c't ADMIN

Verstehen • Vernetzen • Administrieren

PLUS
Videokurs
im Wert
von 99,- Euro

Mit komplettem Active-Directory-

ONLINEKURS



47 Lektionen: Active Directory mit Windows Server 2019 anschaulich erklärt

- *Prüfen Sie das Gelernte in Wissenstests*
- *Fragen beim Experten über das Q&A-Modul*
- *Machen Sie mit bei praktischen Übungen*
- *Ideal für die Fachinformatiker-Ausbildung*

Active Directory beherrschen

Nutzerkonten, Gruppen und Berechtigungen

Windows-PCs mit Gruppenrichtlinien

Domain Controller ausfallsicher betreiben

FritzOS 7.50 ist da

Was das große Gratis-Update bringt

Die beste Fritzbox für Ihren Anschluss

VPN optimal einsetzen

Schwachstellen im Netz finden

SBOM: Wege aus der Abhängigkeitshölle

NPM-Universum: Wie schlimm es wirklich ist

SIEM: Angriffe im Netzwerk erkennen

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

4 195957 614908 04

WIR MACHEN
KEINE WERBUNG.
WIR MACHEN EUCH
EIN ANGEBOT.

c't

ct.de/angebot

Jetzt gleich bestellen:
ct.de/angebot
+49 541/80 009 120
leserservice@heise.de

ICH KAUF MIR DIE c't NICHT. ICH ABONNIER SIE.

Ich möchte c't 3 Monate lang mit 35 % Neukunden-Rabatt testen.
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

**Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl,
z. B. einen RC-Quadrocopter.**



Editorial

Liebe Leserin, lieber Leser,

wie baut man heute in der Firma und zu Hause leistungsfähige Netzwerke, welche Elemente müssen modernisiert werden, wie hält man sie in Gang?

Fangen wir beim Wichtigsten an, dem Geld: Wenn Sie Ihr Netz noch per DSL ins Internet bringen, und sich die Chance bietet, wechseln Sie zur Glasfaser. Denn während das Internet-Datenvolumen stetig wächst, birgt nur die Glasfaser Kapazitäten für Jahrzehnte. Deshalb wird DSL für Netzbetreiber eines Tages unrentabel und folgt ISDN und UMTS in den Orkus. Dann dürfte die Glasfaserförderung aber ausgelaufen sein.

Wenn eine Fritzbox Ihr Netz ins Internet bringt, bestehen gute Chancen, dass Sie eine Router-Modernisierung gratis mitnehmen können: Das neue FritzOS 7.50 wird der Hersteller AVM zumindest für aktuelle Fritzbox-Modelle anpassen. Unsere VPN-, Smart-Home- und Telefonie-Tests belegen: Es lohnt sich.

Für Admins großer Netze lohnt sich auch die Windows-Verwaltung mit Active Directory. Sind die Clients erstmal am Domänen-Controller angemeldet, verwaltet man sie aus der Ferne und muss sich nur dann rühren, wenn die Hardware eine fürsorgliche Hand braucht.

Moderne Kommunikations-Software braucht hingegen unerwartete Zuwendung: Sie besteht aus vielen Elementen und wenn nur eines davon versagt, droht der Zusammenbruch der Produktion. Lesen Sie, wie das kommt und was dagegen hilft.

Das Hauptmerkmal der Netzwerkbetreuung ist, dass man nie wirklich fertig ist: Ob in der Firma oder daheim, die Infrastruktur soll immer neue Anforderungen erfüllen. Gut, dass Ethernet auf Kupferkabeln Reserven bis 10 Gbit/s bietet. Abseits von den Hauptwegen helfen Ethernet-Ersatzmedien weiter.



Dušan Živadinović

Inhalt

FRITZBOXEN AUFRÜSTEN

Das runderneuerte FritzOS 7.50 kann sich sehen lassen: Fritzbox-Router erhalten damit kostenlos bessere VPN-Funktionen, die Smarthome-Geräte arbeiten endlich zusammen und die Telefonie wird komfortabler. Wir erklären die wesentlichen Neuerungen und zeigen, wie Sie die richtige Fritzbox finden.

8 FritzOS 7.50: Update für Fritzboxen
14 Die richtige Fritzbox für jeden Zweck
18 Fritzbox-VPN: Warum WireGuard cool ist

VERNETZEN MIT FUNK UND KABEL

So viele Herausforderungen die In-Haus-Vernetzung bergen mag: Fast immer bietet die Technik gute Lösungen. Wenn also Ethernet als Optimallösung ausscheidet, vernetzen Sie die letzten Winkel mit WLAN oder Ersatzmedien über Koax- oder Telefonleitungen – wir zeigen, wie.

26 Gigabit-Internet im Haus verteilen
30 Funknetzprobleme selbst lösen
36 Alternative Wege fürs Gigabit-Internet
44 Routersteuerung mit FlexiWAN

GLASFASERANSCHLUSS RICHTIG AUSWÄHLEN

Wird die Glasfaser zum DSL-Killer? Der Glasfaser-Zug rollt jedenfalls und lockt mit hohen Rabatten für Neuanschlüsse: Wir haben das Wichtigste über Ausbau, Tarife und Technik zusammengefasst.

50 Glasfaser-Internet: Ausbau, Tarife, Technik
52 Glasfaser-Internet: Ausbau & Tipps
58 Glasfasertarife für Privatkunden
64 Die Technik des Glasfaser-Internet
68 FAQ: Per Glasfaser ans Internet
72 Fritzbox 5590 für Glasfaser-Internet

SCHWACHSTELLEN IM NETZ FINDEN

Moderne Applikationen bestehen aus vielen Bausteinen und die Stabilität der Programme hängt von jedem einzelnen ab – damit aber auch die Produktion von Unternehmen. Mit speziellen Werkzeugen identifizieren Sie die Gefährder und wappnen sich so gegen Ausfälle.

74 Raus aus der Abhängigkeitshölle
76 Ein Framework unter der Lupe
82 Abhängigkeiten erkennen
88 Sicherheitsvorfälle in Logs aufspüren

ACTIVE DIRECTORY BEHERRSCHEN

Für Admins großer Windows-Netze ist Active Directory fast unverzichtbar. Hat man einmal die Richtlinien zusammengesteckt, tanzen alle PCs nach dem gleichen Rhythmus. Hier finden Sie Grundlagen zur Technik, Strategien zur Fernsteuerung und zur Absicherung gegen Ausfälle.

96 Das Active Directory im Windows-Netzwerk

104 Windows mit GPOs steuern

110 Redundante Domaincontroller

ZUM HEFT

3 Editorial

6 Aktion: heise-Academy-Kurs „Active Directory mit Windows Server 2019“

95 Impressum



6

AKTION
4:33 STUNDEN VIDEOKURS
MIT 100 % LESERRABATT

heise Academy

Active Directory mit Windows Server 2019

Lerne, wie man ein Active Directory mit Windows Server 2019 aufbaut und es an das Azure Active Directory anbindet. IT-Experte Tom Wechsler zeigt Schritt für Schritt alle Grundlagen in einem Online-Videokurs, der für die Käufer dieser Ausgabe kostenlos ist.

Im Active Directory können Objekte wie Computer, Benutzer und Gruppen zentral verwaltet sowie Zugriffe und Freigaben auf andere Ressourcen wie Fileserver im Unternehmen gesteuert werden.

In diesem Online-Videokurs führt IT-Trainer Tom Wechsler in dieses Thema ein und zeigt dir, wie du die Active Directory-Domänendienste unter Windows Server 2019 planen, implementieren und verwalten kannst. Dabei lernst du nicht nur, mit Benutzerkonten, Computerkonten, Gruppen und Organisationseinheiten zu arbeiten, sondern auch, wie du eine gesunde Active-Directory-Infrastruktur aufrechterhältst.

Im ersten Schritt wirst du Benutzer- und Computerkonten erstellen, diese in Gruppen und Organisationseinheiten organisieren und das Active Directory durch Passwort und differenzierte Kennwortrichtlinien sichern. Anschließend geht es darum, das Windows Active Directory an das Azure Active Directory anzubinden. Du lernst, welche Schritte dazu notwendig sind und welche Vorbereitungen getroffen werden müssen, damit diese Hybrid-Umgebung reibungslos funktioniert.

Dieser Kurs richtet sich an Personen, die den Aufbau und die Verwaltung einer Microsoft Domäne lernen oder ihr Wissen im Bereich Microsoft Active Directory vertiefen wollen. Wer darüber hinaus einen ersten Einblick in die PowerShell erhalten will, ist hier genau richtig.

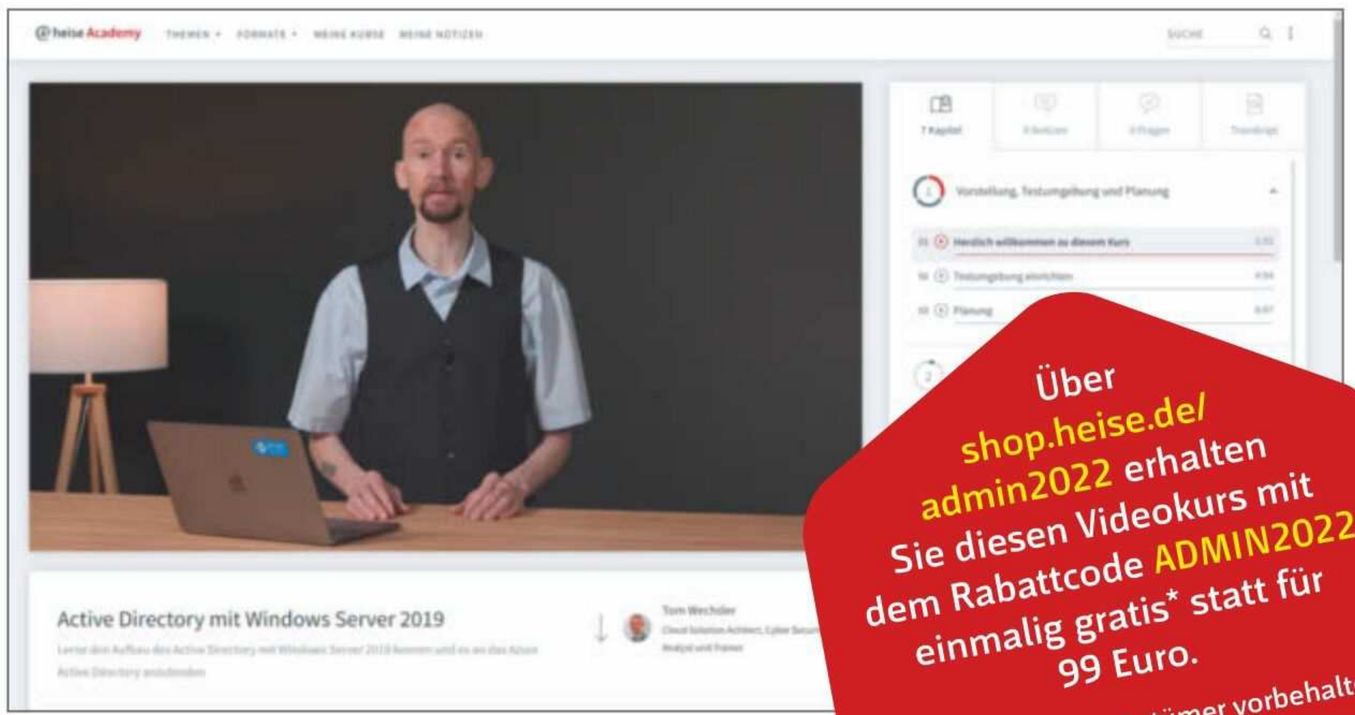
Um diesem Kurs gut folgen zu können, solltest du die Möglichkeit haben, eine virtuelle Testumgebung einzurichten. Darüber hinaus ist es hilfreich, wenn du grundlegendes Wissen zu Microsoft Betriebssystemen (Server und Client) und allgemeine Netzwerk-Kenntnisse mitbringst.

Tom Wechsler ist seit mehr als 20 Jahren professionell in der Informatikbranche tätig. Seit 2007 arbeitet er als selbstständiger Cloud Solution Architect, Cyber Security Analyst und Trainer. Seine Schwerpunkte liegen in den Bereichen Netzwerktechnik (Cisco), Microsoft Azure, Microsoft 365, Windows Server und Active Directory.

Lernen bei der heise Academy

In den Videokursen von heise Academy lernst du IT-Themen anschaulich und verständlich. In den Videos schaust du den Experten bei der praktischen Arbeit zu und lässt dir dabei alles genau erklären. Das Wissen ist in viele kleine Lernschritte und Aufgaben unterteilt – du kannst den Kurs Lektion für Lektion durcharbeiten oder gezielt zu Themen springen, die dich interessieren.

Die persönliche Lernumgebung der heise Academy unterstützt dich mit vielen Funktionen beim Lernen, die alle in einer Ansicht schnell und einfach zugänglich sind: Du siehst deinen Lernfortschritt, kannst Lesezeichen setzen, direkt im Video Notizen speichern oder mit der Volltextsuche in den Videos konkrete Informationen wiederfinden.



In sieben Kapiteln mit insgesamt 52 Video-Lektionen erlernen Sie an praktischen Beispielen den Umgang mit dem Active Directory.

Über shop.heise.de/admin2022 erhalten Sie diesen Videokurs mit dem Rabattcode ADMIN2022 einmalig gratis* statt für 99 Euro.

*Preis- und andere Irrtümer vorbehalten. Das Angebot ist gültig bis zum 31.07.2023 (Stand: November 2022).

Alle Video-Lektionen im Überblick:

1. Vorstellung, Testumgebung und Planung

- Herzlich willkommen zu diesem Kurs
- Testumgebung einrichten
- Planung

2. Aufbau einer Infrastruktur

- Intro
- DC01 und DC02
- Netzwerkeinstellungen anpassen
- DC01 zu einem Domain Controller heraufstufen
- Nachkonfiguration beim DC01
- DC02 zu einem Domain Controller heraufstufen
- Nachkonfiguration beim DC02
- DNS-Einstellungen beim DHCP Server prüfen
- FS01 und die beiden Clients
- Server Core App Compatibility Feature on Demand (FOD)
- Quiz: Aufbau der Infrastruktur

3. Actice Directory Terminology

- Intro
- Gesamtstruktur und Domäne
- Gesamtstruktur- und Domänenfunktionsebenen
- Betriebs-Master-Rollen
- Quiz: Active Directory Terminology

4. Aufbau des Active Directory

- Intro
- Planen der Organisationseinheiten
- Erstellen eines neuen Benutzers
- Das persönliche Laufwerk einrichten
- Das persönliche Laufwerk testen
- Gruppen erstellen
- Mit der PowerShell Benutzer erstellen
- Quiz: Aufbau des Active Directory

5. Verwaltungsaufgaben im Active Directory

- Intro
- Zentrale Ablage der Firmendaten mit zugriffsbasierter Aufzählung
- Kerberos-Delegierung
- Zuweisen der Objekt-verwaltung
- Ordnerkontingente einrichten
- Fine Grained Password Policy: differenzierte Kennwortrichtlinien
- Mit der PowerShell eine Fine Grained Password Policy einrichten
- Windows-Server-Sicherung
- Diagnostizieren von Active Directory-Replikationsfehlern
- Quiz: Verwaltungsaufgaben im Active Directory



6. Gruppenrichtlinien

- Intro
- Einführung in das Thema Gruppen-richtlinien
- Einen zentralen Speicher einrichten
- Freigabe der Firmendaten mittels Zuweisen von Gruppenrichtlinien
- Die lokalen Administratoren erweitern
- Energiesparmodus konfigurieren
- Quiz: Gruppenrichtlinien

7. Windows Active Directory und Azure Active Directory

- Intro
- Blick ins Azure Active Directory
- Azure AD Connect installieren
- Azure AD Connect konfigurieren
- Azure AD Connect prüfen
- Mit der PowerShell das UPN ersetzen
- Ein Tipp zum Schluss
- Fazit und Kursabschluss

FritzOS 7.50: Update für Fritzboxen

Alle paar Jahre bekommen AVMs Router gratis ein großes Firmware-Update, das die vielseitigen Geräte noch nützlicher macht. Über FritzOS 7.50 dürfen sich Fritzbox-Nutzer freuen: Es bringt mehr Wumms ins VPN, macht das Telefonieren komfortabler und das Smart Home schlauer. Hier schildern wir, was das frische FritzOS kann. In den folgenden Beiträgen gibt es Tipps für einen neuen Router und eine ausführliche Anleitung zu WireGuard auf Fritzboxen.

Von **Ernst Ahlers und Dušan Živadinović**

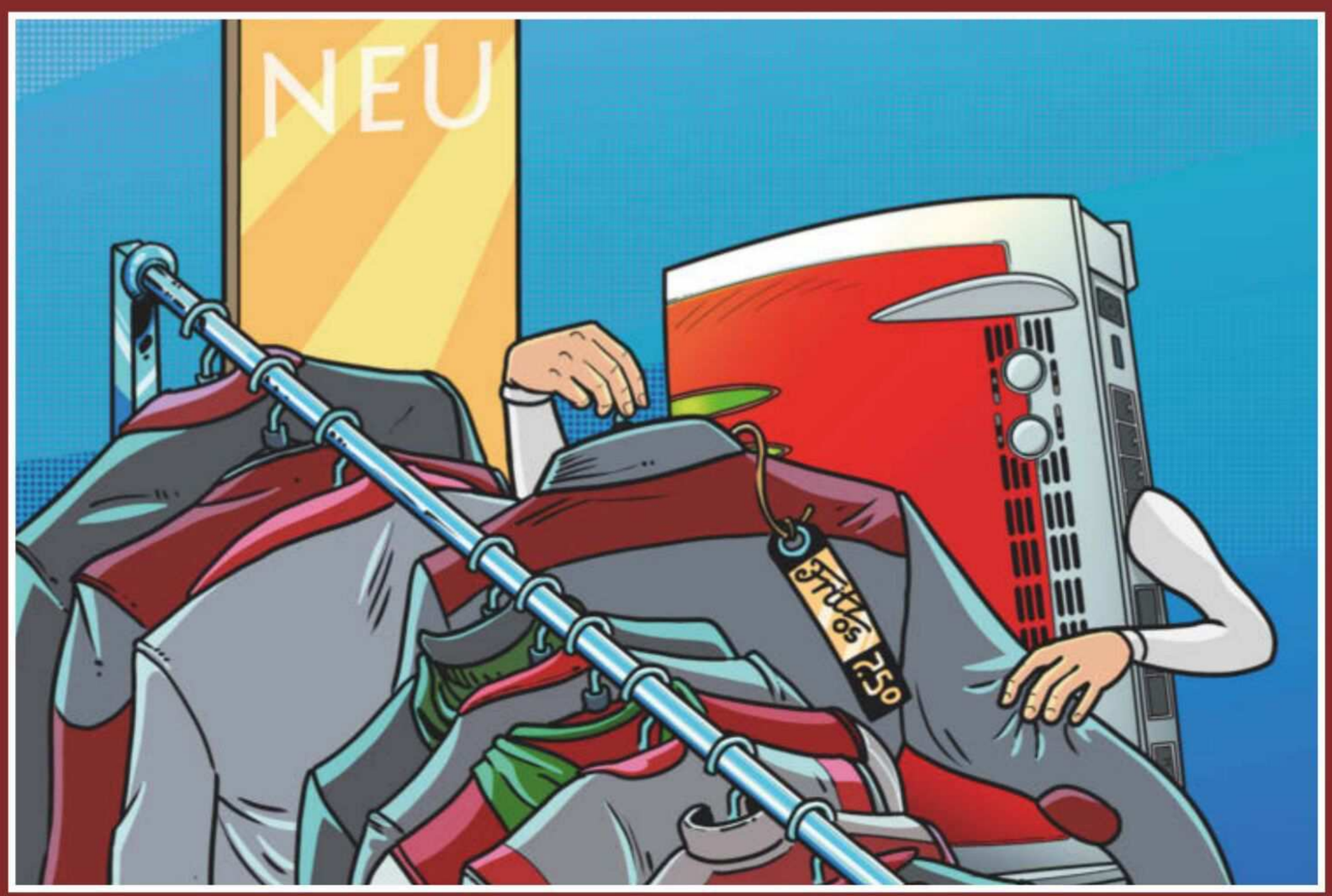


Bild: Michael Vogt

Die Neuerungen von FritzOS 7.50	8
Die richtige Fritzbox für jeden Zweck	14
Fritzbox-VPN: Warum WireGuard cool ist	18

Auf den ersten Blick unterscheidet sich FritzOS 7.50 wenig vom Vorgänger. AVM hat das Browsermenü dezent modernisiert. Es ist nun auf großen Bildschirmen besser lesbar. Falsche Klicks, durch die man Änderungen ungewollt verwirft, sollen dank geschickter angeordneten „Übernehmen“- beziehungsweise „Verwerfen“-Knöpfen nicht mehr vorkommen.

Die nützlichen Fortschritte stecken unter der Haube: Laut der Liesmich-Datei zur Beta-Firmware hatte AVM bis Ende September weit über hundert Funktionen verbessert und Fehler behoben. Dazu kommen 17 neue Funktionen und 27 Änderungen. Die wichtigsten haben wir uns vorab in der Beta-Version 7.39 angesehen.

Wie früher dürften die zurzeit vertriebenen Fritzboxen und WLAN-Repeater das neue Betriebssystem erhalten, vielleicht sogar auch noch einzelne ältere Modelle wie die verbreitete 7490. Ist Ihr Router nicht darunter, liefern wir ab Seite 14 Tipps, wie Sie eine passende neue Fritzbox für Ihren Anschluss finden.

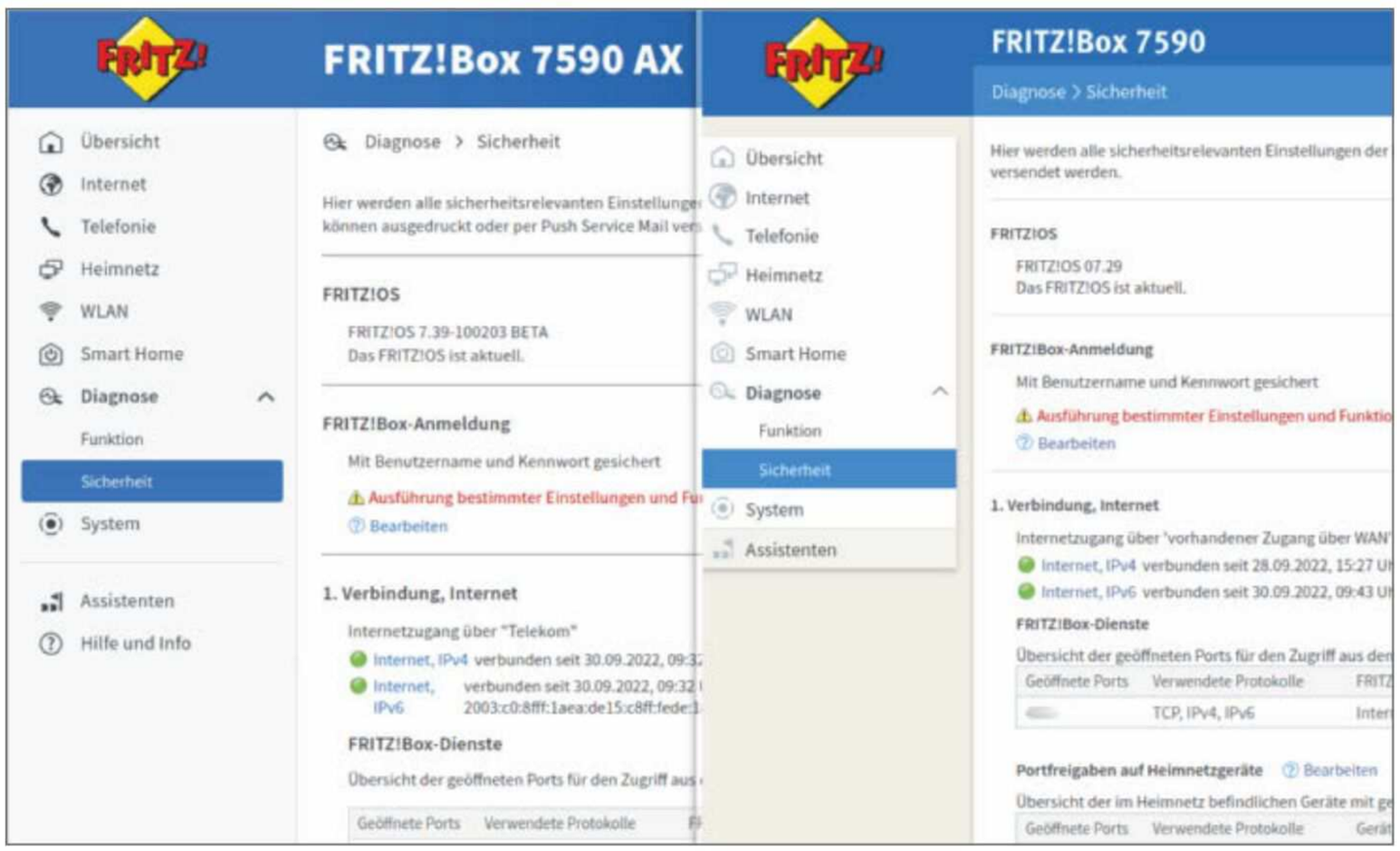
Mit einem virtuellen privaten Netz (VPN) kann man über eine verschlüsselte Verbindung beispielsweise aus der Ferne den Schwiegereltern Hilfestellung in ihrem Heimnetz geben. In Unternehmen verschaffen VPNs Heimarbeitern Zugriff auf Ressourcen im Firmennetz.

Hier steckt die größte Neuerung von FritzOS 7.50: WireGuard wird der moderne Kompagnon des alten IPsec-basierten Fritz-VPN. Ab Seite 18 beschreiben wir ausführlich, wie man WireGuard auf Fritzboxen einrichtet und verwendet. Als Beispiel dient ein VPN zwischen der Fritzbox als Zentrale und zwei Linux-Peers, einem Raspi mit Raspbian und einer Debian-VM auf einem NAS.

Deshalb folgt an dieser Stelle nur das Wichtigste zu WireGuard. Der VPN-Neuling hat sich in den letzten Jahren rasant ausgebreitet und er ist nach einigen Querelen in den Linux-Kernel eingezogen. So setzten die Admins des c’t-Mutterschiffs Heise Medien schon vor dem pandemiebedingten Homeoffice-Aufschwung darauf.

Bei WLAN-Routern war die Deutsche Telekom der hiesige WireGuard-Pionier: Schon im Frühjahr 2020 erschien in Speedport-Geräten die erste Umsetzung für einen einzigen Zugang. Inzwischen lassen sich fünf definieren, aber nach wie vor können Speedports WireGuard erstens nur alternativ zu IPsec nutzen und zweitens VPN-Tunnel nur über IPv4 als Trägerprotokoll aufbauen [1]. IPv6 soll Anfang 2023 dazu kommen.

Vielleicht hat das Telekom-Vorpreschen AVM dazu bewegt, WireGuard ebenfalls einzubauen. Das haben die Berliner dann gleich richtig angegangen, mit vielen möglichen Zugängen, parallelem Betrieb beider VPN-Typen und beiden IP-Varianten als Träger. Schon die erste FritzOS-7.39-Laborversion auf der Fritzbox 7590 Anfang 2022 überraschte uns [2]: Wir



Auf großen Bildschirmen sind die Fritzbox-Konfigurationsseiten mit FritzOS 7.50 (links) besser lesbar.

maßen seinerzeit mit WireGuard den doppelten VPN-Durchsatz (Down/Upstream-Mittelwert 146 Mbit/s) gegenüber IPsec (70 Mbit/s).

VPN mit Wumms

Je nach Verfügbarkeit nutzt AVM beim VPN fürs Ver- und Entschlüsseln nun Hardware-Kryptobeschleuniger oder Befehlssatzerweiterungen der Router-Prozessoren. Das hat den VPN-Durchsatz noch mal deutlich gesteigert.

Mit der Laborversion 7.39-100202 von Ende September maßen wir auf der 7590 gegenüber dem Jahresanfang jetzt satte 69 Prozent mehr WireGuard-Durchsatz (247 statt 146 Mbit/s). IPsec legte auf ihrem MIPS-Dualcore-Prozessor sogar um 80 Prozent zu (126 statt 70 Mbit/s).

Die Fritzbox 7520, eine Providervariante der 7530 mit ARM-Quadcore-Prozessor, kam mit 7.39-100201 bei WireGuard sogar auf 352 Mbit/s. Mit IPsec schaffte sie indes nur 107 Mbit/s. Wie die konkreten Durchsätze bei anderen Fritzboxen aussehen, wird sich zeigen.

Übrigens funktioniert IPsec, früher das alleinige Fritz-VPN, nun auch mit IPv6 als Träger. Damit können Nutzer, deren Internet-per-TV-Kabel- oder Glasfaseranschlüsse wegen DS-Lite oder CG-NAT keine öffentliche IPv4-Adresse haben, jetzt mit beiden VPN-Spielarten von außen ins Heimnetz gelangen.

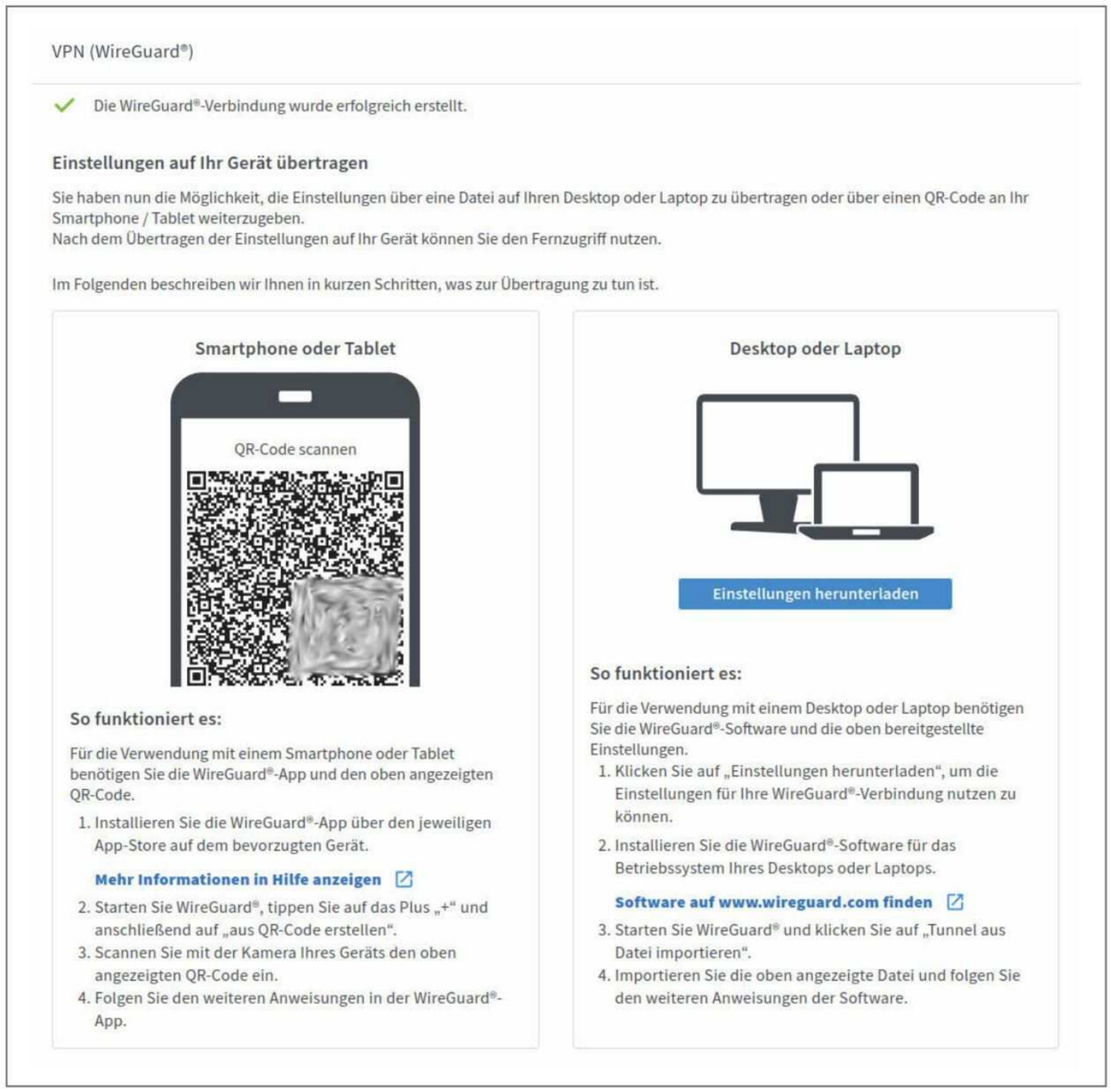
Dafür muss das Netz, in dem die Roadwarrior gerade unterwegs sind, IPv6 anbieten. Dieses immer wichtigere Protokoll aktivieren Fritzboxen beim Einrichten aller Internetzugangstypen nun endlich automatisch.

Falls Sie den Adressbereich fürs interne Netz ändern wollen, etwa von 192.168.178.1 auf 192.168.59.1, dann tun Sie das vor der VPN-Konfiguration. Denn das Ändern des Bereiches macht die VPN-Einstellungen hinfällig und Sie müssen von vorn anfangen.

Nützlich wäre noch, wenn sich die Info-Leuchte der Fritzboxen so konfigurieren ließe, dass sie auch „VPN-Tunnel aufgebaut“ signalisiert. Dann sähe man auch ohne Browser, ob gerade jemand von außen im Heimnetz ist.

Smarteres Smart Home

AVM hat im Laufe einiger Jahre eine Handvoll Smart-Home-Geräte auf der Basis der Schnurlostechnik DECT herausgebracht, sodass man etwa die Heizung, das Licht oder elektrische Verbraucher automatisch



Einfacher geht es kaum, einen VPN-Tunnel zur Fritzbox auf dem Smartphone zu erzeugen: QR-Code mit der WireGuard-App fotografieren, fertig.

steuern kann, etwa gemäß dem Wochenverlauf. Bisher führte jedes der Geräte weitgehend ein Eigenleben, ob Heizkörperthermostat (FritzDECT 301/302), intelligentes Leuchtmittel (FritzDECT 500) oder schaltbare Steckdose (FritzDECT 200/210).

Zwar kann man beispielsweise mehrere Thermostate zu einer Gruppe zusammenfassen und gemeinsam umschalten, aber die ganze Gruppe bekommt dieselben Absenk- und Komforttemperaturen. Das geht an der Praxis vorbei, wenn man etwa im Flur und Bad nur mäßig heizen möchte, im Arbeitszimmer aber 20 Grad haben und alle drei zu gleichen Zeitpunkten umschalten will.

Mit FritzOS 7.50 bleibt die Gruppenbindung erhalten, aber man kann mittels individueller Vorlagen, Szenarien und Routinen mehrere Geräte und auch Gruppen mit unterschiedlichen Temperaturen gemeinsam schalten. Dafür bieten sich die FritzDECT-Schalter 400 und 440 an. Wer eine fernschaltbare

Fritz-Steckdose hat, kann sich die Taster sparen und hat damit sogar mehr Optionen.

Sensor-Mehrwert

Denn mit den neuen Wenn/Dann-Regeln kann man den Schalttaster der Fritz-Steckdosen nun als Sensor für Smart-Home-Routinen nutzen. So kann ein Tipp darauf alle an einer Steckdosenleiste angeschlossenen Bürogeräte wie PC, Monitor und Drucker gemeinsam anwerfen und zusätzlich etwa Smart-Lampen ein- und Thermostaten umschalten. Das funktionierte in unserem Versuch tadellos und erleichtert das Familienleben, wenn man wie der Partner manches Fritzbox-Admins die unmittelbare Kontrolle bevorzugt.

Anders als bei den DECT-Tastern gibt es sogar eine visuelle Rückmeldung: Leuchtet die Schalt-LED, ist das Homeoffice in Betrieb, beleuchtet und beheizt. Ist sie aus, sind nicht nur die Homeoffice-Geräte vom Strom getrennt und die LED-Leuchte aus, sondern auch die Thermostate abgesenkt.

Die mit älteren FritzOS-Versionen eingebrachten Automatiken, etwa für Urlaubsabwesenheiten, kann man weiter nutzen und mit den neuen Routinen kombinieren. Der Fritzbox-Admin sollte sich für derartigen Komfortgewinn ein wenig Zeit zur Einarbeitung nehmen und vor Beginn der Konfiguration eine Tabelle mit sinnvollen Begriffen für Vorlagen, Szenarien und Routinen anfertigen. Das erleichtert die Übersicht und die spätere Erweiterung.

