Editorial

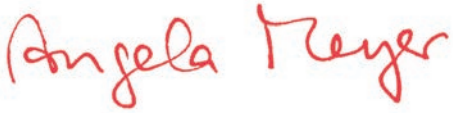
Mehr wissen, besser verstehen

IT entwickelt sich ständig weiter: Neue Hardware-Standards, Softwareklassen oder Betriebssystem-Versionen eröffnen und erfordern andere Wege, sich sein System gut einzurichten. Da fällt es selbst dem Profi nicht immer ganz leicht, das eigene IT-Know-how auf dem aktuellen Stand zu halten.

Dieses c't-Sonderheft will Sie mit einigen technischen Hintergründen und Zusammenhängen rund um Hardware, Software und Netzwerktechnik unterstützen. Zu den Themen, die wir in der letzten Zeit nützlich fanden, gehören zum Beispiel: Wie blickt man durch im USB-Bezeichnungs-Chaos? Was muss man über die Registry wissen? Wie nutzt man eigentlich Docker-Container? Und wie verkabelt man sein Heimnetz so, dass dort WLAN bestmöglich läuft?

Wir hoffen, dass Sie mit unseren Antworten auf diese und andere Fragen Ihren praktischen Problemen zielgerichteter auf den Grund gehen können und sich so Ihren IT-Alltag erleichtern. Und vielleicht finden Sie, so wie wir, viele der Themen in diesem Heft schon allein deshalb spannend, weil Sie schon immer wissen wollten, was eigentlich dahintersteckt. Lassen Sie sich überraschen!

Eine aufschlussreiche Lektüre wünscht



Angela Meyer

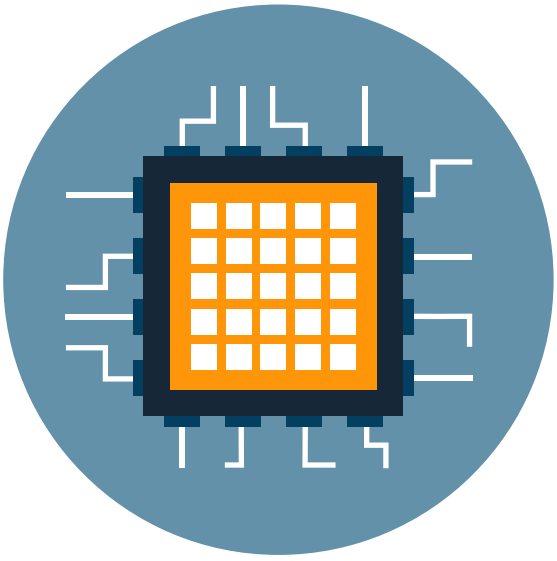
Inhalt

HARDWARE-KNOW-HOW

6 Wie Flash-Speicher funktionieren
10 Was hinter dem Chaos bei USB-Namen steckt
16 Tintendruck-Technik: Piezo oder Bubblejet?
20 Mikrocontroller versus Mikroprozessoren
24 Technik gegen Stromausfälle

SOFTWARE-KNOW-HOW

28 Wissenswertes zum Windows-10-Explorer
34 Grundwissen Dateisysteme
42 Was Sie wissen müssen zur Registry
48 E-Mail: Begriffe und Protokolle
56 Docker verstehen und loslegen
64 Serverinfrastruktur mieten in der Cloud

