur sicher. Sie ist arg hoch, sodass die Tasten in der niedrigsten Einstellung rund 3,5 Zentimeter über dem Tisch liegen. Hinten kann man die Tastatur mickrige 3 mm höherstellen, was eher unebene Tischplatten ausgleicht als die Tastatur schrägzustellen. Eine Handballenaufgabe fehlt. (jube@ct.de)

Azio Retro Classic BT

Bluetooth-Tastatur im Schreibmaschinen-Look	
Hersteller	Azio, www.aziocorp.com
Verbindungstyp / Stromversorgung	Bluetooth, USB / Li-Ion-Akku (5000 mAh)
Preis	229 € (USB, Bluetooth) / 190 € (USB) / 220 € (kompakt, USB, Bluetooth)

```
<!DOCTYPE html>
<title>Highlight.js im Test</title>

<style>body {width: 500px;}</style>

<script type="application/javascript">
  function $init() {return true;}
</script>
```

Code-Dekorateur

Mit highlight.js werden Code-Blöcke auf Webseiten ansehnlich und lesbar. Die JavaScript-Bibliothek erkennt die verwendete Sprache sogar selbst und orientiert sich an bekannten IDEs.

Unformatierter Programmcode ist nicht leicht zu lesen. Daher sind Programmierer es gewohnt, in einer Entwicklungsumgebung zu arbeiten, die farbliche Akzente setzt – je nach Programmiersprache sind es andere Schlüsselwörter, die sich absetzen müssen. Für sinnvolles Highlighting muss die Syntax der Sprache in der IDE hinterlegt sein.

Wer seinen Code in einem Blog oder in einer Online-Dokumentation vorstellen möchte, bekommt mit der JavaScript-Bibliothek highlight.js gut funktionierende und sinnvolle Hervorhebungen. Einmal in die Webseite eingebunden (in Form einer CSS- und einer JavaScript-Datei), sucht die Bibliothek nach <code>- und <pre>-Blöcken und versucht selbst, die verwendete Sprache zu erkennen.

Wer die Bibliothek in einem Word-Press-Blog einsetzen will, bekommt ein passendes Plug-in. 185 Sprachen kennt die Bibliothek nach eigenen Angaben, eine große und aktive Community kümmert sich um die Pflege. Außerdem bringt highlight.js zahlreiche Stile mit, die das Aussehen aller gängigen IDEs nachahmen. Es gibt sowohl klassische Stile mit hellem Hintergrund als auch solche im modernen dunklen Layout.

(jam@ct.de)

highlight.js

Syntaxhervorhebung für Webseiten	
Anbieter	highlightjs.org
Preis	kostenlos, BSD License

Reinemacher

Fensterputzroboter Winbot X mit Akku und Sicherungsleine

Staubsaugroboter nehmen schon länger einen Teil der lästigen Hausarbeit ab. Fürs Fensterputzen gibt es ebenfalls technische Helfer. Der Winbot X von Ecovacs wischt Scheiben automatisch feucht, braucht aber mehr Unterstützung als ein Saugroboter.

Von Stefan Porteck

Ähnlich wie ein Staubsaugroboter hat auch der Winbot X eine Saugeinheit. Sie entfernt aber keinen Schmutz, sondern erzeugt den nötigen Unterdruck, mit dem sich der Bot am Fenster festsaugt. Zum Vorwärtsschreiten nutzt er zwei Gummiringe, die ihn wie einen Kettenantrieb übers Fenster schieben. Das klappte in unseren Tests zuverlässig – selbst an schrägen Dachfenstern.

Obwohl sich der Winbot X fest an die Scheiben ansaugt, funktioniert er nur mit einer mechanischen Sicherung – das Risiko, dass er beim Ausfall des Gebläses oder bei leerem Akku mehrere Stockwerke in die Tiefe fällt und Passanten trifft, ist einfach zu hoch.

Als Sicherung dient ein kleiner Puck mit einem Durchmesser von etwa zehn Zentimetern. Er besteht aus einem Saugnapf, mit dem er am Fenster befestigt wird und einem ausziehbaren Sicherungsseil (2,7 Meter), das man am Winbot arretiert. Um das jeweilige Fenster vollständig zu putzen, lässt sich der Puck bei der Innenreinigung außen anbringen und umgekehrt. Der Puck hat einen Unterdrucksensor und überwacht so seinen festen Sitz. Seine Elektronik wird von zwei AAA-Batterien versorgt. Trotz der Sicherung rät Ecovacs vom Überkopfbetrieb ab.

Das Aufsetzen und Starten des Winbot X klingt zunächst kompliziert, doch die Handgriffe gehen einem schnell in Fleisch und Blut über: Puck einschalten und an die Scheibe drücken – Sicherungsseil herausziehen und im Bot arretieren – den Bot einschalten und auf die Scheibe setzen.

Anschließend fährt der Winbot X das Fenster zunächst einmalig in voller Höhe und Breite ab und entscheidet anschließend, ob er in horizontalen oder vertikalen Bahnen reinigen soll. Im Gehäuse stecken Kontakte, die auslösen, sobald der Bot am Ende der Scheibe an den Fensterrahmen stößt. In unseren Tests klappte das problemlos: Alle Bereiche des Fensters wurden mindestens ein Mal überfahren. Ungereinigt blieb bauartbedingt lediglich ein rund drei Millimeter breiter Bereich direkt am Fensterrahmen.

Für die sichere Navigation auf dem Fenster muss der Fensterrahmen laut Ecovacs eine Stärke von mindestens vier Millimetern haben. Das sollte man vor dem Kauf ausmessen, denn falls der Bot auf den Rahmen fährt, kann er mangels Unterdruck abstürzen. Milchglasscheiben, Riffelungen und Aufkleber sollen dagegen kein Problem darstellen.

Nicht ohne Handarbeit

Die eigentliche Reinigung der Scheiben erfolgt passiv. Den Schmutz nimmt der Winbot X ausschließlich mit einem Mopp an seiner Unterseite auf. Vor jeder Reinigung muss man deshalb eines der vier Reinigungstücher mit einigen Sprühdüsen des mitgelieferten Putzmittels benetzen und es anschließend per Klettverschluss an der Unterseite des Bots befestigen.

Die Bedienungsanleitung schweigt sich aber über die passende Menge an Reinigungslösung aus – falls es sie überhaupt gibt: Uns gelang es in etlichen Versuchen nicht, die optimale Menge zu ermitteln. Bei zu trockenem Tuch blieben gröbere oder eingetrocknete Verschmutzungen auf dem Fenster zurück. Befeuchteten wir das Tuch zu stark, zeigten sich Schlieren. Unabhängig davon benötigten wir bei stark verschmutzten Fenstern oft einen zweiten Durchgang mit einem frischen Reinigungstuch. Doch auch danach konnte das Ergebnis nicht mit händischem Fensterputzen und anschließendem Abledern mithalten – was sich spätestens zeigte, wenn Sonne aufs Fenster schien.

Der Akku des Winbot X reicht für etwa 50 Minuten Betrieb bei drei bis fünf Minuten pro Fenster. Zwangspausen waren trotzdem notwendig, weil wir die Mopps nach der Hälfte der zu reinigenden Fenster ausspülen und trocknen mussten. Mit nassen Tüchern soll man den Winbot laut Anleitung nicht betreiben, weil er ins Rutschen kommen und herunterfallen kann. Wer in einem Rutsch putzen will, muss weitere Tücher für fünf bis zehn Euro pro Stück (je nach Anbieter und Menge) nachkaufen. Eine Sprühflasche des Winbot-Glasreinigers schlägt mit fünf Euro zu Buche. Auch hier empfiehlt Ecovacs keinen beliebigen Reiniger zu nutzen und begründet das mit einer Beeinträchtigung der Reinigungswirkung und dem sicheren Betrieb auf der Scheibe.

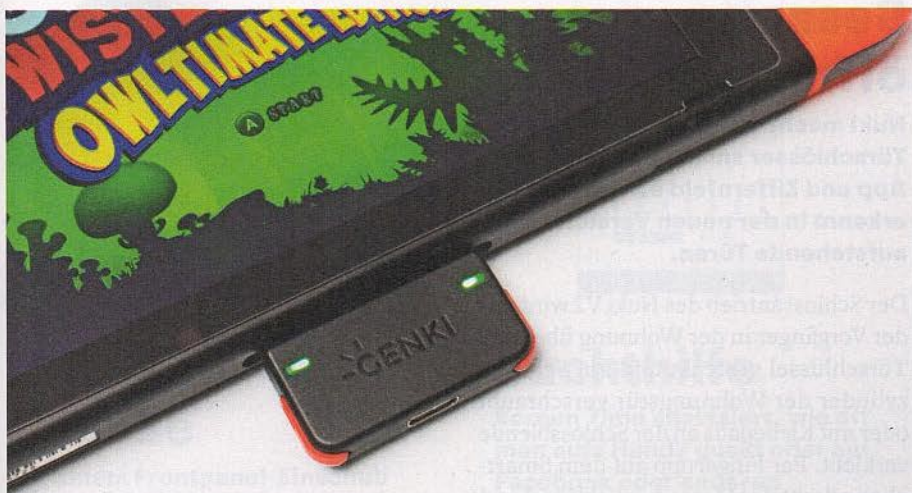
Fazit

An die Geschwindigkeit und das streifenfreie Ergebnis herkömmlichen Fensterputzens kommt der Winbot X nicht heran. Im Vergleich zu anderen technischen Helfern wie Dampfreinigern ist er vergleichsweise teuer.

Er eignet sich somit eher für Nutzer mit sehr vielen Fensterflächen oder Wintergärten. Auch bei schlecht erreichbaren Fensterflächen, nicht zu öffnenden Bereichen oder sehr hohen Oberlichtern empfanden wir den Winbot X hilfreich – und dort stört die manchmal etwas schwache Reinigungsleistung nicht so. (spo@ct.de) **ct**

Ecovacs Winbot X

Fensterputzroboter	
Hersteller	Ecovacs, www.ecovacs.de
Länge, Breite, Höhe	24 cm, 24 cm, 11 cm
Gewicht	1,8 kg
Lautstärke	74 db(A)
Laufzeit	ca. 50 min
Lieferumfang	IR-Fernbedienung, Poliertuch, 4 × Reinigungstücher, Sicherungsadapter, Reinigungsmittel (230 ml)
Preis	400 €



Von der Leine gelassen

Bluetooth-Audio-Adapter für Nintendo Switch

Nintendos Spielkonsole bindet über Bluetooth zwar Controller an, aber keine drahtlosen Kopfhörer. Ein USB-C-Adapter schafft hier Abhilfe und kann sogar zwei Empfänger gleichzeitig und latenzfrei mit Spielesound beliefern.

Von Nico Juran

Als das US-Start-up Human Things im Sommer 2018 seine Kickstarter-Kampagne für einen universellen Bluetooth-Audio-Dongle namens „Genki“ zum Anstecken am USB-C-Port der Nintendo Switch startete, dürfte kaum jemand geahnt haben, welchen Nerv es damit trifft: Die erhofften 30.000 US-Dollar kamen in zwei Stunden zusammen, bis heute wuchs die Summe auf knapp 1,5 Millionen Dollar an.

Mittlerweile lässt sich Genki regulär kaufen – einzeln aktuell für 39 US-Dollar (später angepeilter Verkaufspreis 50 US-Dollar) und im „Combo“-Set mit weiterem Zubehör für 59 (statt 80) US-Dollar. Hinzu kommen jeweils 5 Dollar Versandkosten und eventuell Zollgebühren.

Beim Auspacken gab es die ersten positiven Überraschungen: Zum einen passen Design und hohe Verarbeitungsqualität gut zur Nintendo Konsole, zum anderen kommt das komplette Set in einer

Hülle, in der sonst Switch-Spiele ausgeliefert werden. So gehen die Kleinteile nicht so leicht verloren und die besagte Hülle bietet noch Platz für vier Gamecards.

Bessere Alternative

Im Unterschied zu anderen Bluetooth-Adaptoren, die man in die Kopfhörerbuchse der Switch steckt, läuft Genki ohne Akku und muss folglich nicht aufgeladen werden. Stattdessen bedient sich der Dongle am Akku der Konsole, benötigt dabei laut Entwickler aber weniger Leistung als die Lautsprecher der Switch. Tatsächlich konnten wir beim Einsatz des Genki keine negativen Auswirkungen auf die Laufzeit der Konsole feststellen. Die USB-C-Buchse der Konsole wird durchgeschleift, die Switch lässt sich also weiter aufladen.



Nutzt man den Dongle (Mitte) häufig stationär, sind der USB-Adapter und das Mikrofon (rechts) nützlich.

Im Combo-Set ist noch ein Adapter von USB-A auf USB-C enthalten, der die Nutzung des Genki am Dock der Switch erlaubt, sodass man auch im stationären Betrieb Bluetooth-Kopfhörer und -Lautsprecher nutzen kann. Weiterhin liegt ein Mikrofon bei, das sich in die frei bleibende Kopfhörerbuchse stecken lässt, um über die Voice-Chat-Funktion von Titeln wie Fortnite mit anderen Spielern zu sprechen. Unklar bleibt, warum Genki nicht einfach Bluetooth-Headsets unterstützt.

Abgerundet wird das Paket durch einen zusammenfaltbaren Ministänder, der die Switch mit Dongle hält.

Der Genki wird von der Switch als Bluetooth-Audio-Gerät erkannt, sodass sich die Lautstärke über die Volume-Tasten an der Konsole regulieren lässt. Die Kopplung mit Bluetooth-Lautsprechern und -Kopfhörern lief im Test problemlos, dank Unterstützung von Bluetooth 5.0 auch mit neueren Geräten wie Apples AirPods. LEDs am Genki zeigen an, welche der beiden Funkverbindungen man gerade nutzt.

Die wahre Stärke des Genki ist seine Unterstützung des Audio-Codec aptX-LL (Low Latency). An passenden Kopfhörern und Wireless-Audio-Empfängern übertragen wir so Spielesound ohne spürbare Latenz. Auch der Ton von YouTube-Videos lief lippensynchron. Die gleichzeitige Audio-Übertragung an zwei Kopfhörer funktionierte; unterstützte davon nur einer aptX-LL, traten aber schon mal leichte Asynchronitäten auf.

Alles in allem ist das Genki eine gelungene Lösung. Ein Wermutstropfen ist das Fehlen eines CE-Zeichens und einer deutschen Bedienungsanleitung, die nach Rückmeldungen von Unterstützern schon dazu führten, dass der Zoll den Import nach Deutschland unterbunden hat.

(nij@ct.de) **ct**

Genki

Bluetooth-Audio-Dongle für Nintendo Switch	
Hersteller	Human Things, https://www.humanthings.co/
Funk	Bluetooth 5.0
Audio-Codex	aptX-LL, aptX, AAC, SBC
Reichweite	ca. 20 m
Leistungsaufnahme laut Hersteller	25 mW
Maße	38 mm × 20,3 mm × 7,7 mm (B × H × T)
Preis	39 / 59 US-\$, jeweils plus 5 US-\$ Versand und eventuell Zollgebühren

SMARTE FLEDERMAUS-LEUCHE



**ODER
AUTONOME DROHNE?**

Neugierig geworden?

Testen Sie jetzt 3 Ausgaben
Technology Review und sparen
Sie über 9 Euro.

Lesen, was wirklich zählt in
Digitalisierung, Energie, Mobilität,
Biotech.



Bestellen Sie jetzt unter
trvorteil.de/3xtesten

trvorteil.de/3xtesten

+49 541/80 009 120

leserservice@heise.de

**Technology
Review**
DAS MAGAZIN FÜR INNOVATION

Sesam, öffne dich

**Nuki macht bestehende
Türschlösser smart, lässt sich per
App und Ziffernfeld öffnen und
erkennt in der neuen Version
aufstehende Türen.**

Der Schlossantrieb des Nuki V2 wird wie der Vorgänger in der Wohnung über den Türschlüssel gesteckt und am Schließzylinder der Wohnungstür verschraubt oder mit Klebepads an der Schlossblende verklebt. Per Fingertipp auf dem Smartphone dreht der Motor den Schlüssel und automatisiert so das Auf- und Zuschließen der Haustür.

Dank dieser Funktionsweise ist Nuki mit nahezu allen Haustüren kompatibel. Aus Sicherheitsgründen empfiehlt es sich aber, ein paar Euro in einen Schließzylinder mit Not- und Gefahrenfunktion zu investieren, der sich von außen aufschließen lässt, obwohl innen ein Schlüssel steckt. Das erspart bei leeren Batterien oder einem Defekt des Nuki einen teuren Schlüsseldienst.

Optisch gleicht Nuki 2 dem vorherigen Modell. Die solide Mechanik öffnet und schließt zuverlässig und im Vergleich zu anderen Motorschlössern recht flott und mit moderatem Geräuschpegel. Außer Google Assistant und Alexa unterstützt Nuki nun auch Apples Smart-Home-Standard HomeKit.

Eine sinnvolle und von vielen Nutzern gewünschte Neuerung ist der mitgelieferte Magnet, der neben dem Schloss an den Türrahmen geklebt wird. Dadurch erkennt das Schloss, ob die Tür offen oder zugezogen ist und schließt beispielsweise auf Wunsch automatisch ab, sobald man die Tür zuzieht. Zudem zeigt die App nun außer dem Zustand des Schlosses auch den der Tür an und warnt, wenn man versucht, eine offen stehende Tür abzuschließen.

Als Zubehör für das neue und das alte Nuki-Schloss ist das Nuki Pad erhältlich. Das kleine Tasten-Pad öffnet die Tür per Code-Eingabe. Es ist etwas größer als ein Feuerzeug und wird mit einer Knopfzelle betrieben und soll damit laut Hersteller ein Jahr laufen.

Die gummierte Oberfläche soll ein Eindringen von Wasser und Staub verhindern (IP65). Das Keypad wird mit Klebestreifen oder Schrauben außen an der Tür oder dem Rahmen montiert.



Nach Eingabe eines sechsstelligen Codes sendet es via Bluetooth den Befehl zum Öffnen ans Nuki-Schloss. Dafür müssen Pad und Schloss zunächst einmalig in der Nuki-App auf dem Smartphone gekoppelt werden. Während der intuitiven Einrichtung lässt sich der gewünschte Entsperrcode festlegen.

In unseren Tests ließ sich die Tür stets zuverlässig per Codeeingabe öffnen. Zur Sicherheit nimmt das Pad nach jedem falschen Code für eine wachsende Zeitspanne keine weiteren Eingaben mehr an, ein Brute-Force-Angriff dauert laut Hersteller über ein Jahr. Praktisch: Wer Verwandten, Besuchern oder Putzkräften einen temporären Zugang zur Wohnung verschaffen will, legt dafür verschiedene Codes an und kann diese in der Gültigkeit beschränken oder an gewünschte Zeitfenster koppeln. Ein weiterer Vorteil für Familien: Statt verlorene Schlüssel nachzukaufen, bekommt der Nachwuchs Öffnungscodes zum Nulltarif.

Damit stellt das Keypad für viele Nuki-Besitzer eine praktische Ergänzung dar. Das Schloss selbst wartet in der zweiten Generation mit sinnvollen Verbesserungen auf und hinterlässt wie der Vorgänger einen guten Eindruck. (spo@ct.de)

Nuki 2 und Keypad

Smartes Türschloss	
Systemanf.	Smartphone mit Android ≥ 4.4 oder iOS ≥ 9.2
Abmessungen	110 mm × 60 mm × 60 mm (L × B × H)
Batterien	4 × AA
Straßenpreis	230 €
Keypad	
Abmessungen	85 mm × 25 mm × 12 mm (L × B × H)
Batterien	1 × CR2032
Straßenpreis	80 €



Schnelle Buchse

Mit einem Frontpanel-Einschub lässt sich bei PC-Gehäusen die verdrehsichere USB-C-Buchse für Smartphones, Speichersticks und externe SSDs nachrüsten.

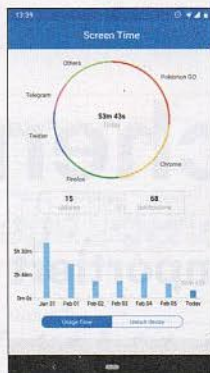
Viele Mainboards für Core-i- und Ryzen-Prozessoren sind bereits mit USB 3.1 Gen 2 (SuperSpeedPlus) ausgestattet, das Peripheriegeräte mit bis zu 10 GBit/s anbindet. Immer mehr Boards stellen das schnelle USB auch für Typ-C-Frontanschlüsse über einen internen, geschirmten, 20-poligen Anschluss zur Verfügung. PC-Gehäuse mit USB-C sind aber noch selten.

Inline bietet deshalb für 3,5"-Laufwerksschächte eine Blende an, die eine Typ-C-Buchse sowie zwei USB-A-Anschlüsse bereitstellt. Wir haben die Geschwindigkeit mit dem M.2-USB-C-Adapter LM902 und einer Samsung SSD 960 Pro getestet. Damit konnten wir an unserem Bauvorschlag Intel-Allrounder aus c't 26/2018 am Typ-C-Boardanschluss die für USB 3.1 Gen 2 maximal mögliche Geschwindigkeit von knapp über 1 GByte/s erreichen. Bei USB 3.0 (Typ A) waren es 460 MByte/s.

Das Frontpanel von Inline rüstet für 25 Euro moderne USB-Buchsen bei PC-Gehäusen nach. Bei diesem Preis sollte aus unserer Sicht aber ein Adapter für 5,25"-Schächte dabei sein, denn vielen Gehäusen fehlt eine von außen zugängliche 3,5"-Einbauposition. (chh@ct.de)

Inline Frontpanel (33394p)

Frontpanel mit Typ-C-Buchse für USB 3.1 Gen 2	
Hersteller	Inline, www.inline-info.com
Frontanschlüsse	1x USB C, 2x USB A
Interner Anschluss	1 x 20 polig (USB C), 1 x 19 polig (2x USB A)
Preis	25 €



Suchthilfe

Screen Time analysiert, wie oft man aufs Handy guckt oder auf Facebook oder anderen Zeitfressern herumdadelt.

Gerade werbefinanzierte Apps sind auf maximales Suchtverhalten getrimmt, im Silicon-Valley zynisch „stickiness“ genannt. Obwohl selbst nicht ganz unschuldig, bieten Apple und Google seit iOS 12 und Android 9 Bordmittel gegen das Klebrigkeits-Problem an – zur Selbsttherapie oder um den Nachwuchs zu beaufsichtigen.

Das aktuelle Android 9 gibt es zurzeit nur für wenig Smartphones. Die App „Screen Time – Phone Usage Tracker“ bildet die „Wellbeing“-Funktion auch auf älteren Android-Version nach. Sie schlüsselt übersichtlich auf, welche Apps man wie lange benutzt und wie oft man über den Tag das Handy entsperrt hat. Außerdem kann man Zeitlimits für einzelne Apps festlegen (etwa maximal 30 Minuten am Tag für Facebook) und Auszeiten einstellen. In einer Auszeit lassen sich nur bestimmte Apps nutzen. Startet man eine blockierte Software, poppt ein Warnhinweis auf. Das funktionierte im Test zuverlässig als Selbstkontroll-Hilfe. Besonders clever: Man kann jedwede Einstellungsänderung mit Fingerabdruck oder Wischmuster schützen. Wer der App vertraut und ihr den Zugriff auf Benachrichtigungen erlaubt, kann auch diese tracken lassen. Screen Time nervt in der kostenlosen Version mit Werbung, die Vollversion kostet 1,99 Euro. Eine deutsche Version gibt es (noch) nicht. (jkj@ct.de)

Screen Time

Nutzungskontroll-App	
Hersteller	Agooday
System	Android ab 5.0
Laufzeit	1 Jahr (Herstellerangabe)
Preis	1,99 €



M. Sc. Internet-Sicherheit

Ein innovativer, zukunftsorientierter und praxisnaher Masterstudiengang am Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen.

Lernen in Forschungsprojekten
Profitieren von Kontakten zur Wirtschaft
Förderung der persönlichen Weiterentwicklung

Mitarbeit an Themen von morgen
Hervorragendes offenes Arbeitsklima
Hohe Reputation des Instituts

Ausgezeichnete Jobperspektiven
Ideale Promotionsmöglichkeiten am Institut
Optimale Grundlage für Startups



Jetzt bewerben unter:
it-sicherheit.de/master

Hörbare Zeichen

Gratis-Notensatzsoftware importiert PDF-Noten

Statt mit Bleistift und liniertem Papier schreibt man Noten mit einem leistungsstarken Gratis-Programm: MuseScore bietet dem Musiker einen großen Funktionsumfang – einschließlich PDF-Import und Positionsautomatik.

Von Dr. Justus Noll

Nach vier Jahren Entwicklung traf am Heiligen Abend 2018 endlich die Nachricht ein, dass eine neue Ausgabe des freien Notensatzprogramms MuseScore auf dem digitalen Gabentisch der Fan-Gemeinde liegt. Die Version 3 bringt ein lang erwartetes Killerfeature mit: Musikalische Zeichen erscheinen nun kollisionsfrei auf dem virtuellen Notenpapier (Autoplace-ment); dabei folgten die Entwickler möglichst dicht den Regeln des historischen,

professionellen Notenstichs. Mit dieser Funktion war die größte Hürde überwunden, um MuseScore in die Oberklasse der Notensetzer einzuordnen.

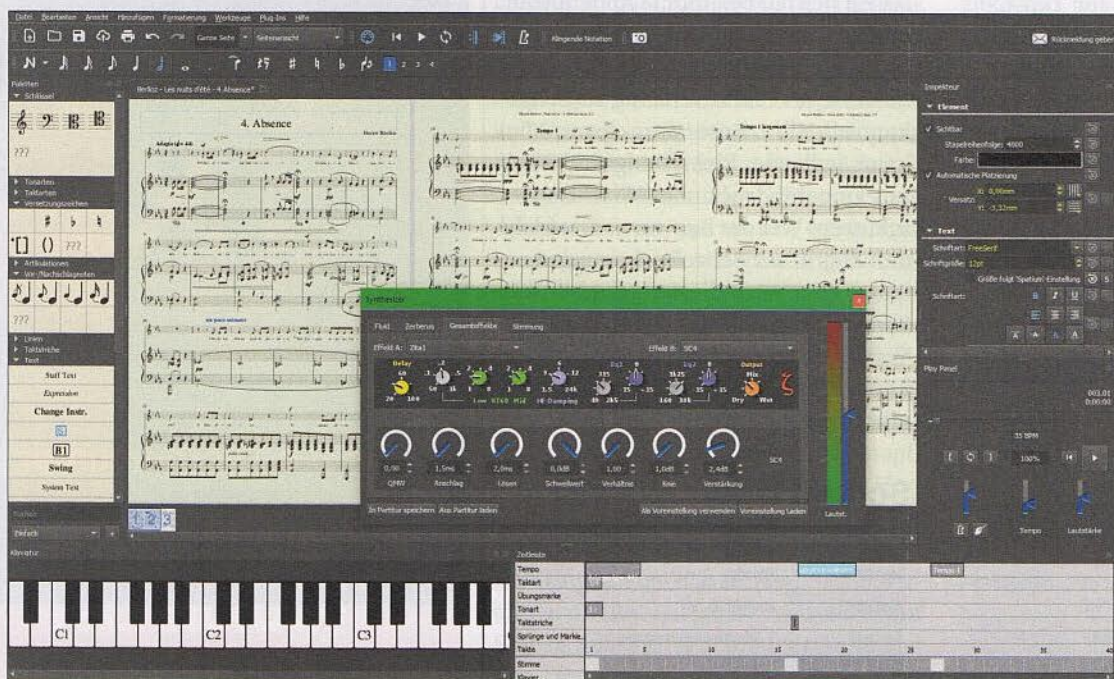
Seinen Bildschirm teilt MuseScore im Wesentlichen in fünf Bereiche ein. Im Zentrum steht das Notenbild, eingerahmt von Palettenverzeichnis oder Zeichenfilter (links) und dem „Inspektor“ (rechts). Letzterer enthält wechselnde Eigenschaften-Kataloge, je nach angeklickter Noten-, Text-, Zeilen- und System-Objekte. Den Kopf des Bildschirms füllen mehrere der üblichen Menüzeilen aus, deren unterste die elementaren Notenzeichen zum direkten Anklicken enthält, also unter anderem Noten, Notenwerte, Pausen und Vorzeichen. Der untere Rand des Bildschirms kann mit nützlichen Helferlein belegt werden, zum Beispiel dem Navigator, einer Bildschirm-Klaviatur, der neuen Zeitleiste oder dem Werkzeug zum Partiturvergleich.

Die neue Version gestattet es, eigene Arbeitsplatz-Varianten anzulegen und ab-

zuspeichern, vom fast nackten Noten-Vollbild bis zur palettenüberfüllten Bedienoberfläche. Dass die zahlreichen Paletten stets über ihren buchstäblichen Namen (etwa „Ornamente“, „Artikulationen“, „Umbrüche & Abstandhalter“) angesprochen und zum Ausklappen bewegt werden, verbessert die Übersicht auf verblüffend einfache Weise – im Unterschied zu den grafisch opulenten Tastenblöcken wie bei Sibelius oder netten, aber nichtsagenden Icons wie bei Finale und Capella. Obendrein lässt sich etwa die Belegung des Tastenblocks über leicht zu verändernde Shortcuts anpassen. Eine Suchfunktion erleichtert den Umgang mit dem Funktionsvorrat. Auf Wunsch erscheinen intelligente „Touren“ durch die neuen Programmfähigkeiten, abhängig von der aktuellen Arbeitssituation. Nach Updates sucht die Software nun automatisch.

Zwei Neuerungen erleichtern die Navigation durch den Notentext: Eine Zeitleiste verdeutlicht die wichtigsten Abschnitte der Partitur (beispielsweise Takt- oder Tempowechsel) und spult den Noten-Cursor an die entsprechende Stelle. Der neue Einzelseitenmodus erlaubt es, durch alle Systeme der Partitur ausschließlich in vertikaler Richtung zu scrollen. Die Piano-Rollen-Ansicht hat jetzt einen verbesserten Zugriff auf die Playback-Parameter, der Mixer wurde rund-erneuert.

Erfreuliche Neuigkeiten entdeckten wir auch bei der Noteneingabe und der



Mit Version 3 hat MuseScore an Darstellungsqualität zugelegt. Die Bedienoberfläche lässt sich nach Belieben umgestalten.

Verwaltung von Notensystemen und Stimmauszügen. Der „timewise input“ erlaubt es, einen Takt mit beliebigen Notenwerten aufzufüllen, was das Erstellen unregelmäßiger oder nicht-metrischer Takte zum Kinderspiel macht. Mit dem Muse-Jazz-Font erhalten nun wirklich alle Elemente der Partitur ein handschriftliches Aussehen. Ach ja: Wer Dudelsack spielt, findet wohl nur bei MuseScore eine Palette mit Verzierungen für Dudelsack-Noten.

Systeme können jederzeit ihre Eigenschaften ändern oder umdefinieren: Sie erscheinen beispielsweise „abgeschnitten“, zeigen ihre Notenköpfe mit Notennamen an oder ändern die Anzahl der Linien. Eventuelle System-Trenner wurden automatisiert. Stimmauszüge sind jetzt innerhalb eines Einzelinstruments für jede der vier möglichen Notenzeilenstimmen möglich.

Mit zwei kleineren Updates hatten die Programmierer unter anderem den Wizard für neue Partituren und den Import von alten MuseScore 2.x-Partituren verbessert. Die Eingabe von Fingersätzen wurde überarbeitet.

Das neue Autopacement erleichtert und verbessert insgesamt das Layout. Beim Notensatz spielen – im Gegensatz zum reinen Textumbruch – zusätzliche praktische Anforderungen an die Lesbarkeit wie Blätterstellen eine wichtige Rolle. MuseScore lässt in der Regel nicht beliebig enge Zeichenabstände zu, so kann man die Mindestbreite von Takten nicht unterschreiten. In Sibelius dagegen könnte man eine komplette Partitur in eine Zeile quetschen.

Zusammengerückt

Die Flexibilität moderner Notensatzprogramme wurde auch von namhaften Verlagen dazu ausgenutzt, Platz – also Papier – zu sparen. Während das in unserem Test verwendete Stück in alten gestochenen Ausgaben vier Seiten einnimmt, dampfte die neue Berlioz-Ausgabe von Bärenreiter (2005) es auf drei Seiten ein, wodurch das Notenbild (nicht nur für Kurzsichtige) unpraktisch klein wird. So etwas vermeidet MuseScore meist; einen Zeilenumbruch mittels „Dehnen“ und „Stauchern“ anzulegen ist allerdings ziemlich zeitaufwendig.

Es wäre schon einfacher, mit der Maus an den Systemen einer Seite ziehen zu können – wie etwa bei Sibelius. Allerdings führt das unter Umständen zu einem völlig verkorksten Layout. Natürlich lässt sich auch MuseScore zu absur-



Mit Autopacement erscheinen Zeichen, die sich sonst überdecken (oben), korrekt angeordnet (unten).

den Ergebnissen verleiten, etwa wenn man die Vorgabe für das alle anderen Maße bestimmende Spatium (typischer Wert 1,66 mm) zu gering ansetzt. Doch in den allermeisten Fällen kann man die Vorgaben des Programms bedenkenlos akzeptieren.

Importmeister

MuseScore 3.0.2 lief während der Tests im Wesentlichen stabil, die wichtigsten Funktionen arbeiten in der Hauptsache einwandfrei. Im Zweifelsfalle hilft die automatisch erstellte Sicherung weiter. Unter den Dateiformaten, die MuseScore versteht, verdienen besonders der Import diverser XML-Formate und der PDF-Export eine lobende Erwähnung.

Bemerkenswert darüber hinaus ist der PDF-Import, der bei MuseScore über einen Server im Internet läuft. Ein PDF-Dokument, das tatsächlich Notenzeichen enthält und nicht nur ein Abbild davon (etwa ein Scan im JPEG- oder TIF-Format), wird nach dem Upload auf dem MuseScore-Server per Open-Source-Software Audiveris in ein MuseScore-Dokument umgewandelt und lässt sich anschließend nach Belieben umgestalten. Die Ergebnisse der Übersetzung sind zwar nicht fehlerfrei, doch die notwendigen Korrekturen sind schnell gemacht. Gerade wenn es darum geht, ein bekanntes Stück auf das eigene Ensemble anzupassen, ist diese Funktion eine sehr willkommene Alternative dazu, die Noten einzeln und per Hand „nachzubauen“.

Andererseits stößt man noch auf so manche Baustelle. Eine solche ist die wichtige Plug-in-Schnittstelle, die MuseScore unter Mithilfe der MuseScore-Com-

munity zu zahlreichen Erweiterungen verhilft. Ihre Infrastruktur sei derzeit weitgehend nicht funktionsfähig, teilte das MuseScore-Team im Handbuch der Version 3 mit; viele ältere Plug-ins arbeiten nicht mehr. Ab Version 3.0.2 vom 19. Januar läuft das Plug-in-Framework wieder, allerdings noch nicht zuverlässig; Versuche mit einigen, wohl nur provisorisch eingebauten Demo-Plug-ins führten zu Abstürzen.

Die drei Autoren von MuseScore betrachten ihr Programm primär als Notensatzprogramm und nicht als Ersatz für eine digitale Audio-Workstation (DAW). Die seit Version 2 verstärkt immer wieder im Netz auftauchenden Wünsche nach umfangreicherem MIDI-Ausbau hat man bisher also nur teilweise erhört. Die eingebauten Soundfonts, Synthesizer und Effekte bieten nach Meinung der MuseScore-Väter einen ausreichenden Klang-eindruck.

Hierin unterscheidet sich das Programm deutlich von Sibelius, Finale und Dorico von Steinberg. So ist die begehrte Einbindung virtueller Instrumente (VST) für MuseScore zwar nicht unmöglich, aber unter Windows benötigt man dafür zusätzliche MIDI- und Audio-Treiber – wie das Jack Audio Connection Kit – und das MIDI-Software-Kabel LoopBe.

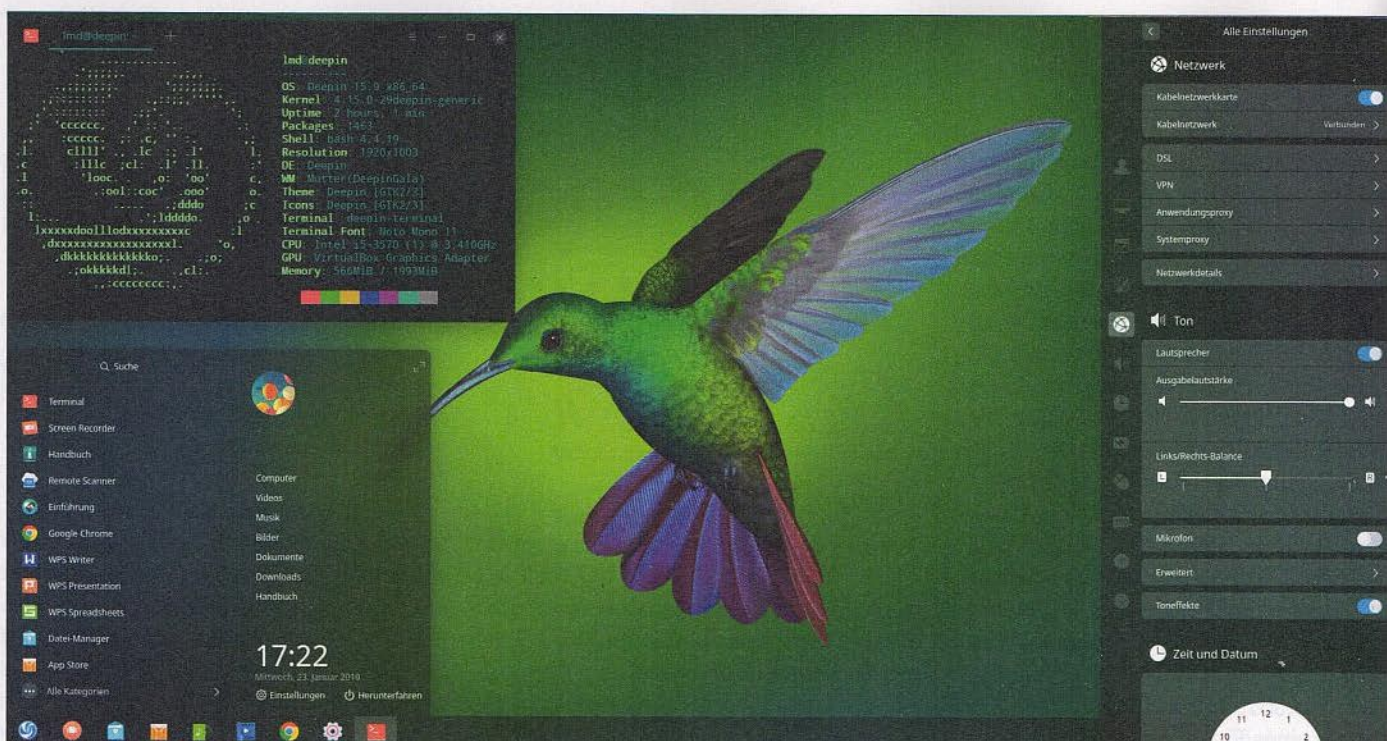
Fazit

Mit Version 3 hat MuseScore einen entscheidenden Sprung nach vorne gemacht. Das zeitraubende Hin- und Herschieben von sich bis dato überdeckenden Zeichen fällt durch das Autopacement weitgehend weg. So kommt man nicht nur zu einem überzeugenden Notenbild, sondern auch zu einem befriedigenden Gesamtlayout, dessen Vorbild der historische klassische Notenstich ist. Deutlich schneller ist das Programm obendrein geworden. Wer aber eingebaute fortgeschrittene MIDI-Fähigkeiten oder bessere Sounds zur Notenwiedergabe erwartet, sollte sich unter den kommerziellen Notensatzprogrammen umsehen.

(uh@ct.de) ct

MuseScore 3.0.2

Notensatzprogramm	
Hersteller	Werner Schweer, Thomas Bonte, Nicolas Froment
Web	https://musescore.org
Systemanf.	Windows ab 7 (32, 64 Bit), macOS ab 10.12, Linux: Applimage 64 Bit für alle Distributionen
Preis	kostenlos



Einsteiger-Linux

Deepin 15.9 mit flexiblem Desktop

Die Linux-Distribution Deepin 15.9 ist ganz auf den Desktop-Einsatz zugeschnitten: Wer damit arbeitet, braucht kaum Linux-Kenntnisse und kann das System leicht mit grafischen Tools anpassen. Die eigens entwickelte Desktop-Oberfläche ist gut gelungen und flexibel.

Von Liane M. Dubowy

Deepin 15.9 ist mehr als nur ein weiteres Debian-Derivat: Die chinesische Linux-Distribution bringt nicht nur eine eigene Desktop-Umgebung, sondern auch viele eigene Tools mit. Ganz im Vordergrund stehen dabei die Bedürfnisse der Desktop-Anwender. Seit 2014 gibt es das System außer in Chinesisch auch in anderen Sprachen, darunter Deutsch und Englisch. Die Distributoren von Wuhan Deepin Technology bauen das System auf der Basis von Debian Unstable, nutzen aber eigene Paketquellen. Das Rolling Release verwendet den Paketmanager apt; unter der Haube arbeitet der Linux-Kernel 4.15.

Das ISO-Installations-Image von Deepin 15.9 liegt ausschließlich für 64-Bit-x86-Systeme vor. Wer das Linux ausprobieren will, muss es in einer virtuellen Maschine oder auf einem Testgerät installieren, denn ein Live-System zum Ausprobieren fehlt. Das Booten des Images von DVD oder USB-Stick startet direkt die Installation. Der sehr einfach gehaltene grafische Assistent führt dann in wenigen Schritten durch die Einrichtung. Dabei wählt man als Systemsprache Deutsch, legt einen Desktop-Benutzer an und wählt den Installationsort. Der Installer kann neue Partitionen anlegen und sie bearbeiten, das Einrichten eines verschlüsselten Systems beherrscht er allerdings nicht.

Deepin 15.9 lässt sich im Gegensatz zu seinem Vorgänger auch auf Touchscreens bedienen. Einfaches Tippen simuliert einen Mausklick, doppeltes Tippen fungiert als Doppelklick. Etwas längeres Drücken öffnet ein Kontextmenü, außerdem kann man den Displayinhalt zum Scrollen auf und ab wischen. Für Eingaben steht eine Bildschirmtastatur bereit. Für das neue Release haben die Entwickler außerdem die Energieverwaltung verbessert und weiter am Desktop gefeilt.

Den Download von Updates soll Smart Mirror Switch beschleunigen. Aktiviert man die Funktion, wechselt der Paketmanager automatisch zum schnellsten Spiegelservers. Neu ist auch die Möglichkeit, das Hintergrundbild des Bootloaders Grub einfach per Drag & Drop im Kontrollzentrum auszutauschen. Den Vorgang muss man nur noch mit seinem Passwort bestätigen.

Flexibler Desktop

Die eigens entwickelte grafische Oberfläche Deepin Desktop Environment, kurz DDE, basiert ursprünglich auf HTML5 und Webkit. Mittlerweile wurde sie auf Qt5 portiert. Der Desktop lässt sich auch ohne Linux-Kenntnisse leicht an eigene Vorstellungen anpassen.

In den „Personalisieren“-Einstellungen im Kontrollzentrum stehen vier Icon-Varianten zur Wahl sowie ein dunkles und ein helles Fenster-Theme. Mit wenigen Klicks erhält der Desktop so ein anderes Gesicht. Auf dem Desktop lassen sich auch Dateien und Ordner ablegen.

Ein Klick auf den Starter ganz links in der Leiste präsentiert die Icons aller installierten Anwendungen in einem groben Raster – ähnlich wie bei Gnome. Per Klick auf das Icon rechts oben in der Übersicht wechselt man alternativ in den sogenannten Mini-Modus, der die Programme in ein traditionelles Menü mit Suchfunktion, Favoriten und Kategorien sortiert.

Zur Systemkonfiguration bringt Deepin das Kontrollzentrum mit, das als Seitenleiste am rechten Bildschirmrand erscheint. Hier konfigurieren Sie System-

einstellungen wie Audio, Benutzerkonten, Netzwerk, Tastatur und Maus sowie Zeit und Datum. Optische Feinheiten wie Theme, Icons, Schriftart und Transparenz lassen sich hier anpassen.

Interessant ist DDE auch für Besitzer hochauflösender Bildschirme: Anders als beim Gnome-Desktop kann man hier die Anzeige in 25-Prozent-Schritten skalieren.

Eigene Werkzeugkiste

Wie bei vielen Desktop-Linux-Systemen wird bei der Installation eine festgelegte Software-Auswahl eingespielt, auf die man erst nach Abschluss der Einrichtung Einfluss nehmen kann. Bestand die Software-Ausstattung der Distribution in früheren Versionen noch aus zusammengewürfelten Tools anderer Distributionen, bringt Deepin mittlerweile für die meisten Bereiche eigene Programme mit. Der Quellcode der Open-Source-Anwendungen liegt bei Github.

Deepin 15.9 sieht für Textverarbeitung, Tabellenkalkulation und Präsentationen das Büropaket **WPS Office** vor. Standardbrowser ist **Google Chrome**, als Mailclient fungiert **Thunderbird**. Für viele weitere Aufgaben stellt Deepin eigene Tools bereit, die meist den Namen ihres Aufgabenbereichs tragen, etwa den Videoplayer **Movie**, der Audioplayer **Music**, das **Terminal** für Konsolenaufgaben, den **Editor** mit Syntaxhighlighting zum Programmieren und Bearbeiten von Textdateien, den **File Manager** zur Dateiverwaltung sowie **Screenshot** und **Screen Recorder** zur Aufnahme von Bildschirmfotos und Screencasts. Auch den **Dokumentenbetrachter** zum Öffnen von PDF-Dateien, den **Bildbetrachter** zum Ansehen von Fotos sowie weitere kleine Werkzeuge hat die Distribution nach der Installation bereits an Bord.

Weitere Anwendungen installiert man über den Deepin Store nach. Gerade dort merkt man der Distribution ihre Herkunft an: Für den asiatischen Markt wichtige Anwendungen wie WeChat oder BaiduNetdisk sind dort prominent präsentiert. Aber auch die hierzulande bekannten Tools sind in den Paketquellen vorhanden. Wer Bibliotheken oder einen anderen Desktop, etwa Xfce oder Cinnamon nachinstallieren will, wird im Deepin Store allerdings nicht fündig. Sie liegen zwar in den Paketquellen vor, man muss sie aber auf der Kommandozeile mit dem von Debian übernommenen Paketmanager `apt` installieren. Unterstützung für



Wie bei Gnome zeigt Deepin die installierten Programme in einer Rasterübersicht. Per Klick auf das Icon oben rechts schaltet man in den Mini-Modus um.

Snap-Pakete fehlt; die für Flatpak lässt sich aus den Paketquellen nachrüsten, so dass man dann auch Pakete von flathub.org verwenden kann. Beim Wechsel des Grafiktreibers assistiert der Graphics Driver Manager, der die verfügbaren Treiber anbietet.

Frühere Versionen der Distribution waren in die Kritik geraten, weil der Deepin Store einen Tracker enthielt, der statistische Daten erhob und sich auch nicht deaktivieren ließ. Nachdem Kritik daran aufkam, entfernte der Distributor den Tracker, in aktuellen Versionen ist er nicht mehr enthalten.

Hilfe beim Einstieg

Beim ersten Start des Desktops startet automatisch ein Tutorialvideo, das die Bedienung und Funktionsweise des Desktops vorstellt. Es erklärt Icons, Menü, Leiste und stellt das Deepin Manual vor, das zwar unter „Handbuch“ zu finden ist, aber nur in Englisch vorliegt. Auf älteren Systemen oder in der virtuellen Maschine bietet ein Assistent dann an, Fenstereffekte zu deaktivieren – die Einstellung lässt sich im Kontrollzentrum rückgängig machen.

Beim Aufbau des Desktops lässt Deepin angenehmerweise die Wahl: Wählt man den standardmäßig aktivierten „Designer-Modus“ für den Desktop, zielt diesen unten ein mittig platziertes Dock mit Anwendungsstartern. Der alternative „Profi-Modus“ platziert am unteren Bildschirmrand eine Leiste über die ganze Bildschirmbreite. Mit einem Rechtsklick auf das Dock lässt sich der Desktop-Modus auch später noch wechseln, allerdings heißen die beiden Modi hier „Mode-Modus“ und „Effizienter Modus“.

Deepin macht es einem besonders einfach, den Desktop in vielen Kleinigkeiten anzupassen, ohne den Anwender mit allzu vielen Einstellungen zu erschlagen. Schnell ist das unten platzierte Dock nach oben, links oder rechts verschoben. Um das Hintergrundbild oder den Bildschirm-schoner auszutauschen, klickt man rechts auf den Desktop und öffnet „Wallpaper und Screensaver“. Bequem scrollt man durch die verfügbaren Bilder/Schoner und aktiviert sie per Mausklick – das Hintergrundbild wahlweise nur für Desktop oder Sperrbildschirm.

Fazit

Deepin 15.9 bietet einen modernen Desktop auf einer soliden Debian-Linux-Basis. Die wichtigsten Programme sind bereits vorinstalliert, das System aber nicht mit unnötiger Software vollgemüllt. Gerade Windows-Umsteigern dürfte Freude machen, wie einfach sie den Desktop auch ohne Linux-Kenntnisse anpassen können. Die deutsche Übersetzung ist recht gut gelungen, allerdings gibt es noch einige Lücken. Glücklicherweise füllt Deepin diese mit englischen statt chinesischen Begriffen. Die fehlende Verschlüsselung im Installer macht die Distribution allerdings ungeeignet für den Notebook-Einsatz unterwegs. (lmd@ct.de) **ct**

Deepin 15.9

Linux-Distribution	
Hersteller	Wuhan Deepin Technology, www.deepin.org
Systemanf.	Intel Pentium 4 2 GHz, 2 GByte RAM, 16 GByte Festplattenplatz
Preis	kostenlos



Ein wenig Raytracing für alle

**Sechs Grafikkarten mit GeForce RTX 2060
in preiswert und kurz, lang und leise**

Die Nvidia GeForce RTX 2060 stellt Spiele mit 2560 x 1440 Pixeln und vollen Details ruckelfrei dar. Die billigsten Karten gibt es schon ab 350 Euro. Wer mehr zahlt, bekommt nur wenig Mehrleistung, aber eine leisere Karte.

Von Benjamin Kraft

Die GeForce RTX 2060 ist das erste Mitglied der Turing-Familie, das zum Marktstart ein besseres Preis-Leistungs-Verhältnis als die Vorgängergeneration bietet. Sie liefert die Performance einer werksübertakteten GeForce GTX

1070 Ti oft zum deutlich geringeren Preis: Die günstigste 2060-Karte in diesem Vergleich kostet etwa 350 Euro, rund 80 Euro weniger als die billigste lieferbare 1070 Ti.

Wir holten sechs Grafikkarten verschiedener Hersteller ins Labor, um sie miteinander, aber auch mit Nvidias Quasi-Referenzkarte GeForce RTX 2060 Founders Edition zu vergleichen [1]. Die Karten unterscheiden sich nicht nur im Preis, sondern auch beim GPU-Takt und den Dimensionen des Kühlers. Von der Kompaktkarte bis zum überlangen Board in mehr als doppelter Bauhöhe ist das volle Spektrum vertreten.

Die beiden günstigsten Karten im Test sind mit etwa 350 Euro die Palit GeForce RTX 2060 StormX im Mini-ITX-Format und die KFA2 GeForce RTX 2060 [1-Click

OC]. Das obere Ende des Preisspektrums bildet ab 420 Euro das Trio aus der Asus ROG Strix GeForce RTX 2060, der Gigabyte GeForce RTX 2060 Gaming OC Pro und der GeForce RTX 2060 Gaming Z 6G von MSI. Dazwischen platziert Zotac seine Gaming GeForce RTX 2060 Amp für etwa 380 Euro.

Gestutzte TU106 mit 6 GByte RAM

Für die GeForce RTX 2060 hat Nvidia die von der GeForce RTX 2070 bekannte TU106-GPU zurechtgestutzt, um einen Performance- und Preisabstand zu kreieren. So verfügt die RTX 2060 über 1920 Shader-Kerne, 120 Textur- und 48 Rasterseinheiten. Die theoretische Rechenleistung beträgt mit Referenztakt etwa 6,45 TFlops. 240 Tensor-Cores stehen für

maschinelles Lernen oder andere KI-Anwendungen bereit, 30 RT-Cores sollen Raytracing-Effekte beschleunigen.

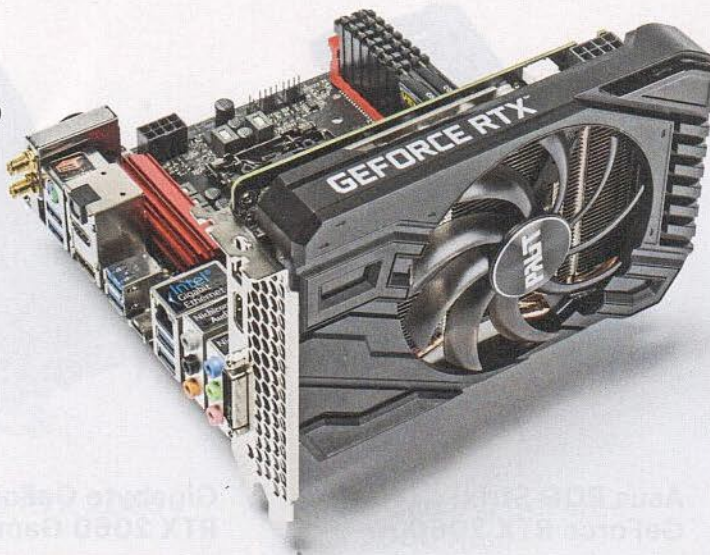
Ein weiterer wichtiger Unterschied betrifft den Grafikspeicher: Der GeForce RTX 2060 stehen statt 8 nur 6 GByte GDDR6-RAM zur Verfügung, das zudem nur mit 192 Bit angebunden ist und einen Durchsatz von 336 GByte/s erzielt. Damit erreicht die bislang kleinste Turing-Karte auf dem Papier 85 Prozent der Rechenleistung und 75 Prozent des Speicherdurchsatzes einer GeForce RTX 2070.

Anschlussfragen

Nvidias GeForce RTX 2060 Founders Edition bringt vielfältige Anschlussmöglichkeiten mit, vom in die Jahre gekommenen DVI über die aktuellen Standards DisplayPort 1.4 und HDMI 2.0b bis hin zur USB-C-Buchse. Da können die hier getesteten Modelle nicht mithalten. Durchweg fehlt ihnen beispielsweise die USB-C-Buchse und damit die Möglichkeit, darüber USB-3.1-Geräte oder mittels VirtualLink eine VR-Brille anzusteuern.

Die günstigen Karten von KFA2 und Palit haben sogar nur drei Display-Anschlüsse, nämlich Dual-Link-DVI, HDMI 2.0b und einen DisplayPort 1.4. Das reicht zwar prinzipiell auch für zwei 4K-Displays oder insgesamt drei Monitore, schränkt aber an anderer Stelle ein: Beispielsweise können diese Karten nur je ein G-Sync-Display antreiben, da Nvidias adaptives Sync-Verfahren nur am DisplayPort funktioniert. Gigabyte, MSI und Zotac geben ihren Karten je drei DisplayPorts und einen HDMI-Ausgang mit, bei Asus gibt es zweimal HDMI und zweimal DP.

Die kompakte GeForce RTX 2060 StormX von Palit eignet sich für Gaming-taugliche Rechner im Mini-ITX-Format.



Zwei Karten zu einem theoretisch doppelt so leistungsfähigen SLI-Verbund zusammenzuschalten, gelang schon in der Pascal-Generation erst ab der GeForce GTX 1070 aufwärts. Bei Turing wird dieses Feature innerhalb der Produktfamilie noch weiter nach oben verschoben: Nur die GeForce RTX 2080 und RTX 2080 Ti verfügen über die nötigen NVLink-Kontakte. Ein günstiges Turing-Duett fällt damit aus.

Nvidia gibt die TDP der TU106-GPU mit 160 Watt an. Wie die Founders Edition haben alle Karten daher einen achtpoligen PCIe-Stromanschluss. Allein Asus packt noch einen sechspoligen zusätzlich auf die Platine. Warum ist nicht klar, denn die ROG Strix RTX 2060 zieht nicht mehr Leistung aus der Steckdose als die gleich schnellen Mitbewerber.

Performance wie die GTX 1070 Ti

Nvidia spezifiziert für die GeForce RTX 2060 einen Nominaltakt von 1365 MHz

und einen Boost-Takt von 1680 MHz. Um ihre Produkte voneinander abzusetzen, versprechen die Hersteller teils deutlich höhere Taktraten, vor allem im Boost. So dreht beispielsweise Gigabyte die MHz-Schraube bis 1800 hoch, MSI und Zotac gehen sogar bis 1830. In der Praxis kratzen einige Karten sogar an der 2-GHz-Marke – wie lange sie in diesen Taktsphären verweilen, hängt vom Kühler ab.

Bei manchen Karten ist der Werksturbo in der Firmware hinterlegt, bei anderen muss man ihn in der Hersteller-Software aktivieren. Bei Asus gibt es zudem noch einen Schiebeschalter, mit dem man zwischen dem Quiet- und Performance-Mode umschaltet.

Das Ergebnis der Takt-Kur fällt letztlich mager aus: Sie bringt zwar in synthetischen Benchmarks wie dem 3DMark oder Compute- und Render-Aufgaben à la LuxMark Vorteile, aber in Spielen merkt man davon nichts. Die langsamsten Karten liegen auf dem Niveau der GeForce RTX

Grafikkarten mit Nvidias GeForce RTX 2060: Performance

Grafikkarte	3DMark Port Royal / Time Spy / Firestrike Extreme [Punkte]	GTA V (DX 11) Maximum, 4 x MSAA (4K/WQHD/Full HD) [fps]	Far Cry 5 (DX 11) Ultra, SMAA, HD Textures (4K/WQHD/Full HD) [fps]	Shadow o. t. Tomb Raider (DX 12) Maximum, SMAA (4K/WQHD/Full HD) [fps]	Luxmark 3.1 Luxball HDR [Punkte]
	besser ▶	besser ▶	besser ▶	besser ▶	besser ▶
Gigabyte Radeon RX Vega 64 Gaming OC	–/6366/8619	33/58/80	46/86/115	33/63/95	32126
MSI GeForce GTX 1060 Gaming X 6G	–/4610/6116	25/49/71	26/51/74	18/36/56	12648
Asus ROG Strix GeForce GTX 1070 Ti Advanced	–/6962/9079	37/71/93	40/76/106	29/57/85	17195
Asus ROG Strix GeForce RTX 2060 ¹	3907/7943/9140	39/73/95	39/80/112	31/61/93	21965
Gigabyte GeForce RTX 2060 Gaming OC Pro	3881/7885/9044	38/72/94	42/81/113	31/59/91	21782
KFA2 GeForce RTX 2060 [1-Click OC]	3741/7521/8666	37/71/93	40/78/109	30/58/89	21292
MSI GeForce RTX 2060 Gaming Z 6G	3898/7908/9053	39/73/95	42/81/111	31/61/93	22034
Nvidia GeForce RTX 2060 Founders Edition	3785/7534/8744	38/73/93	40/78/109	30/58/90	21170
Palit GeForce RTX 2060 StormX	3795/7539/8719	37/71/92	38/78/108	30/58/89	21176
Zotac Gaming GeForce RTX 2060 Amp	3870/7772/8966	38/72/94	42/80/112	31/60/93	21398
Nvidia GeForce RTX 2070 Founders Edition	4865/8949/10604	48/84/100	49/93/123	37/70/104	30333

Testsystem: Intel Core i7-8700K (OC 4,7 GHz), 32 GByte DDR4-RAM, Windows 10 (1809) 64 Bit, V-Sync aus; Grafiktreiber: AMD Adrenalin 2019 Edition 18.12.3, Nvidia GeForce 417.71
MSAA/SMAA/FXAA: Kantenglättungsverfahren ¹ alle Messungen im Quiet-Mode



Asus ROG Strix GeForce RTX 2060

Die mit 300 Millimeter längste und 132 Millimeter breiteste Karte im Vergleich bringt 1,3 Kilo auf die Waage und trägt den gleichen Triple-Slot-Kühler wie ihre größeren Turing-Geschwister. Der ist Overkill. Schon im Quiet-Mode, der ordentliche 3D-Leistung über dem Niveau von Nvidias Founders Edition liefert, erwärmt sich die GPU auf maximal 62 °C.

Per Schiebeschalter in den Performance-Mode versetzt, erzielt die Karte zwar mehr 3D-Mark-Punkte, aber in Spielen keine höheren Bildraten. Gegenüber dem Quiet-Mode steigt die Lautstärke unter Volllast von guten 0,8 auf nur noch befriedigende 1,3 Sone, weil die schneller drehenden Lüfter die GPU auf unter 60 °C kühlen. Bei normaler 3D-Last bleibt die Karte akustisch zurückhaltend. Die Leistungsaufnahme ist in beiden Modi identisch und die zweithöchste im Testfeld, aber kein Grund, der Karte zusätzlich zum 8-Pin- noch einen 6-Pin-Stromanschluss mitzugeben.

Strix-typisch hat Asus' RTX 2060 die konfigurierbare Aura-Sync-Beleuchtung an Bord, die sie per dreipoligem Kabel mit dem Mainboard abstimmen kann. Zusätzlich finden sich am Kartenende zwei Lüfteranschlüsse, die beispielsweise Gehäuselüfter in Abhängigkeit der GPU-Temperatur regeln können. Am Anschlussfeld trägt sie zwei DisplayPorts und zwei HDMI-Ausgänge. Mit 430 Euro gehört sie zu den teuersten Karten im Test.

- 🟢 im Quiet-Mode schnell und leise
- 🟢 effizient
- 🔴 lang, überbreit und teuer



Gigabyte GeForce RTX 2060 Gaming OC Pro

Die Gigabyte-Karte ist mit 28 Zentimetern zwar beinahe so lang wie das Asus-Modell, dabei aber schmaler und blockiert anders als bei Asus und MSI nur zwei PCIe-Erweiterungssteckplätze. Der Kühler mit seinen drei 90-Millimeter-Lüftern, von denen der mittlere gegenläufig zu den äußeren rotiert, ist ein alter Bekannter: Er kommt auch auf den teureren RTX-Karten von Gigabyte zu Einsatz und ist für die TU106-GPU eigentlich überdimensioniert.

Das an der Seite eingelassene Gigabyte-Logo durchläuft standardmäßig ein Farbrad. Mit installierter Aorus-Engine-Software darf man ihm Farben fest zuweisen, sie pulsieren lassen oder andere Effekte wählen – und mit einem Gigabyte-Mainboard synchronisieren. Außerdem bringt das Tool weitere Tuning-Funktionen mit.

Zeigt der Bildschirm den Windows-Desktop, stoppt der Kühler die Lüfter und schweigt. Unter Volllast geben sie etwas rauhe 0,9 Sone von sich, beim Spielen meist weniger. Die 3D-Leistungsaufnahme ist mit 185 Watt die niedrigste im Spitzentrio und liegt insgesamt im Mittelfeld.

Mit 420 Euro gehört Gigabytes RTX 2060 Gaming OC Pro zu den teuersten Karten im Feld. Die dreijährige Garantie fällt gut, aber nicht großzügig aus.

- 🟢 schnell und noch leise
- 🟢 Dual-Slot-Kühler
- 🔴 lang und teuer



KFA2 GeForce RTX 2060 [1-Click OC]

Die Karte mit der eckigen Klammer im Namen steht im Preisvergleich ab 360 Euro. Der Namenszusatz 1-Click OC soll darauf hinweisen, dass die Karte per Treiberprofil, das in der Herstellersoftware hinterlegt ist, mit höherem Takt betrieben werden kann. Mit Standardtreiber läuft die RTX 2060 von KFA2 mit Nvidias Referenztakt, hält aber schon dann mehr als 1900 MHz im Boost. Dabei beschleunigen die beiden 90-Millimeter-Lüfter nach und nach auf über 2000 Umdrehungen pro Minute. Bei dieser Geschwindigkeit laufen sie rau, brummelig und zumindest akustisch unruhig, begleitet von Rauschen.

Aufgrund des höheren Boost-Taktes kann sich die KFA2-Karte in Spielen minimal von der Palit-Karte absetzen, liegt aber ihrerseits meist etwa 3 fps hinter dem Spitzentrio. Mit 3D-Last fordert sie sparsame 162 Watt aus der Steckdose, nur Palit ist noch genügsamer.

Die RTX 2060 [1-Click OC] misst nur 23 Zentimeter und gehört zu den kürzesten Modellen im Testfeld; da stehen die Chancen gut, dass sie auch in engeren Gehäusen nicht mit dem Laufwerkskäfig oder anderen Aufbauten kollidiert. Zwei ihrer drei Signalausgänge können 4K-Displays antreiben: via HDMI bis 60 Hz, am DisplayPort 1.4 bis 120 Hz. Mit DL-DVI-Anschluss ist bei 2560 x 1600 und 60 Hz Schluss. Die Garantie beträgt nur zwei Jahre, alle anderen Hersteller im Vergleich bieten mehr.

- 🟢 23 Zentimeter kurz
- 🔴 kürzeste Garantie im Testfeld
- 🔴 laut und brummelig unter Last



MSI GeForce RTX 2060 Gaming Z 6G

Zwar nur knapp 25 Zentimeter kurz, geht MSIs Karte in die Breite: 13 Zentimeter kann in engeren Gehäusen schon knapp werden. Außerdem ragt ihr Kühler bereits in den angrenzenden PCIe-Slot, sodass die Karte insgesamt drei blockiert. Mit beinahe 950 Gramm ist auch sie kein Leichtgewicht, macht aber fest verschraubt noch keine Probleme.

In einem Gehäuse mit Fenster macht die Karte viel her: Die RGB-LEDs in den Einrahmungen der beiden 100-Millimeter-Lüfter wechseln ebenso wie eine kleine Leuchtfläche an der Kartenseite ständig ihre Farbe. Das Farbenspiel, das bei MSI Mystic Light heißt, lässt sich per Software steuern und mit dem eines passenden Mainboards koordinieren.

Im Leerlauf komplett still, säuseln die Lüfter auch unter Last nur dezent mit 0,8 Sone. Damit wäre die MSI-Karte allein nach den Messwerten die leiseste im Testfeld. Allerdings zischten oder zirpten bei unserem Exemplar die Spulen der Spannungsversorgung je nach 3D-Last, was nicht jeder Nutzer ausblenden kann. Mit 199 Watt genehmigte sich die RTX 2060 Gaming Z zudem noch mehr elektrische Leistung als die Konkurrenten. Mit 430 Euro gehört sie zu den teuersten Karten im Test.