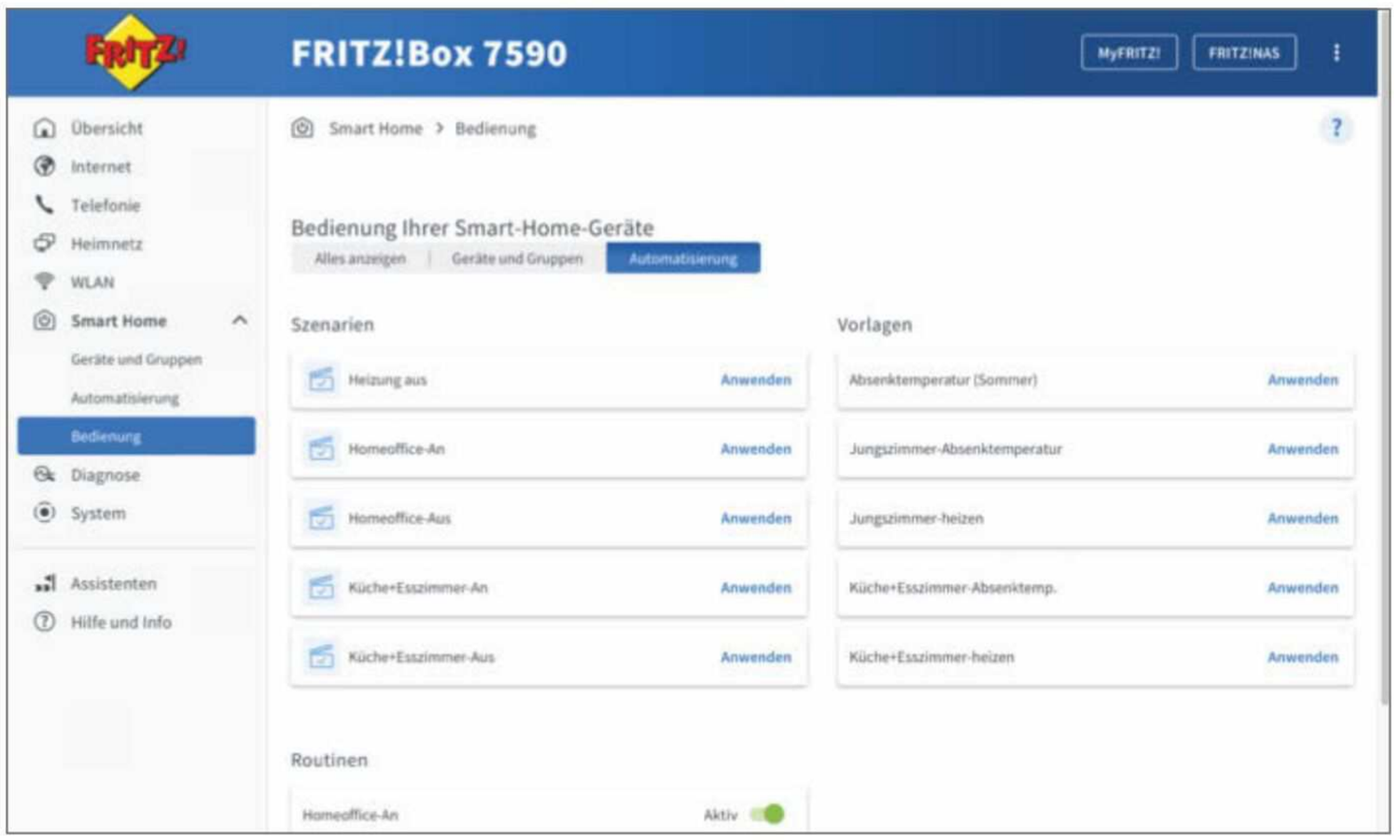
Praktisch auch: Der Browser bleibt mit der Fritzbox so lange verbunden, bis man nach üblicherweise 20 Minuten wegen Inaktivität automatisch abgemeldet wird. Währenddessen zeigt er an, wenn sich Betriebszustände ändern, etwa eine per Smartphone-App ausgeschaltete Steckdose oder die Temperatursteuerung.

Anruferansage

Mit dem neuen „Sprachklingeln“ lernen AVM-Schnurlostelefone, Anrufer statt eines Düdelüt mit ihren im Telefonbuch hinterlegten Namen zu melden. Bei unterdrückter Rufnummer hört man „Anruf von Unbekannt“. Die Funktion steckt im Menü bei „Telefoniegeräte“. Über den „Bearbeiten“-Stift kommt man zum „Klingeltöne“-Reiter eines an die Box gekoppelten DECT-Telefons.

Das Sprachklingeln lauert weit unten in den Ausklappern für die zugewiesenen Rufnummern. Die Wahl zwischen männlicher oder weiblicher Stimme sowie der optional einschaltbare Zusatzklingelton gelten immer für alle Telefone. Einen akustischen Hinweis auf unterschiedliche Rufnummern (Privat, Mobil, Geschäftlich) eines Eintrags gibt es nicht, diese Information erscheint wie vorher nur im Display.

Zurzeit funktioniert das Sprachklingeln nur bei aktiviertem MyFritz-Konto. AVMs verlinkte Datenschutzerklärung verrät, dass die Fritzbox noch nicht zu lokal gespeicherten Soundschnipseln konvertierte Namen mittels eines AVM-Clouddienstes übersetzt.



Das Smart Home wird mit Wenn/Dann-Regeln schlauer. Damit kann man nun beispielsweise den Taster von Schaltsteckdosen verwenden, um mehrere Stromverbraucher gleichzeitig einzuschalten und die Temperatur einer Gruppe von Thermostaten umzuschalten.

Die Box soll dabei nur die zu wandelnde Zeichenkette übermitteln. Kennt der AVM-Dienst diese nicht, fragt er beim Amazon-Dienst Polly an.

Positiv durchgelassen

Weiterleitungen und Rufsperren für ankommende Anrufe kann man nun auf eine einzelne eigene Rufnummer beschränken. Mit dem neuen Rufnummernbereich „Nicht im Telefonbuch“ weist die Box unbekannte Anrufer generell ab und leitet ihre Anrufe nicht weiter. So wird das Telefonbuch zu einer Positivliste für erwünschte Kontakte.

Mit der neuen Firmware bekommen AVM-Telefone einen Terminkalender dazu. Einträge erzeugt man übers Telefonmenü bei den „Komfortdiensten“. Komfortabler ginge das Befüllen des Kalenders freilich per Browser übers Fritzbox-Menü. Die Krönung wäre das Synchronisieren mit Smartphones und externen Diensten über das CalDAV-Protokoll. AVM will das in kommenden FritzOS-Updates nachliefern.

Termine wie auch Weckrufe sagen die Fritz-Fons auf Wunsch ebenfalls an. Kurzwahlen für die Tasten 2 bis 9 lassen sich am Telefon jetzt per langem Drücken anlegen.

Mobilfunk-Bonbons

Fritzboxen können schon länger Mobilfunksticks per Failover/Fallback als zweiten Internetzugang nutzen, um Ausfälle des Hauptanschlusses (DSL, TV-Kabel etc.) zu überbrücken. Das klappte nun erstmals auch über den USB-C-Port eines 5G-Mobilfunkrouters, in unserem Versuch ein Zyxel NR2101.

Zwar hat dieser Router auch einen Gigabit-Ethernet-Port, sodass man ihn an den WAN-Port einer Fritzbox hängen könnte. Aber USB ist praktischer, weil der Mobilrouter darüber auch Strom bekommt und man so kein zusätzliches Netzteilchen in die überfüllte Steckerleiste zwängen muss.

Fritzboxen mit eingebautem Mobilfunkmodem können jetzt eine der SIM-Karte zugeordnete Rufnummer in die Fritzbox-Telefonie einbinden. Auf einer 6850 5G war der Vorgang mit drei simplen Klicks erledigt. Dazu muss der zur Karte gehörende Tarif aber Telefonie über VoLTE enthalten.

Geschmeidiger vernetzt

Einige interessante Erweiterungen stecken unter der Haube. So sendet die Fritzbox jetzt mehrere Bonjour-Annoncen, mit denen sie ihre Dienste im internen Netz ankündigt. Das können Fritz-Apps nutzen, um die Fritzbox schnell zu finden.



Fritzboxen kündigen ab FritzOS 7.50 Dateifreigaben auch per mDNS an. Die finden macOS- und Linux-Systeme ebenso wie Windows 11 automatisch und bieten sie in der Netzwerkübersicht zum Einbinden an.

Nicht nur Windows, sondern jetzt auch Linux- und macOS-Anwender sehen in der Netzwerkübersicht automatisch die Fritzbox-Angebote und können mit einem Klick auf NAS-Inhalte und das Webinterface zugreifen, ohne den Hostnamen oder die IP-Adresse des Routers kennen zu müssen.

Ferner annonciert die Fritzbox Dienste, die für Programmierer interessant sein dürften, darunter den für Skript-Projekte genutzten TR-064-Port (http://fritz.box:49000/tr64desc.xml).

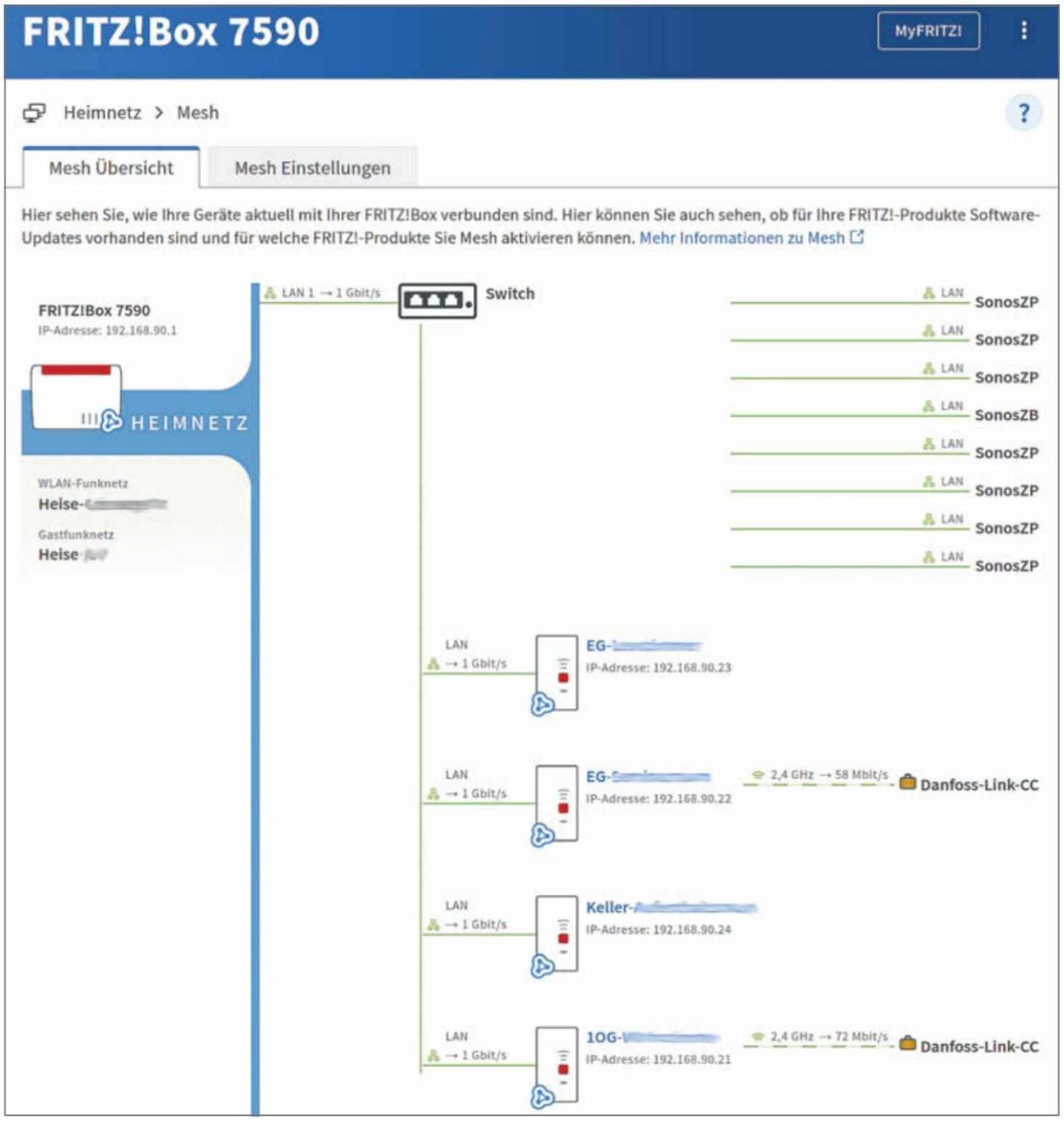
Die veraltete Provider-Fernwartung gemäß TR-069 hat AVM durch die flexiblere und abwärtskompatible Variante TR-369 ersetzt. So muss man sich jetzt nicht mehr per Browser direkt auf der Fritzbox anmelden, sondern kann über den MyFritz-Dienst aus der Ferne Statusinformationen der Box – etwa Verbindungs- und Anschlussparameter – auslesen oder Firmware-Updates anstoßen.

Netz-Feinschliff

Bei einigen Fritzbox-Modellen – zum Redaktionsschluss 7590, 7590 AX, 7530, 7530 AX, 7520, 7510 – führt AVM eine automatische Priorisierung im internen Netz und im Gastnetz ein. Die Funktion soll die verfügbare Internetbandbreite fairer verteilen. Diese und die schon vorher mögliche Priorisierung einzelner Netzwerkgeräte wirkt nun auch auf IPv6-Verkehr.

Im 5-GHz-Band stört oft ein erzwungener Kanalwechsel. Er führt zu einer kurzen WLAN-Unterbrechung, wenn die Fritzbox Radarsignale erkennt. Dann wechseln viele Clients auf das 2,4-GHz-Band,

In der Mesh-Übersicht zeigt FritzOS auch Switches an. Hier hat es einen solchen aber mit den Koax/Ethernet-Adaptern fürs Weiterleiten des LANs übers TV-Kabelnetz verwechselt.



Literatur

[1] Ernst Ahlers, **Faser-Spezi**, Telekom-Router Speedport Smart 4 Plus für Glasfaser-Internet getestet, c't 22/2022, S. 72

[2] Ernst Ahlers, **VPN-Turbo**, WireGuard verdoppelt VPN-Geschwindigkeit bei Fritzbox 7590, c't 4/2022, S. 35

wo der Verkehr wegen frequenzmäßig schmalerer Signale und mehr Nachbar-Konkurrenz deutlich langsamer fließt. Das optimiert AVM nun bei mehr Boxen mit Zero-Wait-DFS. Nach dem Erkennen eines Radarpulses wechselt der Router vorübergehend auf die 5-GHz-Kanäle 36 bis 48, sucht im Hintergrund nach radarfreien Frequenzen und geht dann auf höhere, schwächer belegte Kanäle.

Fritzboxen können schon länger als Mesh-Repeater arbeiten, um die WLAN-Abdeckung des Routers am Internetanschluss zu vergrößern. Als Mesh-Repeater halten sie die Verbindung zur Zentrale aber nur in einem WLAN-Band. Zuerst lernt die 7590 mit der neuen Firmware, dynamisch beide Funkbänder zu nutzen. Das soll die Mesh-Performance optimieren.

Fazit

Das neue FritzOS zeigt sich teils schneller und in der Bedienung geschmeidiger als zuvor. Dazu tragen auch Details wie Bonjour-Annoncen oder TR-369 sowie die Verbesserungen bei Telefonie und Smart-Home bei. Neben den Arbeiten am modernen VPN-Neuling WireGuard hat AVM das alte Fritz-VPN nicht vernachlässigt. Es bekam einen Leistungsschub und hat gelernt, auch IPv6 als Tunnel-Transporter zu nutzen.

So demonstriert AVM mit FritzOS 7.50 erneut, dass Produktpflege mehr bedeuten kann, als nur eine kurze Zeit lang bestenfalls gravierende Fehler auszubügeln. Davon dürfen sich andere Routerhersteller gern anregen lassen. (ea) c't



Bild: Michael Vogt

Die richtige Fritzbox für jeden Zweck

Wenn ein neuer Router her muss, liegt der Griff zu einer Fritzbox nahe. Die Marke glänzt seit Langem mit vielen Funktionen und stabilem Betrieb. Doch AVMs Produktpalette ist inzwischen schwer überschaubar. Wir schlagen eine Schneise durch den Boxen-Dschungel.

Von **Ernst Ahlers**

Gründe für einen neuen Router gibt es viele: Der alte fällt aus, der Wechsel zu einem attraktiveren Internetangebot mit anderem Leitungstyp steht an oder der aktuelle Internetverteiler hat Macken in seiner Firmware, die neuen Wünschen im Weg stehen – IPv6 lässt grüßen. Dann locken Fritzboxen mit ihren ausgefeilten Funktionen und der bekannt langen Produktpflege.

Die Router berlinischer Herkunft sind zu Recht keine Sonderangebote, was sich auch an hohen Preisen im Gebrauchtmarkt zeigt. Doch erwägen Sie gründlich, ob beim Routerwechsel eine Fritzbox aus zweiter Hand genügt.

Zwar arbeiten die Geräte oft jahrelang stabil. So läuft eine 2013 erworbene Fritzbox 7360 seit einigen Jahren bei den Schwiegereltern mit sehr wenigen

Neustarts. Beim Schreiben dieses Artikels war der Router ein halbes Jahr durchgehend online.

Gebrauchtboxen fallen aber früher aus dem Hersteller-Support heraus als Neugeräte. Sie bekommen hernach nur ausnahmsweise Firmware-Updates, die dann allenfalls kritische Lücken stopfen [1], aber keine neuen Funktionen wie die ab Seite 8 geschilderten mitbringen.

Ältere Boxen nutzen tendenziell auch ältere WLAN-Technik, weshalb sie sehr schnelle Internetanschlüsse bestenfalls ansatzweise ausschöpfen (siehe S. 50). Und wenn der Router im Zweitjob mit einem USB-Massenspeicher als zentraler Datentümpel der Familie fungiert, nervt ein veralteter USB-Port mit gemächlichen 480 Mbit/s beim Speichern großer Dateien übers LAN ungemein.

Wer sich für einen neuen Router entscheidet, steht bei AVM vor einer großen Palette. Aktuell listet die Website 17 Modelle. Wir haben die nützlichsten zehn herausgesucht und ihre wichtigsten Eigenschaften in der Tabelle zum leichteren Vergleich versammelt.

Das wichtigste Auswahlmerkmal ist die Art Ihres (neuen) Internetanschlusses: Telefonleitung (DSL), TV-Kabel (DOCSIS), Mobilfunk (LTE/5G), Glasfaser oder Ethernet. Fritzboxen der letzteren Kategorie kann man über ein separates Modem an beliebigen Anschlüssen verwenden oder kaskadiert zu verschiedenen Netzwerkzonen. Das wird beispielsweise in Wohngemeinschaften hilfreich, wo sich mehrere Leute einen Internetanschluss teilen, aber separate (W)LANs haben möchten.

Ein zusätzlicher WAN-Port kann an einem zweiten Internetanschluss beim Ausfall der Hauptverbindung als Failover dienen. Das ist für kleine Firmen und Selbstständige nützlich, die auf den Zugang zum Internet angewiesen sind. Alternativ können sie einen USB-Mobilfunk-Stick oder einen Mobilfunkrouter mit USB-Anschluss an Fritzboxen als Notnagel betreiben. Das Modell 6890 LTE beherrscht den Failover mit ihren DSL- und LTE-Modems ab Werk.

Die Glasfaser-Fritzboxen 5530 und 5590 liefert AVM mit zwei SFP-Steckmodulen für unterschiedliche Anschlusstypen aus. Das für Active Optical Network (AON) arbeitet mit 1 Gbit/s in beide Richtungen. Jenes für Gigabit Passive Optical Network (GPON) überträgt 2,5 Gbit/s im Downstream (Internet ins Haus) und 1,25 Gbit/s im Upstream. Die Boxen haben indes einen SFP+-Slot, der auch Module für 10 Gbit/s aufnimmt, was zur sehr hohen Internetdatenrate in der Tabelle führt.

WLAN-Wahl

Ein neuer Router sollte heute nach dem aktuellen WLAN-Standard Wi-Fi 6 alias IEEE 802.11ax in beiden wichtigen Frequenzbändern 2,4 und 5 GHz funken,



Zehn Router für fünf Internet-Anschlusstypen (paarweise von links nach rechts, vorn zuerst): Fritzbox 7530AX und 7590AX für DSL, 6660 und 6690 für TV-Kabel, 6850 5G und 6890 LTE für Mobilfunk, 5530 und 5590 für Glasfaser, 4040 und 4060 für Ethernet. Bis auf die Mobilfunkrouter und das Ethernet-Modell 4040 im rot-silbernen Kleid funken alle mit dem modernen Wi-Fi 6.

was erfreulicherweise die meisten der gelisteten Modelle tun. Das seit Sommer 2021 erlaubte 6-GHz-Band spielt noch keine große Rolle: Wi-Fi-6E-Clients sind noch rar und eine größere Auswahl an Produkten für den nächsten WLAN-Standard Wi-Fi 7 wird es wohl frühestens 2024 geben.

Wi-Fi 6 bringt besonders in dicht besetzten Gegenden mit vielen konkurrierenden Netzen mehr Durchsatz und stabilere Verbindungen als die älteren Standards [2]. Bei den Mobilfunk-Boxen ist das schon 10 Jahre alte Wi-Fi 5 (11ac) noch akzeptabel. Denn LTE und auch 5G liefern im Alltag oft nur einige dutzend Mbit/s an, allenfalls ausnahmsweise mal wenige hundert Mbit/s oder mehr.

Die Anzahl der MIMO-Streams entspricht der Zahl der verwendeten Antennen [3]. Sie bestimmt neben dem verwendeten Standard und der Funksignalbreite über die maximal erreichbare Datenrate. Mehr ist besser, aber dann braucht auch die Gegenseite mehr. Notebooks, Tablets und Smartphones funken heute jedoch bestenfalls über zwei WLAN-Antennen.

Dennoch sind Router mit drei oder vier MIMO-Streams die geschicktere, wenn auch teurere Wahl. Sie eignen sich besser, um mit passenden Repeatern ein Mesh-WLAN aufzubauen, das größere Wohnungen lückenlos abdeckt. Außerdem können sie mit der WLAN-Funktion Multi-User-MIMO (MU-MIMO) Daten an mehrere Clients gleichzeitig schicken. Das steigert den Summendurchsatz in der Funkzelle, was allen nützt, auch wenn dieser Fall in der Praxis eher selten eintritt.

Schnelleres LAN

Lange Zeit war Ethernet mit 1 Gbit/s (Gigabit-Ethernet, GE) die Standardtechnik fürs lokale Netz. Die damit möglichen 115 MByte/s beim Übertragen großer Dateien liegen heute aber weit hinter der Maximalgeschwindigkeit von Festplatten (über 200 MByte/s) und erst recht SSDs (550 MByte/s bei SATA und bis 7500 MByte/s bei NVMe).

Deshalb breitet sich Multigigabit-Ethernet in PCs, Netzwerkspeichern (NAS) und eben auch Routern immer weiter aus [4], jedoch derzeit nur in der kleinsten Evolutionsstufe mit 2,5 Gbit/s (230 MByte/s). Der zugehörige NBase-T-Standard (IEEE 802.3bz) definiert indes auch 5 Gbit/s und 10 Gbit/s.

Soll der neue Router nur das Internet mit höchstens 1000 Mbit/s ins Haus holen, dann genügt GE weiterhin. Wer absehbar einen schnelleren Anschluss buchen will, der profitiert von den Fritzboxen mit 2,5-Gbit/s-Ports. Selbstständige, die dauernd riesige Dateien wie Images virtueller Maschinen im LAN hin

Aktuelle Fritzboxen für fünf Anschlusstypen

Modell	Internet-Typ	Maximale Datenrate	WAN-Port	WLAN 2,4 GHz	MIMO-Streams	Maximale Bruttorate	WLAN 5 GHz	MIMO-Streams	Maximale Bruttorate	LAN-Ports[1]	davon 2,5 Gbit/s	USB-Ports	DECT-Basis
7530 AX	DSL	300 Mbit/s	–	Wi-Fi 6 (11ax)	2	600 Mbit/s	Wi-Fi 6 (11ax)	3	1800 Mbit/s	4	–	1 × 480 Mbit/s	✓
7590 AX	DSL	300 Mbit/s	1 Gbit/s	Wi-Fi 6 (11ax)	4	1200 Mbit/s	Wi-Fi 6 (11ax)	4	2400 Mbit/s	4	–	2 × 5 Gbit/s	✓
6660	TV-Kabel	6000 Mbit/s	–	Wi-Fi 6 (11ax)	2	600 Mbit/s	Wi-Fi 6 (11ax)	2	2400 Mbit/s	5	1	1 × 480 Mbit/s	✓
6690	TV-Kabel	6000 Mbit/s	–	Wi-Fi 6 (11ax)	4	1200 Mbit/s	Wi-Fi 6 (11ax)	4	4800 Mbit/s	4	1	2 × 5 Gbit/s	✓
6850 5G	Mobilfunk	1300 Mbit/s	–	Wi-Fi 5 (11ac)	2	400 Mbit/s	Wi-Fi 5 (11ac)	2	867 Mbit/s	4	–	1 × 5 Gbit/s	✓
6890 LTE	Mobilfunk + DSL	300 + 300 Mbit/s	1 Gbit/s	Wi-Fi 5 (11ac)	4	800 Mbit/s	Wi-Fi 5 (11ac)	4	1733 Mbit/s	4	–	1 × 5 Gbit/s	✓
5530	Glasfaser	10.000 Mbit/s[2]	–	Wi-Fi 6 (11ax)	2	600 Mbit/s	Wi-Fi 6 (11ax)	2	2400 Mbit/s	3	1	–	✓
5590	Glasfaser	10.000 Mbit/s[2]	2,5 Gbit/s[3]	Wi-Fi 6 (11ax)	4	1200 Mbit/s	Wi-Fi 6 (11ax)	4	2400 Mbit/s	4[3]	–[3]	2 × 5 Gbit/s	✓
4040	Ethernet	1000 Mbit/s	–	Wi-Fi 5 (11ac)	2	400 Mbit/s	Wi-Fi 5 (11ac)	2	867 Mbit/s	4	–	1 × 5 Gbit/s, 1 × 480 Mbit/s	–
4060	Ethernet	2500 Mbit/s	–	Wi-Fi 6 (11ax)	4	1200 Mbit/s	2 × Wi-Fi 6 (11ax)	2 × 4	2 × 2400 Mbit/s	3	–	1 × 5 Gbit/s	✓

[1] ein LAN-Port zu WAN umkonfigurierbar [2] Maximum mit passenden Optikmodulen, siehe Text [3] WAN-Port zu LAN wandelbar

und her schieben oder auf dem NAS lagernde Videos bearbeiten, schaffen sich mit separaten NBase-T-Switches die passende Infrastruktur.

Wenn dereinst ein Internet-Upgrade auf 10 Gbit/s ansteht, die auch im (W)LAN ankommen sollen, dann genügt keine heute erhältliche Fritzbox. Denn mehr als 2,5 Gbit/s kann aktuell keine an einen einzelnen Host weiterreichen.

Extras

Die oben erwähnten USB-Ports mit 5 Gbit/s, früher als USB 3.0 bezeichnet, heute USB 3.2 Gen 1, haben gegenüber der langsameren Variante (USB 2.0) einen weiteren Vorteil. Sie liefern mehr Strom (0,9 statt 0,5 Ampere) und eignen sich deshalb besser für stromhungrige USB-Geräte, etwa jene ebenfalls erwähnten Mobilfunksticks als Reserve-Internetzugang und USB-Festplatten.

Ein zweiter USB-Port erlaubt, parallel zu solchen Devices auch einen Drucker im Netz zu teilen, falls der nicht selbst WLAN hat. Über die Fritzbox-Funktion „USB-Fernanschluss“ kann man schließlich auch andere Geräteklassen wie beispielsweise Scanner zentral bereitstellen.

Klassischerweise haben Fritzboxen als All-in-one-Router eine Basis für DECT-Funk, über die sie Schnurlostelefone anbinden. Wer nicht übers Festnetz telefoniert, kann darauf verzichten. Soll die Fritzbox aber über DECT-ULE (Ultra Low Energy) Smart-Home-Gadgets wie Lampen, Schaltsteckdosen oder Thermostate steuern, dann fallen Modelle ohne DECT-Basis heraus.

Ein ISDN-S0-Port etwa für alte Telefonanlagen ist heute eine Seltenheit: Aus unserer Auswahl haben lediglich eine der in zwei Ausführungen erhältlichen Fritzbox 7590 AX und die 6890 LTE den Oldie noch.

Fazit

Mit seinem Produktportfolio ist AVM überwiegend auf der Höhe der Zeit. Es gibt Router für alle wesentlichen Internet-Anschlusstypen, und die meisten Fritzboxen funken mit dem modernen Wi-Fi 6. Wi-Fi 6E im 6-GHz-Band spielt weltweit noch keine große Rolle. Daher würde es nicht verwundern, wenn die Berliner diesen Schritt auslassen und gleich auf das kommende Wi-Fi 7 gehen.

Wer jetzt eine neue Fritzbox sucht, wird mit etwas Umsicht das optimale Modell finden, das mindestens für die nächsten fünf Jahre gut ist. Währenddessen kommen gewiss einige nützliche Firmware-Updates und es gibt modernisierte Geräte, wenn der nächste Routerwechsel ansteht. (ea) c't

Literatur

[1] Ernst Ahlers, Ronald Eikenberg, **Jetzt updaten!**, Router-Lücke gefährdet viele Fritzbox-Nutzer, c't 6/2014, S. 39

[2] Dr. Guido R. Hiertz, Dr. Sebastian Max, **Volle Packung**, Wie die Verbesserungen von Wi-Fi 6 wirken, c't 3/2020, S. 112

[3] Ernst Ahlers, **WLAN: Häufige Fragen und Antworten**, c't 11/2021, S. 178, auch: ct.de/-6033808

[4] Ernst Ahlers, **LAN extraflott**, Multigigabit-Ethernet für mehr Netzwerkdurchsatz, c't 16/2020, S. 52



Auch als Heft + PDF mit 29 % Rabatt

Komplett auf 32 GByte USB-Stick. Desinfec't startet direkt vom Stick.

Ihr Erste-Hilfe-Set:

Das Notfall-System für den Ernstfall

Heft für 14,90 € • PDF für 12,99 €
• Bundle Heft + PDF 19,90 € Desinfec't-Stick 19,90 €

shop.heise.de/desinfect22

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

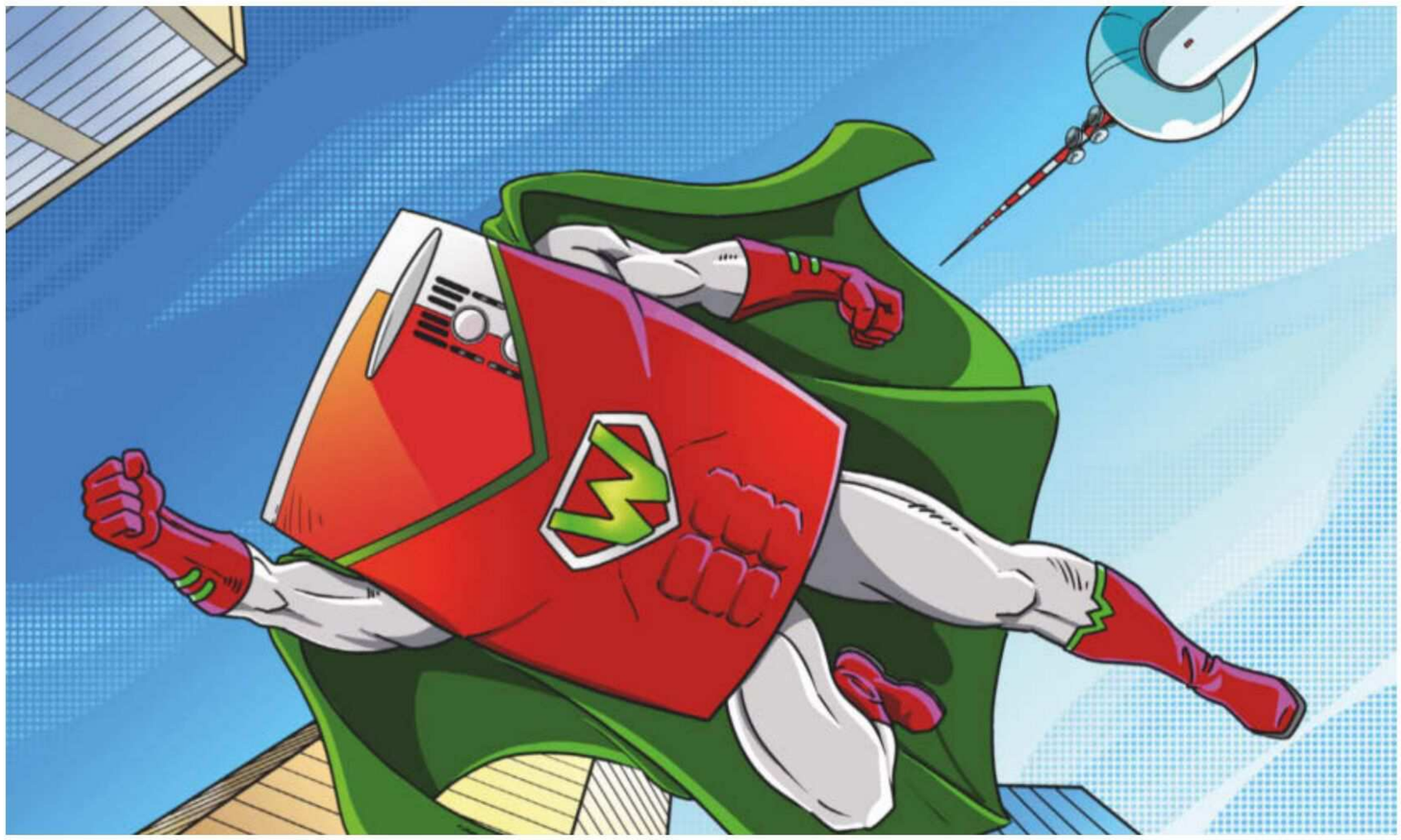


Bild: Michael Vogt

Fritzbox-VPN: Warum WireGuard cool ist

Für viele Fritzbox-Admins dürfte das kommende FritzOS-Update auf Version 7.50 einen kleinen Traum erfüllen: Es bringt die schnelle und zugleich komfortable VPN-Technik WireGuard mit. Das erleichtert den Homeoffice-Betrieb, Fernwartungen und Filialkopplungen. Was WireGuard auf Fritzboxen leistet, wie man es konfiguriert, wo die Grenzen liegen – wir gehen auf alles detailliert ein.

Von **Dušan Živadinović**

Gemessen daran, dass Router die meiste Zeit des Tages nur die Verbindung zum Internet halten, nutzt man deren VPN-Funktionen zwar selten. Aber sobald Zugriffe auf Netzwerkgeräte und Daten in der Ferne erforderlich sind, erweisen sie sich als wertvoll. Das liegt auch an der Verbreitung von Homeoffice-Arbeitsplätzen: VPN-Tunnel ersparen Fahrten, wenn man auf dem Heim-PC vergessene Dateien in die Firma holen will. Und der Familien-Admin muss seinen Regiesessel gar nicht erst verlassen, wenn er Onkel Hotte beim Konfigurieren des neuen NAS unter die Arme greift.

Für diese und ähnliche Anwendungen gibt es auch andere Methoden, darunter etwa die Fernwartung per TeamViewer oder FaceTime-Freigabe. Aber die Vertrauenswürdigkeit solcher Alternativen ist oft

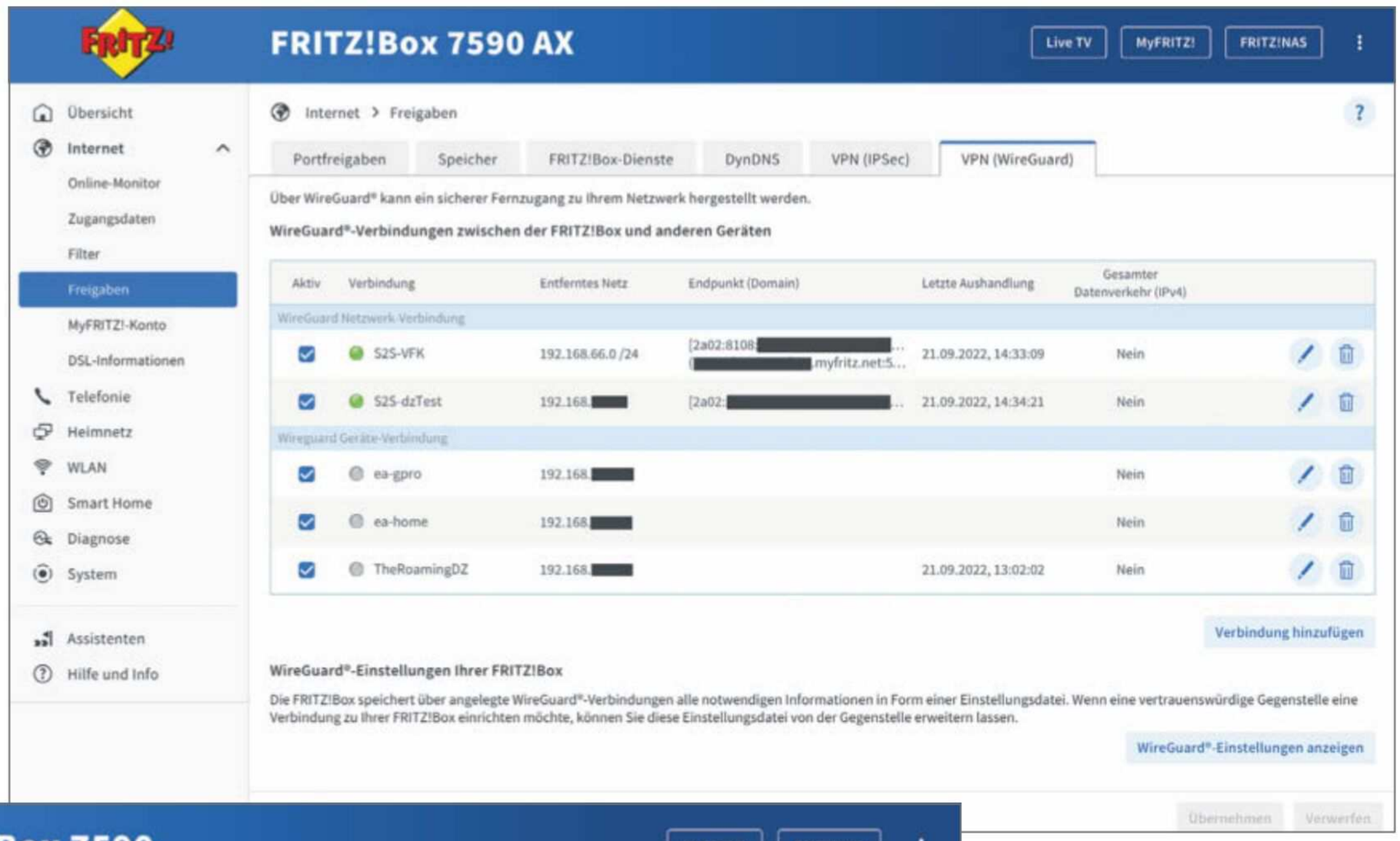
unklar, ebenso wie die Anfälligkeit gegenüber Attacken [1]. Demgegenüber sind etablierte VPNs quelloffen und können somit von Fachleuten leicht auf Herz und Nieren geprüft werden.