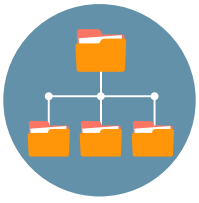


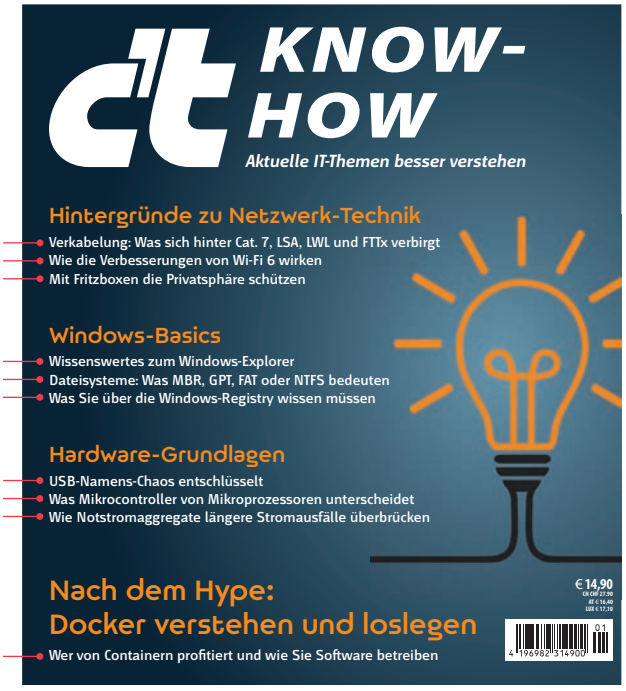
NETZWERK-KNOW-HOW

72 Grundwissen zur Heimnetzverkabelung
78 FAQ: Multigigabit-Ethernet
82 Wie Wi-Fi 6 das WLAN beschleunigt
90 FAQ: WLAN
94 Dienste ins Internet bringen
100 Beim Surfen die Privatsphäre schützen
106 FAQ: Verschlüsselte DNS-Anfragen
110 Glasfasern fürs LAN und fürs Internet

ZUM HEFT

3 Editorial
71 Impressum





Technik gegen Stromausfälle

Fällt im Rechenzentrum der Strom aus, liefert ein Batteriespeicher ausreichend Energie – aber nur für kurze Zeit. Bei längeren Ausfällen hilft ein Dieselaggregat weiter.

Von **Lutz Labs**

Rechenzentren sind in den allermeisten Fällen über eine ausreichend dimensionierte unterbrechungsfreie Stromversorgung (USV) vor einem Stromausfall geschützt. Wenn aber der eigene Desktop-PC noch läuft, während es in der ganzen Straße um einen herum dunkel ist, dann ist wahrscheinlich ein anderer Energielieferant im Spiel: ein Stromgenerator, den ein starker Dieselmotor antreibt.

Am Hauptsitz der Heise Gruppe steht dazu – in einem eigenen kleinen Gebäude etwas abseits – ein größeres Dieselaggregat. Der gewaltige 720-Kilowatt-Generator versorgt bei Stromausfall nicht nur alle Rechner im Haus weiter, sondern auch Parkplatzbeleuchtung, Brunnen und Aufzüge – und der Diesel ist dann immer noch nicht einmal bei 50 Prozent Last angelangt.

Maschinenbau par excellence

Solche Dieselaggregate dienen häufig zur Notstromversorgung, aber auch auf großen Jachten kommen sie zum Einsatz. Für Straßenfahrzeuge sind solche Motoren mit mehr als drei Tonnen Leergewicht zu schwer. Unser Diesel läuft mit 1500 Umdrehungen pro Minute, hat 16 Zylinder mit insgesamt 32 Litern Hubraum und einen Abgasturbolader. Die Tanks im Gebäude fassen 2400 Liter Diesel, bei der Heise-üblichen Last reicht das für rund 24 Stunden Dauerbetrieb aus.

Prinzipiell könnte auch ein Benzingenerator zum Einsatz kommen, für diesen Einsatzzweck aber ist