- ⬆️ schnell und leise
- ⬆️ Spulenzischen im 3D-Betrieb
- ⬆️ teuer



Palit GeForce RTX 2060 StormX

Mit nur 16,8 Zentimeter die mit Abstand kürzeste Karte im Test, ist sie auch die einzige, die sich für ein Mini-ITX-System mit potenter Grafikkarte eignet. Mit je einem DL-DVI-Anschluss, einem DisplayPort und einer HDMI-Buchse bringt sie nicht so viele Anschlüsse wie die meisten Konkurrenten mit, treibt aber immerhin zwei 4K-Displays mit 60 Hz an.

Die GeForce RTX 2060 StormX tritt mit Referenztakt an, doch weil die GPU den kleinen Kühler schnell aufheizt, muss sein 100-Millimeter-Lüfter früher als bei den Konkurrenten hochdrehen und sich mehr ins Zeug legen. Um die GPU unter 3D-Last unter 80 °C zu halten, rotierte er im Test mit mehr als 2400 Umdrehungen pro Minute und produzierte sägende 1,3 Sone. In Spielen mit wechselnden Lastszenarien vibrierte sporadisch der Lüfterrahmen rasselnd mit.

Trotz der Kühlanstrengungen fällt der Turbo im Schnitt mit 1635 MHz vergleichsweise niedrig aus. Bei längerer Last fällt er auch unter 1600 MHz, weshalb die Palit-Karte zwar eine der GPU angemessene Leistung erzielt, aber nicht mit dem Spitzenfeld mithalten kann: Sie liefert im Schnitt 3 bis 4 fps weniger als die schnellsten Karten im Testfeld. Dafür ist sie im 3D-Betrieb die sparsamste Karte im Vergleich und hält sich exakt an Nvidias TDP. Im Onlinehandel ist die Kompaktkarte ab 350 Euro zu finden, ebenso wie ihr Zwilingsmodell Gainward GeForce RTX 2060 Pegasus.

- ⬆️ 16,8 Zentimeter kurz
- ⬆️ billig
- ⬆️ laut unter Last



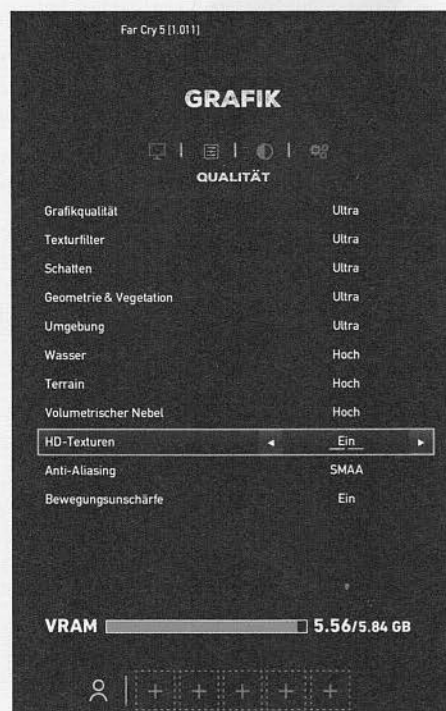
Zotac Gaming GeForce RTX 2060 Amp

Zotacs GeForce RTX 2060 Amp ist mit 21 Zentimetern Baulänge eine der kürzesten Karten im Feld und damit eine gute Wahl für kleinere Gehäuse. Für Mini-ITX ist sie aber noch etwa vier Zentimeter zu lang. Optisch trifft sie eine interessante Mischung aus Eleganz und Wuchtigkeit. Ersteres ergibt sich aus dem silbergrau-schwarzen Farbschema mit dem weiß leuchtenden Logo an der Seite, letzteres aus dem kantigen Styling und der sich an den Kartenseiten emporwölbenden Backplate.

Mit 380 Euro liegt die Amp Edition leicht über Nvidias Founders Edition, liefert aber zumindest auf dem Papier mehr Performance. Das kleine Leistungsplus geht allerdings zu Lasten der Lautstärke: Die beiden 90-mm-Lüfter schalten sich auch im Leerlauf nicht ab und rauschen brummelig mit 0,2 Sone. Aufgrund der aggressiven Lüfterkurve erreicht die Karte im 3D-Betrieb nach einiger Zeit 1,6 Sone, die auch aus dem unterm Tisch stehenden, geschlossenen Gehäuse vernehmbar sind.

Am Anschlussfeld trägt sie drei DisplayPorts und eine HDMI-Buchse. Wer seine Karte registriert, bekommt von Zotac großzügige fünf Jahre Garantie. Ohne Registrierung sind es zwei Jahre.

- ⬆️ großzügige Garantie
- ⬆️ 21 Zentimeter kurz
- ⬆️ laut unter Last



In Far Cry 5 geht der RTX 2060 selbst in 4K mit allen Schikanen und HD-Texturen der Speicher nicht aus.

2060 Founders Edition und der GeForce GTX 1070 Ti, die schnellsten rendern nur vier Bilder pro Sekunde mehr. Eine GeForce GTX 1060 6 GByte hängen sie allesamt locker ab, im Vergleich mit der Konkurrenz ordnen sie sich zwischen AMDs Radeon-Karten RX Vega 56 und Vega 64 ein.

Damit sind sämtliche Karten im Test auch für aktuelle 3D-Spiele in WQHD gerüstet: Mit allen Reglern am Anschlag und aktivierter Kantenglättung stellen sie je nach Spiel zwischen 60 und 80 fps (frames per second) dar. Schaltet man auf Full HD zurück, sind es rund 30 fps mehr. Damit qualifizieren sie sich durchweg als 3D-Antrieb für 144-Hz-Displays, die sich mit variabler Bildwiederholrate ansteuern lassen. Seit Kurzem müssen das nicht mehr zwingend G-Sync-Displays sein, auch mit FreeSync-Anzeigen spielen aktuelle GeForce-Karten seit dem Treiber 417.71 zusammen.

Raytracing und Speicher

Beim Einsatz von Raytracing-Effekten schwindet das komfortable Performance-Polster der GeForce RTX 2060. Ob sie über gerade noch genug oder schon zu wenig RT-Leistung verfügt, lässt sich erst sagen, wenn mehr Spiele mit RT-Effekten erschienen sind. Eine erste Einschätzung, wo sich die Karten innerhalb der Turing-

Hierarchie einsortieren, liefert der Raytracing-Benchmark Port Royal, der seit Januar 2019 Teil der 3DMark-Suite ist. Die GeForce RTX 2060 Founders Edition erzielte 3785 Punkte, die Karten im Testfeld zwischen 3741 und 3975 Punkten. Nvidias GeForce RTX 2070 Founders Edition schnitt 30 Prozent besser ab (4865 Punkte), bei der Gainward GeForce RTX 2080 Phoenix GS betrug das Plus knapp 58 Prozent (5968 Punkte), eine GeForce RTX 2080 Ti ist nahezu doppelt so schnell (7527 Punkte) wie die RTX 2060.

Was das in der Praxis bedeutet, zeigt der Ego-Shooter Battlefield V, das bislang einzige erschienene Spiel mit Raytracing-Effekten. In den ersten Bereichen der Kampagne „Tirailleur“ lieferte die GeForce RTX 2060 in WQHD mit Detailstufe Ultra knapp 80 fps. Sobald wir allerdings die DXR-Effekte zuschalteten, brach die Performance ein; selbst mit der niedrigsten Raytracing-Stufe „low“ schaffte die RTX 2060 im Mittel nur noch 53 fps. Auch in Full HD rutschte die Bildrate häufiger unter die Marke von 60 Bildern pro Sekunde. Zweifelsohne hübschen die realitätsnahen Reflexionen und weichen Schatten die Szene auf – doch ob man im Eifer des Feuergefechts für solche Details ein Auge hat und dafür diese Performance-Einbußen in Kauf nehmen möchte, muss jeder Spieler selbst entscheiden.

Zum Vergleich: Die GeForce RTX 2070 Founders Edition erzielte in WQHD mit identischen Einstellungen und DXR auf „low“ durchschnittlich noch 59 fps, Gainwards RTX 2080 Phoenix GS 71 fps. Unklar ist derzeit noch, ob die RT-Leistung allein auf die vergleichsweise geringe Anzahl an RT-Cores zurückgeht oder auch der kleinere Speicher seinen Anteil hat. Die Tools MSI Afterburner und GPU-Z zeigten bei der RTX 2060 in Battlefield V in WQHD eine Speicherauslastung von 5,7 GByte an, doch ist nicht auszuschließen, dass sie danebenlagen – oder das Spiel oder der Treiber den knappen Speicher erkennt und von sich aus diese Grenze zieht.

Wer seine neue Karte also mit einem Auge auf die strahlende Raytracing-Zukunft aussucht, muss sich der relativ geringen RT-Leistung der GeForce RTX 2060 bewusst sein. Dass sie schon jetzt kämpfen muss, um in Full HD über 60 fps zu bleiben, ist kein gutes Omen. Man darf davon ausgehen, dass die Spielekomplexität weiter zunimmt, vor allem bei solchen von Nvidia forcierten Vorzeigefeatures wie Raytracing.

An anderer Stelle ist indes Entwarnung angesagt: Die Befürchtung, 6 GByte Grafik-RAM seien für aktuelle Spiele zu knapp bemessen, trifft in aller Regel nicht zu. In der WQHD-Auflösung, bei der sich diese Karten wohl fühlen, sind sie gut gerüstet. Selbst in 4K mit allen Reglern am Anschlag geht der Speicher nicht aus. Allerdings gilt auch hier: Spieleentwickler entwerfen immer detailliertere Welten mit feineren Modellen und Texturen, sodass der Speicherhunger der Spiele stetig steigt.

Leistungsaufnahme und Lautstärke

Eigentlich ist die Turing-Architektur etwas effizienter als ihre Pascal-Vorgängerin. In der Messpraxis merkt man davon allerdings wenig. Mit einem angeschlossenen Full-HD-Display nehmen die RTX-2060er im Leerlauf zwischen 8,5 und 12 Watt auf, mit einem 4K-Display sind es 11 bis 13 Watt. Das konnte die GeForce GTX 1070 Ti besser. Eine Mischbestückung mit drei Full-HD-Displays und einem 4K-Monitor scheint für Nvidia-Karten das Worst-Case-Szenario zu sein; dann zeigte das Leistungsmessgerät zwischen 34 und 40 Watt. Mit 3D-Last rangierte die Leistungsaufnahme zwischen 160 und 200 Watt – auch das liegt auf oder über dem Niveau der GeForce GTX 1070 Ti.

Bei der Lautstärke gab es zwischen den Prüflingen größere Unterschiede, wobei erwartungsgemäß mehr Kühlfläche auch mehr Laufruhe bedeutet. Tatsächlich gehören die überlangen Karten von Giga-byte und, zumindest im Quiet-Mode, auch Asus zu den leisesten im Feld, doch die RTX 2060 von MSI agiert noch sanfter. Getrübt wird ihr gutes Ergebnis von einem Spulenzischen, das mit der Bildrate variiert. Palits Mini-ITX-Karte zieht auf dem Papier mit der Asus-Karte im Performance-Mode gleich, dreht aber früher auf und klingt viel kerniger. Außerdem vibrierte manchmal ihr Lüfterrahmen mit. Auf dem Papier gleich laut, lassen sich die Zotac-Lüfter besser ausblenden als die brummigen und unruhig laufenden der KFA2.

Fazit

Die GeForce RTX 2060 ist eine würdige Nachfolgerin, allerdings nicht für die GeForce GTX 1060. Dafür ist sie schlicht zu teuer; diese Rolle wird vielmehr den GeForce GTX 1660 und GTX 1660 Ti zufallen, die im Laufe des Februars erscheinen sollen. Stattdessen beerbt sie die GeForce

GTX 1070 Ti zum kleineren Preis und liefert genug Performance, um mit allen Schikanen in WQHD-Auflösung zu spielen. Allein hinter der praktischen Raytracing-Performance steht ein Fragezeichen, wie die Stichproben mit Battlefield V zeigen.

Was die 3D-Performance anbelangt, sind alle Karten in diesem Vergleich so gut wie gleich schnell – das langsamste und das schnellste Modell trennen nie mehr als 4 fps, aber immerhin gut 80 Euro. Den Aufpreis nehmen Asus, Gigabyte und MSI für bessere, leisere Kühllösungen, die allerdings durch besonders hohes Gewicht, Überbreite oder -länge herausstechen.

Wer ein kompaktes Mini-ITX-System zusammenstellen möchte, sollte sich die GeForce RTX 2060 StormX von Palit anschauen. Die ist zwar kein Leisetreter, punktet aber mit dem niedrigsten Preis in diesem Vergleich.

Den besten Kompromiss aus Preis, Leistung und Lautstärke trifft jedoch am

Günstigere Modelle haben drei verschiedene Signalausgänge, teurere bringen vier mit, beschränken sich aber auf HDMI und DisplayPort.



Ende keiner der Kartenhersteller, sondern Nvidia selbst mit seiner hauseigenen GeForce RTX 2060 Founders Edition. Die bleibt ähnlich leise wie die MSI-Karte ohne zu zischen, kostet mit 370 Euro weniger als die gleich schnelle Zotac-Karte und bringt obendrein noch eine USB-C-Buchse mit. Damit darf sie

derzeit tatsächlich als Referenz unter den Grafikkarten mit GeForce RTX 2060 gelten. (bkr@ct.de) **ct**

Literatur

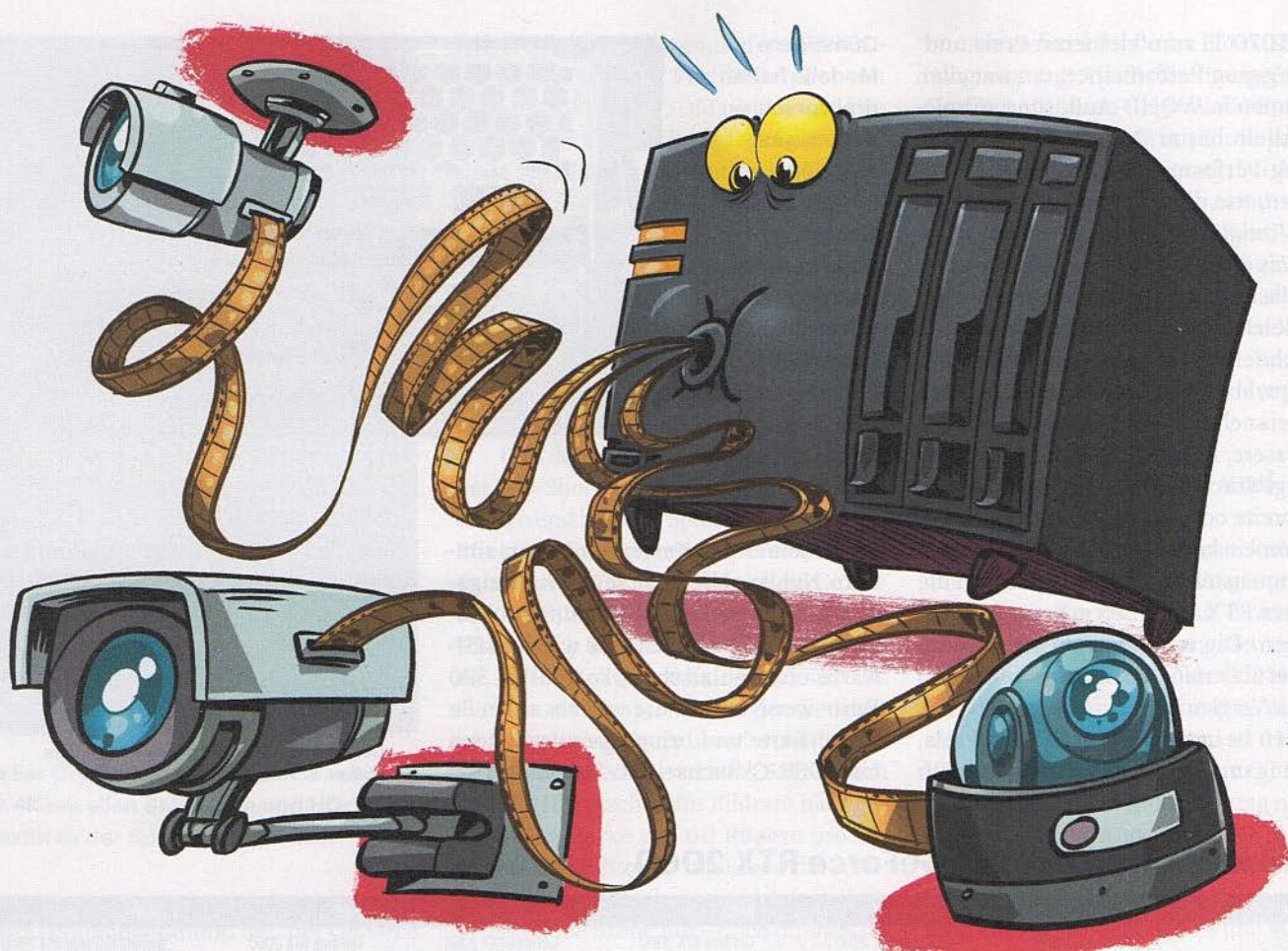
- [1] Benjamin Kraft, Raytracing-Einsteiger, Nvidia GeForce RTX 2060 Founders Edition zum Zocken in WQHD, c't 3/2019, S. 69

Grafikkarten mit Nvidias GeForce RTX 2060

Hersteller	Asus	Gigabyte	KFA2	MSI	Palit	Zotac
Modell	ROG Strix GeForce RTX 2060	GeForce RTX 2060 Gaming OC Pro	GeForce RTX 2060 [1-Click OC]	GeForce RTX 2060 Gaming Z 6G	GeForce RTX 2060 StormX	Gaming GeForce RTX 2060 Amp
GPU	TU106	TU106	TU106	TU106	TU106	TU106
Shader / TMU / ROP / RT / Tensor	1920 / 120 / 48 / 30 / 240	1920 / 120 / 48 / 30 / 240	1920 / 120 / 48 / 30 / 240	1920 / 120 / 48 / 30 / 240	1920 / 120 / 48 / 30 / 240	1920 / 120 / 48 / 30 / 240
Chip- / Boost-Taktfrequenzen ¹	1395 MHz / 1710 MHz (OC Mode) ²	1365 MHz / 1830 MHz	1365 MHz / 1710 MHz (OC Mode) ²	1365 MHz / 1830 MHz	1365 MHz / 1680 MHz	1365 MHz / 1800 MHz
Speichermenge / -typ / -takt	6 GByte / GDDR6 / 1750 MHz	6 GByte / GDDR6 / 1750 MHz	6 GByte / GDDR6 / 1750 MHz	6 GByte / GDDR6 / 1750 MHz	6 GByte / GDDR6 / 1750 MHz	6 GByte / GDDR6 / 1750 MHz
Stromversorgung	1 × 8-Pin + 1 × 6-Pin PCIe	1 × 8-Pin PCIe	1 × 8-Pin PCIe	1 × 8-Pin PCIe	1 × 8-Pin PCIe	1 × 8-Pin PCIe
Abmessungen (T × B × H) / Gewicht	300 mm × 132 mm × 50 mm / 1281 g	280 mm × 116 mm × 40 mm / 810 g	228 mm × 131 mm × 41 mm / 609 g	247 mm × 129 mm × 52 mm / 947 g	168 mm × 126 mm × 40 mm / 414 g	210 mm × 119 mm × 41 mm / 625 g
Bauhöhe	Triple-Slot	Dual-Slot	Dual-Slot	Triple-Slot	Dual-Slot	Dual-Slot
Lüfter / Zero-Fan-Modus ³	3 × Axiallüfter (90 mm) / ✓ ⁴	3 × Axiallüfter (80 mm) / ✓	2 × Axiallüfter (90 mm) / ✓	2 × Axiallüfter (100 mm) / ✓	1 × Axiallüfter (100 mm) / ✓	2 × Axiallüfter (90 mm) / –
Ausstattung						
Anschlüsse	2 × DisplayPort 1.4, 2 × HDMI 2.0b	3 × DisplayPort 1.4, 1 × HDMI 2.0b	1 × DisplayPort 1.4, 1 × DVI, 1 × HDMI 2.0b	3 × DisplayPort 1.4, 1 × HDMI 2.0b	1 × DisplayPort 1.4, 1 × DVI, 1 × HDMI 2.0b	3 × DisplayPort 1.4, 1 × HDMI 2.0b
sonstige Hardware-Beigaben	2 × Klett-Kabelbinder, Treiber-CD, Handbuch	Treiber-CD, Schnellstartanleitung	Adapterkabel 2 × Molex auf 8-Pin PCIe	–	–	–
Technische Prüfungen						
3DMark Port Royal / Time Spy / Firestrike Extreme	3975 / 7976 / 9144 (3907 / 7943 / 9140) ⁴	3881 / 7885 / 9044	3741 / 7521 / 8666	3898 / 7908 / 9053	3795 / 7539 / 8719	3870 / 7772 / 8966
LuxBall HDR (LuxMark 3.1)	22101 (21965) ⁴	21782	21292	22034	21176	21398
Leistungsaufnahme 2D / 3D / Peak ⁴	10,7 (16,6) / 191 / 258 Watt	8,5 (14,6) / 185 / 268 Watt	11 (17,6) / 162 / 235	10,7 (17,1) / 199 / 282 Watt	12 (16,4) / 160 / 233	9,7 (18,4) / 171 / 254 Watt
Lautheit 2D / 3D / Maximum ⁵	<0,1 / 1,3 / 1,3 Sone (<0,1 / 0,8 / 0,9 Sone) ⁴	<0,1 / 0,9 / 0,9 Sone	0,2 / 1,5 / 1,6 Sone	<0,1 / 0,7 / 0,8 Sone	<0,1 / 1,3 / 1,3 Sone	0,2 / 1,6 / 1,6 Sone
Bewertung						
Spieleleistung Full HD / WQHD / 4K	⊕⊕ / ⊕ / ⊖	⊕⊕ / ⊕ / ⊖	⊕⊕ / ⊕ / ⊖	⊕⊕ / ⊕ / ⊖	⊕⊕ / ⊕ / ⊖	⊕⊕ / ⊕ / ⊖
Geräuscentw. Leerlauf / Last	⊕⊕ / ⊖ (⊕) ⁴	⊕⊕ / ⊕	⊕⊕ / ⊖	⊕⊕ / ⊕ ⁶	⊕⊕ / ⊖	⊕⊕ / ⊖
Garantie	3 Jahre	3 Jahre	2 Jahre	3 Jahre	3 Jahre	5 Jahre (nach Registrierung)
Preis (zirka)	430 €	420 €	360 €	430 €	350 €	380 €

¹ Herstellerangaben ² per Software-Profil ³ Lüfter stehen im Leerlauf still ⁴ Im Quiet-Mode ⁵ Windows-Idle-Modus mit einem bzw. drei angeschlossenen Monitoren / Mittelwert im 3DMark 11 GT1 / kurzzeitig auftretende Spitzenwerte ⁶ Spulenzischen

⊕⊕ sehr gut ⊕ gut ⊖ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden k. A. keine Angabe



Videoschlucker

Heimüberwachung: Videostreams mit dem NAS aufzeichnen

Netzwerkvideorekorder (NVR) zeichnen Videostreams von IP-Kameras auf. Viele NAS können neben Ihrer eigentlichen Funktion als Speicher auch als NVR arbeiten und so Aufzeichnungen sicherer unterbringen. Wir haben die App-Angebote der zwei größten Hersteller getestet.

Von Andrijan Möcker

Überwachungskameras, die Ihre Videostreams über vorhandene IP-Netze senden, machen die Heimüberwachung besonders einfach. Dennoch muss man sich bei der Einrichtung seiner Kamera nach wie vor entscheiden, wo man die Aufnahmen unterbringt. Viele IP-Kameras machen das nicht optimal. Sie speichern beispielsweise in der Cloud oder auf einer SD-Karte. Ist Erstere nicht erreichbar und Zweitere geklaut, sind die Aufnahmen verloren.

Die Lösung des Problems steht unter Umständen schon zu Hause im Technikschrank: Viele Netzwerkspeicher (NAS) werden per App-Nachrüstung zum NVR, ohne dass man zusätzliche Hardware kaufen muss. Bei den beiden größten NAS-

Herstellern Synology und QNAP erhält man die Surveillance-Station-Apps mit kostenlosen Lizenzen für je zwei Kameras. QNAP bietet zusätzlich QVR Pro mit 8 Lizenzen an. Wir haben uns die drei Angebote mit Fokus auf die Anforderungen von Heimnutzern angesehen und zeigen Ihnen, wo die Stärken und Schwächen liegen.

Kompatibilität

Grundsätzlich muss eine IP-Kamera für einen sinnvollen Einsatz am NAS direkten Zugang zu den Videodaten gewähren. Solche Modelle haben meist ein lokales Webinterface, über das sie sich konfigurieren lassen, und einen RTSP-Videoserver. Reine Cloud-IP-Kameras, die ihr Bild le-

diglich über eine Web- oder Smartphone-App liefern, eignen sich selten, da der Hersteller den lokalen Zugriff gar nicht erst vorgesehen hat.

QNAP und Synology brüsten sich auf ihren Websites mit über 4000 unterstützten Kameramodellen. Diese riesigen Listen entstehen nur, weil sich NAS- und Kamerahersteller an einen gemeinsamen Standard zur Steuerung der Kameras halten. Dahinter steht die Vereinigung von Sicherheitstechnikherstellern „Open Network Video Interface Forum“, kurz ONVIF. Das gleichnamige Protokoll definiert sechs sogenannte Profile, die je nach Anwendung verpflichtende und optionale Funktionen beschreiben. Der Austausch zwischen Client (NVR/IP-Kamera-Anwendung) und Server (IP-Kamera) erfolgt mittels XML über HTTP(S).

ONVIF Profil S ist das wichtigste Profil für IP-Videoüberwachung. Konforme Kameras müssen ihre Videodaten mindestens als Motion-JPEG-Stream bereitstellen, aber auch Zugang zu Benutzer-, Netzwerk- und Streaming Einstellungen gewähren. Gibt es Dreh-, Neige- und Zoommotoren (Pan, Tilt, Zoom; PTZ), müssen diese auch über ONVIF steuerbar sein.

Profil T ergänzt Profil S um die modernen Videocodecs H.264 und H.265, von denen die Kamera in mindestens einem enkodieren können muss, um konform zu sein.

Meist geben die Hersteller die Profile nicht separat an, sondern erklären lediglich ihre ONVIF-Kompatibilität und schreiben H.264 und H.265 als mögliche Codecs ins Datenblatt.

Installation

QNAP und Synology stellen ihre Network-Video-Recorder-Apps über die integrierten Paketverwaltungen (App-Center) im Webinterface der NAS bereit. Eine Anmeldung beim jeweiligen Hersteller verlangen sie nicht, die Apps lassen sich installieren, sofern eine Internetverbindung besteht.

Während die Surveillance Stations beider Hersteller auf allen aktuellen NAS-Modellen mit ARM- oder x86-Prozessor laufen, benötigt QNAPs neue App „QVR Pro“ zusätzlich die Container Station, die nicht für alle Modelle verfügbar ist. Außerdem empfiehlt QNAP mindestens 4 GByte Arbeitsspeicher. Zwar verweigert die App die Installation nicht, wenn weniger RAM verfügbar ist, Hilfe von QNAP im Problemfall sollte man jedoch nicht er-

warten. Eine Liste kompatibler NAS finden Sie in den Fußnoten der Container-Station-Webseite bei QNAP (siehe ct.de/y4wv).

Startet man die NVRs auf der NAS-Web Oberfläche, öffnet sich ein separater Browser-Tab mit einer Anmeldemaske. Hier erzählen beide Hersteller dem Nutzer nicht, dass er die gleichen Anmeldedaten wie an der NAS-Oberfläche verwenden kann.

QNAPs ältere Surveillance Station fragt nach der Installation zwar, in welchem Ordner die Videoaufnahmen landen sollen, lässt einen danach aber allein. Das kleine Fragezeichen am rechten Rand ist keine Hilfe: Das verknüpfte Hilfefenster erklärt lediglich, was sowieso schon zu sehen und klar beschriftet ist. Die Anleitung auf QNAPs Website findet man zwar per Suchmaschine, sie ist jedoch veraltet (August 2014) und passt an einigen Stellen nicht mehr zur Gegenwart.

Synology begrüßt im klassischen Fenster-Look und geht wesentlich einsteigerfreundlicher vor: Ein Hilfefenster öffnet sich sofort beim Login und lässt einen zwischen kompakt formulierten ersten Schritten inklusive aktueller Screenshots und einer ausführlichen Dokumentation wählen. Sie liefert gut geordnet und detailliert Erklärungen zu allen Funktionen der Anwendung.

QNAP hat sich bei der neueren NVR-App „QVR Pro“ wesentlich mehr Mühe gegeben: Die Anwendung übernimmt QNAPs übersichtliches Fenster-Design und hat ein Hilfe-Center. Die ersten Schritte sind etwas knapper gehalten als

bei Synology, helfen dennoch mit zielgerichteten Erklärungen gut weiter.

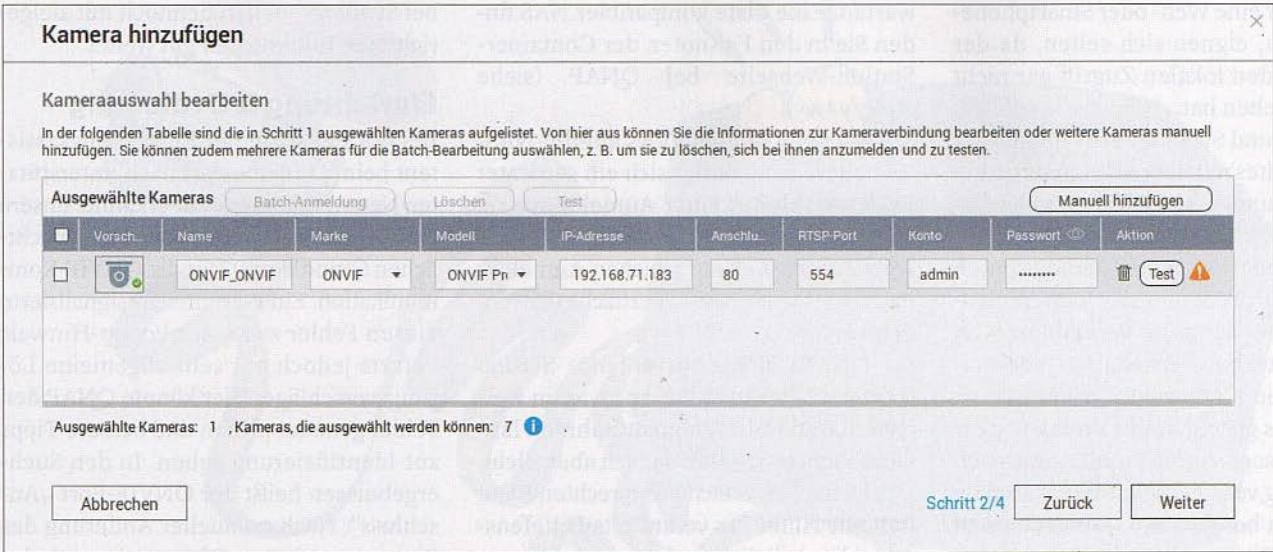
Einrichtung & Bedienung

In QVR Pro sucht der Einrichtungsassistent beim Öffnen sofort nach unterstützten Netzwerkkameras. Er erkannte unsere ONVIF-Kamera, wählte aber ohne ersichtlichen Grund Port 92 für die ONVIF-Kommunikation. Ein Warndreieck signalisierte diesen Fehler zwar, der Popup-Hinweis lieferte jedoch nur sehr allgemeine Lösungsvorschläge. Hier könnte QNAP den Fehler genauer prüfen und bessere Tipps zur Identifizierung geben. In den Suchergebnissen heißt der ONVIF-Port „Anschluss“. Nach manueller Änderung des Eintrags auf Port 80 verschwand das Warndreieck. Nachfolgend fragt der Assistent direkt, ob man die Aufnahmeeinstellungen anpassen möchte, sprich wie lange der NVR die Videodaten aufbewahren soll.

Um die Live-Bilder und Aufnahmen der Kameras abzurufen, benötigt man den QVR Pro Client für Mac, Windows oder Ubuntu, da das Webinterface keine Videoansicht bietet. Im Test unter Ubuntu zeigte sich die Software stabil und gut sortiert. Eingebundene Kameras weist man per Drag & Drop der Übersicht zu und die Funktion „Region von Interesse“ erzeugt aus großen Kamerabildern mehrere kleine Vergrößerungen in separaten Fenstern. Wer mehrere unterschiedliche Übersichten erstellen will, kann sie separat abspeichern. Benachrichtigungen und Warnungen vom NAS, wie Kamera- oder Festplattenausfälle, zeigt die Software ebenso.



Synologys Surveillance Station unterstützt Einsteiger mit einer ausführlichen Hilfe, die sich beim ersten Start automatisch öffnet.



Der Einrichtungsassistent von QVR Pro sucht Kameras automatisch im Netzwerk. Die erkannten Parameter kann man aber manuell anpassen.

Wie in QVR Pro hilft in Synologys Surveillance Station ein Einrichtungsassistent, und ONVIF-Kameras werden problemlos mit dem richtigen Port erkannt. Die Ansicht im Browser benutzt einen HTML5-Videooplayer, sodass kein browser- oder betriebssystemabhängiges Plug-in notwendig ist. Ab zwei Kameras wechselt der Player in die Mehrfachansicht. Wie in QVR Pro sind hier mehrere Layouts mit freier Kamerazuweisung einstellbar.

In QNAPs Surveillance Station trat bei der Einrichtung zunächst der gleiche Fehler wie in QVR Pro auf: Unsere Testkamera wurde auf Port 80 erkannt, erhielt jedoch Port 92 zugewiesen. Dies behoben wir erneut manuell. Dazu konnte die Anwendung die von der Kamera unterstützten Auflösungen oder Bildraten nicht ermitteln. Das leere Auflösungs-menü in Erwartung eines Ladevorgangs offen zu lassen, führte zum Absturz der Kameraverbindung, obwohl das Gerät im Netzwerk noch erreichbar war. Die Lösung brachte, das Kameraprofil manuell von „ONVIF Profile S Cameras“ auf „ONVIF Cameras“ zu ändern. Die Software hatte sich automatisch für das Profil entschieden, sodass die Videodaten im ineffizienten MJPEG-Modus abgerufen wurden.

Die NVR-App kommt auch nicht ohne Zusatzsoftware aus: Den benötigten QVR Client gibt es für Windows und macOS. Er bietet ebenso eine Mehrfachansicht, kann aber zusätzlich aus der Software auf die Kameraeinstellungen (auf dem NAS) zugreifen.

In puncto Aufnahmeeinstellungen nehmen sich die drei NVR-Apps nicht viel. Alle bieten Speichergrenzen nach Zeit oder Archivgröße in Gigabyte – sowohl individuell für jede Kamera als auch insgesamt für die ausgewählte Aufnahmefestplatte. Synology hat einen praktischen Speicherrechner, der anhand der Bitrate des Streams den durchschnittlichen Tages-Speicherverbrauch bei dauerhafter Aufzeichnung ausgibt.

Überwachungsfunktionen

Alle NVR-Apps bringen eine einfache Bewegungserkennung mit, die bei Veränderungen im Bild eine Aufzeichnung starten kann.

In Synologys Surveillance Station und QVR Pro ist dies gut gelöst: Für jede Kamera wählt man eine oder mehrere Bildregionen, in denen die Erkennung läuft. Die NVRs versenden Benachrichtigungen per SMS, E-Mail oder an die jeweilige Smartphone-App, auf Wunsch mit angehängten Fotos des Auslösemoments. QVR Pro weist jedoch eine Einschränkung auf, die gerade Besitzer neuerer IP-Kameras enttäuschen wird: Die Bewegungserkennung funktioniert nur bis zur Full-HD-Auflösung. Wer bereits eine 4K-Kamera hat, kann deren Videostream nicht in voller Auflösung auswerten. Das Problem kann man zwar lösen, indem man die Kamera mit niedrigerer Auflösung erneut einbindet, das kostet jedoch eine weitere Lizenz.

QNAPs Surveillance Station beherrscht keine eigenständige Bewegungs-

erkennung. Die Kamera muss die Bewegung erkennen und dies per ONVIF mitteilen. Gerade im günstigeren Kamerasegment erfordert die Einrichtung oft ein umständliches Internet-Explorer-Plug-in.

Synology trumpft mit tollen Zusatzfunktionen im Surveillance Station Client für Windows und Mac auf. Seine „Clever Suche“ erlaubt dem Nutzer beispielsweise, den genauen Zeitpunkt in den Aufzeichnungen festzustellen, zu dem ein Objekt aus dem Bild verschwunden oder



Synologys Smartphone-App „DSCam“ bietet mobilen Zugang zum NVR. Per HTTPS klappt das auch sicher aus dem Internet.

ein neues Objekt aufgetaucht ist. Die Live-Ansicht-Analyse erlaubt Gleiches für das Bild in Echtzeit. Beides klappt jedoch nur auf dem Client-Computer und ist bisher nicht auf dem NAS möglich.

Zusatzsoftware erhält man in Synologys Surveillance Station und QVR Pro über den integrierten App-Store. QNAPs Surveillance Station bietet keine Erweiterungen.

Während der Store in QVR Pro noch leer ist, bietet Synology eine Reihe kostenloser Erweiterungen, die sich primär an anspruchsvolle Nutzer richten. Der „Archive Vault“ spiegelt beispielsweise aufgezeichnete Videodaten auf eine andere Surveillance Station, um Datenverlust zu vermeiden. Sollen viele Clients gleichzeitig auf die Streams zugreifen, klappt dies mit „Live-Ansicht-Multicast“ netzwerk- und CPU-schonender.

Smartphone-Apps

Beide Hersteller bieten für ihre NVR-Anwendungen Smartphone-Apps für iOS und Android an. Wir haben sie unter Android ausprobiert. Alle können sowohl per HTTP als auch per HTTPS auf die Aufzeichnungen zugreifen, öffnet man die entsprechenden Ports im Router. So kommt man auch von unterwegs verschlüsselt an die Aufnahmen heran oder erhält Benachrichtigungen. Ein vollständiger Ersatz für die PC-Clients und Webinterfaces sind die Apps jedoch nicht, denn die Einstellungen der NVR-Anwendungen kann man nicht bearbeiten.

Synology bietet DS cam – der Client ist aufgeräumt und bietet über eine Zeitleiste und Untermenüs Zugang zu Aufzeichnungen und Schnappschüssen. Der „Home Mode“ steuert auf Wunsch per Smartphone-Geofencing die Alarm- und Aufzeichnungseinstellungen auf dem NAS, damit diese nicht unnötig ausgelöst werden, wenn der Besitzer zu Hause ist. Leider reduziert der Hersteller die Datenrate für die App nicht. Wer von unterwegs nach dem Rechten schauen möchte, muss viel Datenvolumen einplanen.

In QVR Pro ist dies auf den ersten Blick besser gelöst, denn die App bietet die Option, die Auflösung auf 640 × 480 Pixel oder 320 × 240 Pixel zu reduzieren. Damit bekamen wir aber nur noch ein übermäßig verpixeltes Bild alle 5 Sekunden, obwohl wir per WLAN im gleichen Subnetz auf das NAS zugriffen. Der originale H.264-Stream lief problemlos. Nach Registrierung des myQNAPcloud-

Accounts empfängt die App auch Benachrichtigungen vom NAS.

Die App für QNAPs Surveillance Station gleicht dem Nachfolger im Funktionsumfang fast vollständig. Das Layout wirkt altbacken, eine Mehrfachansicht gibt es auch nicht. Benachrichtigungen kann die App aber empfangen.

Betriebskosten

Alle NVR-Anwendungen bringen den Nachteil mit sich, dass sie die Festplatten dauerhaft beanspruchen – selbst wenn die Aufnahmeeinstellungen nur bestimmte Aufnahmezeiten oder Bewegungserkennung vorschreiben. Das NAS-Betriebssystem schickt die HDDs nicht in den Standby, wenn nichts vor der Linse los ist. Bisher können die NAS von Synology und QNAP auch nur alle oder keine Festplatte schlafen legen. Läuft eine NVR-Anwendung, bleiben also alle Festplatten an, selbst wenn nur eine beschrieben wird. Das Gerät fordert somit dauerhaft die Leistung, die Sie in c't-NAS-Tests als „idle“ in der Tabelle finden. Je nach NAS und Festplattenmodellen können dies 15 bis 30 Watt sein, also rund 40 bis 80 Euro pro Jahr.

Hinzukommt, dass klassische NAS-Festplatten nicht für den Dauerbeschuss mit Videodaten gedacht sind, sodass der Verschleiß höher und die Zeit bis zum Ausfall kürzer ist. Wer permanent auf-

zeichnen möchte, sollte in eine Surveillance-Festplatte investieren [1].

Fazit

Beide Hersteller liefern brauchbare Lösungen zur Abfrage von IP-Kameras. QNAPs Surveillance Station ist veraltet und vor allen Dingen vernachlässigt im Angesicht der neuen QVR Pro. Ihren primären Job erledigt sie zwar, die eigene Bewegungserkennung als übliche Funktion fehlt ihr aber.

QNAPs neue NVR-Anwendung wirkt besser durchdacht, kommt mit guter Dokumentation und im neuen Design. Besitzer von Einsteiger-NAS mit kleinem Arbeitsspeicher sind jedoch außen vor und müssen sich mit der alten Surveillance Station begnügen.

Die Heimüberwachung läuft am rundesten mit Synology. Die Surveillance Station läuft effizient und RAM-schonend auf allen aktuellen Modellen. Der Store bietet tolle Erweiterbarkeit, die Dokumentation macht es Einsteigern leicht.

(amo@ct.de) **ct**

Literatur

[1] Lutz Labs, Plattenkarussell, Festplatten für die Videoaufzeichnung, c't 18/2018, S. 92

Links und weitere Informationen:
ct.de/y4ww

Netzwerkvideorecorder für NAS

NVR-Apps	QNAP Surveillance Station	Synology Surveillance Station	QVR Pro
Version	5.1.3.4.4	8.2.2-5766	1.2.1.0
Preis	kostenlos	kostenlos	kostenlos
kostenlose Kameralizenzen	2 / 4 (best. große Modelle)	2	8
weitere Kameralizenzen	55 € (1 ×), 170 € (4 ×)	50 € (1 ×), 150 € (4 ×)	51 € (1 ×), 180 € (8 ×)
Eigenschaften			
ONVIF	✓	✓	✓
Videocodecs	MxPEG, MJPEG, H.264	MxPEG, MJPEG, H.264, H.265	MxPEG, MJPEG, H.264, H.265
Webplayer	–	✓	–
eigenst. Bewegungserkennung	–	✓	✓
Speicherung nach Tagen	✓	✓	✓
Speicherung nach Größe (GByte)	✓	✓	✓
Software			
NAS-Kompatibilität	ab QTS 4 (für aktuelle Version)	ab DSM 6.0 (für aktuelle Version)	mind. QTS 4.3.4
Desktop-Software	Windows, macOS	Windows, macOS	Windows, macOS, Ubuntu
Mobile-Apps	Android, iOS	Android, iOS	Android, iOS
Bewertungen			
Einsteigerfreundlichkeit	⊖	⊕⊕	⊕
Bedienbarkeit	○	⊕	⊕⊕
Funktionsumfang	○	⊕⊕	⊕
Mobile-App	○	⊕	⊕
Desktop-Software	○	⊕⊕	⊕
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden			



Anschlussbereit

Preiswerte Midi-Tower-Gehäuse mit USB-C-Anschluss

Viele Smartphones und schnelle externe SSDs nutzen bereits die verdrehsichere Typ-C-Buchse. Bei PC-Gehäusen hält der moderne Anschluss mit etwas Verzögerung nun ebenfalls Einzug, sodass man für USB-C nicht mehr umständlich hinter den Desktop-Rechner greifen muss.

Von Christian Hirsch

Langfristig löst USB-C den Wildwuchs bisheriger USB-Buchsen wie Typ A, Mini B und Micro B ab. Der Alleskönneranschluss erlaubt nicht nur schnelle Transfers per USB 3.1 Gen 2 und dem kommenden USB 3.2, sondern kann darüber hinaus Notebooks aufladen und Monitore mit Bilddaten versorgen. Inzwischen bieten bereits die Hälfte der aktuell angebotenen Mainboards für AMD Ryzen und Intel Core i an der I/O-Blende einen Typ-C-Anschluss, während PC-

Gehäusen mit dieser Buchse erst jetzt auftreten.

Für den Test haben wir vier Gehäuse im Midi-Tower-Format ausgewählt, die mit einem USB-C-Frontanschluss ausgestattet sind: Corsair Obsidian 500D, Fractal Design Define R6 Blackout, In Win 101C und Lian Li Lancool Digital One kosten zwischen 100 und 140 Euro. Sie nehmen Mainboards im ATX-Format auf, eignen sich zum Bau eines sparsamen Office- oder Allround-PCs gleichermaßen und bieten ausreichend Platz für High-End-Grafikkarten einer Gaming-Maschine.

Bei der Auswahl haben wir darauf geachtet, dass die Typ-C-Buchse jeweils intern den für diesen Zweck entwickelten 20-poligen Stecker verwendet. Nicht berücksichtigt haben wir preiswerte Midi-Tower, bei denen der Typ-C-Frontanschluss per Kabel durch die Gehäuserückseite geführt und außen an der I/O-Blende des Mainboards angeschlossen wird.

USB-C-Vielfalt

Der USB-Stecker vom Typ C wurde bereits Ende 2014 vom zuständigen Gremium Universal Serial Bus Implementers Forum (USB-IF) vorgestellt. Die für Anwender auffälligste Neuerung ist der symmetrische Aufbau. Im Unterschied zu den bisherigen USB-Buchsen passt der Stecker in beiden Ausrichtungen hinein. Bei schnellen SSDs, Docking-Stationen für Notebooks und Smartphones machen die Hersteller bereits reichhaltig Gebrauch von USB-C, erste PC-Gehäusen damit gibt es jedoch erst seit rund einem Jahr.

Das liegt unter anderem daran, dass die internen Steckverbinder für USB-C-Frontanschlüsse am Mainboard erst Anfang 2017 definiert wurden. Statt des bei USB 3.0 gängigen 19-poligen Pfostensteckers für zwei USB-Typ-A-Buchsen gibt es nun zwei geschirmte Buchsen mit 20 oder 40 Kontakten. Erstere unterteilt sich nochmals in zwei Ausführungen: die sogenannte Key-A-Variante, die für den Anschluss einer Typ-A- oder einer Typ-C-USB-Buchse taugt, und die dazu inkompatible Key-B-Version für zwei USB-A-Buchsen. Der interne Anschluss mit 40 Kontakten kann zwei Typ-C-Buchsen ansteuern – sowohl auf Mainboards als auch in PC-Gehäusen wird derzeit lediglich die 20-polige Key-A-Variante für eine USB-C-Buchse verwendet.

Einer der Vorteile des neuen internen Anschlusses ist die bessere Schirmung

gegen elektromagnetische Strahlung. USB-3.0-Transfers führen bei manchen Systemen zu Störungen im 2,4-GHz-Band von WLAN, denn die Basisfrequenz von USB 3.0 von 2,5 GHz liegt recht nah an diesem WLAN-Band (2,400 bis 2,483 GHz) – und am Frequenzbereich, der für Funkeingabegeräte wie drahtlose Mäuse genutzt wird.

USB-C-Optionen

Zudem stellt der moderne interne Konnektor 20 statt 9 Leitungen bereit [1]. Zwar benötigt USB 3.0 und die zweite Generation von USB 3.1 für Datentransfers mit 5 GBit/s (SuperSpeed) beziehungsweise 10 GBit/s (SuperSpeedPlus) die zusätzlichen Leitungen von USB-C nicht. Aber die moderne Typ-C-Buchse wird auch für andere Schnittstellen genutzt: Außer Thunderbolt 3 mit 40 GBit/s kann USB-C auch Bilddaten per DisplayPort und HDMI an Monitore übertragen, sofern die Geräte an beiden Enden des Kabelstrangs diese Funktion unterstützen. Dafür werden alle vier Leitungspaare von

USB-C benötigt. Gleiches gilt für kommende USB-3.2-Geräte mit 20 GBit/s Bruttotransfergeschwindigkeit [2].

Ein weiterer Bonus von USB-C: Stecker und Kabel sind grundsätzlich für eine Stromstärke von 3 Ampere spezifiziert. Dadurch laden beispielsweise Smartphones schneller. Über USB Power Delivery sind auch höhere Spannungen bis 20 Volt und stärkere Ströme bis 5 Ampere fürs Laden mit bis zu 100 Watt möglich. Das nutzen bereits viele Notebooks, es erfordert aber spezielle Kabel, die die höhere Leistung verkraften.

Für PC-Gehäuse spielen die zusätzlichen Möglichkeiten von USB-C derzeit noch keine Rolle, weil es kein Mainboard gibt, das am internen USB-C-Anschluss Power Delivery, DisplaySignale oder Thunderbolt ausgibt.

Wir haben bei allen vier Gehäusen die Transfergeschwindigkeit mit einer schnellen externen USB-SSD sowohl über Typ C mit USB 3.1 Gen 2 als auch über die jeweils zwei vorhandenen Typ-A-Buchsen mit USB 3.0 gemessen. Auffälligkeit

gab es dabei nicht: Alle Midi-Tower erreichten die zu erwartenden 1 GByte/s beziehungsweise 450 MByte/s. Wie stabil die Verbindung dabei ist, hängt von der Kabellänge und -qualität des Peripheriegeräts ab. Abhängig von der Schirmung des Kabels läuft das bei USB 3.1 Gen 2 mit 10 GBit/s auf eine Länge von 30 bis 60 Zentimetern hinaus. Das interne Anschlusskabel im PC-Gehäuse sowie die einzelnen Steckverbindungen zählen dabei mit. Gibt es Probleme, dass beispielsweise externe Datenträger die Verbindung verlieren, sollte man das Anschlusskabel für das Peripheriegerät durch ein kürzeres und besser geschirmtes Kabel ersetzen.

Gehäusetrends

Nicht nur bei Frontanschlüssen, sondern auch beim Aufbau der PC-Gehäuse hat sich in den letzten Jahren eine Menge getan. Um Platz für große Wärmetauscher von Wasserkühlungen zu schaffen, platzieren die Hersteller die Einbauposition für Netzteile nun mehrheitlich am

PC-Gehäuse mit USB-C-Buchse

Modell	Obsidian 500D	Define R6 USB-C Blackout	101C	Lancool One Digital
Hersteller	Corsair, www.corsair.com	Fractal Design	In Win, www.in-win.com	Lian Li, www.lian-li.com
Bauart / Format / Netzteilformat	Midi-Tower / E-ATX / ATX	Midi-Tower / ATX / ATX	Midi-Tower / ATX / ATX	Midi-Tower / ATX / ATX
Abmessungen (H × B × T)	50,5 cm × 22,8 cm × 50,7 cm	46,4 cm × 23,4 cm × 54,6 cm	44,7 cm × 23,0 cm × 47,5 cm	47,5 cm × 22,7 cm × 47 cm
Kensington-Lock / Schloss	n. v. / n. v.	n. v. / n. v.	n. v. / n. v.	n. v. / n. v.
Lüfter / -anschluss				
hinten	1 × 12 cm / 3-Pin	1 × 14 cm / 3-Pin	n. v.	1 × 12 cm / 3-Pin
vorn	1 × 12 cm / 3-Pin	2 × 14 cm / 3-Pin	n. v.	1 × 12 cm / 3-Pin
weitere Einbauplätze	oben: 2 × 12 / 14 cm, unten: 3 × 12 / 14 cm	oben: 3 × 12 cm oder 2 × 14 cm, unten: 2 × 12 / 14 cm	seitlich: 2 × 12 cm, unten: 3 × 12 cm	vorn: 1 × 12 cm, oben: 3 × 12 cm oder 2 × 14 cm, unten: 2 × 12 cm
Staubfilter	oben, unten, vorne	oben, unten, vorne	unten	vorne, unten
Einbaumöglichkeiten				
Laufwerke	2 × 3,5", 3 × 2,5"	1 × 5,25", 6 × 2,5"/3,5", 2 × 2,5"	2 × 2,5"/3,5", 2 × 2,5"	2 × 3,5", 4 × 2,5"
Erweiterungskarten	7 + 2	7 + 2	7	7 + 2
CPU-Kühlerrhöhe	17,5 cm	18,5 cm	16 cm	18 cm
Grafikkartenlänge	39 cm	31,5 cm (44 cm) ¹	43 cm	38 cm
Frontanschlüsse				
Power- / Reset-Taste	✓ / ✓	✓ / ✓	✓ / n. v.	✓ / n. v.
LEDs: Power / Festplatte	✓ / n. v.	✓ / ✓	✓ (RGB) / ✓	✓ (RGB) / ✓
Anschlüsse (Typ)	1 × USB 3.1 Gen 2 (C), 2 × USB 3.0 (A), 2 × 3,5 mm Audio	1 × USB 3.1 Gen 2 (C), 2 × USB 3.0 (A), 2 × USB 2.0 (A), 2 × 3,5 mm Audio	1 × USB 3.1 Gen 2 (C), 2 × USB 3.0 (A), 2 × 3,5 mm Audio	1 × USB 3.1 Gen 2 (C), 2 × USB 3.0 (A), 2 × 3,5 mm Audio
Zubehör				
Montagematerial	Klettstreifen, Kabelbinder	Kabelbinder	Kabelbinder	Kabelbinder
Handbuch	mehrsprachig	mehrsprachig	mehrsprachig	QR-Code für PDF-Download, mehrsprachig
Messwerte				
USB 3.1 Gen 2 Lesen / Schreiben	928 / 1060 MByte/s	960 / 1064 MByte/s	952 / 1064 MByte/s	1044 / 1085 MByte/s
USB 3.0 Lesen / Schreiben	450 / 462 MByte/s	450 / 462 MByte/s	450 / 462 MByte/s	452 / 467 MByte/s
Geräusch Lüfter	1,1 Sone (○)	0,7 Sone (⊕)	n. v.	0,8 Sone (⊕)
Preis	130 €	140 €	100 €	100 €
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden n. v. nicht vorhanden k. A. keine Angabe ¹ ohne Laufwerkschächte				



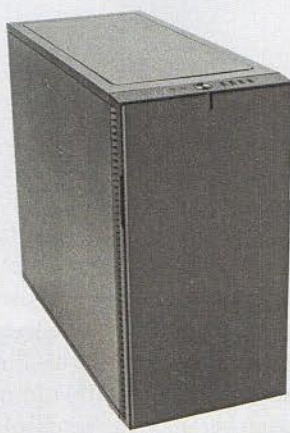
Corsair Obsidian 500D

Das Obsidian 500D eignet sich für zwei Anwendergruppen: Dank zweier getönter Glasseitenwände macht es die Bling-Bling-Fraktion glücklich, die ihre Hardware von RGB-LEDs beleuchtet im Blick haben möchte. Aber auch Bastler kommen auf ihre Kosten, denn die Seitenwände lassen sich wie Türen nach hinten wegklappen, ohne dass man dafür Schrauben oder Verriegelungen lösen muss. Sie halten ebenso wie die Staubfilter an Dach und Front magnetisch.

Wir empfehlen, die beiden 12-cm-Lüfter an die geregelten Anschlüsse des Mainboards anzuschließen, da bei voller Drehzahl das Lüfterrauschen in leiser Wohnumgebung mit 1,1 Sone deutlich zu hören ist. Hinter der Front und unter dem Dach lassen sich weitere Ventilatoren oder Wärmetauscher von Wasserkühlungen einbauen. Das Gehäusedach des Obsidian 500D ist fest mit dem restlichen Gehäuse verbunden, die warme Abluft kann aber durch einen etwa ein Zentimeter breiten Spalt zwischen Dach und Gehäuse entweichen. Für die Montage von Lüftern unter dem Dach gibt es deshalb im Inneren ein separates, abnehmbares Befestigungsblech.

Damit die Luft im Inneren möglichst ungehindert strömen kann, sitzen Festplatten und SSDs vertikal auf Schlitten auf der Rückseite des Mainboard-Trägers. Gut gefallen hat uns, wie Corsair die Kabel für die Frontanschlüsse unterbringt: Sie werden nicht nur durch Klettstreifen gehalten, sondern verschwinden zusätzlich hinter einer abnehmbaren Metallblende.

- Hardware leicht zugänglich
- Oberflächen aus Aluminium



Fractal Design Define R6 USB-C Blackout

Leser, die unseren Bauvorschlag für den Threadripper-PC aus c't 26/2018 nachgebaut haben, dürfte das Define R6 bekannt vorkommen. Als einziger Testkandidat bringt es hinter der gedämmten Aluminiumtür einen von außen zugänglichen 5,25"-Schacht für ein optisches Laufwerk oder einen Kartenleser mit. Auch sechs Schlitten für 2,5"- und 3,5"-Festplatten sind überdurchschnittlich viele, die sich zudem an elf unterschiedlichen Positionen befestigen lassen.

Um unter dem Dach Lüfter oder den Wärmetauscher einer Wasserkühlung einzubauen, kann man den Deckel auf Knopfdruck entriegeln und abnehmen. Die obere Abdeckung lässt sich von diesem Deckel entfernen, sodass die warme Abluft ungehindert aus dem Gehäuse aufsteigen kann.

Als Besonderheit bringt der Midi-Tower einen Lüfter-Hub mit, der das PWM-Signal von einem geregelten Mainboard-Anschluss an drei 4-Pin-Ausgänge weiterleitet. Zudem nutzt der Hub dieses Signal, um die Spannung von sechs 3-Pin-Ausgängen zwischen 5,5 und 12 Volt zu variieren. Die zwei mitgelieferten 3-Pin-Lüfter hinter der Front sowie der rückwärtige Ventilator mit jeweils 14 Zentimetern Kantenlänge laufen mit maximal 1000 U/min und sind dabei ungeregelt noch annehmbar leise (0,7 Sone). Schallschutzmatten an den Seitenwänden und der Fronttür dürften geräuschempfindlichen Naturen ebenfalls Freude bereiten.

- leise Lüfter
- viel Platz für Festplatten



In Win 101C

Allein schon durch seine mattweiße lackierte Oberfläche unterscheidet sich das In Win 101C von den übrigen PC-Gehäusen. Das Design ist sehr schlicht gehalten, so gibt es beispielsweise in Front und Dach keinerlei Lüfteröffnungen. Stattdessen lassen sich insgesamt fünf 12-cm-Ventilatoren hinter der rechten Seite oder am Gehäuseboden installieren. Diese muss man aber selbst besorgen, denn der Hersteller liefert keinen Lüfter mit.

An die Hardware gelangt man, indem man zwei Schnellverschlüsse an der linken Seitenwand aus Glas öffnet. Im Unterschied zu den meisten modernen Midi-Towern sitzt das Netzteil beim 101C oberhalb des Mainboards in einem separaten Abteil. Dahinter schließt sich ein Käfig mit zwei 3,5"-Schlitten an. Für lange, schwere Grafikkarten liegt dem Gehäuse ein Halter bei. CPU-Kühler dürfen maximal 16 Zentimeter hoch sein, weshalb einige sehr leistungsstarke Modelle nicht hineinpassen.

Anstelle einer üblichen Power-LED wird das Plexiglaselement mit dem Herstellernamen von RGB-LEDs beleuchtet. Um diese nutzen zu können, muss das Mainboard mit einem vierpoligen RGB-LED-Anschluss ausgestattet sein. Über eine Verzweigung lässt sich ein zusätzlicher RGB-LED-Leuchstreifen anschließen. Alternativ bietet In Win das 101C auch in schwarzer Farbe an.

- RGB-LED-Beleuchtung
- keine Lüfter dabei





Lian Li Lancool One Digital

Lian Li ist für Aluminiumgehäuse bekannt, bietet aber auch preiswertere Modelle mit Stahlskelett an, wozu das Lancool One Digital zählt. Ganz vom Aluminium lösen konnte sich der Hersteller aber nicht: Die Frontblende des Midi-Towers besteht aus gebürstetem, schwarz gefärbtem Aluminium. Für den optischen Wow-Effekt sorgen RGB-LEDs in der Mitte. Für diese benötigt man kein Mainboard mit RGB-LED-Anschluss und Steuerungssoftware, stattdessen lassen sich Farben und Wechselzyklen über einen Knopf an der Geräteoberseite umschalten.

Hinter der Front und auf dem Dach sitzen abnehmbare Staubfilter mit Magnethalterung. Ab Werk kühlen je ein 12-cm-Lüfter in Front und Heck die Hardware-Komponenten. Mit 0,8 Sone Lautheit bei maximaler Drehzahl empfiehlt es sich, sie an geregelten 3-Pin-Anschlüssen zu betreiben. Um einen Frontlüfter in der untersten Position zu installieren, muss man eine kleine Abdeckung am Luftkanal für das Netzteil abnehmen. Dann werden auch die beiden Festplattenschlitten mitgekühlt. An der Oberseite des Netzteilkanals lassen sich wahlweise zwei Lüfter oder zwei SSDs installieren. Die Position des hinteren Ventilators kann vertikal in fünf Stufen um insgesamt zwei Zentimeter verändert werden, um beispielsweise Platz für einen Radiator unter dem Dach zu schaffen.

Statt eines gedruckten Handbuchs liefert Lian Li nur eine digitale PDF-Version. Der Link ist als QR-Code auf der Packung des Montagematerials aufgedruckt.

-  RGB-LED-Beleuchtung
-  kein gedrucktes Handbuch

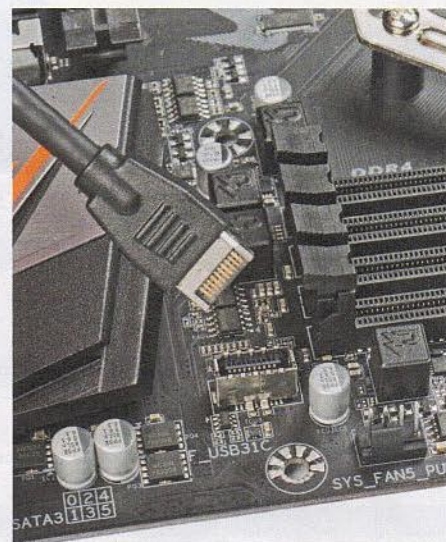
Boden. Das hat den positiven Nebeneffekt, dass der Netzteil Lüfter nicht direkt über dem Prozessorkühler sitzt und dessen heiße Abluft ansaugen muss. Stattdessen atmet er durch Staubfilter geschützt kühle Umgebungsluft durch Öffnungen am Boden ein. In vielen Gehäusen sitzt das Netzteil zudem in einem separaten Luftkanal mit den Laufwerken und bildet dadurch eine eigene thermische Zone. Auch ohne Wasserkühlung bringt die Anordnung Vorteile, weil die Abwärme von Prozessor und Grafikkarte ungehindert durch Öffnungen im Dach in Richtung der natürlichen Konvektion aus dem Gehäuse strömen kann.

Zudem verschwinden die von außen zugänglichen Einbauschächte für 3,5"- und 5,25"-Laufwerke. Im Zeitalter von Streaming-Anbietern wie Amazon, Netflix und YouTube sind optische Laufwerke für die Audio- und Filmwiedergabe auf dem Rückzug. Der Spieleverkauf läuft dank schneller Internetleitungen inzwischen ebenfalls zum Großteil über digitale Vertriebsplattformen wie Steam, Origin und Uplay. Und per USB angebundene Kartenleser sind auf dem Schreibtisch leichter zu erreichen als im Tower unter der Tischplatte.

Den frei gewordenen Platz hinter der Gehäusefront nutzen die Hersteller ebenfalls für Ansaugöffnungen und Einbauplätze für Lüfter oder Radiatoren. Zudem passen leistungsfähige Grafikkarten mit über 30 Zentimetern Länge leichter hinein. Im Vergleich zu den engen, zugestopften Midi-Towern von vor zehn Jahren wirken moderne Gehäuse regelrecht leer.

Ähnlich wie bei Autos wachsen sie aber in die Breite. So ist mehr Platz für große Prozessorkühler. Der früher ungenutzte Spalt zwischen Mainboard-Träger und rechter Seitenwand dient inzwischen als praktischer Stauraum für Strom- und Datenkabel. Damit die Leitungen von einer in die andere Gehäusahälfte gelangen, gibt es passende Öffnungen. Oft nutzen die Hersteller diesen Bereich, um dort platzsparend hochkant SSD-Halterungen unterzubringen.

Durch diese Änderungen ist das PC-Innenleben wesentlich aufgeräumter als früher. Transparente Seitenwände aus gehärtetem Glas gestatten passend dazu einen Einblick auf die PC-Hardware. Um diese noch besser in Szene zu setzen, tragen viele Speicherriegel, Grafikkarten und Mainboards beleuchtete Logos. Falls



USB-C-Buchsen hängen über einen geschirmten 20-poligen Anschluss am Board.

nicht schon im Gehäuse vorhanden, lassen sich RGB-LED-Streifen nachrüsten.

Fazit

In dieser Preisklasse kann man beim Kauf eines PC-Gehäuses nur wenig falsch machen. Für 100 Euro und mehr liefern alle Hersteller stabile Gehäuse mit hochwertiger Verarbeitung und funktionierender USB-C-Buchse. Trotz ähnlicher Abmessungen und auf den ersten Blick gleichem Aussehen setzt jeder Hersteller bei Ausstattung und Aufbau eigene Akzente.

Das Corsair Obsidian 500D gewährt Bastlern beispielsweise leichten Zugang zu den PC-Komponenten. Wer viele Festplatten unterbringen möchte, greift zum Fractal Design Define R6. Das In Win 101C richtet sich an Designliebhaber, die eigene Lüfter verwenden wollen. Mit seinen RGB-Effekten dürfte das Lancool Digital One von Lian Li in manchem Jugendzimmer für leuchtende Augen sorgen. Für die Zukunft wünschen wir uns, dass USB-C bald auch in preiswerteren PC-Gehäusen zur gängigen Ausstattung zählt. (chh@ct.de) **ct**

Literatur

- [1] Florian Müssig, Alles kann, nichts muss, Technische Hintergründe zu USB Typ C, c't 4/2017 S. 124
- [2] Florian Müssig, USB 3.2 kommt, Doppelte Datenrate, schnelleres Laden und höhere Sicherheit für USB-Verbindungen, c't 4/2019, S. 48



Cloud-Ableger

Zwei Apps für die digitale Aktenablage

Rechnungen einscannen, in Text verwandeln und digital speichern – das erleichtert den Büroalltag. Aber da geht noch mehr, und zwar mit den hier vorgestellten Apps.