Die Fritzboxen sind in dieser Hinsicht auf den ersten Blick gut aufgestellt: Das seit Jahren angebotene IPsec-VPN gilt unter Spezialisten als sicher. Aber die Konfiguration ist umständlich und der Datendurchsatz auf Fritzboxen bestenfalls gemächlich – zwei Schwächen für ein Handicap in VPN-Gestalt.

Deshalb wird WireGuard den Fritzboxen guttun. Anders als bei IPsec muss man für die Konfiguration von Clients keine wirren Zeichenketten abtippen (fehlerträchtig) und WireGuard ist auf Fritzboxen rund doppelt so schnell wie IPsec. Auch baut WireGuard VPN-Tunnel wahlweise über das moderne IPv6 oder über das veraltete IPv4 auf. Wer eine Fritzbox an einem DS-Lite-Anschluss betreibt, braucht für das entfernte Tunnelende IPv6. Falls IPv6 am entfernten Ende fehlt, können Sie es hilfsweise mit einem Raspi als Router nachrüsten [2].

Smartphones und PCs anbinden

Die meisten Anwender bauen sich ein VPN in Sterntopologie auf, wobei ein oder mehrere Geräte



Fritzboxen können ab FritzOS 7.50 endlich VPN-Tunnel mittels der WireGuard-Technik aufbauen. Dabei kann man sowohl Netze koppeln (Site-to-Site, obere zwei Einträge), als auch Clients in einer Sterntopologie anbinden (untere drei Einträge).



Um eine LAN-zu-LAN-Kopplung aufzusetzen, muss man nur wenige Fragen beantworten. Kleine Tricks vorausgesetzt, kann man die fertigen Konfigurationsdateien auch auf Linux-Systemen verwenden und so WireGuard hinter Routern aufsetzen, denen die moderne VPN-Technik fehlt.



Auch die Routing-Konfiguration setzt die Fritzbox in Normalfall automatisch korrekt, man muss ihr dafür nur das Subnetz nebst Netzmaske des entfernten Routers nennen.

(Smartphone, Laptop …) eigene Tunnel zu einer Fritzbox aufsetzen. Wie man das mit WireGuard macht, erklären wir hier in vier Schritten (siehe auch [3]).

Doch bevor Sie loslegen, klären Sie, ob Sie auch LAN-zu-LAN-Kopplungen aufsetzen wollen. Falls ja, dann müssen beide Netzwerke verschiedene Subnetze nutzen (z. B. 192.168.178.0/24 und 192.168.59.0/24). Andernfalls funktioniert das Routing nicht. Das Subnetz der Fritzbox sollte man aber vor der VPN-Einrichtung ändern, weil diese Einstellungen nach Ändern des Subnetzes hinfällig sind und neu gemacht werden müssen. Weitere Einzelheiten zu LAN-zu-LAN-Kopplungen finden Sie im gleichnamigen Abschnitt weiter unten.

Und nun zum Aufsetzen von Clients in Sterntopologie:

Schritt 1: Stellen Sie sicher, dass Ihre Fritzbox anhand einer DynDNS-Domain ansprechbar ist (MyFritz geht am schnellsten, Details dazu siehe [3].

Schritt 2: Installieren Sie WireGuard auf die für den Fernzugriff gedachten Geräte (siehe wireguard.com/install).

Schritt 3: Öffnen Sie auf der Fritzbox das Menü „Internet/Freigaben/VPN (WireGuard)" und klicken Sie auf „Verbindung hinzufügen". Übernehmen Sie die „vereinfachte Einrichtung" und klicken Sie auf „Weiter". Geben Sie dem eingehenden Tunnel einen Namen, zum Beispiel den des Tunnelnutzers ergänzt um den Gerätetyp und schließen Sie die Tunnelkonfiguration über „Fertigstellen" ab.

Schritt 4: Lassen Sie das Webinterface bis zum Abschluss der Konfiguration offen und laden Sie die Konfiguration zunächst auf den PC herunter, mit dem Sie die Fritzbox steuern. So haben Sie ein Backup für alle Fälle. Wenn Sie mehrere WireGuard-Tunnel zu verschiedenen Boxen brauchen, geben Sie den Dateien verständliche Namen, etwa „wg_zuHause-iPhone.conf" oder „wg_OnkelHotte-Laptop.conf".

Auf Smartphones lesen Sie eine Tunnelkonfiguration am einfachsten ein, indem Sie in WireGuard über die Kamera den QR-Code vom Webinterface der Fritzbox ablichten. Für Laptops und PCs bringen Sie die Konfiguration auf das jeweilige Gerät und lesen die Datei dann in WireGuard ein. Auf macOS und Windows geht das am einfachsten über das Menü „Tunnel aus Datei importieren". Auf Linux übergibt man die Datei dem WireGuard-Plug-in des Network-Managers. Damit ist die Konfiguration abgeschlossen und Sie können den Tunnel über das WireGuard-Menü aktivieren.

Alternativ bringen Sie auf Linux die Konfigurationsdatei per Terminal in den Ordner /etc/wireguard und speichern sie dort unter dem Namen wg0.conf (wg1.conf, falls der Name belegt ist, oder die nächste freie

Zahl). Falls Sie keinen NetworkManager verwenden: WireGuard startet man auf der Kommandozeile mit dem folgenden Befehl:

```
sudo sysctl start wq-quick@wg0
```

Setzen Sie statt wg0 den Interface-Namen ein, den Sie für die Datei verwendet haben. Statusmeldungen liefert der Befehl `sudo wg`.

Im Test ließen sich über Wochen stabile WireGuard-Tunnel zu diversen Fritzboxen an Glasfaser-, DSL- und Kabelanschlüssen aufbauen, obwohl FritzOS 7.50 noch in der Entwicklungsphase steckte. Die Stabilität und Vielseitigkeit dürfte auch Nutzer von Kabel-Fritzboxen freuen, denn der Kabelrouter nimmt ab FritzOS 7.50 Verbindungsanfragen für den Tunnel endlich über IPv6 an. So umgeht er die IPv4-blockierende CG-NAT des Providers (Carrier-Grade NAT).

LAN-zu-LAN-Kopplung

Auch LAN-zu-LAN-Kopplungen lassen sich mit WireGuard auf Fritzboxen mit überschaubarem Aufwand aufsetzen. Damit die Boxen den lokalen und entfernten Verkehr korrekt routen können, müssen sie verschiedene Subnetzbereiche verwenden.

Öffnen Sie auf den beiden Boxen, die Sie vernetzen wollen, die Webinterfaces in zwei Browserfenstern; wenn eine entfernt ist, nutzen Sie den Fernzugriff über MyFritz.

Falls eine der beiden noch keinen WireGuard-Tunnel enthält, starten Sie die Konfiguration auf der

WireGuard auf Fritzboxen: Die Besonderheiten

WireGuard ist auf Fritzboxen rund doppelt so schnell wie das VPN auf IPsec-Grundlage (rund 247 Mbit/s gegenüber nur 126 Mbit/s, siehe S. 8). Deshalb ist es auch für Admins einen Blick wert, die schon länger IPsec-Tunnel produktiv einsetzen. Aber AVM hat WireGuard auf eigene Art implementiert. VPN-Teilnehmer erhalten keine IP-Adressen aus einem separaten Subnetz, sondern aus dem Netz der Fritzbox, zu der der Tunnel aufgebaut wird.

Das ist besonders bei LAN-zu-LAN-Kopplungen ungewohnt; dabei erhält die lokale Fritzbox für den Tunnel eine IP-Adresse aus dem entfernten Subnetz. So bringt sie in der Grundeinstellung sämtliche lokalen Netzwerkgeräte über den Tunnel in Kontakt mit dem entfernten Subnetz (siehe Infografik). Wenn nur bestimmte Geräte auf den Tunnel Zugriff haben sollen, muss man den Zugriff in der Tunnelkonfiguration auf ausgewählte Geräte beschränken. Unterm Strich ist das aus Sicht des gelegentlichen Fritzbox-Admins schön einfach. Unkomfortabel ist allerdings, dass man jedes einzelne unerwünschte Gerät per Einzelklick zur Verbotsliste hinzufügen muss – lästig, wenn an der Box viele Geräte angeschlossen sind.

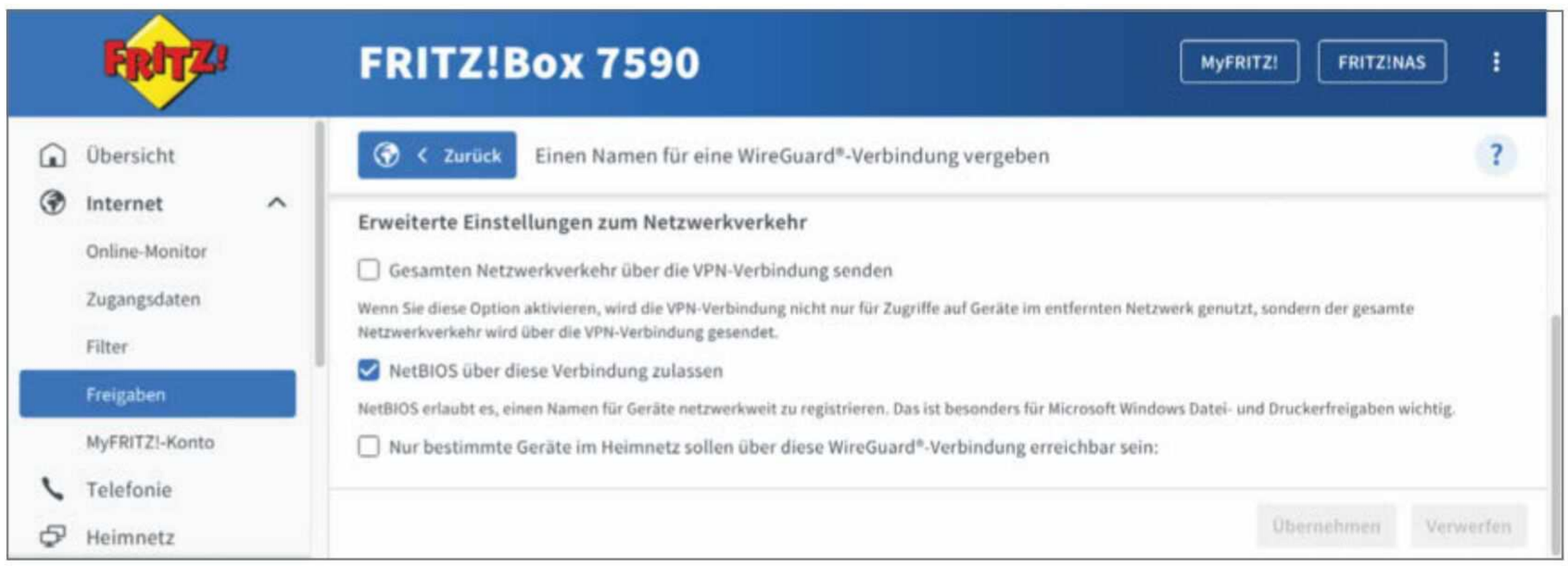
Auch zur Vereinfachung trägt bei, dass Fritzboxen im WireGuard-Tunnel bisher nur IPv4-Pakete befördern; das genügt ja, um auf gängige Geräte im entfernten Netz zuzugreifen. Aber wer auf ein IPv6-Netz hinter einer Fritzbox zugreifen will, muss einen separaten WireGuard-Peer aufsetzen und braucht die Fritzbox dann nicht.

Den Tunnelaufbau kann man nicht anhand von Fritzbox-Benutzernamen reglementieren, das geht nur bei IPsec. Stattdessen kann man in der VPN-Verwaltung einzelne WireGuard-Tunnel einfach deaktivieren.

Auf den PC heruntergeladene Konfigurationsdateien sind nicht nur als Backups nützlich. Sie erlauben auch kleine Optimierungen. Zum Beispiel ist es empfehlenswert, vor der Installation einer Konfigurationsdatei einen zusätzlichen DNS-Resolver wie 9.9.9.9 einzutragen und zwar vor dem, den die Fritzbox automatisch setzt. Der automatisch gesetzte ist nämlich jener der entfernten Fritzbox, was zwar gut ist für die Namensauflösung im entfernten Netz, aber nachteilig, wenn der Tunnel nicht zustande kommt. Manche Clients behalten dann trotzdem den entfernten Resolver in der Systemkonfiguration und können ihn nicht erreichen, sodass gar keine DNS-Auflösung mehr klappt. In dieser Situation hilft ein externer DNS-Resolver. Ein Beispiel sieht so aus:

```
DNS = 9.9.9.9, 192.168.59.1, fritz.box
```

Dabei entspricht 192.168.59.1 dem entfernten Resolver. 9.9.9.9 ist hingegen die Adresse des öffentlichen Resolvers des gemeinnützigen Anbieters Quad9.



Im Grundzustand lässt eine Fritzbox keinen NetBIOS-Verkehr in den VPN-Tunnel hinein. Das kann man aber auch nach der Konfiguration eines Tunnels genehmigen, um dann auf Windows-Freigaben per SMB-Protokoll zugreifen zu können.

anderen, weil Sie sich so einen Importschritt ersparen. Wenn hingegen beide Boxen WireGuard-Konfigurationen enthalten, spielt es keine Rolle, auf welcher Sie die Konfiguration beginnen. Zusammengefasst erzeugt man auf einer Box die Konfigurationen für beide Router und bringt dann eine exportierte Konfigurationsdatei auf den anderen.

Der Vorgang im Einzelnen: Öffnen Sie das Menü „Internet/Freigaben/VPN (WireGuard)“, klicken Sie auf „Verbindung hinzufügen“ und wählen Sie „Benutzerdefinierte Einrichtung“. Beantworten Sie die Frage, ob auf der anderen Fritzbox bereits ein WireGuard-Tunnel konfiguriert ist – aber klicken Sie nur dann auf „nein“, wenn auf der anderen Fritzbox tatsächlich kein WireGuard-Tunnel konfiguriert ist. Andernfalls klicken Sie „ja“ und fahren Sie mit dem übernächsten Absatz fort.

Wenn die entfernte Fritzbox keine WireGuard-Konfiguration enthält, beantworten Sie den Dialog mit „nein“ und geben Sie dem Tunnel einen aussagekräftigen Namen, zum Beispiel „Zentrale“.

Als Nächstes müssen Sie das Subnetz und die Subnetzmaske der entfernten Fritzbox eingeben. Um das Subnetz zu ermitteln, öffnen Sie das Webinterface der zweiten Fritzbox und klicken dort auf das Menü Heimnetz/Netzwerk. In der ersten Gerätezeile steht die LAN-IP-Adresse der Fritzbox, beispielsweise 192.168.59.1. Ersetzen Sie die letzte 1 mit 0, dann haben Sie das Subnetz, also beispielsweise 192.168.59.0. Tragen Sie es in der geöffneten WireGuard-Konfiguration der ersten Fritzbox ein und darunter die Subnetzmaske 255.255.255.0. Klicken Sie auf „Fertigstellen“. Nach einigen Sekunden ist die Konfiguration fertig. Laden Sie sie auf den PC herunter und bringen Sie diese auf die zweite Box über „Verbindung hinzufügen“, „Benutzerdefinierte Einrichtung“ und „ja“. Geben Sie dem Tunnel einen Namen und importieren Sie die Datei über „Datei auswählen/Fertigstellen“. Beide Boxen bauen den Tunnel dann umgehend auf. Das kann man beispielsweise im Menü System/Ereignisse lesen („Es wurde erfolgreich eine WireGuard-Verbindung zur Gegenstelle ‚Zentrale‘ aufgebaut“).

Die Einrichtung weicht von der obigen ab, wenn die zweite Box bereits WireGuard-Tunnel hat. Dann muss man deren Konfiguration exportieren und in die erste Box bringen. Das ist ein wenig umständlich, aber immerhin erkennt die erste selbstständig, welches Subnetz die Gegenseite verwendet und setzt das Routing passend. Der Rest läuft wie oben ab, man bringt also die von der ersten Fritzbox erzeugte neue Datei auf die zweite.

Nach erfolgtem Tunnelaufbau kann man Geräte testweise im entfernten Netz anpingen, beispielsweise von der ersten Fritzbox aus die entfernte:

```
ping 192.168.59.1
```

Wenn das funktioniert, sollten Zugriffe auf Freigaben wie Webserver klappen. Für SMB-Zugriffe (Windows-Dateifreigaben) muss man auf beiden Fritzboxen in den Tunneleinstellungen die Übertragung von NetBIOS-Paketen zulassen. Bei einem aufgebauten Tunnel kann es etwa eine Minute dauern, bis der Vorgang abgeschlossen ist. Anschließend kann man entfernte SMB-Freigaben anhand ihrer IP-Adresse öffnen.

Himbeer-Verbindung

LAN-zu-LAN-Kopplungen lassen sich auch gemischt mit einem Router anderer Couleur aufbauen. Wir

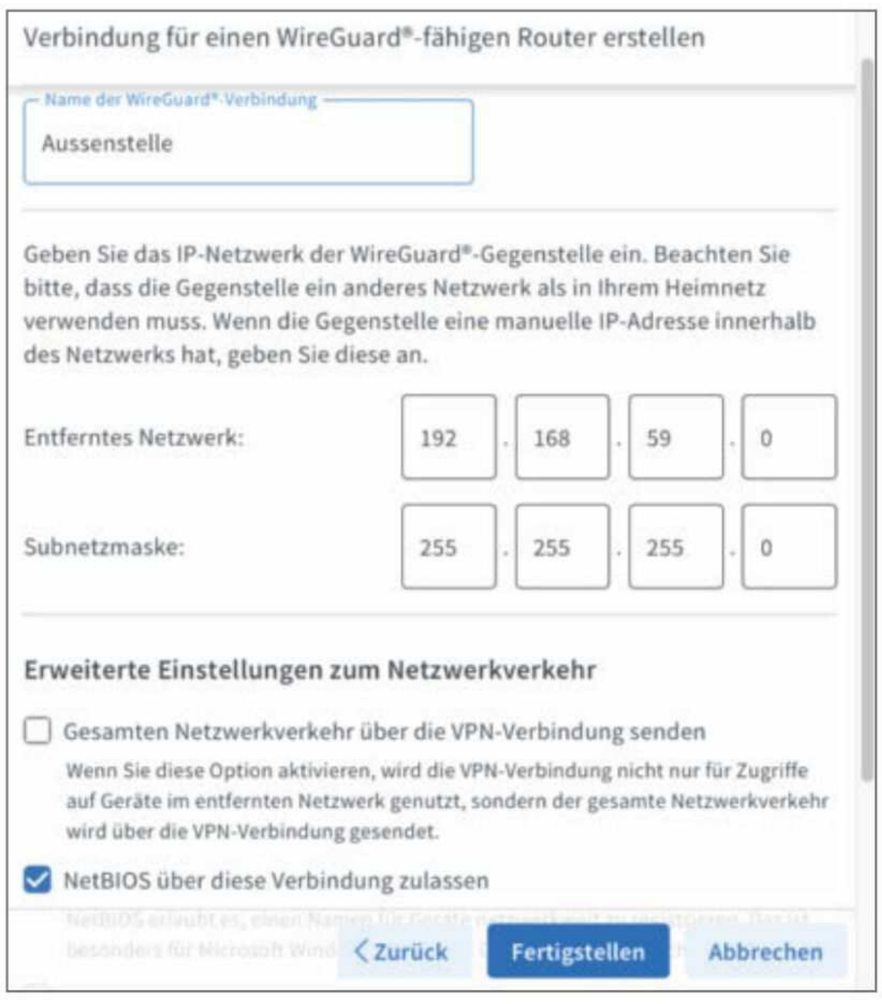
haben es mit einem Raspi und einer auf einem Synology-NAS erzeugten Debian-VM mit der aktuellen Betriebssystemversion Bullseye ausprobiert. Mit einem solchen Linux-System kann man WireGuard auch hinter Fritzboxen nutzen, denen AVM kein Update auf FritzOS 7.50 spendiert.

Am einfachsten geht es, wenn man vom Linux-System aus das Webinterface der entfernten Fritzbox über ihre MyFritz-Adresse öffnet. Dort erstellt man wie oben beschrieben eine Konfiguration für einen Router, der noch keine Tunnelkonfiguration enthält.

Dann trägt man auf Nachfrage das Subnetz ein, in welchem das Linux-System läuft und ergänzt die Subnetzmaske (z. B. 192.168.59.0, 255.255.255.0), damit die Fritzbox allen WireGuard-Verkehr aus ihrem eigenen Subnetz in den Tunnel bringt. Die so erzeugte Datei speichert man im Ordner des aktuellen Linux-Benutzers, also etwa /home/pi. Anschließend müssen auf einem jungfräulichen Linux einige Pakete mittels Terminalbefehlen nachinstalliert werden:

```
sudo apt update
sudo apt dist-upgrade
sudo apt install wireguard resolvconf↵
↳ raspberrypi-kernel-headers
```

Kopieren Sie dann die Tunnelkonfiguration (z. B. wg-config.conf) in den Ordner /etc/wireguard:



Bei LAN-zu-LAN-Kopplungen muss man für korrektes Routing nur das entfernte Subnetz eingeben.

```
cd /home/pi
sudo cp wg-config.conf↵
↳ /etc/wireguard/wg0.conf
```

Ersetzen Sie /home/pi mit dem Ordner des aktuellen Benutzers.

Eine Fritzbox erzeugt eine Tunnelkonfiguration normalerweise für einen Router, der sowohl den Internet-Zugang aufbaut, als auch den WireGuard-Tunnel; entsprechend trägt sie in der Config-Datei eine Route für das gesamte entfernte Netz ein:

```
Address = 192.168.59.0/24
```

Eine entfernte Fritzbox muss dann eingehende WireGuard-Pakete nur noch zu dem Switch-Port umlenken, an dem der angesprochene Client angeschlossen ist. Doch in unserem Szenario funktioniert das nicht, weil der Linux-Rechner hinter dem Internet-Router steht. Er muss stattdessen die Pakete vom virtuellen WireGuard-Interface (z. B. wg0) auf das physische Interface schicken (z. B. eth0).

Damit das klappt, weist man seinem wg0-Interface nachträglich per Hand eine zweite IP-Adresse aus seinem Subnetz zu. Öffnen Sie das Webinterface des Routers, hinter dem das Linux-System läuft und suchen Sie eine freie IP-Adresse. Die meisten Router blenden die belegten IP-Adressen zum Beispiel auf der Startseite in Statusmeldungen ein, Fritzboxen im Menü Heimnetz/Netzwerk. Im Weiteren verwenden wir als Beispiel 192.168.59.140.

Tragen Sie die freie Adresse mit einem Editor wie `nano` in `/etc/wireguard/wg0.conf` ein und zwar im Abschnitt [Interface] in der Zeile „Address“. Passen Sie dort die Subnetzmaske von 24 auf 32 an, weil in der Variablen nicht mehr ein komplettes Subnetz steht, sondern nur eine einzelne Adresse. Ein Beispiel sieht so aus:

```
Address = 192.168.59.140/32
```

Speichern Sie die Änderungen mit Strg+X,Y und schalten Sie die Paketweiterleitung ein, damit Linux den ein- und ausgehenden Tunnelverkehr zwischen dem physischen und dem WireGuard-Interface bewegen kann:

```
sudo sysctl net.ipv4.ip_forward=1
```

Um diese Einstellung nach einem Neustart automatisch zu setzen, ergänzen Sie /etc/sysctl.d/99-sysctl.conf wie folgt:

WireGuard Site-to-Site nach AVM-Art

Wenn man zwei Netzwerke mittels WireGuard auf Fritzboxen koppelt, erhalten beide Router für den Tunnel je eine IP-Adresse aus dem entfernten Subnetz. Dann gewähren sie mittels passenden Routing-Einstellungen sämtlichen lokalen Netzwerkgeräten auf einen Schlag Zugriff auf das jeweils entfernte LAN.




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

Starten Sie dann WireGuard:

```
sudo systemctl start wg-quick@wg0
```

Ob der Tunnel aufgebaut ist und ob Verkehr darüber läuft, zeigt wieder ein `sudo wg`. Wenn alles klappt, lassen Sie den Tunnel automatisch beim Neustart mit

```
sudo systemctl enable wg-quick@wg0
```

aufbauen und starten Linux neu mit `sudo reboot`. Anschließend sollte der Tunnel automatisch errichtet werden. Damit das gesamte Subnetz auf den Tunnel zugreifen kann, setzen Sie im Router, hinter dem das Linux-System sitzt, eine statische Route zum entfernten Netz (z. B. 192.168.178.0, 255.255.255.0), die über den Linux-Rechner führt (192.168.59.140).

Beispielsweise geht das auf Netgear-Routern über das Menü „Erweitert/Erweiterte Einrichtung/Statische Routen“. Auf DrayTek-Routern findet man die Funktion in „LAN/Static Route“.

Auch auf Fritzboxen muss man bloß die statische Route hinzufügen. Sie finden die Option im Menü Heimnetz/Netzwerk/Netzwerkeinstellungen, „Weitere Einstellungen“, „IPv4-Routen“. Klicken Sie auf „Neue IPv4-Route“ und tragen Sie im Dialog das Subnetz der entfernten Fritzbox ein (z. B. 192.168.178.0), die Subnetzmaske 255.255.255.0 und die IP-Adresse des Linux-Systems, auf dem WireGuard läuft (hier 192.168.59.140).

Anschließend können Sie den Tunnel mit dem Ping-Befehl von beiden Seiten aus testen.

Wenn das klappt, kann man von beiden Seiten aus auf Freigaben des entfernten Netzwerks zugreifen, also etwa auf entfernte Webserver. Für SMB-Zugriffe muss nur das Durchlassen des NetBIOS-Verkehrs auf der Fritzbox aktiviert werden.

Was nicht geht

Anders als von anderen VPN-Implementierungen gewohnt, kann man WireGuard-Konfigurationen auf Fritzboxen nicht nachträglich ändern. Ein Editiermodus dafür wäre aber wünschenswert, damit man etwa bei Änderungen eines der beiden Subnetze einfach das Routing per Hand anpassen kann, anstatt wie jetzt alles neu machen zu müssen (Konfiguration erzeugen, auf Zielgerät bringen, ggf. statische Route im Zielgerät ändern).

Router, die Internetzugang wie die Fritzbox 6850 5G per Mobilfunk aufbauen, können keine unverlangt eingehenden VPN-Verbindungen annehmen (Serverbetrieb), obwohl sie vom Betreiber globale IPv6-Adressen erhalten – die Provider blockieren

Literatur

[1] Dušan Živadinović, **Freie VPN-Fahrt**, Fritzbox, WireGuard und IPSec: Endlich VPN via IPv6, c’t 07/2022, S. 65

[2] Dušan Živadinović, **Himbeertunnel**, Raspi versorgt LAN mit IPv6-Adressen, c’t 20/2022, S. 172

[3] Dušan Živadinović, **Freie VPN-Fahrt**, Fritzbox, WireGuard und IPSec: Endlich VPN via IPv6, c’t 07/2022, S. 62

WireGuard-Clients, -Erweiterungen und Infos

ct.de/wgmp

dabei unverlangt eingehenden Verkehr. Manche geben an, Basisstationen mit knappen Ressourcen vor Überlastung schützen zu wollen. Tatsächlich haben sie aber für den Serverbetrieb separate Tarife im Angebot, beispielsweise „Vodafone-Zuhause“.

Die Deutsche Telekom bietet ausschließlich für Geschäftskunden den Dienst „Mobile IP VPN“. Dabei teilt der Betreiber über einen privaten APN eine öffentliche IPv4-Adresse zu. Mit Glück kann man sich mit dem kostenlosen Telekom-APN internet.t-d1.de behelfen. Der teilt zumindest in manchen Regionen öffentliche IPv4-Adressen zu, sodass man eingehende VPN-Verbindungen über das alte Protokoll aufsetzen kann.

Einen Root-Server vorausgesetzt, kann man sich den Zugang zu einem Netz hinter einem Mobilfunkrouter auch mittels einer eigenen WireGuard-Infrastruktur konfigurieren. Das erfordert jedoch reichlich Know-how.

Ebenso verhält es sich, wenn man fortgeschrittene Funktionen mit WireGuard umsetzen will, beispielsweise eine Verschleierung der Paketinhalte, um Firewall-Blockaden zu entgehen. Mit gängigen Linux-Implementierungen kann man dafür auf die „Iptables WireGuard obfuscation extension“ zurückgreifen, die kürzlich auf GitHub erschienen ist (siehe ct.de/wgmp) – sie lässt sich auf Fritzboxen nicht installieren.

Was gut geht

So wird klar: AVM will mit seiner WireGuard-Implementierung möglichst viele Nutzer mit geringen Vorkenntnissen ansprechen und lässt dafür Dinge weg, die kompliziert, aber selten nachgefragt sind. Das Resultat kann sich sehen lassen. Es macht nicht nur Spaß, die Technik auszuloten, sie ist auch nützlich. (dz) c't





Gigabit-Internet im Haus verteilen

Internet mit einem Gigabit pro Sekunde ist für manche keine Utopie mehr, sondern schon Alltag. Eine weitere Beschleunigung wird so sicher kommen wie die nächste Steuerforderung. Spätestens wenn das Gigabit-Internet bei Ihnen anklopft, wird es Zeit zu prüfen, ob das hausinterne Netz der Datenflut gewachsen ist.

Von **Ernst Ahlers**



Bild: Andreas Martini

Schnelles Internet im Haus verteilen	26
Funknetzprobleme selbst lösen	30
Alternative Wege fürs Gigabit-Internet	36
Routersteuerung mit FlexiWAN praktisch erproben	44

Das pandemiebedingte Homeoffice wirkt als Katalysator für den Wandel der Internetzugänge: Statt nur passive Konsumenten digitaler Medien zu sein, wofür ein mit 100 Mbit/s schon zügiger Anschluss locker genügt, werden die Heimarbeiter tagsüber zu Produzenten. Große Dateien sollen nicht nur möglichst schnell heruntergeladen werden (Downstream), sondern nach dem Bearbeiten ebenso flott wieder in die Firma oder die Cloud zurückwandern (Upstream).

Zwar wird die Mehrheit der Beschäftigten ins Büro zurückgekehrt sein, wenn sich die SARS-CoV-2-Pandemie endlich zu einer gesellschaftlich und wirtschaftlich leichter verdaubaren Endemie gewandelt hat. Aber auch dann wird das Homeoffice für eine große Zahl der bevorzugte Tätigkeitsort bleiben, wenn nicht alltäglich, so doch bestimmt mehrere Tage pro Woche.

Deshalb ist nicht nur der Upstream der verschiedenen Internetanschlusstypen wichtiger geworden, sondern die nutzbare Geschwindigkeit überhaupt – die natürlich auch beim Weiterleiten vom Anschluss im Wohnzimmer zum Schreibtisch im Arbeitszimmer am anderen Ende des Hauses erhalten bleiben soll.

Nebenbei freut sich der Nachwuchs, wenn der Download des dutzende Gigabyte schweren neuen Lieblingsspiels nicht mehr drei Stunden, sondern nur noch eine Viertelstunde braucht. Gegen solche Schwergewichte verblasst freilich der Bandbreitenbedarf aller anderen Anwendungen (siehe Tabelle „Typische App-Datenraten“).

Zwar wären viele abseits der Bevölkerungszentren Lebende schon froh, Internet per Telefonleitung (VDSL) mit den oben genannten 100 Mbit/s und 40 Mbit/s im Downstream zu bekommen. Doch mit Super-Vectoring und 250/50 Mbit/s ist diese Technik auch schon am Anschlag. Mehr ist nicht zu erwarten.

Für die propagierte Gigabit-Gesellschaft müssen folglich andere Zubringertechniken einspringen: Internet per TV-Kabel, per Glasfaser (siehe S. 50) sowie 5G- und später 6G-Mobilfunk.

Landet das Netz mittels Fiber-to-the-Building (FTTB, Glasfaser bis in den Keller) im Haus und wird dort mit der Übertragungstechnik G.fast in die Telefonleitung zur Wohnung eingespeist, gehen prinzipiell bis zu 1000 Mbit/s in beide Richtungen. Dieses Maximum bremst der Provider gemäß seinen Tarifen ein.

Glasfaseranschlüsse mit GPON-Technik (siehe S. 64) bis in die Wohnung erreichen zurzeit maximal 2,5 und 1,25 Gbit/s (Down-/Upstream). Der längst definierte Nachfolger XGS-PON alias 10GPON treibt das auf bis zu 10 Gbit/s in beide Richtungen hoch.

In der Schweiz gibt es mit Init7 sogar schon einen Provider, der Punkt-zu-Punkt-Glasfaseranschlüsse mit 25 Gbit/s symmetrisch anbietet. Sie kosten dieselben 65 Schweizer Franken monatlich wie langsamere Init7-Zugänge mit 10 oder 1 Gbit/s.

Internet per TV-Kabel kann mit dem schon weitgehend ausgebauten DOCSIS 3.1 maximal 10 Gbit/s im Downstream und 1 Gbit/s in Gegenrichtung transportieren. DOCSIS 4.0 wird den Upstream weiter auf bis zu 6 Gbit/s beschleunigen.

Zwar teilen sich mehrere Haushalte die TV-Kabel- und GPON/XGS-PON-Bandbreite (Shared Medium), typische „Split-Verhältnisse“ für Letztere können bei 1:32 liegen. Aber wenn nicht alle gleichzeitig Daten übertragen, wird man bei Down- und Uploads zumindest vorübergehend tatsächlich die Spitzendatenraten bekommen. Dafür muss jedoch die Infrastruktur mitspielen, also die Netze der Provider ebenso wie die Quell- und Zielserver.

Bis sich Multigigabit-Zugänge über terrestrische Netze verbreitet haben, wird es gewiss noch geraume Zeit dauern. Gibt es am eigenen Lebensmittelpunkt noch keines, kann man sich das schnelle Internet eventuell per 5G- oder später 6G-Mobilfunk drahtlos ins Haus holen.

Auch diese Techniken können mehrere Gigabit pro Sekunde liefern – wenn man momentan der einzige Nutzer der Funkzelle und diese flott genug angebunden ist. Die in den USA schon erhältliche, Fixed Wireless Access genannte 5G-Variante für Festnetzanschlüsse ist hierzulande nicht abzusehen.

Schnelles Netz schnell verteilen

Wer jetzt schon Gigabit-Internet bekommen kann, will es verlustfrei in der ganzen Wohnung nutzen. Dafür drängt sich WLAN alias Wi-Fi als beliebteste, weil bequemste Technik fürs Vernetzen über die letzten Meter auf: Man muss kein Kabel ziehen – was

Typische App-Datenraten

Anwendung	Datenrate in Mbit/s
Chat/Messaging	0,01
Telefonie[1]	0,05–0,20
Audiostreaming[1]	0,06–0,26
Videokonferenz-Upstream (HD)[1]	0,6–3,5
Full-HD-Video[1]	4–10
4K-Video[1]	10–30
Up- und Downloads	was die Leitung hergibt

[1] je nach App, Einstellungen und Kompressionsgrad

bei Mobilgeräten ohnehin nicht geht – und die Verbindung ist mit ein paar Klicks eingerichtet.