Komponenten eines dieselbetriebenen Notstromaggregats

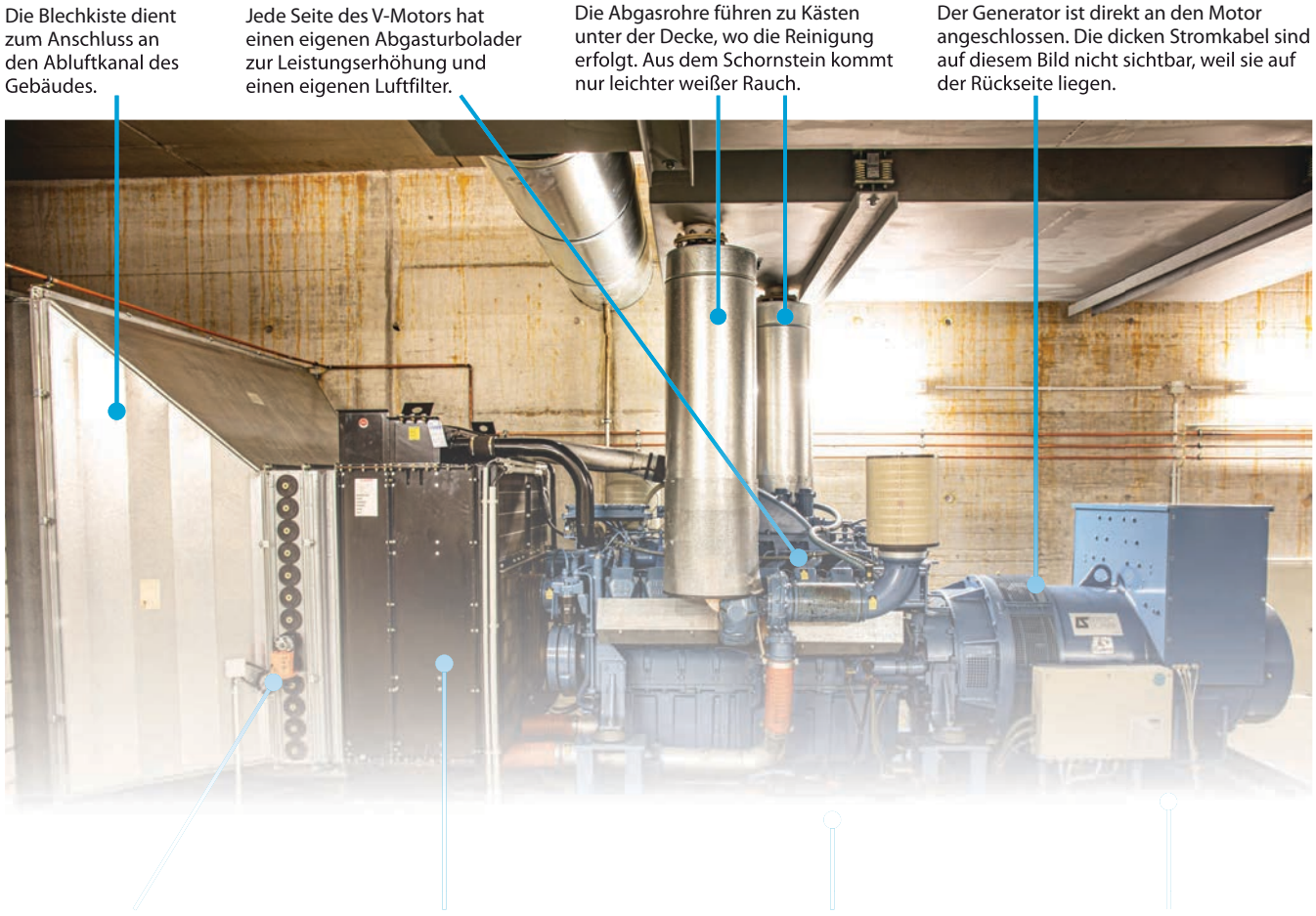


Bild: Sven Hauth

Serverinfrastruktur mieten in der Cloud

Flexibilität, schnelle Skalierung bei Lastspitzen und niedrigere Kosten – das sind die Versprechen der Cloudanbieter. Mit dem Anmieten von Servern ist es aber nicht getan: Wer in die Cloud umzieht, sollte Anwendungen und Gewohnheiten anpassen. Nur dann profitiert man wirklich von der Cloudinfrastruktur.

Von **Jan Mahn**

Dass Betreiber von Rechenzentren ihre Server vermieten, ist kein neues Geschäftsmodell, sondern seit Jahrzehnten üblich. Unter Bezeichnungen wie „Root-Server“, „vServer“ oder „Dedicated Server“ bekommt man ganze physische Server oder virtuelle Maschinen mit unterschiedlich viel zugesicherten Ressourcen bei zahlreichen Anbietern. Darauf läuft meist eine Linux-Server-Distribution, manchmal auch Windows Server. Einsetzen kann man die Maschinen für unterschiedlichste Serversoftware, vom Webserver über eine Videokonferenzsoftware bis zur KI-gestützten Datenaus-

wertung. Gemein ist diesen Angeboten, dass man auf dem Server die volle Kontrolle über das Betriebssystem hat und nach Belieben Software installieren darf. Das unterscheidet das Serverhosting vom Webhosting – dort gibt es einen vorinstallierten Webserver (und oft einen SQL-Datenbankserver) und als Kunde darf man nur Dateien fürs eigene Webangebot in einem Ordner ablegen.