Von Peter Schüler

Geschäftsbriefe aller Art bewahrt man im Unternehmen am besten digital auf – nicht nur, weil das für elektronische Dokumente sowieso Vorschrift ist und es naheliegt, sie gemeinsam mit anderen Unterlagen zu speichern. Weitere Argumente dafür sind, dass man Inhalte so schneller wiederfindet als in einem Aktenregal, und dass man sie auch von unterwegs sichten kann – vorausgesetzt, sie sind in einem

Cloudspeicher abgelegt. Um freilich eine Rechnung aus dem Kuvert auf die Festplatte zu übertragen, muss man sie zuerst scannen und dann – womöglich im selben Arbeitsschritt – den Inhalt in eine Form bringen, die systematische Recherchen und digitale Arbeitsabläufe ermöglicht.

Beim Test von Apps zum Digitalisieren herkömmlicher Schriftstücke (siehe c't 26/2018, S. 116 und c't 21/2018, S. 138) sind uns zwei Anwendungen aufgefallen, die sich durch passende Speicherfunktionen speziell für Geschäftsleute empfehlen. Dabei handelt es sich um die Kauf-App Docutain und das Hybridsystem fileee aus Gratis-App und Webdienst-Abo. Beide Anwendungen sortieren fotografierte Rechnungen und andere Geschäftsunterlagen mitsamt Begleitinformationen direkt in ein zugehöriges Dokumentenmanagementsystem ein.

Die Digitalisierung beginnt damit, dass man das Schriftstück fotografiert, die Software das Foto korrigiert und lokal speichert. Danach wird das Bild wie in den Kästen auf Seite 112 beschrieben bei Docutain automatisch, bei fileee in einem gesonderten Schritt einer Zeichenerkennung unterzogen.

Die Anwendungen verwenden die erkannten Texte in erster Linie für einen Index zur Volltextsuche. Das ist bequem und macht die Unterlagen leicht auffindbar. Textpassagen, die nicht richtig erkannt wurden, liefern keine Suchtreffer.

Immerhin kann man Unterlagen nicht nur anhand des Volltexts, sondern auch über Metadaten wie Absender, Datum oder Schlagwörter wiederfinden. Bei vielen Dokumentenmanagementsystemen ist die Eingabe dieser Informationen mühselig und wird vom Anwender oft übersprungen. Mit den hier vorgestellten Apps machen diese Eingaben dagegen nur ganz wenig Arbeit.

Testverfahren

Wie korrekt die Zeichenerkennung funktioniert, haben wir an Rechnungen überprüft, die wir wahllos aus dem Archiv der Redaktionsbuchhaltung entnommen haben. Die Versuchsanordnung zum Foto-

grafieren dieser Unterlagen war dieselbe wie in den oben genannten Artikeln – also wurden die Dokumente exakt parallel zur Papierebene und mit identischen Abständen und Beleuchtungsverhältnissen fotografiert. Als Testgeräte dienten ein iPad pro mit iOS 12.2 und für vereinzelte Stichproben ein Android-Tablet Huawei M3 mit Android 7.0. In Docutain lässt sich der erkannte Text über eine unscheinbare Schaltfläche anzeigen. In fileee gibt es keine solche Option, aber in der Premium-Variante dieser App konnten wir Dokumente als durchsuchbare PDF-Dateien exportieren.

Diese zeigen im Dateibetrachter unabhängig davon, welchen Text die Software erkannt hat, jeweils das Foto des Schriftstücks und enthalten den erkannten Text als unsichtbare Ebene. Wir haben diese Dokumente im Webbrowser Firefox geöffnet und mit Strg-A allen Text markiert. An der farbigen Hinterlegung zeigte sich dann, dass an manchen Stellen – etwa am Dokumentenrand – Textpassagen gar nicht analysiert worden waren, und bei den weit überwiegenden Bereichen mit erkanntem Text wurde nach dem Import in einen Editor erkennbar, welche Zeichen falsch erkannt worden waren. Obwohl die Volltextsuche deshalb nicht immer auf den kompletten Text zugreifen konnte, lieferte sie in allen unseren Stichproben korrekte Ergebnisse.

Beide Apps bieten keine unterschiedlichen Erkennungssprachen an, kamen im Test aber auch mit englischen Rechnungen klar. Nur an den handschriftlich ausgefüllten Posteingangsstempeln unserer Mustervorlagen scheiterten sie.

Wir haben die Fehlerraten anhand derselben sechs Referenz-Dokumente ausgezählt wie in bisherigen Tests. Die Erkennungsraten lagen etwa gleichauf mit den Ergebnissen der früher getesteten OCR-Apps, jedoch waren die Wörter der Musterrechnungen aus dem Archiv in den Textexporten zum Teil bunt durcheinandergewürfelt. Deshalb taugen die Volltexte nicht, um sie unkontrolliert etwa in ein Programm zur Auftragsbearbeitung oder Buchhaltung zu übernehmen.

Apps zur Aktendigitalisierung

App	Docutain	fileee Premium
Anbieter	Infosoft	fileee
nutzbar mit Android / iPhone / iPad	✓ / ✓ / ✓	✓ / ✓ / ✓
Erfassung		
Kamera / Datei	✓ / ✓	✓ / ✓
Bild drehen / automatisch / Bildaufbesserung	✓ ¹ / – / 3 Kontrastprofile	✓ / – / –
Erkennung		
OCR offline / online	✓ / –	– / ✓
Besonderheiten	Adressbuch	Formularerkennung, Adressbuch, Wiedervorlage, Verfalldatum, sicheres Cloud-DMS
Export		
Formate	PNG, PDF ² , TXT ²	PDF ² , PDF ³
Dienste	AirDrop, iMessage, iCloud, Dropbox, Google Drive, OneDrive + 8 weitere Cloudspeicher	fileee-Cloudspeicher
in vorhandenes Dokument / Zwischenablage	✓ / –	✓ / –
Dokumentenmanagement		
Speicherort / Verarbeitung	Mobilgerät / Mobilgerät	Mobilgerät, Web / Web
Inhalte	Dokumententyp, Absender, Schlagwörter, Datumsbereich, Steuerrelevanz, Volltext	Dokumententyp, Absender, Schlagwörter, Volltext
Sonderfunktionen	Adressbuch	sichere Weitergabe, Verfalldatum, Wiedervorlage, Formularerkennung, Adressbuch
Bewertungen		
Bedienung	○	⊕
Erkennung	⊕	⊕
Dokumentenmanagement	○	⊕
Ausgabe	⊕	⊕
Preis	Basisversion kostenlos, Premiumversion 2,99 € (Android) / 3,49 € (iOS)	Basisversion kostenlos, Premiumversion 4,99 € / Monat bis 200 Dokumente / Monat
¹ ohne Auswirkung auf OCR ² Premium- oder Pro-Version ³ nur als Bild ohne OCR		
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden		

Aktenverwaltung

Das Dokumentenmanagement haben wir jeweils auf dem iPad und bei fileee außerdem mit dem Webbrowser Firefox am Desktop-PC untersucht. Mit beiden Systemen lassen sich gespeicherte Dokumente bequem und zuverlässig wiederfinden. Mit fileee kann man die im Web gespeicherten Akten zudem verschlüsselt an Kollegen weitergeben, zur Wiedervorlage vormerken und mit einem Verfalldatum versehen.

Beide Systeme sind eher als Aktenablage denn als Speicher für regelmäßig überarbeitete Dokumente konzipiert. Sie bieten aber keinen Schutz vor heimlichen Veränderungen am Dokumentenbestand. Geschäftsleute müssen die digitalisierten Unterlagen daher zusätzlich in ein revisions-

sicheres Archiv kopieren, um Ärger mit dem Finanzamt vorzubeugen.

Fazit

Sowohl Docutain als auch fileee helfen wirksam, den geschäftlichen Schriftverkehr zu digitalisieren. Die Anwendungen ersetzen zwar kein revisionssicheres Archiv, wohl aber einen Dokumentenscanner und motivieren zur sofortigen Eingabe der wichtigsten Metadaten. Das Mietsystem fileee ist mit Webspeicher und Formularerkennung die elegantere und mächtigere der beiden Anwendungen, doch für einige Funktionen aufs Internet angewiesen. Wer ohne Netz und Abokosten auskommen und seine Unterlagen keinesfalls in der Cloud verarbeiten lassen will, ist bei Docutain richtig. (hps@ct.de) **ct**

OCR-Trefferquoten

App	Bestellung, optimal	Bestellung, schräg	DB-Ticket	Buchseite, optimal	Buchseite, Trapez	Buchseite, wellig
	[%] besser ▶	[%] besser ▶	[%] besser ▶	[%] besser ▶	[%] besser ▶	[%] besser ▶
Docutain	97	90 ¹	99	98	60 ²	99
fileee	98 ¹	99	80	98	99	70 ²
¹ Textpassagen durcheinander ² große Textbereiche nicht analysiert Die Balkenlänge entspricht jeweils dem Logarithmus des Werts (1 / (1 – Trefferquote)).						



Docutain pro

Mit Docutain fotografiert man ein Dokument und gibt unmittelbar danach Metadaten wie Dokumententyp und Absenderadresse ein. Letztere verwaltet die App in einem eigenen Adressbuch, aus dem man bekannte Adressen mit einem Fingertipp übernehmen kann. Außerdem lässt sich für jedes Dokument notieren, ob es steuerrelevant ist. Als Belegdatum trägt die App automatisch das Scandatum ein. Dieses kann man zwar von Hand durch das Belegdatum ersetzen, besser wäre jedoch, wenn es Felder für Scan- und Belegdatum gäbe. Die Zeichenerkennung läuft lokal im Hintergrund. Dadurch kann man ohne Rückgriff aufs Internet im Dokumentenbestand recherchieren.

Beim Fotografieren verhält sich Docutain etwas mimosenhaft: Zwar stellt es automatisch den Scanbereich ein und löst auf Wunsch sogar automatisch aus, sobald die Software meint, sie hätte ein Schriftstück korrekt im Visier. Nur leider muss man sehr genau mit der Ausrichtung von Dokument und Gerät zirkeln, damit auch der richtige Bereich erfasst wird. Andernfalls zeigt das gespeicherte Foto womöglich nur einen verzerrten Ausschnitt der Vorlage, weil die Software nur einen unregelmäßig viereckigen Ausschnitt erfasst und dann zu einem Rechteck „entzerrt“ hat. Eine Möglichkeit, den Erkennungsbereich festzulegen, besteht erst nach der Aufnahme – mitunter zu spät, um nicht erfasste Bereiche doch noch zu berücksichtigen. Daher brauchten wir auch mit unserer Testanordnung und reproduzierbaren Vorlagenpositionen bei manchen Schriftstücken mehrere Anläufe für ein korrektes Foto. Hat man diese Klippe überwunden, lassen sich Unterlagen mit Docutain sehr flott und bequem digitalisieren.

Das Dokumentenfoto kann man als iMessage oder als E-Mail-Anhang weitergeben, als nicht durchsuchbares PDF-Dokument exportieren oder in der Cloud hinterlegen. Über eine unscheinbare Schaltfläche öffnet sich zudem eine unformatierte Textansicht, aus der man Passagen etwa in eine E-Mail kopieren kann.

Docutain ist eine pragmatisch nutzbare digitale Aktenablage, die ohne Hilfe aus dem Internet auskommt, Sicherheitsunkritische Unterlagen aber auch in der Cloud bereitstellen kann. Verbesserungswürdig ist jedoch die Automatik zur Erkennung des Scanbereichs.

- 🟢 offline voll funktionsfähig
- 🔴 fummelige Fotoausrichtung
- 🔴 Belegdatum nicht erfasst

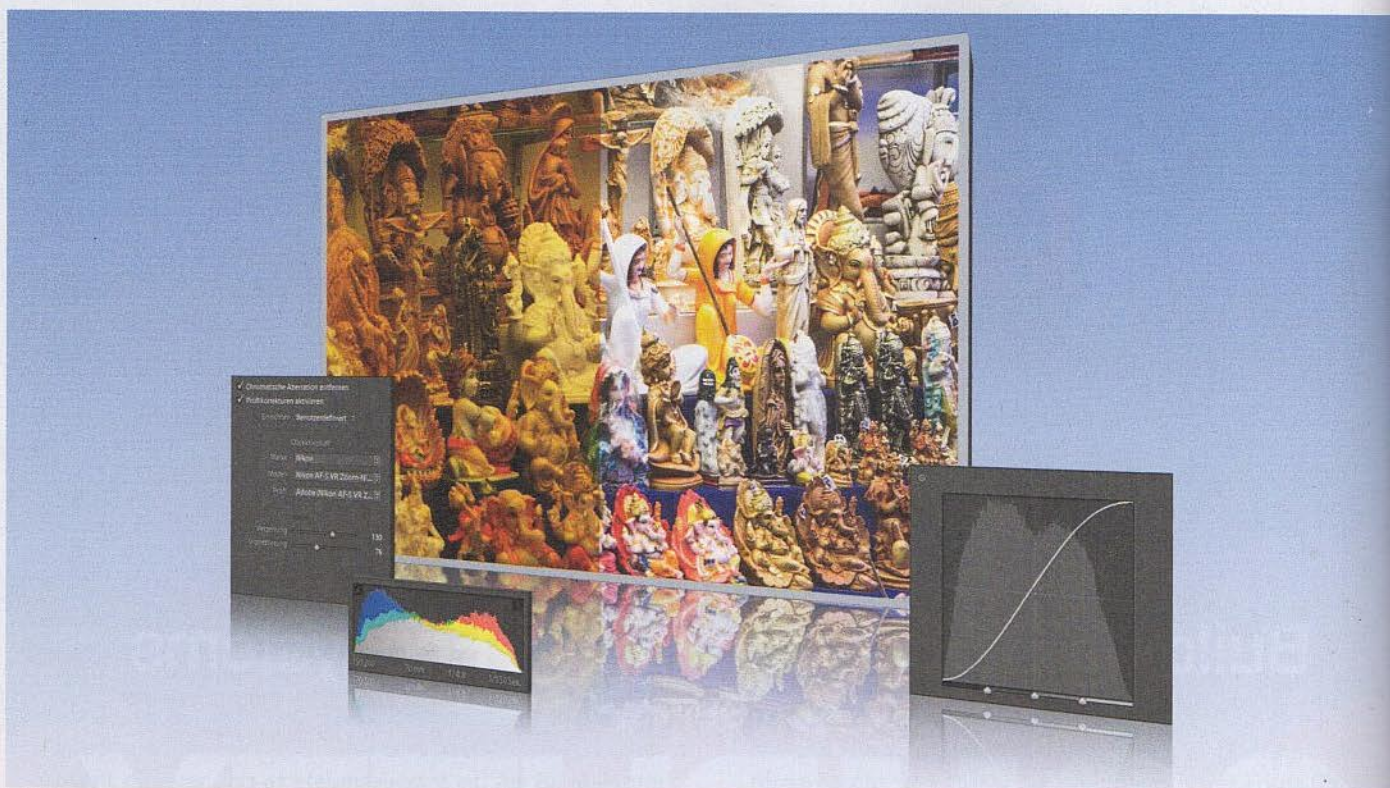


fileee

Der Hersteller fileee vermarktet unter demselben Namen eine iOS- und Android-App zur Dokumentenerfassung sowie ein zugehöriges webgestütztes Dokumentenmanagementsystem. Mit der App lassen sich Dokumente bequem fotografieren und halbautomatisch katalogisieren. Die Software identifiziert recht zuverlässig, welcher Bereich des Fotos für die Zeichenerkennung relevant ist – nur selten mussten wir die Grenzen von Hand korrigieren, was problemlos gelingt. Nach der Aufnahme genügen zwei Fingertipps, um das Dokument zu speichern und per Internet vom fileee-Server analysieren zu lassen. Dieser brauchte im Test 20 bis 50 Sekunden für die Zeichenerkennung in einem einseitigen Dokument und die gleichzeitige Identifikation von Eckdaten wie Dokumententyp, Absender, Datum, Rechnungsnummer und -betrag. Die vorgeschlagenen Metadaten waren in rund 70 Prozent aller Fälle korrekt. Die Software ließ sich nicht durch Währungs- und Datumsangaben in US-amerikanischen Rechnungen irritieren, wohl aber durch ungewöhnliche Layouts, etwa mit einer Datumsangabe unterhalb der Unterschrift. Schlimm ist das freilich nicht, denn fileee lässt sich seine Erkenntnisse ohnehin nach der Analyse vom Anwender bestätigen, sodass man nicht oder falsch erkannte Informationen sofort korrigieren kann. Schlecht ist dagegen, dass die Software mitunter manchen Text auf einem Dokument nicht analysiert, etwa in einer Fußzeile. Die Entwickler stehen aber zum Lernbedarf ihres Produkts und stiften Bonus-Speicherkontingente, wenn man ein Dokument anonym so hochlädt, dass sie es zum Training der Software nutzen dürfen.

Die App dient in erster Linie als Frontend des webgestützten Dokumentenmanagementsystems fileee.com. Ohne Netzwerkverbindung kann sie zwar die mit dem Gerät aufgenommenen Scans anzeigen und den Dokumentenbestand nach Metadaten und Volltext filtern. Die Zeichenerkennung und der Export eines durchsuchbaren PDF-Dokuments gelingen aber nur im Zusammenspiel mit der Webseite. Dokumente und Metadaten werden auf dem Server mit individuellen Passwörtern verschlüsselt. Ein gespeichertes Dokument kann man selektiv mit anderen fileee-Nutzern teilen, ein Einbrecher auf dem Server könnte es allenfalls dann lesen, wenn er das Anmeldepasswort eines berechtigten Nutzers kennt.

- 🟢 gute Scanauslösung
- 🟢 automatische Formularerkennung
- 🔴 umständliche Dokumentenverarbeitung



Zum besseren Bild

Acht nichtdestruktive Foto-Entwickler für schnellen Workflow

Foto-Entwickler wie Lightroom und Capture One wenden sich an Profis und Hobbyisten, die tief in die Materie einsteigen wollen. Für Gelegenheitsnutzer gibt es interessante und intuitiv bedienbare Alternativen. Einige sind kostenlos und laufen unter Windows, macOS und Linux.

Von André Kramer

Professionelle Fotografen bearbeiten jedes einzelne Bild minutiös bis ins Detail. Gelegenheitsknipser teilen ihre Fotos oft unbearbeitet auf sozialen Medien. Dazwischen gibt es ein breites Betätigungsfeld für begeisterte Hobbyfotografen. Denn schaut man mit kritischem Blick auf ein Foto, gibt es viel zu korrigieren: Hier ist der Himmel zu hell, dort der Schatten zu dunkel, mal das Rauschen zu stark, der Horizont schief oder der Kontrast zu flau.

Korrektur ist aber nicht alles: Digitalkameras produzieren zwar technisch immer bessere, aus kreativer Sicht aber leblose Fotos. Im vorigen Jahrhundert entschied die Filmauswahl über die Farbgebung. Die Packungen der Farbfilme von Fujifilm waren grün und die von Kodak gelbrot, weil das in etwa dem Look der damit produzierten Fotos entsprach. Die Farbgebung ließ sich mit Labortechniken wie Cross-Entwicklung und Bleach-Bypass auf die Spitze treiben. Im Digitalzeitalter braucht man keine Dunkelkammer mehr, um solche Effekte zu erzielen. Viele Raw-Entwickler bringen außer Korrekturfunktionen auch Effektfiler mit, die der klassischen Fotografie verpflichtet bleiben.

Die acht Programme im Test machen aus Kamerarohdaten fertig entwickelte Fotos, verleihen aber auch JPEG-Dateien den letzten Schliff. Sie wenden ein Set aus Einstellungen auf die Datei an, ohne die Pixel in der Raw-Datei selbst zu verändern. Dabei wechselt man von Bild zu Bild, bewegt die gewünschten Regler oder wendet Vorlagen an und exportiert erst am Ende alle Fotos in einem Rutsch. Ob

Raw oder JPEG – der Charme eines Foto-Entwicklers besteht verglichen mit Photoshop oder Gimp im schnellen Workflow, mit dem in Kürze eine Vielzahl Fotos bearbeitet ist.

Für Profis und Einsteiger

Im Test finden sich die Profiprogramme Lightroom CC beziehungsweise dessen Vorgänger Lightroom Classic CC von Adobe und Capture One Pro 12 vom dänischen Kamerahersteller Phase One. Verschiedene Hersteller haben ihre Programme anhand der Vorbilder zu vollständigen Raw-Entwicklern ausgebaut. Dazu gehören ACDSee Photo Studio Ultimate 2019, Alien Skin Exposure X4, DxO PhotoLab 2 und ON1 Photo Raw 2019. Alle bisher genannten Kandidaten stehen sowohl für Windows als auch für macOS zur Verfügung. ACDSee geht einen Sonderweg und entwickelt parallel das funktionseingeschränkte ACDSee Photo Studio für Mac 5. Die kostenlos erhältlichen Open-Source-Programme darktable 2.6 und RawTherapee 5.5 laufen unter Windows, macOS und Linux.

Obwohl die Kamerahersteller ihre Modelle stetig weiterentwickeln, ist deren Dynamikumfang immer noch nicht so hoch wie der des menschlichen Auges. Bei kontrastreichen Szenen muss man sich meist zwischen Detailzeichnung im Himmel und gut ausgeleuchteten Schatten entscheiden. Der Raw-Modus bietet da größtmöglichen Spielraum für Korrektur und Kreativität: Solange die Lichter nicht ausgefressen sind, kann man aus einer Raw-Datei noch einiges herausholen.

Raw-Dateien speichern Helligkeitswerte in bis zu 16 Bit Farbtiefe pro Kanal; üblicherweise legt die Kamera die Daten in einer Farbtiefe von 12 oder 14 Bit pro Kanal ab. Ein JPEG unterstützt mit 8 Bit Farbtiefe pro Kanal 256 Helligkeitsabstufungen; bei 14 Bit sind es über 16.000 Stufen mehr.

Fotos korrigieren

Alle Programme bieten Regler für die Grundeinstellungen Belichtung, Kontrast, Schwarz- und Weißpunkt, Lichter und Schatten sowie Sättigung. Den Weißabgleich korrigiert man am einfachsten mit einer Grauwertpipette. Den Tonwerten kommt man mit Gradationskurven und einem HSL-Dialog bei (Farbton, Sättigung, Luminanz).

Der aus Lightroom bekannte Regler „Klarheit“ erhöht den Kanten- oder Detailkontrast. Woanders heißt er Struktur oder Mikrokontrast. Die Lightroom-Funktion „Dunst entfernen“ verstärkt Kontrast sowie Sättigung und lässt damit Nebel verschwinden. „Dynamik“ beeinflusst die Sättigung auf nichtlineare Weise und wirkt sich vor allem auf ungesättigte Bereiche aus, ohne die bereits sehr farbigen zu überzeichnen. Alle drei Funktionen finden sich mittlerweile in den meisten Produkten.

Objektivprofile beschleunigen die Korrektur von Linsenverzerrung, Farbsäumen und Randabschattung. Hier tut sich vor allem DxO hervor. Der Hersteller misst unterschiedlichste Kamera-Objektiv-Kombinationen im Labor aus und korrigiert damit auch Bildrauschen. Lightroom bringt eine große Profildatenbank mit, die selbst Objektive von Smartphones und Action-Kameras umfasst. Capture One konzentriert sich auf Profi-Objektive; ACDSee, Exposure und ON1 Photo Raw liefern auch Profile für Einsteigerkameras mit.

Die DCP-Kameraprofile (DNG Color Profiles) von Adobe korrigieren Belichtung, Kontrast und Sättigung, um damit gezielt bestimmte Farbtöne zu manipulie-

ren. So kann man eigene Looks für Streetfotografie, Landschaft oder bestimmte Hauttöne erstellen. Solche Profile kann man auch selbst generieren, indem man eine Farbtabelle fotografiert und die Werte anschließend in einer DCP-Software korrigiert. In RawTherapee lassen sich DCP-Profile einbinden.

Hilfreich sind Werkzeuge zur Perspektivkorrektur, mit denen man die stürzenden Linien im Bild nachzeichnen kann. Die Software zieht sie im zweiten Schritt automatisch gerade. Solche Hilfslinien bieten Capture One, Lightroom und ON1 Photo Raw. Darktable hat eine gut funktionierende Automatik. Bei DxO kann man die Option für 79 Euro hinzukaufen. Bei den übrigen korrigiert man die Perspektive mit Reglern.

Selektiv bearbeiten

Fotos mit großem Dynamikumfang bearbeitet man am besten selektiv, beispielsweise indem man den Himmel abdunkelt und alles darunter aufhellt. ACDSee, Exposure, Capture One, Lightroom, PhotoLab und ON1 Photo Raw wenden unterschiedliche Einstellungssets auf Bildregionen an. Solche Bereiche definiert man mit einem Pinsel oder einem Verlaufsfilter. Der Verlauf verhindert harte Übergänge. Ein linearer Verlauf trennt das Bild beispielsweise entlang des Horizonts, ein radialer markiert das Hauptmotiv, um es dezent aufzuheben und vom Hintergrund abzuheben.

Die Retusche von Objekten ist eigentlich Aufgabe von Photoshop oder Gimp. Einen einfachen Reparaturpinsel bieten aber auch viele Raw-Entwickler. Meist



Lightroom gibt es in zwei Varianten. Außer dem Desktopklassiker hat Adobe ein Cloud-gestütztes Lightroom CC im Programm, das die Bibliothek online speichert und auch auf Mobilgeräten läuft.

eignet er sich zum Kaschieren von Pickeln oder Plastiktüten am Strand, nicht aber für komplizierte Arbeiten. In Lightroom kann man immerhin die Bildquelle verschieben, die die retuschierte Stelle überdecken soll. Bei allen anderen ist die Reparatur Glückssache.

Kreative Umsetzung

Zu den üblichen Effekten, die dem Foto einen individuellen Touch verleihen, gehören Vignettierung in Form heller oder dunkler Ränder, Filmkorn und Tonung in einer Farbe oder in zwei Tönen jeweils für Lichter und Schatten. Schwarzweißumsetzung sollte sich in mindestens sechs Farbbändern steuern lassen. Das umfasst in etwa das Effektspektrum von Lightroom, Capture One, ACDSee, darktable und RawTherapee.

Einige Testkandidaten kommen aus dem Umfeld von Effekt-Plug-ins für Photoshop und haben Raw-Entwicklung erst auf dem zweiten Bildungsweg dazugelernt. So hat Exposure von Alien Skin etliche Filmsimulationen an Bord, die dem Foto den Look von klassischen Diapositiv- und Negativfilmen in Schwarzweiß und Farbe verpassen. ON1 Photo Raw bringt eine Vielzahl von Effektfiltren mit, die Bleach Bypass und Cross-Entwicklung simulieren, den Kontrast erhöhen oder einen verträumten Weichzeichner übers Bild legen. DxO hat die Nik Collection von Google übernommen und bietet die bewährten Plug-ins nun zu einem Preis von 69 Euro für sein PhotoLab an. Außerdem kann man das FilmPack hinzukaufen, das ähnlich wie Exposure Analogfilme simuliert.



ACDSee Photo Studio 2019



ACDSee kam als Bildbetrachter und Bilddatenbank zur Welt. Den Foto-Entwickler hat der Hersteller später ergänzt. Dementsprechend spielt das Programm seine Stärken beim Sichten und Verwalten aus.

Aus den vier Varianten des Programms werden Uneingeweihte kaum schlau. Nur die Ultimate-Version bietet selektive Bearbeitung mit Ebenen, Masken und Überblendmodi sowie mithilfe von Frequenztrennung. Die Pro-Version für 114,99 Euro enthält den Raw-Entwickler, die Standard-Version für 68,99 Euro nur die Verwaltungsfunktionen.

Die Bildverwaltung bringt einen komfortablen IPTC-Editor mit. Sie unterstützt Bewertungen sowie Farbetiketten, die sich in andere Programme importieren lassen, und bringt ein eigenes Kategoriensystem mit. ACDSee erzeugt ohne weitere Aufforderung XMP-Begleitdateien inklusive aller Metadaten und erhält dabei Lightroom-Entwicklungseinstellungen. Neben Geotagging ist in Version 2019 auch Gesichtserkennung an Bord.

Im Raw-Entwickler trägt ein Pinsel Einstellungen von Lebendigkeit, Weißabgleich, Farbüberlagerung, Sättigung, Helligkeit, Farbton und Kontrast sowie der Gradationskurven auf. Die Schwarzweißumsetzung kann man in einem HSL-Dialog gezielt steuern. Besonders intuitiv arbeitet es sich mit dem Farb- und Licht-Equalizer. Man kann im Werkzeug die Kurve über das gesamte Helligkeits- beziehungsweise Farbspektrum bewegen und damit Belichtung und Sättigung selektiv bearbeiten oder mit der Maus einen Bildbereich im Vorschaufenster ansteuern und den Wert ändern, indem man den Mauscursor nach oben oder unten bewegt.

Der Bearbeiten-Modus bietet darüber hinaus Anpassungslayer für Belichtung, Kurven und anderes sowie Werkzeuge für Rote-Augen-Korrektur, Rahmen, Vignettierung und Verzeichnung. ACDSee legt solchermaßen bearbeitete Fotos in einem eigenen Dateiformat ab. Der Modus folgt nicht dem nichtdestruktiven Konzept eines Raw-Entwicklers und wirkt aufgrund seines umständlichen Workflows nicht mehr zeitgemäß.

ACDSee bringt einen soliden Raw-Entwickler mit, der aber mit Lightroom und Capture One nicht konkurrieren kann. Die Farben spielen oft ungewollt ins Bonbonhafte, nach großen Eingriffen in die Belichtung wirkt das Bild flau.

- umfangreiche Verwaltung
- schlechte Resultate bei tiefgreifender Bearbeitung



Alien Skin Exposure X4



Ursprünglich war Exposure ein Photoshop-Plug-in zur Simulation von Filmtypen und zum Ergänzen von schmutzigen Rändern, wie sie bei manueller Belichtung in der Dunkelkammer entstehen, von Lightlecks undichter Kameragehäuse, von Staub sowie von Kratzern, die entstehen, wenn man den abgerollten Film auf dem Laborboden hinter sich herschleift.

Mittlerweile ist ein Bildbrowser mit Bewertungssystem hinzugekommen, der XMP-Daten liest. Ihn hat der Hersteller Alien Skin zusammen mit der Filmsimulation in der linken Fensterleiste platziert. Sie enthält fast 500 Effekteinstellungen, unter anderem für Schwarzweißfilme von Agfa, Fuji, Ilford und Kodak, für Farbfilme wie Fuji Pro, Kodak Ektar und Kodak Gold sowie für Diafilme wie Fuji Provia, Fuji Velvia, Kodak Ektachrome und Kodachrome. Außerdem simuliert Exposure Dunkelkammernethoden wie Cross-Entwicklung. Die Filter sind in ihrer Ausprägung oft recht drastisch. Über die Ebenenpalette kann man sie maskieren und mithilfe eines Deckkraftreglers abschwächen.

Rechts findet sich zusammen mit den genannten Overlays für Rahmen, Lichtflecken und Dreck ein Raw-Entwickler mit Grundeinstellungen für Belichtung, Kontrast, Schatten und Lichter wie in Lightroom. Darüber hinaus bietet Exposure Paletten für Farbkorrektur, Teiltonung, Gradationskurven und Schärfe. Ferner fügt das Programm Vignettierung hinzu, die sich detailliert steuern lässt, und ergänzt auf Wunsch Bokeh. Dabei kann man die Form der Blendenöffnung wählen, auf die Intensität Einfluss nehmen und radiale oder lineare Masken nutzen, um die Unschärfe zu steuern. All das fasst Alien Skin mühelos in einer einheitlichen Oberfläche zusammen, ohne die Funktionen in viele Arbeitsbereiche zu zergliedern.

Exposure hat zahlreiche gute Effektfiler und Voreinstellungen an Bord, bekommt aber keine vernünftige Bildkorrektur hin. Der Regler für Belichtung übersteuert bereits auf halber Strecke und taucht das Bild in helles Weiß oder tiefes Schwarz. Die Funktion für Lichter und Schatten hingegen bewegen selbst auf Anschlag gezogen viel zu wenig, um die Zerstörung abzumildern. Die Einstellungen für Schwarz- und Weißpunkt verdienen den Namen nicht. Hier hat Alien Skin die Oberfläche von Lightroom kopiert, ohne deren Funktion nachbilden zu können.

- gute Effektfiler
- unbrauchbare Belichtungssteuerung



Capture One Pro 12



Herzstück von Capture One ist ein umfangreicher Raw-Entwickler, der leuchtende Farben und feine Details produziert. Capture One erhält die Farbgebung, was sich vor allem bei der Porträtbearbeitung positiv auswirkt, und arbeitet auch mit großen Dateien vergleichsweise schnell.

In jüngeren Jahren ist eine Bilddatenbank hinzugekommen. Von insgesamt zehn Reitern auf der linken Seite sind drei namens Bibliothek, kabelgebundene Aufnahme und Metadaten für die Verwaltung zuständig. Am rechten Bildrand zeigt eine Bibliotheksleiste den Inhalt eines ausgewählten Ordners. Mit Pfeiltasten kann man durch die Bilder wechseln und sie mit Zifferntasten bewerten. Ein Tastendruck erzeugt virtuelle Kopien, beispielsweise um eine Variante eines in Farbe entwickelten Bilds in Schwarzweiß zu entwickeln.

Im ersten von vier Entwicklungsbereichen bearbeitet man Perspektive, Farbsäume und Objektivverzerrung, im zweiten den Weißabgleich und Farbbalance, im dritten Belichtung, Kontrast sowie Klarheit und im vierten Bildschärfe, Rauschen und künstliches Filmkorn. Hier findet sich auch eine Ebenenpalette, in der man Farbe, Belichtung und Details selektiv mithilfe von Masken anwenden und über den Deckkraftregler deren Wirkung abschwächen kann. Seit der neuesten Version 12 muss man Masken nicht mehr pinseln, sondern kann radiale und lineare Verläufe ins Bild ziehen, was die selektive Bearbeitung deutlich vereinfacht.

Die Kopfzeile umfasst eine Symbolleiste mit Schaltflächen zum Rückgängigmachen des letzten Arbeitsschritts oder Zurücksetzen auf Anfang sowie diverse Werkzeuge. Dazu gehören die Hand zum Verschieben und die Lupe, um Details zu bearbeiten, aber auch intuitive Tools für Zuschnitt, Perspektivkorrektur und schiefen Horizont. Bei der Trapezkorrektur platziert man einfach zwei vertikale Striche entlang der stürzenden Linien, beim Geraderichten zieht man eine Linie entlang des Horizonts.

Ein zusätzlicher Arbeitsbereich fasst Bildstile für Schwarzweißumsetzung und Farbverfremdung zusammen. Fährt man mit der Maus über die Liste, sieht man im Dokumentfenster eine Vorschau. Ein Klick wendet den Effekt an. Die übrigen beiden erledigen Export und Stapelverarbeitung.

- sehr gute Farbwiedergabe
- hohe Arbeitsgeschwindigkeit

Für Softwerker

C. Ebert

Systematisches Requirements Engineering

Anforderungen ermitteln, dokumentieren, analysieren und verwalten

6. Auflage

2019, 496 Seiten

€ 39,90 (D)

ISBN 978-3-86490-562-9

NEU



E. Wolff

Microservices

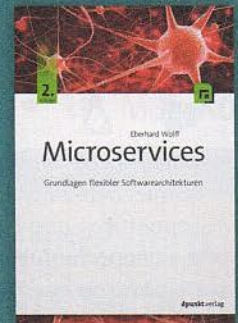
Grundlagen flexibler Softwarearchitekturen

2. Auflage

2018, 384 Seiten

€ 36,90 (D)

ISBN 978-3-86490-555-1



T. Weikiens · A. Huwaldt · J. Mottok · S. Roth · A. Willert

Modellbasierte Softwareentwicklung für eingebettete Systeme verstehen und anwenden

2018, 384 Seiten

€ 39,90 (D)

ISBN 978-3-86490-524-7



K. Hightower · B. Burns · J. Beda

Kubernetes

Eine kompakte Einführung

2018, 204 Seiten

€ 29,90 (D)

ISBN 978-3-86490-542-1



T. Geis · K. Polkahn

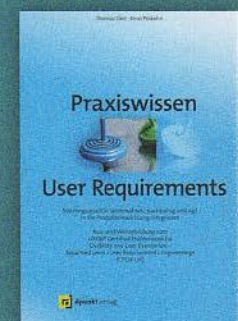
Praxiswissen User Requirements

Nutzungsqualität systematisch, nachhaltig und agil in die Produktentwicklung integrieren

2018, 220 Seiten

€ 32,90 (D)

ISBN 978-3-86490-527-8

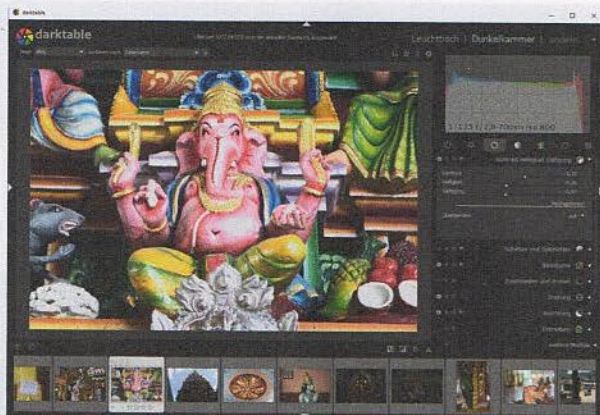


dpunkt.verlag

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

plus+

Buch + E-Book:
www.dpunkt.de/plus



Darktable 2.6



Darktable ist Open Source und steht für Windows, macOS sowie Linux zur Verfügung. Die beiden Hauptmodule heißen Leuchttisch und Dunkelkammer. Auf dem Leuchttisch kann man importierte Fotos zunächst vorsortieren und bewerten. Seit Anfang des Jahres besitzt darktable einen Duplikat-Manager, über den man verschiedene entwickelte Varianten eines Fotos anlegen kann.

Darktable schreibt Metadaten zwar als XMP-Begleiter, setzt die Endung aber hinter den kompletten Namen der Raw-Datei, statt deren Endung auszutauschen. Das ist unüblich und wird von anderen Programmen nicht gelesen, sofern man die Endung nicht manuell wieder ändert.

Zur Bearbeitung gehts in die Dunkelkammer. Die Beschriftung der Regler ist vergleichsweise klein und die Zeilen stehen eng, weshalb man sich an die Oberfläche erst mal gewöhnen muss. Auch die schiere Menge an Paletten erschlägt zunächst. Diese sind aber in sechs Reiter sinnvoll gegliedert und lassen sich in der Favoriten-Palette organisieren. Darktable bietet umfangreiche Funktionen, um die Helligkeitsbereiche fein zu steuern. Die Gradationskurve lässt sich im RGB- und im Lab-Modus verwenden. Eine Grauwertpipette fehlt; stattdessen zieht man für den Weißabgleich ein Rechteck im Bild auf.

In Version 2.6 hat darktable noch einmal kräftig aufgeholt. Die Basiswerkzeuge können beim extremen Aufhellen bonbonartige Farben produzieren. Außerdem treten bei tiefen Eingriffen leicht Halos auf – heiligscheinähnliche Artefakte an kontrastreichen Kanten. Beim neuen Werkzeug „filmisch“ passiert das nicht. Es soll den Look analoger Filme imitieren. Dessen Kern sind Gradationskurven. Kontrast, Sättigung und Belichtung lassen sich aber auch durch eine Vielzahl von Reglern fein steuern. Ebenfalls neu ist auch ein Korrekturpinsel zur Retusche von Bildfehlern. Er nutzt im Hintergrund Frequenztrennung, erhält also beim Kaschieren von Hautunreinheiten die Porenstruktur.

Darktable arbeitet zügig und erzielt gute Resultate. Die können sich zwar nicht mit Lightroom und Capture One messen, das Programm ist aber Open Source, somit kostenlos erhältlich, auch für Linux verfügbar und verdient daher einen eingehenden Blick.

- 🟢 feine Steuerung der Belichtung
- 🔴 unübersichtliche Oberfläche



Lightroom CC



Parallel zum klassischen Desktop-Lightroom entwickelt Adobe das Internet-gestützte Lightroom CC. Es steht nahezu funktionsgleich für Windows, macOS, Android und iOS sowie als Web-Anwendung zur Verfügung und speichert die gesamte Bibliothek in der Cloud. Getestet haben wir Lightroom Classic CC 8.1, dessen Funktionsumfang immer noch der Maßstab ist. Adobe bietet beide Ausprägungen ausschließlich im Abo für 11,89 Euro monatlich an. Dabei hat man die Wahl: Lightroom Classic CC, Photoshop CC und das neue Lightroom CC inklusive 20 GByte Cloud-Speicher oder nur das neue Lightroom CC plus 1 TByte Cloud-Speicher.

Die Bilddatenbank liest und schreibt Metadaten standardkonform im XMP-Format. Das Kartenmodul vergibt Geotags per Drag & Drop, die Gesichtserkennung arbeitet zuverlässig, allerdings sehr langsam. Leider lassen sich die Bibliotheken der beiden Lightroom-Varianten nicht sinnvoll in einem Workflow vereinen.

Kernstück beider Varianten ist das Entwickeln-Modul mit den Paletten Grundeinstellungen, Gradationskurve, HSL/Farbe, Teiltonung, Details, Objektivkorrekturen, Transformieren, Effekte und Kalibrierung. Damit stehen vielseitige Werkzeuge zur Verfügung, um saubere Korrekturen und vielfältige Looks zu erzielen. Hinzu kommen eine leistungsstarke Bereichsreparatur und selektive Entwicklung mit Maskierung über Pinsel sowie radialen und linearen Verlauf. Die Module für Fotobücher, Druckseiten und Web-Galerien gehören nicht zu den Glanzleistungen der Entwickler.

Über die Plug-in-Schnittstelle von Lightroom Classic lassen sich Programme wie Exposure, DxO PhotoLab und ON1 Photo Raw integrieren. Spezifische Funktionen wie Klarheit und Dunst entfernen kopieren andere Hersteller, weil Lightroom aufgrund seiner hohen Verbreitung die Referenz für andere Raw-Entwickler ist.

Bei der Profilkorrektur geht das DxO PhotoLab deutlich differenzierter zu Werk; Capture One kitzelt mehr Details aus den Raw-Fotos heraus. Lightroom setzt diesen Herausforderern eine vergleichsweise intuitive Oberfläche entgegen, mit der man seine Ziele schneller erreicht als bei der Konkurrenz. Mit wachsender Bildauflösung wird die Performance zum Problem, denn Lightroom arbeitet gerade bei Import, Export und Gesichtserkennung sehr langsam.

- 🟢 intuitive Entwicklungswerkzeuge
- 🔴 langsames Arbeitstempo



DxO PhotoLab 2



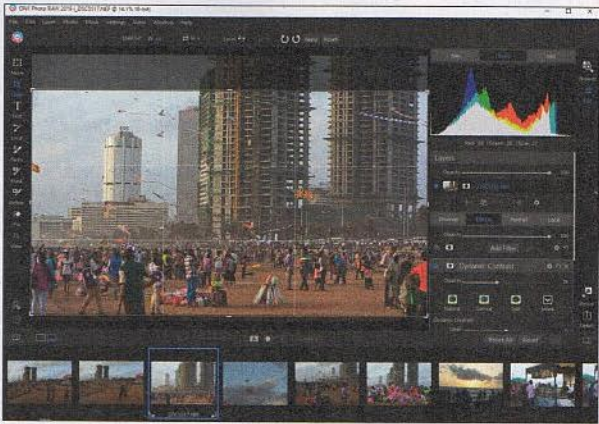
DxO baut auf sein Labor in Paris, in dem der Hersteller alle erdenklichen Kamera- und Objektivkombinationen ausmisst, um damit seine Korrekturalgorithmen zu füttern. Das PhotoLab, welches aus DxO Optics Pro hervorgegangen ist, lädt diese Profile bei Bedarf herunter und korrigiert daraufhin Verzerrung, Farbsäume und Vignettierung. Außer diesen Objektivmängeln mildert das PhotoLab auch Bildrauschen abhängig vom ISO-Wert. Die umfangreiche Profildatenbank wird stetig erweitert. DxO bietet das Programm in zwei Varianten an: einer 100 Euro kostenden für Einsteiger- und Mittelkameras und einer um 50 Euro teureren für Profigeräte.

Das PhotoLab 2 bringt eine einfache Bilddatenbank zum Bewerten, Sortieren und Filtern mit. Von der Fotothek gehts in den Bearbeiten-Modus. Über die Korrekturprofile hinaus nimmt die Software dem Nutzer eine Menge Arbeit ab. „DxO Smart Lighting“ korrigiert die Belichtung, „DxO ClearView Plus“ funktioniert ähnlich wie die Funktion „Dunst entfernen“ in Lightroom. Beide erzielen sehr gute Ergebnisse und arbeiten mehr oder minder automatisch. Das PhotoLab überzeugt mit Stabilität und flottem Arbeitstempo.

Der Workflow ist auf Automatik ausgelegt, man kann Belichtung, Schatten, Lichter, Kontrast, Mikrokontrast und andere Parameter aber auch über Regler sowie Gradationskurven beeinflussen. Eine Symbolleiste bietet Werkzeuge zur Korrektur schiefen Horizonts, roter Augen und anderer Probleme an. Hier finden sich auch eine Grauwertpipette und ein recht guter Reparaturpinsel. Für die selektive Korrektur hat DxO Niks patentierte U-Point-Technik implementiert: Mithilfe von Kontrollpunkten kann man Bildregionen markieren und damit Lichter von Schatten oder Objekte vom Hintergrund trennen. Für derart definierte Bildregionen lassen sich Belichtung, Kontrast, Tiefen, Lichter und andere Parameter selektiv einstellen.

Für Farbverfremdung, Schwarzweißumsetzung und andere Effekte hat das PhotoLab eine Reihe Presets zu bieten. Insgesamt sind die kreativen Möglichkeiten aber begrenzt. Dafür hat DxO andere Programme im Angebot, beispielsweise das Filmpack 5, das Fotofilme und Entwicklungstechniken simuliert. Auch diese Effekte basieren auf Laboranalysen der entsprechenden Filme. Darüber hinaus bietet DxO nun auch die Nik Collection unter anderem mit den Effektfiltern Analog Efex, Color Efex und Silver Efex zum Kauf an.

- sehr gute automatische Korrektur
- begrenzttes Effektangebot



ON1 Photo Raw 2019



ON1 Photo Raw ist aus einem halben Dutzend Photoshop-kompatibler Plug-ins entstanden, die nach und nach zu einem ebenso mächtigen wie unübersichtlichen Programm zusammenwachsen. Es wirkt bei jedem Wechsel in ein neues Modul wie eine völlig andere Software.

Beim Start erscheint der Bildbrowser mit Bewertungssystem, Suchfilter, umfangreichem Metadateneditor, Einbindung kabelgebundener Kameras und der Cloud-Dienste von Dropbox, Google und Microsoft. Ganz rechts oben wechselt man vom Bildbrowser (Browse) in den Bearbeiten-Modus (Edit). In letzterem präsentiert das Programm rechts Bedienelemente wie Paletten und Regler. Links stehen Werkzeugleiste, Presets oder Effektfiler zur Verfügung. Welche Bedienelemente rechts erscheinen, entscheidet die Wahl eines der vier Module „Develop“, „Effects“, „Portrait“ und „Local“. Nur im Effects-Modul sind links die Filter sichtbar. Bei Aktivierung des Faces-Werkzeugs aus der Leiste wechselt das Programm in das Portrait-Modul. All das ist genauso undurchschaubar, wie es sich anhört.

Die Regler zur Foto-Entwicklung arbeiten ausgewogen und überzeugend. Mit ihnen kann man Grundeinstellungen, Schärfe und Rauschen, Objektivfehler sowie Perspektive korrigieren. Um stürzende Linien zu begradigen, kann man ein Trapez aufziehen und den Rest der Software überlassen. Die Regler für Mitteltonkontrast und Dunst arbeiten sehr gut. Der Porträtbereich hilft mit halbautomatischer Gesichtserkennung bei der Retusche von Haut, Augen und Lippen. Der Bereich zur selektiven Korrektur hat ebenso umfangreiche Werkzeuge zu bieten wie Lightroom.

Hinzu kommen 27 Filter im Effects-Bereich, die auch Bearbeitungsstandards wie HSL-Dialog und Gradationskurven umfassen. Hier versammeln sich Klassiker wie Bleach Bypass, Schwarzweißumsetzung, Cross-Entwicklung, Glow-Effekt, Vignettierung, Filmkorn und Linsenreflexion. Die Filter lassen sich übereinanderstapeln und in der Deckkraft verringern. Im Layers-Modul direkt darüber lassen sich einfache Bildkompositionen erstellen.

ON1 Photo Raw ist das Programm mit dem größten Funktionsumfang im Test. Der Preis dafür ist eine inkonsequente Benutzerführung gepaart mit einer träge reagierenden Oberfläche.

- vielseitige Effektfiler
- kaum durchschaubare Oberfläche



RawTherapee 5.5



RawTherapee ist das zweite Open-Source-Programm im Test, welches nicht nur für Windows und macOS, sondern auch für Linux zur Verfügung steht. Der vorgeschaltete Bildbrowser samt Bewertungssystem, Farbmarkierungen und umfangreichem Filter zeigt den Inhalt auferufener Ordner recht zügig an. Leider schreibt RawTherapee keine XMP-Begleitdateien.

Ein Doppelklick auf ein Foto öffnet es im Editor. Über eine Zeile ganz links kommt man in den Browser zurück. Eine Filmstreifenansicht am oberen Rand erleichtert es, ein Bild nach dem anderen zu entwickeln. Die wichtigsten Entwicklungswerkzeuge organisiert das Programm in den Reitern Exposure, Detail, Color, Advanced und Transform. Die Werkzeuge sind vielseitig. Im Alltag benötigt man aber längst nicht alle und Neulinge verlieren hier leicht den Überblick.

Die Regler zur Belichtungskorrektur sowie für Schwarz und Weiß schießen schnell übers Ziel hinaus und produzieren Grauschleier. Der Dialog für Schatten und Lichter wiederum macht genau das, was er soll. Ein Plus sind die Gradationskurven im Lab-Modus, mit denen sich Farbe und Helligkeit getrennt voneinander behandeln lassen.

Auch im Detailbereich präsentieren sich die Funktionen in ganz unterschiedlicher Qualität. Schärfe und Mikrokontrast lassen sich fein dosieren, der lokale Kontrast erzeugt schnell unangenehmen HDR-Look. Der Farbbereichsfilter glänzt mit Grauwertpipette sowie umfangreichen Werkzeugen für HSL und RGB-Kurven. Unter „Transform“ kann man einen schiefen Horizont über eine ins Bild gezogene Linie korrigieren, muss die Perspektive aber per Regler ausgleichen. Objektivfehler behebt RawTherapee automatisch. Für nicht unterstützte Objekte lassen sich LCP-Profil von Adobe einbinden.

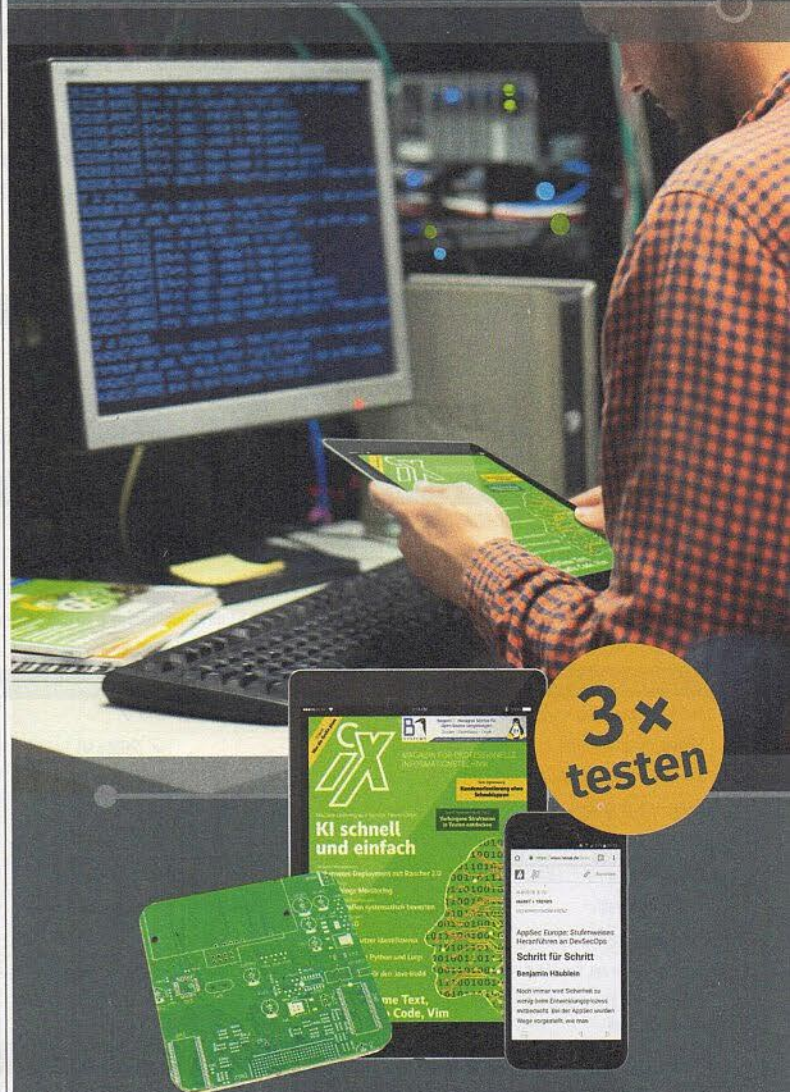
Die History-Palette in der linken Leiste fasst alle Änderungen zusammen und nimmt sie auf Wunsch wieder zurück. Eine Symbolleiste bietet Werkzeuge wie Beschnitt, Weißabgleichpipette und Rotation in 90-Grad-Schritten.

RawTherapee hat eine Menge Werkzeuge zu bieten, die ein Foto spürbar verbessern. Die Oberfläche räumt ihnen viel Platz ein, sodass sie sich komfortabel bedienen lassen. Allerdings arbeiten nicht alle Werkzeuge gleich gut. Die Korrektur von Schatten und Lichtern, die Gradationskurven und die Dialoge zur Farbbearbeitung führen aber zu guten Ergebnissen.

- vielseitige Werkzeuge
- unübersichtliche Oberfläche

Es gibt 10 Arten von Menschen.

iX-Leser und die anderen.



**3x
testen**

Jetzt Mini-Abo testen:

3 digitale Ausgaben + Leiterplatten-
Untersetter nur **14,70 €**

www.iX.de/test

iX
MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK



www.iX.de/test



leserservice@heise.de



49 (0)541 800 09 120

Verwaltung und Ausgabe

Die meisten Hersteller schalten ein Modul für Auswahl und Bewertung vor ihren Entwickler, denn nicht wenige Shootings und Urlaube hinterlassen 1000 Bilder oder mehr. Das Mindeste sollte ein Bildbrowser mit Fünf-Sterne-Bewertung und Farbetiketten sein, um die Fotos vorzusortieren. Wünschenswert sind Gesichtserkennung und Geotagging sowie ein Metadateneditor, der das Aufnahmedatum ändert und IPTC-Metadaten im Standard XMP

schreibt. Einige Programme unterstützen kabelgebundene Aufnahme im Studio, das Tethered Shooting.

Lightroom bringt eine mächtige Bilddatenbank mit. ACDSee bietet in Sachen Bildverwaltung ebenfalls viele Funktionen. Capture One ist auf diesem Feld noch nicht sehr weit. Bei darktable muss man sich an ein paar Eigenarten gewöhnen. Die übrigen Kandidaten beschränken sich auf einen Bildbrowser. Nach getaner Arbeit kann man in der Regel eine ganze

Sammlung von Fotos per Stapelverarbeitung als JPEG- oder TIFF-Dateien exportieren.

Fazit

Ob das Programm als Komplettlösung taugt, steht und fällt mit den Grundfunktionen zur Foto-Entwicklung. Capture One kitzelt auch das letzte Detail aus dem Bild heraus. Das DxO PhotoLab punktet mit sehr guten Automatikfunktionen für schnelle Resultate. Mit Lightroom bear-

Foto-Entwickler

Produkt	ACDSee Ultimate 2019	Exposure X4	Capture One Pro 12	darktable 2.6
Hersteller	ACDSee	Alien Skin	Phase One	darktable Team
Web	www.acdsee.com/de	www.alienskin.com	www.phaseone.com/	www.darktable.org
Sprache	Deutsch	Englisch	Deutsch	Deutsch
Systemanforderungen	Windows ab 7, macOS ab 10.12 (stark eingeschränkt)	Windows ab 7, macOS ab 10.10	Windows ab 7, macOS ab 10.11	Windows ab 7, macOS ab 10.7, Linux
Import und Export				
Import	Raw, DNG, HEIC, JPEG, PNG, PSD, TIFF	Raw, DNG, JPEG, PNG, PSD, TIFF	Raw, DNG, JPEG, PNG, PSD, TIFF	Raw, DNG, JPEG, PNG, TIFF
Export	JPEG, PNG, PSD, TIFF, WBP u. a.	JPEG, PSD, TIFF	JPEG, JP2000, PNG, PSD, TIFF u. a.	JPEG, JP2000, PNG, TIFF, WBP u. a.
Import / Export im Hintergrund	✓ / -	- ¹ / -	✓ / ✓	- / ✓
Integration in Bildbearbeitung	-	Photoshop ab CS6, Lightroom ab 6	-	-
Verhalten in Photoshop	-	erstellt neue Ebene als Kopie der aktiven Ebene	-	-
Foto-Entwicklung				
Farbtemperatur / Grauwertpipette	✓ / ✓ ²	✓ / ✓	✓ / ✓	✓ / ✓ (Grauwertrechteck)
Gradationskurven / HSL	✓ (RGB) / ✓	✓ (RGB) / ✓	✓ (RGB, Luma) / ✓	✓ (RGB, Lab) / ✓
Klarheit ³ / Dunst entfernen	✓ / ✓ ²	✓ / -	✓ / -	✓ / ✓
Lichter wiederherstellen	✓	✓	✓	✓
Entrauschen ⁴ / Schärfen	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Objektkorrektur mit Profilen	✓ ²	✓	✓ (für Wechselobjektive)	✓
Perspektivkorrektur	✓ (manuell)	✓ (manuell)	✓ (manuell und mit Hilfslinien)	✓ (manuell und automatisch)
Reparaturpinsel	✓ ²	-	✓	✓
Maskierung für sel. Korrektur	Pinsel, linearer und radialer Verlauf ²	Pinsel, linearer und radialer Verlauf	Pinsel, linearer und radialer Verlauf	-
Einstellungen übertragen / virtuelle Kopien	✓ / -	- / -	✓ / ✓	- / -
Effekte				
Schwarzweißumsetzung	✓ (acht Farbbänder)	✓ (mit Filmsimulation)	✓ (sechs Farbbänder)	✓ (virtueller Farbfilter)
Teiltonung	✓	✓	✓	-
Vignettierung / Filmkorn	✓ / ✓ ²	✓ / ✓	✓ / ✓	✓ / ✓
weitere Effekte	einfache Farbeffekte	Vorlagen für Infrarot, Lichtlecks, Alterung u. a.	Stile für Farbeffekte und SW	-
Filmsimulation	-	knapp 500 Presets für SW-, analoge Filme	-	-
Texturierung	-	Rahmen, Lichtlecks, Staub/Kratzer	-	-
Verwaltung und Ausgabe				
Bilddatenbank	umfangreiche Bilddatenbank	einfacher Bildbrowser	Bilddatenbank mit Tethered Shooting	Bilddatenbank mit Diashow und Tethered Shootinh
Geotagging / Gesichtserkennung	✓ / ✓ ²	- / -	- / -	✓ / -
Bewertung / Farbetiketten	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
IPTC-Editor / XMP-Export	✓ / ✓	✓ (einfach) / - (.exposure)	✓ / ✓	✓ / ✓ (.RAW).XMP)
Metadatenfilter	✓	✓	✓	✓
Farbmanagement	✓	✓	✓	✓
Bewertung				
Bedienung	⊕	○	○	⊖
Foto-Entwicklung	○	⊖⊖	⊕⊕	○
Effekte und Schwarzweiß	○	⊕	⊕	○
Preis	171,99 €	149 US-\$	349 €	kostenlos

¹ kein Import nötig ² nur unter Windows ³ auch unter dem Namen Kantenkontrast, Detailkontrast oder Struktur ⁴ Luminanz- und Farbrauschen ⁵ kostenpflichtiges Zusatzprogramm
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden - nicht vorhanden k. A. keine Angabe

beitet man viele Bilder in kurzer Zeit und erzielt Korrekturen auf sehr hohem Niveau. Das neue Lightroom CC bietet die Option, über die Cloud und damit auf iPad Pro, iPhone oder Android-Smartphone zu arbeiten.

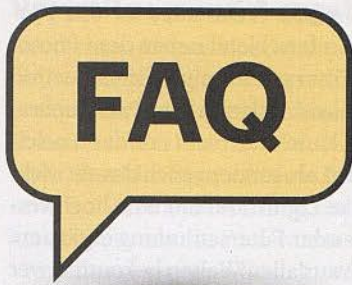
Bei darktable und RawTherapee muss man eine Weile herumprobieren, bis man aus der Vielzahl Funktionen eine gefunden hat, die dem Foto gut tut. Für Tüftler finden sich hier zwei Tools zum Nulltarif, mit denen man durchaus eini-

ges erreichen kann. RawTherapee punktet mit einer gut verständlichen Oberfläche, darktable geht etwas mehr in die Tiefe.

Alien Skin Exposure bekommt keine gute Foto-Entwicklung hin. ON1 Photo Raw wirkt langsam und träge. ACDSee macht seine Sache recht gut, der Schwerpunkt liegt aber auf der Verwaltung. Diese Programme wollen alles sein: Verwalter, Entwickler, Effektschmiede. Diese Rechnung geht nicht auf.

DxO packt nicht alles in ein Programm, sondern bietet neben dem PhotoLab die Filtersammlung Nik Collection und die Filmsimulation FilmPack separat an. Damit kann man nicht nur das haus eigene PhotoLab, sondern auch das entwicklungsstarke Lightroom um eine hochwertige Film- oder Filtersammlung ergänzen. Das Beste aus allen Welten bekommt, wer die Kandidaten geschickt im Team kombiniert. Leider ist die Nik Collection nicht mehr kostenlos erhältlich. (akr@ct.de) **ct**

Lightroom Classic CC 8.1	PhotoLab 2	ON1 Photo RAW 2019.1	RawTherapee 5.5
Adobe	DxO	ON1 Software	RawTherapee Team
www.adobe.com/de	www.dxo.com	www.on1.com	rawtherapee.com
Deutsch	Deutsch	Englisch	Englisch
Windows 10, macOS ab 10.12 (LR Classic CC auch unter Windows ab 7)	Windows ab 7, macOS ab 10.12	Windows ab 7, macOS ab 10.11	Windows ab 7, macOS ab 10.9, Linux
Raw, DNG, HEIC, JPEG, PNG, PSD, TIFF	Raw, DNG, JPEG, TIFF	Raw, DNG, JPEG, PNG, PSD, TIFF	Raw, DNG, JPEG, TIFF
JPEG, PSD, TIFF, DNG	JPEG, TIFF, DNG	JPEG, PNG, PSD, TIFF	JPEG, PNG, TIFF
✓ / ✓	✓ / ✓	– / ✓	– / ✓
Export nach Photoshop	Lightroom CC	PS ab CS6, PS Elements ab 14, Lightroom ab 6	Export nach Gimp und Photoshop
–	verrechnet Effekt mit aktiver Ebene	verrechnet Effekt mit aktiver Ebene	–
✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
✓ (RGB) / ✓	✓ (RGB) / ✓	✓ (RGB) / ✓	✓ (RGB, Lab) / ✓
✓ / ✓	✓ / ✓ (ClearView)	✓ / ✓	✓ / ✓
✓	✓	✓	✓
✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
✓ (auch für Smartphones)	✓ (umfangreich)	✓	✓ (unterstützt DCP-Profil)
✓ (manuell und mit Hilfslinien)	– (über Viewpoint) ⁵	✓ (manuell und mit Hilfslinien)	✓ (manuell)
✓	✓	✓ (und Porträtwerkzeuge)	–
Pinself, linearer und radialer Verlauf	Nik U-Points	Pinself, linearer und radialer Verlauf	–
✓ / ✓	✓ / ✓	✓ / ✓	– / –
✓ (acht Farbbänder)	– (über Nik Collection) ⁵	✓ (umfangreich)	✓ (virtueller Farbfilter)
✓	✓	✓	✓
✓ / ✓	– / –	✓ / ✓	✓ / –
Stile für Farbeffekte und SW	✓	24 Effekt-Filter enthalten	–
–	– (über FilmPack) ⁵	Filter „Black & White“	parametrische Simulation
–	–	Filter „Textures“ mit ca. 70 Overlays	–
Bildbrowser mit Tethered Shooting und Vergleichsmodus	Bildbrowser mit Bewertungen und Vergleichsmodus	Bildbrowser mit Vergleichsmodus und Tethered Shooting	Bildbrowser mit Stapelverarbeitung
✓ / ✓	– / –	– / –	– / –
✓ / ✓	✓ / –	✓ / ✓	✓ / ✓
✓ / ✓	✓ / – (.DOP)	✓ / ✓	✓ / – (.PP3)
✓	✓	✓	✓
✓	✓	✓	✓
⊕⊕	⊕⊕	⊖	○
⊕	⊕	○	○
⊕	⊖	⊕⊕	○
11,89 € pro Monat	129 € (199 € für Profikameras)	99,99 US-\$	kostenlos



Optimaler PC

Zu unseren PC-Bauvorschlägen erreichen uns regelmäßig Leser-anfragen zum Zusammenbau oder zur Auswahl der Teile. Antworten auf wichtige Fragen finden Sie in dieser FAQ.

Von Carsten Spille

Teiletausch möglich?

? Ich möchte gern eines der Teile Ihres Bauvorschlages gegen ein anderes tauschen. Ist das möglich?

! Natürlich – darum sind es ja auch Bauvorschl^äge. Sie sollten allerdings bedenken, dass dann je nach Art des Bauteils einige oder alle der von uns ermittelten Messwerte nicht mehr passen. Ein paar Beispiele: Die lautlose SSD können Sie tauschen, ohne dass die Lautheitsmessung ungültig wird. Beim CPU-Kühler dagegen sieht das anders aus. Hier sind mindestens die Geräuschemessung und die CPU-Temperaturen nicht mehr vergleichbar, möglicherweise aufgrund höherer Temperaturen auch die Leistungsaufnahme.

Auch das Mainboard spielt eine zentrale Rolle bei den ermittelten Werten. Es bestimmt überdies mit seinen Voreinstellungen der Lüftersteuerung und Konfigurationsmöglichkeiten im BIOS-Setup, ob etwa der Prozessor innerhalb seiner Spezifikation läuft. Auch bei den empfohlenen Grafikkarten raten wir dazu, auf die genaue Modellbezeichnung zu achten: Viele Hersteller bieten alternative Produkte mit sehr ähnlich klingenden Namen an, die sich zum Beispiel bei der Kühlung unterscheiden. Wo wir bei unseren Bauvorschl^ägen auf geringe Lärmentwicklung achten, kann sich ein Alternativmodell als wahrer Radaubruder entpuppen.