Doch WLAN bringt typischerweise nur dann hohe Performance (siehe Tabelle „Datenraten“ auf voriger Seite), wenn Client und Basis (Access-Point, AP, meist in den Router integriert) im selben Raum sind. Quer durch eine 4-Zimmer-Wohnung bricht die Geschwindigkeit drastisch ein: Einerseits dämpfen Wände und Einrichtungsgegenstände das Hochfrequenzsignal stark, andererseits schießen in dicht besiedelten Gegenden Nachbar-WLANs quer, weil sich alle das Medium Funk teilen müssen.

Diese Effekte treffen auch Mesh-WLAN-Systeme, die mehrere Basen in einer Wohnung über einen separaten Funkkanal verknüpfen. Mittelschnelle Internetzugänge bekommt man mit aktuellen Mesh-Systemen auf Wi-Fi-6-Basis zwar verlustarm weiterverteilt, aber 1 Gbit/s durch mehrere Wände wird auch das in wenigen Jahren kommende Wi-Fi 7 ziemlich sicher nicht schaffen.

Flinkeres WLAN

Der nächste WLAN-Standard verdoppelt zwar die maximale Funkkanalbreite nochmals auf 320 Megahertz (MHz) und nutzt bei exzellenter Signalqualität die sehr hochstufige Modulationstechnik 4096QAM, was zusammen den 2,4-fachen Durchsatz gegenüber Wi-Fi 6 bringt.

Der extrabreite Kanal ist aber nur im neuen 6-Gigahertz-Band nutzbar, wo die Streckendämpfung etwas höher als bei Wi-Fi 6 im 5-GHz-Bereich ist. Außerdem sinkt die spektrale Leistungsdichte wegen der verdoppelten Kanalbreite. Zusammen dürften beide Effekte dafür sorgen, dass Wi-Fi 7 einen Multigigabit-Durchsatz auf Anwendungsebene nur innerhalb eines Raumes erreichen wird.

Um mit dem Notebook auch weiter weg vom Router einen schnellen Zugang zu haben, bringt man das Netz geschickterweise über andere Wege dahin und setzt erst vor Ort aufs WLAN um. Das bedeutet: Stellen Sie überall dort einen modernen Access-Point hin, wo Sie sich oft aufhalten.

Ein Tipp zum Optimieren des WLANs (siehe S. 30) sei vorweggenommen, weil er sehr viel bringt: Der Access-Point kann auch ein bisher drahtlos angebundener Repeater mit LAN-Buchse sein. Denn der wandelt sich zum AP, wenn man ihn per Ethernet-Kabel mit dem Router verbindet. In unseren Tests von Mesh-Systemen ergab das mit einem Notebook als Client stets einen großen Geschwindigkeitsgewinn. Beim ZenWifi AX Mini von Asus – dem kompakten Würfelchen links im Bild – etwa verdoppelte sich der Durchsatz von 125 auf 267 Mbit/s [1], gemessen über sechs Meter und eine Steinwand zwischen Access-Point und Notebook im 5-GHz-Band.

Stellt man den zum AP gewandelten Repeater nun in dem Raum auf, wo sein WLAN-Signal am häufigsten gebraucht wird, dann klettert die erzielbare Geschwindigkeit weiter – mit Glück sogar über die in der Tabelle genannten typischen Nettowerte für sehr gute WLAN-Verbindungen.

Am besten per Kabel

Der optimale Weg ist folglich, Access-Points per LAN-Kabel anzubinden: Gigabit-Ethernet für 1000 Mbit/s ist Standard. Multigigabit-Ethernet (NBase-T) bis 2,5 Gbit/s breitet sich bei Routern, APs, PC-Mainboards, Netzwerkspeichern und Switches zunehmend aus. NBase-T mit 5 oder 10 Gbit/s ist noch selten, aber technisch ausgereift [2, 3].

Doch den Aufwand zum Verlegen neuer Kabel scheuen viele, und das zu Recht: In einer bezogenen

Datenraten gängiger Inhaus-Vernetzungstechniken

Netzwerktyp	Medium	Brutto (max., Mbit/s)	Netto (Mbit/s)[2]	Netto (MByte/s)[2]
Fast Ethernet	Kabel[1] (CAT5)	100	95	12
Wi-Fi 4 (IEEE 802.11n)	Funk (2,4 GHz)	600	100	13
Wi-Fi 5 (IEEE 802.11ac)	Funk (5 GHz)	6900	400	50
Wi-Fi 6 / 6E (IEEE 802.11ax)	Funk (2,4 + 5 / 6 GHz)	9600	500	60
Gigabit-Ethernet	Kabel[1] (CAT5e)	1000	950	115
NBase-T 2,5 Gbit/s	Kabel[1] (CAT5e)	2500	2400	290
NBase-T 5 Gbit/s	Kabel[1] (CAT5e)	5000	4700	570
10-Gigabit-Ethernet	Kabel[1] (CAT5e/6a/7)	10.000	9500	1150

WLAN-Datenrate und Reichweite grundsätzlich variabel, abhängig unter anderem von Signalqualität, Kanalbreite, Anzahl Antennen, Nachbar-WLANs, Gebäudekonstruktion, Geräteausrichtung [1] Twisted-Pair, 10 Gbit/s auf CAT5e-Kabel bis ca. 50 m, auf CAT6a/CAT7 bis 100 m [2] typischer Wert bei guter Verbindung



Ungehobene Schätze: Bindet man WLAN- oder Mesh-Repeater über ihre LAN-Buchse an den Router an, werden sie zum Access-Point. Das kann fern des Routers die Datenrate auf Anwendungsebene mal eben verdoppeln.

Literatur

[1] Ernst Ahlers, **Günstigere Wi-Fi-6-Masche**, Kurztest Asus ZenWifi AX Mini, c't 23/2020, S. 87

[2] Ernst Ahlers, **LAN extraflott**, Multigigabit-Ethernet für mehr Netzwerkdurchsatz, c't 16/2020, S. 52

[3] Andrijan Möcker, **Bitautobahn**, Hardware fürs Multigigabit-LAN, c't 16/2020, S. 56

[4] Jan Mahn, **Undurchsichtiges Glas**, LWL-Grundwissen für Admins und Hausvernetzer, c't 18/2020, S. 72

[5] Jan Mahn, **Legen und legen lassen**, LWL-Grundwissen: Stecker und Kabel, c't 18/2020, S. 76

Wohnung möchte niemand Möbel verrücken, Nuten in Wände fräsen, Leitungen einbringen und Netzwerkdosen anschließen. Diese Arbeiten müssen bis zur nächsten Renovierung warten. Bis die Infrastruktur für schnelles Ethernet so allgegenwärtig ist wie elektrischer Strom und fließendes Wasser, werden deshalb noch einige Dekaden vergehen.

Bis dahin können Sie sich mit zwei Methoden behelfen. Optimieren Sie Ihr WLAN und bringen Sie das Netz über einen Kabel-Umweg mit etwas neuer Hardware näher ans Ziel. Denn in vielen Wohnungen gibt es mindestens zwei, oft gar drei Leitungstypen, die sich für den Datentransport zweckentfremden lassen: das Hausstromnetz (Powerline), Telefonleitungen (Ethernet over Phoneline) und die TV-Signalverteilung auf Koaxkabeln (Ethernet over Coax).

Ab Seite 36 schildern wir die Vor- und Nachteile, die Randbedingungen für den Einsatz sowie die Leistungsgrenzen der drei Techniken. Mit zweien kann man das Gigabit ganz praktisch knacken, bei einer geht sogar schon das Doppelte auf Anwendungsebene durch (2 Gbit/s).

Infrastruktur-Upgrade

Falls Sie Ihrem Heim bei der Sanierung eine leistungsfähige Netzwerkinfrastruktur spendieren, entsteht die Frage, ob diese auf optischer Basis oder klassisch elektrisch entstehen soll.

Für das Verlegen von Glasfasern alias Lichtwellenleitern [4, 5] spricht deren enorme Bandbreite: Optisches Ethernet für Verbindungen innerhalb von Rechenzentren läuft zurzeit mit maximal 400 Gbit/s auf einer Faser (400GBASE-FR8 mit 8 Wellenlängen oder Farben bis 2000 Meter Reichweite); 800 Gbit/s sind auch schon spezifiziert. Bei Weitverkehrsstrecken (WAN) sind zurzeit 400 Gbit/s auf einer Wellenlänge möglich. Mit bis zu 88 Farben (Dense Wavelength Division Multiplexing, DWDM) transportiert eine Faser dann maximal 35.000 Gigabit/s oder 35 Terabit/s.

In Firmen kommen LWL für stockwerksübergreifende, schnelle Verbindungen zwischen Abteilungs-Switches oder zwischen Gebäuden zum Einsatz, bisher typischerweise mit 10 Gbit/s, mancherorts auch schon mit 25 oder 40 Gbit/s. Für passende Glasfasermodule haben die Switches SFP+- oder QSFP-Schächte.

Vorerst noch mit Kupfer

Bei der Inhaus-Vernetzung bedingt eine LWL-Verkabelung aber, dass man an den allermeisten Geräten Umsetzer – Medienwandler – von der optischen auf die elektrische Ebene braucht. Denn an PCs, Internet-Routern, TV-Geräten und Settop-Boxen ist Gigabit-Ethernet per Twisted-Pair-Kabel mit RJ45-Steckern nach wie vor Standard. Für die Medienwandler zahlt man nicht nur bei der Anschaffung, sondern über ihre Leistungsaufnahme auch fortlaufende Stromkosten. Dennoch kann eine Glasfaserstrecke auf Privatgrund sinnvoll sein, beispielsweise zum Anbinden eines als Arbeitsbereich genutzten Nebengebäudes.

Die klassische Kupferverkabelung mit CAT6a- oder CAT7-Leitungen taugt für mindestens 10 Gbit/s, was mittelfristig bei Weitem ausreichen sollte. Denn bis die Glasfaserzugänge der Internetprovider weiträumig mehr als 10 Gbit/s liefern, wird es wohl noch geraume Zeit dauern. Obendrein kann man per Twisted-Pair-Kabeln kompatible Access-Points oder LAN-Kameras auch gleich mit Energie versorgen (Power-over-Ethernet) und sie so auch dort platzieren, wo keine Stromsteckdose in der Nähe ist.

Wer seine Gebäude beim Sanieren für die fernere Zukunft rüsten will, legt parallel zu den Kupferleitungen jetzt schon in jeden Raum zwei Glasfaserstränge. Der geringe Aufpreis für die zusätzlichen Leitungen macht sich spätestens dann bezahlt, wenn unsere Nachkommen das Netzwerk dereinst für das 100-Gigabit-Zeitalter aufrüsten. (ea) c't



Bild: Andreas Martini

Funknetzprobleme selbst lösen

Wenn der Netflix-Stream stockt und Downloads schneckenlangsam kriechen, rätseln viele über die Ursache. Unser Ratgeber gibt Ihnen die Grundlagen, viele WLAN-Probleme selbst zu lösen, passend einzukaufen und Ihr Netz gigabittauglich zu machen.

Von **Andrijan Möcker**

Kabellose lokale Netzwerke auf Basis des Standards IEEE 802.11, besser bekannt als WLAN (Wireless Local Area Network) oder Wi-Fi (Wireless Fidelity) haben sich innerhalb der letzten 20 Jahre weltweit in allen Bereichen des Lebens als das Mittel der Wahl durchgesetzt, um mobile und stationäre Geräte unkompliziert an ein Computernetzwerk und damit auch meist ans Internet anzubinden.

Die meisten Menschen benutzen WLANs täglich und ein privater Internetanschluss ohne WLAN-Router ist heute kaum noch vorstellbar – in der Regel bekommt man einen vom Anbieter dazu. Aber gerade im privaten Bereich, wo Fachwissen seltener ist als in Firmen, haken Funknetze regelmäßig – beispielsweise aufgrund störender Nachbarnetze oder schlechter Abdeckung. Doch Sie müssen kein Hochfrequenztechniker sein, um Ihre WLAN-Probleme in

den Griff zu bekommen; lediglich etwas Verständnis für die Technik und ein bisschen Spaß am Ausprobieren ist nötig.

Router, Access-Point, Repeater, Mesh

Um sich in der WLAN-Welt zurechtzufinden, sollten Sie zunächst etwas Terminologie abspeichern: Ein Router übersetzt zwischen dem Internet und dem Heimnetz und schützt letzteres durch seine Firewall vor Eindringlingen von außen. Im Heimbereich sind heute nahezu ausschließlich Router mit eingebauter WLAN-Basis üblich – die Geräte kombinieren also mehrere Netzwerkfunktionen.

Alles dahinter ist kein Router: Der Repeater war lange Zeit das Mittel der Wahl, um die WLAN-Abdeckung zu erhöhen. Er wird kurz vor der Reichweitengrenze des Routers eingesteckt, verbindet sich mit dessen WLAN und strahlt das Netz mit gleichen Zugangsdaten erneut ab. Muss er die Daten auf dem gleichen Kanal zum Router übertragen, wird die Datenrate aufgrund der Wartezeit etwas mehr als halbiert. Mittlerweile gibt es jedoch moderne Repeater, die das Problem mit einer dritten WLAN-Schnittstelle lösen, die ausschließlich für die Verbindung zum Router zuständig ist.

Viele Hersteller sind vom Begriff „Repeater“ abgewandert und bieten heute Mesh-Systeme an. Sie umfassen eine Basis, die per Kabel mit dem Router verbunden wird, sowie kabellose Mesh-Knoten und folgen nicht mehr dem klassischen Repeater, sondern verwenden proprietäre Protokolle, um sich untereinander zu vernetzen. Die Kommunikation muss dabei nicht direkt zur Basis laufen, sie kann auch über mehrere Mesh-Punkte „springen“. Nachteil: Systeme unterschiedlicher Hersteller sind nicht zueinander kompatibel.

Das schnellste WLAN erhalten Sie aber noch immer per Kabel: Ein Access-Point ist eine WLAN-Basis, die die Daten per Netzwerkkabel ins Heimnetz leitet. Da man dort alleiniger Nutzer des Mediums ist, flutschen die Daten immer mit der Maximalgeschwindigkeit des Mediums, bei Gigabit-Ethernet circa 950 Mbit/s auf Anwendungsebene.

Frequenzen und Kanäle

In Europa stehen derzeit vier Frequenzbereiche (Bänder) für WLAN zur Verfügung: 2,4, 5, 6 und 60 Gigahertz (GHz). Die ersten beiden sind etabliert und werden von den meisten modernen Geräten unterstützt; das 6-GHz-Band kam erst 2021 hinzu und ist bislang nur bei wenigen Geräten an Bord; das besonders hochfrequente 60-GHz-WLAN ist derzeit nur für Richtfunkstrecken im Einsatz. Damit nicht jeder Router beziehungsweise Nutzer eine separate Lizenz oder Anmeldung benötigt, werden Funkbänder über Allgemeinzuteilungen freigegeben. Sie legen fest, in welchem Frequenzbereich mit welcher Sendeleistung gesendet werden darf und dass sie anmeldefrei sind.

Um zu regeln, wo innerhalb des Funkbandes gesendet wird, gibt es standardisierte Kanäle. Sie legen die Mittenfrequenz fest, also die Frequenz, von der aus Geräte den Kanal „aufspannen“. Für Kanal 1 auf 2,4 GHz ist das beispielsweise 2,412 GHz. Die Bandbreite legt fest, wie viel des Bandes ober- und unterhalb der Mittenfrequenz für die Datenübertragung genutzt wird – je mehr Bandbreite, desto mehr Netto-

WLAN-Spektrum in der EU ab 2021

Die Öffnung des 6-GHz-Bandes hat das Funkspektrum für WLAN in Europa nahezu verdoppelt. In den USA steht seit Sommer 2020 noch einiges mehr zur Verfügung.





Viele Router – in diesem Fall eine Fritzbox – erlauben Ihnen, die WLAN-Kanaleinstellungen zu ändern. In Umgebungen mit vielen Nachbarnetzen ist das jedoch nicht sinnvoll, da diese unvorhergesehen den Kanal wechseln können. Nutzen Sie deshalb die Autokanalfunktion.

datenrate. Ein 20 MHz breiter Kanal auf Kanal 1 geht somit von 2,402 GHz bis 2,422 GHz – also 10 MHz in beide Richtungen. Die Krux: Anders als etwa bei CB-Sprechfunkgeräten sind WLAN-Kanäle nicht überlappungsfrei; Kanal 2 beginnt bereits bei 2,417 GHz. Im 83,5 MHz breiten 2,4-GHz-Band stehen somit vier überlappungsfreie 20-MHz-Kanäle zur Verfügung: 1, 5, 9 und 13. Oder eben zwei 40-MHz-Kanäle (1+5 und 9+13).

Die Hauptgründe für Störungen im Netz: Sie sind in den Frequenzbereichen selten alleine, denn die Nachbarn haben schließlich meist auch einen WLAN-Router und mehrere Geräte, und gerade im 2,4-GHz-Band kommen noch Bluetooth, Smart-Home-Funkstandards und so weiter hinzu. Auch deshalb ergeben 40-MHz-Kanäle auf 2,4 GHz heute keinen Sinn mehr, wenn Sie Nachbarn in der Nähe haben. Das Band ist zu überlaufen, sodass breitere Kanäle das Netz eher instabil machen, als die Datenrate zu steigern.

Vergeuden Sie nicht Ihre Zeit mit der Suche nach dem optimalen Funkkanal, sondern überlassen Sie das der Router-Automatik. Es ist besonders in dichter besiedelten Gegenden wegen der Vielzahl konkurrierender Nachbar-WLANs unsinnig, eine feste Betriebsfrequenz und Kanalbreite vorzugeben. Denn andere WLANs mit aktiver Automatik wechseln ihren Kanal unvorhersehbar.

Anders als etwa ein LTE-Netz kennt WLAN keine zentrale Kontrolle der Sendevorgänge. Stattdessen lauscht das Gerät, egal ob Router, Repeater oder Smartphone, in den Kanal hinein, ob dieser frei ist und sendet dann; ähnlich, wie wenn mehrere Menschen in einem Raum ein Gespräch führen und eine Lücke abwarten – wer die Lücke erwischt spricht, während die Anderen warten; sprechen mehrere gleichzeitig, kommt es zu Verständnisschwierigkeiten. Das passiert im WLAN durch das Hidden-Station-Problem ständig; weil die Störreichweite immer höher ist als die Nutzreichweite, können sich nie alle Kanalnutzer gegenseitig empfangen. Einige gehen dann fälschlicherweise davon aus, dass der Kanal frei ist. Das ist so, als ob Sie (Access-Point) innerhalb eines Hauses über Flure hinweg mit jemandem (Smartphone) kommunizieren, der währenddessen durch ein offenes Fenster von einem Streit (Nachbar-WLAN) auf der Straße gestört wird, den Sie unten in der Küche aber nicht hören können.

In den 5- und 6-GHz-Bändern ist das Problem weniger ausgeprägt: Einerseits ist darin mehr Platz, sodass auch Kanäle mit 40, 80 oder sogar 160 MHz möglich sind; außerdem werden die höheren Frequenzen stärker durch Hindernisse gedämpft, sodass die Nachbarnetze weniger stören. Das 5-GHz-Band hat jedoch einen Nachteil: Auf ein paar Kanälen sind Wetterradare bevorrechtigt und Router müssen, sobald sie Radarimpulse erkennen, den Kanal wechseln. In der Konsequenz fällt die 5-GHz-Zelle kurz aus, manche Clients wechseln auf das langsame 2,4-GHz-Netz.

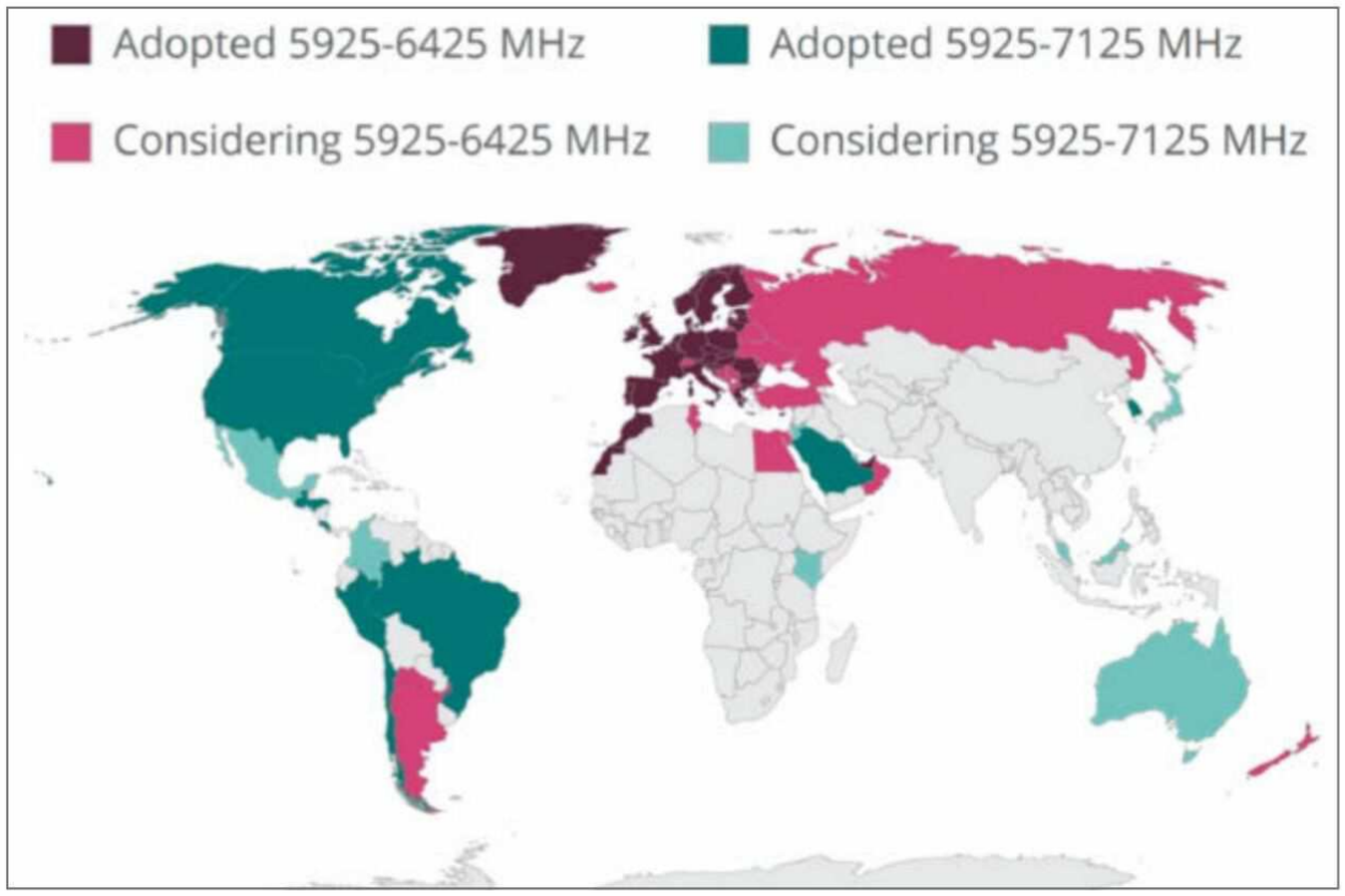


Bild: Wi-Fi Alliance, Stand: Januar 2022

2021 wurden die zwei etablierten Frequenzbereiche für WLAN bei 2,4 und 5 GHz um ein drittes „Wi-Fi 6E“ getauftes Band zwischen 5,9 und 7,1 (dunkelgrün) beziehungsweise 5,9 und 6,4 GHz (dunkelrot) erweitert, um die Kapazität zu erhöhen. Alle europäischen Länder mit Ausnahme des Kosovo haben es bereits freigegeben.

Haben Sie trotz guter Empfangsstärke schlechte Latenz und Datenrate, ist vermutlich lahme WLAN-Hardware der Grund, denn wer in stark ausgelasteten Funkumgebungen die kurzen Lücken anderer Teilnehmer aufgrund zehn Jahre alter Technik nicht effizient nutzen kann, erhält nur maue Ergebnisse.

WLAN ≠ WLAN

Seit der Verabschiedung der ersten WLAN-Spezifikation IEEE 802.11 im Jahr 1997 hat sich eine Menge getan und neue Spezifikationen mit Verbesserungen sind hinzugekommen – ähnlich wie bei Bluetooth und USB. Deshalb ist es besonders wichtig, dass Sie wissen, was aktuell ist und mit welcher Spezifikation die Hardware arbeitet, die Sie derzeit benutzen oder kaufen wollen.

Welchen WLAN-Standard ein Gerät unterstützt, erkennen Sie bei Routern, Access-Points und Repeatern in der Regel schon auf der Verpackung; bei Endgeräten (Laptops, Smartphones und so weiter) meist im Datenblatt. Unterschieden wird anhand eines an den Basisstandard IEEE 802.11 angehängten Buchstaben: IEEE 802.11a, b, g, n, ac und ax sind derzeit üblich. Um die Verständlichkeit für weniger technisch versierte Nutzer zu erhöhen, hat die Wi-Fi Alliance 2018 eine Nummerierung ab 802.11n eingeführt, das nun auch „Wi-Fi 4“ heißt – das noch taufrische 802.11ax somit Wi-Fi 6, und mit angehängtem „E“, wenn das Gerät zusätzlich das neue 6-GHz-Band bedient.

Geräte mit IEEE 802.11b (1999, 11 Mbit/s) und 802.11g (2003, 54 Mbit/s) sollten Sie heute nicht mehr betreiben. Wie vorher beschrieben, sind Sie im Frequenzband nicht alleine und müssen die Zeit, die Sie zum Senden haben, effizient nutzen – insbesondere, wenn die Funkumgebung stark durch andere Netze und Geräte (Bluetooth, ZigBee usw.) ausgelastet ist. Von den 11 oder 54 Mbit/s Bruttowert – also der während einer Paketübertragung genutzten Link-Datenrate – bleiben nur wenige Hundert bis Tausend Kilobit pro Sekunde über.

Außerdem muss das moderne Smartphone nicht zwangsläufig tadellos mit dem alten Access-Point zusammenspielen – gerade wenn letzterer keine Wi-Fi-Zertifizierung hat. Sie wird vom Herstellerverband „Wi-Fi Alliance“ vergeben und garantiert die Erfüllung der 802.11-Spezifikationen und damit die Interoperabilität von Geräten unterschiedlicher Hersteller. Kurzum: Geräte mit 802.11b und g gehören ins Recycling und durch neuere Hardware ersetzt, allein schon, weil sie keine sichere Verschlüsselung des Funkverkehrs beherrschen.

Mehrantennennetz

Wi-Fi 4 (IEEE 802.11n) kam ab 2005 auf den Markt und ist heute noch bei vielen WLAN-Basen der Standard für Datenübertragungen auf 2,4 GHz. Mit der Spezifikation kam unter anderem der Funkbeschleuniger „MIMO“ (Multiple Input Multiple Output) in die

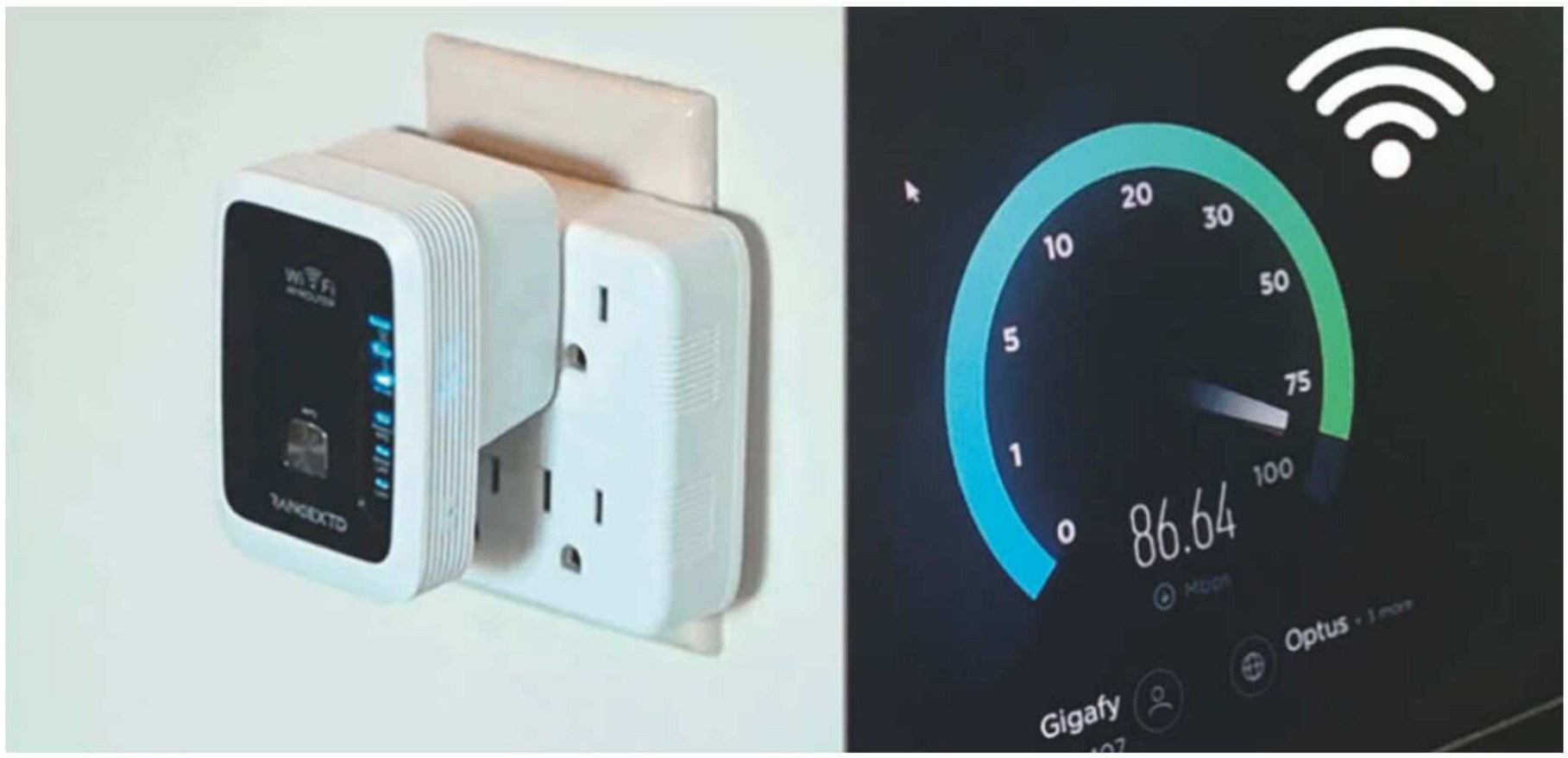


Bild: primetechtrends.com

Im Internet taucht derzeit immer wieder Werbung für Wunder-Repeater auf, die 50 bis 130 Euro kosten. Tatsächlich handelt es sich oft um lahme Wi-Fi-4-Single-Band-Repeater im Wert von rund 20 Euro. Wer einen richtig schnellen Internetzugang im Haus weiterleiten will, sollte davon die Finger lassen.

WLAN-Welt, der auf dem gleichen Kanal über mehrere Antennen unterschiedliche Daten gleichzeitig übertragen kann. Die Technik macht sich zunutze, dass in den hohen WLAN-Frequenzbereichen selbst kleine Veränderungen des Antennenstandorts dafür sorgen, dass sich die Ausbreitung der elektromagnetischen Wellen durch den Raum verändert – sie strahlen also wortwörtlich aneinander vorbei. Mit mehreren um ein paar Zentimeter versetzten Antennen kann die Datenrate bis zu vervierfacht werden, was bei Wi-Fi 4 rund 600 Mbit/s bedeuten würde; üblich waren jedoch zwei Antennen, daher das „bis zu 300 Mbit/s“ auf vielen Verpackungen und in Datenblättern. Die Anzahl der Antennen, auch „Streams“ genannt, wird meist als „2×2-“, „4×4-“ oder „8×8-MIMO“ im Datenblatt angegeben und in c’t-Tabellen in Klammern hinter der Wi-Fi-Version notiert, also etwa „Wi-Fi 4 (2)“.

Wi-Fi 4 machte zudem das 5-GHz-Band populärer, da zusehends Dual-Band-fähige Geräte auf den Markt kamen.

Alte Wi-Fi-4-Basen mit mindestens zwei MIMO-Streams können Sie in weniger dicht besiedelten Gebieten und dort, wo dreistellige Datenraten nicht nötig sind, weil etwa nur die Kinder YouTube-Videos auf Smartphones schauen oder Hörbücher im Garten gestreamt werden, noch problemlos einsetzen. Das spart Geld und verzögert die oft umweltschädliche Verschrottung der Hardware. Ist das Gerät jedoch nicht Dual-Band-fähig, sollten Sie es nicht als Repeater benutzen, denn dabei wird die Datenrate etwas mehr als halbiert, da der Repeater das Paket erst empfangen und dann auf demselben Kanal erneut aussenden muss; das geht nicht gleichzeitig. Im Access-Point-Modus – also der Weiterleitung der Daten ins Heimnetz und Internet per Kabel – auf einem separaten Kanal, macht das Surfen nach wie vor Spaß [1]. Aber der veraltete WLAN-Standard setzt dennoch eine harte Grenze bei ungefähr 150 Mbit/s Nutzdatenrate.

Wi-Fi 5 (IEEE 802.11ac) wurde 2013 verabschiedet und brachte WLAN unter anderem 80 und optional 160 MHz breite Kanäle bei, die aber ausschließlich bei 5 GHz genutzt werden können. Die Spezifikation befähigt WLAN-Basen zudem erstmalig, mehrere Clients gleichzeitig zu bedienen: Multi-User-MIMO teilt die unterschiedlichen Antennen des Routers auf kompatible Clients auf – die Summendatenrate steigt und die Latenz sinkt, sodass etwa Internettelefonie oder Onlinespiele profitieren. Das klappt auch, wenn der Router vier Antennen hat, die Clients aber nur zwei. Wi-Fi 5 kann bis zu 6,9 Gbit/s Brutto

liefern, allerdings nur mit acht MIMO-Streams und auf einem 160-MHz-Kanal. Diese Ausstattung haben nur wenige Geräte; üblich sind vier Streams und 80-MHz-Kanäle, was 1,7 Gbit/s Brutto erlaubt. In der Praxis bleiben davon einige Hundert Megabit pro Sekunde über.

Wi-Fi 5 ist heute Standard bei modernen WLAN-Geräten und sollte Ihr Mindestanspruch sein, wenn Sie Hardware neu kaufen. Auch der Gebrauchtmarkt ist voll mit Geräten dieser Kategorie [2].

Gigabit knacken

Die neueste WLAN-Spezifikation ist Wi-Fi 6 (IEEE 802.11ax), die die IEEE erst im Februar 2021 veröffentlicht hat. Sie macht 160-MHz-Kanäle sowie höhere Modulationsstufen zur Standardausstattung, sodass pro Stream (Antenne) 1200 Mbit/s brutto durch die Luft gehen. In der Praxis konnten wir die Gigabit-Grenze auf Anwendungsebene mit zwei Streams, also 2400 Mbit/s brutto, knapp überwinden. Das klappt allerdings auch nur mit Wi-Fi-6-fähigen Clients und nur auf kurzer Distanz, denn die dafür nötigen hohen Modulationsstufen benötigen gute Signalstärke. Lassen Sie sich also nicht täuschen: Echtes Gigabit-WLAN erreichen Sie bei den derzeit üblichen MIMO-Ausstattungen (2 oder 4 Streams) in Mobilgeräten meist nur in dem Raum, in dem die Basis steht; mit viel Glück auch mal im Nebenzimmer.

Wi-Fi 6 hat aber viele andere Vorteile, die das Aufrüsten interessant machen: Es kann erstmalig den Kanal aufteilen, um mehrere Clients gleichzeitig zu bedienen (OFDMA), sogar in Kombination mit Multi-User-MIMO. Letzteres funktioniert nun auch im Uplink (mehrere Clients senden gleichzeitig an die Basis). „Spatial Reuse“ erlaubt Basen und Clients zudem, störende Nachbarnetze zu ignorieren und trotzdem zu senden – vorausgesetzt das andere Netz ist nur ganz schwach zu hören. Das klappt zwar ebenso nur mit Wi-Fi-6-fähigen Clients, doch wer jetzt in neue Hardware investieren möchte, um langfristig viele Clients zu bedienen oder mehr Stabilität und Datenrate in gedrängten Funkumgebungen zu erzielen, sollte auf Wi-Fi 6 nicht verzichten [3, 4].