Üblich sind beim Serverhosting eher lange Vertragslaufzeiten: Mindestens einen Monat, gerne auch 12 oder 24 Monate muss man dem Vermieter treu bleiben und den Server nutzen. Der Wechsel auf ein anderes Paket, zum Beispiel mit mehr Leistung, ist meist mit Kosten oder gar manuellem Umzugsaufwand verbunden. Oft verlangen die Anbieter einen Obolus für die Ersteinrichtung.

Ab etwa 2010 nahm dann ein neues Geschäftsmodell Fahrt auf: **Cloud Computing**. Von den Marketingabteilungen wurde der Begriff seitdem inflationär benutzt und auch IT-Laien, die nie in Verlegenheit kommen würden, selbst Server zu mieten, haben schon von „der Cloud“ gehört. Dabei ist der Kern der Idee derselbe wie beim klassischen Hosting – vermietet werden vor allem Server, aber auch Speicherplatz oder gleich fertig installierte und vom Anbieter gepflegte Serverdienste wie zum Beispiel Datenbanken.

Minutenpreise

Der große Unterschied ist das Abrechnungsmodell: Abgerechnet wird bei Cloudanbietern in Sekunden, Minuten oder Stunden, nicht in Monaten oder Jahren, und die Mindestlaufzeit liegt oft nur bei einer Minute. Die Vermieter haben die Prozesse auf Basis von gängigen Virtualisierungstechniken so automatisiert, dass ein virtueller Server innerhalb von wenigen Sekunden einsatzbereit ist. Damit werden ganz neue Einsatzbereiche möglich: Ein Ingenieur beispielsweise, der für die Berechnung eines mathematischen Modells nur eine halbe Stunde am Tag eine Hochleistungsmaschine mit 12 Prozessorkernen und 64 GByte RAM braucht, kann eine solche in der Weboberfläche eines Cloudanbieters bestellen, darauf seine Berechnung ausführen und die Maschine nach 30 Minuten wieder löschen. Für ein paar Euro bekommt er so Rechenleistung, für die er sich sonst teure Hardware ins Büro stellen müsste.

Aber auch Dienste, die rund um die Uhr laufen, profitieren von der Flexibilität in der Cloud – bestes Beispiel ist ein typischer Webshop, der im Zeitraum von Ende November bis zum 24. Dezember im Weihnachtsgeschäft mehr Kunden bedienen muss als im restlichen Jahr zusammen. Mit einem klassischen virtuellen Server in einem langfristigen Tarif würde er in elf von zwölf Monaten für eine Infrastruktur bezahlen, die kaum ausgelastet ist, weil sie auf den Ansturm des Weihnachtsgeschäfts ausgelegt ist. Das lohnt sich nur für den Vermieter. Bei Cloudanbietern dagegen könnte der Händler die Ressourcen, die seiner gemieteten virtuellen Maschine zugewiesen werden, Mitte November in Erwartung des Adventsansturms anpassen und nur bezahlen, was auch gebraucht wird.

Milliardengeschäft

Dieses Modell ist für Kunden wie Anbieter gleichermaßen attraktiv. Allein im ersten Quartal 2021 hat Amazon mit seinen Clouddiensten „Amazon Web Services“ (AWS) 13,5 Milliarden US-Dollar umgesetzt. Seit 2014 konnte das Unternehmen den Umsatz in jedem einzelnen Quartal steigern. Entgegen der landläufigen Meinung bedeutet Cloud-Computing aber nicht zwangsläufig, sich in die Abhängigkeit von einem der drei großen US-Anbieter Google