Kurzum: Sobald Sie wesentliche Komponenten des Bauvorschlages ändern, sind Sie in vielen Fällen auf sich allein gestellt – denn leider können wir Ihnen nur für einen Bruchteil der möglichen Austauschteile mit Rat dienen.

Nicht lieferbare Komponenten

? Eine der Komponenten ist nicht lieferbar – was nun?

! Nach Auswahl der Bauteile prüfen wir stets deren Verfügbarkeit und fragen dazu auch den Hersteller, ob diese eventuell bald nicht mehr lieferbar sind und durch Nachfolger ersetzt werden. Ist uns so etwas im Vorfeld bekannt, sehen wir uns nach einem anderen Produkt um. Sie können bei den Bauvorschl^ägen also davon ausgehen, dass es sich bei Lieferengpässen um eine kurzfristige Knappheit handelt, auch wenn Teile manchmal wochenlang nur schwer zu bekommen sind.

C-States einstellen

? Beim Intel-Bauvorschlag mit dem MSI Z390M Gaming Edge AC rät c't, bei den Package-C-States nur C6 einzustellen. Wäre C10 nicht besser?

! Da die C-States die Aktivitätszustände für den Prozessor und damit die Leistungsaufnahme regeln, haben Sie im Prinzip recht. In unseren Tests stellte sich jedoch heraus, dass mit C10-Einstellung die optionale Grafikkarte RTX 2070 nicht in den sparsamsten Powerstate wechselt und das System damit etliche Watt zu viel schluckt. Mit C6 tritt das Problem nicht auf und der Unterschied in der Leistungsaufnahme ist vernachlässigbar gering.

Lüftermontage

? Wieso versetzt Ihr den vorderen Gehäuselüfter des be quiet Pure Base 600 nach oben und lasst ihn absaugen? Braucht man für einen Luftstrom nicht auch einblasende Lüfter?

! Im Auslieferungszustand ist der Lüfter an der Front montiert und bläst tatsächlich Luft ins Gehäuse. Das ist am ehesten sinnvoll bei vollgestopften PCs mit mehreren schnell drehenden Festplatten in den Laufwerkskäfigen. Für unseren Bauvorschlag ist es sinnvoll, einen Wärmestau an den heißesten Komponenten zu vermeiden – das sind die CPU und die sie umgebenden Spannungswandler. Durch die Position der Gehäuselüfter in der hinteren oberen Ecke – weit weg vom Benutzer – wird der Luftstrom des CPU-Kühlers unterstützt und die Konvektion ausgenutzt. Der entstehende Unterdruck saugt durch die Gehäuseöffnungen ausreichend Frischluft an. So erreichen wir mit minimalen Drehzahlen und damit geringer Geräuscentwicklung den größten Kühlungseffekt.

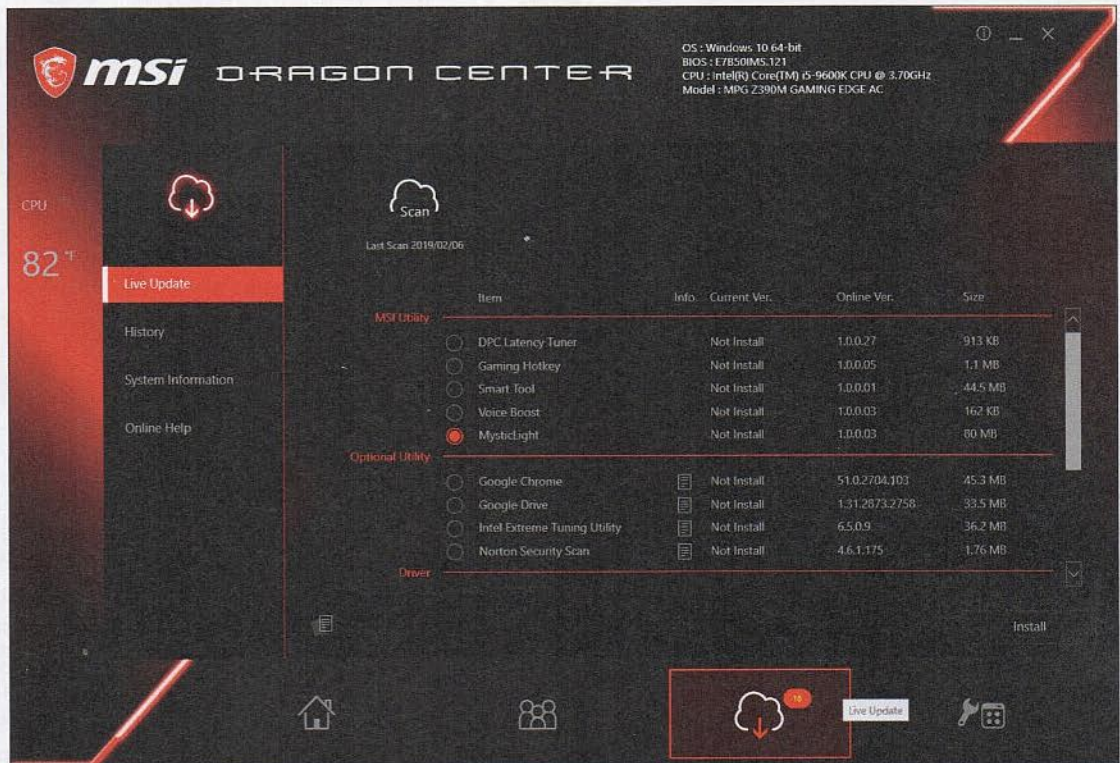
Mainboard-Stecker anschließen

? Das Netzteil des Intel-Bauvorschlages hat zwei vierpolige ATX-12-Volt-

Oben, hinten, möglichst weit weg vom Nutzer und die natürliche Konvektion ausnutzend: So haben wir die Gehäusebelüftung für unsere Bauvorschl^äge gewählt.



Die LED-Lichtorgel des MSI-Boards lässt sich nur in der haus-eigenen Software abschalten – dann aber dauerhaft.



Stecker. Wie schließe ich diese an das Mainboard an? Dort sind ein achtpoliger und ein vierpoliger Anschluss vorhanden.

! Die beiden vierpoligen Stecker vom Mainboard lassen sich kombinieren. Bitte verwenden Sie den zusammengeführte achtpoligen Stecker an CPU_Pwr1 und lassen Sie CPU_Pwr2 frei.

Netzteil-Leistung

? Ich möchte beim Allrounder-Bauvorschlag gern alle Register ziehen und sowohl den Achtkern-Prozessor als auch die RTX 2070 einbauen. Reicht das 500-Watt-Netzteil dann noch aus? Für die Grafikkarte wird online mindestens ein 550-Watt-Netzteil empfohlen. Andererseits: Wenn ich nur die Basiskonfiguration verwende, sind dann 500 Watt nicht überdimensioniert?

! Wir haben das empfohlene Netzteil mit der von Ihnen genannten Maximalbestückung unseres Bauvorschlages ausführlich getestet und keine Probleme festgestellt. Allgemeine Netzteilempfehlungen müssen immer auch billige Vertreter ihrer Art berücksichtigen, die ihre Spezifikationen vielleicht nicht so genau einhalten. Für die Basiskonfiguration brauchen Sie zwar kein 500-Watt-Modell, aber

der Unterschied in Sachen Leistungsaufnahme liegt bei weniger als einem Watt im Leerlauf. Dafür sind Sie dann auch bei einer späteren Aufrüstung mit einer energiehungrigen Grafikkarte auf der sicheren Seite und haben die nötigen Stecker parat. Übrigens: Auf die Variante mit Kabelmanagement verzichten wir bewusst, um potenzielle Fehlerquellen bei den Steckverbindern und deren Zuordnung zu vermeiden.

Mehr Speicher

? Für meine Anwendungszwecke benötige ich mehr Arbeitsspeicher. Kann ich auch 32 GByte in die Allrounder einbauen?

! Ja, das geht. Wir haben die Bauvorschläge auch mit Bestückung aller vier RAM-Steckplätze und folglich 32 GByte ausprobiert. Dabei traten keine Auffälligkeiten auf. Sofern Sie eine Vollbestückung planen, sollten Sie bei den Ryzen- und Threadripper-Bauvorschlägen die niedrigere spezifizierte Speichergeschwindigkeit beachten. Je mehr der logischen Speicherränge (Memory Ranks) bestückt sind, desto niedriger ist die offiziell erlaubte Geschwindigkeit. Bei Vollbestückung mit vier Modulen à zwei Rängen sichert AMD fehlerfreien Betrieb nur

noch für DDR4-1866 zu. Natürlich können Sie auf eigenes Risiko höhere Takt-raten ausprobieren.

LED-Beleuchtung stört

? Beim Intel-Bauvorschlag stören mich die LEDs und ich finde im BIOS-Setup keine passende Option.

! Leider gibt es diese Option tatsächlich weder im BIOS-Setup noch als Jumper auf dem Board selbst. Die Lösung liegt in der MSI-Software, die hat sich seit unserem Test allerdings etwas verändert. Innerhalb der Software „Dragon Center“ müssen Sie unter Live Update einen Scan durchführen, der dann die Installation des „Mystic Light“ anbietet. Dazu klicken Sie im Live Update auf „Scan durchführen“ und lassen dort das „Mystic Light“ installieren. Ist das Tool installiert, können Sie darin die LEDs abschalten – diese Einstellung bleibt unabhängig von Betriebssystem auch nach einem Neustart erhalten.

WLAN ausschalten

? Ich brauche das WLAN-Modul beim Intel-Allrounder nicht. Lässt es sich im BIOS-Setup abschalten und wird der

PC durch den eingesparten Treiber vielleicht sogar schneller?

! Nein und nein. Sie können den WLAN-Adapter nur im Windows-Gerätemanager oder unter Gnome im Network-Manager deaktivieren. Auf die Performance wirkt sich das Modul bei modernen Systemen wie dem Bauvorschlag nicht aus. Übrigens auch kaum auf den Stromverbrauch: Wir haben das WLAN-Modul im Rahmen unserer Tests herausgeschraubt und eine Verringerung der Leistungsaufnahme um nur 0,4 Watt gemessen. Ein großer Energieverschwender ist das Modul also nicht.

Luftkühlung beim Threadripper

? Ich möchte den Threadripper-Bauvorschlag umsetzen, habe aber Bedenken wegen der Wasserkühlung Enermax LiqTech TR4 II 240. Genügt nicht auch ein Luftkühler?

! Wir nutzen diese Wasserkühlung seit über einem Jahr für unser Threadripper-Testsystem. Mit ihr und auch anderen Kompakt-Wasserkühlungen haben wir bezüglich der Zuverlässigkeit und Dichtigkeit noch keine Probleme gehabt.

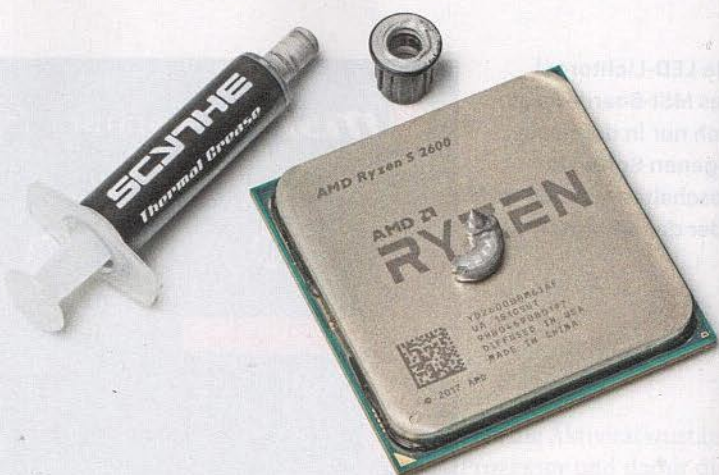
Wir haben uns beim Bauvorschlag bewusst für eine Wasserkühlung entschieden. Denn speziell bei einer zusätzlich verbauten Gamer-Grafikkarte erhöhte sich die Ansaugtemperatur im Gehäuse so stark, dass auch ein sehr leistungsfähiger Luftkühler den Threadripper nicht vor dem Drosseln unter Vollast bewahrt.

Einbauposition der SSD

? Sie geben bei den Bauvorschlägen unterschiedliche Möglichkeiten an, die SSD zu montieren: Die Rückseite des Mainboardträgers und einen der Festplattenkäfige. Hat das einen Grund?

! Nein, das ist gehupft wie gesprungen. Wir wollten nur ein paar mögliche Beispiele zeigen. Gerade bei SSDs, die auf bewegliche Teile verzichten und geräuschlos arbeiten, ist die Einbauposition den persönlichen Vorlieben überlassen: „Aus den Augen, aus dem Sinn“ hinter dem Mainbord oder gut zugänglich im Laufwerkskäfig in der Gehäusefront.

Kleiner Klecks, große Wirkung: Das Verteilen der Wärmeleitpaste auf der CPU übernimmt der Anpressdruck des Kühlers.



Bei Festplatten hingegen sollten Sie darauf achten, diese entkoppelt zu montieren – etwa mit dem optional empfohlenen Vibe-Fixer.

Einstellung am Netzteil

? Welche Einstellung empfehlen Sie beim Cosair-Netzteil für den Threadripper-Bauvorschlag bei den 12-Volt-Schienen?

! Ab Werk ist das Netzteil auf getrennte 12-Volt-Schienen konfiguriert und liefert dabei jeweils 40 Ampere pro Leitung. Das reichte in unseren Tests auch vollkommen aus.

Nach fest kommt ab?

? Wie fest muss ich die Schrauben anziehen, von denen der von Ihnen empfohlene Kühler Mugen 5 auf den Prozessor gepresst wird?

! Da der Anpressdruck durch die unterlegten Federn reguliert wird, sollten Sie die Schrauben bis zum Gewindeanschlag anziehen. Idealerweise drehen Sie jede Schraube reihum um zwei bis drei Umdrehungen.

Gehäuse-Lüftersteuerung ungenutzt?

? Das empfohlene Gehäuse der Allround verfügt über eine eigene, dreistufige Lüfterregelung. Sehe ich das richtig, dass die im Bauvorschlag gar nicht genutzt wird?

! Genau. Anstelle der grobstufigen Gehäuseregulierung lassen wir die Lüfter

lieber über das BIOS-Setup regeln. Das hat den Vorteil, jeden Lüfter getrennt voneinander einstellen zu können und vor allem, temperaturabhängige Drehzahlen vergeben zu können. Damit drehen die Quirle nur so schnell wie nötig und gehen nicht unnötig auf die Nerven. Außerdem ist dadurch kein manueller Eingriff, etwa für den Spiele- oder Renderbetrieb nötig.

Powerlimit Core i7/i9

? Welche Einstellungen für das Powerlimit 1 und 2 muss ich für einen Achtkerner wie den Core i7-9700K oder i9-9900K setzen?

! Wie der empfohlene Core i5-9600K sind auch die beiden Achtkerner 95-Watt-CPU's. Das bedeutet, ihre vom Hersteller Intel vorgesehene Leistungsaufnahme unter Dauerlast liegt langfristig bei 95 Watt. Kurzzeitig darf dieser Wert wie beim 9600K um 25 Prozent, also bis 118,75 Watt, überschritten werden. Die Einstellungen im BIOS-Setup sind für die drei Prozessoren also identisch.

Wärmeleitpaste

? Wie und wie viel der mitgelieferten Wärmeleitpaste muss ich auftragen?

! Für ein gutes Ergebnis genügt ein linsengroßer Klecks in der Mitte des Heatspreaders des jeweiligen Prozessors – egal ob Core i oder Ryzen. Empfehlungen, nach denen man eine hauchdünne, gleichmäßige Schicht über den kompletten Wärmedeckel verteilen soll, sind hauptsächlich für Übertakter relevant, bei denen es auf jedes Kelvin Temperaturunterschied ankommt. (csp@ct.de)

Tipps & Tricks

Sie fragen – wir antworten!

Schlechter Bluetooth-Codec am Galaxy S8

? Mein Galaxy S8 wählt bei meinem Bluetooth-Kopfhörer immer nur den klanglich schlechten SBC-Codec, obwohl sowohl Handy als auch Kopfhörer AAC unterstützen. AAC in den Entwicklereinstellungen zu erzwingen, hat auch nicht geklappt. Ist das ein Bug?

! Vermutlich haben Sie die Funktion „Dual Audio“ in den Bluetooth-Einstellungen des Handys aktiviert. Mit Dual Audio kann das Handy zwei Bluetooth-Audiogeräte zugleich mit Ton versorgen, aber das nur per SBC. Schalten Sie Dual Audio ab, dann klappt es auch mit den besseren Codecs.



Ist Dual Audio bei Galaxy-Smartphones aktiv, kann man keine hochwertigen Bluetooth-Audio-Codecs mehr nutzen

Allerdings muss das nicht unter allen Umständen eine Verbesserung bedeuten: SBC liefert zwar keine so hohen Kodieraten wie AAC oder APT-X, passt sich aber dynamisch an den Störpegel an und kann seine Kodierate nach Bedarf absenken oder erhöhen. Bei starken Störungen, beispielsweise durch WLAN, kann mit SBC deshalb eine bessere Klangqualität herauskommen als mit Codecs mit starrer Kodierate. (mls@ct.de)

Fußball-Streaming: DAZN läuft auf Samsung nicht

? Ich habe vor einer Weile den Sport-Stream von DAZN abonniert und der Empfang auf PC, Laptop, Tablet und Smartphone funktioniert reibungslos. Nun habe ich ein Samsung-Smart-TV der Serie Q7 dazu bekommen, für das es in Samsungs Store ebenfalls eine DAZN-App gibt. Obwohl ich mit dem Fernseher die maximal zulässige Anzahl von sechs Geräten nicht überschreite, klappt damit lediglich die Anmeldung – ich kann bisher keinen einzigen Stream abrufen und die App liefert die Fehlermeldung F11-064-011. Mache ich etwas falsch?

! In einigen Fällen hat es geholfen, die App zu deinstallieren und dann neu einzurichten. Falls Sie die App in der Start-Leiste verankert haben, entfernen Sie sie zunächst von dort, bevor Sie sie komplett vom Gerät löschen. Dabei werden auch die Zugangsdaten getilgt, sodass Sie diese nach der Neuinstallation erneut eingeben müssen.

Falls das keine Besserung bringt und Sie den Stream nicht vom Laptop via HDMI-Kabel auf den Bildschirm bringen wollen, nutzen Sie den im Smart-TV eingebauten Internetbrowser. Mit der Samsung-Fernbedienung lässt sich der DAZN-Dienst im Browser nicht ganz so bequem steuern wie in der DAZN-App, aber an-

sonsten funktioniert das Streaming-Angebot einwandfrei. Samsungs Browser merkt sich ebenso wie die App Ihren Nutzernamen und Ihr Passwort unaufgefordert, sodass Sie diese Daten nur bei der ersten Anmeldung eingeben müssen. (dz@ct.de)

ESP-Türklingel mit direktem Taster

? Ich würde den ESP-Türklingelwächter aus Heft 17/2018 gerne direkt mit einem potenzialfreien Taster verbinden und die Schaltung in einem Briefkasten unterbringen. Funktioniert das?

! Ihrer Idee steht nichts im Wege. Schließen Sie den Reset-Pin gegen Masse, erwacht der ESP aus dem Tiefschlaf und löst das Klingeln aus – das klappt auch über einen Schalter. Treten ungewollte Resets auf, agiert die Leitung zum Taster vermutlich als Antenne. Ein 10-kOhm-Widerstand zwischen Spannungspin (3,3 Volt) und Reset zieht den Pin sicher „High“, sodass ungewollte „Lows“ vermieden werden.

Da ein Briefkasten je nach verwendeten Materialien unter Umständen stark abschirmt, sollten Sie jedoch vor der Installation testen, ob der ESP im Briefkasten noch WLAN-Empfang hat. Der „Hello-Server“ in den ESP8266-Webserver-Beispielen aus der Arduino-IDE eignet sich dazu. (amo@ct.de)

Direktzugriff auf Sysinternals-Tools

? Sie haben in c't immer mal wieder darauf hingewiesen, dass man Sysinternals-Tools wie Autoruns, Process Explorer und Process Monitor nicht nur per Browser herunterladen kann, sondern auch direkt vom Sysinternals-Server im Explorer starten kann. Dazu trägt man

einfach den Netzwerkpfad `\\live.sysinternals.com` in die Adresszeile des Explorers ein, was bei mir auch jahrelang funktioniert hat – neuerdings aber nicht mehr.

! Das hat Sysinternals zwischenzeitlich geändert. Verwenden Sie als Pfad `\\live.sysinternals.com\tools`, dann funktioniert der Aufruf im Explorer wieder. (axv@ct.de)

MQTT auf der Kommandozeile

? Ich habe für meine Hausautomation einen MQTT-Server eingerichtet. Jetzt würde ich gern aus einem Linux-Shell-Skript MQTT-Nachrichten verschicken. Gibt es einen MQTT-Client ohne grafische Oberfläche?

! Unter Linux (zum Beispiel Ubuntu) reicht es, ein Paket zu installieren: `sudo apt install mosquitto-clients`. Mit

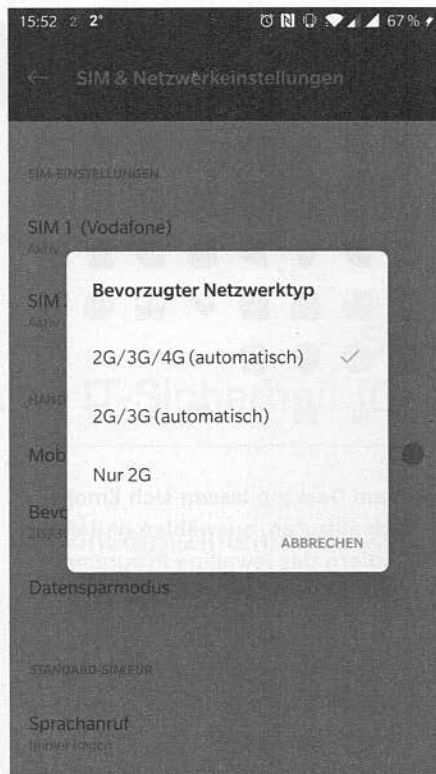
```
mosquitto_pub -h
<IP des Brokers>
-t meintopic -m "Test"
```

senden Sie eine Nachricht ab. (jam@ct.de)

Phantom-Verbindungen auf Mobilfunk-Rechnung

? Während meiner letzten China-Reise hatte ich wegen der hohen Kosten auf meinem Smartphone nicht nur Roaming deaktiviert, sondern die mobile Datenverbindung gleich komplett abgeschaltet. Trotzdem fand ich auf meiner Mobilfunkrechnung für jeden Tag meiner Reise mehrere „GPRS-Auslandsverbindungen“. Mein Provider hat mir die Beträge auf meine Reklamation hin wieder gut geschrieben. Wie aber kann so etwas passieren?

! Die Mobilfunkanbieter haben im LTE-Netz offenbar Schwierigkeiten, Signalisierungs- und Nutzdaten auseinanderzuhalten. Wenn Sie zuverlässig verhindern wollen, dass solche Phantomverbindungen auftauchen, sollten Sie beim Roaming die Nutzung des 4G-Netzes (LTE) im Menü komplett unterbinden. Auf Android-Geräten finden Sie diese Einstellungen unter „WiFi & Internet/SIM & Netzwerk/Bevorzugter Netzwerktyp“. Auf iOS-Geräten unter „Einstellungen/Mobiles Netz/Datenoptionen/LTE aktivieren“.



In den Einstellungen lässt sich LTE deaktivieren, um Phantomverbindungen im Roaming zu vermeiden.

Wenn Sie ohnehin keine Datenverbindungen nutzen wollen, hat das keine Auswirkungen auf den sonstigen Betrieb. Da viele Smartphones noch kein VoLTE unterstützen, müssen Netzbetreiber für Telefonate weiterhin flächendeckend 2G oder 3G vorhalten – diese Netze können Sie dann nutzen. Sie sollten sich aber einen Knoten ins Taschentuch machen, dass Sie nach Rückkehr in die EU das Netz wieder umstellen, sonst leidet die Performance der Datenverbindungen erheblich. (uma@ct.de)

Skript-Rechte und Schrift im Browser einstellen

? Ich möchte gerne JavaScript und das Erzwingen einer bestimmten Schriftart in meinem Browser schnell an- und abschalten können. Mein Arbeitgeber hat bei den Mitarbeiter-Rechnern über Policies die Einstellmöglichkeiten für Firefox und Internet Explorer beschränkt – nicht aber für Opera. Allerdings vermisste ich dort entsprechende Einstellungen. Kennen Sie eine Lösung für mein Problem?

! Diese Probleme sollten sich mit Browser-Erweiterungen lösen lassen. Die Auswahl im Opera-Store ist mit ungefähr 2500 Add-ons begrenzt, aber da Opera mit Chrome einen großen Teil des Codes teilt, funktionieren auch die meisten Erweiterungen aus dem riesigen Chrome Web Store – Sie müssen dafür nur „Install Chrome Extensions“ installieren.

Ein Ersatz für NoScript, mit dem Sie in Firefox die Rechte von Skripten auf Webseiten einschränken können, wäre zum Beispiel uMatrix. Anpassungen der Darstellung können Sie mit Benutzerskripten erzwingen. Das sind JavaScript-Dateien, die Sie für ausgewählte oder für alle Webseiten im Browser hinterlegen und welche unter anderem die Darstellung einer Webseite verändern können. Damit solche Benutzerskripte laufen, benötigen Sie in Opera Tampermonkey. Es gibt auch Erweiterungen, in denen Sie eigenes CSS hinterlegen können.

Auch wenn Sie einen „einfachen“ Browser suchen, könnte Vivaldi für Sie eine sinnvolle Alternative sein. Darin können Sie nämlich auch ohne Erweiterung Mindestschriftgröße und Schriftart festlegen (Einstellungen/Webseiten). Außerdem enthält er einen benutzerfreundlichen Lesemodus. Chrome-Erweiterungen funktionieren mit Vivaldi ebenfalls. Allerdings sollten Sie mit Ihrem Arbeitgeber klären, ob er keine Einwände dagegen hat, dass Sie seine Vorgaben umgehen. (Herbert Braun/uma@ct.de)

Browser-Erweiterungen: ct.de/ygjk

Digital, aber streifig

? Um alte Super-8-Filme digital zu überspielen, habe ich sie mit meiner Kamera abgefilmt. Der Projektor lieferte scharfe und helle Bilder auf der Leinwand, aber die digitale Aufnahme hat nervige dunkle Streifen, die quer durchs Bild laufen und sich von oben nach unten bewegen. Gibt es eine Software, mit der man diese Streifen wegbekommt?

! Die störenden Streifen entstehen durch eine mangelhafte Synchronisierung von Filmprojektor und Videokamera. Während der Projektor den Film mit typischerweise 18 Bildern pro Sekunde auf die Leinwand wirft, tastet die Videokamera mit 25 oder 50 Bildern pro Sekunde ab. In dem Moment, in dem der Projektor den

Filmstreifen ein Bild weiter transportiert, zeichnet die Videokamera einen dunklen Schatten auf, der sich als Streifen bemerkbar macht. Ihn nachträglich herausfiltern zu wollen, ist aussichtslos.

Besser zeichnet man erneut auf, stellt den Projektor auf 16 2/3 Bilder/s ein und synchronisiert seinen Bildwechsel mit dem der Videokamera. Da dies aber in den meisten Fällen nicht klappt, ist es sinnvoller, entweder einen preiswerten Filmscanner zu verwenden (Test siehe c't 4/2019, S. 130) oder – für besonders wertvolle Aufnahmen – einen auf solche Über spielungen spezialisierten Dienstleister zu bemühen. (uh@ct.de)

UEFI-BIOS aus der Eingabeaufforderung aufrufen

? Gibt es eine Möglichkeit, von Windows 10 ins BIOS-Setup zu wechseln, ohne den umständlichen Weg über das Startmenü, Shift-Taste + Neu starten, Problembearbeitung, Erweiterte Optionen, UEFI-Firmwareeinstellungen gehen zu müssen?

! Das BIOS-Setup können Sie auch über die Eingabeaufforderung aufrufen. Diese finden Sie mit Windows-Taste und dem Suchbegriff `cmd`. Mit Rechtsklick auf Eingabeaufforderung klicken Sie im Drop-down-Menü auf „Als Administrator ausführen“. Geben Sie nun den Befehl `shutdown /r /fw /t 0` ein. Der Parameter `/r` steht für Reboot, `/fw` für den Aufruf der Firmware-Oberfläche und `/t 0` für den sofortigen Neustart des Rechners.

Sobald Sie den Befehl mit Enter bestätigen, beendet Windows alle Programme, startet den PC neu und wechselt anschließend sofort in die Oberfläche der UEFI-Firmware. Vorher sollten Sie also alle offenen Dokumente speichern. Bei älteren Rechnern mit einem Mainboard von vor 2013, die noch das klassische BIOS und nicht das modernere UEFI verwenden, funktioniert der Tipp leider nicht. (chh@ct.de)

Emojis in Texten

? Ich möchte Emojis auch in Programmen verwenden, die dafür eigentlich nicht vorgesehen sind. In Instant Messengern sind Eingabemöglichkeiten vorgese-



Auch am Desktop lassen sich Emojis einfach aufrufen, auswählen und einfügen, sofern das jeweilige Programm mit den Zeichen umgehen kann.

hen, was aber ist beispielsweise mit Textverarbeitungsprogrammen?

! Die gängigen Desktop-Betriebssysteme bieten inzwischen auch Eingabemöglichkeiten für Emojis. Unter Windows ist es Windows+, unter MacOS Ctrl+Cmd+Leertaste. Alternativ kann man es als Unicode-Zeichen direkt eingeben, die meisten Zeichen finden sich in den Bereichen 1F600 und 1F900. Allerdings muss die verwendete Schriftart das Zeichen enthalten, sonst wird nur ein leeres Rechteck oder Ähnliches angezeigt. (uma@ct.de)

Zweikanal-RAM mit ungleichen Modulen

? Mein PC ist mit einem einzigen Speicherriegel bestückt. Nun möchte ich den Arbeitsspeicher aufrüsten und will sicherstellen, dass der Prozessor danach den schnelleren Zweikanalbetrieb nutzt. Muss ich dazu ein genau gleiches Speichermodul kaufen?

! Nein, nicht unbedingt, zumindest nicht bei PCs aus den letzten fünf bis zehn Jahren. Schon seit Pentium-4-Zeiten beherrschen viele Intel-Prozessoren den „Flexible Mode“: Wenn Sie beispielsweise ein Modul mit 8 GByte und ein zweites mit 16 GByte einsetzen, dann nutzt der Speicher-Controller die volle Kapazität des kleineren Moduls sowie dieselbe Kapazität des größeren Moduls im Zweikanal-Modus, im Beispiel also 16 GByte (2 × 8

GByte). Die restlichen 8 GByte laufen dann im Einkanalmodus. Somit kann der Prozessor beziehungsweise sein eingebauter Grafikprozessor (IGP) im größten Teil des RAM-Adressbereichs von der verdoppelten Transferrate profitieren. Das klappt auch beim AMD Ryzen und dem damit verwandten Athlon.

Der Flex Mode funktioniert allerdings nicht in jeder beliebigen Kombination von zwei Speicherriegeln. Wichtig ist, dass die beiden DIMMs in den Fassungen unterschiedlicher Speicherkanäle stecken – sonst ist nur Einkanalbetrieb möglich. Und man braucht einen Prozessor sowie ein Mainboard, die tatsächlich zwei Speicherkanäle anbinden und nicht bloß einen. Schließlich muss auch das BIOS mitspielen. Das sind allerdings alles Voraussetzungen, die auch für Zweikanalbetrieb mit gleichen DIMMs in beiden Kanälen gelten.

In besonders unglücklichen, aber seltenen Kombinationen von Speichermodulen versagt der Flex Mode, zumindest bei älteren Prozessoren. Mit einem simplen RAM-Benchmark wie dem „Memory Mark“ des Passmark (Testversion, Tests/Memory/Read uncached) können Sie die Transferraten vor und nach dem Einbau des zweiten Speicherriegels vergleichen. Im Zweikanalbetrieb sollte sie annähernd doppelt so hoch sein. Im Flex Mode ist der Zuwachs eventuell geringer, wenn der Benchmark auf unterschiedliche RAM-Bereiche zugreift und die Ergebnisse mittelt.

Grundsätzlich darf man von der höheren RAM-Transferrate keine Wunderdinge erwarten: Bei vielen typischen Desktop-Anwendungen puffern die Caches im Prozessor dermaßen viele Zugriffe ab, dass man vom schnelleren Speicher nichts merkt. Es ist also kein Beinbruch, wenn das RAM nur im Einkanalmodus arbeitet. (ciw@ct.de)

Fragen richten Sie bitte an

ct hotline@ct.de

f c't magazin

tw @ctmagazin

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter www.ct.de/hotline.

Sie fragen, ein Bot antwortet

Studien: Menschen fremdeln noch mit Chatbots

Immer öfter antworten Chatbots auf Ihre Fragen als Kunde oder Interessent. Das hat Vorteile, aber so richtig beliebt sind sie deshalb noch nicht.

Von Horst Schröder

Warteschleifen und -schlangen sollen kürzer werden. Das wünschen sich viele und offenbar würden viele dafür auch akzeptieren, wenn nicht ein Mensch ein Anliegen bearbeitet oder eine Frage beantwortet, sondern ein Chatbot. Das sind Computerprogramme, die einfache Dialoge mit Nutzern führen können – per Sprachdialog oder Messenger. Wie Computer-Avatare in Spielen sollen sie Eingaben richtig interpretieren und entsprechend reagieren. Sie könnten beispielsweise Änderungen von Kundendaten in einem Online-Shop oder bei Versicherern entgegennehmen oder auf die üblichen Fragen direkte Antworten liefern.

Unternehmen wie die Lufthansa, H & M sowie die Sparkassen hatten bereits früh eigene Quasselautomaten, und auch etliche andere haben Chatbots im Einsatz. Sie hoffen, damit zwei Fliegen mit einer Klappe zu schlagen: Intensiveren Kundenkontakt bei gleichzeitig sinkenden Ausgaben dafür – so ein Bot schläft nie.

Chatbots kommen zunehmend in Banken zum Einsatz und zwar besonders bei Direktbanken ohne eigenes Filialnetz, das ihre Kunden nutzen könnten. Aber auch Filialkunden, die ihre Finanzgeschäfte am Computer erledigen, haben zunehmend mit Chatbots zu tun. Sie nehmen nicht bloß einfache Aufgaben wie Kontostandabfragen entgegen, sondern beraten schon jetzt oder bereiten eine Beratung zumindest vor.

Am ehesten trifft man über Messengerdienste auf Chatbots, etwa im Facebook-Messenger. Und das immer öfter: Im April 2017 gab es 100.000, im Januar 2018 schon 200.000 und aktuell sind es

mehr als 300.000 Chatbots allein auf Facebook, wie die US-Website VentureBeat herausfand. Die MessengerPeople-Studie des Markt- und Meinungsforschungsinstituts YouGov aus dem Oktober 2018 stellt heraus, dass mehr als 10 Millionen Nutzer solche Dienste verwenden. Anscheinend funktionieren Chatbots im Messenger-Fenster vielfach bloß als Briefkästen, sodass nur 38 Prozent tatsächlich sofort beziehungsweise innerhalb eines Tages Antwort bekommen haben.

Das US-Unternehmen Liveperson hat die grundsätzliche Haltung zu Chatbots in verschiedenen Ländern erfragt (siehe Bild). Zur Frage, wozu sie ihn nutzen wür-

den, sagten 64 Prozent der in Deutschland Befragten: in erster Linie zur Terminvereinbarung, was allerdings 15,4 Prozent auf keinen Fall wollen. Etwas mehr als die Hälfte aller Teilnehmer der Umfrage geben einem sprachunkundigen oder lahmen Chatbot kein Pardon und verlangen daher bei Verständnisproblemen sofort menschliche Gesprächspartner. Gerade an der Mehrsprachigkeit von Chatbots hapert es noch.

Zwischen Hoffen und Bangen

Dennoch: Eine YouGov-Befragung von 997 Briten fand, dass Chatbot-Nutzer es zu gut 60 Prozent gut fanden, nicht von Telefon- oder Öffnungszeiten abhängig zu sein und nicht in der Warteschleife zu landen. In Deutschland fragte YouGov ebenfalls. Im Juni wollten nur 6 Prozent der 1164 Befragten auf jeden Fall mit einem Chatbot sprechen. 21 Prozent sind nicht ganz abgeneigt. Etwa 60 Prozent finden Chatbots nicht gut. Jeweils etwas mehr als die Hälfte der Befragten traut Bots nicht zu, individuelle oder komplexere Fragen beantworten zu können. Bemerkenswert: 41 Prozent finden den aus Bots resultierenden Arbeitsplatzabbau inakzeptabel.

Viele, die für oder gegen etwas sind, wissen allerdings nicht, worüber sie urteilen sollen. Der Preisvergleichser Idealo stellte in seiner Studie E-Commerce Trends 2018 lapidar fest, dass wissentlich nur 28 Prozent der Nutzer Kontakt mit einem Chatbot hatten. 50 Prozent waren überzeugt, noch nie Kontakt zu einem Chatbot gehabt zu haben. 20 Prozent konnten das nicht einschätzen und 2 Prozent wussten nicht mal, was ein Chatbot ist. 70 Prozent von denen, die es wissen und Chatbots gut finden, wollen damit auch Dinge bestellen können. Knapp die Hälfte erhofft sich, dass ein Automat sie bei Fragen zum Produkt unterstützt oder sie sogar beraten kann. Nur: Lediglich 64 Prozent würden dem vertrauen, was ein Bot rät. Und gerade bei Beschwerden wollen Menschen nach wie vor einen richtigen Menschen, bei dem sie ihrem Ärger Luft machen können.

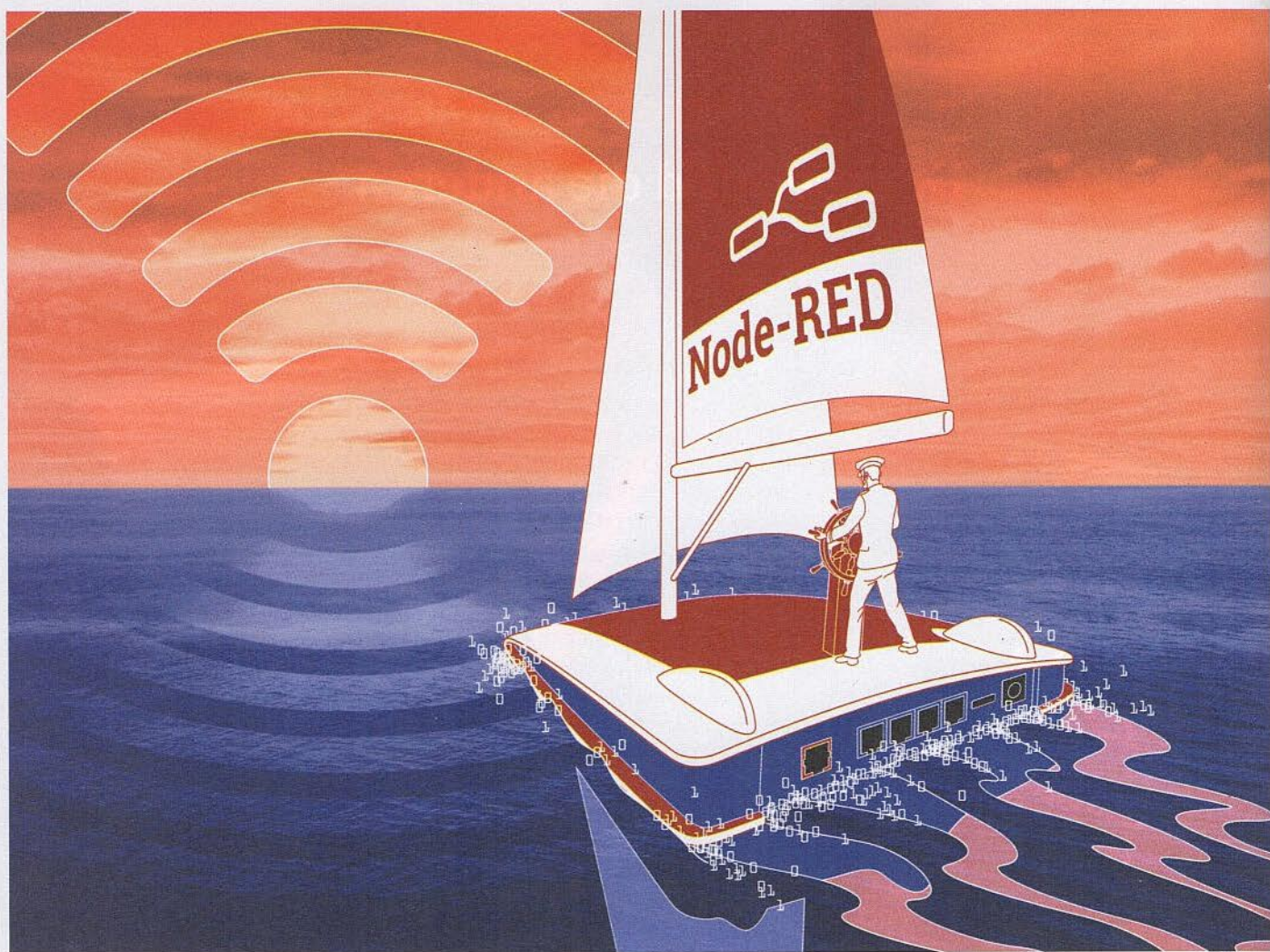
Das Marktforschungs- und Beratungsunternehmen Grand View Research in Kalifornien rechnet mit einer Zunahme von Chatbots und prognostiziert, dass eine verbesserte Erkennung verschiedener Sprachen einen wesentlichen Anteil am Zuwachs haben werde. (mil@ct.de) **ct**



Daten: Liveperson

Chatbots werden je nach Land ganz unterschiedlich gemocht.

Studien: ct.de/yxvv



Routers Meer

Fritzboxen mit Node-Red auslesen und steuern

Mit Node-Red kann man die heimische Fritzbox vielseitig ins Smart-Home integrieren. Sie hilft bei der Präsenzerkennung, wechselt das Gäste-WLAN-Passwort automatisch und leistet noch viel mehr.

Von Merlin Schumacher

Licht, Heizung und Türsensoren sind typische Geräte für die Heimautomation. Der Router, der im modernen Haushalt eine wortwörtlich zentrale Rolle innehat, bleibt oft außen vor, weil man ihn nur als schnöden Vermittler von Geräten

wahrnimmt. Dabei kann man aus einer Fritzbox im Zusammenhang mit Node-Red viel mehr machen. Wenn Sie Node-Red noch nicht kennen, finden Sie eine kurze Einführung unter ct.de/smarthome.

Ist das Kind zu Hause? Die Fritzbox verrät es, denn sie weiß, dass sich dessen Handy im WLAN eingebucht hat. Muss man mal eben aus dem Haus, will aber einen wichtigen Anruf nicht verpassen? Kein Problem: Einfach per Klick die Anrufumleitung aufs Handy aktivieren. Gerade in der Werkstatt am Sägen? Wenn das Telefon zu leise ist, kann die Hue-Lampe mit Blinken auf Anrufer aufmerksam machen.

Damit all diese Tricks funktionieren, brauchen Sie das Modul „node-red-contrib-fritz“ von Jochen Scheib. Für die Kommunikation mit der Fritzbox setzt es

unter anderem auf das Konfigurationsprotokoll TR-064. Dieses wurde zur Router-Steuerung innerhalb des lokalen Netzes entwickelt. Zwar ist TR-064 standardisiert, aber Hersteller dürfen eigene Erweiterungen dranstricken. Davon hat AVM fleißig Gebrauch gemacht und Parameter für praktisch alle Funktionen der Fritzbox eingebaut. Auch viele Programme, die zur Steuerung der AVM-Geräte dienen, greifen auf TR-064 zurück. Pflichtbewusst dokumentiert AVM die Erweiterungen und Veränderungen an der eigenen TR-064-Implementierung ausführlich. Den Link zu dieser und die Beispiele zu diesem Artikel finden Sie über ct.de/ysvw. Da der Funktionsumfang der Schnittstelle sehr groß ist, gibt dieser Artikel nur Anregungen für eigene Szenarien.

Einrichtung

Das nötige Node-Red-Modul „node-red-contrib-fritz“ installieren Sie in der Node-Red-Oberfläche über das Drop-down-Menü an der rechten Seite über „Manage Palette“. Wechseln Sie dort in den Reiter „Install“ und tippen Sie `node-red-contrib-fritz` ein. Anschließend klicken Sie auf „install“. Das Modul sollte mit jeder Node-Red Installation [1] funktionieren, da es keinerlei externe Abhängigkeiten hat. Nach der Installation finden Sie in der Liste an der linken Seite vier neue Node-Typen: „FRITZ!Box“ dient zur Abfrage der TR-064-Schnittstelle. „FRITZ!Box-Callist“ gibt die Anrufliste der Fritzbox im JSON-Format zurück. „FRITZ!Box Callmonitor“ greift auf den Anrufmonitor zu, der Anrufe signalisiert. Diesen müssen Sie manuell durch die Wahl von `#96*5*` auf einem verbundenen Telefon aktivieren. Mit `#96*4*` können Sie den Dienst wieder abschalten. Der letzte Node „FRITZ!Box Lookup“ dient der Suche von Namen im Fritzbox-Telefonbuch anhand von eingespeisten Rufnummern. Das ist sinnvoll, um die vom Anrufmonitor gelieferten Nummern zu identifizieren. In diesem Artikel wird aber nur vom ersten Modul „FRITZ!Box“ Gebrauch gemacht.

Um Ihre Node-Red-Installation mit Ihrer Fritzbox bekannt zu machen, ziehen Sie ein „FRITZ!Box“-Node in einen leeren Flow und doppelklicken Sie, um dessen Einstellungen zu öffnen. Mit einem Klick auf das Stiftsymbol an der rechten Seite des Feldes „Device“ legen Sie ein Profil für Ihre Fritzbox in einem Konfigurations-Node fest. Geben Sie dem Profil zunächst einen Namen. Möchten Sie mehrere Router verwalten, wählen Sie hier eine eindeutige Bezeichnung. In das Feld „Host“ tragen Sie den Hostnamen oder die IP-Adresse des Routers ein. Die Vorgabe `fritz.box` ist meist ausreichend. Den Port 49000 sollten Sie auf 49443 ändern und den Haken bei „Is SSL connection?“ setzen, sodass die Daten der Fritzbox nicht unverschlüsselt durchs (W)LAN geistern.

Eine vernünftig eingerichtete Fritzbox muss mindestens mit einem Passwort

gesichert sein. Damit Node-Red zugreifen darf, braucht es diese Zugangsdaten. Die tragen Sie in die Felder Username und Password ein. Ist nur ein Passwort für die Anmeldung vergeben, lassen Sie das Feld Username leer. Bestätigen Sie die Einstellungen durch einen Klick auf „Add“.

Jemand zu Hause?

Als Einstieg bietet sich eine einfache Präsenzerkennung an. Dazu schickt Node-Red der Fritzbox regelmäßig die MAC-Adresse eines Smartphones, womit diese prüft, ob das Gerät verbunden ist. Ist dem so, kann man davon ausgehen, dass dessen Besitzer daheim ist.

Dem soeben in den Flow gezogenen Node geben Sie einen Namen wie etwa „Gerät angemeldet?“. Klicken Sie dann auf das Lupensymbol hinter „Service“, um die von der Fritzbox angebotenen TR-064-Dienste abfragen zu lassen. In der Liste finden Sie allerhand Dienstbezeichnungen. Die Tabelle auf Seite 136 liefert eine gekürzte Übersicht der wichtigsten Dienste und Funktionsbereiche.

Wählen Sie aus dieser Liste den Dienst `urn:dslforum-org:service:Hosts:1` aus. Der stellt Informationen über die an der Fritzbox angemeldeten Geräte bereit. Jetzt müssen Sie noch eine von diesem Dienst angebotene Aktion aussuchen. Ein Klick auf das Lupensymbol hinter „Actions“ fordert eine weitere Liste von der Fritzbox an. Zur Abfrage des Status eines Geräts ist `GetSpecificHostEntry` die richtige Wahl.

Für jede Aktion erscheint unten ein kurzer Hilfetext, der auf die von dieser Aktion als Eingabedaten erwarteten JSON-Daten hinweist. Diese Hilfe steht bei jeder der Aktionen. Scheint eine Aktion nicht so zu arbeiten wie erwartet, lohnt ein Blick in die eingangs erwähnte AVM-Dokumentation. Bestätigen Sie die Einstellungen mit einem Klick auf „Done“.

Fügen Sie dem Flow als Nächstes einen Inject-Node hinzu, um die nötigen Eingabedaten für die ausgewählte Aktion zu erzeugen. Öffnen Sie die Einstellungen des Inject-Node. Klicken Sie auf die Zeile

„Payload“ und stellen Sie den Inhalt der Nutzdaten von „timestamp“ auf JSON um. Tragen Sie in das Feld nun die MAC-Adresse eines Ihrer Geräte in folgender Form ein:

```
{ "NewMACAddress": "00:80:41:ae:fd:7e" }
```

Damit Node-Red die Fritzbox regelmäßig nach dem Status des Geräts fragt, müssen Sie beim Inject-Node noch zwei Einstellungen vornehmen: Setzen Sie zunächst den Haken bei „Inject once after 0.1 seconds, then“ und ändern Sie die Zeit auf 5 Sekunden. Diese Karenzzeit verschafft Node-Red nach einem „Deploy“ fünf Sekunden Zeit, um sich mit der Fritzbox zu verbinden. Kommt eine Abfrage zu früh, meldet Node-Red „Device not ready“.

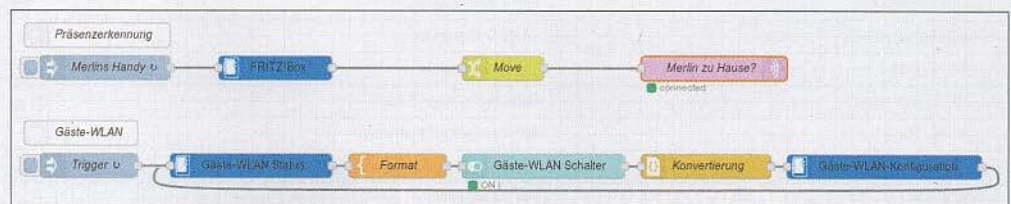
Als Abfrageintervall sollte eine Minute ausreichen, um verlässlich zu prüfen, ob Sie daheim sind. Im Drop-down-Feld „Repeat“ wählen Sie die Einstellung „interval“ und tragen darunter 1 Minute als Abstand ein. Abschließend legen Sie noch einen Namen fest, etwa „Mein Handy“. Verbinden Sie nun den Inject-Node mit dem Eingang des Fritzbox-Node, damit die Nachrichten an die Fritzbox geschickt werden.

Ob Ihr Flow funktioniert, sehen Sie, wenn Sie noch einen Debug-Node einfügen und mit dem Ausgang des Fritzbox-Nodes verbinden. Klicken Sie nun auf „Deploy“, um die Änderungen am Flow zu übernehmen und werfen Sie einen Blick in den Debug-Reiter rechts. Dort sollten Sie eine JSON-Ausgabe ähnlich der folgenden sehen:

```
{
  "NewIPAddress": "192.168.178.36",
  "NewAddressSource": "DHCP",
  "NewLeaseTimeRemaining": "863657",
  "NewInterfaceType": "802.11",
  "NewActive": "1",
  "NewHostName": "Mein Handy"
}
```

An „NewActive“ erkennen Sie, dass Ihr Gerät mit dem WLAN der Fritzbox verbunden ist. Es ist Zeit für einen ersten Test der Erkennung: Trennen Sie Ihr Gerät

Mit dem Node-Red-Dashboard und dem TR-064-Node, kann man nicht nur das Fritzbox-WLAN aus dem Smarthome-Dashboard ein- und ausschalten.



vom WLAN und klicken Sie auf den kleinen abgerundeten Auslöseknopf links am Inject-Node, um eine erneute Abfrage auszulösen. Diesmal sollte im Feld „NewActive“ eine „0“ stehen. Den erfassten Status können Sie durch einen Change-Node mittels einer Verschieberegeln („Move“) von msg.payload.NewActive nach msg.payload verschieben und die übrig gebliebene 1 oder 0 weiterverarbeiten. Im Unterschied zu Lösungen, die per Ping überprüfen, ob ein Gerät im Netz erreichbar ist, funktioniert dieser Weg auch bei Geräten wie iPhones und iPads, die im Tiefschlaf nicht auf Pings reagieren.

WLAN nur für Gäste

Per TR-064 kann man nicht nur Dinge aus der Fritzbox auslesen, sondern auch Einstellungen festlegen. Etwa das Gäste-WLAN an- und abschalten oder dessen Passwort regelmäßig ändern. Möglicherweise schlägt dieses Beispiel bei Ihrer Fritzbox mit der Fehlermeldung „Action failed“ fehl. Schuld daran ist ein Bug in Fritz!OS 7. Der Bug ist jedoch in den aktuellen Laborversionen der Fritzbox-Firmware korrigiert und sollte mit dem nächsten offiziellen Release verschwinden. Ältere Fritz!OS-Versionen sind von dem Problem nicht betroffen. Um Einfluss auf das Gäste-WLAN zu nehmen, müssen Sie einen frischen Fritzbox-Node in einen Flow ziehen und erneut einen dafür passenden Dienst auswählen. Die Fritzbox nummeriert die für WLANs zuständigen Dienste durch. Ihr Name beginnt mit „urn:dsforum-org:service:

WLANConfiguration“ und endet mit einer Ziffer. Welcher Eintrag der passende ist, müssen Sie durchprobieren, indem Sie jeden einzelnen mit der Aktion GetInfo befragen. Um diese Abfrage auszulösen, fügen Sie einen Inject-Node ein und verbinden Sie ihn ohne weitere Einstellungen mit dem Fritzbox-Node. Ans Ende der Kette hängen Sie einen Debug-Node. Der zeigt beim Auslösen im Debug-Reiter im Abschnitt NewSSID der JSON-Ausgabe den Namen Ihres Gäste-WLANs. Bei Fritzboxen ohne 5-GHz-Modul ist es zur Zeit 2, bei solchen mit 3.

Mit diesem Wissen können Sie mit Node-Red Ihr Gäste-WLAN ein- und ausschalten. Dazu brauchen Sie einen Fritzbox-Node mit dem Dienst für das Gäste-WLAN, etwa urn:dsforum-org:service:WLANConfiguration:3. Als Aktion müssen Sie SetEnable konfigurieren. Zusätzlich erzeugen Sie zwei weitere Inject-Nodes, die Sie zum Ein- und Ausschalten verwenden. Legen Sie dort für den Einschalt-Node die JSON-Payload {“NewEnable”: “1”} fest. Der Ausschalt-Node bekommt {“NewEnable”: “0”} als Payload zugewiesen. Denken Sie daran, beiden aussagekräftige Namen zu geben. Ziehen Sie nun Verbindungen von den beiden Inject-Nodes zu dem Fritzbox-Node.

Mit einem Klick auf den Einschalt-Node können Sie nun das Gastnetz aktivieren und mit dem Abschalt-Node deaktivieren. Das Fritzbox-Webinterface sollte diese Änderungen widerspiegeln. Im Zusammenspiel mit dem Node-Red-Dash-

board lässt sich ein Schalter bauen, der das WLAN schaltet und den aktuellen Status des Netzes anzeigt, auch wenn es außerhalb von Node-Red geschaltet wurde[2]. Mit der Aktion „SetSecurityKeys“ können Sie das Passwort Ihres Gäste-WLANs ändern. Senden Sie dieser eine JSON-Payload in folgender Form:

```
{
  "NewWEPKey0": "",
  "NewWEPKey1": "",
  "NewWEPKey2": "",
  "NewWEPKey3": "",
  "NewPreSharedKey": "",
  "NewKeyPassphrase": "MeinPasswort"
}
```

Achten Sie dabei darauf, dass Sie nur „NewKeyPassphrase“ mit Ihrem Passwort befüllen. Der Rest sollte leer bleiben. Die Schlüssel für das unsichere WEP wollen Sie ohnehin nicht festlegen und den Inhalt von „NewPreSharedKey“, den Passwort-Hash, erzeugt die Fritzbox selbst aus dem Passwort in „NewKeyPassphrase“. Anschließend lautet das Passwort für Ihr Gastnetz „MeinPasswort“, wie Ihnen die Oberfläche der Fritzbox verraten wird. Ändern Sie das Passwort anschließend wieder in etwas Sicheres. Ein komplexeres Beispiel, das das Passwort täglich in eine zufällige Zeichenfolge ändert, stellen wir online bereit.

Tiefer eintauchen

Die TR-064-Schnittstelle der Fritzbox lässt einen praktisch alles steuern, was sich auch in der Fritzbox-Weboberfläche findet, weit mehr, als in diesen Artikel passt. Es bietet sich an, einfach zu schauen, welche Informationen man der Box entlocken kann; entweder auf eigene Faust oder anhand der AVM-Doku. Wir haben neben den vorgestellten noch weitere Beispiele zusammengestellt und auf GitHub hochgeladen. Den Link finden Sie über ct.de/ysvw. Zum Import der Beispiele gehen Sie über das Hamburger-Menü in Node-Red zu „Import/Clipboard“ und fügen Sie die JSON-Daten der Beispiele dort ein. (m/s@ct.de) ct

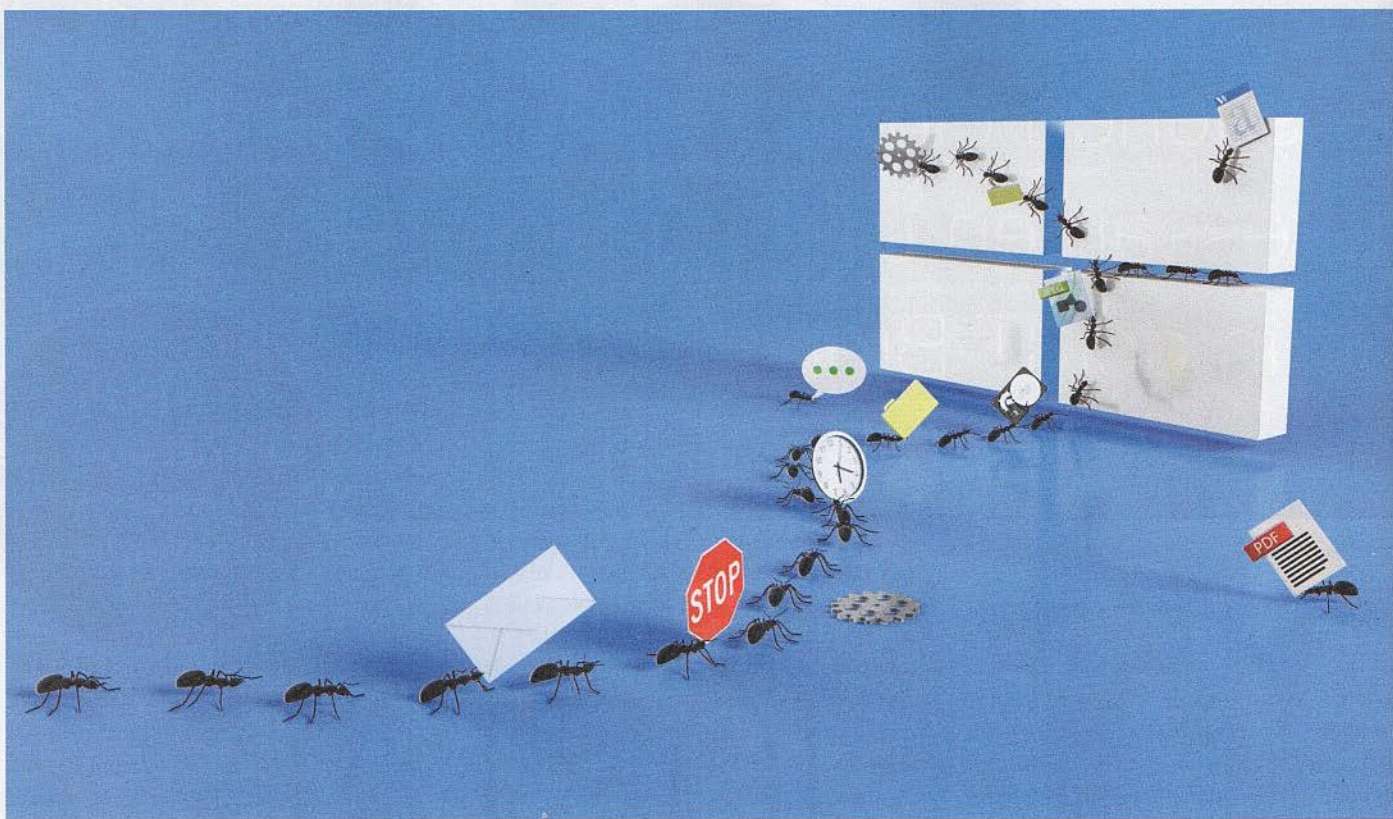
Literatur

[1] Jan Mahn, Reaktionsmaschine, Einstieg in Heimautomation mit Node-Red, c't 15/2018, S. 142
[2] Merlin Schumacher, Rotfront!, Grafische Oberflächen für Node-Red entwickeln, c't 2/2019, S. 160

Downloads und Links: ct.de/ysvw

TR-064-Dienste der Fritzbox (Auswahl)

Schnittstellename (gekürzt)	Funktion
DeviceConfig:1	Router-Konfiguration
DeviceInfo:1	Router-Informationen
Hosts:1	Geräteinformation
LANEthernetInterfaceConfig:1	LAN-Status
LANHostConfigManagement:1	IP-Konfiguration
Time:1	Zeitabfrage
UserInterface:1	Firmware-Informationen
WANCommonInterfaceConfig:1	WAN-Informationen
WANDSLInterfaceConfig:1	DSL-Informationen
WANDSLLinkConfig:1	PPPoE-/ATM-Konfiguration
WANPPPConnection:1	PPPoE-Konfiguration
WLANConfiguration:1-3	WLAN-Konfiguration
X_AVM-DE_Dect:1	DECT-Konfiguration
X_AVM-DE_Homeauto:1	Hausautomations-Geräte
X_AVM-DE_TAM:1	Anrufbeantworterinformation
X_AVM-DE_UpnP:1	UPnP-Konfiguration
X_VoIP:1	VoIP-Konfiguration



Fleißige Helfer

Tipps zur Windows-Aufgabenplanung

Böse Zungen behaupten, mit der Aufgabenplanung erledige der Computer Jobs, die man ohne ihn gar nicht an der Backe hätte. Das stimmt nur zum Teil: Wer den Taskplaner beherrscht, kann mit ihm durchaus auch seine eigene Bequemlichkeit pflegen.

Von Hajo Schulz

Um sich selbst aktuell und sicher zu halten und Datenmüll auf der Festplatte und im Speicher nicht endlos wachsen zu lassen, führt Windows ständig allerlei Wartungsarbeiten durch. Wann und wie oft sie fällig sind, hängt von der jeweiligen Aufgabe ab: Das Defragmentieren der Festplatte hat Zeit, bis der Rechner mal wieder im Leerlauf ist, Sicherheits-Updates sollten dagegen möglichst bald nach Verfügbarkeit eingespielt werden.

Als universelles Werkzeug, das all diese Aufträge verwaltet und die Arbeiten zu den gewünschten Zeitpunkten startet, enthält Windows die Aufgabenplanung.

Sie ist nicht nur für das Betriebssystem da: So manche installierte Anwendung legt hier Aufgaben ab, typischerweise zum Aktualisieren des Programms oder zum Synchronisieren von Daten. Auch Anwender können die Aufgabenplanung damit beauftragen, Dinge für sie automatisch zu erledigen.

Konfigurieren lassen sich die Aufträge in einem eigenen Fenster, das man am einfachsten öffnet, indem man nach dem Drücken der Windows-Taste die ersten Zeichen von „Aufgabenplanung“ in die Startmenü-Suche eintippt. Alternativ startet die Aufgabenplanung durch Eingabe von `taskschd.msc` in den Windows+R-Dialog oder eine Eingabeaufforderung.

Das Layout des Fensters erinnert entfernt an den Windows-Explorer: In der linken Spalte findet sich eine Baumstruktur mit Ordnern, in denen weitere Ordner

oder Aufgaben stecken können; eine direkte Entsprechung im Dateisystem besitzen aber beide nicht. Auf einem frisch installierten Windows finden sich die meisten Aufgaben in Unterordnern von „Aufgabenplanungsbibliothek\Microsoft\Windows“; installierte Anwendungen von Drittanbietern verewigen ihre Aufgaben meist direkt in der „Aufgabenplanungs-bibliothek“. Wenn ein Ordner Aufgaben enthält, erscheinen sie bei Auswahl in der oberen Hälfte der mittleren Fensterspalte. Die Auswahl einer Aufgabe blendet wiederum deren Eigenschaften in dem unter der Liste angeordneten Fenster ein. Mehr als eine Vorschau ist das aber nicht – die Details der in einer Aufgabe enthaltenen Elemente lassen sich hier nicht ergründen, auch ändern kann man nichts.

Grundausstattung

Beides ermöglicht das Eigenschaften-Fenster, das sich per Doppelklick auf eine Aufgabe öffnet. Auf Gerätewohl an den vorhandenen Aufgaben herumzumanipulieren empfiehlt sich allerdings nicht. Um die Funktionen der Aufgabenplanung auszuprobieren, können Sie sich unterhalb der „Aufgabenplanungs-bibliothek“ einen eigenen Ordner erstellen, indem Sie diese selektieren, anschließend rechtsklicken und den Befehl „Neuer Ordner“ auswählen.

Zum Erstellen neuer Aufgaben stehen in den Kontextmenüs von Ordnern und Aufgabenlisten zwei Befehle zur Verfügung: „Einfache Aufgabe erstellen“ ruft

einen Assistenten auf den Plan, der den Benutzer durch die wichtigsten Schritte zur Definition einer Aufgabe leitet. Viele Details lassen sich hier aber nicht einstellen. Sämtliche Optionen bekommt man nur mit dem Befehl „Neue Aufgabe erstellen“ zu Gesicht: Er ruft dasselbe Fenster auf, das ein Doppelklick auf eine bestehende Aufgabe öffnet, allerdings zunächst leer. Alternativ kann man eine neue Aufgabe auch erst mit dem Assistenten anlegen und die Feinheiten anschließend im Eigenschaften-Fenster konfigurieren.