Außerdem kommt noch das zuvor erwähnte neue 6-GHz-Band Wi-Fi 6E hinzu. Zwar können viele Mobilgeräte damit noch nicht umgehen, doch wenn Sie für Ihre Räume mangels Netzwerkverkabelung ein Mesh-Set benötigen und möglichst viel Datenrate erreichen wollen, sollte das neue Band zur Ausstattung gehören. Es dient dann als Backbone zwischen den Mesh-Knoten und da satte 500 MHz frei sind, profitiert die Nachbarschaft von mehreren parallel nutzbaren 160-MHz-Kanälen für hohe Geschwindigkeiten. Zudem entfällt die Radarerkennung, die auf 5 GHz zu Unterbrechungen führt. Aber auch hierfür gilt: Dämpfung durch Wände, Türen und Einrichtung lässt die Datenraten schnell fallen; die besten Ergebnisse erzielen Sie, wenn die Daten auf kürzestem Weg durch die Luft ihren Weg auf ein echtes Netzwerkkabel finden. Die Lösung lautet also, alle Räume, in denen man sich häufig aufhält, mit einer eigenen, per LAN-Kabel angebundenen WLAN-Basis auszustatten. (amo) c't

Literatur

[1] Andrijan Möcker, **Befreite Box**, OpenWrt-Spartipp: Fritzbox 7362 SL, c't 21/2020, S. 146

[2] Andrijan Möcker, **Drosselkiste**, Fritzbox 7520: Unechte Einschränkungen, c't 8/2020, S. 136

[3] Andrijan Möcker, **Flottfunk**, Wann sich Wi-Fi 6 für Sie lohnt, c't 3/2021, S. 16

[4] Ernst Ahlers, **Sechsmal sechs**, 6 Router für Wi-Fi 6 im Test, c't 3/2021, S. 20

Antworten auf häufige WLAN-Fragen

ct.de/wkep

Make:

DAS KANNST DU AUCH!





2× Make testen und über 9 € sparen!

Ihre Vorteile:

✓ **GRATIS dazu:** Make: Tasse
✓ **Zugriff auf Online-Artikel-Archiv***
✓ Jetzt auch im Browser lesen!
✓ Zusätzlich digital über iOS oder Android lesen

Für nur 16,10 € statt 25,80 €

* Für die Laufzeit des Angebotes.

Jetzt bestellen:

make-magazin.de/miniabo



Bild: Andreas Martini

Alternative Wege fürs Gigabit-Internet

Kommt das Notebook nicht ins WLAN, muss das WLAN zum Notebook kommen. Leicht gesagt, aber schwer getan, wenn ein LAN-Anschluss für einen zusätzlichen Access-Point fehlt. Ist der Königsweg Ethernet-Kabel nicht realisierbar, bringt ein Umweg über andere Leitungssysteme das schnelle Netz näher heran. Manche Nebenstrecken taugen viel, andere weniger.

Von **Ernst Ahlers**

Groß ist der Frust, wenn der Provider den Internetanschluss auf 1 Gbit/s beschleunigt hat, aber beim Notebook im Arbeitszimmer per WLAN nur ein Zehntel ankommt. In der Firma würde der Admin einen zusätzlichen Access-Point näher am Schreibtisch aufstellen, doch zu Hause mangelt es in der Regel an einem Gigabit-Ethernet-Port in der Nähe.

Falls es also irgendwie geht, verlegen Sie ein Ethernet-Kabel. Das ist auf Dauer preisgünstiger, als die Nebenstrecke zu aktivieren: Fast jedes Netzwerkgerät enthält einen LAN-Port von Haus aus, während

man für die Ersatzwege zusätzliche Adapter anschaffen muss, die auch zusätzlich Strom verbrauchen.

Ist das nicht machbar, gibt es glücklicherweise in vielen Häusern zwei bis drei unterschiedlich gut geeignete Kabelsysteme, die man fürs Datenweiterleiten in der Wohnung einspannen kann: das Stromnetz (Powerline, PLC), ungenutzte Telefonleitungen (Ethernet over Phoneline) und das TV-Koaxialkabel, kurz Koax (Ethernet over Coax, EoC).

Letzteres betrachten wir ausführlicher als die anderen Medien, weil darauf oft schon andere Dienste laufen (Digital-TV, Kabel-Internet). Dann gilt es beim parallelen Einsatz für den Inhaus-Transport ein paar Randbedingungen zu beachten, nicht nur um gegenseitige Störungen zu vermeiden, sondern um überhaupt eine Datenverbindung zu bekommen.

Beim Einordnen der Techniken helfen ein paar kurze Begriffsklärungen. Alle Systeme setzen das Ethernet-Signal auf die eigene Transportmethode über Adapter um. Viele davon arbeiten in einer Bus-Topologie: Alle Adapter hängen am selben Medium. Bei Powerline ist das die verzweigte Stromleitung, beim EoC das Koax-Kabel des TV-Verteilsystems. Dabei gilt: Wenn einer sabbelt, müssen alle anderen schweigen (Shared Medium).

Die auf dem Medium erzielbare Bandbreite teilen sich alle Adapter und die daran angeschlossenen Geräte (Hosts). Wenn vier Hosts scheinbar gleichzeitig kommunizieren, bekommt jedes Paar im Schnitt die halbe Datenrate. Bei Powerline und Koax lassen sich je nach System maximal 8 oder 16 Adapter vernetzen.

In der Stern-Topologie gibt es dagegen einen zentralen Verteiler. Bei Ethernet ist das beispielsweise der in den Router integrierte Switch. Hier können Datentransfers zwischen verschiedenen Host-Paaren gleichzeitig laufen. Basis dafür ist eine Punkt-zu-Punkt-Konstellation (P2P): Genau zwei Adapter kommunizieren miteinander, beim Ethernet-Switch ist das einer seiner Ports und das per LAN-Kabel daran angeschlossene Gerät. Der Switch leitet die Daten intern zwischen seinen Ports weiter. So kann ein 8-Port-Switch für Gigabit-Ethernet bei gleichzeitiger Übertragung über alle Ports in beide Richtungen (Vollduplex, simultanes Senden und Empfangen) bis zu 16 Gbit/s umschlagen.

Powerline-Durchsatz in einer Wohnung

Der Durchsatz bei Powerline-Datenübertragung fällt je nach Steckdose anders aus. Je weiter weg die Gegenstelle leitungstechnisch vom Router liegt, desto niedriger ist der Durchsatz in Mbit/s. Das kann sogar Steckdosen im selben Raum treffen. Diese Messwerte von 2015 sind auch 2022 noch typisch.



Inhaus-Vernetzungstechniken abseits von Ethernet und WLAN

Methode	Medium	Übliche Topologie	Maximale Linkrate	Erzielbarer Nettodurchsatz
HomePlug AV2	Stromleitung	Bus	1200 Mbit/s	400 Mbit/s[1]
G.hn Wave 2	Stromleitung	Bus	2400 Mbit/s	400 Mbit/s[1]
MoCA 2.5	Koax-Kabel	Bus	3500 Mbit/s	2300 Mbit/s
MoCA 3.0	Koax-Kabel	Bus	> 10.000 Mbit/s[2]	9500 Mbit/s[2]
G.hn Wave 2	Koax-Kabel	Bus	2400 Mbit/s	1500 Mbit/s[3]
G.hn Wave 2 erweitert	Koax-Kabel	Bus	> 10.000 Mbit/s[2]	9500 Mbit/s[2]
G.fast (Profil 106a)	Telefonleitung	Stern	1000 Mbit/s[4]	750 Mbit/s
G.fast (Profil 212a)	Telefonleitung	Stern	2000 Mbit/s[4]	1500 Mbit/s
G.hn Wave 2	Telefonleitung	Punkt-zu-Punkt	2400 Mbit/s	1500 Mbit/s[3]

[1] unter optimalen Bedingungen; in realen Hausstromnetzen niedriger (30 – 240 Mbit/s bei HomePlug AV2, 50 – 230 Mbit/s bei G.hn Wave 2) [2] geschätzt [3] MAC-Durchsatz laut Chiphersteller MaxLinear ca. 1700 Mbit/s [4] Summe Down- / Upstream, per Konfiguration aufteilbar, typisch 8:2

Via Stromleitung

Auch wenn das Hausstromnetz in mehreren Strängen vom Sicherungskasten als Sternpunkt verzweigt, ist es aus der Sicht von Powerline-Adaptern ein Bus. Denn sie schicken Daten mittels eines schwachen Hochfrequenzsignals auf die Stromleitung, das fast gleichzeitig bei allen anderen PLC-Adaptern in der Wohnung und oft auch beim Nachbarn ankommt.

Von den Nebenstrecken ist Powerline die holprigste: Stromkabel sind für den Energietransport ausgelegt, die Datenübertragung setzt da nur parasitär auf. Deshalb ist das praktisch dafür nutzbare Spektrum mit 2 bis zirka 80 Megahertz (MHz) recht klein. Zudem sind davon einige Bereiche ausgenommen (Notching), um den Amateurfunk zu schonen. Und besonders oben im Spektrum ist die Signaldämpfung hoch und wegen der in jeder Wohnung anderen Leitungsführung stark variabel. Deshalb sind auch die zu erwartenden Datenraten sehr unterschiedlich.

Zwar hat sich die mit Powerline mögliche Bruttodatenrate seit Anfang des Jahrtausends von winzig anmutenden 14 Mbit/s auf inzwischen 1200 Mbit/s bei der verbreiteten Übertragungstechnik HomePlug AV2 gemausert. Bei dem nicht zu HomePlug AV2 kompatiblen G.hn Wave 2 sollen nominell sogar bis 2400 Mbit/s gehen.

Doch auf Anwendungsebene schleusen Powerline-Adapter realistisch nur in wenigen Fällen 200 oder mehr Mbit/s durch, etwa bei exzellenter Verbindung zwischen zwei Steckdosen auf beiden Seiten einer Wand. Je nach Steckdosenkombination streut der Durchsatz in einer Wohnung typischerweise zwischen 10 und etwas über 100 Mbit/s [1].

Zudem beharken VDSL- und Powerline-Modems einander manchmal: Laufen eine PLC-beaufschlagte Stromleitung und die VDSL transportierende Telefonleitung im Haus nah beieinander, kann es zu Übersprechen kommen. Beide kompensieren solche Störungen unterschiedlich, aber der Durchsatz sinkt trotzdem etwas.

Allerdings kann gelegentlich die DSL-Synchronisation zusammenbrechen, dann ist für ein bis zwei Minuten „das Internet weg“. Gegen diesen besonders lästigen Effekt hat der Powerline-Entwickler Devolo ein Kraut gezüchtet [2].

Übern Telefondraht

Für den Datentransport über Strecken bis zu einigen hundert Metern hat die Telefonleitung mit den 250 Mbit/s der Super-Vectoring-VDSL-Internetzugänge absehbar ihr Maximum erreicht. Oberhalb der dort eingesetzten 35 MHz steigt die Signaldämpfung schnell in unpraktikable Höhen, denn Telefonkabel waren ursprünglich nur zur Übertragung von Sprache bis knapp 4 Kilohertz (0,004 MHz) vorgesehen.

Über die innerhalb von Gebäuden deutlich kürzeren Distanzen bis einige dutzend Meter kann dieses Medium aber gute Dienste leisten: Internetanbieter von Fiber-to-the-Building (Glasfaser bis in den Keller) nutzen Telefonkabel für das Inhaus-Weiterverteilen in Stern-Topologie mittels der Technik G.fast. Sie erreicht mit rund 200 MHz Signalbandbreite bis zu 2000 Mbit/s, was die Provider typischerweise 8:2 auf Down- und Upstream verteilen. Dabei sorgt Vectoring zwischen den Adernpaaren in Sammelkabeln dafür, dass die G.fast-Datenströme verschiedener Kunden einander möglichst wenig stören.



Devolos Giga-Bridge-Adapter transportieren Ethernet-Daten wahlweise über eine freie Telefonleitung oder ein TV-Koax-Kabel.



Die MoCA-Adapter goCoax MA2500D schleusten im c't-Labor schon 2,3 Gbit/s auf Anwendungsebene durchs Koax.

Fürs Vernetzen über Telefonleitungen innerhalb von Wohnungen hat sich der Parallelstandard G.hn Wave 2 etabliert. Beispielsweise bietet Devolo mit der Giga Bridge einen Adapter an, der das Glasfasermodem im Keller an den Router im Wohnzimmer koppelt. Im Test [3] probierten wir diese alternative Betriebsart der Devolo-Geräte aus und erzielten über 35 Meter Telefonleitung 950 Mbit/s.

G.hn-Adapter gibt es auch von anderen Anbietern, beispielsweise Giga Copper oder Allnet. Achten Sie bei der Auswahl auf die Signalbandbreite: Manche Hersteller setzen ihren Adaptern eine niedrigere Maximalfrequenz von beispielsweise 76 MHz, um Störungen von Funkdiensten und UKW-Radios durch Abstrahlungen ungünstig verlegter Leitungen zu vermeiden. Solche Adapter schaffen maximal um die 500 Mbit/s.

Multifon

Wer mehr als zwei Punkte über Telefonleitungen verbinden muss, sollte nach G.hn-Switches für eine Stern-Topologie Ausschau halten. Der G.hn-Switch ersetzt die alte Telefonanlage; an die Stelle der Telefone kommen passende Modems. Beides bietet beispielsweise Giga Copper, wobei ein Zweiersatz Modems mit 230 Euro vergleichsweise günstig ist, ein 8-Port-Switch aber gleich mit 1700 Euro ins Kontor schlägt.

Wichtig bei dessen Einsatz: Die Telefonleitungen sollten idealerweise einzeln und nicht über längere Strecken als Bündel oder in den oben erwähnten Sammelkabeln verlegt sein. Zwar verwenden G.hn-Switches eine Störminderungstechnik (Neighbor Domain Interface Mitigation). Aber weil das für Powerline-Übertragungen ausgelegte NDIM auf Telefonkabeln wahrscheinlich nicht so effizient ist wie das Vectoring bei G.fast, könnten G.hn-Systeme einander wegen des gemeinsam genutzten Spektrums beeinträchtigen.

Vor zwei Sackgassen beim Vernetzen über Telefonleitungen sei noch gewarnt: Lassen Sie gebrauchte HomePNA-Switches und -Adapter links liegen. Diese 1999 gestartete Technik der Home Phoneline Networking Alliance erreichte 2007 mit 3.1 ihre letzte Version. HomePNA-3.1-Adapter haben 100 Mbit/s langsame Ethernet-Ports, können also auch höchstens diese Datenrate transportieren. 2013 schloss sich die HomePNA dem Homegrid Forum an, das G.hn propagiert.

Manche Heimvernetzer verbinden als Notlösung eine vieradrige Telefonleitung per RJ45-Stecker direkt mit Switch und PC, denn für Fast-Ethernet-Verbindungen genügen zwei Adernpaare. So lassen sich aber nur 20, vielleicht mal 30 Meter mit 100 Mbit/s überbrücken.

Durchs TV-Kabel

Koaxialkabel, kurz Koax, dienen seit Dekaden als breitbandiges Medium für Funkanwendungen, darunter Radio- und Fernsehsignale. Sie leiten auch sehr hochfrequente Signale verlustarm weiter, beispielsweise in Notebooks das WLAN-Signal zwischen Platine und Antenne.

In Wohngebäuden dienen Koax-Leitungen zum Verteilen des TV-Signals (heute Digital Video Broadcasting, DVB), entweder vom Hausanschluss des Kabel-TV-Anbieters (DVB-C) oder von einer (Gemeinschafts-)Satellitenschüssel zur Settop-Box (DVB-S).

Der Internetzugang per TV-Kabel mit DOCSIS-Technik (Data Over Cable Service Interface Specification) ist ein Nebenprodukt, das sich das Spektrum im Kabel mit den DVB-C-Fernsehsignalen teilt.

Anfang des Jahrtausends tauchten erste Adapter auf, die Ethernet-Daten parallel zum TV-Signal mit 60 bis 70 Mbit/s durch das Koax transportieren (Kurztest Corinex CableLAN AV200, [3]). Seitdem hat sich die Technik stark weiterentwickelt.

Moderne Ethernet-over-Coax-Adapter schaffen oft vollen Gigabit-Ethernet-Durchsatz [4], wofür sie die Übertragungstechniken G.hn Wave 2 der International Telecommunication Union (ITU) und MoCA 2.5 der Multimedia over Coax Alliance nutzen. EoC-Adapter, die nach älteren Standards arbeiten, sind nicht mehr zeitgemäß, weil langsamer.

Ganz frisch auf dem Markt: Der 85 Euro teure MoCA-Adapter goCoax MA2500D mit Multigigabit-Ethernet-Port transportierte bei einem ersten kurzen Test per TCP 2,3 Gbit/s. Der Weg in die Multigigabit-Gesellschaft ist also im Koax schon gebahnt. Andere Hersteller und Anbieter wie Allnet, Axing, Cablehome oder Devolo dürften bald nachziehen.

Mit einem frequenzmäßig erweiterten G.hn Wave 2 und MoCA 3.0 werden prinzipiell auch 10 Gigabit/s auf dem Koax-Kabel möglich. Aber das funktioniert nicht mehr parallel zu anderen Diensten wie Digital-TV (DVB-C oder DVB-S), weil die Inhaus-Datenübertragung dann das volle Koax-Spektrum belegt. Jenseits von 2 Gbit/s muss man sich also für einen der Dienste entscheiden. Angesichts der stetig schwindenden Bedeutung von linearem TV via DVB-C oder DVB-S spricht künftig mehr für Ethernet, das ja auch Live-Fernsehen transportieren kann, nämlich als Multicast-IPTV-Streams wie etwa beim MagentaTV der Telekom.

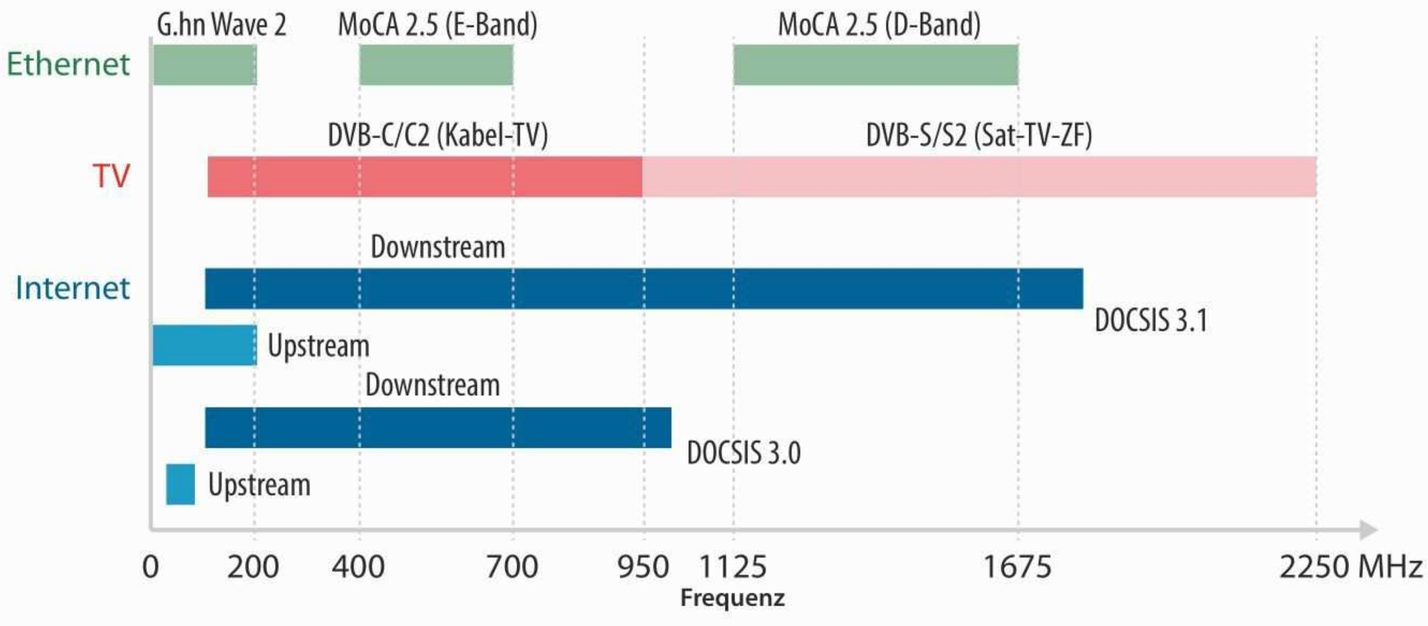
Paralleldienst

In den meisten Heimen ist das Koax-Verteilsystem schon von mindestens einem Dienst belegt, typischerweise entweder Kabel-TV (DVB-C/DVB-C2) nebst Internetzugang oder Satelliten-TV (DVB-S/DVB-S2). Man muss also vor dem Kauf eines EoC-Adapters überlegen, welche Technik am besten passt. Die kleine Checkliste (Seite 41) gibt eine erste Orientierung, und die Spektrumsgrafik zeigt detaillierter, welche Dienste in welchen Frequenzbereichen arbeiten, damit man Kollisionen vermeidet.

Einfach ists, wenn das Internet per TV-Kabel an der ersten TV-Dose des Kabelstrangs ankommt und Kabel-TV ungenutzt bleibt. Dann kann man dort den Strang auftrennen (Kabel-Router an erste Dose, EoC-Adapter ans weiterführende Koax-Ende). Doch in der Praxis ist die Situation oft komplizierter und für den optimalen Einsatz ist die Kenntnis der Kabelwege unerlässlich.

Koax-Spektrum

Auf einem Koax-Kabel können mehrere Dienste parallel laufen, typischerweise der Internetzugang (DOCSIS) und Kabelfernsehen (DVB-C/C2). Soll das Koax zusätzlich Ethernetdaten transportieren, muss man einen Adaptertyp wählen, dessen Spektrum nicht mit dem anderer Dienste überlappt.



EoC im Eigenbau geht nur dann glatt und risikoarm über die Bühne, wenn die Koax-Verteilung in Ihrer Bleibe vom Netz des Kabel-TV-Anbieters getrennt ist. Andernfalls kann das EoC-Signal ins Providernetz hinüberschwappen: Das Kabel-Internet der Nachbarn fällt aus, einzelne TV-Programmbouquets oder der per Kabel verteilte Digitalrundfunk werden gestört. Findet die vom Provider entsandte Technikerin den Fehler in Ihrem Eigenbau, landet neben deren Rechnung womöglich eine kostenpflichtige Unterlassungsaufforderung des Provider-Anwalts in Ihrem Briefkasten. Das Geld sollten Sie lieber für eine sachgerechte EoC-Installation durch eine Fachfirma einplanen.

Voraussetzungen

Eine Voraussetzung für den schnellen Datentransport übers Koax-Kabel sind rückkanalfähige TV-Verteilerdosen ohne Filter, damit das gesamte Spektrum (0 bis 2,2 GHz) an allen Anschlüssen verfügbar ist. Beispiele für Durchleitungsdosen (zwei Kabelenden in der Wand) sind Axing BSD 21-11 oder Kathrein ESD-44; die Pendants als End- beziehungsweise Einzeldosen heißen BSD 21-00 und ESD-84. Damit ist man auch für das kommende Kabel-TV/Kabel-Internet mit DOCSIS 4.0 gerüstet, das vollduplex arbeitet.

Wenn die Wohnung nur einen Koax-Strang hat, dann braucht man neue Dosen an allen Stellen, wo das EoC-Signal durchgeht, also jenen für die Adapter und alle dazwischen. Die Durchleitungsdosen dämpfen das EoC-Signal beim Weitergeben etwas. Deshalb bauen Adapter, zwischen denen ein längerer Kabelstrang mit vielen Dosen liegt, manchmal keine

Koexistenz im Koax-Kabel

Datentechnik versus Dienst	Koax frei	DVB-C/DOCSIS	DVB-S
G.hn Wave 2	✓	✓[1]	✓
G.hn Wave 2 erweitert	✓	–	–
MoCA 2.5	✓	✓[2]	✓[3]
MoCA 3.0	✓	–	–

[1] Filter zwischen Hauseinspeisung und Inhaus-Verteiler nötig [2] MoCA im D-Band, DVB-C/DOCSIS nur bis 1 GHz [3] MoCA im E-Band

Verbindung zueinander auf. Dann kann es helfen, auf dem Weg ungenutzte Dosen durch eine Kupplung zu ersetzen.

Gibt es in größeren Gebäuden mehrere Koax-Stränge und die EoC-Adapter hängen an verschiedenen, dann muss der gesamte Weg ertüchtigt werden. Im Zweifel ist es einfacher, gleich alle Dosen zu erneuern. Das betrifft auch den zentralen Verteiler im Sternpunkt, von dem die Stränge abgehen: Ein passiver Verteiler darf wie die Dosen keine Filter enthalten und muss bis 2,2 GHz geeignet sein.

Sitzt dort aber ein aktiver DVB-C-Verteiler, dann muss der durch eine Variante mit EoC-Einspeisung ersetzt werden. Solche Geräte bietet beispielsweise Digital Devices an. Die Grafik „Sternverteiler“ zeigt das Prinzip. Die Installation ist dann Sache für Fachpersonal.

Energie und Kosten

Einen Alternativweg für die Internetverteilung zu aktivieren, geht nicht ohne Investition: Man braucht




Smart gespart

Dieses **heise online-Sonderheft** rund um den smarten Haushalt zeigt Ihnen viele spannende Produkte, die Zeit und Energie sparen, sich als Helfer im Alltag beweisen und obendrein noch Spaß machen.

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

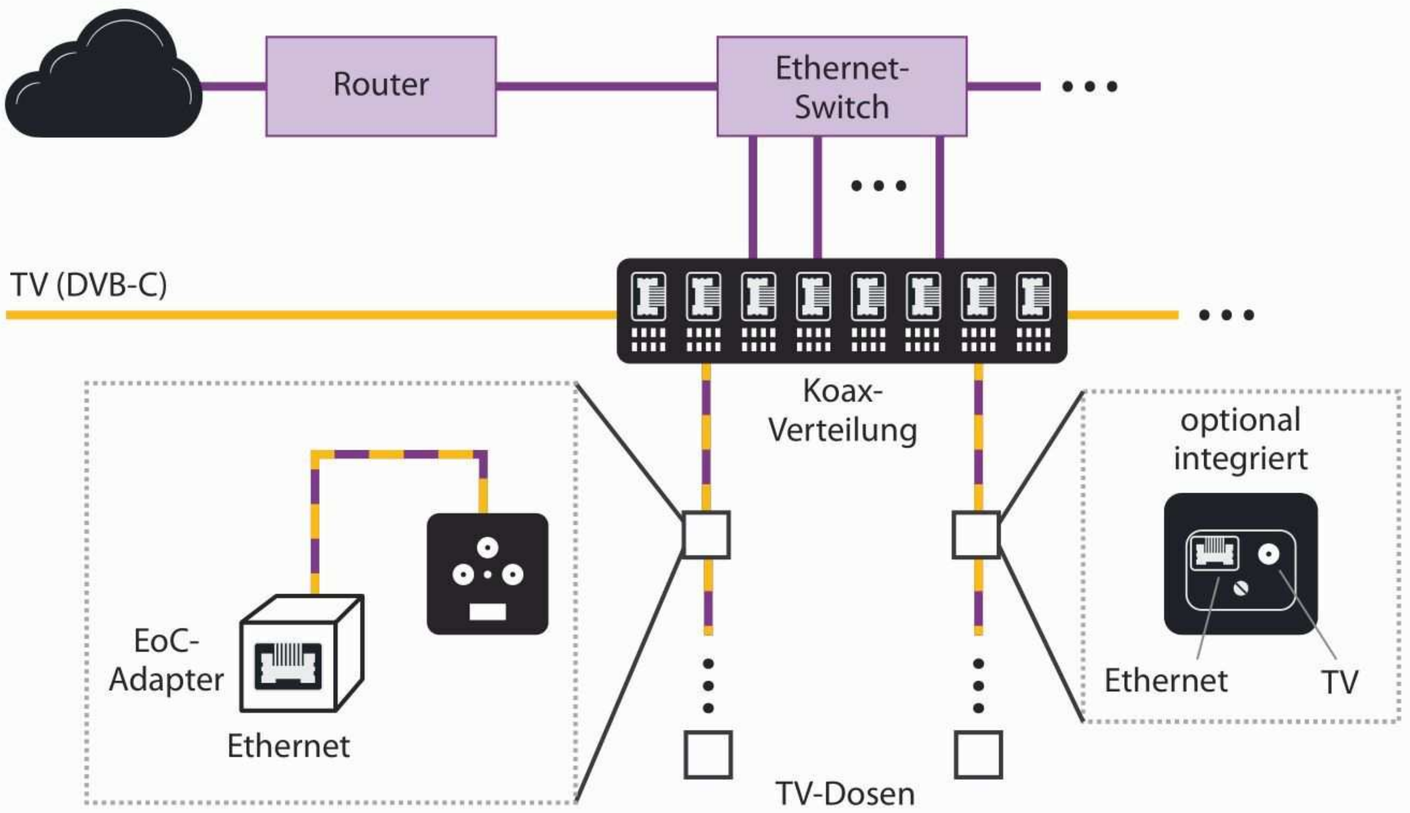
shop.heise.de/ho-wohnen22

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Sternverteiler für TV und Daten

Digital-TV läuft in größeren Häusern oft über mehrere Koaxkabel-Stränge mit einem passiven Verteiler an der Einspeisung. Wenn die Dämpfung im Koax-System zu hoch für simple Ethernet-over-Coax-Adapter an unterschiedlichen Enden ist, hilft ein zentraler Verteiler.



mindestens zwei Adapter, die für Powerline ab zirka 50 Euro pro Stück zu haben sind, aber für Koax und Telefonleitung auch mal einen Hunderter und mehr kosten können.

Dazu kommt bei Koax als Medium der eventuell nötige Austausch der TV-Dosen und die möglicherweise nötige Installation eines Filters durch eine Fachfirma. Eine brach liegende Telefonleitung gängig zu machen kann ebenfalls einen Technikerbesuch erfordern.

Schließlich verursacht die so freigegebene Nebenstrecke Stromkosten: Die Adapter ziehen je nach Typ und Betriebszustand von knapp unter 1 Watt (Standby bei Powerline-Adaptern) bis rund 4 Watt (aktiver Datentransfer bei MoCA-Adaptern).

Typischerweise liegt die Idle-Leistungsaufnahme eines Geräts bei rund 2 Watt. Die schlagen sich bei 30 Cent pro Kilowattstunde jährlich mit etwas über 5 Euro auf der Stromrechnung nieder.

Fazit

Powerline, die Technik zur Inhaus-Vernetzung über die Stromleitungen, hat ihren Zenit überschritten. Zum mehr oder weniger verlustarmen Weiterleiten langsamen und mittelschnellen Internets bis 200 Mbit/s taugt sie zwar weiterhin.

Aber die Gigabit-Musik spielt woanders: Ungenutzte Telefonleitungen transportieren mit passenden Adaptern mehrere hundert bis knapp an 1000 Mbit/s über nennenswerte Distanzen. Über die TV-Koax-Verteilung geht sogar schon das Doppelte. Perspektivisch schafft das Koaxialkabel 10 Gbit/s – wenn man dafür Kabel- und Sat-TV aufgibt. (ea) c't

Literatur

[1] Ernst Ahlers, **Stromnetz-Surfer**, Magic 2 soll die Powerline-Datenrate verdoppeln, c't 25/2018, S. 55

[2] Ernst Ahlers, **Entstördienst**, Powerline-Optimierung gegen DSL-Unterbrechungen, c't 16/2021, S. 126

[3] Ernst Ahlers, **Kabel-Brücken**, Kurztest Corinex AV200, c't 22/2005, S. 83

[4] Ernst Ahlers, **Passagier im Koax**, EoC-Adapter für Datentransfer über TV-Kabel, c't 2/2022, S. 98

betterCode()-Konferenzen

iX heise Developer dpunkt.verlag

CLEAN ARCHITECTURE

Die Heise-Konferenz für ein nachhaltiges Design von Software

6. Dezember 2022 · Online-Konferenz

Jetzt Ticket sichern!

Wartbarer, testbarer und nachvollziehbarer – dank Clean Architecture

Wie geht man **Clean Architecture** sinnvoll an? Wann lohnt sich diese überhaupt? Und wie sieht es aus, wenn man nicht auf der grünen Wiese anfangen kann? Und **welche Tools** können hier helfen? Antworten darauf gibt das Programm der betterCode() Clean Architecture.

- Wie lässt sich Clean Architecture praktisch realisieren?
- Legacy-Software mit tragfähiger Architektur versehen?
- Clean Architecture in einem großen Projekt
- Architektur und Design testen mit ArchUnit
- Architektonische Konzepte direkt in Code mit jMolecules bilden
- Architekturvision in Zeiten von Clean Architecture

clean-architecture.bettercode.eu

+++ Workshop am 1. Dezember 2022 +++

API 2023

Die Heise-Konferenz zu Design, Entwicklung und Management von Web-APIs



Jetzt Vorträge einreichen!

30. März 2023 · Online-Konferenz

Schnittstellen, die die Welt bedeuten

Die betterCode() API bietet Ihnen konzeptuelles Wissen, neueste Entwicklungen der Web-API-Entwicklung sowie umsetzbares Praxis-Know-how und Entscheidungshilfen für **Softwareentwickler:innen, Softwarearchitekt:innen** sowie **API- und Integrationsbeauftragte**.

api.bettercode.eu

Können Sie Konzepte und fortgeschrittene Aspekte von APIs gut erklären? Oder haben Sie Erfahrungen mit APIs gemacht, die Sie mit anderen Fachleuten teilen möchten?

Dann freuen wir uns über Ihre Vorschläge für unser Vortrags- und Workshop-Programm. Reichen Sie Ihre Ideen jetzt über unseren Call for Proposals ein.



Routersteuerung mit FlexiWAN

SD-WAN-Anbieter nutzen zwar offene und standardisierte Protokolle, aber die Kopplung von Controller und Edge-Routern bleibt proprietär. Der Neuling FlexiWAN stellt sein Produkt als Open Source ins Netz, sodass man es im kleinen Rahmen fast kostenlos ausprobieren kann.

Von **Markus Stubbig**

Wagemutige Admins betreiben ihr Software-Defined Wide-Area Network (SD-WAN) auf Open-Source-Basis in Eigenregie. Der Markt dafür ist überschaubar, denn hier gibt es für die großen Teilnehmer nichts zu verdienen. Mit FlexiWAN lassen sich die SD-WAN-Möglichkeiten als schlüsselfertiges Produkt genauso wie im Eigenbau erkunden. Doch eine Warnung vorab: Die grafische Oberfläche ist nicht Open Source. Wer die Zentrale selbst hosten will, muss entweder den öffentlichen FlexiWAN-Server mit einem Trick einspannen oder sie vollständig auf der Kommandozeile per API steuern.

Einen ersten Blick auf FlexiManage gewährt der Anbieter einen Monat lang für maximal fünf Flexi-

Edge-Router ohne Gebühren. Damit kann man immerhin ein SD-WAN für kleine Netze bauen und seine Möglichkeiten auf eigene Faust erkunden. Die Konfiguration eines ausgedehnten Netzes bleibt auch mit grafischen Werkzeugen komplex. Deswegen können wir hier nicht alle Schritte detailliert zeigen, sondern nur einen Überblick als Ausgangsbasis für eigene Versuche geben.

FlexiWAN besteht aus der zentralen Steuersoftware FlexiManage und dem Paket FlexiEdge für die Filialrouter. FlexiManage muss auf einem Server laufen, den die Router über eine öffentliche IP-Adresse erreichen können. FlexiEdge ist eine Sammlung aus mehreren Paketen, die aus einem Ubuntu-Linux einen Edge-Router machen, wahlweise in Hardware oder als virtuelle Maschine. Zusätzlich zum Routing ins öffentliche Internet bauen die Edge-Router untereinander Site-to-Site-VPN-Tunnel auf. Der Admin entscheidet per Mausklick, zwischen welchen Geräten Tunnel entstehen sollen. Links zur englischsprachigen Onlineliteratur über die im Folgenden genannten FlexiWAN-Komponenten haben wir unter ct.de/wgyr zusammengefasst.