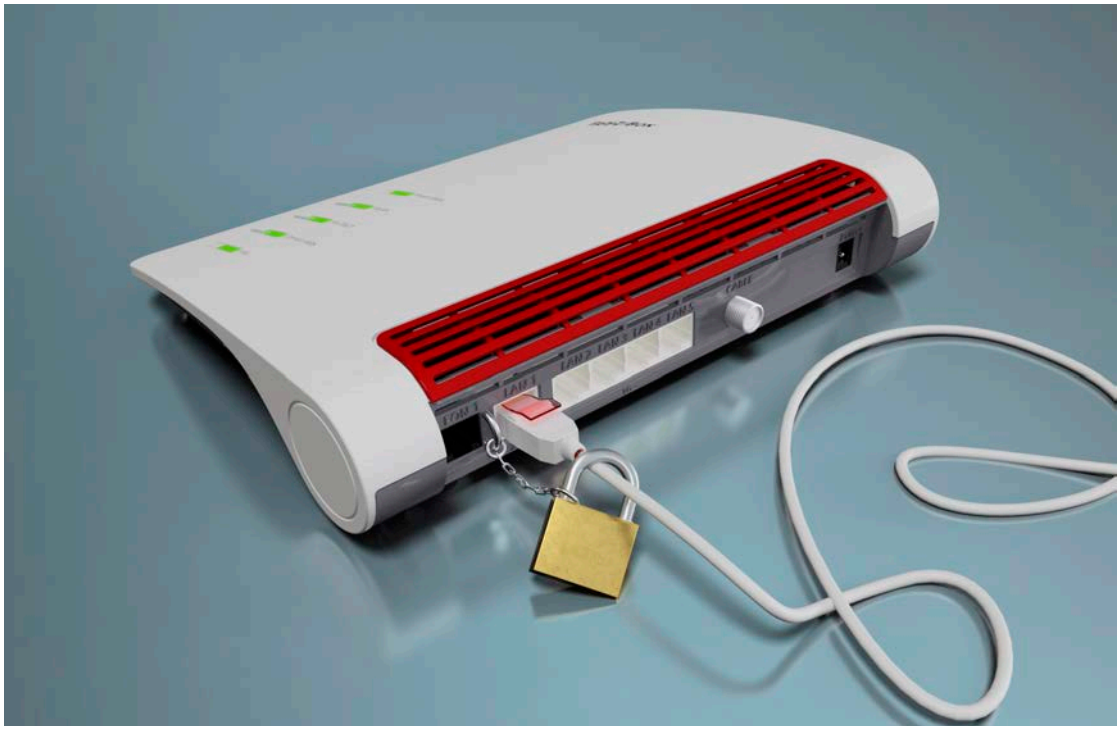


Bild: Andreas Martini

Beim Surfen die Privatsphäre schützen

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

Von **Dušan Živadinović**

Mit FritzOS 7.2x hat auf Fritzboxen eine wenig beachtete Funktion Einzug gehalten: die verschlüsselte Abfrage von Domainnamen, DNS-over-TLS (kurz DoT). Das klingt nach einer der vielen Spezialfunktionen für Netzwerk-Freaks, doch DoT ist für jeden Nutzer von Belang: Richtig angewendet, schützt sie vor einer Methode der Massenüberwachung, die zum Beispiel Geheimdienste und manche Provider einsetzen. Die Grundlage bilden Metadaten, die bei jedem Internetzugriff nebenbei anfallen; wer diese in die Hände bekommt, kann das Surf-Verhalten der Nutzer wie offene Tagebücher

lesen. Manche Provider verkaufen das als Surf-Profile an Werbetreibende.

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

Internet-Tagebuch verschlüsseln

Abhilfe schaffen neue Protokolle, die die Kommunikation mit den Resolvern verschlüsseln. Die wichtigsten sind DNS-over-TLS (DoT) und DNS-over-HTTPS (DoH), die beide die Internet Engineering Task Force spezifiziert hat. Daneben hat auch das proprietäre DNSCrypt eine gewisse Verbreitung erreicht. Alle drei haben wir in diversen Beiträgen beschrieben, siehe ct.de/wftg. DoT soll drei Probleme lösen: die Privatsphäre der Anwender gegen Lauscher schützen, das Einschleusen manipulierter DNS-Informationen verhindern und den Attacken, die gezielt die Resolver mancher Firmen überlasten sollen, ein Ende setzen (Distributed Denial of Service, DDoS).

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

Weil es unpraktisch ist, mehrere Computer und Smartphones einzeln aufzurüsten und aktuell zu halten, richtet man verschlüsselnde DNS-Clients zum Beispiel auf dem DNS-Filter Pi-hole für sein komplettes Netz ein, dann sind auch IoT-Geräte, Medienreceiver, Webcams und sonstige Netzwerkgeräte geschützt, die sich nicht aufrüsten lassen. Einen Pi-hole oder AdGuard Home zu betreiben erfordert allerdings etwas Know-how und Pflegeaufwand. Beides hat AVM in Fritzboxen mit FritzOS 7.2x auf ein Minimum reduziert. Jedoch fehlt der Fritzbox ein Werbeblocker vom Schlage eines Pi-hole oder AdGuard Home.

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

Zwei DoT-Profile

Das zweite Profil „Opportunistic Privacy Profile“ ist weniger streng: Es gewichtet funktionierende

Wie die DNS-Namensauflösung missbraucht werden kann

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