Um mit der Aufgabenplanung etwas Sinnvolles anstellen zu können, muss man die Bedeutung zweier zentraler Begriffe kennen: Eine Aufgabe enthält immer mindestens eine „Aktion“; sie bestimmt, was diese Aufgabe zu tun hat. Ein oder mehrere „Trigger“ definieren, wann das geschehen soll – Details siehe weiter unten.

Zum Konfigurieren der Details einer Aufgabe enthält das Eigenschaften-Fenster mehrere Tabs. Auf dem ersten namens „Allgemein“ ist beim Erstellen einer neuen Aufgabe die Eingabe eines Namens Pflicht; bei einer bestehenden Aufgabe lässt er sich nachträglich nicht mehr ändern. Wenn die Aufgabe unter einem anderen Benutzerkonto als Ihrem eigenen abgearbeitet werden soll, können Sie das unter den Sicherheitsoptionen einstellen; infrage kommt unter anderem auch das Konto „SYSTEM“, das sich beispielsweise für Backups anbietet, weil es benutzerübergreifend auf alle Dateien zugreifen darf.

Der Schalter „Unabhängig von der Benutzeranmeldung ausführen“ bewirkt nicht nur, dass die Aufgabe auch dann ausgeführt wird, wenn der gewählte Benutzer

beim Auslösen eines Triggers nicht angemeldet ist. Vielmehr wirkt er sich auch dann aus, wenn der Benutzer angemeldet ist: Selbst dann findet die Aufgabe nämlich nicht interaktiv auf seinem Desktop statt, sondern unsichtbar im Hintergrund. Das bedeutet, dass er zum Beispiel Fehlermeldungen des ausgeführten Programms nicht zu Gesicht bekommt. Auch eventuelle „Sind Sie sicher?“-Nachfragen des Programms landen im Nirwana. Der Benutzer hat keine Chance, sie zu bestätigen, und die Aktion kann ihren Job unter Umständen nicht wie gewünscht verrichten. Ohne interaktive Anmeldung ist zudem die Benutzerkontensteuerung (UAC) nicht aktiv: Konten, die der Benutzergruppe der Administratoren angehören, besitzen in diesem Kontext stets volle Rechte.

Trigger

Trigger für eine Aufgabe zu definieren ist keine Pflicht – falls Sie die systemeigenen Aufgaben durchstöbern, werden sie etliche ohne Trigger finden. Sinnvoll kann das sein, um etwa eine oder mehrere Aktionen samt Sicherheits- und Ausführungsoptionen als Aufgabe zu speichern, sie aber nicht geplant, sondern etwa per Skript auszuführen. Von Hand starten Sie eine Aufgabe mit dem Befehl „Ausführen“, der sich sowohl in ihrem Kontextmenü als auch im Aktionen-Menü in der rechten Spalte des Aufgabenplanungs-Fensters findet.

Wenn Sie Trigger definieren, ist der wahrscheinlich am häufigsten genutzte Typ die Ausführung nach einem Zeitplan: Damit können Sie Aufgaben regelmäßig, etwa jede Nacht um 3 Uhr ausführen

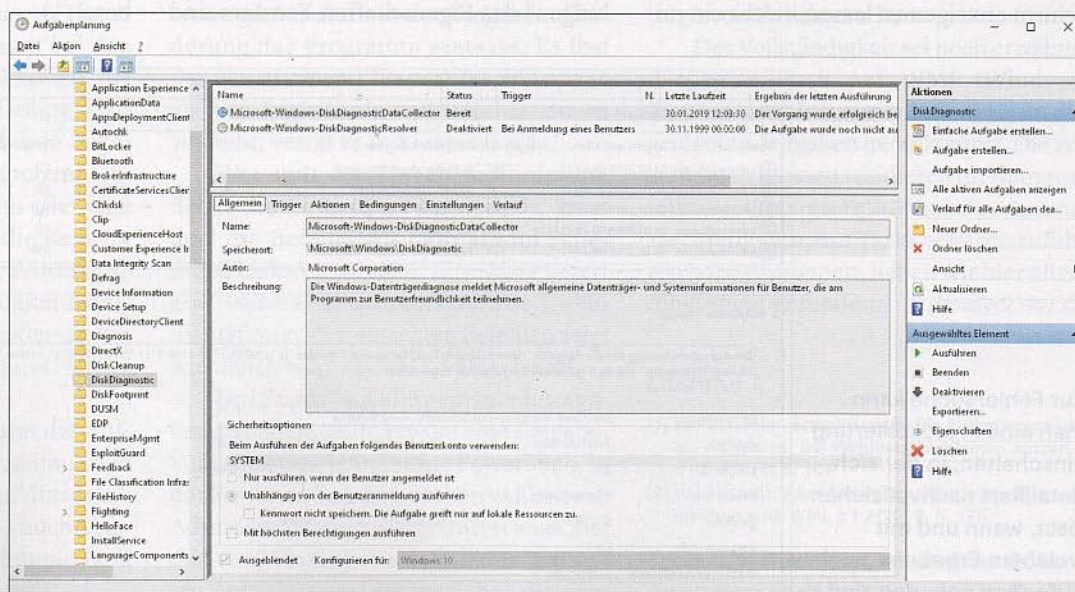
lassen, aber auch erweiterte Pläne wie „jeden zweiten und vierten Donnerstag im Monat“ sind möglich. Auch wenn Sie eine Aufgabe nur zur einmaligen Ausführung vormerken wollen, sind Sie in der Kategorie „Nach einem Zeitplan“ richtig. Eine regelmäßige Ausführung lässt sich durch Einschalten der Option „Ablaufen“ und Ausfüllen der dazugehörigen Felder nach einer bestimmten Dauer auch wieder automatisch beenden.

Die meisten anderen Trigger-Typen sind selbsterklärend. Ausnahmen: „Bei Aufgabenerstellung/-änderung“ heißt nichts anderes als „Jetzt gleich“. Und mit „Bei einem Ereignis“ ist gemeint, dass der Trigger auslöst, sobald ein bestimmter Eintrag ins System-Log geschrieben wird, also in das Protokoll, das Sie mit der Ereignisanzeige betrachten können [1]. Administratoren können sich damit etwa benachrichtigen lassen, wenn der Windows Defender auf einem ihrer Rechner eine Bedrohung gefunden hat (Protokoll: Microsoft-Windows-Windows Defender/Operational, Ereignis-IDs: 1006, 1015, 1116).

Über die „Erweiterten Einstellungen“ können Sie die Ausführung einer Aufgabe nach dem Auslösen des Triggers noch um eine Frist verzögern – sinnvoll ist das zum Beispiel, um mehrere Aufgaben nach der Benutzeranmeldung zeitlich gestaffelt zu starten.

Für Aufgaben, die öfter als einmal am Tag stattfinden sollen, gehen Sie folgendermaßen vor: Wählen Sie zunächst einen täglichen Zeitplan. Aktivieren Sie dann das Kästchen vor „Wiederholen jede“ und wählen Sie das gewünschte Intervall. Bei

Die Aufgabenplanung enthält schon bei einem frisch installierten Windows zahlreiche Tasks, die sich über fast genauso viele Ordner verteilen.



„für die Dauer von“ lassen Sie „1 Tag“ stehen – danach beginnt durch den täglichen Zeitplan die Wiederholung ja von vorn.

Was sich nicht sofort erschließt: Bei den Feldern für die Verzögerung und für die Wiederholungen sind Sie nicht auf die vorgegebenen Werte beschränkt. Die Aufgabenplanung versteht hier auch Eingaben wie „90 Minuten“, „2 Stunden“ oder „4:30“ (für viereinhalb Stunden).

Die Option „Aufgabe beenden nach“ zeigte sich bei unseren Versuchen wirkungslos. Eine funktionierende Alternative birgt das Register „Einstellungen“ des Eigenschaften-Dialogs.

Aktionen

Zu jeder Aufgabe gehört mindestens eine Aktion. Unter Windows 10 steht hier in der Aufgabenplanung als einzige funktionierende Auswahl „Programm starten“ zur Verfügung. Als Argumente braucht so eine Aktion den vollen Pfad zur auszuführenden Datei, optional kann man ihr noch Befehlszeilenargumente übergeben und das zur Ausführungszeit aktuelle Verzeichnis bestimmen.

Die als „veraltet“ gekennzeichneten Aktionen zum Anzeigen einer Meldung und zum Senden einer E-Mail lassen sich zwar noch selektieren, führen dann aber zu einer Fehlermeldung. Das ist zu verschmerzen: Eine E-Mail können zum Beispiel kostenlose Programme wie Blat oder sendEmail (siehe ct.de/yy33) absetzen. Damit können sich etwa (Familien-)Admins regelmäßig einen Report über den Zustand der von ihnen betreuten Maschinen zuschicken lassen, den zuvor ein Programm oder ein Skript eingesammelt hat.

Um eine Meldung auf dem Bildschirm anzeigen zu lassen, reicht ein mi-

nimales VBScript unter Verwendung der Funktion MsgBox – ein Beispiel finden Sie ebenfalls unter ct.de/yy33. Einsetzen können Sie es zum Beispiel, um sich jeden Donnerstag um 17:30 Uhr ermahnen zu lassen, dass Sie jetzt besser Feierabend machen sollten, wenn Sie es noch zum Training schaffen wollen.

Wenn Sie bei einer Aufgabe mehrere Aktionen hinterlegen, führt die Aufgabenplanung die nächste immer erst dann aus, wenn die vorige zu Ende ist. Das ist recht praktisch, wenn man etwa im Anschluss an eine Aufräum-Aktion noch eine Nachricht über deren Ausgang verschicken möchte.

Optionen

Über das Register „Bedingungen“ des Eigenschaften-Fensters lässt sich noch festlegen, dass die Aufgabe nur in bestimmten Systemzuständen zum Zuge kommt: Standardmäßig eingeschaltet ist eine Prüfung, die die Ausführung davon abhängig macht, dass der Rechner mit Netzstrom versorgt wird. Für eher nebensächliche Wartungs-Tasks empfiehlt sich außerdem, sie nur dann starten zu lassen, wenn der Rechner im Leerlauf ist. Das ist aus Sicht der Aufgabenplanung der Fall, wenn mindestens 4 Minuten lang keine Maus- oder Tastatureingaben erfolgt sind (15 Minuten bei Windows 7) und während dieser Frist die CPUs und Datenträger zu mindestens 80 Prozent der Zeit nichts zu tun hatten (90 Prozent bei Windows 7). Auf Wunsch kann die Aufgabenplanung auch eine Zeit lang auf Leerlauf warten sowie eine Aufgabe abwürgen, wenn sie während ihrer Abarbeitung wieder Benutzeraktivitäten erkennt.

Die Optionen auf der Seite „Einstellungen“ des Eigenschaften-Fensters sind

leider nur zum Teil brauchbar. Was der Schalter „Falls Aufgabe scheitert, neu starten“ bewirken soll, war weder durch eine Internet-Recherche noch durch eigene Experimente herauszufinden. Ein von 0 verschiedener Rückgabewert eines Skripts oder Programms wird hier jedenfalls nicht als Fehler erkannt. Auch ein Deaktivieren des Schalters „Beenden der aktiven Aufgabe erzwingen ...“ hatte bei unseren Versuchen keinerlei Effekt.

Fehlersuche

Um einem möglichen Fehlverhalten Ihrer selbst definierten oder auch der systemeigenen Aufgaben auf die Schliche zu kommen, können Sie mit dem Eintrag „Verlauf für alle Aufgaben aktivieren“ im Aktionen-Menü in der rechten Spalte eine Protokollierung einschalten. Dadurch füllt sich nach und nach bei allen ausgeführten Tasks die Liste auf der Seite „Verlauf“ des Eigenschaften-Fensters mit Einträgen, die ausführlich beschreiben, wann die jeweilige Aufgabe gestartet und beendet wurde. Achtung: Das Protokoll wird schnell ziemlich umfangreich. Man sollte das Logging also nur zur Fehlersuche einschalten und nicht vergessen, es irgendwann wieder zu deaktivieren.

Gespeichert werden die Protokolldaten in einem Log, das sich auch mit der Ereignisanzeige betrachten, durchsuchen und nach Belieben filtern lässt. Dazu müssen Sie dort zu dem Protokoll im Pfad „Anwendungs- und Dienstprotokolle/Microsoft/Windows/TaskScheduler/Operational“ navigieren. (In einigen Windows-Versionen hat Microsoft den Pfad offenbar irrtümlich teilweise übersetzt; der letzte Teil heißt hier „Betriebsbereit“.)

Zur Fehlersuche kann man eine Protokollierung einschalten, in der sich detailliert nachvollziehen lässt, wann und mit welchem Ergebnis Aufgaben gelaufen sind.

AllgemeinTriggerAktionenBedingungenEinstellungenVerlauf

Anzahl von Ereignissen: 237

Ebene	Datum und Uhr...	Ereignis-ID	Aufgabenkategorie	Vorgangscod	Korrelations-ID
Informationen	04.02.2019 09:44:42	102	Aufgabe abgeschlossen	(2)	c1e99999-a7b8-4368-9111-5514f75f0680
Informationen	04.02.2019 09:44:42	201	Aktion abgeschlossen	(2)	c1e99999-a7b8-4368-9111-5514f75f0680
Informationen	04.02.2019 09:44:42	200	Die Aktion wurde gestartet.	(1)	c1e99999-a7b8-4368-9111-5514f75f0680
Informationen	04.02.2019 09:44:42	100	Die Aufgabe wurde gestartet.	(1)	c1e99999-a7b8-4368-9111-5514f75f0680
Informationen	04.02.2019 09:44:42	129	Prozess für erstellte Aufgabe	Info	

Ereignis 201, Task Scheduler

AllgemeinDetails

Die Aufgabenplanung hat die Aufgabe "\GoogleUpdateTaskMachineUA", Instanz "[c1e99999-a7b8-4368-9111-5514f75f0680]", Aktion "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" mit Rückgabecode 0 erfolgreich abgeschlossen.

Protokollname:

Microsoft-Windows-TaskScheduler/Betriebsbereit

Quelle:

TaskScheduler

Protokolliert:

04.02.2019 09:44:42

Ereignis-ID:

201

Aufgabenkategorie:

Aktion abgeschlossen

Ebene:

Informationen

Schlüsselwörter:

Benutzer:

SYSTEM

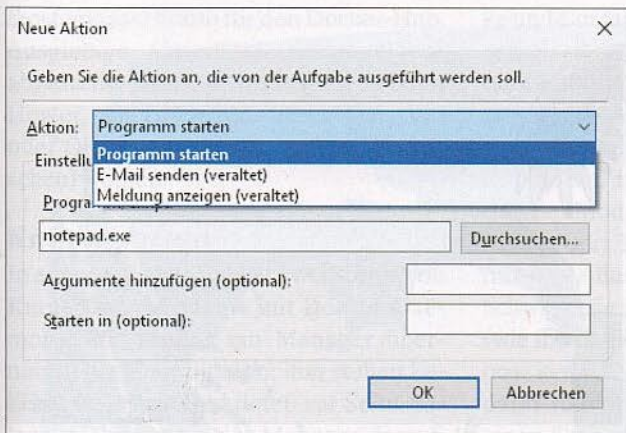
Computer:

Hossa

Vorgangscod:

(2)

Weitere Informationen: [Onlinehilfe](#)



Bei eingeschalteter Protokollierung füllt sich in der Aufgabenplanung auch die Liste „Aufgabenstatus“, die in der mittleren Fensterspalte erscheint, wenn Sie links den Wurzeleintrag der Ordnerhierarchie anklicken. Leider gibt es keine einfache Möglichkeit, von einem Eintrag in dieser Liste zur Definition der betreffenden Aufgabe zu springen – die systemeigenen Aufgaben verteilen sich ja auf eine Vielzahl von Ordnern. Statt die auf der Suche nach der Aufgabendefinition alle von Hand abzuklappen, kann man das Protokoll in der Ereignisanzeige nach dem Aufgabennamen durchsuchen und erfährt so relativ schnell, zu welcher Aufgabe der Protokolleintrag gehört.

Grenzen

Leider hilft auch das nicht immer weiter, wenn man etwa zum Überprüfen eines Malware-Verdachts wissen möchte, welches Programm eine bestimmte Aufgabe startet. Bei den Aufgaben, die Windows von Haus aus mitbringt, gibt es nämlich etliche, bei denen die Aufgabenplanung als Aktion nur „Benutzerdefinierter Handler“ vermeldet. Windows kennt bei den geplanten Aufgaben auch Aktionen, die sich nicht mit der Aufgabenplanung bearbeiten lassen. Zu ihnen gehören sogenannte COM-Handler (Component Object Model), die ein Programm oder eine DLL starten, die zuvor über die Registry im System registriert wurden. Wie man so etwas von einem eigenen Programm aus realisiert, steht in der Entwickler-Dokumentation des Task Scheduler (siehe ct.de/yy33).

Auch als Trigger vermeldet die Aufgabenplanung bei einigen vordefinierten Aufgaben „Benutzerdefinierter Auslöser“. Offenbar kennt Windows also auch Trigger, von denen die Aufgabenplanung nichts versteht.

Unter Windows 10 funktioniert als Aktion nur noch das Starten eines Programms oder Skripts. Die als „veraltet“ gekennzeichneten Aktionen führen zu einer Fehlermeldung.

In Windows 10 besitzt die Aufgabenplanung zudem einen ärgerlichen Bug, der das nachträgliche Bearbeiten einmal erstellter Aufgaben erschwert. Der Versuch scheitert dann mit der lapidaren Fehlermeldung „Fehler für Aufgabe xyz. Mindestens eins der angegebenen Argumente ist ungültig“. Die Fehlermeldung lässt sich sogar schon provozieren, indem man eine neu erstellte Aufgabe, die die Aufgabenplanung ja gerade noch akzeptiert hat, zum Bearbeiten öffnet und dann ohne jede Änderung mit „OK“ erneut bestätigt. Des Rätsels Lösung: Wenn man bei den Sicherheitsoptionen kein anderes als das eigene Benutzerkonto einträgt, verunstaltet die Aufgabenplanung den Benutzernamen, indem sie den Rechnernamen unterschlägt. Man muss also vor jedem Bestätigen den Benutzernamen („Alice“) wieder komplettieren („BüroPC\Alice“).

Alternativen

Die Aufgabenplanung ist nicht der einzige Weg, mit dem man die geplanten Tasks von Windows verwalten kann. Beispielsweise gibt es dafür in der Eingabeaufforderung das Programm `schtasks`. Es löst das von Microsoft für veraltet erklärte `at` ab. Die Argumente und Befehle, die es versteht, verrät es mit `schtasks /?`.

Wer statt der Eingabeaufforderung lieber die PowerShell verwendet, kann dort die Befehle aus dem Modul `ScheduledTasks` verwenden. Eine Liste liefert `gcm -Module ScheduledTasks`. Die Dokumentation zu den einzelnen Befehlen zeigt wie üblich `help <Befehl> -Detailed an`.

Um Zugriff auf alle geplanten Aufgaben zu haben, sollte sowohl eine Eingabeaufforderung als auch eine PowerShell, in der Sie ihnen zu Leibe rücken wollen, mit Administratorrechten gestartet sein. Bei den von Windows vordefinierten geplanten Aufgaben sind etliche dabei, die dem

Anwender mit normalen Benutzerrechten verborgen bleiben.

Sowohl `schtasks` als auch die PowerShell-Befehle lassen sich beispielsweise verwenden, um aus einer Batch-Datei beziehungsweise aus einem PowerShell-Skript heraus eine geplante Aufgabe zu starten. Das sieht in einer Batch-Datei dann so aus:

```
schtasks /run /tn "MeineTasks\Backup"
```

In der PowerShell erledigt dasselbe der Aufruf

```
Start-ScheduledTask `
-TaskPath \MeineTasks\ `
-TaskName Backup
```

Der Befehl `/Query` von `schtasks` ist das Mittel der Wahl, wenn man eine Liste aller definierten Tasks in eine Textdatei schreiben will, etwa um sie mit einem Editor zu durchsuchen oder die Ausgaben von zwei verschiedenen Rechnern zu vergleichen.

Ein weiteres populäres Werkzeug, mit dem man an eine Übersicht der vorhandenen geplanten Aufgaben herankommt, ist das Sysinternals-Tool `AutoRuns`: Auf seinem Tab „Scheduled Tasks“ zeigt es eine Liste der im System vorhandenen geplanten Aufgaben. Häkchen vor jedem Listeneintrag aktivieren und deaktivieren einzelne Tasks. Viel mehr kann man hier mit den geplanten Aufgaben nicht anstellen. Was `AutoRuns` trotzdem zu einem empfehlenswerten Aufgaben-Betrachter macht, ist der Menübefehl „Options/Hide Windows Entries“: Er blendet alle Einträge aus, die zur Betriebssysteminstallation selbst gehören, und schärft damit den Blick für die Einträge von Drittherstellern.

Der Vollständigkeit sei noch erwähnt, dass man auch per WMI (Windows Management Instrumentation) [2] an die geplanten Aufgaben herankommt. Die zuständigen Klassen residieren im Namensraum `Root\Microsoft\Windows\TaskScheduler`. Methoden, um Tasks etwa auszuführen oder zu stoppen, haben wir hier allerdings nicht gefunden. (*hos@ct.de*) **ct**

Literatur

- [1] Jan Schüßler, Ereignisreich, Die Ereignisanzeige als Wegweiser bei Windows-Problemen nutzen, c't 20/2016, S. 104
- [2] Hajo Schulz, Alles-Verwalter, Windows clever managen mit WMI, c't 2/2019, S. 176

Tools zum Download, zusätzliche Dokumentation: ct.de/yy33



Schwärmchen

Docker Swarm: Container verteilen und verwalten

Wenn Container verteilt über mehrere Systeme arbeiten sollen, kann man sie mit Docker-Bordmitteln als Schwarm betreiben. Damit lassen sich große Lasten wuppen und Ausfälle verdauen. Ein näherer praktischer Blick auf Grundlagen und Möglichkeiten offenbart allerdings auch allerhand Einschränkungen.

Von Peter Siering

Docker spukt inzwischen durch viele c't-Artikel: Die in Container gekapselten Prozesse sind nützlich, um in Bastelprojekten wie dem c't Smart Home vierteilige Softwareinstallationen mit wenigen Handgriffen auf einem Raspi zu starten, um Softwarefabriken zu gründen oder nur um Serverdienste zu sortieren und leichter zu aktualisieren [1, 2, 3]. Gedacht waren die Container aber mal für die Industrialisierung der IT, und entsprechend gibt es Infrastruktur, um Container im größeren Rahmen zu betreiben.

Einen vergleichsweise einfachen Ansatz dafür liefert Docker Swarm – letztlich handelt es sich dabei um eine spezielle

Betriebsart des Docker-Daemon, in dem der sich nicht mehr nur um einen einzelnen Computer (Host oder Knoten) kümmert, sondern gleich einen Schwarm koordiniert. Entsprechend krempelt das Aktivieren der Swarm-Betriebsart auf einem vorhandenen Computer allerhand um. Zum Ergreifen der Grundprinzipien oder um von den Vorteilen zu profitieren, genügt aber ein einziger Computer oder eine virtuelle Maschine, in der Docker läuft.

Um die Beispiele im Artikel nachzu-turnen, können Sie auch auf die Online-Testumgebung „Play with Docker“ (siehe ct.de/ybpi) zurückgreifen. Um sich auf der Website anzumelden, benötigen Sie ein

(kostenloses) Konto für den Docker-Hub. Ausgiebige Aktivitäten setzen eigens abgestellte Rechner voraus, sei es beim Host, auf einem Root-Server als VM oder Gleichwertiges hinter dem (heimischen) Router.

Knotensorten

In einem Schwarm gibt es zwei Sorten von Knoten (also Systeme mit Docker-Daemon): Mindestens ein Manager übernimmt die Koordination; ihm stehen beliebig viele Arbeiterknoten zur Seite. Sappo gesagt achtet der Manager darauf, dass die Aufgaben über die Knoten nach Vorgaben verteilt werden. Die Vorgaben können sein, dass zum Beispiel drei Webserver und eine Datenbank laufen sollen. Mit mehreren Managern und Arbeitern entsteht Redundanz wie in einem Cluster.

Welcher Knoten welche Aufgabe übernimmt, entscheidet das Management. Es achtet darauf, dass die Anforderungen erfüllt werden und startet und beendet gegebenenfalls Container auf den Knoten. Das Management kann auch selbst Arbeitsaufträge annehmen – fasst also bei Bedarf mit an. Details, wer was tun soll, lassen sich festlegen. Ein minimaler Schwarm besteht aus einem Knoten, der sowohl Manager- als auch Arbeiterrolle in sich vereint.

Mit der neuen Betriebsart kommen viele neue Namen ins Spiel, zunächst seien die alten kurz eingeführt: Ein System, auf dem Docker läuft, führt Container in einer abgeschotteten Umgebung aus. Ein solcher Container sollte möglichst nur einen Prozess enthalten. Er bekommt standardmäßig eine eigene IP-Adresse aus einem privaten Netz, sodass eingehende Netzwerkanfragen meist über den Host laufen. Container-Images dienen als Vorlage für solche Container.

Daten können Container in Volumes speichern. Das sind standardmäßig auf dem Docker-Host abgelegte Verzeichnisse. Virtuelle Netzwerke dienen dazu, dass mehrere auf einem System laufende Container miteinander in Kontakt treten können, etwa eine Webanwendung in einem Container, die Zugriff auf eine Datenbank in einem anderen erhält.

Um Anwendungen aus mehreren Containern bequem starten zu können, hat sich inzwischen ein Aufsatz für die Docker-Werkzeuge auf der Kommandozeile etabliert: Docker-Compose. Der gleichnamige Befehl `docker-compose` verarbeitet eine YAML-Datei, die Volumes, Netzwer-

ke und Container im Detail beschreibt. Sie enthält oft auch Umgebungsvariablen, um die Container beim ersten Start zu konfigurieren, und Hinweise, wie die Container voneinander abhängen.

Docker im Schwarmmodus ergänzt dieses Modell: Laufende Container heißen dort Tasks. Sie bilden zusammen mit einer Beschreibung, wie häufig ein Schwarm sie ausführen soll, einen Service (wie ihn namentlich schon Docker-Compose kennt). Ein Service kann global sein, dann führt jeder Knoten im Schwarm einen Task aus (Manager und Arbeiter). Alternativ kann ein Service repliziert sein, dann bestimmt seine Beschreibung, wie viele Knoten im Schwarm einen Task des Service ausführen; letzteres beherrscht Compose nicht, es startet Services nur einmal.

Container-Stapel

Mehrere Services, etwa Webserver, Datenbank und Anwendungsserver, bilden schließlich einen Stack, also eine in sich geschlossene Anwendung vergleichbar mit einem in Docker-Compose zusammengestellten Arrangement. Der wesentliche Unterschied besteht darin, dass die Beschreibung eben auch Hinweise im Hinblick auf die Anzahl der Container-Instanzen enthält, die der Schwarm aus-

führen soll, etwa drei Instanzen des Webservers.

Ein Schwarm stellt neben dem Orchestrierungswerkzeug, also den Funktionen, um Services und Stacks auf die Knoten eines Clusters zu verteilen, auch virtuelle Netze zur Verfügung. Sie organisieren die Zusammenarbeit. Ein sogenanntes Ingress-Netzwerk vermittelt die Netzwerkanwendungen im Schwarm an die Außenwelt. Stellt der Schwarm als Service etwa einen nginx-Webserver auf Port 8008 bereit, so lässt er sich dank des Ingress-Netzes an jeder externen IP-Adresse aller Knoten auf diesem Port erreichen.

Ein einfacher Load-Balancer, der auf die im Linux-Kernel eingebauten Funktionen zurückgreift (IPVS), verteilt Anfragen an einen Service standardmäßig reihum an die für diesen Service aktiven Tasks. Die Verteilstrategie lässt sich in vorgegebenen Grenzen mit den Kernel-Bordmitteln beeinflussen. Genügt das nicht, kann man die Aufgabe auch delegieren, etwa durch einen vorgelagerten Load-Balancer.

Services, die gemeinsam eine Anwendung bilden, können über ein sogenanntes Overlay-Netz intern kommunizieren. Stacks richten oft eigene Overlay-Netze ein, sodass sich mehrere Stacks in einem Schwarm nicht in die Quere kommen. Die Daten, die ein Schwarm über die Overlay-Netze überträgt, bleiben unverschlüsselt – nur auf expliziten Wunsch nutzt Docker an dieser Stelle Verschlüsselung (mit der Option `--opt encrypted` bei `docker network create`), was bei öffentlichen Netzen empfehlenswert ist.

Um die Netzwerkgrundausstattung muss man sich nicht selbst kümmern. Das erledigt Docker beim Errichten eines Schwarms einschließlich vieler weiterer Handgriffe im Hintergrund, die Knoten miteinander zu verknüpfen. Docker generiert Zertifikate, erstellt Netzwerkschnittstellen und Brücken, verbindet die miteinander und richtet zahllose IPv4-Firewall-Regeln ein. Die Regeln ergänzt Docker später beim Freigeben von Ports für Services, sorgt etwa dafür, dass ein Web-Server auf Port 80 erreichbar ist. Für das alles müsste selbst ein erfahrener Admin lange skripten.

Läuft der Schwarm erst mal, kann man wie ein Dirigent mit Docker einzelne Container in Stacks arrangieren und so Anwendungen verteilt über die Knoten ausführen lassen. Wenn man das etwa mit einem einfachen Webserver durchspielt, ist das auf den ersten Blick fantastisch:



Schließt man einzelne Knoten von der Verteilung aus, rutschen die Services auf den verbleibenden zusammen. Mit einem Befehl werden aus drei Tasks für einen Service zehn.

Anders als man vielleicht erwarten könnte, verschiebt Docker in solchen Fällen die Container nicht von Knoten zu Knoten, sondern startet sie stumpf neu. Das folgt dem Mantra der Container-Welt, die herkömmliche Software als Haustiere und die in Containern verpackte als Nutztiere beschreibt – Pet versus Cattle. Die einen hegt und pflegt man, die anderen werden schlicht ersetzt.

Realitätscheck

Der ersten Freude folgt schnell Ernüchterung: Viele der heute gebräuchlichen Container-Images eignen sich für den Einsatz im Schwarm nur begrenzt. Entgegen der ursprünglichen Idee sind diese so gebaut, dass sie bei der ersten Inbetriebnahme Zustandsinformationen speichern, die sie bei jedem Start brauchen, um sich auf den intendierten Anwendungsfall einzustimmen (stateful). Der reinen Lehre folgend sollten Container eigentlich ohne solche Daten nutzbar sein (stateless), eben Vieh statt Schoßhündchen.

Den gängigen MySQL-Images teilt man beim Starten eines Containers das

Passwort für Datenbankzugriffe mit und gibt ihnen Plattenplatz, um die Datenbanktabellen zu sichern – den erhalten sie in der Regel in Form eines Volume. Im Fall einer Datenbank ist noch einsichtig, dass stateless sinnlos ist. Das Gleiche gilt aber auch für viele andere Container(-Images), die nicht auf eine Datenbank zurückgreifen und wo das vielleicht nicht gleich auf der Hand liegt, zum Beispiel Helfer zum Einsammeln und Aktualisieren von Zertifikaten. Die müssen schließlich auch irgendwo bleiben.

Beispiele für allgemein interessante Container, die stateless sind, muss man suchen. Ad hoc fallen HTTP-Server ein, die nur statische Seiten ausliefern oder Anfragen an Datenbanken weiterleiten und die Ergebnisse aufbereitet zurückliefern. Stateless Container wird man kaum als Fertigware finden, sondern es wird sich um Container-Images handeln, die man extra für die eigene Verwendung geschaffen hat.

Wer sich jetzt die Augen reibt: Ja, Docker Swarm bringt keinen gemeinsamen Datenspeicher mit. Den muss man

in Eigenregie herstellen. Dafür gibt es diverse Ansätze, die jeder einen eigenen Artikel wert wären: Rex-Ray, Portworx, GlusterFS, EFS et cetera. Alternativ kann

man dafür sorgen, dass im Schwarm nur diejenigen Container auf den Arbeitern herumschwirren, die eben ohne Zustandsdaten klarkommen. Die restlichen müssen dann auf den Managern verbleiben und auf deren lokalen Datenspeicher in Form

von Volumes zugreifen.

Wie so oft, wenn es um das redundante Absichern von Ressourcen geht, fängt man auch in einem Docker-Swarm schnell an, einen recht komplexen Verhauf zu errichten, der letztlich doch wieder an nur einem Nagel hängt: Wenn es trotz der Einschränkungen gelingt, die Datenbanken in einem Schwarm auf den Managern per Replikation redundant einzurichten, kann schließlich immer noch der Load-Balancer, der eingehende Anfragen verteilt, in den Streik treten – den gibt es je Schwarm standardmäßig eben nur einmal.

Losschwärmen

Wenn Docker bereits läuft, ist die Inbetriebnahme des Swarm-Modus schnell getan:

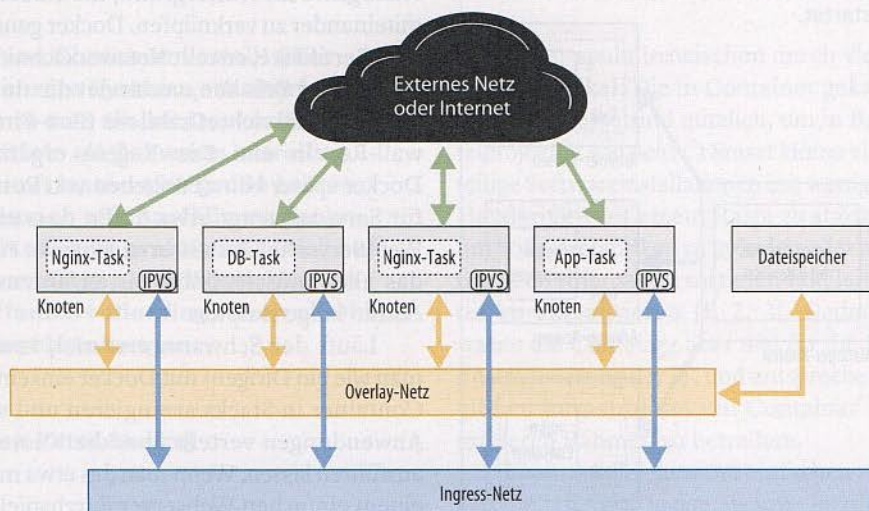
```
docker swarm init
--advertise-addr 2xx.2x.2xx.x
```

richtet ein System als Manager ein und spuckt gleich den Kommandozeilenbefehl aus, die man auf einem anderen System aufrufen kann, um dem Schwarm einen Knoten hinzuzufügen. Die IP-Adresse gibt an, unter welcher seiner Adressen der Knoten Dienste für die Allgemeinheit freigibt, benennt also einen Eintrittspunkt für das Ingress-Netzwerk.

Knoten, die sich hinter einem NAT verstecken, muss man beim Beitritt zum Schwarm ebenfalls eine IP-Adresse mithilfe von --advertise-addr angeben. Das betrifft unter anderem Server in den großen Clouds. In Azure etwa erhalten VMs zunächst eine private IP-Adresse. Eine offizielle muss man einer VM explizit zuweisen. Azure übersetzt eingehende Anfragen von der offiziellen Adresse auf die private. Ein Beitritt zum Schwarm erledigt auf einem zukünftigen Knoten folgender Befehl:

Netzwerkarchitektur im Schwarm

In einem Docker Swarm sorgen zwei Typen von Netzwerken für Verbindungen: Das Ingress-Netz dient dazu, Zugriffe auf freigegebene Ports an einen freien Knoten weiterzugeben, auf dem der nachgefragte Service läuft. Zugriffe können auf jedem Knoten hereinkommen und werden über den Linux-Kernel eigenen Load-Balancer (IPVS) verteilt. Ein Overlay-Netz verbindet hingegen die Knoten untereinander. Es funktioniert wie ein User Defined Network, aber systemübergreifend auf mehreren Knoten.




```
docker swarm join --token   
  <Token> 2xx.2x.2xx.x:2377   
  --advertise-addr 1xx.2xx.x.3
```

DNS-Namen verträgt docker an dieser Stelle nicht, sondern nur IP-Adressen. Die Firewall muss einige Ports durchlassen und, wenn die beteiligten Overlay-Netze die Nutzdaten verschlüsselt übertragen sollen, auch ESP-Pakete passieren lassen.

Welche Knoten aktiv sind und welche Rollen sie ausfüllen, verrät der folgende Befehl:

```
docker node ls
```

Anschließend können Sie den ersten Service in Ihrem Schwarm loslassen:

```
docker service create --detach=false   
  --name www --replicas 3   
  --constraint node.role==worker   
  --publish 80:80 containous/whoami
```

Das Container-Image „containous/whoami“ enthält einen minimalen Webserver, der beim Abfruf der Startseite in einem Browser einige Informationen über seine

Laufzeitumgebung ausspuckt, etwa seine IP-Adresse(n) und den Hostnamen. So können Sie nachvollziehen, welcher Task (letztlich welcher Container) eine Anfrage beantwortet hat.

Die übrigen Parameter bewirken Folgendes: Sie zeigen beim Erstellen des Service den Fortschritt an, geben dem Service den Namen „www“, fordern drei laufende Tasks an, gestatten das Ausführen nur auf den Arbeitern und sorgen dafür, dass der Webserver auf Port 80 für die Außenwelt erreichbar ist. Welcher Knoten, welchen Task für einen Service ausführt, erfahren Sie anschließend mit dem Befehl

```
docker service ps www
```

Mit

```
docker service scale www=1
```

reduzieren Sie die Anzahl der laufenden Tasks auf eins. Einen Knoten Ihres Schwarms befreien Sie schließlich von aller Arbeitslast, indem Sie Docker dazu auffordern:

```
docker node update   
  --availability drain swarm2
```

Der Name „swarm2“ ist der Hostname des Knotens, den Docker beim Einrichten des Schwarms übernimmt.

Helfershelferhelfer

Wie bereits erwähnt, führt man die Handgriffe zum Starten von Services eher nicht manuell aus, sondern fasst alle Services, die zu einer Anwendung gehören, in einem Stack zusammen. Die Docker-Macher greifen auch hier wieder auf Dateien im YAML-Format zurück, die den Inhalt eines Stacks beschreiben – sie entsprechen weitgehend den mit Docker-Compose eingeführten Dateien, aber es gibt einige subtile Unterschiede.

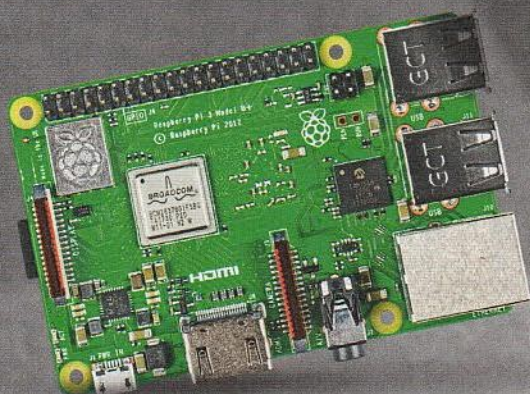
Zunächst ein Trivialbeispiel für die zuvor von Hand mit `docker service create` gestarteten whoami-Webserver:

```
version: '3'   
services:   
  whoami:
```

NEU
+ portofrei

Im heise shop:

Der neue Raspberry Pi 3 B+



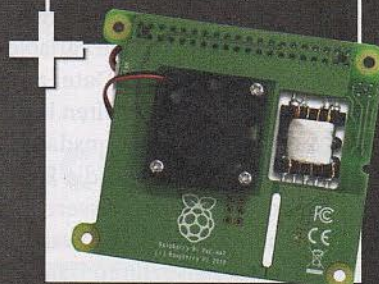
Mehr Power für Ihre Projekte!

- Ca. 10% mehr Leistung (1,4 GHz)
- Gigabit-LAN über USB 2.0 (300 Mbit/s max.)
- WLAN: 2,4 oder 5 GHz (IEEE 802.11ac)
- Bluetooth 4.2
- Vollständig HAT-Kompatibel
- Verbessertes Temperaturmanagement

Perfekt dazu:

PoE HAT-Modul

- speziell für Raspberry Pi 3 B+
- Strom per Ethernet-Kabel
- optimal für IoT- und Embedded-Projekte



Ab einem Einkaufswert von 15 € und für Heise Medien- und Maker Media-Abonnenten sind alle Produkte versandkostenfrei. Preisänderungen vorbehalten.

Jetzt Raspberry Pi und viel Zubehör portofrei im heise shop bestellen!

shop.heise.de/raspi-plus

heise shop

shop.heise.de/raspi-plus




```
image: containous/whoami
deploy:
  replicas: 3
  restart_policy:
    condition: on-failure
ports:
  - 80:80
```

Diese minimale YAML-Datei startet aus dem aktuellen Verzeichnis mit `docker-stack deploy -c ./datei.yml mystack` einen Stack namens „mystack“. Der Name dient als Präfix für die eingerichteten Services, Container und Netze. Der Stack besteht aus einem dreifach laufenden `whoami`-Task. Sie können den Load-Balancer und das Ingressnetz in Aktion erleben, wenn sie mit verschiedenen Webbrowsern auf die Knoten verbinden.

Wer mit Docker-Compose mehrere Container in einem Schlag startet, lagert für die individuelle Konfiguration solcher Anwendungen in der Regel Umgebungsvariablen in eine `.env`-Datei aus. Dort stehen Passwörter, Netzwerkadressen und weitere Details. Beim Start mit `docker-compose up` werden die Variablen dann eingelesen. Der analoge Befehl zum Anlegen eines Stacks `docker create stack` liest ebenfalls eine YAML-Datei, ignoriert aber `.env`-Dateien.

Aus Compose mach Stack

Wer bestehende YAML-Dateien für Docker-Compose hat, die weidlich von `.env`-Dateien Gebrauch machen, muss sie nicht gleich umschreiben. Langfristig dürften die kommenden Docker Apps helfen, YAML-Dateien ähnlich zu parametrisieren. Aber auch jetzt schon kann Docker-Compose helfen:

```
docker-compose config -f ./my.yml
```

liest neben der YAML-Datei auch die `.env`-Datei ein, erledigt alle Ersetzungen von Platzhaltern durch die Variablenwerte und spuckt eine YAML-Datei aus, die `docker stack create` verarbeiten kann.

Für Konfigurationsdateien in einem Schwarm haben sich die Entwickler aber eigentlich etwas Besseres ausgedacht. Container in einem Schwarm können spezielle Dateien in ihren Dateibaum einbinden. Es gibt solche für vertrauenswürdige Daten, etwa Passwörter als „Docker Secrets“ und für unkritische Daten als „Docker Configs“. Nur die erstgenannten bewahrt der Docker-Daemon verschlüsselt auf. Beide Techniken stehen nur zur Verfügung, wenn Docker im Schwarm-

```
ttversion: '3.1'
services:
  db:
    image: mysql:5
    volumes:
      - db_data:/var/lib/mysql
    environment:
      MYSQL_ROOT_PASSWORD_FILE: /run/secrets/db_password
      MYSQL_PASSWORD_FILE: /run/secrets/db_password
    secrets:
      - db_password
  deploy:
    placement:
      constraints: [node.role == manager]
  networks:
    default:
      aliases:
        - db
  wordpress:
    image: wordpress:latest
    ports:
      - "8000:80"
    links:
      - db
    environment:
      WORDPRESS_DB_HOST: db
      WORDPRESS_DB_USER: root
      WORDPRESS_DB_PASSWORD_FILE: /run/secrets/db_password
    secrets:
      - db_password
  secrets:
    db_password:
      file: db_password.txt
  volumes:
    db_data:
```

Die YAML-Dateien, die Docker Compose frisst, ähneln stark dem Input, den Docker für einen Stack erwartet. Einige Dinge fallen weg, wie etwa das Ersetzen von Variablen via `.env`-Datei, andere kommen hinzu, etwa Docker Secrets, um geschützt Passwörter in Container zu übermitteln.

modus läuft – dann auch in Docker-Compose. Auf der Kommandozeile lassen sich beide Gebilde per `docker secret` oder `docker config` mit den üblichen Befehlen zum Erstellen, Auflisten, Einsehen und Löschen (`create`, `ls`...) bearbeiten. So legt

```
echo "Hiho" | docker &
secret create password -
```

ein lausiges Geheimnis als Secret „password“ an. Beim Erstellen eines Service mit `docker service create` lassen sich mit `--secret` und `--config` gezielt solche Daten in Container hineinreichen und darüber bestimmen, wo im Dateibaum des Containers ihre Inhalte als Datei erscheinen.

Für den Einsatz dieser Technik vorbereitete Container (das ist leider nur ein Bruchteil der heute gängigen) kennen deshalb mehrere Möglichkeiten Passwörter zu setzen: zum einen Umgebungsvariablen wie `MYSQL_ROOT_PASSWORD`, die direkt

das Passwort transportieren, zum anderen mit `MYSQL_ROOT_PASSWORD_FILE` Verweise auf Dateien mit dem Passwort – ein solcher Verweis kann auf ein Secret zeigen.

Docker Secrets und Configs sind für alle Knoten eines Schwarms erreichbar. Solange ein aktiver Container sie referenziert, lassen sie sich nicht löschen. Zum Ändern eines Passworts legt man deshalb ein neues Docker Secret an und fügt es dem Container zu Laufzeit mittels `docker service update --secret-add` hinzu und veranlasst dann im Container die Änderung.

Praxisfragen

Leider sind Docker Secrets und Configs eine Einbahnstraße: Zugriff ist aus den Containern nur lesend möglich. Das heißt, sie lassen sich nicht dazu verwenden, Daten wie zum Beispiel Zertifikate, die ein Container beschafft hat, dort zwi-

schenzuspeichern oder – wie das Vorangegangene zeigt – auch das Passwort eines Service dort in aktualisierter Fassung abzugeben. Änderungen müssen immer von außen gemacht werden und sind mit den genannten Umständen verbunden.

Wem die Möglichkeiten an dieser Stelle nicht genügen, das nächste Level in Form einer Kubernetes-Installation aber zu viel erscheint, wird in Helfern wie `etcd` und `confd` womöglich Alternativen finden. Mit dem `etcd`-Dienst lassen sich Konfigurationsdaten speichern und verteilen – er arbeitet auf Wunsch als Cluster also redundant und erlaubt es Containern, auch Daten zu schreiben (mit passender Client-Software im Container). Mit `confd` steht ein Helfer bereit, der Daten aus `etcd` ausliest und in Konfigurationsdateien im Container einflechtet.

Nicht nur an dieser Stelle merkt man, dass Docker Swarm eher ungeeignet ist, um Container zu betreiben, die Daten mit sich herumtragen. Das bestätigt sich auch an anderen Stellen: Versucht man, mit

NFS im Schwarm zumindest rudimentär gemeinsamen Speicherplatz bereitzustellen, stößt man auf weitere Einschränkungen: Swarm-Services können nicht mit mehr Privilegien versehen werden (wie bei `docker create --privileged`). Ebenso wenig funktionieren andere Techniken zum Erlangen höherer Rechte in einem Container (`CAP_SYS_ADMIN`). Das heißt, man kann keinen NFS-Server als Teil eines Schwarms starten, sondern muss ihn von Hand in einem Container oder direkt auf der Hardware laufen lassen. Diese Einschränkungen betreffen letztlich jedes Container-Image, das weitergehende Rechte braucht, etwa um USB-Geräte einzubinden. In der Regel bleibt dann nur, diese außerhalb des Schwarms zu betreiben.

Unterm Strich untermauern auch die zuletzt genannten Grenzen, dass die Qualitäten eines Schwarmbetriebs nun mal darin liegen, Software auszuführen, die stateless und von der Hardware unabhängig funktioniert. Idealerweise baut man die selbst und bewahrt die Daten außer-

halb des Schwarms auf, etwa in einer Datenbank oder auf anderen speziellen Speichern. Die großen Cloud-Hoster haben entsprechende Dienste alle im Angebot.

Falls Sie sich das bis hierher mehrfach gefragt haben: Dieser Artikel ignoriert die Besonderheiten des Schwarmbetriebs unter Windows, der laut Dokumentation durchaus möglich sein soll. Nach bisherigen durchwachsenen Erfahrungen mit Docker unter Windows haben wir angesichts der Einschränkungen und Schwierigkeiten schon unter Linux Abstand von etwaigen Experimenten mit Windows-Schwärmen genommen. (ps@ct.de) **ct**

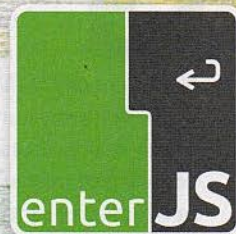
Literatur

- [1] c't Smart Home: <http://ct.de/-4249476>
- [2] Peter Siering, Softwarefabrik, GitLab CI/CD: Mietserver bauen Software, c't 25/2017, S. 88
- [3] Peter Siering, Umbauanleitung, Docker-Container für Heim- und Webserver, c't 15/2017, S. 110

Tutorials, lesenswerte Vertiefungen:
ct.de/ybpbj

bis 28. Juni 2019
mstadium, Darmstadt

enterJS 2019



Angular, React, Node.js?

Ganz egal, Hauptsache mit **JavaScript!**

Programm in Kürze online!

Sponsoren

ZIG COFINPRO

Bronzesponsor

adesso business.
people.
technology.

Veranstalter



heise Developer

dpunkt.verlag

www.enterjs.de



Privatsphärenpflege

Raspberry Pi: Den DNS-Filter Pi-hole aktualisieren und erweitern

Viele Raspberry-Nutzer setzen auf dem Mini-Computer den DNS-Filter Pi-hole ein, um Schadcode, Werbung und Tracker aus ihrem Netz fernzuhalten. Wir fassen die wichtigsten Schritte zur Pflege des kleinen Helfers zusammen. Dazu zählen auch DNS-Verschlüsselung und verbesserte Ausfallsicherheit.

Von Dušan Živadinović und Carsten Strotmann

Am Anfang fast jeder Internet-Verbindung steht die Abfrage der Ziel-IP-Adresse. Dafür befragen Internet-fähige Geräte das Domain Name System – eine weltweit verteilte Datenbank, die menschenlesbare Domainnamen zu IP-Adressen auflöst (DNS). Ursprünglich wurde für den DNS-Verkehr keine Verschlüsselung spezifiziert.

Deshalb schickt auch der DNS-Filter Pi-hole seine Anfragen im Klartext durch das Internet und Dritte können die Pakete auf der Strecke zum DNS-Server leicht mitlesen. Inzwischen gibt es mehrere Verfahren zum Verschlüsseln des DNS-Verkehrs. Die wichtigsten sind DNS-over-HTTPS und DNS-over-TLS (DoH und DoT). Wie man Pi-hole mit DoT nachrüstet, haben wir anhand des kompakten DNS-Resolvers Stubby gezeigt [1].

Um das Ausfallrisiko des Pi-hole zu minimieren, soll Stubby von dem ebenfalls verschlüsselnden DNS-Proxy dnss Unterstützung erhalten. Der springt ein, falls Stubby ausfällt oder gewartet werden muss.

Wir gehen davon aus, dass Sie auf Ihrem Raspi Pi-hole bereits eingerichtet haben. Wie das geht, steht in c't 11/2018 [2]. Für die Umsetzung der Anleitungen in diesem Beitrag sind grundlegende Terminal-Kenntnisse erforderlich.

Boxenstopp

Vor jeglichen Änderungen sollten Sie ein Image der SD-Karte anlegen. Je nach Backup-Verfahren fällt dabei der Pi-hole-gestützte DNS-Dienst für eine Weile aus. Damit das im LAN nicht spürbar wird, öffnen Sie die DNS-Konfiguration Ihres Routers, notieren Sie die DNS-IP-Adresse

(sie verweist auf den Raspi und damit Pi-hole) und stellen Sie dann die DNS-Auflösung zurück auf die Vorgabe des Routers.

Nun können Sie den Raspi herunterfahren:

```
sudo shutdown -h now
```

Trennen Sie ihn vom Strom und entnehmen Sie ihm die SD-Karte. Legen Sie auf Ihrem PC ein Image an. Auf Windows kann man dafür den Win32 Disk Imager nutzen (siehe ct.de/yt3y), auf Linux und macOS den Befehl `dd`:

```
sudo dd bs=4M if=/dev/sdb of=raspi.img
```

Im obigen Beispiel liest das `dd`-Kommando die Daten vom Laufwerk `sdb` aus. Unter welcher Laufwerksbezeichnung die SD-Karte auf Ihrem Mac oder Linux-PC geführt wird, verrät das Kommando `sudo fdisk -l`. Zum Zurückspielen eines Backups eignen sich dieselben Tools.

Aktualisierung prüfen

Wenn das Backup angelegt ist, setzen Sie die SD-Karte wieder in den Raspi ein und starten Sie ihn. Stellen Sie den DNS-Eintrag in Ihrem Server zurück auf die IP-Adresse des Raspi.

Normalerweise aktualisiert sich ein Pi-hole automatisch. Um ihn bei Bedarf manuell zu aktualisieren, geben Sie

```
pihole -up
```

ein. Der Vorgang dauert einige Minuten und gibt zahlreiche Statusmeldungen aus. Am Ende sollte die eingespielte Versionsnummer stehen (z. B. 4.2.1).

Falls etwas schiefgegangen ist: Das Update-Protokoll finden Sie in der Datei `/etc/pihole/install.log`. Einträge, die mit „error“ oder „fail“ markiert sind, sollten Hinweise auf die Fehlerursache liefern.

Mehr DNS-Verschlüsselungen

Pi-hole nutzt für die DNS-Kommunikation den kompakten DNS- und DHCP-Server `Dnsmasq`. Dieses Programm wird auf absehbare Zeit vermutlich weder DoH noch DoT erhalten [3]. Wer den DNS-Verkehr dennoch verschlüsseln will, muss vor `Dnsmasq` einen Proxy schalten. Dafür muss man generell eine etwas höhere Latenz in Kauf nehmen, denn mit dem DNS-Proxy kommt eine zusätzliche Verarbeitungsstation auf dem Weg zum DNS-Server hinzu. Außerdem kommunizieren verschlüsselnde Proxys grundsätzlich nicht

mehr per UDP, sondern mit TCP/TLS, was die Latenz ebenfalls ein wenig erhöht.

Der verschlüsselnde DNS-Proxy `Stubby` löst eine angefragte Domain nicht selbst zur IP-Adresse auf, sondern überlässt das dem vorgeschalteten DNS-Server. Es handelt sich also um einen Stub-Resolver (Stummel) – daher auch der verniedlichende Name.

Manche User möchten statt `Stubby` einen Resolver mit größerem Funktionsumfang vor den Pi-hole schalten, etwa `Unbound` oder `BIND`. Das sollte man nicht tun. `Unbound` eignet sich beispielsweise für Caching, Resolving, DNS-over-TLS, DNSSEC-Validierung, Ad-Blocking und für lokale DNS-Daten kleiner Netze. Aber `Dnsmasq` eignet sich bis auf DoT für dieselben Anwendungen, sodass man sie mit `Unbound` nur unnötig verdoppeln würde. In Kombination mit `Dnsmasq` ist `Stubby` daher die bessere Wahl.

Falls `Stubby` ausfällt, fällt auch Pi-hole aus. Um die Verfügbarkeit des DNS-Dienstes zu erhöhen, sollte man im Router neben Pi-hole einen weiteren DNS-Server eintragen – beispielsweise den vom Provider voreingestellten. Um die Pi-hole-Verfügbarkeit bei gleichzeitiger Verschlüsselung zu erhöhen, kann man einen weiteren verschlüsselnden Proxy auf dem Raspi einrichten.

Wer seine Privatsphäre wahren möchte, nimmt am besten mit Proxys vorlieb, die auch nichtkommerzielle DNS-Server ansprechen können. Eine gute Alternative wäre das quelloffene, in Go geschriebene Projekt `dnss` von Alberto Ber-

togli. Im Test funktionierte das aktuell für den Raspi angebotene Paket aber nicht zuverlässig. Alternativ kann man den DoH-Proxy `cloudflared` einrichten. Der kommuniziert zwar ausschließlich mit Resolv-ern des kommerziellen DNS-Anbieters Cloudflare. Als Notnagel, also wenn `Stubby` ausfällt oder gewartet werden muss, ist `cloudflared` okay.

DNS-Over-HTTPS hinzufügen

Der Hersteller bietet `cloudflared` als vorkompiliertes Binary zum Download an. So laden und installieren Sie es im Ordner `/usr/local/bin`:

```
wget https://bin.equinox.io/c/3VdrWdbjqyF/cloudflared-stable-linux-arm.tgz
tar -xvzf cloudflared-stable-linux-arm.tgz
sudo cp ./cloudflared /usr/local/bin
```

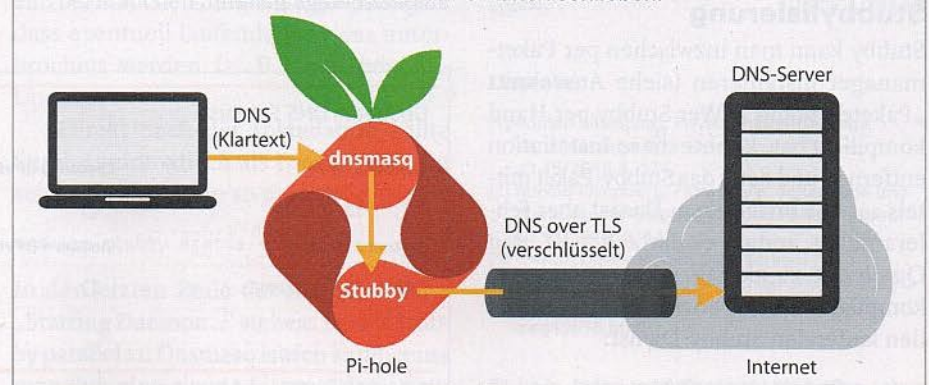
Testen Sie, ob das Tool korrekt läuft mit dem Befehl `cloudflared -v`. Damit die Software nach jedem Booten automatisch startet, sind einige Vorarbeiten nötig. Fügen Sie der Passwortdatenbank den User `cloudflared` hinzu:

```
sudo useradd -s /usr/sbin/nologin -r -M cloudflared
```

Erstellen Sie eine Konfigurationsdatei mit dem Befehl `touch /etc/default/cloudflared`. Öffnen Sie sie mit dem Editor Ihrer Wahl und fügen Sie diesen Inhalt ein:

Verschlüsselte DNS-Anfragen mit DNS over TLS

`Stubby` verschlüsselt die DNS-Anfragen, ehe sie durchs Internet geschickt werden. Wer den Datenverkehr belauscht, kann durch die DNS-over-TLS-Pakete nicht aufs Surfverhalten schließen.




```
CLOUDFLARED_OPTS="--port 5053 --upstr_
team https://1.1.1.1/dns-query --
upstream https://1.0.0.1/dns-query
```

Stellen Sie passende Zugriffsrechte ein:

```
sudo chown cloudflared:cloudflared_
/etc/default/cloudflared
sudo chown cloudflared:cloudflared_
/usr/local/bin/cloudflared
```

Laden Sie das Systemd-Skript von [ct.de/yt3y](https://github.com/ctde/yt3y) und kopieren Sie es an sein Ziel:

```
sudo cp cloudflare.service
/lib/systemd/system/
```

Aktivieren Sie den Systemd-Service:

```
sudo systemctl enable cloudflared
```

In der Ausgabe des Kommandos sollte unter anderem stehen „Created symlink...“. Start Sie den Dienst und prüfen Sie, ob er läuft:

```
sudo systemctl start cloudflared
sudo systemctl status cloudflared
```

Testen Sie mit dem dig-Kommando, ob die Auflösung klappt:

```
dig @127.0.0.1 -p 5053 ct.de
```

Der Befehl schickt eine DNS-Anfrage an die lokale Loopback-Adresse 127.0.0.1, Port 5053. In der Ausgabe sollte die IP-Adresse unserer Domain aufgeführt sein. In der vorletzten Zeile sollte stehen server: 127.0.0.1#5053.

Öffnen Sie im Browser die pi-hole-Einstellungen und dort den DNS-Bereich. Tragen Sie im Feld „Custom 2 (IPv4)“ diese Zeichenkette ein: 127.0.0.1#5053. Setzen Sie das Häkchen davor, um den Eintrag zu aktivieren. Das Feld „Custom 1 (IPv4)“ sollten Sie Ihrem bevorzugten DNS-Proxy überlassen, also etwa Stubby oder einem anderen DNS-Server Ihrer Wahl.

Stubbylisierung

Stubby kann man inzwischen per Paketmanager installieren (siehe Ausschnitt „Paketempfang“). Wer Stubby per Hand kompiliert hat, könnte diese Installation entfernen und dann das Stubby-Paket mittels apt-get installieren. Das ist aber fehleranfällig, sodass es einfacher ist, den Quellcode zu aktualisieren und neu zu kompilieren. Stoppen Sie dafür zunächst den laufenden Stubby-Dienst:

```
sudo systemctl stop stubby
```

Falls auf Ihrem Raspi ein Fallback-DNS-Proxy läuft, sollte die DNS-Auflösung von Pi-hole reibungslos weiterlaufen. Falls nicht: Aktivieren Sie in Pi-hole im Admin-Interface vorübergehend einen der von Pi-hole voreingestellten Upstream-Resolver, etwa Google oder Quad9.

Wechseln Sie mit cd in das Verzeichnis, in dem der Quellcode liegt. Laden Sie den aktuellen Quellcode von GitHub und kompilieren Sie ihn:

```
git pull https://github.com/_
getdnsapi/getdns.git
git submodule update --init
libtoolize -ci
autoreconf -fi
mkdir build
cd build
../configure --prefix=/usr/local_
--without-libidn --without-_
libidn2 --enable-stub-only_
--with-stubby
make
```

Installieren Sie die neue Version mit sudo make install und aktualisieren Sie den Bibliotheken-Cache mit dem Befehl sudo sbin/ldconfig.

Prüfen Sie nun, auf welchem Port Stubby auf eingehende DNS-Anfragen wartet (listen_addresses). Öffnen Sie dazu die Konfigurationsdatei mit sudo nano /usr/local/etc/stubby/stubby.yml. Steht dort 127.0.0.1:5353, ersetzen Sie die Angabe mit 127.0.0.2:53. Port 5353 ist nämlich dem Avahi-Daemon für die lokale Multicast-DNS-Kommunikation vorbehalten. Kommentieren Sie außerdem die IPv6-Loopback-Adresse aus:

```
listen_addresses:
- 127.0.0.2:53
#- 0::1
```

So erwartet Stubby DNS-Anfragen zwar wieder auf Port 53, den auch Dnsmasq benutzt, aber sie verwenden unterschiedliche Loopback-Adressen, sodass sie sich aus dem Wege gehen.

Wenn Sie schon dabei sind, aktivieren Sie im Abschnitt darunter die Sicherheitstechnik DNSSEC, indem Sie das Kommentarzeichen von dieser Zeile entfernen:

```
dnssec: GETDNS_EXTENSION_TRUE
```

Speichern Sie die Änderungen mit Strg+X, y. So kann Stubby signierte DNS-Antworten auf Unverfälschtheit und deren Quelle auf Vertrauenswürdigkeit prüfen. Die gesamte DNSSEC-Einrichtung ist tatsächlich mit dieser einen Änderung erledigt. Anders als bei vielen anderen Resolvern muss man sich nicht um den Download des erforderlichen Trust Anchors kümmern – Stubby holt das Stöckchen selbstständig. Sollte bei einer Antwort die Validierung scheitern, muss Stubby von einer Attacke ausgehen und darf die erhaltene IP-Adresse nicht weitergeben. Ein Browser meldet dann, dass er die angesteuerte Domain nicht erreichen kann.

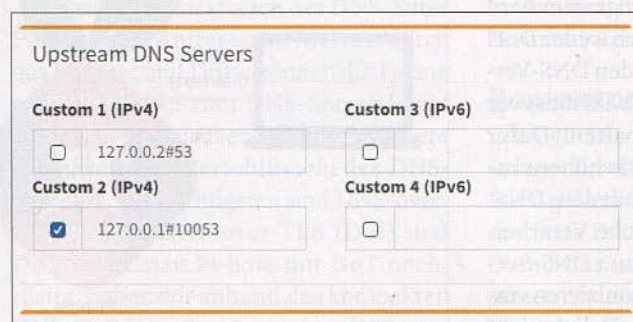
Ist DNSSEC erst mal eingeschaltet, muss man nichtvalidierende Resolver aus jeglichen Konfigurationen entfernen (Pi-Hole, Router, Computer ...). Andernfalls gibt es bei einem DNSSEC-Sicherheitsproblem einen Rückfall auf ungesichertes DNS, was den DNSSEC-Schutz aushebeln würde. Sollte Stubby mal die DNS-Antwort schuldig bleiben, prüfen Sie unbedingt, woran das liegt, bevor Sie nichtvalidierende Resolver in Betrieb nehmen. Andernfalls kann es passieren, dass Sie über nichtvalidierende Resolver einer gefälschten DNS-Antwort aufsitzen.

Belassen Sie den Rest der Stubby-Einstellungen, wie er ist, und starten Sie den Dienst wieder:

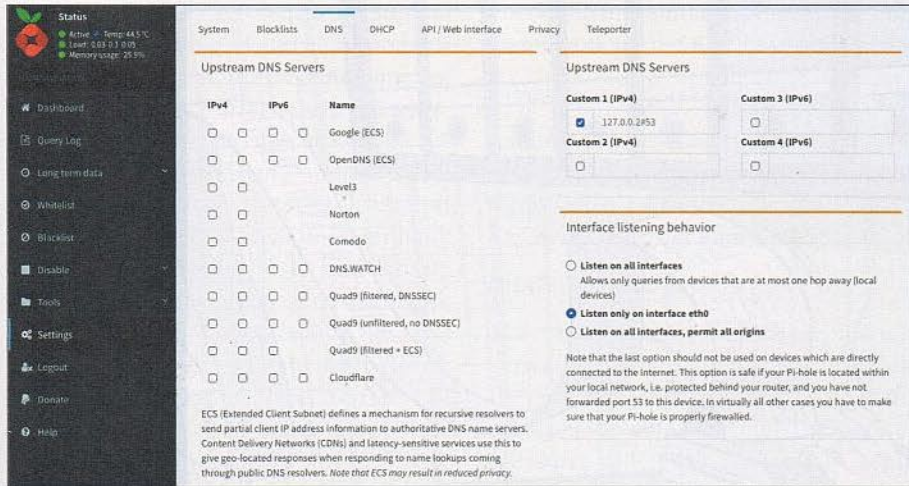
```
sudo systemctl start stubby
```

Nun sollte Stubby an der Loopback-Adresse 127.0.0.2 lauschen. Testen Sie, ob das der Fall ist, indem Sie diesen Befehl in einem zweiten Terminal eingeben:

```
dig @127.0.0.2 ct.de
```



Hilfs-DNS-Proxy: Richtet man den DoH-Proxy dnss auf dem Raspi ein, springt der ein, während man Stubby wartet und umgekehrt. So läuft unterdessen der Pi-hole-Dienst reibungslos weiter.