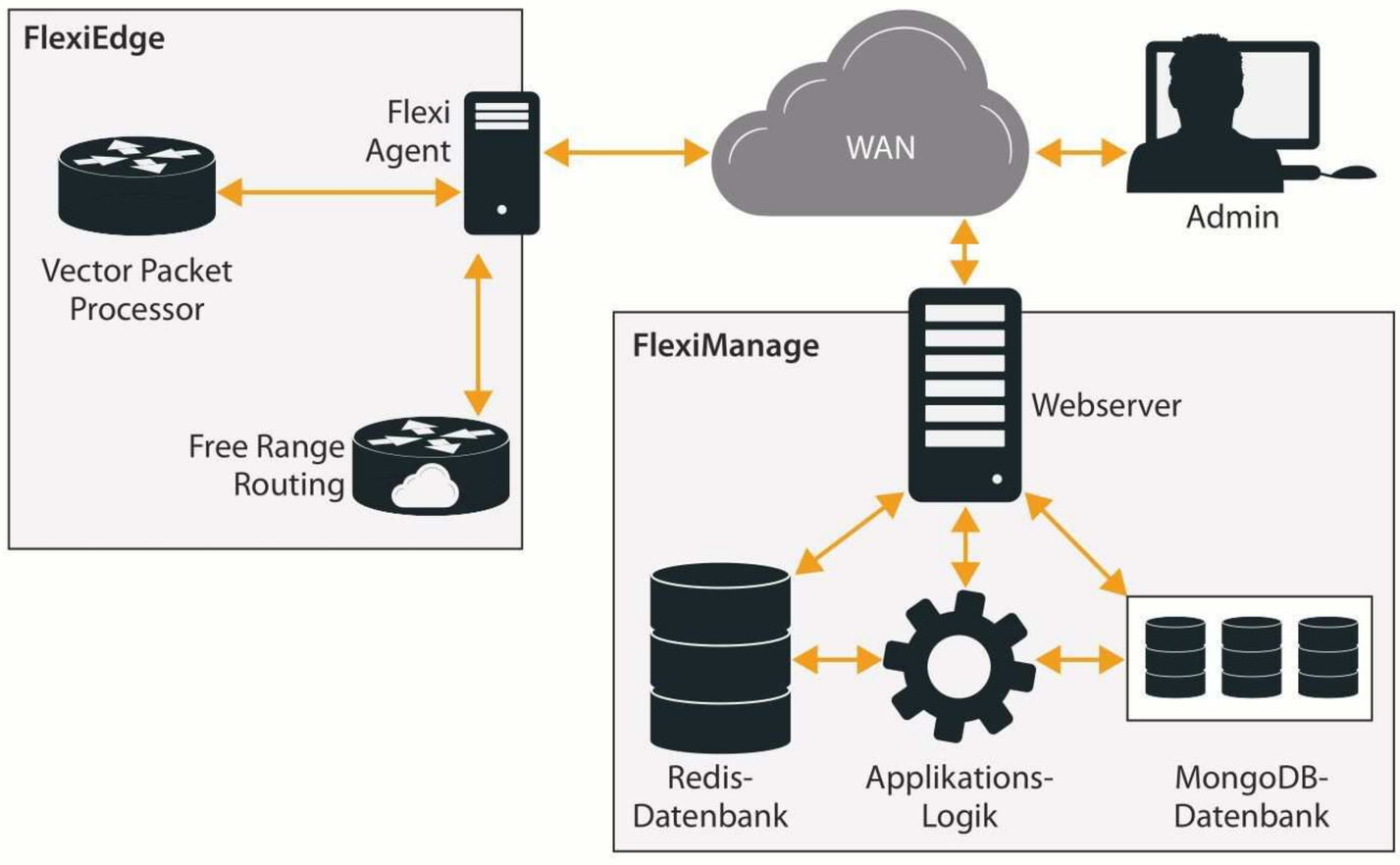
Wählerische Software

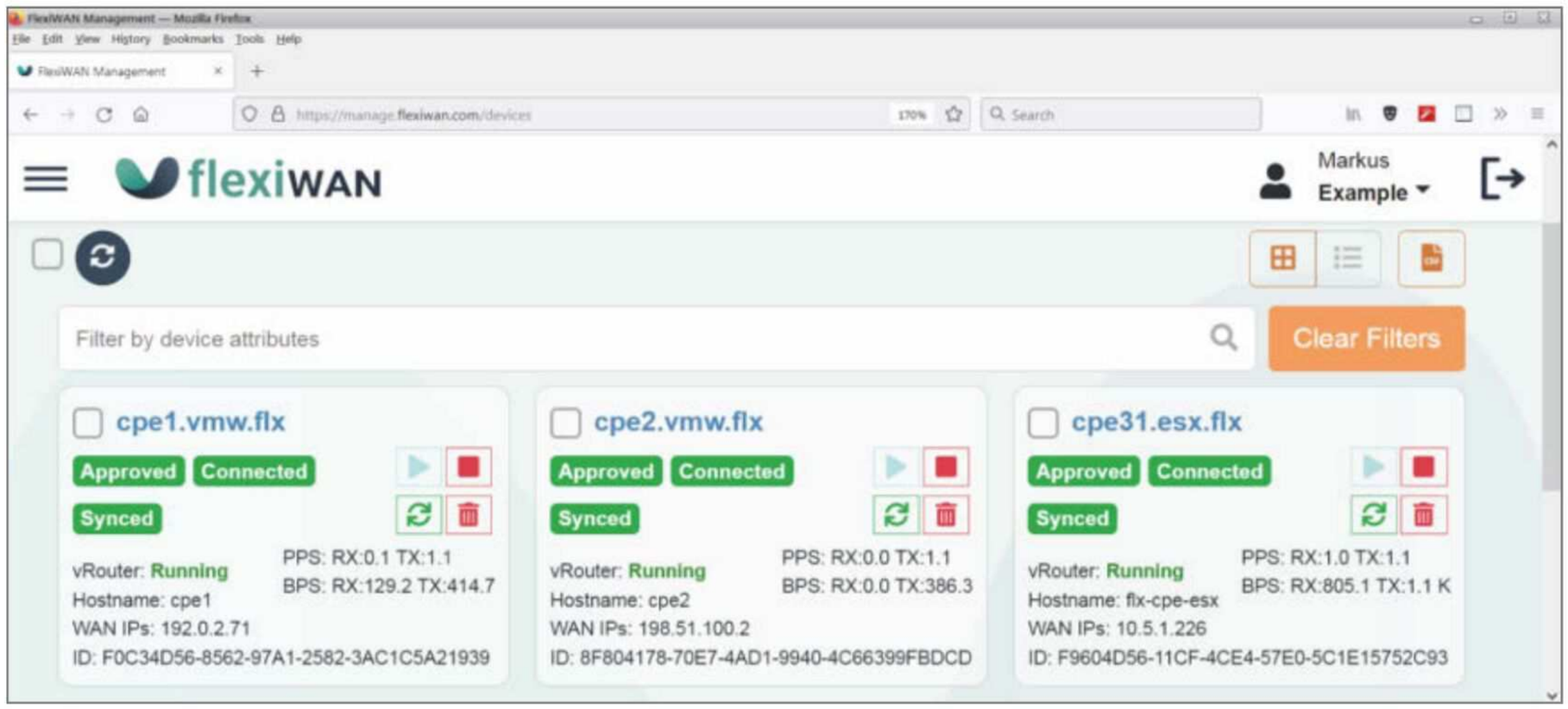
Für die Installation von FlexiEdge auf einem Linux-Rechner stellt der Anbieter den Quellcode und ein fertiges Paket bereit. Der zukünftige Router braucht mindestens: 2 CPU-Kerne, 4 GByte Arbeitsspeicher, 16 GByte Massenspeicher. Bei den Netzwerkadaptern ist FlexiEdge wählerisch: Es müssen mindestens zwei sein, die zum Data Plane Development Kit für Linux, FreeBSD und Windows kompatibel sind (DPDK, siehe ct.de/wgyr). Außer Exoten führt die Liste auch wohlbekannte Marken wie Intel oder Broadcom. Wer sich nicht selbst auf die Suche nach kompatibler Hardware begeben mag, findet passende Router-Appliances bei Vertriebspartnern, in Deutschland beispielsweise Landitec.

Als Linux-Unterbau für FlexiEdge ist nur Ubuntu-Server 18.04 LTS möglich. So weiß die Software genau, womit sie es zu tun hat. Installieren Sie Ubuntu-Server mit den Standardvorgaben, also englischer Spracheinstellung, damit sich FlexiWAN wohlfühlt. Die Installation ist mit zwei Zeilen auf der Kommandozeile erledigt:

FlexiWAN-Konzept

Bei FlexiWAN liegen die zu verteilenden Routing-Regeln in einer zentralen Datenbank. Sie werden über einen eigenen Webserver an die Edge-Router in den Firmenstandorten verteilt.





Bis die FlexiManage-Seite drei laufende FlexiEdge-Router zeigt, ist eine kleine Klickorgie fällig. Doch die ist viel kürzer, als alle Geräte in einer klassischen Installation einzeln zu konfigurieren.

```
curl -sL https://deb.flexiwan.com/\
setup | sudo bash -
sudo apt install flexiwan-router
```

Der erste Befehl bindet das FlexiWAN-Repository in die Ubuntu-Paketverwaltung ein, der zweite installiert die FlexiEdge-Software. Damit man anschließend die Ubuntu-Konfiguration in einem Rutsch anpassen kann, hat der Anbieter ein Goodie beigelegt: Das Tool `fwsystem_checker` prüft das System auf Kompatibilität, erkennt Abweichungen zu FlexiWANs Best Practices und korrigiert diese auf Wunsch.

Wenn der Router alle Prüfungen bestanden hat, geht es an die mit einem einzigen individuellen Eingriff erledigte Einrichtung. Der FlexiAgent braucht ein Token, das den Router in der Verwaltungskonsole dem richtigen Kundennetz zuordnet. Wie Sie das Token erzeugen, folgt ein paar Absätze weiter.

FlexiEdge enthält eine Weboberfläche, die auf dem Port 8080 horcht. Starten Sie einen beliebigen Browser, kontaktieren den Router über seine IP-Adresse (beispielsweise https://192.168.42.23:8080/) und melden sich mit einem routerlokalen Konto an. Im Menüeintrag „Settings“ hinterlegen Sie das Token. Damit ist der Router präpariert.

Zentrale, bitte melden

Der Cloud-Dienst FlexiManage ist der Fahrdienstleiter für das SD-WAN. Hier melden sich alle Router über das API, es entstehen Tunnel, Labels und Richtlinien. Wenn alles fertig ist, visualisiert das Dashboard das entstandene Netzwerk und liefert zu jedem beteiligten Netzadapter den Durchsatz.

Das Token für die WAN-Router erzeugen Sie im Webmenü bei „Inventory/Tokens“. Nach dem Klick auf „New Token“ geben Sie ihm noch einen Namen. Die anschließend erscheinende lange Zeichenkette kopieren Sie in die FlexiEdge-Webseite der Router.

Sobald sich ein Gerät mit dem Token meldet, erscheint es im Bereich „Devices“ als unbestätigtes Gerät. Erst wenn der Admin dem Neuling mit dem Umlegen des „Approved“-Schalters seinen Segen spendet, darf der Router im SD-WAN mitspielen. Dazu muss er auf den Namen des Routers klicken und findet den Schalter im „General“-Reiter unter Eigenschaften.

Bei „Interfaces“ erscheinen alle erkannten Netzadapter des Gerätes mit den konfigurierten IP-Adressen. Dort stellt man für jede Schnittstelle ein, ob sie am SD-WAN teilnimmt (Assigned = Yes) und welche Rolle sie dabei spielt: Internetverbindung (Type = WAN) oder internes Netz (LAN). Zwei wichtige Einschränkungen: IPv6 gibt es noch nicht. FlexiWAN spricht zwar auch PPPoE auf der WAN-Schnittstelle. Aber das muss man lokal konfigurieren und kann die Einstellungen später nicht ferngesteuert über FlexiManage ändern. Wir haben FlexiWAN nur mit DHCP ausprobiert.

Im DHCP-Reiter definiert man den im internen Netz des Routers zu vergebenden Adressbereich. „Update Device“ speichert schließlich die Konfiguration und schiebt sie zum Router. Kurz darauf wechseln die Anzeiger auf Grün, aber erst der Klick auf

den Play-Button startet im fernen FlexiEdge-Gerät den Routingprozess.

Tunnelbau

Bis jetzt haben die FlexiEdge-Taxis ihre Motoren zwar gestartet, aber warten noch auf Fahrgäste und Ziele. Die Interaktion zwischen den WAN-Inseln gestaltet FlexiWAN über Labels, Tunnel und Richtlinien. Ein Site-to-Site-Tunnel zwischen zwei oder mehreren Routern ist schnell angelegt: die beteiligten Router unter „Inventory/Devices“ anticken und den Tunnelwunsch bei „Actions/Create Tunnels“ aussprechen. Kurz darauf sendet FlexiManage den Arbeitsauftrag an die Geräte und präsentiert das Ergebnis bei „Inventory/Tunnels“.

Hier zeigt FlexiWAN vorauseilenden Gehorsam, denn die Tunnelendpunkte haben bereits IP-Adressen und die Subnetze der LAN-Segmente befinden sich in den Routingtabellen der FlexiEdge-Router. Ab jetzt können sich die Teilnehmer der lokalen Netze erreichen, als hätte ein Admin die Tunnel händisch gebaut.

Skaliert!

Bis hierhin bringt FlexiWAN noch keinen großen Vorteil gegenüber einem Admin mit flinken Fingern. Das ändert sich, sobald die Zahl der Router wächst. Bei sechs Standorten ist die Konfiguration der einzelnen Tunnel noch überschaubar: Falls alle miteinander schwätzen sollen, sind 15 Tunnel notwendig.

Wenn der Firmenverbund aber viele Niederlassungen umfasst, läuft der Konfigurationsaufwand schnell aus dem Ruder. Denn die Zahl der Links wächst exponentiell: Mit den bei 30 Standorten resultierenden 435 Tunneln hat FlexiManage eindeutig die Nase vorn. Will man sein SD-WAN dann um einen Router erweitern, benötigt FlexiManage gerade mal vier Mausklicks (nachgezählt!), um Verbindungen zu allen Partnern anzulegen.

Softwaresteuerung …

FlexiManage ist aber mehr als ein zentraler Konfigurationsgenerator für ein vermaschtes VPN. Das Attribut „Software-Defined“ verdient es sich mit der Steuerung der Pfadentscheidungen seiner Router. Per Konfigurations-Download lernen die FlexiEdge-Router binnen Sekunden ihre Regeln für die Firewall, Tunnel und Anwendungserkennung – die man freilich einmal zentral anlegen muss.

Hätte der Router nur eine einzelne Verbindung ins Internet, dann müsste er keine Pfadentscheidungen treffen. Typischerweise haben Firmenstandorte aber mehrere Uplinks, beispielsweise eine breitbandige Glasfaserleitung und eine günstige DSL-Verbindung als Ausfallreserve. Die SD-WAN-Richtlinie könnte dann geschäfts- und zeitkritische Anwendungen wie VoIP-Telefonie oder Datenbankreplikation über die Glasfaser schicken und den Pausenverkehr der Belegschaft vom Firmen-WLAN per DSL weiterleiten.

Dafür muss FlexiManage die Außenleitungen kennenlernen, wozu der Admin jedem als WAN markierten Netzwerkadapter ein oder mehrere Kennzeichen (Labels) verpasst, die er selbst bei „Inventory/Path Labels“ anlegt. Die Internetzugänge der Standorte könnten beispielsweise `wan1`, `wan2` et cetera heißen. Wenn eine Richtlinie ein solches Label enthält und WAN-Adapter dieses Label führen, dann übernehmen die Router diese Richtlinie für ihre lokalen Routingentscheidungen.

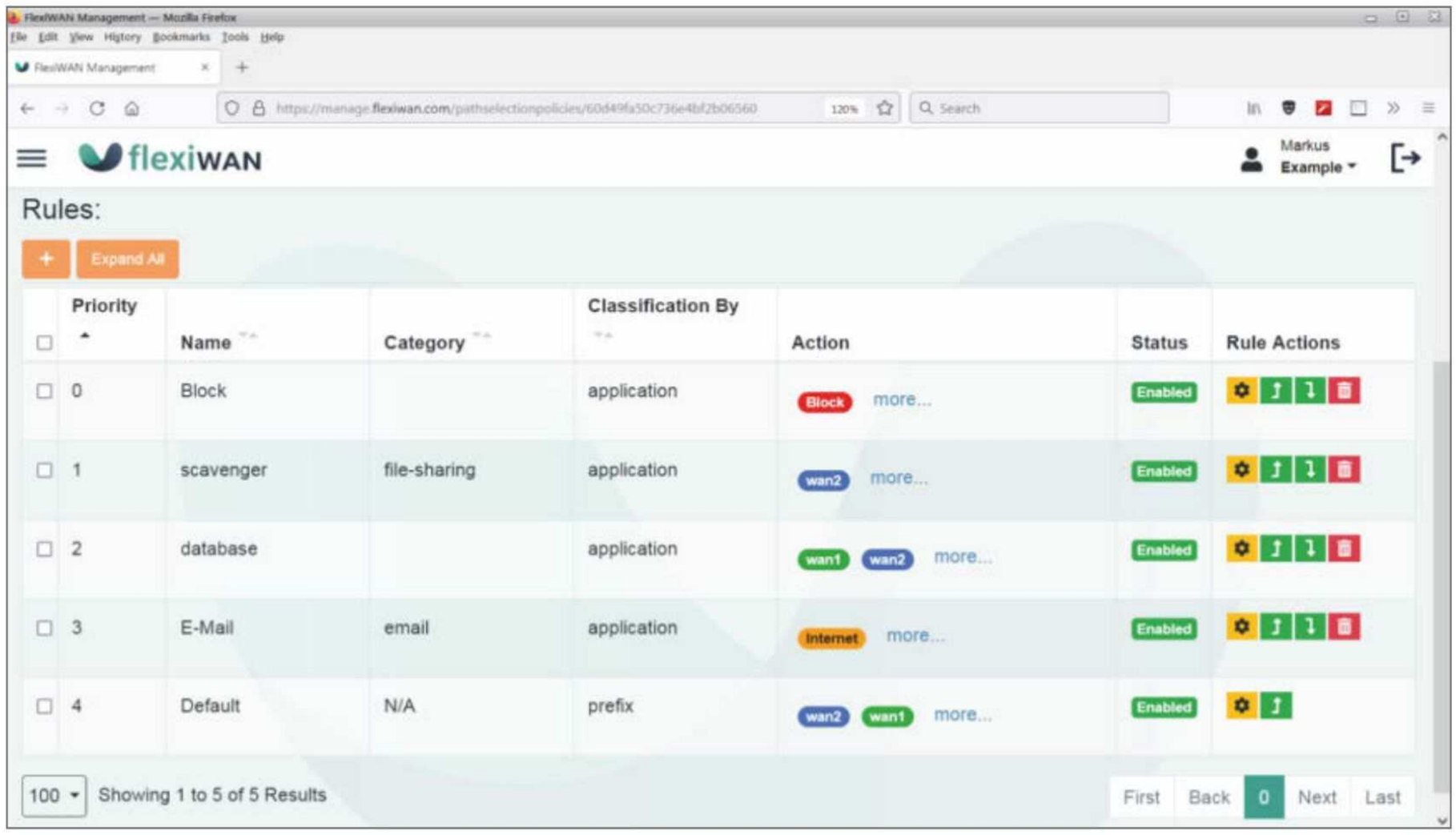
… konfigurieren

Bei „Path Selection“ geht es dann endlich in die SD-WAN-Denkfabrik: Ähnlich wie bei einer Firewall legen Sie fest, für welche Anwendungen oder IP-Bereiche Regeln gelten sollen (Traffic Classifier) und was bei einer Übereinstimmung geschehen soll (Action).

Die FlexiWAN-Entwickler haben praktischerweise über einhundert „App Identifications“ vorbereitet, sowohl einfache wie `https` für verschlüsselten Webverkehr oder `smtp` für zeitunkritische E-Mail als auch komplexe Konstrukte wie `file-sharing` oder `netflix`. Wie das System diese Dienste erkennt, kann man im „Inventory“ nachschlagen und den eigenen Vorstellungen anpassen.

Als Aktion einer Regel legt man eine Liste von Labels fest, deren zugehörige Netzadapter der Router für den Transport der Pakete einspannen darf. Dabei ist die Reihenfolge entscheidend: Die beispielhafte Richtlinie im Bild auf der nächsten Seite sendet Datenbankverkehr über alle Pfade mit dem Label `wan1` und allen anderen Traffic über `wan2`. Beide Labels geben sich gegenseitigen Ausfallschutz. Die oberste Regel mit dem Label `Block` – das keiner Schnittstelle zugewiesen ist – enthält alle gesperrten Dienste. Deren Verkehr verwerfen die Router.

Im letzten Schritt muss man die Richtlinie auf einen oder mehrere Router anwenden. Das passiert nicht automatisch, sondern verläuft wie beim An-



Die SD-WAN-Router vergleichen ausgehende IP-Verbindungen mit den Regeln der Richtlinie und erfahren so, welchen Pfad die Datenverbindungen nehmen sollen.

legen der Tunnel: Router bei „Inventory/Devices“ markieren, unter „Actions“ auf „Install Policy“ klicken. Nach ein paar Minuten haben die Geräte die Änderung übernommen.

Verteiltes Updaten

Wie jede Software erhält auch ein SD-WAN regelmäßig Updates. Um die Aktualisierung von FlexiManage auf seinen Servern kümmert sich der Anbieter. Bei den Edge-Routern muss deren Admin die Installation neuer FlexiEdge-Versionen unter „Inventory/Devices“ anstoßen: Router markieren und bei „Actions“ dann auf „Upgrade Device“ klicken.

Per „Schedule Device Upgrade“ lässt sich das auf einen Zeitpunkt verschieben, wo die kurze Dienstunterbrechung nicht stört, etwa tief in der Nacht. Allen, die das nicht regelmäßig tun, greift FlexiManage mit dem „Auto Upgrade“ unter die Arme, sobald der Softwarestand eines Routers älter ist, als der Hersteller toleriert.

Wichtig zu wissen: Nicht alle Updates sind abwärtskompatibel. Dann bleiben VPN-Tunnel zwischen zwei Routern unterschiedlicher Softwarestände offline und man muss alle Router auf den aktuellen Stand hieven.

Im Maschinenraum

Die FlexiWAN-Macher lassen den TCP/IP-Stack von Linux links liegen und greifen für den High-Speed-Paketversand zum Netzwerkstack des Open-Source-Projekts FD.io (ct.de/wgyr). Es setzt Ciscos Vector Packet Processor (VPP) als quelloffene Variante um. Darunter liegt Intels Data Plane Development Kit (DPDK), das Treiber und Bibliotheken für den Hardwarezugriff beisteuert. So kann sich VPP beispielsweise mehrere ähnliche Pakete bei der Netzwerk-I/O-Schicht abholen und gleichzeitig verarbeiten.

Der VPP-Dienst erhält seine Konfiguration von FlexiManage und wendet sie auf die lokalen Schnittstellen an. Das Verhalten kann man auf der Kommandozeile mit dem Befehl `vppctl` beeinflussen, der vom Monitoring bis zur Konfiguration alles leistet (ct.de/wgyr). Läuft VPP, dann ändern sich die Interface-Namen von den unter Ubuntu üblichen Bezeichnungen wie enp2s0 zu vpp0, vpp1 und so weiter.

LAN-seitig können die Router über das dynamische Routingprotokoll OSPF von benachbarten Geräten IP-Netze erfahren. Dahinter steckt das Softwareprojekt Free Range Routing (FRR), das neben OSPF noch zig weitere Protokolle drauf hat. Die

Konfiguration ist minimalistisch: Der OSPF-Daemon verkündet jedes Subnetz des LAN-Adapters und jedes WAN-Tunnels.

Die VPN-Tunnel bauen die FlexiEdge-Router per IPsec mit Generic Routing Encapsulation (GRE). Dieser Umweg ist unvermeidlich, weil OSPF seine Nachbarn per Multicast findet und pures IPsec kein Multicast transportiert. Das kostet nur ein paar zusätzliche Bytes im Paketheader. Die zweite Header-Erweiterung VXLAN ist weniger üblich, ermöglicht den Routern aber, unterschiedliche Datenströme leichter zu unterscheiden, beispielsweise um VoIP-Telefonate bevorzugt zu behandeln. Ob die Tunnel funktionieren, prüfen die VPN-Endpunkte per Ping und berichten die Paketumlaufzeit und Verlustrate zurück an den Aufpasser FlexiManage.

Eine kleine Anmerkung noch: Das Routing-Regelwerk fußt auf den „App Identification Rules“, die aus IP-Adressen und UDP/TCP-Ports bestehen. Eine Analyse der Anwendungsdaten (Deep Packet Inspection) findet nicht statt. So lässt sich eine Anwendung zwar erahnen, aber nicht zuverlässig erkennen.

Zentrale selbst bauen

Die Management-Ebene von FlexiWAN kann man auf eigener Hardware betreiben. Die Lizenzpolitik des Anbieters ist sogar so offen, dass der Code bei GitLab liegt und förmlich auf ein `git clone` lauert. Als Distribution eignet sich erneut Ubuntu, diesmal aber die aktuelle Version. Es kann auf eigener Infrastruktur oder auf virtuellen Servern von Anbietern wie OVH, Hetzner und anderen laufen. Wer Kosten bei der FlexiWAN-Probefahrt vermeiden will, erstellt sich bei Amazon AWS eine Instanz der Kategorie „12 Months Free“, der Typ „t2.micro“ genügt.

FlexiManage ist in JavaScript programmiert und benötigt die Node.JS-Laufzeitumgebung. Der Datenbestand kommt in einer MongoDB unter und Konfigurationszustände liegen in der In-Memory-Datenbank Redis. Zum Versenden von Benutzerregistrierungen per E-Mail braucht FlexiManage einen Mailerdaemon.

Die folgenden Anweisungen installieren alle benötigten Komponenten auf derselben Maschine und sind für eine Testumgebung unter Ubuntu gedacht. Für ein Produktivsystem sollte zumindest das MongoDB-Cluster auf verschiedenen VMs und unterschiedlichen Hosts laufen, damit Ausfallschutz besteht [1]. Falls die Zentrale doch mal abstürzt, arbeiten die FlexiEdge-Router mit ihrer lokal gespeicherten Konfiguration weiter.

Redis ist auf dem Ubuntu-Server als Root mit einem einzelnen Befehl installiert und gestartet: `apt install redis-server`. Für die Datenhaltung erwartet FlexiManage ein Replica-Set, bestehend aus drei MongoDB-Instanzen. Solch ein Konstrukt lässt sich mit drei Zeilen erstellen:

```
apt install npm
npm install run-rs -g --unsafe-perm
run-rs --keep
```

Das `--keep` bewirkt, dass der Datenbankinhalt einen Neustart übersteht. Bei der Mailserver-Konfiguration reicht ein SMTP-Dienst, der auf TCP-Port 25 Mails annimmt und als Textdatei im Dateisystem ablegt. Wir nahmen den Mini-Mailserver Dummy-SMTP, dessen Quellcode auf eine DIN-A4-Seite passt:

```
git clone https://github.com/Napsty/\
Dummy-SMTP.git
python Dummy-SMTP/listen.py
```

Damit sind die Voraussetzungen erfüllt und FlexiManage ist an der Reihe. Klonen Sie das öffentliche GitLab-Repository, bemühen den Installer und geben zuletzt den Startschuss:

```
git clone https://gitlab.com/flexi\
wangroup/fleximanage.git
cd fleximanage/backend
npm install
echo "127.0.0.1 $(hostname)" \
>>/etc/hosts
cp /usr/include/nodejs/openssl.cnf \
/etc/ssl/openssl.cnf
npm start
```

Wenn alles glattgeht, verbindet sich das FlexiManage-Backend mit der MongoDB, meldet sich bei Redis und stellt sein API auf TCP-Port 3443 bereit. Zwar gibt es keine Weboberfläche, aber FlexiManage ist trotzdem nutzbar, denn jeder Befehl des API ist dokumentiert und mit Beispielen versehen (ct.de/wgyr).

Wer auf die Weboberfläche von FlexiManage nicht verzichten will, kann über einen Trick den öffentlichen FlexiManage-Server mit der eigenen Instanz verknüpfen. Dazu muss der Browser – oder ein zwischengeschalteter Reverse-Proxy – die Anfragen an `/api` an die eigene Instanz senden und alle anderen Requests an manage.flexiwan.com weiterreichen. Das Ergebnis ist das Look-and-Feel von FlexiManage mit dem selbstgehosteten Unterbau. (ea) c't

Literatur

[1] Jan Mahn, **Wolkenformation**, Cloudserver redundant und flexibel im Cluster betreiben, c't 22/2021, S. 154

Literatur-Links

ct.de/wgyr

Glasfaser-Internet: Ausbau, Tarife, Technik

Kupfer ist am Anschlag, deshalb kommen nun Glasfasern ins Haus – mit Geschwindigkeitsreserven für viele Jahrzehnte. Der Wechsel lohnt sich schon heute, denn günstiger als aktuell kommt man in Zukunft nicht an einen Glasfaseranschluss.

Von **Ernst Ahlers**



Bild: Moritz Reichartz

Glasfaser-Internet steht vor der Tür	50
Glasfaser-Internet: Ausbau & Tipps	52
Glasfasertarife für Privatkunden	58
Die Technik des Glasfaser-Internet	64
FAQ: Per Glasfaser ans Internet	68
Fritzbox 5590 für Glasfaser-Internet getestet	72

Hätte jemand vor 10, 15 Jahren DSL mit 100 Mbit/s als langsam bezeichnet, hätte er Gelächter geerntet. Doch in der Pandemie mit Home-Schooling und Heimarbeit ruckelte es bei vielen Nutzern doch gelegentlich, wenn sie große Dateien auf einen Server schieben wollten. Mit den Umständen ändern sich eben auch die Ansprüche.

Wer jetzt von langsamem DSL auf einen Glasfaseranschluss umsteigt, der freut sich, dass die ganze Familie oder WG flotteres Internet bekommt und große Uploads zügiger laufen. Bei Videostreams in hoher Auflösung sind minutenlanges Puffern vorm Filmstart und Stocken mittendrin vergessen. Etwas weiter gedacht wird Glasfaser-Internet in zehn Jahren womöglich unverzichtbar sein, weil wir dann den halben Tag mit Virtual-Reality-Helm im Metaverse arbeiten und spielen.

Mitte 2022 konnte immerhin schon ein Viertel der bundesdeutschen Haushalte angeschlossen werden (Homes Passed, siehe Grafik). Wo die Internetanbieter nicht mal mittelfristig Interesse zeigen, können Kommunen und Bürgerinitiativen dank großzügiger Fördertöpfe selbst anpacken. So kommt die flinke Faser hoffentlich bald in jedes Haus (siehe Seite 52).

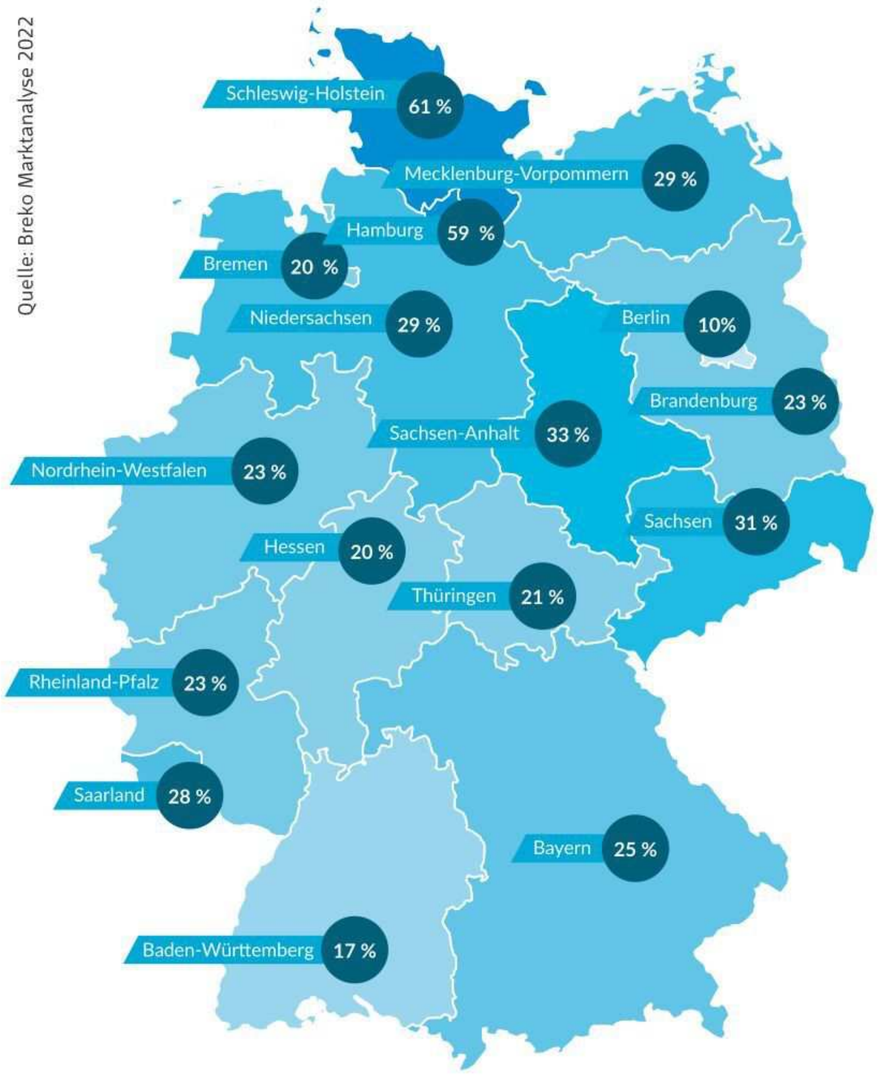
Falls Ihr Provider per Werbebrief oder E-Mail Glasfaser-Internet anbietet, prüfen Sie die Offerte. Es muss ja nicht gleich die Maximalgeschwindigkeit zum teuersten Tarif sein (Seite 58). Auch mit dem Basisangebot kommen Sie an den bei Ausbaukampagnen vergünstigten oder sogar kostenfreien Faseranschluss.

Anders als die Kupferader des DSL-Anschlusses hat die Faser genügend Reserven für steigenden Bedarf in den nächsten Jahrzehnten. Längst liegende Glasfasern können heute schon 10 Gbit/s liefern, während im Heimnetz noch 1 Gbit/s als Standard gilt. Zwar bauen sich komplexe Webseiten mit Elementen von vielen Servern damit auch nur wenig flotter auf und Insta-Chats werden nicht bunter. Aber wer jetzt nicht auf den Faser-Zug aufspringt, kommt vielleicht jahrzehntelang nicht mehr so günstig drauf.

Klingelt es an der Tür, dann vergewissern Sie sich, dass der Vertreter wirklich von Ihrem Anbieter kommt: Manchmal läutet eine Drückerkolonne, die Sie zum Wechsel von DSL aufs TV-Kabel drängen will, das im Maximum auch 1000 Megabit pro Sekunde bietet. Kabel-Internet ist aber weder so zukunftssicher wie die Faser noch so energieeffizient (Seite 64).

Vergleichen Sie das vorgelegte Angebot schließlich mit den Tarifen auf der Webseite des Providers. Selbst wenn alles passt, tauchen manchmal versteckte Hürden auf. Im Nebenhaus der Wohnung des Autors hat der Vermieter laut Anbieterwebseite dem Anschluss seines Gebäudes widersprochen. Beim Prüfen der Verfügbarkeit für das Haus erschien nämlich nur ein DSL-Angebot, obwohl links und rechts Glasfaser bestellbar war. Die Sperre wurde erst mit einem kleinen Trick ersichtlich: Wir fragten auf https://glasfaser.telekom.de/ unsere Adresse ab. In der folgenden Bestellseite variierten wir die Zahl im URL, bis die Seite die Nachbaranschrift anzeigte.

Falls Sie Mieter in einem solchen Objekt sind: Bewegen Sie den Eigentümer, sein Veto zurückzuziehen. Dem Argument des aktuell günstigeren Ausbaus dürfte er sich kaum verschließen, steigt doch dank der Glasfaser die Attraktivität und damit der Wert seiner Immobilie. Mit Glück profitieren auch Sie dann bald vom rasanten und effizienten Internet per Licht. Was Sie brauchen und wie das geht, folgt auf den nächsten Seiten. (ea) c't



Der Norden leuchtet: Mitte 2022 konnten rund 60 Prozent der Hamburger und Schleswig-Holsteiner Haushalte einen Glasfaseranschluss bekommen. Bundesweit war es im Schnitt jeder vierte (26 Prozent). Bis 2025 soll die Branche nach der Vorgabe der Bundesregierung die Hälfte erreichen.



Bild: Moritz Reichartz

Glasfaser-Internet: Ausbau & Tipps

Schnelles Internet gepaart mit langfristiger Zukunftstauglichkeit gibts nur per Lichtwellenleiter, und mittlerweile kommt auch in Deutschland der Glasfaserausbau ins Rollen. Über welche Wege Sie Ihren Anschluss erhalten und worauf Sie achten müssen, wenn die Installation ansteht, haben wir zusammengefasst.

Von **Andrijan Möcker**

Die Glasfaserleitung kommt langsam, aber sicher in deutsche Privathaushalte. Neue Förderpakete kurbeln derzeit den Ausbau an. Wer jetzt zugreift, bekommt seinen Anschluss kostenlos oder stark vergünstigt. Die Zeit dafür ist reif: Schließlich hat die Kupferdoppelader – die klassische Telefonleitung – als Standard-Medium für den Hausanschluss mittlerweile fast 140 Jahre auf dem Buckel. Während Lichtwellenleiter aus Glas in Weitverkehrsnetzen schon über 40 Jahre im Einsatz sind,

mussten sich Privatkunden insbesondere in Deutschland lange mit der Telefon- oder Koaxialleitung zufriedengeben. Mit den Übertragungstechniken ADSL, VDSL, G.fast und DOCSIS (Internet per TV-Koaxkabel) versuchten die Netzbetreiber das letzte bisschen Bandbreite aus der vorhandenen Infrastruktur zu pressen – nicht selten mit mäßigem Erfolg.