Pi-hole kommuniziert ab Werk mit kommerziellen DNS-Servern. Man kann aber auch einen lokalen Stub-Resolver einrichten. Hier schickt Pi-hole DNS-Anfragen an die Loopback-Adresse 127.0.0.2 auf Port 53.

Der Befehl sollte die aktuelle IPv4-Adresse unserer Domain liefern und unten sollte in der Zeile `SERVER` die Adresse des antwortenden Servers stehen, also 127.0.0.2. Testen Sie nun die DNSSEC-Funktion:

```
dig @127.0.0.2 fail01.dnssec.works
```

Diese Domain ist für Prüfzwecke aufgesetzt und der Befehl sollte den Fehlercode „SERVFAIL“ liefern. Kommt stattdessen ein NOERROR mit einer IPv4-Adresse zurück, so greift der DNSSEC-Schutz nicht. Überprüfen Sie dann die Stubby-Konfiguration.

Mit dieser Abfrage sollte Stubby hingegen korrekt signierte DNS-Antworten erhalten und validieren:

```
dig @127.0.0.2 postbank.de
```

Im oberen Bereich sollte status: NOERROR aufgeführt sein und darunter im Feld `flags` die zusätzliche Flagge `ad` stehen (authenticated data). Ist das der Fall, hat Stubby eine signierte Antwort erhalten. Diese ist unverfälscht und die Quelle der Antwort vertrauenswürdig.

Aktivieren Sie in Pi-hole wieder Stubby als Upstream-Resolver und schalten Sie Google oder was immer sie ersatzweise eingestellt hatten, wieder ab. Damit ist das Update erledigt und Pi-hole sollte seine DNS-Anfragen wieder an Stubby schicken, der sie dann verschlüsselt weitergibt.

Paketempfang

Wer Stubby noch nicht für Pi-hole verwendet, kann das Tool über den Paketmana-

ger `apt-get` installieren. Beim aktuellen Raspbian (Debian Stretch) ist es im Paket `getdns-utils 1.1.0~a2-2` versteckt. Das ist jedoch veraltet und enthält keine Konfigurationsdatei.

Wir haben stattdessen die am 11. Januar erschienene Stubby-Version 0.25 aus dem Buster-Repository erfolgreich auf einem Raspi 3B eingesetzt. Buster ist freilich noch im Teststadium. Falls Sie Stubby 0.25 ausprobieren wollen: Legen Sie ein Backup vom Raspi an und fügen Sie den Bezugsquellen das Buster-Repository hinzu (`nano /etc/apt/sources.list`). Fügen Sie der ersten Zeile `testing` hinzu, sodass sie folgendermaßen aussieht:

```
deb http://raspbian.raspberrypi.org/
raspbian/ testing main contrib non-
free rpi
```

Aktualisieren Sie die Paketliste mit `apt-get update` und installieren Sie Stubby mit `apt-get install stubby`. Je nach Bestückung Ihres aktuellen Raspbian installiert `apt-get` nun eine Hand voll Pakete. Für manche blendet der Installer Begleittexte ein, bei manchen muss man genehmigen, dass eventuell laufende Services unterbrochen werden (z. B. bei OpenSSL-Updates).

Direkt nach der Installation sollte Stubby automatisch als Dienst gestartet sein. Das kann man so prüfen:

```
service stubby status -l
```

In der letzten Zeile der Ausgabe sollte „Starting Daemon...“ stehen. Damit Stubby parallel zu `Dnsmasq` laufen kann, muss man ihm eine eigene Listen-Adresse zu-

weisen. Editieren Sie dafür `/etc/stubby/stubby.yml`. Ändern Sie die Listen-Adresse und schalten Sie DNSSEC ein wie im Abschnitt „Stubbylisierung“ beschrieben.

Navigieren Sie dann zum Abschnitt `Upstreams` und stellen Sie sicher, dass mindestens je eine DNS-Resolver-IP-Adresse für IPv4 und IPv6 eingetragen ist. Normalerweise sollten sogar mehrere vorhanden und aktiv sein. Weitere Vorschläge finden Sie darunter im Abschnitt `Optional Upstreams`. Damit Stubby die gewünschten zusätzlichen Server verwendet, genügt es, die Kommentarzeichen `#` zu entfernen. Zu beachten ist, dass Server von kommerziellen Anbietern wie Cloudflare (1.1.1.1) zwar schnell antworten und zuverlässig erreichbar sind, aber Verbindungsprotokolle speichern und auswerten. Wenn Sie das vermeiden wollen, lassen Sie die Kommentarzeichen vor den kommerziellen Servern stehen. Speichern Sie die Änderungen und starten Sie Stubby neu:

```
service stubby restart
```

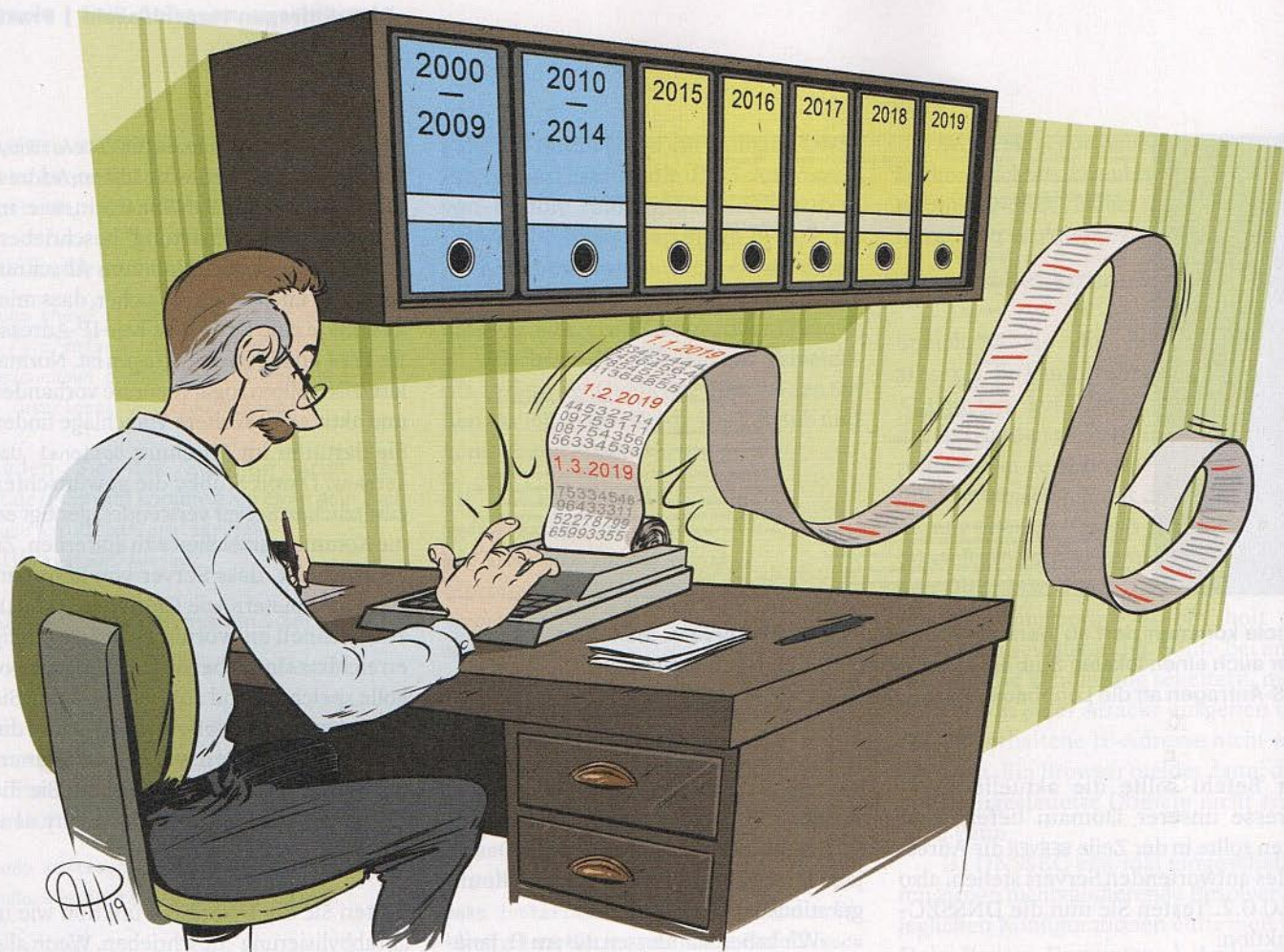
Testen Sie die DNSSEC-Funktion wie in „Stubbylisierung“ beschrieben. Wenn alle Ampeln auf Grün sind, öffnen Sie das Admin-Interface von Pi-hole im Browser und dort die DNS-Einstellungen. Schalten Sie alle Upstream-DNS-Server ab, also auch den Hilfsproxy `dnss`, und fügen Sie im Feld „Custom 1 (IPv4)“ die IP-Adresse 127.0.0.2#53 ein. Stellen Sie sicher, dass der Pi-hole ebenfalls die DNSSEC-Validierung anwendet, damit die Sicherheitstechnik durchgängig angewendet wird. Klicken Sie unten rechts auf „Save“, um die Änderungen zu speichern und zu aktivieren.

Damit sind Pi-hole und Stubby eingerichtet und Pi-hole sollte auf seinem Dashboard anzeigen, dass DNS-Anfragen eingehen und bearbeitet werden. Sollte Stubby einmal ausfallen, deaktivieren Sie den zugehörigen DNS-Eintrag in Pi-hole und aktivieren Sie den Hilfs-Proxy `dnss`, um den Fehler ohne Zeitdruck zu beseitigen. (dz@ct.de) **ct**

Literatur

- [1] Ronald Eikenberg, Privatsphären-Upgrade, Verschlüsselte DNS-Anfragen mit Pi-hole, c't 15/2018 S. 174
- [2] Ronald Eikenberg, Filterbeere, Schadcode und Werbung mit Raspberry Pi und Pi-hole filtern, c't 11/2018, S. 144
- [3] Warum Dnsmasq den DNS-Verkehr nicht verschlüsselt: <https://www.mail-archive.com/dnsmasq-discuss@lists.thekelleys.org.uk/msg12016.html>

Pi-hole-Infos und Tools: ct.de/yt3y



Geschichtsschreiber

InfluxDB: Spezialisierte Datenbank für Messwerte und Logging

Eine SQL-Datenbank ist meist die erste Wahl für alle Arten von Daten. Für Messwerte ist der Generalist aber nicht unbedingt die beste Lösung. Eine Zeitreihendatenbank wie InfluxDB arbeitet schneller und kann alte Daten automatisch zusammenfassen.

Von Jan Mahn

Messwerte können aus vielen Quellen stammen: zum Beispiel von physischen Sensoren, seien sie im vernetzten Zuhause, im Rechenzentrum oder in einer Industrieanlage. Aber auch Software kann

Messwerte produzieren: Prozessor- und Netzwerkauslastung, Anzahl von Anfragen oder Bestellungen. Gründe, solche Messwerte zu speichern, gibt es ebenfalls viele: um Ursachen für Probleme zu finden, Durchschnittswerte zu berechnen oder übersichtliche Diagramme zu generieren.

Wer schon eine relationale Datenbank wie MySQL, MariaDB oder SQL Server im Einsatz hat, ist versucht, diese Datenbank auch für Zeitreihendaten, also die Zuordnung von Messwerten zu Datum und Uhrzeit, einzusetzen. Um zu verstehen, welches Problem Zeitreihendatenbanken lösen, kann man das Vorgehen bei einer MySQL-Datenbank einmal durchdenken. Es genügt eine Tabelle mit drei Spalten: Name des Messwerts, gemessener

Wert, Zeitstempel. Das Speichern klappt mit `INSERT INTO` noch problemlos.

Datenbergbau

Probleme gibt es aber bei der Auswertung großer Datenmengen. Angenommen, 10 Temperatursensoren melden alle 30 Sekunden einen Messwert an die Datenbank. Das ergibt 28.800 Messwerte am Tag und über 10 Millionen im Jahr. Bei der Auswertung stellt man aber schnell fest, dass die einzelnen Messwerte für sich wertlos sind – interessant ist nicht die Information, dass die Temperatur am 5. Juni 2018 um 12:34:56 genau 25,1 Grad betrug. Stattdessen sucht man nach aggregierten Daten, also zusammenfassenden Werten für bestimmte Zeitabschnitte, zum Beispiel Höchst- und Niedrigstwerte pro

Tag oder Durchschnittswerte pro Stunde. Solche Berechnungen kann man durchaus mit SQL-Abfragen immer dann generieren, wenn sie jemand lesen will. Dazu bastelt man ein Skript, das geschickt mit GROUP BY-Anweisungen und den Datumsfunktionen der verwendeten Datenbank hantiert und Daten aus der MySQL-Datenbank holt. Wer eine solche Lösung im Einsatz und viele Messwerte in der Datenbank hat, bemerkt aber irgendwann, dass das Aggregieren spürbar Rechenzeit kostet. Soll aus den Durchschnittswerten ein Diagramm gezeichnet werden, nervt die Wartezeit richtig.

Schöner wäre es doch, die Daten regelmäßig zu Blöcken zusammenzufassen, die Aggregate in einer neuen Tabelle abzuspeichern und sich von alten Daten zu trennen. Kein Problem für den SQL-Entwickler – mit einem weiteren Skript und einem Cron-Job unter Linux oder einer geplanten Aufgabe unter Windows. Wirklich übersichtlich und leicht zu warten ist diese Lösung aber nicht. Perfekt wäre es dagegen, wenn die Datenbank diese Aufgaben selbst übernehmen könnte. All diese Funktionen bekommt man, wenn man seine Daten gleich in einer Zeitreihendatenbank ablegt, die genau für diese Anwendung erfunden wurde.

Inselbegabung

Große Verbreitung unter den Zeitreihendatenbanken (Time Series Databases) hat InfluxDB gefunden. Die Software gibt es in einer Open-Source-Ausgabe, die fast alle Funktionen enthält. Nur für den Aufbau eines Clusters aus mehreren Datenbanken muss man zahlen. InfluxDB gehört zu den NoSQL-Datenbanken – das Schema mit den Tabellenspalten muss also nicht definiert werden, bevor man Werte speichern kann. Es entsteht beim Einfügen von Daten automatisch.

Eine Testinstanz von InfluxDB richten Sie auf Ihrem Linux-, Windows- oder macOS-System am schnellsten mit Docker ein. Wie Sie das installieren und wie Container funktionieren, haben wir in einem Online-Artikel auf dem aktuellen Stand zusammengefasst, zu finden über ct.de/yyyyw. Für InfluxDB gibt es einen offiziellen Docker-Container. Für den Einstieg reicht der folgende Befehl:

```
docker run --name=influxdb
  -d -p 8086:8086 influxdb
```

Docker startet InfluxDB und verbindet Port 8086 der Netzwerkschnittstelle mit

Port 8086 im Container. Diesen nutzt die Datenbank für die Kommunikation. Mit

```
docker exec -it influxdb influx
```

landen Sie im InfluxDB-Kommandozeilenprogramm im Container und können direkt Befehle absetzen. Zunächst braucht das Beispielprojekt eine Datenbank:

```
CREATE DATABASE measure
```

Mit `USE measure` wird diese ab jetzt verwendet. Eine Datenbank ist die Hülle für mehrere Messwertreihen. Die ersten Messpunkte einer Beispiel-Temperaturmessung sollen zur Messreihe „temp“ gehören und zwei Werte enthalten, einen für „inside“ und einen für „outside“:

```
INSERT temp inside=24.2,outside=10.1
```

InfluxDB entscheidet selbst, welcher Datentyp sinnvoll ist – in diesem Fall zwei Floats. Auch Strings, Integer und Bool-Werte sind möglich. Versucht man später, einen Wert eines anderen Typs zu speichern, beschwert sich der Server. Kein Problem ist es aber, später eine Zeile mit einem dritten Wert, zum Beispiel einen String mit dem Namen „middle“ abzuspeichern – einer der Vorteile einer NoSQL-Datenbank.

Jeder Messpunkt bekommt einen Zeitstempel. Gibt man keinen an, setzt InfluxDB den aktuellen. Das sieht man beim Auslesen der gespeicherten Werte. SQL-Nutzern kommt die Syntax bekannt vor:

```
SELECT * FROM "temp"
```

InfluxDB arbeitet mit Unix-Timestamps in Nanosekunden – die Zahl gibt die Nanosekunden seit dem 1. Januar 1970 an.

Wer das nicht im Kopf umrechnen möchte, kann das Kommandozeilenprogramm dazu bringen, ein lesbares Format auszugeben:

```
precision rfc3339
```

Auch die Formatierung der Ergebnisse einer Suche kann man ändern. Möchte man die Werte nicht als Tabelle auf der Kommandozeile betrachten, reichen die Befehle `format json` oder `format csv` für eine JSON- oder CSV-Darstellung.

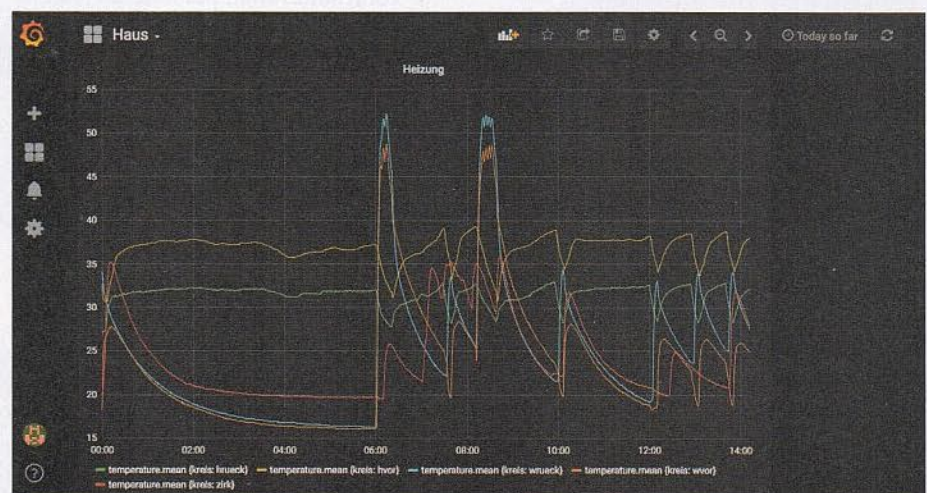
Hat man mehrere Sensoren, muss man nicht für jeden Sensor eine Messreihe eröffnen (mit `INSERT temp_room2`). Stattdessen sollte man mit Tags arbeiten, die man an Messwerte anheftet. Diese werden im INSERT-Befehl direkt nach dem Namen der Messreihe, getrennt durch ein Komma, angegeben. Die Sensorwerte im Beispiel sollen mit einem Namen des Raums und des Gebäudes versehen werden:

```
INSERT temp,room=bad,
  ↳building=ferienhaus
  ↳inside=22.9,outside=11.5
```

Nach den Tags folgt ein Leerzeichen, alles nach diesem interpretiert InfluxDB als Messwert. Nach Tags kann man später effizient filtern. Sie werden von InfluxDB automatisch indiziert, sind also schnell durchsuchbar. Auch die Filter-Syntax entspricht der aus der SQL-Welt:

```
SELECT * FROM temp WHERE
  ↳ "room" = 'bad'
```

Auch nach Messwerten kann man mit WHERE filtern. Das dauert aber, weil die Werte nicht indiziert sind, etwas länger als die Suche nach Tags.



Möchte man die Daten aus InfluxDB ansprechend visualisieren, kann man auf das Open-Source-Programm Grafana setzen.


```
CREATE CONTINUOUS QUERY "temp_1h" ON "temp" BEGIN
  SELECT mean("inside") AS "mean_inside", mean("outside") AS "mean_outside",
    max("inside") AS "max_inside", max("outside") AS "max_outside"
  INTO "oneyear"."temp_calc"
  FROM "temp"
  GROUP BY time(60m)
END
```

Diese Abfrage fasst alle 60 Minuten die Messwerte zu Mittel- und Maximalwerten zusammen und speichert diese in „temp_calc“.

Wegwerfen

Nachdem die Werte in der Datenbank landen, ist es an der Zeit, die automatische Zusammenfassung und Löschung einzurichten. Dazu braucht es eine „Retention Policy“, also eine Regel zur Aufbewahrung von Daten. Die bekommt einen sprechenden Namen, den Namen der Datenbank, in der sie angelegt wird, und eine Laufzeit. Außerdem muss man angeben, auf wie vielen Instanzen die Werte vorgehalten werden – in der Open-Source-Version immer nur einmal. Angelegt wird die Richtlinie mit einem CREATE-Befehl:

```
CREATE RETENTION POLICY ǀ
  "oneyear" ON "measure" ǀ
  DURATION 52w REPLICATION 1
```

Die Regel mit dem Namen „oneyear“ existiert jetzt, hält die Daten 52 Wochen vor, wird aber noch nicht angewendet. Um Messwerte zu speichern, auf die die Regel angewendet wird, übergibt man ihren Namen im INSERT INTO-Befehl:

```
INSERT INTO oneyear temp,room=bad,ǀ
  building=ferienhaus ǀ
  inside=20.1,outside=9.4
```

Soll eine Regel immer dann gelten, wenn man keine andere Regel angibt, kann man sie beim Anlegen mit DEFAULT am Ende als Standardregel definieren.

Zusammenfassen

Die Lösung von InfluxDB für automatische Zusammenfassungen von Daten heißt „Continuous Query“. Als Anwender muss man eine solche nur anlegen, um die Ausführung kümmert sich InfluxDB. Die Beispiel-Temperaturwerte sollen zu einstündigen Blöcken zusammengefasst werden – jeweils ein Durchschnittswert (englisch „mean“) und der Maximalwert für innen und außen sollen in einer neuen Messwertreihe „temp_calc“ landen und dort ein Jahr lang gespeichert bleiben. Den vollständigen Befehl finden Sie auf dieser Seite.

Innerhalb des Befehls muss zwingend eine GROUP BY-Anweisung vorkommen, die angibt, wie groß die Zeitabschnitte sein sollen. Neben Funktionen wie mean() und max() versteht InfluxDB noch zahlreiche weitere Rechenoperationen. Die Dokumentation, zu finden über ct.de/yyyyw, listet die Möglichkeiten auf. Mit einem SELECT-Aufruf kann man sich das Ergebnis ansehen – vorausgesetzt, man wartet eine Stunde oder gruppiert in einem kürzeren Zeitraum. Die Aggregate zeigt:

```
SELECT * FROM temp_calc
```

In der Praxis

Um eine InfluxDB-Instanz in der Praxis einzusetzen, sollte man sich erst einmal einen Plan machen, welche Daten wie lange als Rohdaten vorliegen sollen und welche Aggregate man später braucht – diese Denkarbeit kann die Datenbank nicht abnehmen. Die Genauigkeit kann mit zunehmendem Alter abnehmen: Zwei Wochen lang könnten alle Messwerte für die schnelle Fehlerdiagnose bleiben, zwei Monate lang die stündlichen Zusammenfassungen, dann zehn Monate lang Tageshöchstwerte und so weiter.

Verarbeitet man personenbezogene Daten in der Datenbank, wird der Datenschutzbeauftragte ein Wort bei der Entscheidung über die Zeiträume mitreden. Mit SHOW RETENTION POLICIES bekommt man eine Übersicht über alle angelegten Richtlinien und kann ihm so schnell belegen, wie lange Daten gespeichert werden.

Anders als in der Testumgebung möchte man später nicht über die Kommandozeile mit der Datenbank sprechen. Ein großer Vorteil gegenüber vielen SQL-Datenbanken: InfluxDB nutzt kein eigenes Netzwerkprotokoll, für das man einen eigenen Client bräuchte. Stattdessen stellt der Server ein REST-API über HTTP bereit. Die Anwendung muss also nur HTTP sprechen können. Der Endpunkt

zum Schreiben von Werten heißt /write. Wer die Kommunikation über das Netzwerk testen will, kann ein weiteres Kommandozeilenfenster öffnen und mit Curl einen Messwert schreiben:

```
curl -i -XPOST "http://localhost:8086ǀ
  /write?db=measure" ǀ
  --data-binary 'temp,room=bad ǀ
  inside=15.6'
```

Für viele gängige Programmiersprachen gibt es aber Bibliotheken, die die passenden HTTP-Aufrufe erstellen, sodass man umhinkommt, die komplette Dokumentation für das API zu studieren. Möchte man InfluxDB einsetzen, um Messwerte aus der Hausautomation zu speichern, muss man das Rad ebenfalls nicht neu erfinden. So gibt es etwa für Node-Red ein Plug-in, mit dem man die Daten ganz ohne Programmierarbeit in die Datenbank bekommt.

Wenn Sie sich dafür entscheiden, InfluxDB nicht nur zu Testzwecken im Docker-Container einzusetzen, müssen Sie dem Container ein Docker-Volume übergeben, damit die Daten auch nach einem Neustart des Containers erhalten bleiben. InfluxDB erwartet die Daten innerhalb des Containers im Ordner „/var/lib/influxdb“. Außerdem sollten Sie sich Gedanken darüber machen, welche Applikation auf den Server zugreifen kann – in der Standardkonfiguration steht das HTTP-API ohne Anmeldung offen. Die Dokumentation erklärt, wie Sie Benutzer für Datenbanken einrichten und Zugriffsrechte anlegen.

Administratoren, die Messwerte aus ihren Servern auslesen und in die InfluxDB bringen möchten, können auf ein weiteres Werkzeug der InfluxDB-Entwickler zurückgreifen: „Telegraf“ ist eine handliche, in Go geschriebene Anwendung, die zum Beispiel die Prozessor- und Arbeitsspeicherauslastung ausliest und an die Datenbank meldet – die Installationsanleitung finden Sie über ct.de/yyyyw. über Plug-ins ist die Open-Source-Software Telegraf leicht erweiterbar.

Rund um InfluxDB gibt es noch andere kompatible Open-Source-Projekte anderer Hersteller. Freunde ansprechender und funktionaler Diagramme sollten sich die Visualisierungsplattform Grafana ansehen, die Messwerte einer InfluxDB schnell und schön darstellen kann.

(jam@ct.de) **ct**

Dokumentation: ct.de/yyyyw



Besser tunneln

Sichere VPN-Verbindungen mit WireGuard

Die neue VPN-Technik WireGuard soll einfacher als IPsec und performanter als OpenVPN sein, Daten auf dem Weg durchs Internet genauso gut schützen und auf mobilen Clients Netzwerk- oder Adresswechsel ohne Tunnelabriss überstehen. Wir beleuchten die Hintergründe und zeigen, wie leicht sich WireGuard unter Windows, Linux und Android aufsetzen lässt.

Von Carsten Strotmann

Linux-Vater Linus Torvalds lobt WireGuard über den grünen Klee: „... verglichen mit [...] IPsec und OpenVPN ist es ein Kunstwerk“ [1]. Die Einschätzung könnte daran liegen, dass der Entwickler Jason A. Donenfeld WireGuard von Grund auf neu und mit modernen Krypto-Algorithmen als schnelle und sichere VPN-Lösung entworfen hat. Es lockt mit simpler Konfiguration, flottem Verbindungsaufbau und abrissfreien Tunneln, auch wenn mobile Clients das Netzwerk wechseln.

WireGuard ist sowohl VPN-Protokoll als auch VPN-Software. Manche Dienstleister bieten parallel zu anderen Proto-

kollen auch schon auf WireGuard basierende Tunnel an. Das experimentelle, gratis nutzbare TunSafe (www.tunsafe.com) wurde nur zu dem Zweck aufgesetzt, das neue Protokoll zu testen.

Donenfeld hat bei WireGuard darauf geachtet, dass der Programmcode gut zu lesen und zu verstehen ist, eine wichtige Eigenschaft für sicherheitskritische Software, erlaubt sie doch eine einfache Überprüfung des Programms. Für das Protokoll wurden wesentliche Krypto-Eigenschaften schon formal bestätigt (ct.de/yxcc), unter anderem bezüglich Correctness, Strong Key Agreement and Authenticity und Forward Secrecy.

Unter Linux verschlüsselt WireGuard die Netzwerkdaten direkt im Kernel. Weil damit bei jedem einzelnen Datenpaket Kontextwechsel zwischen Kernel und Userland entfallen, ist es schon prinzipiell um einiges schneller als Konkurrenten wie OpenVPN oder Tinc. Da WireGuard-Software nur das eigene Protokoll implementieren muss, ist sie auch leichtgewichtiger und zumindest beim Verbindungsaufbau flinker als das ebenfalls im Kernel laufende IPsec.

VPN-Monolith

Ältere VPNs enthalten zwecks Kompatibilität zahlreiche kryptografische Algorithmen. Beim Neu- und Wiederaufbau von Verbindungen müssen sich die Kommunikationspartner (Peers) erst auf die zu benutzenden Methoden einigen. Bei WireGuard entfällt dieser Schritt, denn es sind nur die unbedingt nötigen Algorithmen im Protokoll festgeschrieben, unter anderem ChaCha20-Poly1305, Curve25519 und Blake2-Hash.

So kann es beim Handshake auf die Methodenauswahl verzichten, muss nur einen Sitzungsschlüssel aushandeln und kann dann schon Daten transportieren. Während die Wiederaufnahme einer Verbindung bei OpenVPN und IPsec mehrere Sekunden dauern kann, geht das bei WireGuard so flott, dass man es meist gar nicht spürt.

Die monolithische Gestaltung hat freilich auch einen Nachteil: Tritt bei einem der von WireGuard benutzten Krypto-Algorithmen irgendwann eine Sicherheitsschwachstelle zutage, so kann man nicht per Konfiguration auf andere, noch sichere Protokolle umschwenken. Es müssen dann sowohl Protokoll als auch Software angepasst werden.

Peer Group

WireGuard arbeitet als Peer-to-Peer-Protokoll über UDP. Das Umgehen von Firewalls per TCP, wie es OpenVPN beispielsweise auf den HTTP/HTTPS-Ports anbietet, gehörte nicht zu den Designzielen.

Softwareseitig gibt es keine Unterschiede zwischen den WireGuard-VPN-Teilnehmern, sodass allein die Konfiguration entscheidet, ob ein Rechner als Client (Road Warrior) oder als VPN-Server arbeitet. Dabei kann der Tunnel über IPv4 oder IPv6 als Trägerprotokoll zwischen den Peers laufen. Außerdem transportiert er IPv4 und IPv6.

Anders als etwa IPsec ist das WireGuard-Protokoll nicht als Internet-Standard (RFC) niedergelegt. Immerhin sind Teile des Protokolls dokumentiert (ct.de/yxcc). Wer sich für Implementierungsdetails interessiert, findet bei der Internet Engineering Task Force (IETF) eine Zusammenfassung für gängige VPNs [2], darunter TLS, IPsec und WireGuard.

Unterbrechungsfrei

WireGuard arbeitet verbindungslos: Anders als bei IPsec und vielen anderen VPNs können sich die IP-Adressen der Peers ändern, ohne dass der Tunnel zusammenbricht. Er besteht praktisch auch beim Übergang zwischen unterschiedlichen Netzwerktypen weiter, etwa zwischen LAN, WLAN und Mobilfunk.

Selbst wenn ein WireGuard-Gateway-Server – unter Beibehalten des DNS-Namens – auf eine neue IP-Adresse etwa bei einem neuen Hoster umzieht, bleiben die Tunnel bestehen. Schickt man einen Rechner mit laufendem Tunnel per Suspend oder Hibernate schlafen, dann läuft das VPN nach dem Aufwachen weiter.

Das klappt dank des „Cryptokey Routing“ in WireGuard: Jeder Peer führt eine Tabelle mit den öffentlichen Schlüsseln und erlaubten IP-Adressen seiner Gegenstellen. Daraus leitet WireGuard eine interne Routing-Tabelle ab, die den Weg für jedes Paket weist.

Sichere Schnittstelle

WireGuard erzeugt im Kernel eigene Netzwerk-Schnittstellen. Die können beliebige Namen bekommen, eingebürgert haben sich wg0, wg1 und so weiter. Pakete für das VPN gelangen anhand der

Linux-Routing-Tabelle zum WireGuard-Interface, wo sie mit dem öffentlichen Schlüssel der Gegenstelle chiffriert werden. Das Chifftrat wandert dann in UDP verpackt über die aktive physische Netzwerkschnittstelle (LAN oder WLAN) weiter.

Das WireGuard-Protokoll gibt dabei keinen Well-known Port vor, die Software wählt ohne Eingriff ihren Port zufällig. Beim Server sollte der Administrator also manuell einen Port setzen.

Ein Peer kann hinter einem IPv4-Masquerading-NAT (Network Address Translation) sitzen, wenn der UDP-Port seiner Gegenstelle direkt im Internet erreichbar ist. Das darf wie üblich auch über IPv4-Portweiterleitung an einen Host im LAN hinter einem Router realisiert sein. Einfacher geht es freilich mit IPv6 und direkt erreichbaren, globalen Adressen. Hier müssen nur die von WireGuard benutzten UDP-Ports in der Firewall freigeschaltet werden.

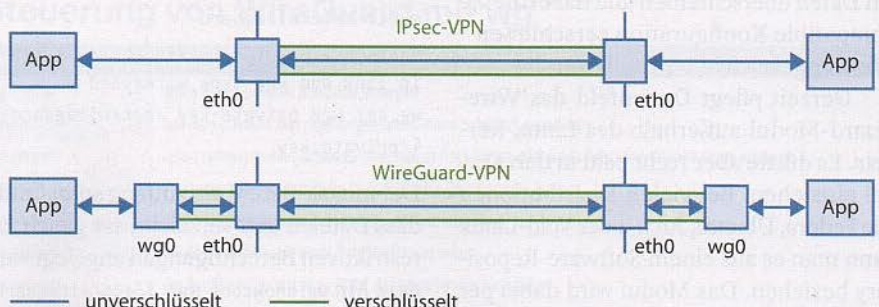
Manchmal trackbar

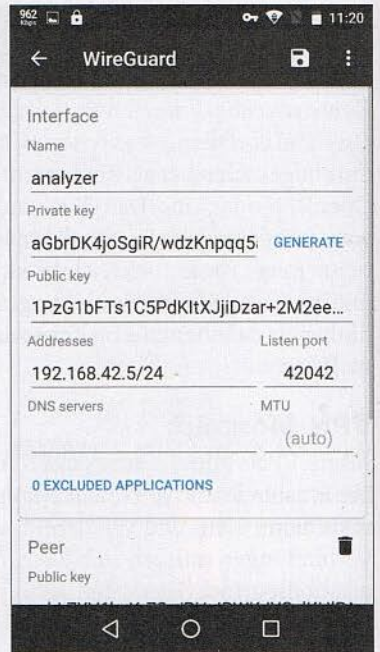
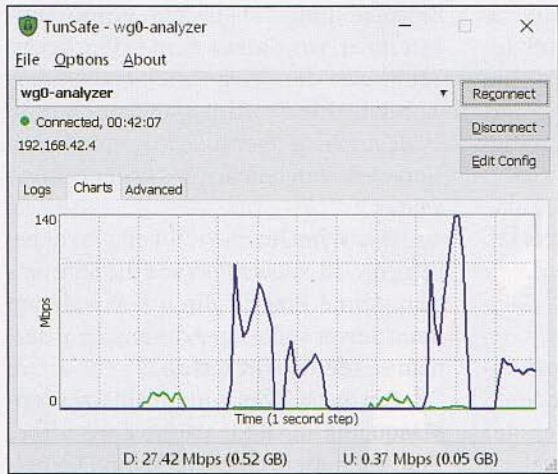
Zwar transportiert WireGuard auch IPv6, aber das klappt zurzeit nur mit statischen Adressen, die in der Peer-Konfiguration hinterlegt sind. So kommen Clients immer mit derselben Quell-Adresse bei Webservern im Internet an, was das Tracking des Benutzers enorm erleichtert.

Bei IPv4 steht das WireGuard-Gateway in der Regel aber hinter einem NAT-Router. Dadurch kommen alle Clients „draußen“ mit derselben IPv4-Adresse an wie jene im (W)LAN und sind dadurch anonymisiert. Wer keine Angst vor der Internet-Polizei hat [3], kann NAT auch für

IPsec- und WireGuard-VPN

Ein wesentlicher Unterschied zwischen IPsec und WireGuard ist die zusätzliche logische Netzwerkschnittstelle bei Letzterem. Außerdem läuft WireGuard über UDP auf einem frei konfigurierbaren Port, während IPsec einen separaten IP-Tunnel baut.





Die Windows-App TunSafe wurde für den gleichnamigen experimentellen VPN-Dienst programmiert. Linuxe mit der Plasma-GUI bekommen ab deren Version 5.15 ein WireGuard-Plug-in für den Network Manager. In der Android-App WireGuard kann man die Tunnel klassisch manuell, per Import einer Textdatei oder – viel einfacher – per Fotografieren eines QR-Codes anlegen.

IPv6 einrichten. Linux' iptables und andere Open-Source-Firewalls unterstützen dies.

Die Hauptfunktionen von WireGuard stecken im gleichnamigen Kernel-Modul. Um die Schnittstelle manuell konfigurieren zu können, nutzt man das in der Sprache „Go“ geschriebene Programm wg. Damit lassen sich private Schlüssel erzeugen oder eine Liste der im Tunnel erlaubten IP-Adressen an das WireGuard-Kernel-Modul übergeben; die Tabelle auf Seite 161 zeigt alle acht Befehle. Das Shell-Skript wg-quick fasst die nötigen Schritte zum Errichten eines WireGuard-Tunnels anhand einer Konfigurationsdatei zusammen.

Kontrollwerkzeug

wg und wg-quick nutzen dieselbe Datei, typischerweise /etc/wireguard/wg0.conf, aber leider mit zum Teil inkompatiblen Optionen. Man sollte sich folglich für eines der Tools entscheiden und dieses beibehalten. Sonst könnte wg-quick unverhofft die Konfigurationsdatei mit aktuellen Daten überschreiben und dabei die wg-kompatible Konfiguration zerschießen – oder umgekehrt.

Derzeit pflegt Donenfeld das WireGuard-Modul außerhalb des Linux-Kernels. Es dürfte aber recht bald in den Kernel einziehen. Bei vielen Distributionen wie Fedora, Ubuntu, Arch- oder Void-Linux kann man es aus einem Software-Repository beziehen. Das Modul wird dabei per DKMS (Dynamic Kernel Module Support)

nach einem Kernel-Update automatisch neu gebaut, sodass WireGuard immer mit dem gerade aktiven Kernel kompatibel ist.

Auf den Ubuntu-Varianten bringen Sie WireGuard mit gerade mal drei Shell-Befehlen an den Start:

```
sudo apt-add-repository \
  'ppa:wireguard/wireguard'
sudo apt update
sudo apt install wireguard
```

WG-Praxis

Bei WireGuard erhält jeder VPN-Teilnehmer (Peer) ein Paar aus privatem und öffentlichem Schlüssel, die effektiv 256 Bit lang sind. Der öffentliche wandert in die Konfiguration seines Gegenübers. Den Verbindungsaufbau kann man optional mit einem gemeinsamen Geheimnis (symmetrischer 256-Bit-Schlüssel, Pre-Shared Key, PSK) weiter abhärten. Sind Modul und Steuer-Tools installiert, errichten Sie als root eine WG-Schnittstelle mit fünf Befehlen auf der Linux-Shell:

```
umask 077
mkdir /etc/wireguard
wg genkey >/etc/wireguard/private.key
ip link add wg0 type wireguard
wg set wg0 private-key /etc/wireguard\
  /private.key
```

Der umask-Befehl am Anfang sorgt dafür, dass Dateien und Verzeichnisse gleich mit restriktiven Berechtigungen angelegt werden. Mit wg showconf wg0 >/etc/wireguard/wg0.conf sichern Sie diese Basiskonfigura-

tion in eine systemkonform benannte Datei, die wg-quick oder der Systemdienst systemd später verwerten können. wg show zeigt dann die aktive Konfiguration inklusive des für die Peers nötigen öffentlichen Schlüssels.

VPN-Server aufsetzen

Die WireGuard-Schnittstelle auf dem VPN-Gateway gibt die in ihren Tunneln verwendeten IP-Adressen vor. Diese dürfen sich wie üblich nicht mit lokal verwendeten, privaten IPv4-Blöcken (RFC 1918) überschneiden. In den folgenden Beispielen nutzen wir die für Carrier-Grade-NAT reservierten privaten IPv4-Adressen (100.64.0.0/10, RFC 6598). So können die Tunnel-IPs nie mit Adressbereichen kollidieren, die ein mobiler Peer beispielsweise in fremden WLANs zugeteilt bekommt (meist 192.168.x.y).

```
echo "Address = 100.64.0.1/10" >> \
  /etc/wireguard/wg0.conf
```

Der öffentliche Schlüssel jedes Clients kommt zusammen mit seiner vom Admin festgelegten individuellen Tunnel-IP-Adresse in einen [Peer]-Abschnitt der Konfigurationsdatei:

```
cat << EOF >> /etc/wireguard/wg0.conf
[Peer]
PublicKey = <Client-Key>
AllowedIPs = 100.64.0.101/32
EOF
```

Nachdem alle Peers angelegt sind, ist die Server-Konfiguration komplett. Entfernen

Sie die Schnittstelle `wg0` und starten Sie sie wieder mit `wg-quick`, damit die neuen Einstellungen greifen:

```
ip link del wg0
wg-quick up wg0
wg show
```

Wenn Clients über den Tunnel auch ins Internet gelangen können sollen, muss der VPN-Server Masquerading-NAT anwenden, wofür bei `iptables`-Firewalls eine zusätzliche Zeile genügt:

```
iptables -t nat -A POSTROUTING -s 100.64.0.0/10 -o eth0 -j MASQUERADE
```

Die Entsprechung für `firewalld` könnte so aussehen:

```
firewall-cmd --zone=external --add-j masquerade --permanent
firewall-cmd --reload
```

Client-Seite

WireGuard-Peers erhalten ihre Tunneladresse, den öffentlichen Schlüssel des Gegenüber – hier der VPN-Server – und weitere Netzwerkparameter (im Tunnel erlaubte Adressbereiche, DNS-Name oder IP-Adresse des Peers, verwendeter UDP-Port) aus ihrer wie folgt erweiterten Konfigurationsdatei:

```
cat << EOF >> /etc/wireguard/wg0.conf
Address = 100.64.0.101/32
[Peer]
PublicKey = <Pub-Key-des-VPN-Servers>
AllowedIPs = 0.0.0.0/0
Endpoint = wg.example.org:<Port>
EOF
```

Damit ist die Peer-Konfiguration vollständig. Entfernen Sie die Schnittstelle und starten Sie sie neu:

```
ip link del wg0
wg-quick up wg0
wg show
```

Können die Peers übers Internet kommunizieren, dann zeigt der letzte Befehl die bestehende WireGuard-Verbindung an. Sie können sie mit `wg-quick [up|down] wg0` ad-hoc auf- und abbauen.

Für permanente Verbindungen lässt sich WireGuard bei den meisten Distributionen ins Startup-System einbinden. Ist der Tunnel heruntergefahren, erreichen Sie das bei einem SystemD-Linux mit `systemctl enable --now wg-quick@wg0`. Ob es geklappt hat, zeigt `systemctl status wg-quick@wg0`.

WireGuard ist noch jung. Aber seine Popularität lässt sich schon jetzt an der Unterstützung anderer Betriebssysteme ablesen. Die Portierung fällt leicht, weil es das Protokoll neben der Kernel-Version auch in einer Go-Implementierung gibt, die das TUN/TAP-Interface anderer Betriebssysteme nutzt und als normales Programm läuft. Sie ist so zwar langsamer und energieintensiver als die native Linux-Kernel-Version, taugt aber auf Smartphones und Tablets problemlos zum Testen von WireGuard.

WireGuard-Apps

Der experimentelle VPN-Dienst TunSafe bietet eine gleichnamige Windows-App an, deren Quellcode auf Github veröffentlicht ist ([ct.de/yxccc](https://github.com/yxccc/tunsafe)). macOS-Nutzer können WireGuard über den Paketmanager Homebrew (<https://brew.sh>) mit dem Kommando `brew install wireguard-tools` installieren. Für BSD-Systeme auf x86-Prozessoren gibt es WireGuard-Implementationen ebenso wie für Android und iOS.

Unter Android bietet sich alternativ zur WireGuard-App die Variante von TunSafe an. Bei beiden Apps kann man die WG-Konfiguration aus Dateien einspielen, manuell eintragen und ändern oder – besonders komfortabel – per Kamera durch Scannen eines QR-Codes importieren. Das kann die iOS-App ebenfalls.

Beim Router-Linux OpenWRT lässt sich WireGuard als Paket nachrüsten. Die pfSense-Entwickler wollen mit der Einbindung noch abwarten, bis WireGuard offiziell in den Linux-Kernel eingezogen und damit als stabil anerkannt ist.

Ausblick auf Zinc

Diesem Ziel steht zurzeit noch das existierende Kryptographie-Framework des Linux-Kernels gegenüber, auf das unter anderem IPsec und weitere Systemdienste zugreifen, beispielsweise die DM-Crypt-Festplattenverschlüsselung. Es gilt als

komplex und schwierig zu nutzen: Programmierern können leicht Fehler unterlaufen, was die Sicherheit der Software und der Benutzerdaten gefährdet.

Die Linux-Kernel-Entwickler waren zunächst wenig erfreut, dass Jason Donenfeld WireGuard auf ein eigenes, schlankes Krypto-Framework (Zinc) gesetzt hat, das parallel zu dem des Kernels läuft. Aber er baut Zinc so um, dass es zum Basis-Krypto-Framework des Linux-Kernels werden und nahtlos auf das ältere Framework aufsetzen kann. Das soll doppelte Funktionalität vermeiden, wobei sich aber die etablierte Linux-Kernel-Krypto-Schnittstelle weiternutzen lässt. Neue Programme haben dann die Wahl zwischen dem schlanken Zinc und der bestehenden Schnittstelle.

Die Linux-Entwickler stellen hohe Anforderungen an neue Krypto-Funktionen im Linux-Kernel. Daher ist nicht absehbar, wann Zinc und damit WireGuard direkt in den Linux-Kernel aufgenommen wird [4].

Für technikaffine Linux-Nutzer ist WireGuard jetzt schon eine sehr interessante VPN-Lösung, denn es lässt sich vergleichsweise leicht in bestehende Systeme einbauen und zeigt sich stabil und zuverlässig. Wer will, kann WireGuard bereits produktiv einsetzen, sollte aber im Hinterkopf behalten, dass die Arbeiten daran noch nicht abgeschlossen sind.

(ea@ct.de) **ct**

Literatur

- [1] Linus Torvalds zu WireGuard, <https://lkml.org/lkml/2018/8/2/663>
- [2] A Survey of Transport Security Protocols, <https://tools.ietf.org/html/draft-ietf-taps-transport-security>, auch über ct.de/yxccc
- [3] Es gibt keine Internet-Polizei, nur Admins, die meinen, es besser zu wissen :)
- [4] New WireGuard Snapshot Released With Linux 5.0 Support, Other Fixes, https://www.phoronix.com/scan.php?page=news_item&px=WireGuard-0.0.20190123

WireGuard, Apps, Links: ct.de/yxccc

Steuerung von WireGuard mit wg

Befehl	bewirkt
<code>wg genkey</code>	einen neuen privaten Schlüssel erzeugen
<code>wg pubkey</code>	aus dem privaten den zugehörigen öffentlichen Schlüssel generieren
<code>wg genpsk</code>	einen symmetrischen Schlüssel (Pre-Shared Key) als gemeinsames Geheimnis für alle Peers erzeugen
<code>wg set</code>	Parameter einer Schnittstelle (z. B. PSK oder Peer-Adresse) ändern
<code>wg showconf</code>	die Konfiguration einer Schnittstelle als Text ausgeben
<code>wg setconf</code>	die Konfiguration aus einer Datei lesen und setzen
<code>wg addconf</code>	die Konfiguration aus einer Datei der bestehenden hinzufügen
<code>wg show</code>	Verbindungsdaten und Status einer Schnittstelle anzeigen

Preisreduziert

Der BGH schränkt die Kosten für Fotoabmahnungen ein

Wer Fotos im Netz unerlaubt veröffentlicht, muss im Fall einer Abmahnung bisweilen tief in die Tasche greifen. Für Fotografen sind solche Abmahnungen oft einträglicher als der Verkauf der Fotos – jetzt schränkte der Bundesgerichtshof die Schadensersatzhöhe in solchen Fällen ein.

Von Joerg Heidrich

Ein fehlender Urheberrechtshinweis, eine falsche Creative-Commons-Kennzeichnung – auch jenseits von vor-sätzlichem „Fotoklau“ verstößt man schnell gegen die rigiden Vorgaben des Urheberrechts. Und das kann richtig teuer werden: Forderungen im vierstelligen Bereich sind die Regel. Hauptstreitpunkt bei derartigen Abmahnungen ist die Bemessung der Lizenzgebühren und die Höhe der geltend gemachten Anwaltsgebühren.

Eine zentrale Rolle bei der Bestimmung des fiktiven Schadens, der durch eine unerlaubte Bildnutzung zu berechnen ist, spielt eine Publikation der Mittelstandsgemeinschaft Foto-Marketing (mfm) namens „Bildhonorare – Übersicht der marktüblichen Vergütungen für Bildnutzungsrechte“. Es handelt sich um ein ziemlich komplexes Regelwerk mit vielen Variablen, das mit schöner Regelmäßigkeit von Foto-Abmahnern angewandt wird, um die Preise für die Nutzung von Fotos zu berechnen. Die Vertreter der Abgemahnten wiederum lehnen die bisweilen absurde Höhe der Forderungen ebenfalls unter Hinweis auf die mfm-Übersicht ab. Die Berechnungen der mfm standen nun zusammen mit einigen anderen Fragen im Fokus einer Entscheidung des Bundesgerichtshofs (BGH, Urteil vom 13.09.2018 – I ZR 187/17).

Teurer Sportwagen

Ausgangspunkt des Verfahrens war das Foto eines Sportwagens, das der Kläger, ein Hobby-Fotograf, auf einer Veranstal-

tung des Beklagten im Jahr 2014 aufgenommen und auf Facebook veröffentlicht hat. Der Beklagte bearbeitete das Bild, versah es mit einem Hinweis auf seine Veranstaltung im nächsten Jahr und stellte es auf seine Website. Daraufhin erhielt er 2015 vom Kläger eine Abmahnung. Zur Erledigung der Sache gab der Website-Betreiber eine strafbewehrte Unterlassungserklärung ab.

Der Kläger verlangte für die Veröffentlichung des Fotos auf der Internetseite Schadensersatz in Höhe von 450 Euro, dazu weitere 450 Euro wegen fehlender Namensnennung und schließlich Abmahnkosten in Höhe von 887,03 Euro – insgesamt also rund 1800 Euro. Dies sah das zunächst zuständige Amtsgericht Leipzig anders. Es sprach dem Kläger lediglich einen Schadensersatz in Höhe von 200 Euro sowie Abmahnkosten in Höhe von 571,44 Euro zu. Das Landgericht Leipzig hatte diese Entscheidung später bestä-

tigt und die im Hinblick auf diese Teilabweisung eingelegte Berufung des Klägers zurückgewiesen.

Der Bundesgerichtshof folgte nun in seiner Entscheidung dem Urteil der Vorgerichte: Der Kläger kann demnach für die unberechtigte Vervielfältigung und öffentliche Zugänglichmachung seines Fotos durch den Beklagten auf dessen Internetseite nur einen Betrag von 100 Euro nebst Zinsen verlangen. Eine Berechnung auf Grundlage der Honorartabelle der mfm sei im vorliegenden Fall abzulehnen.

Es erscheint dem BGH bereits grundsätzlich fraglich, ob die einseitig von der Mittelstandsvereinigung Fotomarketing erstellten mfm-Empfehlungen überhaupt branchenübliche Vergütungssätze enthalten – schließlich handelt es sich um eine Interessenvertretung der Fotografen. Diese Empfehlungen seien jedenfalls dann eindeutig nicht anwendbar, wenn die Bilder nicht von professionellen Fotografen erstellt worden sind. Im zu entscheidenden Fall handele es sich um ein einfaches Foto. Mit dem Betrag von 100 Euro seien die Qualität dieses Lichtbilds und die Wiedergabe des vom Kläger gewählten Motivs auch unter Berücksichtigung der gewerblichen Nutzung durch den Beklagten angemessen berücksichtigt. Dieser Betrag sei wegen der Verletzung des Rechts auf Anerkennung der Urheberschaft noch einmal um 100 Euro zu erhöhen – also weil der Beklagte den Namen des Klägers als Urheber des Fotos nicht genannt hatte.

Bemessung der Anwaltsgebühren

Vorgaben lieferte der BGH auch hinsichtlich der Bemessung des Gegenstandswerts, aus der sich die Anwaltskosten berechnen. Statt der vom Kläger angesetzten 10.000 Euro sei lediglich ein Wert von 6000 Euro anzusetzen. Hierbei sei bereits die gewerbliche Nutzung des Fotos durch den Beklagten berücksichtigt worden, die sich erhöhend auswirke. Im Endeffekt sprach der BGH daher dem Anwalt des Klägers statt knapp 900 Euro lediglich 570 Euro zu. Im Ergebnis lässt der BGH die Opfer von Urheberrechtsverletzungen damit nicht schutzlos, er senkt aber die Einkommensmöglichkeiten für Massenabmahner. Dies gilt allerdings erst einmal nur für Fälle, in denen kein Profifotograf am Werk war.

(dwi@ct.de) **ct**




VORBESTELLUNG:	VORBESTELLUNG:
Bildhonorare Print	Digital-Paket
2019	Bildhonorare 2019 –
28,00 €	ePaper für mobile
zzgl. Versandkosten	iOS-/Android-Geräte
In den Warenkorb	und Desktop
	38,00 €
	In den Warenkorb

Die Mittelstandsgemeinschaft Foto-Marketing gibt jedes Jahr aktualisierte Übersichten zu Bildhonoraren heraus. Wer die Broschüre einsehen will, muss sie im Shop erwerben.



Adam Alter

Unwiderstehlich

Der Aufstieg suchterzeugender Technologien und das Geschäft mit unserer Abhängigkeit

Berlin Verlag, 2018

ISBN: 978-3-8270-1294-4

368 Seiten, 22 €

(Epub-/Kindle-E-Book: 20 €)

Digitale Drogen

Digitale Medien ziehen Menschen in ihren Bann – in immer stärkerem Maße. Entwickler von Geräten und Anwendungen feilen an Nutzererlebnissen mit Suchtpotenzial. Der US-Psychologe Adam Alter warnt, die Abhängigkeit von den digitalen Kicks sei bereits zum Massenphänomen geworden.

Alter nimmt Verhaltenssuchte als Schattenseite des digitalen Zeitalters unter die Lupe. Es geht also um Suchterkrankungen, die nicht auf Substanzen bezogen sind. Dabei liegt sein Fokus nicht etwa auf speziellen Gruppen wie exzessiven Online-Gamern oder Instagram-süchtigen Z-Promis. Er stellt vielmehr die These auf, dass etwa die Hälfte der westlichen Bevölkerung von Verhaltenssuchten betroffen ist. Als Suchtverhalten bewertet er unter anderem das Checken des E-Mail-Postfachs im Minutentakt, die zwanghafte Beschäftigung mit dem Smartphone, „Binge Watching“ von Serien-Streams sowie die Unterwerfung unter das Diktat strenger Fitness-Apps.

Um seine These zu untermauern, unternimmt der Autor einen ebenso fachlich fundierten wie unterhaltsamen Exkurs in die Geschichte der Substanzabhängigkeit. Anhand vieler historischer Fallbeispiele wie Sigmund Freuds Schilderungen zum Kokainrausch arbeitet Alter zunächst die Charakteristika typischen Suchtverhaltens heraus. Mithilfe von Erkenntnissen zur Drogenabhängigkeit, die auf Versuchen beruhen, ergänzt er diese Ausführungen und zieht anschließend überzeugende Parallelen zu den modernen Verhaltenssuchten rund um Tablet und Smartphone.

Alter erklärt, wie digitale Medien – etwa mit Belohnungsmechanismen und sozialen Interaktionen im virtuellen Raum – solche Süchte erzeugen und festigen. Damit vermittelt er seinem Lesepublikum notwendige Informationen, damit es das eigene Konsumverhalten kritisch hinterfragen kann.

Anders als illegale Substanzen ist suchterzeugende Technik nicht nur problemlos verfügbar, sondern auch fester Bestandteil von Privatleben und Berufsalltag der meisten Menschen. „Abstinenz ist keine Lösung“, befindet Alter – und gibt stattdessen Tipps zu einem bewussten, verantwortlichen Umgang mit digitalen Medien. Seine Empfehlungen sind überwiegend hilfreich und lassen sich gut in den Alltag integrieren – mit Ausnahme der eher seltsam anmutenden Idee, sich selbst mit einem Elektroschock-Armband zu konditionieren.

(ovw@ct.de)

Gestaltung mit Konzept

Damit Flyer, Broschüren, Plakate, Präsentationen, Fotobücher oder Einladungskarten gelingen, braucht man solides Grundlagenwissen. Worauf es in der Praxis ankommt, erfahren (angehende) Gestalter und interessierte Laien im „Printdesign“-Buch von Ralph Burkhardt.

Man muss nicht als Künstler geboren sein, um professionell wirkende Drucksachen zu gestalten. Diese beruhigende Erkenntnis stellt sich nach Lektüre des Grundlagenbuchs von Ralph Burkhardt ein. Es vermittelt nicht nur solides Handwerkszeug, sondern auch Strategien zur Planung und Umsetzung von Print-Projekten aller Art und Größe.

Nach einer kurzen Einführung geht es in vier Kapiteln detailliert zur Sache. Der erste Teil widmet sich auf knapp 170 Seiten dem Thema Flyer, ebenso viel Raum bekommt die Broschüre, gefolgt von einem kürzeren Kapitel zur Plakgestaltung. Im letzten Teil dreht sich alles um Corporate Design und Geschäftsausstattung vom Logo über das Briefpapier bis hin zur Visitenkarte.

Dabei führt Burkhardt immer durch den kompletten Entstehungsprozess des jeweiligen Produkts: Konzeption, Gestaltung und Druck. Im Rahmen der Konzeption lernt der Leser etwas über die Wirkungsweise von Flyer, Broschüre & Co., wie man die Zielgruppe definiert, Zeitplan und Budget kalkuliert sowie auf Grundlage von Recherche und Vorüberlegungen ein schlüssiges Konzept erstellt.

Der kreative Teil gibt wertvolle Tipps zur Wahl des richtigen Formats, zu Typografie, Farbgestaltung und der Auswahl von Bildern. Er verrät auch, wie man Text und Bild zu einem ansprechenden Ganzen kombiniert. Nicht zuletzt die zahlreichen, sehr gut gewählten Beispiele sowie die zusammenfassenden Checklisten lassen beim Leser ein Gespür dafür entstehen, was zählt.

Viele Themen sind in jedem Kapitel aufs Neue vertreten – allerdings in wechselnden Zusammenhängen. Der Autor vermittelt stets die für das jeweilige Printobjekt wichtigen Design-Prinzipien.

Design-Studenten und Agenturneulinge bewahrt die Lektüre vor dem Praxisschock. Aber auch abseits der Kreativbranche kann so mancher von der Erfahrung des Design-Dozenten profitieren – etwa bei der Gestaltung von Präsentationen, Vereinsheften oder Gemeindebriefen.

(atr@ct.de)



Ralph Burkhardt

Printdesign

Das umfassende Handbuch

Rheinwerk, Bonn 2019 (2. Auflage)

ISBN: 978-3-8362-6726-7

634 Seiten, 50 €

(PDF-/Epub-E-Book: 45 €)

Druckausgabe mit E-Book: 55 €

Wo war das nochmal?

KI errät Geodaten zum Foto

Geolokalisierung, die Ortsbestimmung zu einem Foto ohne Metadaten – Google erforscht und nutzt sie hinter den Kulissen und ein Leibniz-Institut in Hannover hat ebenfalls eine Lösung entwickelt. Sein KI-System kann jetzt öffentlich ausprobiert werden.

Von Arne Grävemeyer

Ein Foto ohne Metadaten, wo wurde es wohl geschossen? Eventuell sind auf dem Bild markante Gebäude oder Bergkämme zu erkennen, aber nur wenige Globetrotter werden den Ausschnitt damit einem Ort zuweisen können. Auch die Websuche nach Bildhinweisen ist mühsam und misslingt oft. Wer eine Privataufnahme nicht mehr einer bestimmten Reise zuordnen kann oder wer glaubt, eine Fake News über ein Foto entlarven zu können, für den gibt es mit Geolokalisierung durch künstliche Intelligenz ein schnelles Hilfsmittel. Etwas ehrlicher ist allerdings die Bezeichnung Geo-Estimation, übersetzt also Geografie-Schätzung.

An einem Mittwoch im September kam es auf der European Conference on Computer Vision (ECCV) 2018 in Mün-

chen zum Showdown. Unabhängig voneinander präsentierten zwei Forschungsgruppen ihre KI-Systeme zur Foto-Geolokalisierung. Auf der einen Seite der Datenriese Google und auf der anderen Hannoveraner Wissenschaftler der Leibniz-Gemeinschaft.

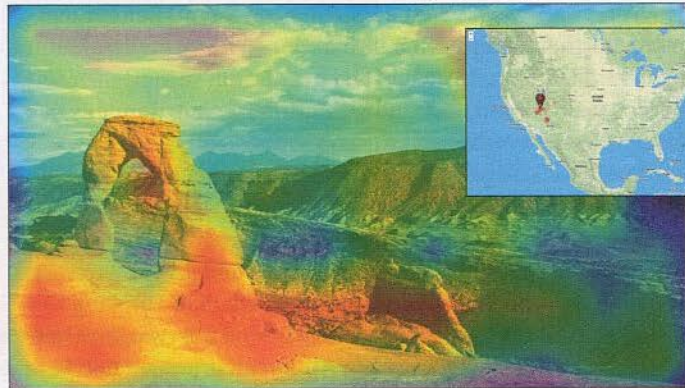
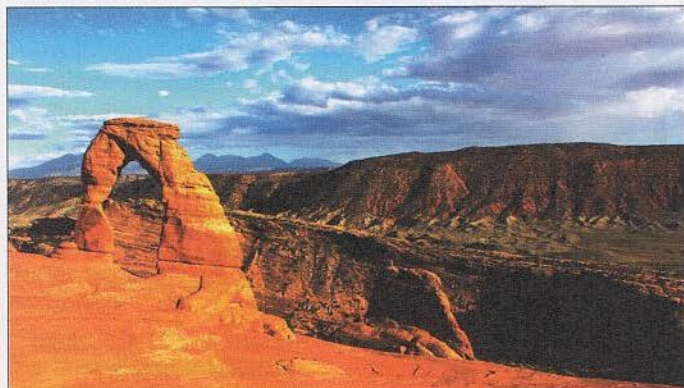
Den 2016 entwickelten PlaNet-Ansatz aus dem Google-Konzern hat ein Team um Tobias Weyand und Paul Hong-suck Seo verfeinert und als CPlaNet neu vorgestellt. Bei beiden Ansätzen klassifiziert ein neuronales Netz die eingehenden Fotos auf die Maschen eines Netzes, das um den gesamten Erdball gespannt wird. Wurde der erste Ansatz noch mit sagenhaften 91 Millionen Fotos trainiert, so verringerten die Forscher beim CPlaNet-Ansatz die Zahl der Trainingsbilder auf etwa 30 Millionen. Das Google-Tool ist offenbar für den internen Einsatz bestimmt, über seine Aufgaben innerhalb der Google-Produkte verrät der Konzern auf Anfrage nichts. Wird es einen Zugang für Privatanutzer geben? Kein Kommentar.

Der Herausforderer kommt aus Hannover. Professor Ralph Ewerth leitet die Forschungsgruppe Visual Analytics am Leibniz-Informationszentrum Technik und Naturwissenschaften (TIB – Technische Informationsbibliothek). Die TIB dient als zentrale Fachbibliothek für Technik, betreibt aber auch eigene Forschung,

etwa zusammen mit dem Forschungszentrum L3S der Leibniz Universität Hannover. Zwei Promovierende aus der Gruppe Visual Analytics, Eric Müller-Budack und Kader Pustu-Iren, haben eine eigene künstliche Intelligenz zur Geolokalisierung entwickelt. Auch bei diesem Ansatz wird allein aus der Bildinformation ein Tipp auf den Aufnahmeort abgeleitet. Die TIB-KI ist mit nur etwa fünf Millionen Fotos trainiert worden, danach gelang ihr die Überraschung: Das System hat die Google-Konkurrenz beim Benchmark mit Standard-Testdaten übertrumpft.

Lokalisierer jetzt im Web

Seit Ende Januar kann das Geolokalisierungstool der TIB mit beliebigen Fotos ausprobiert werden (siehe ct.de/yn7a). Dabei wird auch deutlich, wie die Software vorgeht. „Unser Ansatz entwickelt die erste Google-Lösung PlaNet weiter. Auch unser Tool teilt die Erdoberfläche in Parzellen ein und nimmt für jedes Foto eine Klassifizierung auf diese Zellen vor“, berichtet Müller-Budack. Allerdings haben die Forscher eine wichtige Verfeinerung vorgenommen: Ein Filter unterteilt die eingehenden Fotos gleich zu Beginn in Stadtscenen, Innenaufnahmen oder Naturbilder. Damit gliedert sich das Tool zur Geolokalisierung in vier spezialisierte Subnetze, nämlich den Vorfilter sowie drei



Nicht hundertprozentig lokalisiert: Der Grand Canyon liegt, wie auf der Karte angezeigt, größtenteils in Arizona. Der imposante Delicate Arch auf dem Foto steht allerdings doch weiter westlich in Utah.



Hamburg, Speicherstadt: Die Class Activation Map (rechts) markiert die für die Klassifizierung entscheidenden Bildelemente. Beim Zoom in die Ergebniskarte zeigt sich, dass die KI diese Ansicht sogar auf zwei Straßenzüge genau lokalisieren kann.

separate Schätzer für entweder Stadt-, Innen- oder Naturaufnahmen. „Am stärksten sind neuronale Netze, wenn sie auf eine Aufgabe spezialisiert sind“, betont Müller-Budack. Bei sich überschneidenden Aufgabengebieten für ein entsprechend größeres neuronales Netz wären hingegen schwächere Ergebnisse zu erwarten.

Beim öffentlichen Einsatz im Web lädt die TIB-Geolokalisierung zunächst zum Ratespiel ein. Der Besucher der Webseite kann nicht nur eigene Fotos hochladen und einschätzen lassen, er kann auch persönlich gegen die KI antreten. Zu dem Zweck stehen derzeit 48 Fotos zur Auswahl, die selbstverständlich nicht Bestandteil des Trainingssets der KI waren. Der Besucher kann sich eines aussuchen und dazu dessen Herkunft auf der Weltkarte schätzen. Danach versucht es der Web-Dienst selbst. Am Ende werden die Differenzkilometer zum tatsächlichen Aufnahmeort verglichen. Ein schöner Partyspaß, der nach 48 Versuchen allerdings zu Ende ist.

Krokodile in London

Schon dabei zeigt sich, dass die KI starke Momente hat, aber auch ganz schwache Versuche. Einmal wird eine Brücke in Venedig exakt erkannt und das nächste Mal eine Landschaft im Umland von Rom an die spanische Atlantikküste verlegt. Beim Foto eines Krokodils aus Südostasien tippte die KI der Hannoveraner gar auf London; allerdings nicht wegen der aktuellen Debatten im Unterhaus, sondern weil es im Norden des Regent's Parks einen gut sortierten Zoo gibt. Ewerth erläutert, dass für die Trainingsphase des zugrundeliegenden neuronalen Netzes etwa fünf Millionen flickr-Fotos mit eindeutigen Geo-

tags genutzt worden sind. „Dabei hatten wir eine höhere Abdeckung in Europa und Nordamerika und eine geringere Abdeckung etwa afrikanischer oder südostasiatischer Landstriche.“

Die TIB-Webseite bietet Einblick in die Entscheidungsvorgänge der KI. Die sogenannte Scene Classification gibt einen Score-Wert aus, der in der Regel mit klarem Votum bestimmt, ob das Foto eine Stadtszene, Natur oder eine Indoor-Aufnahme zeigt. Noch informativer ist die Class Activation Map, also eine Heatmap, die auf dem Eingangsfoto farblich markiert, welche Bildbereiche für die Klassifizierung relevant waren.

Und das geht so: Sowohl das Tool der TIB als auch das von Google setzen für die Foto-Klassifikation auf sogenannte Convolutional Neural Networks (CNN), eine Form von neuronalen Netzen, die schon bei vielen Projekten in der Erkennung von Bildinhalten ihre Stärken bewiesen haben. CNN heben in den ersten Verarbeitungsschichten zunächst einfache Bildelemente wie Linien und Kanten hervor. Darauf aufbauend werden dann in tieferen Schichten komplexere Strukturen in die Klassifikation einbezogen. Um die Entscheidungsfindung eines derartigen neuronalen Netzes nachträglich zu erklären, werden sogenannte Class Activation Maps zu einer speziellen Fotoklassifizierung berechnet. Im Prinzip wird die letzte Schicht eines neuronalen Netzes bei dieser Methode rückwärts durchlaufen und überprüft, welche Bildbereiche die typischsten Merkmale einer bestimmten Region enthalten. Ein einfacher Farbcode von kaltem Blau für wenig Einfluss über Gelb bis leuchtend Rot für große Auswirkungen kann dann das Foto überdecken. So erkennt der Betrachter schnell, welches Zwiebeltürm-

chen, welche Fensterform, welche Einrichtungsgegenstände oder welche Pflanzenart letztlich für die getroffene Lokalisierungsentscheidung ausschlaggebend war.

Damit lassen sich Fehlentscheidungen zumindest nachvollziehen. So kann ein ungewöhnliches Ornament an einer Fassade die KI auf eine falsche Fährte locken. Ebenso kann ein Gartenfoto falsch verortet werden, wenn dort eine ortsfremde Pflanze zu sehen ist. Die Heatmap erklärt dann wenigstens, welche Merkmale zur Irritation führten. Ganz generell gelingt die Lokalisierung am besten bei Stadtsichten, die Analyse von Innen- und Naturaufnahmen liefert nicht so gute Trefferquoten.

Test bringt Überraschungen

Beim c't-Test mit eindeutigen Ortsaufnahmen zeigten sich genau diese Probleme recht klar. Eine stimmungsvolle Aufnahme aus der Hamburger Speicherstadt wurde von der TIB-KI eindeutig zugeordnet und sogar auf wenige Straßenzüge genau lokalisiert. Aber schon eine auffällige Felsformation am Colorado River, der sogenannte Delicate Arch, ein eigentlich sehr beliebtes Fotomotiv, wird zwar korrekt in der Nähe des Grand Canyon verortet, aber dann doch mit erstaunlicher Bestimmtheit ein paar Hundert Meilen nach Westen verlegt.

Noch krasser ist die Fehleinschätzung einer Aufnahme des japanischen Fuji. Obwohl auf dem Foto sogar eine Pagode abgebildet ist, verwechselt die KI den Vulkan mit Mount Shasta im Norden Kaliforniens – immerhin auch ein Vulkan.

Man muss die Ergebnisse der Geolokalisierung also mit Vorsicht genießen, aber die Fortschritte auf diesem Gebiet

sind faszinierend. Bereits 2008 hatte ein Team um James Hays an der Carnegie Mellon University in Pittsburgh mit Im2GPS (Image to GPS) ein System der Bildvergleiche vorgestellt. Die Forscher hatten dazu sechs Millionen Fotos indexiert. Zu einem Eingangsfoto wurde dann aufgrund seiner Bildelemente das ähnlichste Foto des Ursprungsdatensatzes ermittelt. Die Geodaten des ähnlichsten Fotos bildeten das Ergebnis der Geolokalisierung. Die Forscher erkannten erfreut, dass sie damit etwa 30-fach besser lagen als mit zufälligem Raten.

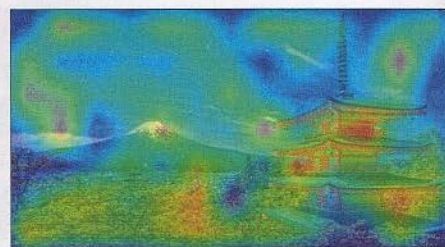
Immerhin: Der von ihnen genutzte Im2GPS-Testdatensatz gilt Forschern heute noch als Standard. Und die Ergebnisse neuerer Tools zeigen rasante Steigerungen. Konfrontiert mit dem Im2GPS-Testfotosatz ordnete der erste Google-Ansatz PlaNet ganze 8,4 Prozent der Fotos auf einen Kilometer genau zu. Im 25-Kilometer-Radius gelang die Lokalisierung von fast 25 Prozent der Fotos. Hier hatte man also immerhin schon die richtige Stadt getroffen. Maximal 200 Kilometer Abstand zum Aufnahmeort wiesen die Einschätzungen bei 38 Prozent der Fotos auf. Das richtige Land sozusagen, nämlich einen Umkreis von 750 Kilometer traf PlaNet bei 54 Prozent der Fotos. In einem Umkreis von 2500 Kilometer und damit wenigstens auf dem richtigen Kontinent bewegten sich die Treffer bei sieben von zehn. Das ist besser als nichts, aber der Begriff Geo-Estimation trifft es eben doch besser als Geolokalisierung.

Trefferquote verdoppelt

Mit dem nachfolgenden CPlaNet-Ansatz gelang Google 2018 eine klare Steigerung. Jetzt trafen fast doppelt so viele Einschätzungen auf einen Kilometer genau, nämlich 16,5 Prozent. In der richtigen Stadt lagen demnach schon 37 Prozent und im richtigen Land 62 Prozent. Und das, obwohl weit weniger Trainingsbilder genutzt worden waren. Der Unterschied: Der PlaNet-Ansatz klassifiziert Fotos schlicht auf ein Netz mit über 25.000 Feldern auf der Erdoberfläche. Dabei sind die Felder übrigens nicht alle gleich groß, da für jedes Feld eine genügende Anzahl von Trainingsfotos eingesetzt werden muss. Entsprechend sind Innenstadt-Parzellen recht eng geschnitten, ländliche Gegenden eher weitläufig eingefasst und entlegene Gebiete wie Ozeane oder die Polkappen bleiben sogar vollständig ausgespart.



Achtung, es ist nur eine Schätzung: Der Fujiyama wird von der KI offenbar mit Mount Shasta in Kalifornien verwechselt. Die Ergebniskarte zeigt leichtere Aktivierungen auch in Japan.



Beim verfeinerten CPlaNet-Ansatz ist zum einen der Trainingsdatensatz besser gepflegt. Er wurde um zahlreiche Indoor-Fotos und unscharfe Aufnahmen bereinigt sowie auch um einander ähnliche Fotos. Zudem wird hier nun nicht mehr nur ein Netz um den Erdball gelegt. Stattdessen werden gleich fünf unterschiedliche Netze aufgespannt und damit im Grunde fünf Klassifizierer parallel genutzt, jeder mit einem eigenen Fotodatensatz trainiert. Die Maschen dieser Netze sind nicht deckungsgleich, wodurch eine Vielzahl an Schnittmengen entstehen. Am Ende ermittelt die Gesamt-KI für jedes Eingangsfoto im Grunde fünf Klassifizierungsergebnisse. Dort, wo sich die Ergebnisfelder überschneiden, gilt die Lokalisierung als besonders valide.

Vorfilter lohnt sich

Der Paukenschlag gelang dem TIB-Team auf der ECCV 2018 in München, als es seine Testergebnisse parallel zum Google-Forscherteam veröffentlichte. Ihre KI verortete sogar 16,9 Prozent der Fotos aus dem Im2GPS-Testfotosatz auf einen Kilometer genau, 43 Prozent wurden wenigstens der richtigen Stadt zugeordnet und sogar 67 Prozent dem richtigen Land. Der Kniff mit der Scene Selection und der Verteilung auf drei thematisch spezialisierte neuronale Netze hatte sich als überlegen erwiesen.

Die TIB-Wissenschaftler dachten bereits über eine Ausweitung ihres Systems

nach. Zusätzlich zu drei Szenen gibt es in der Wissenschaft existierender Benchmark einen Katalog von 16 Unterszenen und sogar 365 Kategorien vor. Tag oder Nacht, Straßenleben oder Baudenkmäler, Tierwelt, Pflanzen oder Gesteinsformationen – die Scene Selection ließe sich noch ausbauen. Aber dieser Schritt erscheint den Forschern kaum umsetzbar, zumal dann für jeden nachfolgenden Klassifizierer eine große Menge passender Trainingsfotos gefunden werden müsste.

Stattdessen arbeiten die Forscher an der TIB derzeit an einem Tool, das in kombinierten Beiträgen eine Text-Bild-Schere erkennt und zudem noch eine Personenerkennung mit in die Analyse integriert. Wobei Ewerth betont, dass die KI immer nur einen Anhaltspunkt liefern kann, der Mensch müsse einen Verdachtsfall stets überprüfen.

Das Sympathische an der TIB-Forschung ist, dass ihre Ergebnisse als Open Source im Web zugänglich sind. So steht nicht nur die Geo-Estimation mit Foto-Upload-Möglichkeit im Web zur Verfügung. Alle Modelle der TIB-Forschungsgruppe Visual Analytics sind zudem auf GitHub verlinkt (siehe ct.de/yn7a) und können damit für beliebige weitere Projekte eingesetzt werden.

(agr@ct.de) **ct**

Geolokalisierung im Web und GitHub-Zugriff auf die Modelle der TIB Hannover: ct.de/yn7a



Aiur ist gefallen!

Wie die DeepMind-KI AlphaStar Profispieler in StarCraft 2 besiegt hat

DeepMind markiert mit einem Sieg über zwei Profispieler in StarCraft 2 einen Meilenstein der KI-Entwicklung. Wir erklären, wie die KI AlphaStar trotz unvollständiger Information schier unbegrenzte Aktionsräume meistert.

Von Pina Merkert

StarCraft 2 gilt nicht nur als eines der anspruchsvollsten Echtzeitstrategiespiele im E-Sport, es stellt auch eine außergewöhnlich große Herausforderung für künstliche Intelligenzen dar. Denn StarCraft erfordert gleichzeitig eine sehr taktische Kontrolle über Dutzende Spielfiguren (in der StarCraft-Szene als Micro-Management bzw. „Micro“ bekannt) und eine Strategie für den Bau von Gebäuden,

das Erforschen von Upgrades und den Bau neuer Spielfiguren („Macro“). Dabei müssen Spieler mit unvollständigen Informationen auskommen, da der „Nebel des Krieges“ meistens die Aktivitäten des Gegners verschleiert. Spielfiguren (Einheiten) lüften den Nebel nur in einem kleinen Umkreis, sodass Spieler mit ihnen zum Gegner ziehen müssen, um dessen Spielfiguren und Gebäude zu sehen und daraus Rückschlüsse auf seine Strategie und Taktik zu ziehen („Scouting“). Professionelle StarCraft-Spieler erkennen bereits an Kleinigkeiten, welche Strategie ein Gegner einschlägt, und passen die eigene Strategie darauf an. Das geht, da StarCraft wie Schere-Stein-Papier funktioniert: Für jeden Angriff gibt es eine passende Verteidigung. Und aus einem gekonnt verteidigten Angriff ergibt sich ein Vorteil für einen Gegenangriff, gegen den der Gegner wiederum mit einer eigenen Strategie antwortet. Dank dieser Dynamik behauptet sich StarCraft seit vielen Jahren als

eines der populärsten und komplexesten E-Sports-Spiele.

Künstliche Intelligenz wird immer wieder daran gemessen, ob sie in Spielen das menschliche Vorbild übertreffen kann. Als Deep Blue 1996 den damaligen Weltmeister Garri Kasparow im Schach besiegen konnte, wurde das rund um die Welt als entscheidender Meilenstein für die Entwicklung von KI wahrgenommen. In den Jahren danach traten KIs immer wieder in Spielen mit unterschiedlichen Eigenschaften gegen menschliche Meister an. 2016 schlug AlphaGo Fan Hui und Lee Sedol – zwei der besten Go-Spieler der Welt. Go hat im Vergleich zu Schach wesentlich mehr Zugmöglichkeiten pro Spielrunde. 2017 schlugen die KIs Libratus und DeepStack professionelle Poker-Spieler im Texas Hold'em. Beim Poker haben Spieler anders als beim Schach und Go nur unvollständige Informationen über die Spielmöglichkeiten der Gegner.

Schwerer als Go und Poker

Für eine KI ist StarCraft eine enorme Herausforderung. Im Prinzip kann sie zu jedem von 60 Einzelbildern pro Sekunde eine ganze Batterie an Spielzügen in Auftrag geben, deren Auswirkungen aber möglicherweise erst nach einer Stunde Spielzeit relevant werden. Gleiches gilt für den Gegner. Der Entscheidungsbaum ist damit um viele Größenordnungen breiter als bei Go. Daher ist es unmöglich, wie beim Schach systematisch alle möglichen

Spielzüge der nächsten Zeit zu bewerten und den effektivsten auszuwählen. Dazu kommt die unvollständige Information: Nur durch aktive Spielzüge beim Scouting erfährt eine KI, wie ihr Gegner genau spielt. Diese Information braucht sie, um eine effektive Strategie auszuwählen. Beim Scouting kommt es aber meist zum Kampf und der Spieler verliert die forschende Figur oft gegen die gegnerische Armee.

DeepMind kooperiert mit Blizzard

Gerade weil StarCraft eine solche Herausforderung darstellt, kooperiert die Google-Tochter DeepMind schon lange mit Blizzard, dem Hersteller von StarCraft. Gemeinsam entwickeln sie ein API namens „PySC2“, das StarCraft 2 so erweitert, dass Computer nicht mehr die Spielgrafik interpretieren müssen, sondern mit Feature-Karten direkt Informationen über das Spielgeschehen bekommen. Solche Feature-Karten bestehen beispielsweise aus einer Matrix, in der in einer Zelle der Typ einer gegnerischen Spielfigur steht. Zellen mit 0 zeigen an, dass dort keine Spielfigur steht. So aufbereitete Daten kann ein Computer viel leichter verarbeiten als die hübsch berechnete 3D-Grafik, aus der Menschen bei StarCraft alle Informationen ziehen. Das Problem, die Spielgrafik direkt zu interpretieren, bleibt auch weiter ungelöst.

Das StarCraft-API PySC2 gibt es seit 2017 als Open Source bei GitHub (Repository und Blogposts dazu siehe ct.de/yxm8). Seitdem nutzen diverse KIs das API und treten in einer eigenen, von Blizzard organisierten Liga gegeneinander an. Diese frühen StarCraft-Bots spielten bislang auf einem recht niedrigen Niveau.

DeepMind beschloss im Sommer 2018, sein StarCraft-Team personell aufzustocken, um ähnlich wie bei Go professionelle Spieler zu schlagen. DeepMind forscht fast ausschließlich an neuronalen Netzen und entschied sich das Problem mit Reinforcement Learning [1] und tiefen neuronalen Netzen anzugehen. Aus diesen Anstrengungen ging die KI „AlphaStar“ hervor. AlphaStar nutzt keine wirklich neue Idee, sondern kombiniert einen Blumenstrauß an aktuellen Techniken aus der Forschung an neuronalen Netzen. DeepMind listet diese in ihrem Blogpost zu AlphaStar nur auf; im Abschnitt zur Technik geben wir jeweils eine ganz kurze Einordnung, wozu die Tricks und Kniffe

dienen. Ein wirklich vollständiges Bild erhält man aber nur, wenn man die zugehörigen Forschungspaper liest. Die Wichtigsten haben wir unter ct.de/yxm8 verlinkt.

Wie AlphaStar spielt

Als AlphaStar den besten StarCraft-Spieler im Team von DeepMind verlässlich besiegen konnte, wandten sich die KI-Forscher an die Spieldesigner bei Blizzard, die ihnen den deutschen Profispieler „TLO“ aus der E-Sports-Mannschaft „Team Liquid“ als Gegner vorschlugen. Da TLO in StarCraft eigentlich Zerg (eine von drei „Rassen“ in StarCraft) spielt, AlphaStar aber bislang nur Protoss gegen Protoss auf einer einzelnen Karte beherrscht, zogen sie später noch TLOs polnischen Teamkollegen „MaNa“ hinzu.

DeepMind wählte für die jeweils fünf Spiele gegen die beiden Profis TLO und MaNa jeweils einen anderen Agenten aus der AlphaStar-Liga aus. Die beiden Menschen konnten daher nicht gezielt nach einer Schwäche in der Strategie eines einzelnen Agenten suchen und wurden von Match zu Match mit sehr unterschiedlichen Taktiken konfrontiert. Menschliche Profis spielen mit ähnlich großer Variation in ihren Strategien, damit ihre Gegner sich nicht so leicht vorbereiten können.

AlphaStar sieht über die Feature-Karten des StarCraft-API gewissermaßen das gesamte Spielfeld auf einmal. Die Agenten können überall auf dem Spielfeld Befehle geben, ohne dafür den Blickwinkel der Kamera verschieben zu müssen. Die Anzahl an Aktionen pro Minute hat DeepMind auf ein für menschliche Profis übliches Maß von etwas mehr als 300 begrenzt. AlphaStar brauchte für die Berechnungen zu einem einzelnen Frame etwa 300 Millisekunden, was sogar über der Reaktionszeit von Menschen liegt.

In der sehr empfehlenswerten Aufzeichnung des Livestreams zu den Matches (siehe ct.de/yxm8) erklärt der

bekannte StarCraft-Kommentator Artosis, warum AlphaStar auf einem nie da gewesenen Niveau spielt: Die Strategien unterscheiden sich von den bekannten Strategien menschlicher Spieler nur in Details: So baut AlphaStar in allen Varianten mehr Drohnen als Menschen, vermutlich um Verluste bei frühen Angriffen des Gegners vorzubeugen. Außerdem stellten nur wenige der AlphaStars dem Gegner am Eingang der Heimatbasis Gebäude in den Weg. Menschen nutzen diese Strategie sehr oft zur Verteidigung.

Viel auffälliger als die langfristige Strategie war das Micro-Management von AlphaStar. Die KI steuerte Spielfiguren ausgesprochen raffiniert und vermied dadurch Verluste. Auch setzte der Computer bevorzugt auf Angriffstaktiken, die ein besonders ausgefeiltes Micro-Management (kurz: Micro) erfordern. Menschen können sich bei solchen Taktiken oft nicht auf genügend viele Spielfiguren gleichzeitig konzentrieren. AlphaStar nutzte sein überlegenes Micro bei allen Spielen, um sich einen Vorteil gegen die menschlichen Profis zu verschaffen, den diese strategisch nicht wettmachen konnten: Sowohl TLO, als auch MaNa verloren fünf Spiele in Folge gegen die KI-Agenten.

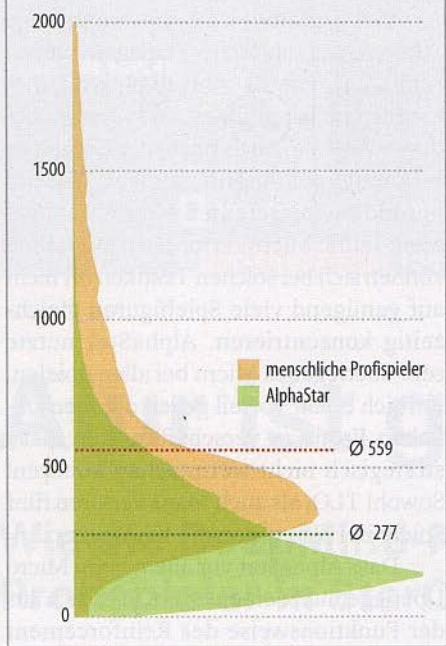
Dass AlphaStar vor allem beim Micro Überlegenheit demonstriert, lässt sich aus der Funktionsweise des Reinforcement Learning erklären: Verändert AlphaStar sein Vorgehen beim Micro, erfährt der Agent nach kurzer Zeit, ob diese Änderung zum Verlust der Spielfigur oder zum Besiegen des Gegners geführt hat. Die kurzfristigen Entscheidungen lassen sich leicht bewerten. Änderungen an der Strategie wirken sich hingegen erst viel später aus, sodass dem Lernalgorithmus meist nur schwache Gradienten zur Verfügung stehen. Das Lernsignal ist dann weniger stark und der Agent braucht zum Lernen erheblich länger. Daher lernt AlphaStar zuerst ein nahezu perfektes Micro, wäh-

Das Warp-Prisma setzte die beiden Immortals mehrfach neben den Drohnen der KI ab und flüchtete, wenn die KI ihre Stalker zurückzog. Die KI hätte das Warp-Prisma mit einem einzigen Phoenix abschießen können. Doch diese konnte die KI nicht bauen.



Aktionen pro Minute

Dieses Histogramm zeigt, wie viele Befehle AlphaStar und Profispieler pro Minute dem Spiel geben. Die Anzahl schwankt stark nach Spielsituation. Menschliche Profis setzen in seltenen Fällen über 2000 Befehle pro Minute ab. Im Durchschnitt sind es aber 559. AlphaStar ist so begrenzt, dass er im Durchschnitt 277 Befehle pro Minute gibt. Dass die KI in einer Minute mehr als 1000 Befehle gibt, kommt praktisch nicht vor.



rend das Macro länger braucht und zum Ende der Trainingszeit auch nicht das gleiche Level an Perfektion erreicht.

Spiel 11

Nach dem klaren Sieg lud DeepMind MaNa zur Präsentation der Ergebnisse ein weiteres Mal nach London ein. Der Profi sollte den kommentierten Livestream (siehe ct.de/yxm8) mit einem letzten live ausgetragenen Spiel abrunden. DeepMind hatte für dieses Spiel extra eine weitere Variante von AlphaStar trainiert. Entgegen seiner Geschwister konnte dieser AlphaStar nicht die ganze Karte auf einmal sehen. Er musste wie ein Mensch die Kamera steuern, um je einen Bildausschnitt zu sehen und konnte auch nur in diesem Bildausschnitt Befehle geben.

Im Training musste sich dieser neue AlphaStar in Spielen gegen seine älteren Geschwister in der AlphaStar-Liga beweisen, die den zusätzlichen Einschränkungen nicht unterworfen waren. Zu Beginn des Trainings hatte er mit dem Bildaus-

schnitt zu kämpfen, doch seine Spielstärke wuchs stetig und erreichte im Verlauf einer Woche fast das gleiche Niveau wie die besten anderen Agenten in der Liga. DeepMind war daher zuversichtlich, dass auch dieser AlphaStar MaNa besiegen könnte.

Zu Beginn des Spiels sah auch alles nach einem weiteren Sieg für AlphaStar aus: Die KI nutzte ihr überlegenes Micro-Management, um nach Minuten bereits einen wirtschaftlichen Vorteil gegenüber MaNa herauszuspielen. MaNa antwortete mit einer riskanten Strategie, bei der er mit einem fliegenden Transporter wenige kampfstärke Einheiten heimlich hinter AlphaStars Drohnen absetzte. Diese Taktik funktioniert normalerweise nur einmal mit begrenztem Schaden, weil der Gegner bereits mit dem Bau eines einzelnen Jagdfliegers eine effektive Abwehr dagegen besitzt. Doch diese Variante von AlphaStar konnte diesen Jagdflieger einfach nicht bauen. Stattdessen baute sie eine unwirksame andere Einheit im gleichen Gebäude. MaNa konnte den Angriff daher mehrmals wiederholen, worauf AlphaStar seine Armee jeweils zurückziehen musste, statt angreifen zu können. Diese Untätigkeit nutzte MaNa aus, baute eine schlagkräftige Armee und zerstörte mit ihr jedes einzelne Gebäude der KI. Ein Mensch hätte an AlphaStars Stelle die Niederlage früher erkannt und kapituliert. Aber DeepMind hatte den Befehl zum Kapitulieren nicht in AlphaStar einprogrammiert.

Die Technik hinter AlphaStar

Deep Learning eignet sich gut, einer KI statistisch fundierte Intuitionen anzutrainieren, die ihr helfen, Entscheidungen zu treffen, die sie zum Sieg führen. Bei AlphaGo [2] hatte DeepMind diese Idee bereits benutzt, um die relevantesten Äste für den zugrunde liegenden Monte-Carlo-Tree-Search-Algorithmus auszuwählen. Da StarCraft aber noch viel mehr Handlungsmöglichkeiten bietet als Go, konnte DeepMind nicht auf Monte-Carlo-Tree-Search aufbauen. Stattdessen trainierte das Team Agenten, bei denen ein neuronales Netz nach Transformer-Architektur (Paper siehe ct.de/yxm8) Sequenzen von Spielzügen generiert. Da sie das mit Long-Short-Term-Memory (LSTM) [3] kombinieren, ähnelt die Idee der Funktionsweise von Google Translate (siehe ct.de/yxm8).

Entscheidungshilfe bietet ein Value-Network, ein zweites neuronales Netz, das darauf trainiert ist, aus den Informationen

über den Spielstand und der Entscheidung zum aktuellen Spielzug eine Wahrscheinlichkeit vorherzusagen, ob der Agent das Spiel gewinnt. Für die Entscheidungen zu einzelnen Spielzügen geht der „Auto-Regressive-Policy-Head“ davon aus, dass sie unabhängig voneinander zum Spiel Ausgang beitragen. Damit ergeben sich bedingte Einzelwahrscheinlichkeiten für jede geplante Entscheidung. Normalerweise wären diese Wahrscheinlichkeiten nicht nur von der Entscheidung abhängig, sondern auch davon, an welcher Stelle in der Sequenz AlphaStar die Entscheidung eingereicht hat. Da das die zu lernenden Wahrscheinlichkeiten unnötig verkompliziert, kombiniert DeepMind das mit von Google Brain entwickelten Pointer-Networks. Die machen die bedingten Einzelwahrscheinlichkeiten unabhängig von der Position eines Spielzugs in der vom Transformer erzeugten Sequenz.

Die Universität Oxford hatte ihre Counterfactual-Multi-Agent-Policy-Gradients (COMA) bereits 2017 mit StarCraft-2-Agenten evaluiert. Dort steuerte je ein Agent eine einzelne Einheit (Micro). Zum Trainieren der Agenten verwendet COMA aber eine „Centralized Value Baseline“. Das ist eine Funktion, die sich das Gesamtergebnis des Zusammenspiels aller Agenten betrachtet und die Agenten dahingehend lobt oder tadelt, wie sie zum Erfolg des Gesamtsystems beitragen. Da jeder Spielzug in der vom Transformer berechneten Sequenz aus einem Befehl für eine einzelne Spielfigur besteht, kann eine solche Funktion individuelles Feedback zu einzelnen Entscheidungen liefern, während die „Centralized Value Baseline“ das Gesamtbild betrachtet.

Überraschend ist bei AlphaStar, dass DeepMind anders als bei ihren Quake 3 spielenden Reinforcement-Learning-Agenten auf ein modellfreies System gesetzt hat. Statt AlphaStar zu zwingen, ein Modell des Spielgeschehens zu erstellen verlässt sich DeepMind darauf, dass AlphaStar alle nötigen Informationen über die Welt und das Spielgeschehen in den Parametern und Aktivierungen seiner neuronalen Netze darstellt. Viele Forscher gingen zuvor davon aus, dass solch ein impliziter Ansatz an der Komplexität von StarCraft scheitern müsste.

Im Blogpost zum Livestream (siehe ct.de/yxm8) äußert DeepMind die Überzeugung, dass sich die Struktur von AlphaStar neben dem Spielen von StarCraft auch für andere sequenzbasierte Auf-

gaben wie Übersetzung und Video- und Textgenerierung eignet. Der Vorteil gegenüber bestehenden Systemen bestünde darin, dass dieses System besser langfristige Strategien verfolgen kann. Beispielsweise hatten KIs bislang beim Erzeugen eines Texts Probleme, bei einem Thema zu bleiben. Von AlphaStar inspirierte KIs lassen hier auf stringendere Texte hoffen.

Imitation

Im Prinzip kann AlphaStar mit dieser Struktur langfristige Strategien verfolgen. Beispielsweise Drohnen zum Abbauen von Mineralien schicken, Warpknotten bauen, die wiederum Stalker produzieren, die den Gegner angreifen. Das Umsetzen einer solchen Strategie dauert in StarCraft 2 mehrere Minuten, in denen dem Agent Millionen verschiedenster Befehle zur Auswahl stehen. Initialisiert man AlphaStar mit Zufallszahlen, erzeugt er auch zufällige Spielzüge, die aber in (fast) allen Fällen nicht zum Erfolg führen. Beim Reinforcement Learning kann ein Agent seine Parameter mit erfolgreichen Beispielen viel gezielter anpassen als mit Negativbeispielen. Mit Zufallsbefehlen lernt der Agent auch mit Tausenden von Beispielen meist nicht einmal die Grundzüge des Spiels.

Bevor AlphaStar auf eigene Faust spielen darf, nimmt ihn DeepMind daher per Imitation Learning an die Hand. Dafür verwandelt DeepMind StarCraft in ein Problem des überwachten Lernens (Supervised Learning), das wesentlich mehr und vor allem positive und damit gezielte Lernsignale liefert. DeepMind nutzte dafür tausende Replays von Spielen, die Menschen in Blizzards Online-Arena BattleNet ausgefochten haben. Mit diesen Spielen als Vorlage sollte AlphaStar zunächst lernen, die exakt gleichen Spielzüge wie der gewinnende Spieler zu erzeugen. Jede Abweichung bestrafte das System mit dem Ändern der Parameter, sodass AlphaStar alle grundsätzlichen Strategien für StarCraft lernte. Der so trainierte Agent spielte nach Angaben von DeepMind bereits auf dem Niveau erfahrener Hobbyspieler (Gold-Level im BattleNet), aber nicht besser als Profis.

Wettbewerb

Ein per Imitation vortrainierter Agent kann, anders als untrainierte Agenten, immerhin sinnvoll ganze StarCraft-Spiele bestreiten – auch wenn er keine Profis besiegt. DeepMind kopierte diesen Agenten

ein paar Mal und variierte ihn jeweils ein wenig. Diese leicht unterschiedlichen AlphaStars ließ DeepMind in der „AlphaStar League“ gegeneinander antreten.

Über die Value-Funktion kann AlphaStar unterschiedliche Ziele verfolgen: So kann ein Agent eine besonders hohe Belohnung erhalten, wenn er einen bestimmten Gegner besiegt. Ein anderer Agent bekommt die hohe Belohnung vielleicht nur, wenn er eine ganze Gruppe an Gegnern verlässlich besiegen kann. Ein dritter bekommt vielleicht eine höhere Belohnung, wenn er bestimmte Spielfiguren baut.

Siegreiche Agenten bekamen nach diesem Schema immer neue Varianten, die sich in der Liga beweisen mussten, während Verlierer nach und nach aus der Liga flogen. DeepMind achtete dabei auf große Diversität. Da StarCraft zu jeder Spielfigur eine effektive andere Spielfigur als Antwort bereithält, gibt es selbst für die besten Strategien erfolgreiche Gegenstrategien. DeepMind passte die Ziele neuer Agenten daher oft so an, dass sie nach Strategien gegen den aktuellen Spitzenreiter suchten.

Dadurch steigerte sich das Spielniveau der AlphaStar-Liga im Laufe des Trainings immer weiter. Da die neuen Agenten nicht mehr auf Replays menschlicher Spieler angewiesen waren, konnten sie neue Strategien entwickeln, die Menschen bei StarCraft noch nie eingesetzt hatten.

Umgerechnet auf Spiele in Echtzeit (DeepMinds KI-Version von StarCraft kann beim Training schneller als in Echtzeit spielen) sammelte jede AlphaStar-Variante etwa 200 Jahre an ununterbrochener Spielerfahrung in StarCraft 2 an. Auf zahlreichen Rechenknoten mit Googles KI-Beschleuniger TPU3 dauerte das Training etwa eine Woche.

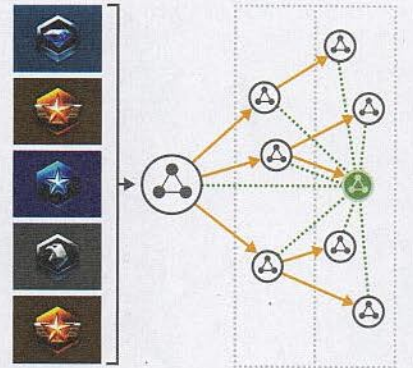
Ein Meilenstein

Nie zuvor hat eine KI menschliche Profis in einem so anspruchsvollen Spiel wie StarCraft 2 besiegt. Die KI punktet nicht nur mit überlegener Arithmetik: AlphaStar besitzt auch die nötige Intuition, um auf Taktiken der Menschen strategisch zu reagieren. Damit beweist die KI Flexibilität und die Fähigkeit, langfristige Pläne zu verfolgen. Am Ball zu bleiben war lange eine Schwäche künstlicher Intelligenz.

Das lässt abseits vom Spiel auf viele ernsthafte Einsatzmöglichkeiten für die Technik hoffen. Von einem Sprachmodell mit Weitblick würden neben Textgenera-

Die AlphaStar-Liga

Nachdem die KI AlphaStar am Beispiel tausender Spiele grundsätzliche Taktiken gelernt hat, muss sie in einer Liga gegen jeweils leicht veränderte Kopien von sich antreten. Die künstliche Evolution der Liga überleben nur die stärksten KIs, die nach einer Woche Training besser als Menschen spielen.



toren auch Sprachassistenten und Hotline-Bots profitieren. Für automatische Übersetzungen lässt die Technik auf Formulierungen hoffen, die besser den Kontext des gesamten Texts miteinbeziehen. Bis dahin ist es aber noch ein weiter Weg, denn bei realen Anwendungen bekommen AlphaStar und seine Nachfolger kein so klares Feedback zu Sieg und Niederlage wie in StarCraft.

Beim E-Sport werden StarCraft-Profis einen genauen Blick auf AlphaStars Spielstil werfen. Möglicherweise wird man im BattleNet in Zukunft häufiger 18 statt 16 Drohnen in Protoss-Basen sehen. Und auch die Taktik des Verbauens der Rampe am Eingang der Basis werden sicherlich einige Spieler auf die Probe stellen. Spannend wird, wie AlphaStar andere Rassen auf anderen Karten spielt.

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

Literatur

- [1] Sebastian Stabinger, Zuckerbrot und Peitsche, Einer selbst gebauten KI per verstärkendem Lernen beibringen Pong zu spielen, c't 21/2018, S. 166
- [2] Harald Bögeholz, Jubel und Ernüchterung, Google AlphaGo schlägt Top-Profi 4:1 im Go, c't 7/2016, S. 44
- [3] Sebastian Stabinger, Langes Kurzzeitgedächtnis, Mit rekurrenten neuronalen Netzen Texte verschlagworten, c't 19/2017, S. 170

Blogpost, Video bei YouTube:
ct.de/yxm8



Mein Android-Store

Mit dem Repomaker eigene App-Kataloge bauen

Repomaker baut individuell zusammengestellte App-Kataloge für F-Droid. Das ist für Entwickler und Organisationen praktisch, aber auch für Nutzer, die häufiger ihre Android-Geräte wechseln.

Von Andreas Itzchak Rehberg

Manch ein Smartphone-Nutzer fühlt sich im App-Store wie Waldi an der Wursttheke: Es gibt so viel Software, dass man sich schwer tut, aus dem Gesamtangebot etwas Passendes zu finden. Das ist auch beim F-Droid-Store nicht anders. In diesem Store, der nur privatsphären-

freundliche Open-Source-Apps verteilt, gibt es zwar bislang „bloß“ 2.900 Programme (Google Play: 2,9 Millionen), man kann darin aber schon viel Zeit beim Suchen von Apps verbringen.

Mehr Übersicht gibt es mit einem eigenen Repository, in das nur reinkommt, was man relevant findet. Entwickler wiederum geben damit ihren Testern eine einfache Möglichkeit, mehrere Versionen einer App zu installieren, Beta-Versionen zu verteilen oder neueste Versionen, ohne dass man gleich APKs per Mail verschicken muss. Praktisch ist ein spezielles Repo auch für Vereine, Firmen oder Organisationen oder schlicht für Familien, die bestimmte Apps besonders leicht auffindbar machen wollen. Kindern kann man beispielsweise einen „Laufstall“ mit

von den Eltern abgesegneten Apps zum Download bieten.

Der eigene App-Katalog ist auch deshalb praktisch, weil Sie jeder App eigene Beschreibungen verpassen können, die dem Nutzer vielleicht klarer als der Standardtext vermitteln, wofür er die App benötigt. Charmant sind eigene Repos auch für Nutzer, die häufig ihre Geräte wechseln und sich so eine Liste mit ihrem Standard-App-Repertoire bauen können.

Lange konnte man eigene Repos nur erstellen, wenn man sich ins fdroidserver-Projekt hineindenkt. Dies setzt einiges an technischen Kenntnissen voraus, sowohl bei der Installation und beim Erstellen des Repos, als auch bei der Verwaltung von Apps darin. Der Repomaker hingegen richtet sich auch an technisch nicht so

versierte Anwender, die mit einem Repo eigentlich nur vorhandene Installationspakete (APKs) für Apps zusammenfassen wollen. Der Repomaker ist noch recht frisch und noch eher spärlich dokumentiert. Diese Anleitung zeigt, wie Sie Ihre individuelle App-Theke zusammenden-gen können.

Kram beschaffen

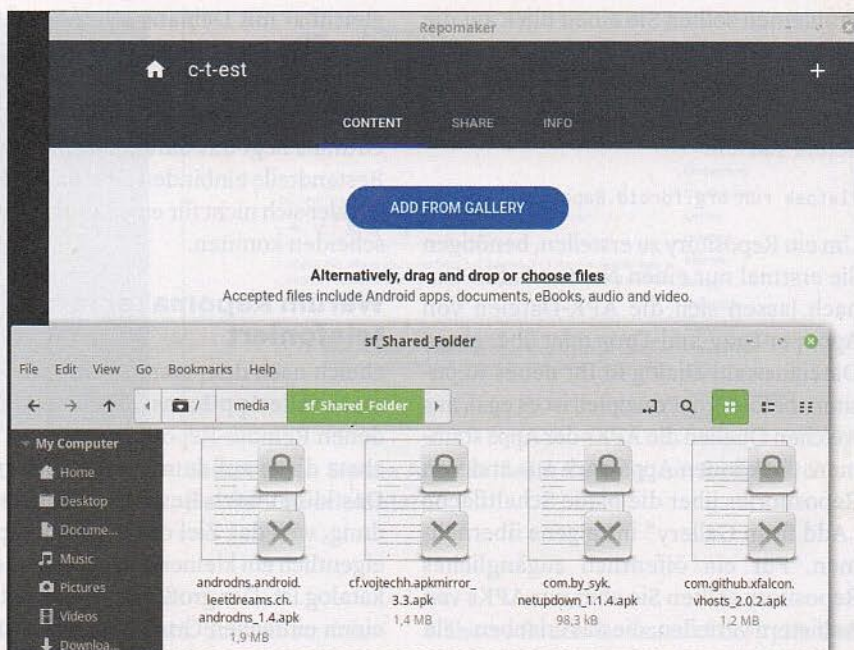
Der Repomaker erzeugt einfache F-Droid-kompatible Repositories. Dazu braucht es keine großartigen technischen Kenntnisse, mit zwei Klicks sind sie erstellt. Für seine Benutzer sind sie über den F-Droid-Client erreichbar, wenn man sie auf eigenen Webspaces verfrachtet oder auf frei verfügbare Entwicklerplattformen schiebt. Das können beispielsweise Dienste wie Github, GitLab oder Amazon S3 sein.

Den Repomaker muss man zunächst installieren, er ist also kein löffelfertiges Tool im Browser. Die Software, ihr Quellcode sowie eine kurze Installationsbeschreibung finden sich im GitLab-Repository von F-Droid unter ct.de/yy18. Dort kann man auch Fehler melden, um Hilfe bitten und sich mit anderen Nutzern austauschen.

Für die Installation und Nutzung benötigen Sie Linux auf Ihrem Rechner. Es reicht ein virtuelles System wie ein in VirtualBox installiertes Debian, Ubuntu oder Linux Mint, weil Sie damit ja das Repo nur bauen und dann auf einen externen Server schieben. Ist es erstmal fertig, greifen die Nutzer nicht auf Ihren Computer zu. Die Anleitung bezieht sich auf Linux Mint 19, das auf Debian fußt.

Während die F-Droid-Website noch die etwas aufwändige manuelle Installation beschreibt, steht der Repomaker seit Mitte Dezember 2018 auch in einem sogenannten Flatpak zur Verfügung und seit Ende Dezember experimentell auch in einem Debian Package. Anders als bei herkömmlichen Linux Packages ist im Flatpak alles enthalten, was Sie an Bibliotheken benötigen – externe Bibliotheken brauchen Sie nicht. Ein Flatpak kann wie eine Matroschka-Puppe weitere Flatpak-Archive enthalten. So ist das auch beim Repomaker.

Flatpak gibt es mittlerweile für 17 Linux-Distributionen, darunter Debian/Ubuntu mit etlichen Derivaten sowie Fedora, CentOS, und openSUSE, Arch Linux und sogar für den Raspi als Raspian. Wer es für seine Geschmacksrichtung nachinstallieren will, kann das bei Debian



Die Programmpakete Ihrer Wunsch-Apps landen durch Ziehen und Ablegen in Ihrem Programm-katalog.

mit `sudo apt install flatpak` tun, bei Red Hat mit `sudo yum install flatpak`. Anschließend noch das Flatpak-Repository für den eigenen User mittels

```
flatpak remote-add --user flathub
https://dl.flathub.org/repo/
flathub.flatpakrepo
```

verfügbar machen, und es kann losgehen. Sie brauchen für den Repomaker 1 GByte freien Speicher zum Installieren. Etwa 700 MByte davon benötigt die Software selbst. Man arbeitet daran, diese Datenmenge einzudampfen.

Sie wollen den Repomaker nur für den aktuell angemeldeten Benutzer installieren und nicht systemweit – daher

brauchen Sie auch keine root-Rechte mit `sudo` anzufordern. Also reicht im Terminal einfach:

```
flatpak install --user flathub
org.fdroid.Repomaker
```

Zusammenschrauben

Anschließend sollte die installierte Anwendung im Startmenü zu sehen sein. Falls nicht, hilft in der Regel ein Neuladen des Desktops. Bei der Desktop-Umgebung Cinnamon geben Sie `Alt+F2`, `R`, `Enter` ein, oder Sie melden sich einfach ab und wieder an. Bei allen folgenden Flatpak-Installationen sollte der Eintrag im Anwendungsmenü zur Verfügung stehen. Bei

Daemon killt Haken

Der Repomaker hakt noch ein wenig hier und da. Sollte das zu oft passieren, sollten Sie alternativ so vorgehen: Greifen Sie zu Hintergrundprozessen, sogenannten Daemons. Mit folgendem Skript startet man Repomaker im Hintergrund, und öffnet anschließend das Web-Interface im Browser:

```
repomaker-server &
repomaker-tasks &
xdg-open http://127.0.0.1:8000/
```

Anstelle des letzten Befehles kann man auch einfach

```
http://127.0.0.1:8000/
```

im Browser öffnen. Im Web-Browser scheint der Repomaker flüssig zu laufen.

Wer eine Flatpak-Installation nutzt, setzt vor die obigen Zeilen

```
flatpak run --command=bash
org.fdroid.Repomaker
```


Problemen sollten Sie einen Blick auf die Diskussionsseiten des Projektes werfen, siehe ct.de/yy18. Natürlich kann man den Repomaker auch per Kommandozeilenbefehl starten:

```
flatpak run org.f-droid.Repomaker
```

Um ein Repository zu erstellen, benötigen Sie erstmal nur einen Namen dafür. Danach lassen sich die APK-Dateien von Apps per Drag-and-Drop oder über einen Dateiauswahl-Dialog in Ihr neues Repository befördern. Prinzipiell ist es egal, aus welchen Quellen die APKs der Apps stammen. Sie können Apps auch aus anderen Repositories über die blaue Schaltfläche „Add from Gallery“ ins eigene übernehmen. Für ein öffentlich zugängliches Repository sollten Sie aber nur APKs von Anbietern verteilen, die das erlauben – ein privater Spiegel des Google Play App Stores wird sie in Schwierigkeiten bringen.

Im Repomaker sind bereits das offizielle F-Droid Repository sowie das des Guardian-Projektes voreingestellt. Guardian fokussiert auf Apps mit besonders rigiden Privatsphäre-Anforderungen. F-Droid-Nutzer kennen beide Kataloge, weil sie auch in der offiziellen App-Store-App konfiguriert sind: Beide Repositories sind vertrauenswürdige Quellen, die Apps aus überprüfem Quellcode enthalten. Weitere Quellen finden Sie unter ct.de/yy18.

Andere Repositories lassen sich leicht hinzufügen: Repomaker verlangt dabei die URL samt Fingerprint. Dieser findet sich häufig auf der Website des jeweiligen Repositories. Beim „IzzyOnDroid“-Repository des Autors etwa steht er direkt auf der dort verlinkten Info-Seite. Dieses Repo ist in der F-Droid Welt etwa ver-

gleichbar mit Debians „Non-Free“. Hier finden sich also Apps, die zwar Open Source sind, jedoch aus verschiedenen Gründen nicht im offiziellen Repository sind. Oftmals liegt das daran, dass sie unfreie Bestandteile einbinden oder dass die Entwickler sich nicht für eine Lizenzform entscheiden konnten.

Warum Repomaker lange telefoniert

Gleich nach dem ersten Start lädt Repomaker alle App-Icons aus den eingebundenen Remote-Repös herunter und speichert diese auf dem lokalen Computer. Das klingt nach Ressourcenverschwendung, weil das Ziel des eigenen Repos ja eigentlich ein kleiner, aber feiner Spezialkatalog ist. Der große Overhead hat aber einen einfachen Grund: Würde man nur gezielt die Icons herunterladen, die man benötigt, könnte man genau sehen, welche Apps genutzt werden.

Haben Sie eine App-Auswahl für Ihr Repo zusammengestellt, ist es zunächst nur auf Ihren lokalen Computer vorhanden. Das lässt sich über die Einträge „Info“ und „Share“ leicht verifizieren. Um das Repository von außen aus verfügbar zu machen, müssen Sie einen externen Speicherplatz konfigurieren, auf den per HTTPS zugegriffen werden kann. Dafür kennt Repomaker drei Möglichkeiten:

Amazon S3: Das ist für den ausfallsicheren Betrieb gedacht, kostet Geld und man benötigt einen entsprechenden Amazon-Account dafür. Für den Heimanwender ist das eher uninteressant.

SSH: Wer einen eigenen Webserver betreibt, egal ob daheim oder bei einem Web-Hoster, kann sein Repository darü-

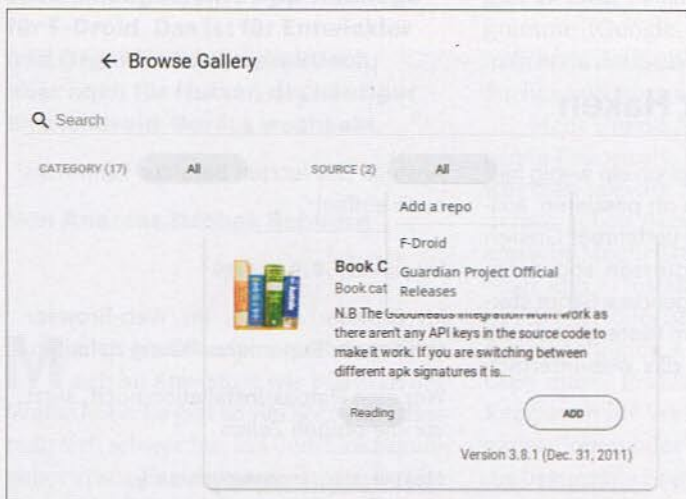
ber zur Verfügung stellen. Dafür braucht man einen SSH-Zugang, der dann im Repository hinterlegt wird.

Git: Das ist für viele die einfachste Möglichkeit. Der dafür benötigte Account bei Github, GitLab oder einen anderen Git-Hosting-Anbieter ist in der Regel für den Privatgebrauch kostenlos und einfach eingerichtet. Auch eigene Git-Server, etwa mit Gitea bieten sich hier an (siehe ct.de/yy18).

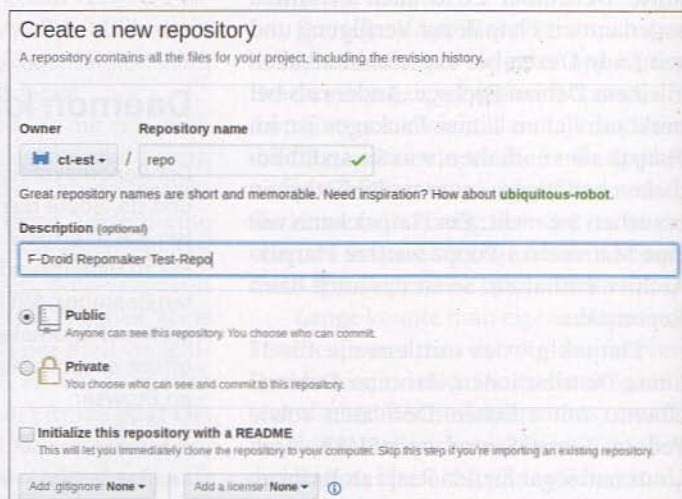
Hinter Git-ter

Für die „Git“-Variante benötigt man einen Nutzer-Account, beispielsweise bei Github. Anschließend legen Sie ein neues Git-Repository Repomaker an. Klicken Sie dazu auf den Button „Start a Project“ oder auf das Plus-Symbol in der oberen rechten Ecke der Git-Seite. Vergeben Sie einen internen Namen und geben Sie eine kurze Beschreibung ein. Die restlichen Felder ignorieren Sie und klicken auf die „Create Repository“-Schaltfläche.

Damit steht Ihr Github-Repo schon zur Verfügung. Um es an den Repomaker anzubinden, benötigen Sie einen SSH-Schlüssel, den Git auch für andere Zwecke nutzt. Dessen öffentlichen Teil hinterlegen Sie in Ihrem Github-Account. Falls Sie noch keinen haben, legen Sie sich den im Terminal an: Der Befehl `ssh-keygen` erledigt den Job. Den Inhalt des öffentlichen Schlüssels `~/.ssh/id_rsa.pub` hinterlegen Sie nun in Ihrem Github-Account. Mit den Standardvorgaben geht das ganz ordentlich. Wer etwas Feintuning beim Vergeben seines SSH-Schlüssels aufwenden will, etwa um die Schlüssellänge oder den Algorithmus gezielt auszuwählen, findet im Netz etliche Tutorials (siehe ct.de/yy18).



Apps lassen sich per Galerie in den Repomaker übernehmen.



Das neue Repo braucht nur wenige administrative Angaben.


```

izzy@vmmint19:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/izzy/.ssh/id_rsa):
Created directory '/home/izzy/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/izzy/.ssh/id_rsa.
Your public key has been saved in /home/izzy/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:jX0Mqg9nCv893gl7TRD3Mzc0yo67Ay46ib+WwTV40rU izzy@vmmint19
The key's randomart image is:
+---[RSA 2048]---+
  o...o  o
  o = EB = o
  . + S o o
  o...+ +
  ..+o..+o
  . =O.*.*O+
  o++oo=OB+
  +---[SHA256]---+
  izzy@vmmint19:~$

```

Den nötigen SSH-Schlüssel generieren Sie selbst auf der Konsole.

Jetzt können Sie Ihrem Repomaker das neue Github-Repository als Speicher hinzufügen und aktivieren. Darauf beginnt Repomaker, ihn im Hintergrund mit den lokalen Daten zu synchronisieren. Ihre Github-Webseite zeigt, ob es geklappt hat. Optional legen Sie mit „Add a Readme“ einen Hinweistext an, der den im Reiter „Share“ genannten „Public Link“ sowie den Fingerprint aus dem Reiter „Info“ enthalten soll, falls man das F-Droid-Repository anderen zur Verfügung stellen möchte.

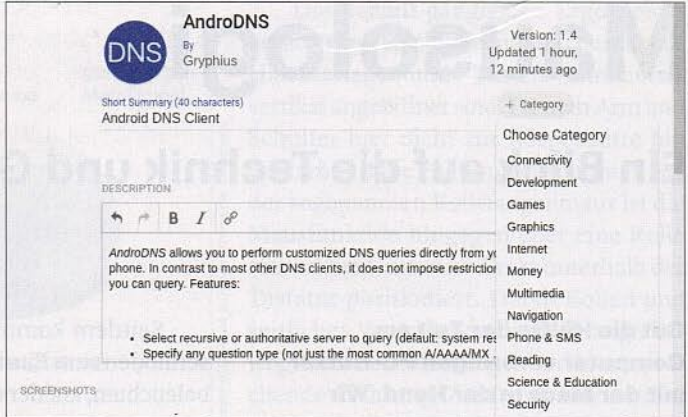
Katalog schön machen

Die Apps in Ihrem Katalog haben nur dann eine Beschreibung, falls diese aus einem Repository übernommen wurden. Falls Sie APKs aus anderen Quellen im Katalog haben, sieht ein Benutzer Ihres Repos kaum Infos zur App: Name der App,

Größe, letztes Update. Schwer zu erfassen, was die App tut.

Die App-Einträge sollten Sie also über ihr lokales Repo bearbeiten. Dazu klicken Sie in der App-Liste auf einen Eintrag und dann auf die Schaltfläche zum Bearbeiten oben rechts. So können Sie den Entwicklernamen ergänzen, eine eigene App-Beschreibung und sogar Screenshots hinzufügen. Damit können Sie bei Ihren Nutzern punkten, denn an ausführlichen und gut gemachten Beschreibungen mangelt es im offiziellen F-Droid-Repo hier und da noch. Die darauf folgende Synchronisierung mit dem Repo im Netz übernimmt Repomaker automatisch im Hintergrund.

Ihr Repository lässt sich in der F-Droid-App auf dem Smartphone sehr leicht über den dortigen Menüpunkt Einstellungen/Paketquellen hinzufügen.



Beschreiben Sie die Apps in Ihrem Katalog, um Besuchern die Wahl zu erleichtern.

Näheres finden Sie unter ct.de/yy18. Den Link dafür zeigt Repomaker im Reiter „Share“ unter „Share public link“. Lassen Sie sich dabei nicht irritieren: Ein Klick auf „view repo“ führt zwar zur unbeliebten „404: Not found“-Fehlermeldung, aber es ist trotzdem alles da. Wer das sicherheits halber prüfen will, ergänzt `/index.xml` am Ende der URL.

Und damit haben Sie ihren eigenen App-Katalog, der sich über seine Adresse und seinen Fingerprint in die F-Droid-App übernehmen lässt. Ein Problem löst der Repomaker aber nicht: Denn Sie müssen selbst dafür sorgen, dass upgedatete APKs von Apps auch in Ihrem Repository landen. (mil@ct.de) **ct**

Dokumentationen und Werkzeuge:
ct.de/yy18

Ubuntu und Debian

Unter Ubuntu und seinen Dialekten ist die Installation einfach: Hier steht experimentell ein Personal Package Archive (PPA) mit Debian-Package zur Verfügung. Da es hier ab und zu noch zu Hängern kommt, sollte man – wie oben beschrieben – einen Daemon einsetzen.

```

sudo add-apt-repository \
  "ppa:fdroid/repomaker"
sudo apt update
sudo apt install repomaker

```

Die erste Zeile stellt das Archiv im eigenen System zur Verfügung, die folgende aktualisiert den lokalen Index mit den

neuen Daten, und die letzte installiert den Repomaker.

Im Gegensatz zu den rund 700 MByte bei der Flatpak-Installation, werden bei einem frisch installierten System nur knapp 250 MByte benötigt. Repomaker startet man dann von der Kommandozeile mit dem Befehl `repomaker`. Es gibt aber auch einen Eintrag im Startmenü, und das sogar ohne Neuanmeldung beziehungsweise ohne Neustart der Oberfläche.

Mit Debian 9 geht man ein wenig anders vor:

```

echo "deb http://deb.debian.org/debian stretch-backports main" >> /etc/apt/sources.list
echo "deb http://ppa.launchpad.net/fdroid/repomaker/ubuntu bionic main" >> /etc/apt/sources.list
apt install dirmngr
apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 9AAC253193B65D4DF1D0A13EEC4632C79C5E0151
apt update
apt install -t stretch-backports repomaker

```


Mausologie

Ein Blick auf die Technik und Geschichte der Computermaus

Gut die Hälfte der Zeit am Computer verbringen PC-Nutzer mit der Maus in der Hand. Wir schauen, was sich im Laufe der Zeit unter der Haube getan hat.

Von Julius Beineke und Henrik Heigl

Auch wenn es durch Touchdisplays, VR-Gesten oder Trackpoints eine breite Auswahl an Mausalternativen gibt, hält sich die Maus wacker auf den meisten Schreibtischen. Douglas C. Engelbart und William English entwickelten bereits 1963 das erste sogenannte Zeigegerät am Augmentation Research Center des Stanford Research Institute. Im Dezember 1968 zeigten sie ihre Entwicklung auf der Herbsttagung der American Federation of Information Processing Societies. Seitdem entwickelten sich Technik, Form und Ausstattung der Maus stetig weiter.

Ihre Position auf dem Tisch erkennen Mäuse entweder mechanisch oder optisch. Bei den ersten Modellen kamen noch mechanische Schleifkontakte zur Koordinatenermittlung zum Einsatz. Diese arbeiteten stromsparend, verdreckten und verschlissen allerdings schnell und wurden schon bald durch optomechanische Mäuse ersetzt. Darin dreht eine meist aus Metall und Gummi bestehende Kugel zwei Lochscheiben vor Lichtschranken. Deren Unterbrechungen registrieren Belichtungssensoren, aus deren Daten die zweidimensionale Bewegung errechnet wird. Da normale Leuchtdioden von anderen Lichtquellen gestört werden können, wurde die Technik nach kurzer Zeit auf Infrarot umgestellt.

Weil die Kugel schnell verschmutzte und die Lichtschranken leicht verstopften, mussten Mäuse dieser Bauart regelmäßig gereinigt werden. Das führte oft zu Schäden an der Mechanik. Daher stieg man bald auf rein optische Methoden um.

Seitdem kommen Leucht- oder Laserdioden zum Einsatz, die die Oberfläche beleuchten, auf der die Maus bewegt wird. Hier wird der sogenannte Speckle-Effekt genutzt – Unebenheiten auf der Unterlage der Maus führen dazu, dass einzelne Lichtwellen in andere Richtungen reflektiert werden. Die Reflexionen nimmt ein optischer Sensor auf, aus dessen Daten die Bewegung errechnet wird. Wesentliche Vorteile sind höhere Genauigkeit und weniger Verschleißteile, die umständlich gereinigt werden müssen. Darüber hinaus ist nicht zwingend eine völlig ebene Oberfläche nötig. Eine wesentliche Schwäche: Weist die Oberfläche nicht genügend oder zu kleine Unebenheiten auf, führt das zu Sensorproblemen – etwa auf Glas oder lackierten Flächen.

Um dem beizukommen, entwickelte Microsoft 2011 die sogenannte BlueTrack-Technik. Ein starke, blaue Lichtquelle an der Unterseite der Maus sollte für stärkere Kontraste sorgen und so die Erkennung von Unebenheiten für die ebenfalls verbesserten, optischen Sensoren erleichtern. Spiegelnde oder durchsichtige Oberflächen blieben aber weiterhin problematisch. Ansatzweise lösen konnte Logitech das Problem mit der Darkfield-Technik, die das Prinzip der Dunkelfeldmikroskopie nutzt. Hierbei wird eine Oberfläche seitlich beleuchtet, sodass ebene, reflektierende Flächen dunkel, Unebenheiten hell und kontrastreich erscheinen. Das macht Strukturen von wenigen Nanometern Größe für den optischen Sensor erkennbar und erhöht dessen Präzision enorm. Auch der Einsatz auf transparen-

ten oder spiegelnden Oberflächen ist so relativ störungsfrei möglich.

Die Auflösung

Die optischen Sensoren in Computermäusen haben eine optische Auflösung oder Punktdichte, angegeben in DPI (dots per inch). Diese ist das Maß für die Detailgenauigkeit: Je mehr Punkte auf einer bestimmten Strecke aufgelöst werden, desto empfindlicher und genauer ist die Maus. 10 dpi entsprechen zehn aufgelösten Punkten auf einem Zoll, also etwa 2,54 Zentimetern.

Die Bandbreite reicht hier von 400 bis 12.000 dpi und mehr. Während für die meisten Anwendungen 800 bis 1200 dpi völlig ausreichen, kann eine höhere Auflösung ab 2000 dpi besonders bei Gaming oder Bildbearbeitung einen Unterschied machen. Es ist von Vorteil, wenn der Nutzer die Empfindlichkeit einstellen kann, denn sonst ist der Mauszeiger im normalen Office-Betrieb kaum zu bändigen und springt schon bei der geringsten Bewegung über den Bildschirm. Die meisten aktuellen Mäuse haben zu diesem Zweck Knöpfe zum Verändern der Auflösung.

Die Klicks

Die erste Maus von Engelbart und English hatte nur eine einzelne Taste, die meisten zeitgenössischen Modelle haben zwei bis fünf häufig programmierbare Tasten, ausgeführt als mechanische Mikrotaster. Besonders in der Gaming-Szene sind weitere Tasten für zusätzliche Funktionen beliebt. Nur Apple bleibt weiterhin dem Ein-Tasten-Prinzip treu.

Der erste Zeigegerät-Prototyp nach D. C. Engelbart und W. English wirkt heute klobig und archaisch.



Bild: SR International [CC BY-SA 3.0]
via Wikimedia Commons

Im Innern einer Kugelmaus

Die Kugel dreht durch Bewegung der Maus Lochscheiben vor den Lichtschranken. Deren optische Sensoren erfassen die Drehrichtung. Anhand der Daten von zwei Achsen wird die Mausebewegung errechnet und am Bildschirm umgesetzt.



Bild: Sador [CC BY-SA 3.0], via Wikimedia Commons

Im Laufe der Jahre kam das Rollrad hinzu, das zum schnellen Scrollen durch Internetseiten, Dokumente und andere Bildschirmhalte verwendet wird. Hier kommt meist ein rastender oder frei drehbarer Inkremetalgeber zum Einsatz, dessen Bewegung üblicherweise durch optische Abtastung erkannt wird. In manchen Mausmodellen lässt sich zwischen rastender und freier Bewegung wechseln, um entweder präzise in kleinen Schritten oder mit hoher Geschwindigkeit zu scrollen.

Bei den meisten aktuellen Modellen ist das Scrollrad, teilweise auch seitwärts, klickbar und dient als zusätzliche Maustaste. Apple setzt hier bereits auf Touch-Bedienung, während wiederum andere Modelle beispielsweise Kippschalter statt Rollrad mitbringen.

Die Datenübertragung

Die Maus wird entweder per Kabel, heutzutage üblicherweise an einem USB-Anschluss, oder kabellos betrieben. Kabellose Mäuse übertragen ihre Daten ähnlich wie Funktastaturen per Bluetooth oder proprietärem Funkprotokoll im 2,4-GHz-Band an einen mit dem PC verbundenen Empfänger. Strom beziehen sie dabei entweder aus eingelegten Batterien oder fest verbauten Akkus, die per USB-Kabel oder induktiv geladen werden. Einige Bluetooth-fähige Mäuse unterstützen Multi-Pairing – man koppelt sie mit mehreren Geräten, zwischen denen man per Knopfdruck nahtlos wechselt.

Kabellose Mäuse reagieren aufgrund der Übertragungszeit und Latenz geringfügig langsamer als kabelgebundene Modelle. Je höher die Sensorauflösung, desto mehr Daten müssen von der Maus zum Computer übertragen und dort in verwertbare Daten umgerechnet werden.

Während via USB-Kabel zwischen 500 MBit/s (USB 2.0) und 5000 MBit/s (USB 3.0) übertragen werden, sind es beispielsweise bei Bluetooth maximal 2,1 MBit/s. Das reicht für die meisten Mäuse, dennoch schwören viele Gamer weiterhin auf kabelgebundene Varianten, um etwaige Verzögerungen bei hohen DPI zu vermeiden. Außerdem übertragen kabellose Eingabegeräte ihre Daten üblicherweise unverschlüsselt an den Computer und sind somit relativ leicht abzuhören. Das ist bei Tastaturen, wo sich teilweise sogar konkrete Texteingaben wie Passwörter abhören lassen allerdings kritischer als bei Mäusen.

Die Ergonomie

Heutzutage verbringen Computernutzer durchschnittlich über die Hälfte ihrer Zeit vor dem Bildschirm mit der Maus in der Hand – viele Stunden täglich. Der andauernde Gebrauch der Maus kann zu Fehlhaltungen und Beschwerden wie Sehnenscheidenentzündungen oder Karpaltunnelsyndrom führen. Abhilfe wollen ergonomische Mausvarianten schaffen, die der natürlichen Hand- und Armhaltung angepasst sind und möglichst belastungsfreie Bewegungsabläufe von Fingern und Gelenken ermöglichen.

Die aktuelle Logitech MX Anywhere 2s mit Bluetooth- und Funkübertragung hat ein vertikal und horizontal klickbares Scrollrad, einen DPI-Button und seitliche Zusatz-tasten.