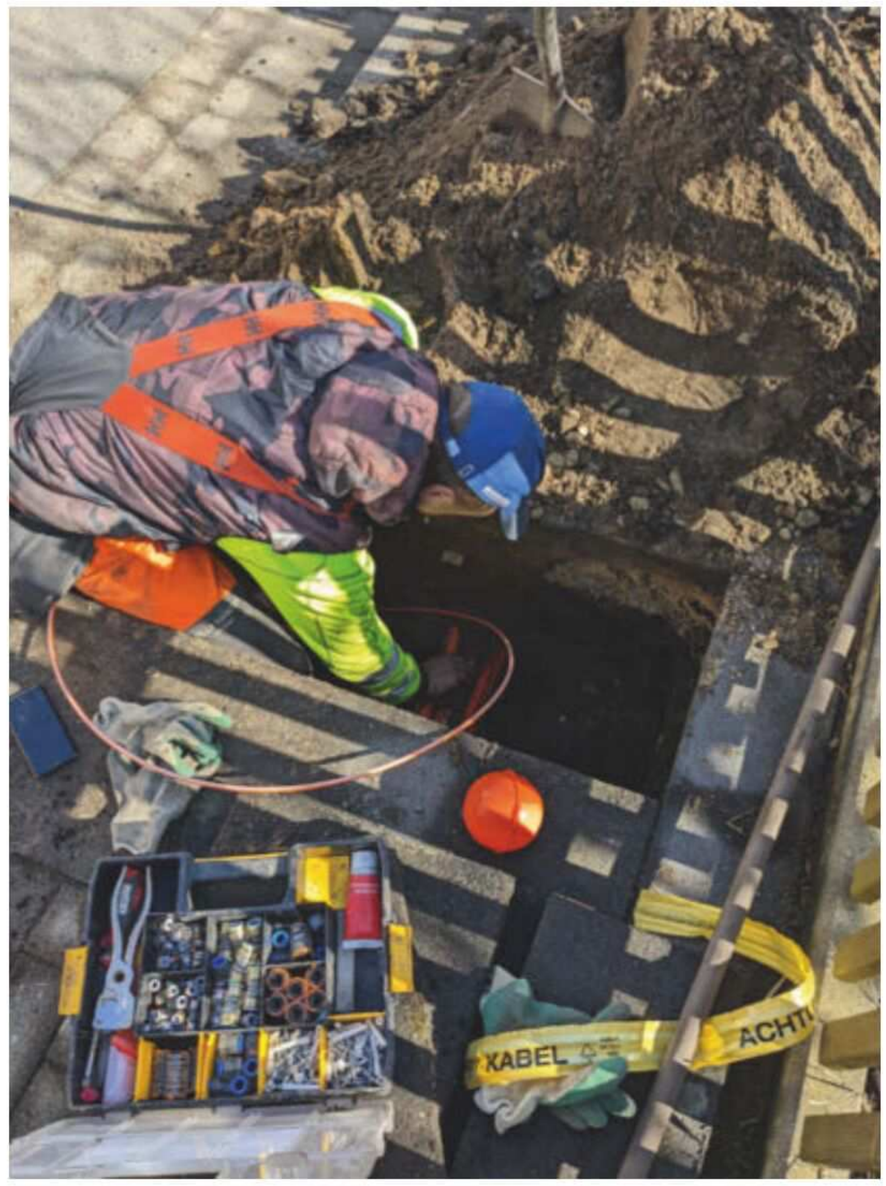
Dabei haben Glasfasern mehrere entscheidende Vorteile gegenüber der Kupfertechnik: Sie sind unempfindlich gegenüber Hochfrequenzstörungen und stören selbst keine anderen Medien. Bei xDSL, G.fast und DOCSIS können beispielsweise Powerline (Heimvernetzung über die Stromleitung), Gewitter oder defekte elektrische Geräte die Datenrate einbrechen oder gar die Verbindung abreißen lassen. Auch wer die Faser nur mit 50 oder 100 Mbit/s bucht, profitiert also von einer robusteren Verbindung.

Durch die geringe Dämpfung in der Faser spielt auch die Leitungslänge eine viel kleinere Rolle. Je nach Datenrate, Streckendämpfung und Wellenlänge sind Direktverbindungen bis 200 Kilometer oft kein Problem; für längere Strecken bereiten Repeater das Signal auf.

Außerdem ist die in einer Glasfaser verfügbare Bandbreite gigantisch: Privatkunden deutscher Anbieter erhalten derzeit maximal Gigabit-Anschlüsse (1 Gbit/Sekunde), aber das ist für die Faser das untere Ende der Fahnenstange. Der verbuddelte Fasertyp – meist OS2 oder vergleichbar – bietet je nach Länge bis zu 100 Terahertz, also 100.000 Gigahertz Bandbreite. Zum Vergleich: Die Übertragungstechniken VDSL und G.fast für Telefonleitungen nutzen 0,03 beziehungsweise 0,2 GHz und kommen damit auf 0,25 und 1 Gbit/s. Moderne Koaxialkabelnetze haben etwa 0,9 GHz Platz, aufgeteilt in Datendienste (DOCSIS) und Fernsehen (DVB-C).

Unternehmen setzen heute schon 400-Gbit/s-Glasfasermodule mit 40 Kilometern Reichweite ein. Mit Multiplexern kann man mehrere solcher Module an eine Faser koppeln und damit die Datenrate über die Terabit-Grenze treiben. Der aktuelle Rekord über vier Fasern liegt bei über einem Petabit pro Sekunde – das sind eine Million Gbit/s.

Zusammengefasst: Die Glasfaser ist unschlagbar zukunftstauglich. Investition und Aufwand werden sich wahrscheinlich für 40 bis 100 Jahre lohnen. Selbst wenn die heute verwendeten Fasern in einigen Jahrzehnten aus noch unbekannten Gründen nicht mehr genügen, kann man sie dank der installierten Mikrorohrsysteme leicht herausziehen und neue Medien einblasen – ohne erneut wie derzeit ganze Stadtteile umzugraben.



Netzbetreiber bauen ihre Infrastruktur heute fast ausschließlich mit Mikrorohrsystemen auf, in die die Glasfasern eingeblasen werden. Hier öffnet ein Tiefbauer ein zuvor verlegtes Mikrorohrbündel, um es mit dem Einzelrohr eines Hausanschlusses zu verbinden. Dafür wird ein kleines Kupplungsstück aufgeklemmt.

Anschlusssuche

In Mehrfamilienhäusern erfahren Sie vom Vermieter beziehungsweise der Eigentümergemeinschaft, ob bereits eine Glasfaserleitung im Haus liegt; oft wird sie bis in den Keller gelegt und erst bei Bedarf im Haus weiter nach oben. Eigenheimbesitzern ist der Anschluss in der Regel bekannt, denn ohne Erlaubnis bohrt diesen niemand in die Hauswand und beim Immobilien(ver)kauf wird der wertvolle Glasfaseranschluss gewiss im Inserat erwähnt. Anders als etwa beim Kupfernetz der Deutschen Telekom müssen Glasfaserbetreiber anderen Providern aber keinen Zugang gestatten. Man ist bei der Faser also meist gebunden und kann nicht frei unter mehreren Anbietern den günstigsten Tarif herauspicken.

Beim Glasfaserausbau in Deutschland herrscht ein wildes Durcheinander: Große Netzbetreiber wie die Telekom oder Vodafone stehen zwar im Rampenlicht, im Hintergrund gibt es jedoch viele kleinere Anbieter und Organisationen. Das reicht von regionalen Anbietern wie htp, Wobcom oder NetCologne mit einigen Tausend bis Hunderttausend Kunden bis hin zu kleinen Gemeinden oder sogar Bürgerinitiativen, die die Mikrorohrsysteme selbst in die Felder einpflügen und dann betreiben oder an einen Infrastrukturbetreiber vermieten oder verkaufen.

Steht der Glasfaserausbau in Ihrem Viertel kurz bevor, erfahren Sie meist früh genug davon, da Unternehmen vorab versuchen, möglichst viele Interessierte zu gewinnen und Initiativen um Unterstützer werben. Sie machen mit Briefen, Flyern und Hausbesuchen auf sich aufmerksam. Schauen Sie sich die Angebote unverzüglich genau an und bitten Sie Vertreter freundlich zur Tür herein; nur über einen gebündelten Ausbau bekommen Sie Ihren Anschluss günstig (500 bis 3000 Euro) oder sogar kostenlos. Lassen Sie die frühe Chance verstreichen, liegen die Rohre zwar unter Umständen schon vor der Haustür, ein späterer Einzelauftrag ist für den Tiefbauer aber wenig interessant und fällt in der Regel signifikant teurer aus.

Tut sich aktuell nichts, recherchieren Sie zunächst im Internet auf den Ausbaukarten der großen und der lokalen Anbieter. Geplante Ausbaugebiete und grobe Zeiträume finden Sie oft auf Anbieterwebsites, noch bevor die Vorvermarktung beginnt; in Interessentenlisten sollten Sie sich eintragen. Freuen Sie sich jedoch nicht zu früh, wenn der Ausbau angeblich kurz bevor steht, denn in vielen Fällen sind die Anbieter zu optimistisch und die Installation verzögert sich um Monate oder sogar Jahre.

Förderprogramme

Fehlende öffentliche Bekanntmachungen müssen nicht bedeuten, dass keine Pläne existieren. Immer öfter nehmen Kommunen den Glasfaserausbau selbst in die Hand. Ob im stillen Kämmerlein schon an Plänen geschmiedet wird, erfahren Sie von der zuständigen Verwaltung.

Unwahrscheinlich ist das nicht, denn mittlerweile existieren viele Fördertöpfe für den Glasfaserausbau auf Bundes- und Landesebene. Diese müssen nicht allein existierenden Netzbetreibern zufließen, auch Bürgerinitiativen und kommunale Netze sind oft förderfähig.

Eines der größten Programme ist die Graue-Flecken-Förderung auf Bundesebene, auch „Gigabit-Förderprogramm“ genannt. Der Geldtopf unterstützt den Ausbau privater Anschlüsse dort, wo weniger als 100 Mbit/s zuverlässige Downlink-Datenrate zur Verfügung stehen, die sogenannte „Aufgreifschwelle“, und umfasst 12 Milliarden Euro. Externe Beratungs- und Planungsdienstleistungen werden bis zu 100 Prozent finanziert; der Ausbau danach mit 50 bis 70 Prozent – jedoch maximal 150 Millionen Euro pro Projekt.

Ab 2023 entfällt die Aufgreifschwelle, sodass alle Kupferanschlüsse unter der Gigabit-Grenze profitieren. Öffentliche Infrastruktur wie Behörden, Schulen oder Krankenhäuser sowie kleine und mittlere Unternehmen mit weniger als 500 Mbit/s Downlink-Datenrate können schon jetzt gefördert werden.

Zusätzlich zur Bundesförderung haben viele Länder Förderprogramme aufgelegt. Bayern etwa fördert private Anschlüsse unter 100 Mbit/s Downlink-Rate sowie gewerbliche unter 200 Mbit/s (symmetrisch) mit 80 oder 90 Prozent. Die Finanzspritze ist auf drei beziehungsweise acht Millionen Euro pro Projekt beschränkt und wird nur dort angesetzt, wo Netzbetreiber mangels Wirtschaftlichkeit in den nächsten drei Jahren nicht ausbauen.

Sachsen hat Anfang Juli ein neues Förderprogramm mit rund 436 Millionen Euro im Topf aufgelegt. Der sächsische Topf kann, wie auch die Programme anderer Länder, mit der Bundesförderung kombiniert werden, um die Kosten zu 100 Prozent aus Fördermitteln zu decken.

Ist Ihre Verwaltung noch nicht tätig, können Sie das zum Anlass nehmen, in Ihrer Nachbarschaft um Interessenten zu werben und gemeinsam zu wirken. Der Prozess ist lang und braucht Arbeit, Sie sind aber nicht der Erste: Die Website ftth.blog liefert eine detaillierte Blaupause für eine Glasfaser-Bürgerinitiative zur Nachfragebündelung. Leben Sie in einer landwirtschaftlich geprägten Gegend, besteht vielleicht die Chance, den Ausbau selbst voranzutreiben (siehe ct.de/wvsv).

Wer das nötige Kleingeld mitbringt, kann einen Alleingang wagen: Manche regionalen Netzbetreiber und die Telekom bauen Glasfaseranschlüsse auch im Einzelauftrag. Wer Glück hat, zahlt „nur“ 10.000 bis 20.000 Euro. Doch sind die Leitungswege lang, kommen leicht sechsstellige Beträge zusammen. Oderbrück im Harz ist das Extrembeispiel: Dem Betreiber des abgelegenen Gasthauses „The Cabin“ an der Bundesstraße 4 schickte die Telekom 2017 einen Kostenvoranschlag über rund eine Million Euro.

Möchten Sie es schwarz auf weiß wissen: Das Angebot der Telekom heißt „Mehr Breitband für mich“ und das Vorabgespräch mit groben Preisschätzungen ist in der Regel kostenlos. Das individuelle Angebot kostet 500 Euro.

Installation

Wie am Ende ausgebaut wird und wie flott das geht, hängt stark von der vorhandenen Infrastruktur und den örtlichen Gegebenheiten ab. Gerade in seit Jahrzehnten oder Jahrhunderten bestehenden Wohngebieten bremsen durchaus mal Überraschungen im Erdboden wie alte Fundamente oder Verunreinigungen den Ausbau. Der Glasfaseranbieter wird sich also nicht lange vorher auf ein Installationsdatum festnageln lassen; die Vorlaufzeit für einen festen Termin beträgt unseren Erfahrungen nach zwischen acht und zwei Wochen.

Einfamilienhausinhaber müssen zwei bis vier Tage für die Arbeiten einplanen: einen Tag für die Erkundung durch das Tiefbauunternehmen und einen weiteren für das Verlegen des Mikrorohrs durch die Hauswand. Bläst der Installateur den Lichtwellenleiter nicht am selben Tag ein, kommt ein weiterer Tag hinzu, ebenso wenn ihm wichtige Komponenten fehlen. Anschließend endet die Glasfaser in einem neuen Kasten, dem Hausübergabepunkt (HÜP) mit einer Buchse. Wie und wo die Glasfaser ins Haus kommt, ist immer individuell; eine Wanddurchführung – sofern nicht schon vorhanden – gehört zum Installationspaket.

In Mehrfamilienhäusern veranschlagen die Netzbetreiber einen oder mehrere Erkundungstermine. Oft prüfen sie mehrere Wege, damit die Installation möglichst unkompliziert abläuft. Das geht am leichtesten über vorhandene Kabelschächte oder Aufputzkabelkanäle im Treppenhaus. Letztere werden bei Bedarf auch nachträglich eingebaut.

Zukunftsorientierte Eigentümer lassen bei der nächsten größeren Renovierung zwei bis vier OS2-Fasern pro Wohnung von einem IT-Systemhaus oder Elektrofachbetrieb legen und im Keller terminieren. So sind sie vorbereitet, wenn in ein paar Jahren die Glasfaser die Straße herunterkommt. Die verbindet der Installateur des Providers unkompliziert mit den im Keller ankommenden Fasern, was kosmetisch befriedigender ist als Aufputzkanäle in Wohnungsflur und Treppenhaus. Wichtig ist nur, dass die Infrastruktur am Ende der Eigentümergemeinschaft gehört, sonst drohen Zankereien zwischen den Netzbetreibern. In neuen Installationen kommt als Steckverbinder heute fast nur noch der Lampert beziehungsweise Lucent Connector (LC) zum Einsatz. Für andere Typen gibt es kurze Adapterkabel auf LC für wenige Euro.

Geschickt verkabelt

Die Glasfaser im Haus zum Aufstellort des Routers zu legen ist oft der kompliziertere Teil, denn während ein Loch, eine Dose und ein Kabelkanal an der Kellerwand nicht stört, möchte man das in Wohnräumen in der Regel nicht.

Es gibt mehrere Optionen von optimal bis Notlösung: Verlegen Sie bei einer Renovierung oder Sanierung Installationsrohr in den Wänden für günstige OS2-Patchkabel mit LC-Stecker; 20 Meter Duplex-Kabel (zwei Fasern) liegen bei 15 bis 20 Euro. Damit sind Sie auf den Glasfaseranschluss vorbe-



Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop



Bild: Jörg Wirtgen

Sie müssen nicht auf den Glasfaserausbau warten, um sich darauf vorzubereiten. In Mehrfamilienhäusern lohnt es sich, beim Neubau oder einer Sanierung eine eigene Glasfaserinfrastruktur einzuziehen, an die sich beliebige Provider anschließen können. Hier sitzen rechts die Wohnungsverteiler; in der Mitte und links steht htp- beziehungsweise Telekom-Technik.

reitet und haben auch gleich eine Reserve, denn Glasfaser-Internet kommt heute über eine einzelne Faser mit unterschiedlichen Wellenlängen für Downstream (Internet ins Haus) und Upstream (Gegenrichtung).

Zwei Kategorie-8-Twisted-Pair-Kabel für eine gleichzeitig oder später aufgebaute Kupfer-Hausverteilung passen im Installationsrohr problemlos neben die Glasfasern – so kommen am Aufstellort des Routers sowohl die Glasfaser als auch das verdrahtete Heimnetz an. Für beide Medien gibt es schicke Unterputzdosen. Im Anschlussraum enden die Leitungen in einem Keystone-Patchpanel, für das es sowohl RJ45- als auch LC-Duplex-Einsätze gibt. Diese Patchpanels erhalten Sie sowohl für 19-Zoll-Schränke als auch zur Wandmontage. Verzichten Sie keinesfalls auf das Rangierfeld, denn gerade bei Glasfaserkabeln verlängert eine Zugentlastung die Lebenszeit des Steckers. Diese Installation können viele Elektriker übernehmen.

Gleich das ganze Haus zu verglasen hat wenig Sinn, denn dass die Gerätehersteller fürs interne Netz (LAN) von Kupfer auf Glas umschwenken, zeichnet sich nicht ab. Mit Kategorie-8-Kabel ist man aktuell bis 40 Gbit/s bis 30 Meter Leitungslänge gerüstet, Hardware für 10 Gbit/s ist zwar schon bezahlbar, aber noch kein Sonderangebot. Nur wenn Ihnen so viel Luft nach oben nicht genügt, planen Sie jetzt schon diese Räume mit Installationsrohr für den späteren Austausch gegen Lichtwellenleiter.

Viele Netzbetreiber bringen zum Installationstermin bis zu 20 Meter Faser mit und legen diese kostenlos in vorbereitete Installationswege – um Letztere müssen Sie sich kümmern. Details zur kostenlosen Installation und Kosten für größere Längen erfahren Sie von Ihrem Anbieter. Oft handelt es sich um eine einzelne Faser, die man etwa hinter Fußleisten verstecken kann. Dann bekommt man oft eine weniger schicke Aufputzdose und geht diese Faser kaputt, gibt es keine Ausweichfaser zum Router. Für den Fall der Fälle sollten Sie sich ein Patchkabel mit passenden Steckern – in der Regel LC – und in passender Länge zur fliegenden Verkabelung in den Schrank legen.

Wenn kein Kabelweg zum Installationsort geschaffen werden kann, bleibt oft nur, den Medienkonverter (Glasfaser/Kupfer-Ethernet) vom Anbieter am HÜP installieren zu lassen und die vorhandene Infrastruktur mit Adaptern zu nutzen – und damit bis zur nächsten großen Renovierung zu leben.



Wer einen Glasfaseranschluss bucht, bekommt einen Medienkonverter oft für ein paar Euro Versandkosten fast geschenkt. Er versteht sich nicht nur mit dem Provider-Router: Damit können Sie Ihren alten Router weiterverwenden, falls dieser einen WAN-Port mit Gigabit-Ethernet hat und das WAN-Protokoll des Providers beherrscht.

Dann machen G.hn-, G.fast- oder MoCA-Medienkonverter Telefon- beziehungsweise Koaxialkabel netzwerktauglich – bei guter Leitungsqualität sogar über die Gigabit-Grenze hinaus [1]. Der Grundlagenartikel zu Ethernet-Alternativen (siehe S. 36) schildert, was es zu beachten gilt, wenn auf der Koaxial- oder Telefoninfrastruktur noch andere Signale laufen (Satelliten- oder Kabel-TV, Internet per TV-Kabel, Telefonie). Telefonkabel mit acht Adern transportieren manchmal sogar Gigabit-Ethernet über kurze Strecken [2].

Modem vs. Router

Trotz neuem Anschluss brauchen Sie nicht automatisch einen neuen Router: Viele Netzbetreiber geben Neukunden den Glasfasermedienkonverter – auch „Glasfasermodem“ genannt – kostengünstig oder kostenlos dazu. Er übersetzt das optische Signal auf handelsübliches Gigabit-Ethernet; seinen RJ45-Port verbinden Sie mit dem WAN-Port Ihres Routers. In der Regel ist die Leistungsaufnahme so gering (1 bis 5 Watt), dass sich ein neuer Router allein aufgrund der Stromkosten lange nicht rechnet.

Einige neuere Modelle der in Deutschland verbreiteten Fritzbox-Router für DSL-Anschlüsse haben solch einen WAN-Port als alternativen Internetzugang. Bei älteren ohne diese Buchse können Sie den ersten Port fürs interne Netz (LAN1) zur WAN-Schnittstelle umkonfigurieren. Router und Mesh-Sets ohne Modem, wie sie etwa von TP-Link oder Netgear vertrieben werden, funktionieren direkt am Medienkonverter – so sie das vom Provider genutzte Protokoll unterstützen. Vergewissern Sie sich dessen durch einen Anruf beim Herstellersupport oder Internetanbieter.

Wer mit der Glasfaser die gebuchte Datenrate nicht gleich vervielfacht, kann auf einen neuen Router wahrscheinlich verzichten. In c’t-Routertests finden Sie die reine IP-NAT-Datenrate sowie die mit PPPoE-Einkapselung in der Tabelle; um die Technik auszureizen, führen wir diese Messungen in der Regel am Gigabit-WAN-Port durch, sodass die Werte auf den Betrieb am Medienkonverter übertragbar sind. So können Sie nachschauen, ob Ihr Router noch für die gebuchte Geschwindigkeit taugt.

Möchten Sie Datenraten über 250 Mbit/s auch im WLAN erreichen, müssen Sie sich wahrscheinlich um Ihre Funknetzausstattung Gedanken machen. Wi-Fi 6 liefert die Datenrate und wir in c’t 3/2021 das nötige Grundwissen [3]. (amo) c't

Literatur

[1] Ernst Ahlers, **Koax-Express**, Kurztest goCoax MA2500D, c’t 5/2022, S. 80

[2] Andrijan Möcker, **Alles Kabel!**, Grundwissen Heimnetzverkabelung: Von Notlösung bis professionell, c’t 26/2020, S. 132

[3] Andrijan Möcker, **Flottfunk**, Wann sich Wi-Fi 6 für Sie lohnt, c’t 3/2021, S. 16

Infrastruktur-Initiativen, Einzelausbau

ct.de/wvsv

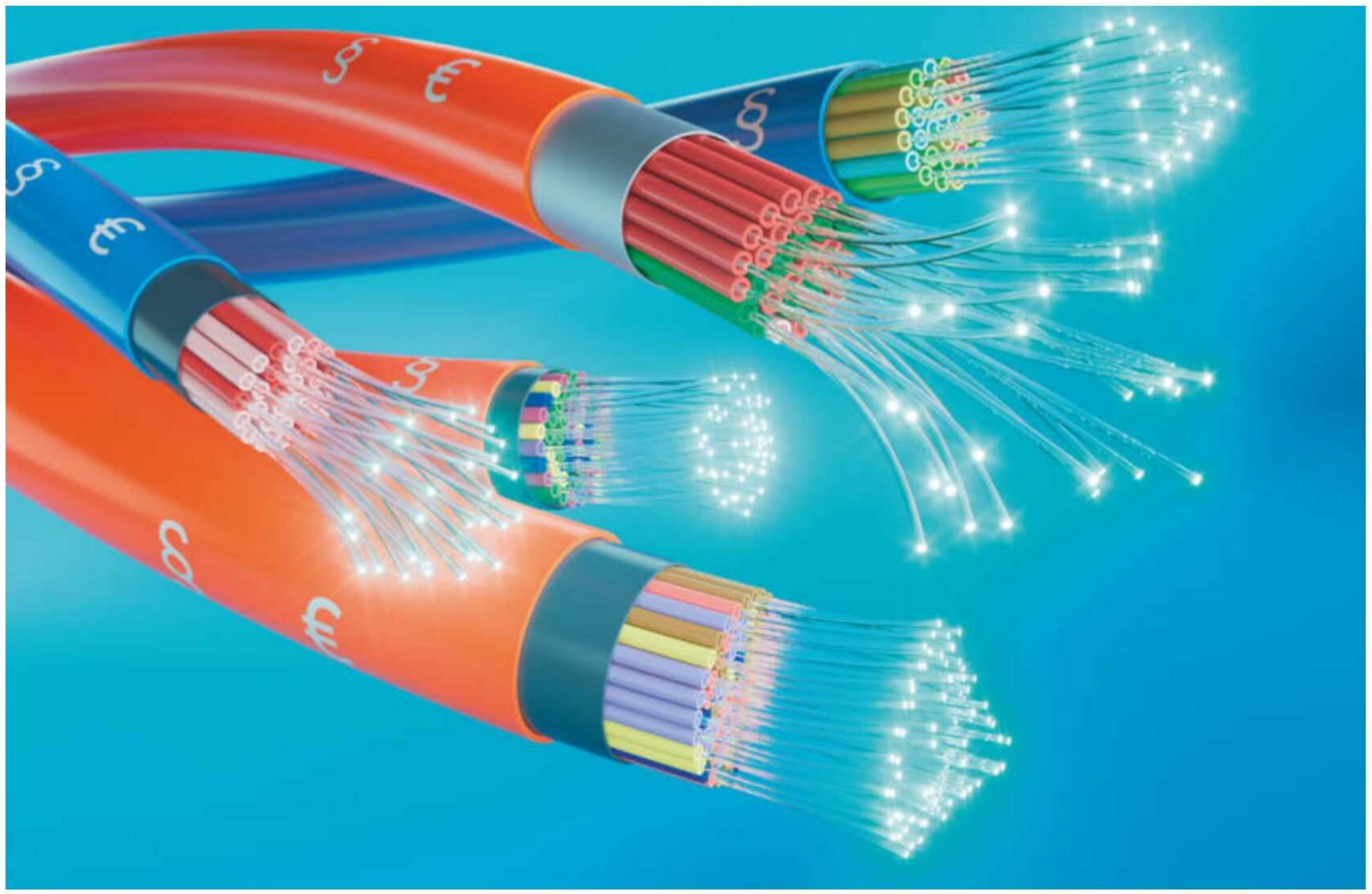


Bild: Moritz Reichartz

Glasfasertarife für Privatkunden

In sehr vielen Haushalten wird schnelles Internet per Glasfaser verfügbar. Um von der neuen Technik zu profitieren, müssen Sie einen neuen Vertrag abschließen und dabei einige Besonderheiten beachten. Wir haben die Details sortiert.

Von **Urs Mansmann**

Der Glasfaserausbau läuft auf Hochtouren: Mit 4,4 Millionen neuen Anschlussmöglichkeiten in 18 Monaten hat Deutschland Ende Juni 2022 die Marke von einem Viertel per Glasfaser erreichbaren Haushalten erreicht, so der Branchenverband Breko Anfang September. Und es geht weiter: In vielen Kommunen graben Bagger, werden Leerrohre gelegt und Fasern eingeblasen. In ein paar Jahren wird der Glasfaseranschluss so selbstverständlich sein wie heute DSL oder TV-Kabel.

Für den Kunden bedeutet der Umstieg in der Regel den Abschluss eines neuen Vertrags. Eigenheimbesitzer bekommen in vielen Fällen nur dann einen kostenlosen Glasfaseranschluss, wenn sie auch einen Zweijahresvertrag für den Internetzugang abschließen. Anders sieht es in Mehrfamilien-

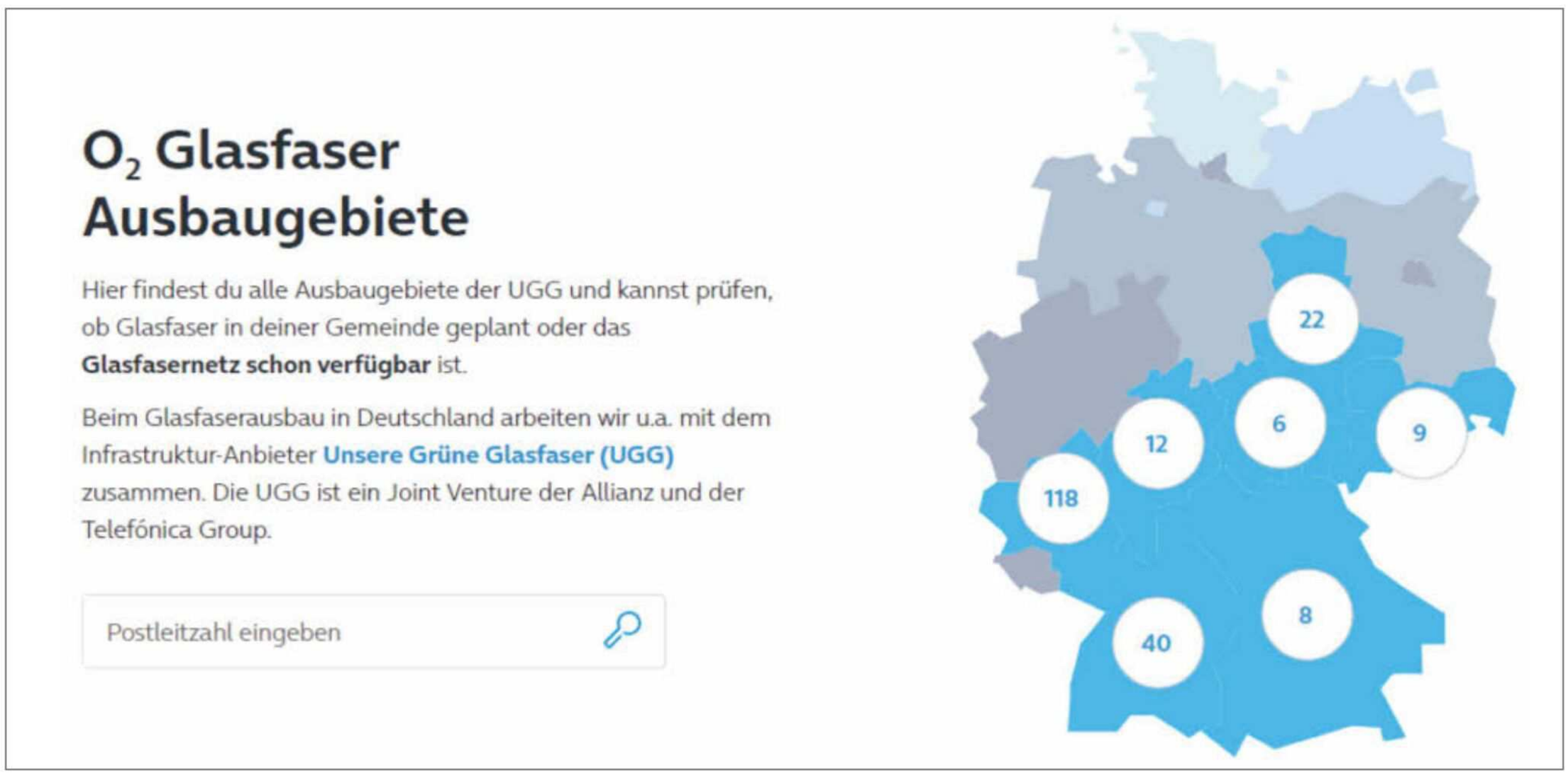
häusern aus: Der Aufwand pro Wohnung ist hier geringer, bei der Erschließung wird deshalb üblicherweise jede Wohnung angeschlossen, auch wenn der Eigentümer oder Mieter zunächst kein Glasfaser-Internet bucht. Wer als Hauseigentümer einen kostenlosen oder günstigen Glasfaseranschluss angeboten bekommt, sollte zuschlagen, denn eine spätere Verlegung wird möglicherweise erheblich teurer.

Bislang haben Glasfaserkunden bei den Tarifen in den meisten Fällen wenig Auswahl. Der Internetzugang kommt üblicherweise von dem Unternehmen, das ihren Anschluss gelegt hat, eine Alternative gibt es nicht. Anders als beim DSL-Internet übers Telefonkabel zwingt die Bundesnetzagentur die Betreiber nicht, ihre Leitungen an Konkurrenten zu vermieten. Denn die Richtlinien, wann eine marktbeherrschende Stellung vorliegt, sind auf den Ex-Monopolisten Telekom zugeschnitten, dem das komplette staatliche Netz aus Kupferanschlussleitungen in jedem Haushalt in den Schoß fiel.

Doch offenbar entsteht auch ohne Eingriffe des Regulierers Wettbewerb. 2016 schloss 1&1 eine erste Kooperation mit dem Internetanbieter Wilhelm.tel (Norderstedt), um Glasfaseranschlüsse zu verkaufen. Im Juni 2022 verkündeten dann 1&1 und die Telekom ihre Zusammenarbeit. Und auch lokal arbeiten immer öfter mehrere Firmen zusammen, etwa in Münster die dortigen Stadtwerke mit der Telekom. Dort vertreiben beide Unternehmen Glasfaseranschlüsse. In solchen Gebieten hat der Kunde die Wahl zwischen verschiedenen Providern, die einen Internetzugang über seinen Hausanschluss anbieten.

Offene Vermarktung

Inzwischen setzen erste Unternehmen offensiv auf eine solche offene Vermarktung: Telefónica hat zusammen mit dem Versicherungskonzern Allianz das Gemeinschaftsunternehmen „Unsere Grüne Glasfaser (UGG)“ gegründet. Laut der Webseite ist der Ausbau in 200 Ortsnetzen geplant oder bereits in Arbeit. UGG bietet die offene Infrastruktur interessierten Vertriebspartnern an. Deshalb verkauft nicht nur O2 UGG-Glasfaseranschlüsse, sondern auch die regionalen Unternehmen Stiegeler in Südbaden



O2 will in naher Zukunft in über 200 Ausbaugebieten Glasfaseranschlüsse anbieten.

und Eifel-DSL in der Eifel, an der Mosel und im Hunsrück. Sie werden vermutlich nicht die einzigen bleiben.

Mit harten Bandagen gingen Mitbewerber gegen den Zusammenschluss von Telekom und EWEtel für den Netzausbau im Nordwesten vor. Vodafone und Deutsche Glasfaser griffen die Genehmigung des Bundeskartellamts für „Glasfaser Nordwest“ per Klage an und gewannen vor dem OLG Düsseldorf. Das Verfahren ist noch nicht abgeschlossen. Der Ausbau im Nordwesten geht zwar wie geplant weiter, aber möglicherweise muss das Kartellamt beispielsweise die Rahmenbedingungen für den Netzzugang ändern.