Die derzeit gängigsten Ergo-Zeigergeräte sind Hochkantmäuse, bei denen Handauflage und Tasten annähernd vertikal angeordnet sind. Da man Arm und Schulter hier nicht zur Körpermitte hin verdreht, ist die Haltung entspannter. Bei der sogenannten Rollstangenmaus ist die Mausfunktion hingegen über eine Rolle verwirklicht, die man direkt unterhalb der Tastatur positioniert. Durch Rollen und seitliches Verschieben dieser Stange bewegt sich der Mauszeiger in die entsprechende Richtung. Zusatz-tasten sind hier nicht nur für Klicks, sondern häufig auch für Kopieren und Einfügen sowie weitere Extrafunktionen vorhanden.

Auch Touchpads und Trackballs – quasi auf dem Rücken liegende Kugel-mäuse – können Beschwerden durch zu viel Mausbedienung vorbeugen. Die mittige Position von Rollstangenmäusen und Touchpads kommt beidhändiger Benutzung und Entspannung in Schulter und Unterarm zugute, da man die Hände stets auf oder vor der Tastatur lassen kann. Das gilt auch für den Trackpoint – ein kleiner „Gummijoystick“, der sich in der Mitte vieler IBM-Notebook-Tastaturen findet und hier als Mauseersatz dient [1].

Aus die Maus?

Wie Computer und Tastatur hält sich die Maus wacker und gehört Smartphone, Touch & Co. zum Trotz noch nicht zum alten Eisen. Große Innovationen sind zwar kaum noch zu erwarten – neue, kleine Weiterentwicklungen besonders in den Bereichen Ergonomie, Konnektivität, Stromversorgung und Sensorgenauigkeit gibt es jedoch regelmäßig. Das Aus der Maus zeichnet sich noch nicht ab.

(jube@ct.de) ct

Literatur

[1] Julius Beineke, Fühlmäuse, Sechs innovative, ergonomische Alternativen zur Computermouse, c't 1/2019, S. 124



Bild: Henrik Heigl

Die Freiheit nehm ich mir

Drahtlose Audioübertragung zu Lautsprechern per WiSA

Das HD-Audio-Funkverfahren WiSA trifft den Nerv der Anwender, die keine Lust darauf haben, Lautsprecherkabel quer durchs Zimmer zu ziehen. Und die Technik hat gute Chancen – dank der Unterstützung durch LG und Microsoft –, in diesem Jahr Fahrt aufzunehmen.

Von Nico Jurran

Kennen Sie WiSA, die „Wireless Speaker and Audio Association“? Wenn nicht, dann sind Sie in guter Gesellschaft. Denn obwohl in dieser Vereinigung seit Jahren bekannte Firmen an der drahtlosen Übertragung von Mehrkanal-Audiosignalen in High-Definition-Qualität arbeiten und sogar schon passende Lautsprecher

auf dem deutschen Markt erhältlich sind (siehe Tabelle am Ende des Artikels), hat sie kaum einer auf dem Schirm.

Wirklich breites Interesse an der Technik weckte erst LGs Ankündigung, seine kommenden Premium-TVs „WiSA ready“ zu machen.

Doch nicht nur wegen der LG-Fernseher stehen die Chancen gut, dass WiSA nun endgültig zu einer Hausnummer im Heimkino- und PC-Audio-Bereich wird. Denn auch Microsofts Spielkonsole Xbox One ist seit einiger Zeit fit für WiSA, Rechner mit Windows 10 als Betriebssystem sollen bald folgen. WiSA-Gründungsmitglied Summit Wireless Technologies schätzt, dass in diesem Jahr sogar bis zu 60 Millionen Geräte „WiSA ready“ werden werden.

Vor allem aber sorgen neue Transmitter-Lösungen dafür, dass die Nutzung der WiSA-Funktechnik wesentlich einfacher

und preiswerter wird als bisher. Aber der Reihe nach.

Ausrichtung

Zunächst einmal sei festgestellt, dass auch WiSA-Systeme nicht völlig „drahtlos“ sind: Um die Audiosignale zu empfangen und auszugeben, stecken in den Funkboxen Verstärker und Elektronik, die Netzstrom benötigen. Allerdings ist es vielen Anwendern immer noch lieber, für jede Surround-Box ein Kabel zur nächsten Steckdose im Rückraum zu legen, als Lautsprecherkabel vom Audio/Video-Receiver durchs ganze Zimmer zu ziehen.

Bis zu acht Kanäle lassen sich mit WiSA übertragen. Das ermöglicht ein komplettes Funkset mit 7.1-Kanälen (sieben Hauptboxen plus ein Subwoofer) beziehungsweise eine 3D-Sound-Ausführung mit 5.1.2 Kanälen inklusive zwei Höhenlautsprechern. Denkbar ist aber auch, dass am Fernseher mit WiSA-Unterstützung die drei Frontboxen (links, rechts und Center) drahtgebunden hängen, so dass sich mit den freibleibenden Funkkanälen auch ein 5.2.4- oder ein 7.1.2-Setup realisieren ließe.

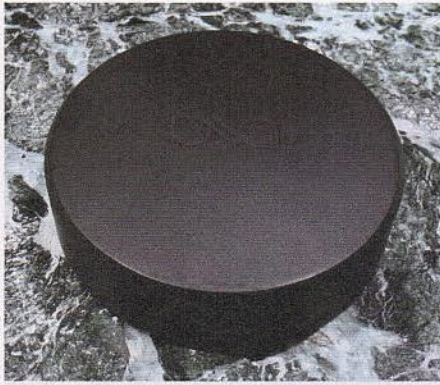
Aber das Einsatzgebiet ist nicht auf Heimkino-Systeme beschränkt: Ebenso lässt es sich nutzen, um beispielsweise zwei kleine Aktivboxen mit Stereomusik zu versorgen, die in einer anderen Ecke des Raumes abseits vom Zuspielder stehen.

Nicht verwechseln darf man WiSA allerdings mit einem Multiroom-System, wie es etwa Sonos oder Yamaha anbietet. Bei WiSA geht es darum, in einem Zimmer Audiosignale an Lautsprecher zu schicken – dafür in bester Qualität und mit möglichst niedriger Latenz.

Harman Kardon zeigt mit seiner Lautsprecher-Reihe „Citation“, dass sich beide Konzepte verbinden lassen: Multiroom-Technik für die Verteilung von Inhalten im Haus und das WiSA-Funkverfahren für die Anbindung von Lautsprechern in einem Set per Funk.



Der schwedische Hersteller Primare bietet bereits den Streaming-Vorverstärker SC15 (oberes Gerät) mit integriertem WiSA-Funkchip an, demnächst soll der größere Vorverstärker Pre35 folgen.



Der WiSA-zertifizierte Axiim-Transmitter soll noch im ersten Quartal auf den Markt kommen. Neben der abgebildeten Version soll auch eine weiße Ausführung erhältlich sein.

Die Übertragung läuft über das lizenzfreie Frequenzband im 5-GHz-Bereich, konkret auf 5,2 bis 5,8 GHz. Um alle Unterbänder nutzen zu können, ist bei WiSA die Fähigkeit zum automatischen Kanalwechsel (DFS) vorgeschrieben. Laut Entwickler ist die Technik darauf ausgelegt, die Audiosignale drahtlos durch einen Raum von einer Größe bis zu 9 x 9 Meter zu schicken.

WiSA übermittelt die Audiodaten mit einer Auflösung von 24 Bit und einer Samplingfrequenz von 44,1, 48 und 96 KHz und erreicht damit HD-Audio-Qualität. Daher werben die WiSA-Unterstützer auch mit einer uneingeschränkten Qualität bei der Wiedergabe der verlustfrei komprimierten Mehrkanal-Audioformate Dolby TrueHD und DTS-HD Master Audio von Blu-ray Disc und Ultra HD Blu-ray. Tatsächlich spielte WiSA bei einer Vorführung dynamisch und auch bei hohen Lautstärken frei von Verzerrungen oder anderen Artefakten auf.

Als maximale Latenz geben die WiSA-Entwickler 5,2 Millisekunden an. Das ist im Vergleich zu Bluetooth herausragend: Dort beträgt die Latenz mit dem Standard-Codec SBC 100 bis 150 ms und sinkt selbst bei Nutzung von aptX Low Latency nur auf Werte um 40 ms. WiSA erfüllt damit die Voraussetzung, dass man bei Filmen und Spielen als Zuschauer nicht den Eindruck bekommt, Bild und Ton liefen asynchron.

Die bisherige Lösung

Damit die einzelnen Audiokanäle (in digitaler Form) an die verschiedenen Lautsprecher geschickt werden können, müs-

sen sie natürlich erst einmal in passender Form vorliegen. Dies bedeutet, dass beispielsweise in den Surround-Formaten Dolby Digital oder DTS kodierte Inhalte zunächst dekodiert werden müssen, bevor die Audiodatenströme für die einzelnen Kanäle über WiSA an die passenden Lautsprecher gefunkt werden.

Die Firmen Axiim und Klipsch bieten unter den Bezeichnungen „Q UHD Wireless Media Center“ und „RP HUB1“ bereits sogenannte „WiSA-Hubs“, die über HDMI-Ports digitale Audio/Video-Datenströme von Zuspiegeln wie UHD-Blu-ray-Playern entgegennehmen. Den angelieferten Surround Sound verarbeiten sie über integrierte Decoder und geben die Videodaten an den Fernseher weiter. Aus technischer Sicht handelt es sich damit um Audio/Video-Vorverstärker. Als solcher wird auch das Modell SC15 Prisma der schwedischen Hifi-Manufaktur Primare angeboten.

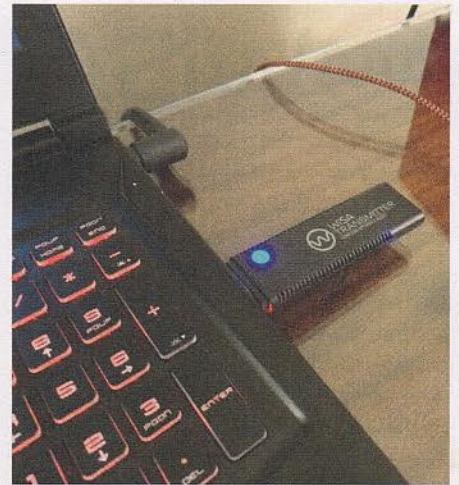
Teilweise wird auch die Bezeichnung „AV-Receiver“ für die Hubs verwendet, allerdings müssten sie dann eigentlich Endstufen integriert haben, um die dekodierten Signale zu verstärken. Die WiSA-Hubs funken hingegen an Aktivboxen, die selbst die Verstärkung übernehmen.

WiSA-ready als neuer Weg

Der große Nachteil der Hubs liegt in ihren vergleichsweise hohen Preisen: Das



Die WiSA-Boxen teilen dem Transmitter mit, zu welcher Art sie gehören – etwa Hauptlautsprecher oder Subwoofer.



Der WiSA-Transmitter von LG Innotek hat gerade einmal die Größe eines gewöhnlichen USB-Sticks.

Klipsch-Modell kostet um die 440 Euro, der Axiim-Hub rund 1000 Dollar und der Primare SC15 Prisma schlägt sogar mit 1500 Euro zu Buche. Die Lösungen sind zudem völlig überdimensioniert, wenn man nur ein Boxenset an seinen Fernseher anschließen will. Zu der Erkenntnis kam offenbar auch WiSA und startete daher im September 2018 sein „WiSA-ready“-Zertifizierungsprogramm, unter das die kommenden LG-TVs, die Xbox One und Windows-PCs fallen.

Die WiSA-ready-Geräte haben zwar keinen Funksender eingebaut, führen aber die oben angesprochene Dekodierung der Surround-Formate selbst durch. Die so erzeugten Audioströme für die einzelnen Lautsprecherkanäle stellen sie dann digital an ihrem USB-Port bereit. Nun muss man nur noch einen passenden WiSA-Sender (Transmitter) anschließen, der jeden Audiostrom zum jeweiligen Lautsprecher schickt.

Einen passenden Transmitter will Axiim noch im ersten Quartal für rund 150 US-Dollar unter dem Namen „Link“ auf den Markt bringen. Der kleine Puck kann neben dem Fernseher Platz finden oder wird an dessen Rückseite mit einem Magneten befestigt. Für den Einsatz am Rechner oder an einer Konsole soll der Link auch im Bundle mit einem 5.1-Lautsprecherset erhältlich sein, dessen Boxen sich äußerlich nicht von drahtgebundenen Modellen aus dem PC-Bereich unterscheiden – nur dass hier eben der Verkabelungsaufwand reduziert ist.

WiSA präsentierte auf der CES zudem einen kommenden Transmitter in Form



WiSA hat bereits mehrfach das Logo geändert. Hier die aktuelle Version.

eines USB-Sticks des zur LG-Gruppe gehörenden Unternehmens LG Innotek. Der soll beispielsweise an Windows-10-Rechnern zum Einsatz kommen, läuft laut Hersteller aber auch unter MacOS, iOS und Android ab 5.0 (Lollipop).

Die USB-Transmitter sind aber nicht nur preiswerter, sondern letztlich auch flexibler als die Hub-Lösung: Sollten neue Surround-Formate auf den Markt kommen, muss nur ein passender Decoder im WiSA-ready-Gerät integriert werden. Für die Funkübertragung ist es letztlich egal, auf welchen Positionen die Boxen montiert sind. Passend dazu bewirbt die WiSA nun auch die Unterstützung von 3D-Sound-Formaten wie Dolby Atmos oder DTS:X.

Laut WiSA ist die komplette Ersteinrichtung in 15 bis 20 Minuten erledigt. In der Regel dürften die WiSA-ready-Geräte die nötige Bedienoberfläche anbieten, um das Setup durchzuführen. Axiims Transmitter kann sich laut Hersteller über Bluetooth LE aber auch mit einem Android- oder iOS-Gerät verbinden. Dann sollen sich über eine darauf laufende App die Lautsprecher konfigurieren und im laufenden Betrieb die Lautstärke und Equalizer-Einstellungen einstellen lassen. Ein ebenfalls im Link integrierter Infrarot-Empfänger ermöglicht schließlich die Steuerung der Box über eine gewöhnliche Fernbedienung.

Lautsprecher

Lautsprecher und Soundbars mit integrierten WiSA-Empfängern haben aktuell Bang & Olufen, Bose, Enclave Audio, Harman Kardon und Klipsch im Sortiment. Weitere sollen in den kommenden Monaten folgen.

Ein interessante Lösung wäre auch ein preiswertes separates WiSA-Empfangsmodul, mit dem sich beliebige Aktivboxen in das System integrieren lassen. Das könnte ein wichtiger Baustein sein, damit sich WiSA noch in diesem Jahr endgültig als herstellerübergreifende Lösung für die Funkübertragung von Audiosignalen etabliert. (nij@ct.de) ct



Von Klipsch gibt es bereits eine Soundbar mit integriertem WiSA-Empfänger. Enclave Audio zeigte einen Prototyp.

WiSA-taugliche Geräte

Hersteller	Modell	Produktgattung	Status
Axiim	Link	USB-Transmitter	angekündigt
	HDLink Wireless Home Theater	5.1-Boxenset + USB-Transmitter	angekündigt
	Q UHD Wireless Media Center	Hub / Vorverstärker	erhältlich (USA)
	WM Series Wireless	Lautsprecher	erhältlich (USA)
	XM.4111SS Surround	Surround-Lautsprecher	erhältlich (USA)
	XM.101SW Subwoofer	Subwoofer	erhältlich (USA)
Bang & Olufsen	BeoLab 17	Lautsprecher	erhältlich
	BeoLab 18	Lautsprecher	erhältlich
	BeoLab 19	Subwoofer	erhältlich
	BeoLab 50	Lautsprecher	erhältlich
	BeoLab 90	Lautsprecher	erhältlich
	BeoLab Receiver 1	Empfänger (proprietäre Anschlüsse)	erhältlich
	BeoLab Transmitter 1	Transmitter (proprietäre Anschlüsse)	erhältlich
Bose	Sound Touch	Streaming-Lautsprecher	erhältlich
Enclave Audio	Cinehome HD 5.1	5.1-Boxenset	erhältlich
Harman Kardon	Citation Bar	Soundbar	erhältlich
	Citation Sub	Subwoofer	erhältlich
	Citation Surround	Surround-Lautsprecher	erhältlich
	Citation Tower	Lautsprecher	erhältlich
	HD Control Center (RP Hub 1)	Hub / Vorverstärker	erhältlich
Klipsch	RP-110WSW	Subwoofer	erhältlich
	RP-140WM	Lautsprecher	erhältlich
	RP-440WC	Center-Lautsprecher	erhältlich
	RW-34C	Center-Lautsprecher	angekündigt
	RW-51M	Lautsprecher	angekündigt
	RW-100SW	Subwoofer	angekündigt
	LG Innotek	WiSA Wireless Audio Tx Dongle	angekündigt
LG	verschiedene 2019er-TVs	Fernseher	angekündigt
Microsoft	Xbox One (S/X)	Spielkonsole	erhältlich
Platin Audio	WS30 Wireless	Lautsprecher	erhältlich
Primare	SC15 Prisma	Hub / Vorverstärker	verfügbar
	Pre35	Hub / Vorverstärker	angekündigt

Peilung per Nahfunk

Was Bluetooth 5.1 bringt, wie es funktioniert

Bis auf 10 Zentimeter genau können Bluetooth-Geräte der nächsten Generation die Position im Raum berechnen. Das gilt als wichtige Grundlage für die Navigation in Gebäuden.

Von Dušan Živadinović

Bluetooth ist ein schmalbandiger Kurzstreckenfunke und schon die vor einigen Jahren eingeführte Variante Low-Energy richtet sich mit niedriger Stromaufnahme und simplen Funkmodulen an das Internet of Things (IoT). Mit der im Januar erschienenen Spezifikation 5.1 lassen sich demnächst Produkte und Dinge im dreidimensionalen Raum bis auf 10 Zentimeter genau orten.

Fachleute meinen, dass die Bluetooth-Navigation in Gebäuden von der Positionsbestimmung ähnlich profitieren könnte wie Navigationsgeräte von GPS. Die Interessenvereinigung Bluetooth Special Interest Group (SIG) erwartet ab 2022 rund 400 Millionen solcher Produkte pro Jahr.

Bereits mit dem vor einigen Jahren mit den Bluetooth Beacons eingeführten Real-Time Location Service (RTLS) lässt sich eine ungefähre Distanz zwischen zwei Objekten ermitteln. Manche Flughäfen setzen RTLS ein, um etwa die Entfernung von Kunden zum Abfertigungsschalter zu ermitteln.

Bluetooth-Beacons nutzen dafür lediglich den Empfangspegel (Received Signal Strength Indication, RSSI). Der RSSI liefert aber keine Angaben über Empfangs- oder Sendewinkel, sodass damit keine Positionsbestimmung möglich ist. Diese Parameter sollen nun Geräte mit Bluetooth 5.1 liefern.

Eingangs- und Ausgangswinkel

Bei Bluetooth 5.1 unterscheidet man zwei Anwendungsszenarien: Angle of Arrival (AoA, Eingangswinkel) und Angle of Departure (AoD, Ausgangswinkel).

Im AoA-Szenario sendet ein Gerät Orientierungspakete mit einer Antenne. Der Empfänger – Locator – nimmt das Signal mit mehreren Antennen auf. Die Orientierungspakete treffen je nach Entfernung zu den Antennen mit unterschiedlichen Amplituden und leicht Phasenverschoben auf. Aus beiden Wertereihen ermittelt der Empfänger die Distanz und Richtung des Senders. Die AoA-Methode eignet sich somit zum Lokalisieren von Dingen, etwa im Museum.

Im AoD-Szenario teilt ein Gerät seine Position direkt mit (z. B. ein Locator Beacon). Dafür sendet es seine Orientierungspakete gleichzeitig über mehrere Antennen ab (Antennen-Array). Sie kommen beim Empfänger, etwa einem Smartphone, zu unterschiedlichen Zeitpunkten mit unterschiedlichen Phasenverschiebungen an, sodass dieser anhand der Unterschiede wiederum die Position des Senders ermitteln kann. Zu den Anwendungen gehört etwa die Funkbeschilderung von Getränkeständen und Ausgängen im Stadion oder Ticketschaltern im Flughafen.


Die Positionsbestimmung ist umso genauer, je weniger Gegenstände und

Lebewesen zwischen Sender und Empfänger stehen und je geringer der Funkstörpegel ist. Umgekehrt kann man also Ungenauigkeiten an belebten Plätzen etwa in Einkaufshallen oder an Veranstaltungsorten erwarten. Auch Wände, Fenster oder Schränke, die Funkwellen unterschiedlich reflektieren oder durchlassen, tragen zu Abweichungen bei. Die Special Interest Group wendet dagegen ein, Vorserien-Chips getestet zu haben. Diese hätten auch unter schwierigen Bedingungen „hohe Genauigkeit“ geliefert. Wie hoch diese ist, das müssen erst praktische Erfahrungen zeigen.

Im privaten Bereich könnte ein Locator helfen, verlegte Schlüssel oder Fernbedienungen wiederzufinden. Aber seine Reichweite ist kurz und nach Lage der Dinge könnte er nicht über die Position von Gegenständen Auskunft geben, die sich zum Beispiel in einem anderen Stockwerk befinden.

Rettungsdienste könnten anhand von Locator-Informationen im Einsatzfall leichter einen Überblick über die Position von hilfsbedürftigen Personen gewinnen. Allerdings setzt auch das ein funktionierendes Smartphone mit eingeschaltetem Bluetooth 5.1 voraus.

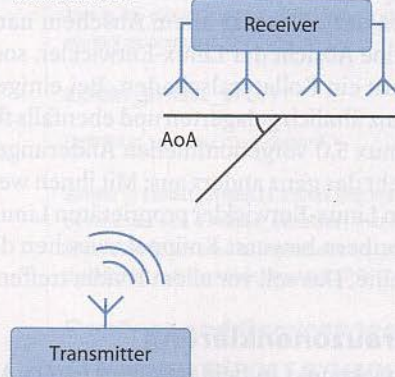
Einige Chip-Hersteller haben bereits erste Bausteine für das laufende Jahr angekündigt. Dazu zählen etwa Nordic Semiconductor und Qualcomm, dessen Snapdragon 845 für Smartphones ausgelegt ist. Bis erste Produkte auf den Markt kommen, dürfte es aber 2020 werden.

(dz@ct.de) 

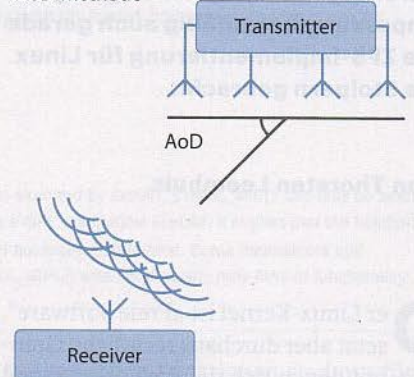
Der Mehr-Antennentrick

Anhand von empfangenen Amplitudenunterschieden und Phasenverschiebungen schließt ein Empfänger auf die Distanz und den Winkel zum Sender.

AoA-Methode



AoD-Methode





Was soll das?

Linux 5.0: Lizenzkennzeichnung trifft Nvidia und ZFS on Linux

Die Linux-Entwickler versperren Nvidias proprietärem Grafiktreiber den Zugang zu einer wichtigen Technik. Das gelingt mit einer kleinen Änderung, die die Lizenz durchdrückt. Eine ähnlich gelagerte Anpassung hat zufällig auch gerade die ZFS-Implementierung für Linux ins Stolpern gebracht.

Von Thorsten Leemhuis

Der Linux-Kernel ist „Freie Software“, setzt aber durchaus rechtliche Grenzen, mit denen sich die Welt arrangieren muss. Das bekamen jüngst Nutzer und

Entwickler von ZFS On Linux (ZOL) zu spüren: Die ZFS-Portierung ließ sich vorübergehend nicht mit Vorabversionen von Linux 5.0 kombinieren, weil sie eine bislang genutzte Funktion aufgrund einer unpassenden Lizenz nicht mehr verwenden darf. Das war allem Anschein nach keine Absicht der Linux-Entwickler, sondern ein Kollateralschaden. Bei einigen ganz ähnlich gelagerten und ebenfalls für Linux 5.0 vorgenommenen Änderungen sieht das ganz anders aus: Mit ihnen werfen Linux-Entwickler proprietären Linux-Treibern bewusst Knüppel zwischen die Beine. Das soll vor allem Nvidia treffen.

Grauzonenklärung

Knackpunkt in beiden Fällen ist die Art und Weise, wie Linux ausgewählte Kernel-

funktionen freigibt, damit Kernel-Module sie nutzen können. Das geschieht mit Symbolen, die anfangs immer das C-Makro `EXPORT_SYMBOL()` exportierte. Ende 2001 kam `EXPORT_SYMBOL_GPL()` dazu. Das war für Entwickler gedacht, die klarstellen wollen: Darüber exportierte Funktionen sind Linux-Interna und nur für Code gedacht, der sich an die Bedingungen der vom Linux-Kernel verwendeten Lizenz GNU General Public License (GPL) v2 hält.

Linus Torvalds untersagte, bestehende Symbole nachträglich auf GPL-Exporte umzustellen. Entwickler dürften sie aber bei neuem Code verwenden – also auch, wenn sie ein existierendes Feature grundlegend überarbeiten. Die Programmierer konnten so selbst entscheiden, ob sie eine rechtliche Grauzone rund um ihren Code

aus der Welt schaffen wollten: Sind unabhängig entwickelte Kernelmodule generell oder ab einem bestimmten Punkt ein vom Linux-Kernel abgeleitetes Werk („derivative work“) und müssen daher die Bedingungen der GPLv2 erfüllen? Eine klare Antwort darauf existiert nicht, denn selbst zentrale Linux-Entwickler sind da nicht einer Meinung. Eine offizielle Aussage fehlt und dürfte im Nachhinein auch schwer einzuholen sein, denn der Kernel hat unzählige Urheber.

Gerichtsurteile könnten Klarheit schaffen. Solche gibt es aber nicht, da das Problem bislang nie vor den Kadi gezeit wurde. Da es Module, die sich nicht an die Bestimmungen der GPL halten, schon lange gibt, lässt sich sagen: Sie werden geduldet, explizit erlaubt sind sie aber nicht.

ZFS stolpert

Das bekam ZFS On Linux (ZOL) jetzt zu spüren, denn das ließ sich einige Wochen nicht mit Vorabversionen von Linux 5.0 (siehe S. 56) paaren. Dort haben Linux-Entwickler zwei Symbole entfernt, über die Module jeweils eine Kernelfunktion aufrufen müssen, bevor und nachdem sie Gleitkommaeinheiten des Hauptprozessors (FPU, SSE, AVX & Co.) verwenden. Von der Nutzung dieser Symbole wird schon lange abgeraten, denn sie waren nur noch aus Kompatibilitätsgründen da, seit jemand vor Jahren die FPU-Infrastruktur von Linux grundlegend überarbeitet hat. Die Exporte wurden jetzt bei 5.0 entfernt, nachdem die letzte Stelle innerhalb des Kernelcodes beseitigt wurde, die diese Symbole brauchte.

Das brachte ZOL zu Fall, das die Symbole nutzte, weil es die Checksummen mit Gleitkommaeinheiten berechnete. Technisch ließe sich das Problem einfach lösen, denn seit der Überarbeitung exportiert der Kernel zwei neue Symbole zur FPU-Nutzung. Der für die Umbauarbeiten zuständige Entwickler wollte aber betonen, dass Nutzer seines Codes sich an die GPL halten sollen, daher hat er die neuen Symbole per `EXPORT_SYMBOL_GPL()` freigegeben. Das setzt diesen Wunsch beim Laden der Module durch, denn der Module-Loader prüft dabei anhand der Metadaten des Modules, ob das unter einer kompatiblen Lizenz steht. Das Kernelmodul von ZOL kann die neuen Symbole daher nicht nutzen: Es enthält Code des ursprünglich für Solaris entwickelten ZFS, der unter der CDDL (Common Development and Distribution License) steht, die

nach gängiger Auffassung als inkompatibel zur GPL gilt.

Nach strenger Auslegung der GPLv2 dürfte man eine Kombination von Linux und ZOL daher womöglich gar nicht vertreiben. Das ist einer der Gründe, warum Linux-Schwergewichte wie Suse und Red Hat (und damit auch Fedora und CentOS) die ZFS-Implementierung für Linux nicht mal mit der Kneifzange anfassen. Andere Distributoren stellen immerhin Wege bereit, um es leicht nachzurüsten. Ubuntu ist eine der wenigen Distributionen, die sich traut, ZOL direkt in das Installationsmedium zu integrieren.

Für die Aufräumarbeiten, die ZOL zu Fall brachten, war Kernelentwickler Sebastian Andrzej Siewior zuständig. Nach Bekanntwerden des Problems hat er selbst dafür plädiert, den Export wieder einzubauen; ein anderer bekannter Linux-Programmierer sprang ihm zur Seite. Der Rückbau wurde allerdings unter anderem von Greg Kroah-Hartman zurückgewiesen, der Linus Torvalds kürzlich während einer Auszeit vertreten hatte. Siewior hatte in der Debatte sogar den Sinn von `EXPORT_SYMBOL_GPL()` infrage gestellt und gefordert, den Ansatz komplett fallen zu lassen. Kroah-Hartman antwortete darauf kurz und knapp: „Es funktioniert, bitte lass es, wie es ist.“

Das zeigt, dass sich selbst die Kernelentwickler uneins sind. Bis zur Ende Feb-

ruar erwarteten Fertigstellung von Linux 5.0 wird sich an der Situation wohl nichts mehr ändern. Ein Workaround wurde aber gefunden und in den Entwicklungszweig integriert: ZOL führt die Checksummenberechnung ab Linux 5.0 ohne Gleitkommaeinheiten durch. Dadurch steigt laut den Entwicklern die CPU-Last ein wenig; sie erwarten aber keinen sonderlichen Einfluss auf die Geschwindigkeit, solange die CPU nicht besonders schwach ist oder bereits am Anschlag läuft. Gleich bei Integration der Änderung haben die Entwickler indes angekündigt, den Code noch optimieren zu wollen, um den Overhead zu reduzieren.

Rote Karte für Nvidia

Die ZOL-Sache wurde im Internet heiß diskutiert, dabei ist das Problem recht überschaubar. Deutlich weniger Aufmerksamkeit erregten hingegen für Linux 5.0 eingepflegte Änderungen, die langfristig wohl viel größere Auswirkungen haben: Die Entwickler haben einige Symbole auf GPL-Exporte umgestellt, die zur Nutzung von Heterogeneous Memory Management (HMM) essenziell sind.

Bei HMM handelt es sich um eine zentrale Technik der Heterogeneous System Architecture (HSA), für die AMD und andere schon seit Jahren trommeln. Sie soll es leichter machen, Rechenaufgaben mit dem jeweils am besten geeigneten Chip

strange on big-endian platforms though so it is a good idea not to do this.

Symbols

Within the kernel proper, the normal linking rules apply (ie. unless a symbol is declared to be file scope with the `static` keyword, it can be used anywhere in the kernel). However, for modules, a special exported symbol table is kept which limits the entry points to the kernel proper. Modules can also export symbols.

`EXPORT_SYMBOL()`

Defined in `include/linux/export.h`

This is the classic method of exporting a symbol: dynamically loaded modules will be able to use the symbol as normal.

`EXPORT_SYMBOL_GPL()`

Defined in `include/linux/export.h`

Similar to `EXPORT_SYMBOL()` except that the symbols exported by `EXPORT_SYMBOL_GPL()` can only be seen by modules with a `MODULE_LICENSE()` that specifies a GPL compatible license. It implies that the function is considered an internal implementation issue, and not really an interface. Some maintainers and developers may however require `EXPORT_SYMBOL_GPL()` when adding any new APIs or functionality.

Routines and Conventions

Von Linux per `EXPORT_SYMBOL_GPL` freigegebene Funktionen sind nur für Kernelmodule zugänglich, die sich an die Lizenz des Kernels halten.

des Systems auszuführen – etwa Grafik- oder Krypto-Prozessoren. HMM verspricht dabei, die Performance signifikant zu verbessern, weil es den Zugriff auf die verarbeiteten Daten durch die verschiedenen Prozessoren erleichtert – etwa indem es zeitraubendes Hin- und Herkopieren zwischen Haupt- und Grafikspeicher vermeidet, wenn man mit CUDA & Co. auf Grafikprozessoren rechnet. Das ist vor allem für High Performance Computing (HPC) oder Machine

Learning wichtig, gewinnt aber auch im Massenmarkt an Bedeutung.

Der Entwickler, der die HMM-Unterstützung zu Linux 4.14 beisteuerte, hat einige für die Technik zentrale Funktionen bewusst ohne GPL-Kennzeichnung exportiert. Ein paar wichtigen Kernelentwicklern schmeckte das von Anfang an nicht, da HMM so von ihnen programmierte Interna in die lizenzrechtliche Grauzone brachte; Andrew Morton bezeichnete das gar als „großes Geschenk an Nvidia“. Die Entwickler drängten darauf, einige für HMM wichtige Symbole nachträglich auf GPL-Export umzustellen, was normalerweise untersagt ist. Nach mehreren Diskussionen auf Mailinglisten und einer Debatte auf dem letzten Treffen zentraler Kernelentwickler wurde diesem Wunsch jetzt bei Linux 5.0 entsprochen. Das allein ist schon ein Novum, aber nicht das einzige: Die entsprechenden Änderungen wurden auch in alle modernen noch gepflegten Versionsreihen eingebaut und sind daher in Linux 4.20.2, 4.19.15, 4.14.93, 4.9.150 und neuer zu finden. In der Begründung heißt es, es sei ein Versehen gewesen, dass diesen Funktionen die GPL-Kennzeichnung gefehlt habe.

Indirektes Problem

Nvidias proprietärer Grafiktreiber zeigt sich von dieser Änderung allerdings unbeeindruckt, denn die HMM-Unterstützung ist dort noch unvollständig und wird daher standardmäßig nicht gebaut. Nvidias Entwickler müssen jetzt sehen, ob oder wie sie ohne die entsprechenden Linux-Funktionen auskommen. Unklar ist, wie stark sich der Schritt der Kernelentwickler auf die Performance auswirkt.

Linux-Entwickler werfen proprietären Treibern bewusst Knüppel zwischen die Beine. Das soll vor allem Nvidia treffen.

AMD und Intel juckt das Ganze übrigens nicht: Sie setzen für solche Dinge auf Open-Source-Treiber, die Bestandteil des

Kernels sind. Dabei müssen die zwei langjährigen Konkurrenten an vielen Stellen zusammenarbeiten.

Die Linux-Geschichte zeigt: Häufig führt genau das zu Lösungen, die letztlich viele Vorteile für Nutzer und die beteiligten Firmen haben.

Die HMM-Problematik wird Nvidia nicht veranlassen, von heute auf morgen auf

quelloffene Treiber für den Linux-Kernel umzuschwenken. Durch solche Einschränkungen wächst aber der Druck auf Nvidia. Und die werden nach und nach mehr, denn der Anteil der mit GPL-Kennzeichnung versehenen Symbole steigt: Ende 2005 trugen circa zehn Prozent der exportierten Symbole die GPL-Kennzeichnung, heute sind es bereits etwas mehr als die Hälfte. Das ist nicht nur für Nvidia relevant, sondern auch für ZOL und Entwickler anderer Treiber, die sich nicht an die Spielregeln der Lizenz des Linux-Kernels halten.

Einschränkungen umgehen

Bei Diskussionen im Netz heißt es oft, Distributionen könnten die GPL-Kennzeichnung doch einfach bei ihren Kernen ent-

fernen, um die ganze Sache für ihre Nutzer aus der Welt zu schaffen. Technisch erfordert das nur ein paar simple Handgriffe. Damit würde sich so ein Distributor aber den Zorn einiger Kernelentwickler zuziehen – zumindest für die großen Linux-Anbieter dürfte das schon Grund genug sein, diesen Pfad nicht zu beschreiten.

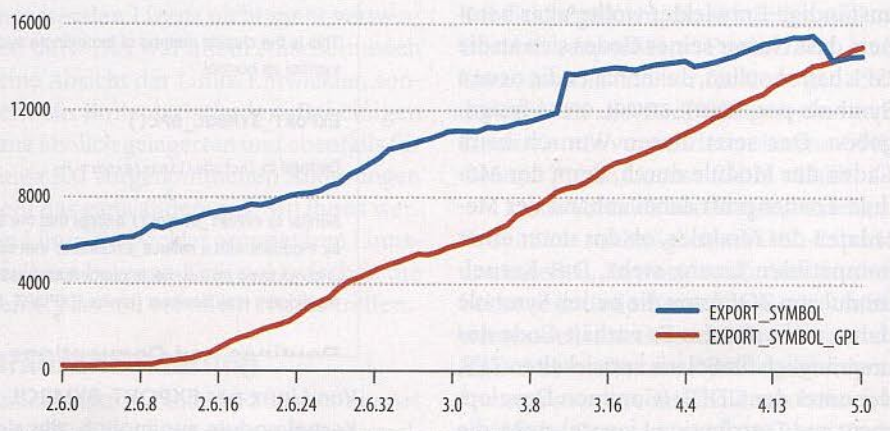
Das eigentliche Problem sind aber die rechtlichen Implikationen: Man entfernt zwar nicht die Lizenz selbst, aber eine Kennzeichnung und Technik, die auf Einhaltung der Lizenz drängt. So ein Schritt dürfte vor Gericht schwer zu vertreten sein. Das veranschaulicht ein Vergleich aus dem echten Leben: Stellen Sie sich ein weitläufiges Bauernhofgrundstück vor, mit einer Hecke, die man leicht übersteigen kann – was Sie und andere gelegentlich machen, um eine Abkürzung zum dahinterliegenden Strand zu nehmen. Nachdem der Eigner das einige Wochen geduldet hat, stellt er ein Schild „Privatgrundstück, Betreten verboten“ auf. Wer das entfernt, muss bereits mit Ärger rechnen. Insbesondere, wenn er die Abkürzung dann weiter nutzt, schließlich hat der Bauer seine Besitzansprüche schon durch die Hecke deutlich gemacht; das Schild sollte nur Zweifel beseitigen.

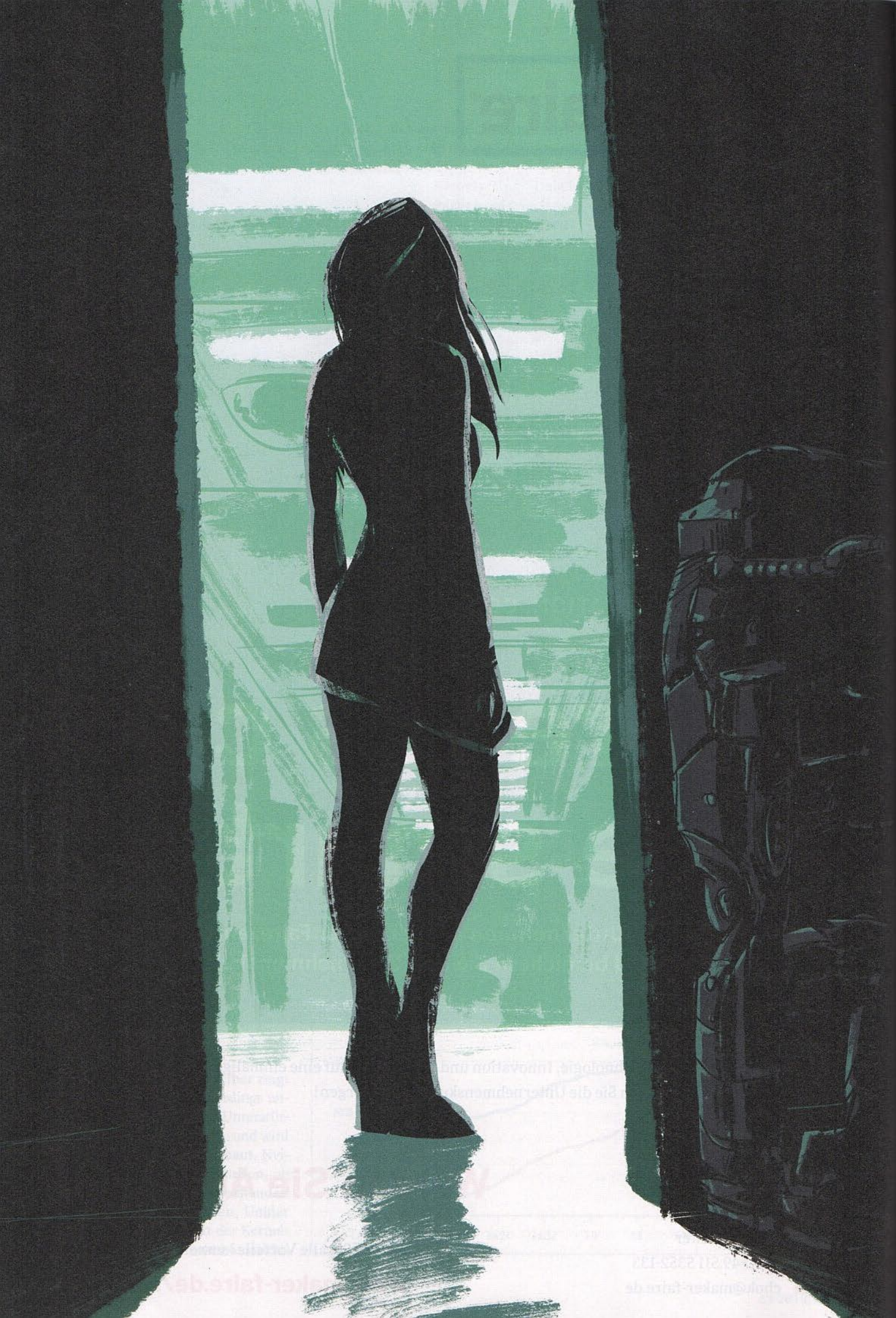
Relevant ist das alles aber ohnehin nur, wenn man denn Software verbreitet, denn erst da greift die GPL. Wer nur für interne Zwecke kompiliert, kann durch GPL-Exporte entstehende Einschränkungen umgehen, ohne dass Ärger droht.

(thl@ct.de) **ct**

Funktionsexporte bei Linux

Der Linux-Kernel exportiert einige Funktionen über Symbole, die nur unter der GPL oder kompatiblen Lizenzen stehende Kernel-Module nutzen dürfen. Deren Anteil hat nach und nach zugenommen; seit Linux 4.19 exportiert der Kernel mehr als die Hälfte der Funktionen auf diese Weise.





TYRUS (1)

VON HILGA HÖFKENS

Mit fahrigten Händen griff er nach der Schnalle und zog sie fest. Warum gab es bei all dieser hochmodernen Technik immer noch so altmodische Befestigungen? Eine Klammer, die sich automatisch um sein Bein schließen würde und selbst den richtigen Druck für sicheren Halt bestimmen könnte, das wäre doch State-of-the-art, oder nicht?

Er packte sein rechtes Bein mit einem festen Griff und als er es anhob, um es in die Halterung zu legen, hatte er etwas zu viel Schwung. Die Ferse knallte auf die Metallkante und ein stechender Schmerz schoss in seinen Kopf.

Ja, ganz toll. Bewegen konnte er dieses tote Fleisch immer noch nicht, nur der Schmerz war schon von Anfang an da. Der Schmerz war nach der Operation zuerst zurückgekommen. Sie hatten es ihm nicht glauben wollen, dass sein ganzer unterer Körper, direkt nach dem Aufwachen aus der Narkose, eine Hölle aus Schmerz war. Zwei Tage hatte er in hilfloser Agonie dagelegen und sich gewünscht, endlich bewusstlos zu werden. Dann hatten irgendwann die Muskelkrämpfe eingesetzt und endlich hatte er Medikamente bekommen.

Mit einer ärgerlichen Handbewegung schob er das nutzlose Bein in die Halteschale, dann hielt er inne und gab sich noch einmal etwas mehr Mühe mit der Positionierung. Wenn er das nicht ordentlich machte, würde sein Bein es ihm bei den Übungen nur mit mehr Schmerz heimzahlen.

Diese beschissenen Maschinen wussten eben doch nicht alles, auch wenn sie das immer behaupteten. Sicherlich hätten sie selbst mit einem einfachen, altmodischen EKG feststellen können, dass er die Wahrheit sagte. Oder besser schrie. Und stöhnte. Zu vernünftiger Kommunikation war er in diesen Tagen nicht in der Lage gewesen und das war es, worauf sie programmiert waren. Entweder sie konnten mit ihren Sensoren eine Veränderung feststellen, so etwas wie die Muskelkrämpfe beispielsweise, oder man sprach vernünftig mit ihnen.

Die Veränderung in seinem Verhalten war natürlich nicht unbemerkt geblieben, oh nein. Das wären ja grauenhaft schlechte Medbots, wenn sie nicht auch die kleinste Abweichung in der Reaktion desjenigen Menschen feststellten, den sie betreuten. Nein, nein, bemerkt hatten sie es

natürlich, aber ihre kalten Schaltkreise waren zum falschen Ergebnis gekommen. Sie hatten es für eine psychische Reaktion auf die Operation gehalten und versucht, ihn mit Psychopharmaka vollzustopfen.

Immerhin konnten sie das nicht gegen seinen Willen tun. So viel Freiheit war ihm in seiner perfekt ausgestatteten Krankenzelle noch geblieben. Solange man bei Bewusstsein war, musste man den Medikationsvorschlag aktiv bestätigen. Nur falls man das Bewusstsein verlor, durften sie ohne Bestätigung lebenserhaltende Maßnahmen ausführen. Und dann mussten sie Alarm geben. An einen Menschen.

**SIE WAREN SCHON RECHT EFFEKTIV,
DIESE MEDBOTS. FAST SCHIEN ES,
ALS KÖNNTEN SIE GEDANKEN LESEN.**

Seine Eingeweide zogen sich zusammen bei dem Gedanken an einen Menschen aus Fleisch und Blut. Seit dem Unfall hatte er niemanden mehr gesehen, aber wie lange war das inzwischen her? Es waren Monate, aber wie viele? Er wusste es nicht mehr.

In diesen riesigen Medizinkomplexen gab es nur sehr wenige menschliche Mitarbeiter – durchweg waren das hochspezialisierte Techniker. Meist wurden ja auch nur einfache und schnelle Operationen und kurze medizinische Behandlungen durchgeführt. So konnten die Patienten fast immer bereits nach einem Tag oder zumindest nach einer Woche wieder entlassen werden. Man wusste natürlich, dass ein Mensch zum Wohlbefinden und zur Heilung auch sozialen Kontakt brauchte. Jeder nahestehenden Person wurden in ihrem Job Freistunden gegeben, wenn sie in dieser Zeit

jemanden im Medkomplex besuchte. Gute Sache soweit. Nur, es gab niemanden. Nicht für ihn.

Mit zitternden Händen schnallte er auch auf der linken Seite das Exoskelett an seinem Unterschenkel fest. Dann richtete er sich auf und sah auf die schlaffen, dünnen Dinger, die jetzt in der mechanischen Vorrichtung steckten. Nicht nur den Gebrauch seiner Beine hatte er bei dem Unfall verloren. Seine kleine Schwester war bei dem furchtbaren Unglück mit dem Transporter gestorben. Gestorben war wirklich eine harmlose Umschreibung. Zerrissen hatte es sie und ihr Körper ... Mit übermächtiger Anstrengung versuchte er, diese Erinnerung zur Seite zu schieben. Es gelang ihm nicht und in einer hastigen Bewegung beugte er sich zur Seite. Er konnte das Würgen nicht mehr unterdrücken.

Nachdem er sich wieder einmal übergeben hatte, schloss er erschöpft die Augen. Wenn das so weiterging, brauchte er sich um Muskeltraining bald keine Sorgen mehr zu machen. Da wäre nichts zum Trainieren mehr übrig. Er wusste nicht, wie viel er schon abgenommen hatte, seit er hier war, aber seine alten T-Shirts sahen aus, als wären sie zwei Nummern zu groß. Von den Hosen war gar nicht zu reden. Den morgendlichen Blick in den Spiegel schenkte er sich inzwischen. Früher hatten ihn seine Freunde für gutaussehend erklärt, aber das hohlwangige Gespenst mit den tief liegenden Augen, das ihn aus dem Spiegel anstarrte, das konnte nicht er sein.

Eine kleine Reinigungseinheit hatte sich bereits um die Sauerei gekümmert, die er gemacht hatte. Neben sich fand er ein Einwegtuch und ein Glas Wasser.

MIT EINEM SEUFZEN VERBAND ER DIE KABEL DER MOTOREINHEITEN MIT DER STEUERUNG AN SEINER HÜFTE.

Sie waren schon recht effektiv, diese Medbots. Fast schien es, als könnten sie Gedanken lesen. Aber im entscheidenden Augenblick versagten sie dann doch. So wie bei den Schmerzen oder einfach bei dem Verlangen nach menschlicher Nähe.

Er schlang die Arme um seinen Brustkorb und zitterte. Es war erbärmlich, dieses Leben oder was von diesem Leben übrig geblieben war.

Bei ihm hatten sie die Unfallfolgen durch mehrere Operationen fast völlig beheben können. Kurz hatte sein Leben auf Messers Schneide gestanden und mehr als einmal hatte er sich in den letzten Wochen schon gewünscht, es wäre in die andere Richtung gekippt.

Zu guter Letzt hatten sie eine Vorrichtung, die er nicht ganz verstand, in seine Wirbelsäule eingebaut, an der Stelle,

wo das Rückenmark durchtrennt war. Vollständige Kontrolle und Sensibilität sollten dadurch wiederhergestellt werden. Na ja, bis jetzt waren nur die Schmerzen zurückgekommen. Manchmal zuckten die Beine auch, manchmal hatten sie furchtbare Krämpfe, aber Kontrolle hatte er immer noch nicht.

Es würde bis zu einem ganzen Jahr dauern, das hatten sie ihm schon wer weiß wie oft gesagt. Was sie nicht gesagt hatten, war, wie er es hier ein ganzes Jahr aushalten sollte. Umgeben von Medbots und kalter, unpersönlicher Effektivität entwickelte er ein geradezu übermächtiges Verlangen nach einer menschlichen Stimme.

Mit einem Seufzen verband er die Kabel der Motoreinheiten mit der Steuerung an seiner Hüfte. Dann schob er die Verbindung zum Implantat unter seinem T-Shirt am Rückgrat hinauf, bis sie an dem Magneten unter seiner Haut hängen blieb.

All diese Bewegungen konnte er inzwischen im Schlaf ausführen, aber immer wieder zweifelte er am Sinn der ganzen Sache. Inzwischen hätte er zu mehr willentlichen Bewegungen auch ohne Exoskelett imstande sein müssen, aber jeder kleine Fortschritt verschlang Wochen. Zeit, in der seine Muskulatur immer weiter abbaute und in der es seine Seele immer tiefer in dem schwarzen Abgrund zog. Irgendwann könnte er vielleicht wieder laufen, aber bis dahin würde er ein psychisches Wrack sein.

Mit den Händen schob er das Exoskelett von der Liege und rutschte nach vorn auf die Kante. Für heute war er bereit für seine Runden mit den elektrischen Beinen, wie er sein Trainingsgerät immer nannte.

Durch die Übungen wurden die neuronalen Verbindungen zwischen dem Implantat und den verschiedenen Arealen im Gehirn etabliert, dann wurden sie automatisch angepasst und eingestellt. Auch die Muskeln mussten natürlich wieder kräftiger werden. Das hatte ihm seine Psychobotstimmte alles ausführlich erklärt.

Er weigerte sich, sie mit dem Namen anzusprechen, mit dem sie sich vorgestellt hatte. Wenn er ihren Namen benutzte, würde er irgendwann vergessen, dass da kein Mensch hinter dieser Stimme war. Es war eine warme, angenehme Stimme und er würde sich ausmalen, wie sie wohl aussah, wie sie sich anfühlte, wenn seine Hände über ihren Körper strichen und seine Lippen ... Er würgte wieder, doch dieses Mal war sein Magen bereits leer.

Wie konnte man so einsam sein, dass man bei dem Gedanken an ein Computerprogramm einen Ständer bekam? So weit war es also schon mit ihm gekommen.

Seine Hände krampften sich um die Griffe der Krücken, bis die Knöchel weiß hervorstachen und mit einem Ruck stand er auf. Hart zu trainieren war immer noch der beste Weg, nicht verrückt zu werden. Wenn sein Körper dann völlig ausgelaugt auf der Pritsche lag, konnte er wenigstens schlafen.

Dann träumte er zwar, verrückte und kaputte Träume voller Schmerz und Sehnsucht, aber das war immer noch besser als wach zu sein und über die nächsten Wochen und Monate nachzudenken.

Er konzentrierte sich auf das Exoskelett, machte den ersten Schritt. Dann den zweiten. Weiter ging er mit größtmöglicher Konzentration durch den Raum und nach der dritten Runde stellte er die Krücken in ihre Halterung. Er durfte sich nur nicht ablenken lassen, dann ging es doch schon ganz gut.

ODER ZUMINDEST MAL UNTERHALTEN PER VIDLINK. WENIGSTENS AB UND AN MIT IHR SPRECHEN UND DIESES WUNDERBARE LACHEN SEHEN.

Langsam schritt er weiter, als er plötzlich von draußen eine Stimme hörte. Sein ganzer Körper krampfte sich zusammen und beinahe wäre er gestürzt. Da war jemand vor seiner Tür. Ein Mensch. Ein richtiger, wirklicher Mensch. Wahrscheinlich Besuch für einen seiner Nachbarn, die er noch nie gesehen hatte. Er hatte auch noch nie jemanden auf dem Gang reden hören. Sein Herzschlag dröhnte in den Ohren und seine Hände zitterten, als er beschloss, die Tür zu öffnen. Wenigstens sehen wollte er sie. Es war ganz eindeutig eine weibliche Stimme gewesen. Einmal ansehen, vielleicht kurz grüßen. Vielleicht würde sie zurückgrüßen. Oder lächeln. Bitte lächeln, bitte.

Die Konzentration, die für die Bewegung seiner Beine notwendig war, verpuffte bei der Vorstellung eines Lächelns und mit drei stolpernden Schritten fiel er fast zur Tür. Gerade noch konnte er sich am Griff festhalten, bevor er der Länge nach hingeschlagen wäre. Dann öffnete er hastig und machte einen unsicheren Schritt nach draußen.

Verzweifelt versuchte er, sich auf seine Beine zu konzentrieren. Sein Blick klebte fest auf dem Boden vor seinen Füßen. Das war nicht richtig, er wusste es. Nicht hinuntersehen! Noch bevor er seinen Fehler korrigieren konnte, spürte er, wie er wie in Zeitlupe nach vorn kippte. Beide Beine waren stehengeblieben. Das taten sie immer, wenn er auf den Boden sah, während sich sein Oberkörper weiter bewegte.

Sie stand unmittelbar vor ihm, er würde gegen sie stoßen. Automatisch schossen seine Hände nach vorn und klatschten gegen die Wand, auf der gegenüberliegenden Seite des Flurs. Es war zu spät. Sein Brustkorb stieß sie nach hinten und er konnte gerade noch sein Gesicht wegdrehen, um ihr nicht auch noch eine Kopfnuss zu geben.

Keuchend stützte er sich gegen die glatte Oberfläche hinter ihr und dann spürte er sie. Seine Brust war gegen ihre gepresst, seine Wange lang an ihrem Haar und seine Arme

rahmten ihre Schultern ein. Ihr Duft zog in seine Nase und die Wärme ihrer Haut brannte wie Feuer überall dort, wo er sie berührte.

Einen Herzschlag lang schloss er die Augen und verlor sich in dem Gefühl ihrer Nähe. Dann raffte er all seine Willenskraft zusammen und stieß sich mit den Händen von der Wand ab. Schwankend taumelte er zurück, bis sein Rücken am Türrahmen seines Medpartments Halt fand.

„Es tut mir leid. Ich wollte nicht ... Ich bin gestolpert, aber ich wollte Ihnen nicht zu nahe treten.“ Seine Augen waren auf den Boden geheftet und er wagte es nicht, den Blick zu heben, um sie anzusehen. Sein ganzer Körper war völlig verkrampft und es fühlte sich an, als ob er haltlos zitterte. Dieser kurze Moment, diese versehentliche Berührung – so tief hatte sie sein Innerstes aufgerissen, dass unwillkürlich Tränen hinten in seinen Augen brannten.

„Das macht nichts. Es ist ja nichts passiert.“ Der fröhliche Ton in ihrer Stimme brachte seinen Herzschlag zum Stolpern und löste in ihm das unbeherrschbare Verlangen aus, sie noch einmal zu berühren.

Langsam hob er den Blick und seine Augen verschlangen ihren graziösen Körper in dem eng anliegenden Kleid. Als er bei ihrem schmalen Gesicht mit der hellen Haut und den wunderbaren Lippen anlangte, breitete sich dort ein freundliches Lächeln aus.

Heiß schoss dieses Lächeln unter sein Brustbein und beinahe hätte ein sehnsüchtiger Seufzer sich aus seinem Mund gestohlen. Gerade noch konnte er es wie ein Räuspern klingen lassen. Während er verzweifelt nach Worten suchte, legte sie eine Hand auf seine Schulter.

„Hey, alles in Ordnung?“ Tief holte er Luft und schüttelte mit zusammengepressten Lippen den Kopf. Er verlor sich in ihren hellen Augen und bemerkte überhaupt nicht, dass er eine Hand nach ihr ausstreckte.

Dann tat sie etwas, womit er niemals gerechnet hätte. Sie machte einen Schritt nach vorn und umfasste mit beiden Händen seine Schultern. Wortlos sah sie ihn an und ihre Hände strichen beruhigend über seine Oberarme.

Mit einer hastigen Bewegung schlang er seine Arme um ihren Körper und zog sie an sich heran. Er konnte nicht anders, er musste sie noch einmal spüren, sie festhalten.

Eigentlich hatte er erwartet, dass sie sich zurückziehen und aus seinen Armen winden würde. Aber sie erwiderte seine Umarmung und fuhr fort, ihre Hände auf und ab zu streichen, jetzt jedoch an seinem Rücken.

Überwältigt von der Intensität seiner Gefühle barg er sein Gesicht an ihrem Hals. Fest presste er sie an sich, als ob er all die Monate der Einsamkeit mit dieser einen Umarmung auslöschen könnte.

Plötzlich überfiel ihn die Erkenntnis, dass sie nicht gekommen war, um ihn zu besuchen. Sie war für jemand anderen hier und er nahm sich gerade, worauf er kein Anrecht hatte. Sie würde jetzt gleich zu diesem Anderen gehen und nie mehr zu ihm zurückkommen. Diese Umarmung würde die einzige bleiben, für immer. Sein Herz krampfte sich bei dieser Erkenntnis so hart zusammen, dass er sicher war, es würde gleich aufhören zu schlagen.

Es konnten nur wenige Augenblicke gewesen sein und doch fühlte es sich für ihn wie ein Zeitalter an, bevor sie sich ein wenig zurücklehnte, um ihm ins Gesicht zu sehen. Sie nahm eine Hand von seinem Rücken und strich in einer unglaublich liebevollen Geste eine Strähne aus seiner Stirn.

„Hey, geht es wieder?“

Nein! wollte er schreien. *Geh nicht weg! Es geht nicht, gar nicht, wenn du mich wieder allein lässt!*

Doch ohne dass er es wollte, nickte er zittrig und holte tief Luft. Dann schaffte er es irgendwie, seine Arme von ihr zu lösen. Ihre Hand lag noch immer auf seiner Schulter.

„Sicher, dass alles in Ordnung ist?“ Wieder nickte sein Kopf ohne sein Zutun, doch seine rechte Hand hielt ihre fest, in einer letzten verzweifelten Auflehnung gegen das Unvermeidliche. Er schaffte es irgendwie, seine Stimme unter Kontrolle zu bringen und zu antworten.

„Es tut mir sehr leid. So einen Überfall hatte ich wirklich nicht vor. Entschuldigen Sie bitte.“ Sie lächelte wieder und die Sonne ging auf. Warum nur konnte er nicht wenigstens dieses Lächeln festhalten, um es immer dann anzusehen, wenn er wieder an der Einsamkeit zu ersticken drohte?

„Das ist in Ordnung, manchmal hat man eben solche Momente. Ich heiße übrigens Freya.“ Sein Herzschlag beschleunigte sich, wenn das denn überhaupt noch möglich war. Ein vorsichtiges Grinsen stahl sich auf sein Gesicht.

„Im Ernst? Die nordische Göttin der Liebe und der Schlacht? Mein Name ist Tyrus. Der ist irgendwie zusammengesetzt aus Tyr und Tius. Das ist ja ein spannender Zufall.“

Sie nickte. „Hallo Tyr, Gott des Kampfes und des Sieges – schön, dich kennenzulernen.“ Ein heißer Funke Hoffnung entstand tief in seinem Inneren. Tyr nannten ihn immer seine Freunde, weil ihnen Tyrus irgendwie zu martialisch klang. Sie hatte es ausgesprochen wie einen Kosenamen, sanft und beinahe zärtlich.

Wenn er sie nur in ein Gespräch verwickeln könnte und sie sich ein wenig kennenlernen würden, wäre es dann möglich, dass sie ihn besuchen würde? Vielleicht hin und wieder?

Oder zumindest mal unterhalten per Vidlink. Wenigstens ab und an mit ihr sprechen und dieses wunderbare Lachen sehen. Er verkrampfte sich bei dem wilden Wunsch, sie wiederzusehen.

„Hallo, Freya.“ Weiter kam er nicht. Sein Gehirn war wie leergefegt. Er öffnete den Mund, aber es kamen keine Worte heraus, also schloss er ihn wieder. Sie trat einen Schritt zurück und atmete einmal tief aus, beinahe klang es wie ein Seufzen.

„Ich muss dann mal wieder. Vielleicht sieht man sich ja.“ Kurz schien sie nachzudenken und sah an ihm herunter. „Obwohl, das ist unwahrscheinlich.“

Doch! schrie seine innere Stimme. *Ich weiß, ich bin ein Wrack, aber das kommt alles wieder in Ordnung. Ich werde wieder laufen können, ich werde bald hier herauskommen und dann werde ich für dich da sein und dich für immer lieben.*

Nur ein kurzer unartikulierter Laut, etwas wie ein „Ah“, schob sich aus seinem zusammengekrampften Brustkorb

und er hob die Hand, um sie wenigstens noch einmal kurz zu berühren. Doch sie hatte sich schon abgewandt und seine Hand schwebte in der Leere zwischen ihnen, bevor sie herabfiel. Bewegungslos stand er mit dem Rücken an der Wand und sah ihr nach.

Ihr perfekter Körper bewegte sich mit beinahe übernatürlicher Anmut, als sie den Gang hinunterschritt und sich dann der nächsten Tür zuwandte. Sie hob den Arm und legte in einer fast schon zärtlichen Geste die Hand auf den Scanner. Sofort öffnete sich die Tür und sie verschwand.

Versteint starrte er dorthin, wo sie soeben noch gestanden hatte. Sie hatte das Medpartment mit ihrem Handabdruck geöffnet. Sie war keine Besucherin. Sie arbeitete hier.

SIE HATTE DAS MEDPARTMENT MIT IHREM HANDABDRUCK GEÖFFNET. SIE WAR KEINE BESUCHERIN.

Blut rauschte in seinen Ohren und die Gedanken fielen alle durcheinander. Verzweifelt versuchte er, Ordnung hineinzubringen.

Das konnte nur heißen, dass sie einer von diesen wenigen Menschen war, die sich immer nur dann um die Patienten kümmerten, wenn diese bewusstlos waren oder die Maschinen aus anderen Gründen nicht mehr klarkamen.

Mit einem Kopfschütteln startete er die halboffene Tür an. Dort war also wahrscheinlich ein Notfall, deswegen hatten die Bots sie gerufen. Man rief sie für Notfälle, dann kam sie zu dem betreffenden Patienten und kümmerte sich um ihn.

Ganz langsam begann ein Plan in einer stillen Ecke seiner Gedanken zu reifen. Es war nur ein Notfallplan. Vielleicht konnte er sie ja doch noch zu einem normalen Besuch überreden, wenn sie dort wieder herauskam.

Auch Mitarbeiter der Medcompany hatten irgendwann Feierabend. Aber würden sie in ihrer Freizeit ausgerechnet einen Patienten besuchen? Ah, nein, sie musste nicht ihre Freizeit opfern. Sie würde dafür Freistunden bekommen. Ganz besonders von der Medcompany und ganz besonders für ihn. Er war immerhin ein schwerer Fall, der extrem lange hierbleiben musste und noch nie Besuch bekommen hatte. Wahrscheinlich war er der einzige Langzeitpatient, der nie Besuch bekam. Wieder presste die Einsamkeit sein Herz zu einem harten Klumpen zusammen. Aber jetzt hatte er Hoffnung. Sie würde ihn besuchen. Ab und an. Vielleicht.

(psz@ct.de) **ct**

Letzter Teil im nächsten Heft

Vorschau 6/2019

Ab 2. März 2019 im Handel und auf ct.de



Mobile WLAN-Router

Wenn das Signal schwächelt oder andere Urlauber den Hotel-Access-Point lähmen, macht das Surfen und Streamen im Urlaub keinen Spaß. Ein Reise-router hilft: Er verstärkt das Hotel-WLAN oder nutzt die LAN-Buchse im Zimmer. Wir testen fünf kompakte Begleiter.



Der optimale Scanner

Dokumente, Pläne, Fotos, Filme und Bücher – für fast jede zu digitalisierende Vorlage gibt es spezialisierte Scanner. Oder genügt ein Multifunktionsgerät mit Scanaufsatz? Wie viel muss man ausgeben? Wir erklären die Vor- und Nachteile der diversen Scanner-Typen und geben Tipps zur Geräteauswahl.

Außerdem:

Windows-Umzug

Wenn ein neuer PC fällig ist, kann man Windows darauf sauber neu installieren oder das vorinstallierte System nutzen. Bequemer ist es freilich, die vom alten PC vertraute Installation einfach mitzunehmen. Das geht auf verschiedenen Wegen, die alle ihre Vor- und Nachteile haben.

Besser finden

Schnell ein paar Begriffe eingetippt und Google wird schon das Richtige herausuchen. Nein, Internet-Recherche geht viel besser: Operatoren und Browser-Adresskürzel helfen bei der Zielfahndung, alternative Dienste schützen die Privatsphäre und finden auch dort etwas, wo Google blind ist.

Tools für schönere Videos

Was haben YouTuber, Familienfilmer und Besitzer von Actioncams gemeinsam? Sie alle brauchen eine Software, um aus ihren Clips einen spannenden Film zu schneiden. Wie elegant das mit gängigen Programmen bis etwa 200 Euro gelingt und welche Funktionen beim Aufbrezeln der Videos helfen, verrät unser Test.

Noch mehr
Heise-Know-how:



Mac & i 1/2019 jetzt im Handel und auf heise-shop.de



c't wissen DSGVO jetzt im Handel und auf heise-shop.de



iX 2/2019 jetzt im Handel und auf heise-shop.de