Glasfaseranschlüsse für Privatkunden (Auswahl)

Anbieter	1&1	1&1	Deutsche Glasfaser	Deutsche Glasfaser	O2	O2	Telekom	Telekom
Tarif	Glasfaser 50 (100) MBit/s	Glasfaser 250 (1000) MBit/s	DG basic 300 (classic 400)	DG premium 600 (giga 1000)	O2 my Home M (L)	O2 my Home XL (XXL)	MagentaZuhause M12 (M, L)	MagentaZuhause XL (XXL, Giga)
URL	dsl.1und1.de	dsl.1und1.de	deutsche-glasfaser.de	deutsche-glasfaser.de	glasfaser.o2online.de	glasfaser.o2online.de	glasfaser.telekom.de	glasfaser.telekom.de
Anschlussart	Glasfaser (GPON)	Glasfaser (GPON)	Glasfaser (AON, GPON)	Glasfaser (AON, GPON)	Glasfaser (k. A.)	Glasfaser (k. A.)	Glasfaser (GPON)	Glasfaser (GPON)
Leistungen/Optionen								
Bandbreite Down- / Upstream Mbit/s	50 / 10 (100 / 50)	250 / 50 (1000 / 200)	300 / 150 (400 / 200)	600 / 300 (1000 / 500)	100 / 40 (250 / 50 (125))	500 / 100 (250) (1000 / 200 (500))	50 / 10 (50 / 10, 100 / 50)	250 / 50 (500 / 100, 1000 / 200)
normalerweise verfügbare Bandbreite Down- / Upstream[1] Mbit/s	50 / 10 (100 / 50)	250 / 50 (850 / 200)	300 / 150 (400 / 200)	600 / 300 (900 / 450)	83 / 33 (40) (200 / 40 (100))	400 / 80 (200) (800 / 160 (400))	50 / 10 (50 / 10, 100 / 50)	250 / 50 (500 / 100, 850 / 200)
Mindestbandbreite Down- / Upstream[1] Mbit/s	45 / 8 (80 / 45)	200 / 45 (700 / 200)	240 / 120 (320 / 160)	480 / 240 (750 / 375)	50 / 10 (23) (105 / 23 (56))	200 / 45 (113) (400 / 90 (225))	50 / 10 (50 / 10, 100 / 50)	250 / 50 (400 / 80, 700 / 200)
öffentliche IPv4-Adresse / IPv6-Präfixgröße	✓ / /56	✓ / /56	– / /56	– / /56	– / /56	– / /56	✓ / /56	✓ / /56
Telefonanschlussart / gleichzeitig. Gespräche / Rufnummern	VoIP / 2 / 3 (VoIP / 2 / 5)	VoIP / 2 / 8 (VoIP / 2 / 10)	VoIP / 1 / 1 (VoIP / 1 / 1[2])	VoIP / 1 / 1[2]	VoIP / 1 / 1[2]	VoIP / 1 / 1[2]	VoIP / 2 / 3	VoIP / 2 / 3
Vertragskonditionen								
Störungsannahme (Rufnummer)	Festnetz (07 21/96 00)	Festnetz (07 21/96 00)	Festnetz (0 28 61/89 06 00)	Festnetz (0 28 61/89 06 00)	Festnetz (0 89/7 87 97 94 00)	Festnetz (0 89/7 87 97 94 00)	kostenlos (08 00/3 30 10 00)	kostenlos (08 00/3 30 10 00)
Laufzeit / Verlängerung / Kündigungsfrist (Monate)	24 / 1 / 1	24 / 1 / 1	24 / 1 / 1	24 / 1 / 1	0 / 1 / 1	0 / 1 / 1	12 / 1 / 1 (24 / 1 / 1, 24 / 1 / 1)	24 / 1 / 1
günstigste mitgelieferte Hardware ONT	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos	49,99 € einmalig	49,99 € einmalig
günstigste mitgelieferte Hardware Router	WLAN-Router, 4,99 €/Monat, 9,90 € einmalig[3]	WLAN-Router, 4,99 €/Monat (6,99 €/Monat), 9,90 € einmalig[3]	WLAN-Router, 2,99 €/Monat, 9,99 € einmalig[3]	WLAN-Router, 2,99 €/Monat, 9,99 € einmalig[3]	WLAN-Router, 3,99 €/Monat, 9,99 € einmalig[3]	WLAN-Router, 3,99 €/Monat, 9,99 € einmalig[3]	WLAN-Router, 6,95 €/Monat, WLAN-Router mit Modem 7,95 €/Monat[3]	WLAN-Router, 6,95 €/Monat, WLAN-Router mit Modem 7,95 €/Monat[3]
Telefonanschluss / Festnetz-Flat / Allnet-Flat monatlich	inklusive / inklusive / 9,99 €	inklusive / inklusive / 9,99 €	inklusive / – (inklusive) / –	inklusive / inklusive / inklusive	inklusive / inklusive / inklusive	inklusive / inklusive / inklusive	inklusive / inklusive / –	inklusive / inklusive / –
Kosten								
Einmalkosten oder Gutschriften[4]	189,99 (269,94) € Gutschrift	299,94 (419,94) € Gutschrift	240 (300) € Gutschrift	660 (780) € Gutschrift	49,99 € Kosten (120 € Gutschrift)	49,99 € Kosten	69,95 € Kosten (0,05 € Gutschrift)	0,05 € Gutschrift (0,05 € Gutschrift, 69,95 € Kosten)
Internet-Anschluss, monatlich	39,99 (44,99) €	49,99 (69,99) €	44,99 (49,99) €	79,99 (89,99) €	34,99 (39,99) €	49,99 (79,99) €	44,95 (39,95, 44,95) €	54,95 (59,95, 79,95) €

[1] Herstellerangabe laut Produktinformationsblatt [2] mehr Rufnummern und mehr gleichzeitige Gespräche gegen Aufpreis [3] Router muss nicht mitbestellt werden, Preis inkl. Versandkosten
[4] bei Online-Bestellung, Gebühren-Gutschriften gerechnet für zwei Jahre Laufzeit ✓ vorhanden – nicht vorhanden k. A. keine Angabe

Mehr Leistung

Wenn in Ihrer Wohnung bereits Glasfaser verfügbar ist, müssen Sie in Erfahrung bringen, wer Ihnen darüber einen Internetzugang anbieten kann. Wenn das Unternehmen, das Ihr Haus erschlossen hat, diesen nicht selbst anbietet, wird es zumindest Informationen bereithalten, wo Sie einen Internetzugang buchen können. Wenn Sie da nicht weiterkommen, können Sie die Verfügbarkeit auf den Webseiten aller infrage kommenden regionalen und überregionalen Unternehmen prüfen.

Wenn Sie von einem DSL- oder TV-Kabelanschluss auf Glasfaser umsteigen, müssen Sie nicht unbedingt einen schnellen, aber teuren Gigabit-Tarif wählen. Vielerorts gibt es Einsteigerangebote mit 50 bis 100 Mbit/s für unter 50 Euro monatlich, die ungefähr so viel kosten wie ein gleichwertiger DSL- oder Kabelanschluss.

Gigabit-Anschlüsse mit erheblich mehr Leistung kosten meist knapp unter 100 Euro im Monat. Achten Sie bei der Auswahl auch auf den Upstream, dessen Datenrate auch bei Glasfaseranschlüssen oft um ein Vielfaches geringer ausfällt als der Downstream. Wenn Sie beispielsweise zu mehreren im Homeoffice arbeiten oder häufig große Datenmengen in die Cloud hochladen, sind 10 Mbit/s im Upstream sehr knapp bemessen.

Selbst bei nominell gleicher Datenrate des alten und neuen Anschlusses lohnt der Umstieg auf die neue Technik. Die praktisch erreichte Datenrate ist bei Glasfaseranschlüssen oft höher. Statt „bis zu“ findet man in der Produktbeschreibung oft ganz konkrete Angaben. Die Anbieter garantieren also dafür, dass die gebuchte Datenrate stets beim Kunden ankommt. Obendrein sind Glasfaseranschlüsse gegen äußere Störeinflüsse sehr viel unempfindlicher als DSL- oder Kabelanschlüsse. Die Anbieter versprechen, dass die Anschlüsse dadurch stabiler laufen.



1&1 verlangt für Glasfaseranschlüsse einen Aufschlag von 5 Euro im Monat gegenüber gleichschnellen DSL-Anschlüssen.

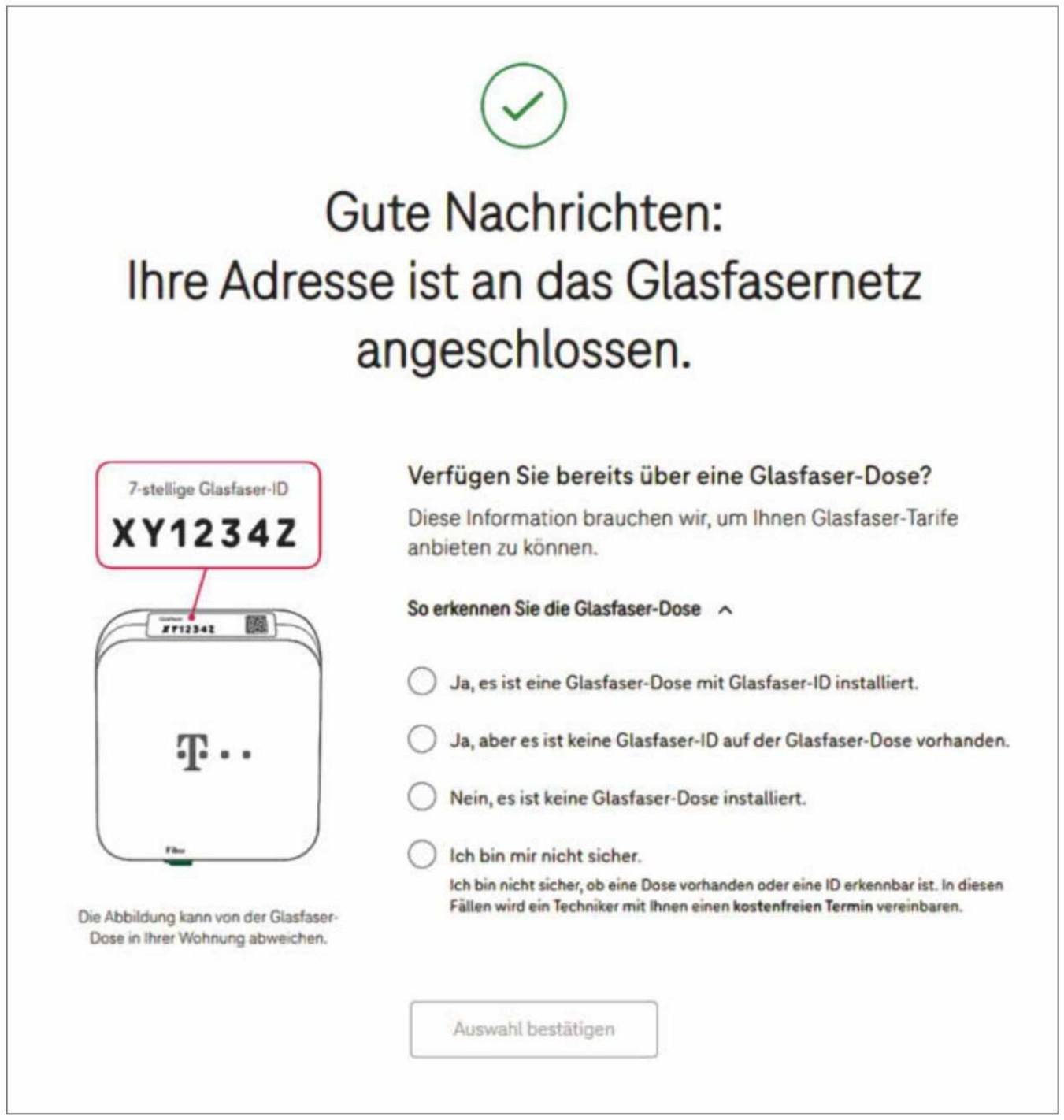
Schnelle Hardware

In einen neuen Router müssen Sie nicht unbedingt investieren: Vorhandene DSL-Router lassen sich oft auch an einem LAN-Anschluss betreiben, das interne DSL-Modem wird in dieser Konfiguration arbeitslos. Üblicherweise stellen die Anschlussprovider standardmäßig, aber mindestens auf Wunsch, einen ONT bereit (Optical Network Termination), mitunter auch als Medienwandler oder Glasfasermodem bezeichnet. An dessen 1-Gbit/s-Ethernet-Buchse können Sie einen beliebigen Router anschließen, solange er das WAN-Protokoll des Anbieters spricht.

Zu schwachbrüstig sollte der alte Router aber nicht sein, denn sonst können Sie den Vorteil der schnellen Anschlüsse nicht ausspielen. Vorteil der ONT-Lösung ist, dass Sie jeden beliebigen Router mit LAN-Anschluss einsetzen können. Nachteil ist, dass der ONT zusätzlich zum Router Strom verbraucht, auch wenn es meist nur wenige Watt sind.

Wenn Sie einen neuen Router beschaffen, können Sie diesen auch direkt mit dem Glasfasernetz verbinden. Dabei müssen Sie aber die Technik Ihres Hausanschlusses kennen, GPON oder AON (siehe auch Seite 64), und einen passenden Router besorgen. Künftig könnten auch andere Varianten zum Einsatz kommen, die Telekom testet derzeit schon FTTH-Zugänge mit 10 Gbit/s (XGS-PON). Wechselt die Anschlusstechnik, muss der optische Transceiver im Router oder der vorgeschaltete ONT ausgetauscht werden. In GPON-Netzwerken ist wie bei TV-Kabelnetzen die Anmeldung des Routers beim Provider erforderlich, da an einem Anschluss mehrere Kunden hängen und die Daten verschlüsselt übertragen werden.

Wenn Sie den Router mieten, haben Sie die Garantie, dass das Gerät an Ihrem Anschluss korrekt funktioniert. Meistens kommt es vorkonfiguriert bei Ihnen an und muss nur noch nach Anleitung angeschlossen werden. Im Laufe der Jahre kommen für die Mietzahlungen zwar größere Summen zu-



Die Telekom fragt bei Online-Aufträgen die Nummer der Glasfaserdose ab, an die später ONT oder Router angeschlossen werden.

sammen, dafür müssen Sie aber keine Rücklagen für eine Neubeschaffung bilden, denn der Provider muss ja dafür sorgen, dass Ihr Gerät funktionstüchtig ist, und es bei Defekten austauschen.

Richtig wechseln

Wenn Ihr bisheriger Zugangsprovider die vorhandene Kupferverkabelung durch Glasfaser ergänzt oder ersetzt, ist der Umstieg einfach und wenig fehleranfällig. Anders sieht es aus, wenn Sie zu einem neuen Anbieter wechseln wollen: Falls die Mindestvertragslaufzeit beim alten Anbieter noch nicht abgelaufen ist, müssen Sie diese abwarten und können erst zum Ende wechseln – oder müssen eine Zeit lang doppelt bezahlen.

Kündigen Sie den bestehenden Anschluss nicht selbst, denn damit verlieren Sie die Garantie, dass Sie bei Problemen weiter vom alten Anbieter versorgt werden und gefährden die Mitnahme (Portierung) Ihrer Festnetznummern. Am besten schließen Sie den neuen Vertrag ab und beauftragen den neuen Anbieter, die Kündigung beim alten Provider vorzunehmen. Die erfolgt dann automatisch zu einem Termin, zu dem die neue Leitung schon steht. Im Idealfall müssen Sie nur den Router vom alten Kupferanschluss an den ONT umhängen, gegebenenfalls noch umkonfigurieren und sind sofort wieder online.

Fazit

Für Glasfaser-Internet gibt es zwar derzeit oft nur wenige Tarife zur Auswahl, diese sind aber durchweg kaum teurer als gleichwertige Anschlüsse per Kupferkabel. Glasfaserzugänge bieten dafür mehr garantierte Datenrate und eine höhere Betriebssicherheit. Der Ausbau schreitet schnell voran, in den kommenden Jahren wird der Glasfaseranschluss auch in Deutschland zum Standard werden. (uma) c't

heise Security -Webinar

Active Directory:

Reale Angriffe verstehen und effektiv verhindern

7. Dezember 2022

Was war, was ist und was kommt auf uns zu?

Berichte zu Sicherheitsvorfällen zeigen, dass das Active Directory immer eine zentrale Rolle spielt und es den Angreifern oft fahrlässig einfach macht, die komplette IT zu übernehmen.

Das Active Directory ist das **Rückgrat der Unternehmens-IT** und enthält kritische Daten für deren Betrieb, oft auch im Zusammenspiel mit Azure AD. Eingerichtet ist es schnell, doch der sichere Betrieb stellt viele vor große Herausforderungen. Dieses **praxisrelevante Webinar** vermittelt Ihnen das nötige Wissen, um Ihr eigenes Active Directory angemessen abzusichern.

Jetzt Tickets sichern!

Programm

- Konzepte, Funktionsweise und Probleme des AD
- So wird das AD real angegriffen – mit Demos
- Härtung des AD – Konzepte, wie Sie Ihr AD sicherer machen

Hier mehr erfahren:
webinare.heise.de/active-directory

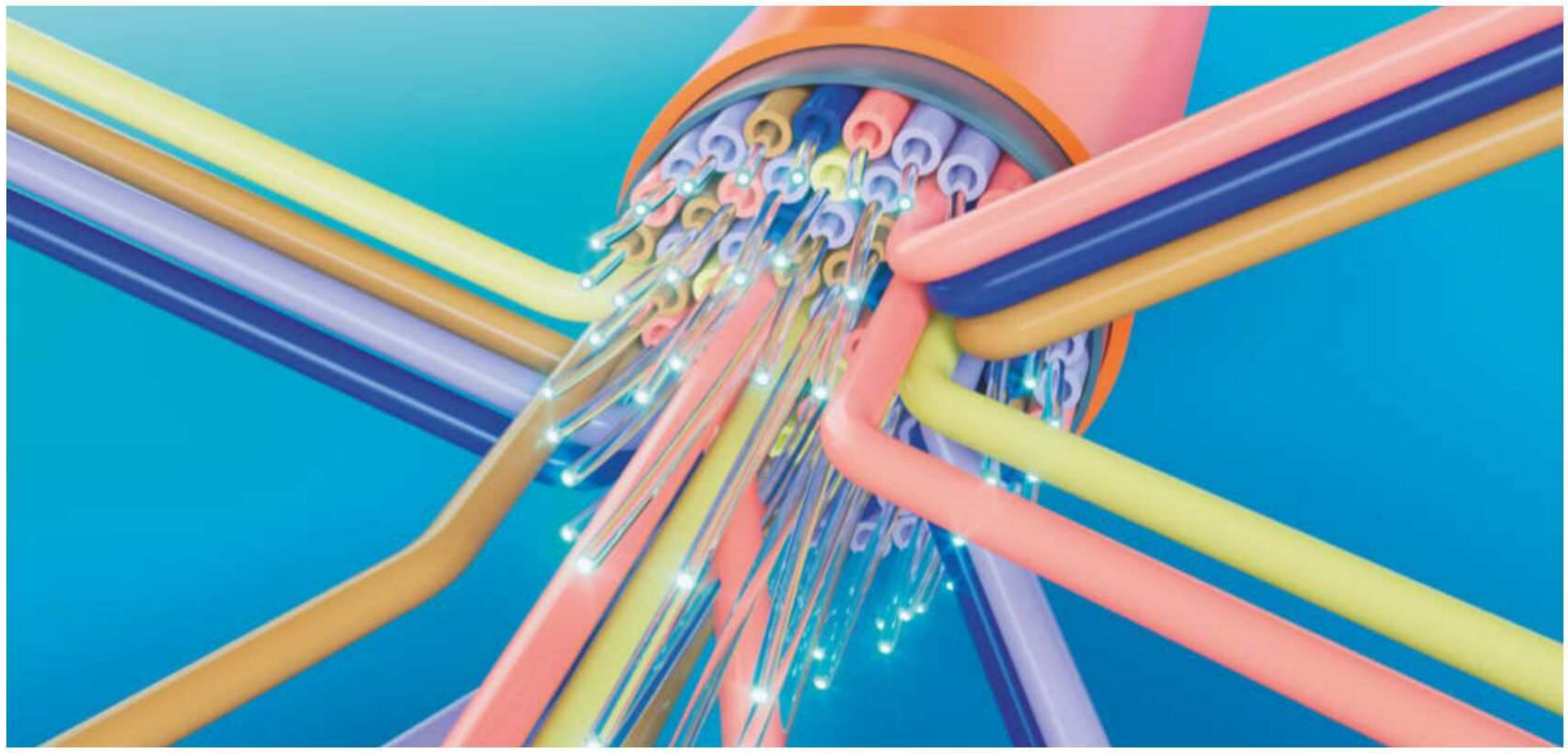


Bild: Moritz Reichartz

Die Technik des Glasfaser-Internet

Glasfaser-Internet ist nicht nur schneller als DSL, es braucht auch weniger Strom. Ein Blick auf die Details verrät, wie das geht. Außerdem geben wir Tipps für die Routerwahl und zur Konfiguration.

Von **Ernst Ahlers**

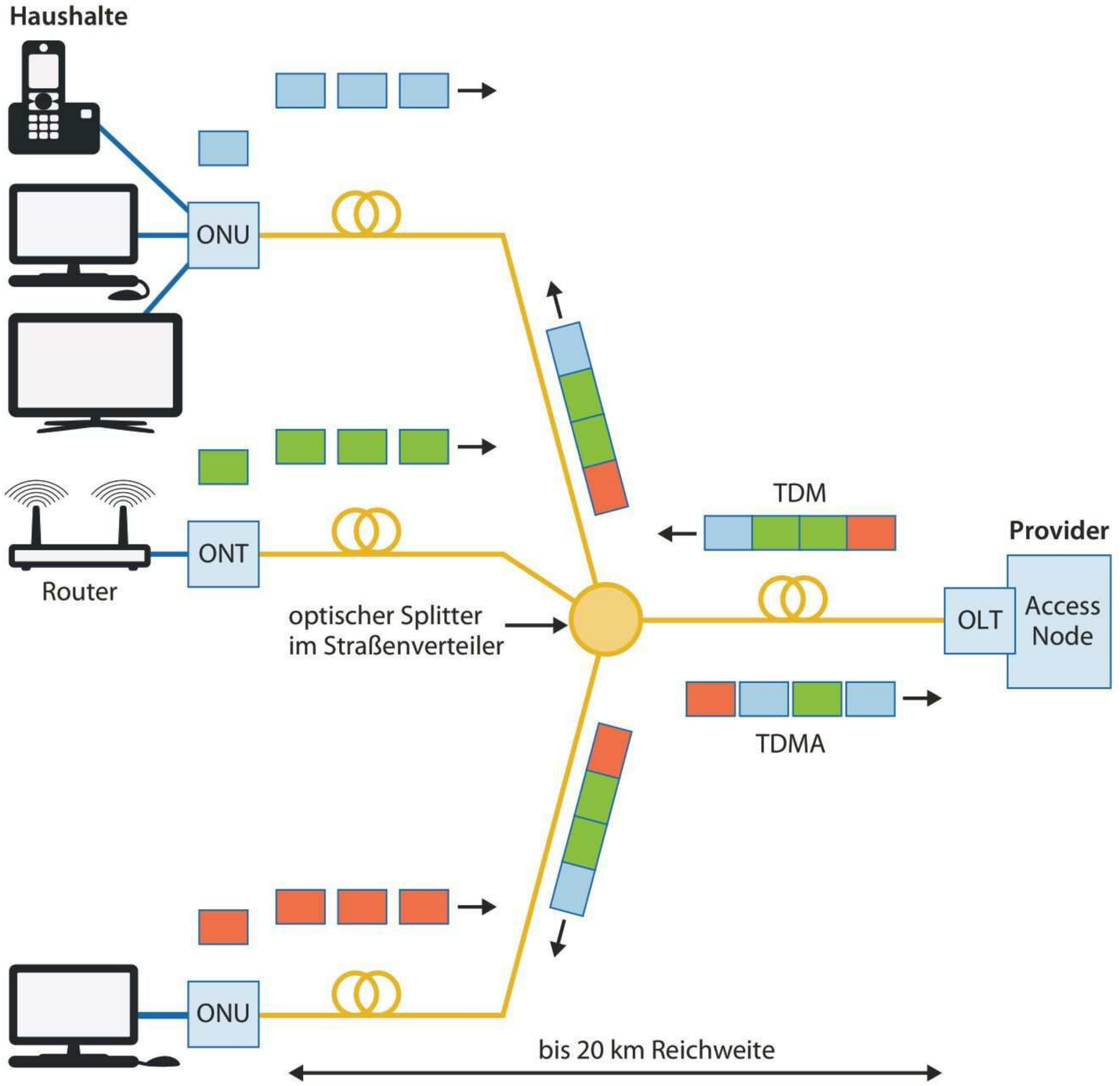
Kennen Sie schon das kleine schmutzige Geheimnis der schönen neuen Glasfaser? Bei der zurzeit verbuddelten GPON-Technik (Gigabit Passive Optical Network) teilen sich bis zu 32 Haushalte das Signal des Providers (Shared Medium, siehe Grafik). Insofern ähnelt GPON sehr dem Internet per TV-Kabel (DOCSIS). Auch dort hängen je nach Belegung eine Handvoll bis über 40 Anschlüsse am selben Koax-Segment. Wenn viele gleichzeitig saugen, verteilt sich die Downstream-Geschwindigkeit – 2,5 Gbit/s bei GPON, maximal 6 Gbit/s bei DOCSIS 3.1 – auf alle.

Doch es gibt keinen Grund, bei solchen Aussichten enttäuscht aufzustöhnen: Dieser Extremfall kommt glücklicherweise im Alltag nur sehr selten vor. Meist werden Kunden, die 1 Gbit/s gebucht haben, die auch bekommen. Denn selbst der größte Download dauert nicht ewig. Und schließlich muss auch die Gegenstelle im Internet, der Download-Server, die Daten schnell genug senden.

Bei GPON lässt sich der Splitter-Engpass bei Bedarf leichter weiten als bei DOCSIS: Der Provider aktiviert eine Reservefaser (Dark Fiber) zum Straßenverteiler, setzt dort einen zusätzlichen passiven Splitter und zieht eine Hälfte der Kunden darauf um. Im TV-Kabelnetz bräuchte man neue aktive Hardware im Verteiler, was eine größere Investition bedeuten würde.

Internet über GPON-Glasfaser

In GPON-Systemen – die Standardtechnik für die jetzt verlegten Glasfasern – teilen sich bis zu 32 Haushalte die Faser zwischen dem optischen Splitter im Straßenverteiler und der Providerzentrale. Wenn mehrere Teilnehmer gleichzeitig Daten aus dem Internet ziehen, bekommen sie zusammen höchstens 2,5 Gbit/s. Andersherum gehen maximal 1,25 Gbit/s über die Faser. Für 10 Gbit/s in beide Richtungen (XGS-PON) und später noch höhere Datenraten braucht man nur die Optikmodule zu tauschen.



Zudem testet die Deutsche Telekom bereits die nächste Glasfasergeneration: XGS-PON überträgt 10 Gbit/s in beide Richtungen. Zum Wechsel braucht man nur auf beiden Seiten die „Optik“ auszutauschen: in der Zentrale die Optical Line Termination (OLT) und kundenseitig das „Glasfaser-Modem“ (Optical Network Termination, ONT), den Router (Optical Network Unit, ONU) oder an diesem ein Einsteckmodul (SFP, Small Form-factor Pluggable, auch SFP+). Die Faser bleibt dieselbe.

Mit 10 Gbit/s wird längst nicht das Maximum erreicht, 100 Gbit/s sind in Weitverkehrsnetzen schon lange üblich. Die Glasfaser hat folglich weit mehr Wachstumspotenzial als das TV-Koaxkabel, das mit DOCSIS 4.0 (10/6 Gbit/s vollduplex) seinen Zenit erreichen dürfte.

Verkehrsregelung

Weil bei GPON bis zu 32 Haushalte dasselbe optische Signal empfangen (Time Division Multiplex, TDM), verschlüsselt der Provider den Datenstrom für jeden Kunden individuell – Mitlauschen ausgeschlossen. In der Gegenrichtung gibt die OLT ferner per Zeitraster vor, wer wann senden darf (Time Division Multiple Access, TDMA), damit Kollisionen ausbleiben.

Anders als bei klassischen optischen Verbindungen in Firmennetzen mit zwei Lichtwellenleitern laufen die beiden Datenrichtungen (Down- und Upstream) bei GPON in derselben Faser, aber auf unterschiedlichen Wellenlängen (Farben). Deswegen haben Anschlussdosen und Kundengeräte nur eine Faserbuchse (siehe Fotos).

Auch wenn die GPON-Optiken typischerweise in die Laserschutzklasse 1 (ungefährlich) oder 1M (ungefährlich, solange keine optischen Instrumente … verwendet werden) fallen: Schauen Sie nicht auf aktive Faserenden. Es gibt schlicht nichts zu sehen, weil das Signal im nahen Infrarot liegt (zirka 1310/1490 nm).

Steht die optische Verbindung, dann ist je nach Provider noch mehr oder weniger viel zu tun, um online zu kommen: Bei der Deutschen Telekom muss man das Zugangsgerät anhand seiner Modem-ID online registrieren. Installiert die Technikerin ein Glasfasermodem, dann erledigt sie das direkt.

Kommt ein Router als Leih- oder Kaufgerät vom Internetanbieter, dann ist er typischerweise bereits authentifiziert. Ob dann im Router noch Zugangsdaten einzutragen sind, hängt wiederum vom Provider ab. In der Regel erhalten Sie eine detaillierte Anleitung, sobald Ihr Glasfaseranschluss einsatzbereit ist.

Modem oder Router

Nach der Faser-Installation hängt in der Wohnung eine Anschlussdose. Dann gibt es zwei Optionen: Glasfasermodem plus Breitband-WLAN-Router oder integriertes Gerät (Glasfaser-Router).

Das Glasfasermodem, eigentlich ein Medienwandler oder -konverter, gibt es typischerweise für ein paar Euro Versandkosten vom Provider. Per Ethernet-Kabel schließt man daran einen beliebigen eigenen Router an. Der muss einen Gigabit-Ethernet-WAN-Port haben (Wide Area Network, Internetanschluss), was auch ein umkonfigurierbarer LAN-Port sein kann. Ferner muss der Router das vom Provider verwendete WAN-Protokoll beherrschen (DHCP/DHCPv6 oder PPPoE, optional mit VLAN-Tagging). Welches gilt, nennt der Provider in der Schnittstellenbeschreibung. Die ist üblicherweise im Support-Bereich seiner Webseite zu finden.

Wer weniger Geraffel im Wohnzimmer liegen haben möchte, kann sich für einen Glasfaser-Router entscheiden, der ein GPON-Optikmodul enthält oder einen SFP-Slot dafür hat. SFP bietet mehr Flexibilität: Hier passen Module für GPON (Punkt-zu-Multipunkt, PtMP) oder AON hinein (Active Optical Network, Punkt-zu-Punkt, PtP). Moderne Router wie die aktuellen Glasfaser-Fritzboxen 5530 [1] und 5590 (siehe S. 72) haben schon einen SFP+-Slot, der auch 10 Gbit/s transportiert und damit auf die nächste GPON-Generation vorbereitet ist.

Energiebedarf in der Fläche

Prinzipiell sind integrierte Geräte etwas energieeffizienter als die Kombination Glasfasermodem plus WLAN-Router, weil der zusätzliche Gigabit-Ethernet-Link und weitere aktive Elektronik im Modem entfallen. So spart man typischerweise zwei bis vier Watt Leistungsaufnahme, was bei 40 Cent pro Kilowattstunde und dem beim Internetzugang üblichen Dauerbetrieb 7 bis 14 Euro Stromkosten im Jahr ausmacht.

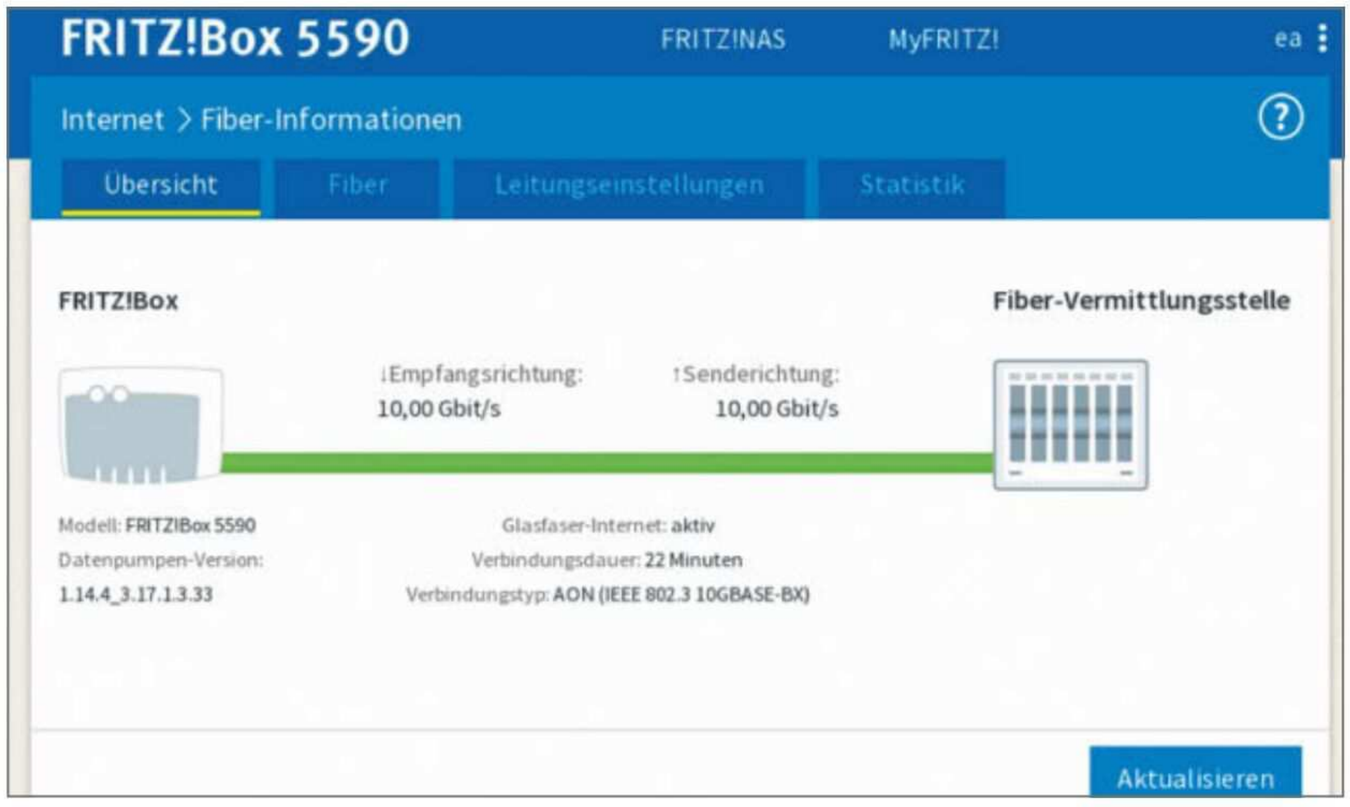
Das führt zur Frage, warum Glasfaser bis in die Wohnung (Fiber-to-the-Home, FTTH) soviel energie-







Liegt die Faser im Haus, gibt es mehrere Optionen: An ein Glasfasermodem (1) kann man einen eigenen Router anschließen. Ein Router mit Faserbuchse (2) spart das zusätzliche Modem und dessen Energiebedarf ein. Solche mit SFP-Slot (3) sind flexibler, falls der Anschluss später auf eine andere Technik umgestellt wird.



AVMs Fritzboxen 5530 und 5590 sind auf Glasfaserzugänge der nächsten Generation vorbereitet: Ihr SFP-Slot akzeptiert auch SFP+-Module, hier für eine Punkt-zu-Punkt-Verbindung (Active Optical Network) mit 10 Gbit/s. Die „Fiber-Vermittlungsstelle" ist dabei ein 10-Gbit/s-Switch im c't-Labor.

effizienter sein soll als DSL (Fiber-to-the-Curb, FTTC), G.fast (Fiber-to-the-Building, FTTB) und TV-Kabel-Internet (DOCSIS). Der Branchenverband Breko hat im Mai 2022 eine Studie der Technischen Hochschule Mittelhessen veröffentlicht (siehe ct.de/wbtp). Sie untersucht, wie nachhaltig der Vollausbau aller 41 Millionen deutschen Haushalte mit den unterschiedlichen Internet-Zugangstechniken wäre. Dabei hat der Autor nicht nur die aufzubringende elektrische Gesamtleistung für den Betrieb abgeschätzt, sondern auch die Masse des nötigen Materials.

In Sachen Strom würde GPON mit 114 Megawatt die Pole-Position einnehmen. G.fast und DSL lägen mit 303 und 350 Megawatt nicht weit auseinander im Mittelfeld. Das Kabel-Internet kam laut Modell mit 644 Megawatt auf den letzten Platz. Auch wenn manche die Modellannahmen für teilweise veraltet halten, dürfte eine Feinanpassung nur etwas an den absoluten Zahlen ändern, aber nicht die Reihenfolge.

… und individuell

Wenn man annimmt, dass die restliche Elektronik des Routers gleich ist, entscheidet der Leistungsbedarf des WAN-Links über die eigene Stromrechnung. Wir haben deshalb zum Vergleich das Pferd vom anderen Ende aufgezäumt und abgeschätzt, wie viel Leistung ein Link der jeweiligen Technik braucht.

Dazu stützten wir uns auf ein Papier des Joint Research Centre der Europäischen Kommission: Der „Code of Conduct on Energy Consumption of Broadband Equipment" definiert haarklein, auf welche Leistung sich einzelne Komponenten – WAN-Port, WLAN, LAN-Ports und anderes – von Modems, Routern oder der Provider-Netzwerkausstattung in verschiedenen Betriebszuständen beschränken sollen (ct.de/wbtp). Da die Grenzen von der Branche selbst gesteckt sind, dürften sie ein gutes Indiz für die heute erreichbare Effizienz sein.

Damit die Ergebnisse zu den Breko-Zahlen vergleichbar sind, haben wir die Gegenseite einbezogen, also den Port in der Providerzentrale. Denn der muss ja laufen, damit man selbst Internet hat. So errechneten wir mit den Werten für 2021 bei einem FTTC-Link mit DSL-Supervectoring 4,3 Watt. FTTB, G.fast 212a mit 8 Parteien pro Konzentrator, kam auf 3,5 Watt. DOCSIS 3.1 lag mit 38 Anschlüssen pro Strang nach unserem Modell bei 10,8 Watt und GPON kam im 1:32-Split auf 1,4 Watt. Über alles ergab sich mit geringen Abweichungen dasselbe Leistungsverhältnis wie im Breko-Modell. Die Ausnahme war DOCSIS, wo unser Verhältnis zu GPON mit Faktor 7,7 etwas ungünstiger war (Breko: 5,6).

GPON profitiert dabei erheblich von seinem passiven Splitter: Ein OLT versorgt im Optimum 32 Kunden in Point-to-Multipoint-Konstellation. Würde man das mit Punkt-zu-Punkt-AON-Technik nachbilden, wären 64 statt 33 Optikmodule nötig, also 31 mehr beim Provider, die aber etwas weniger Leistung brauchen als der GPON-OLT. Ein AON-Vollausbau läge energiemäßig laut Breko mit 154 Megawatt nur wenig über GPON und noch weit unter DSL.

Den größten Effizienzgewinn bringt GPON offensichtlich nicht zu Hause und damit auf der eigenen Stromrechnung, aber dafür eine viel höhere Datenrate als DSL. Gegenüber DOCSIS 3.1 und später 4.0 liefern GPON und das kommende XGS-PON zwar nicht mehr Geschwindigkeit. Aber hier dürfte sich der Leistungsbedarf der heimischen Router deutlicher unterscheiden. Das kann – je nach Entwicklung des Strompreises – ein paar Euro bis wenige Dutzend Euro im Jahr sparen.

Tendenziell wird mit dem Umstieg auf GPON die Energieaufnahme und damit der CO_2-Ausstoß der Internet-Hardware bei Kunden und Providern sinken. Der Umstieg vom Kupfer aufs Glas für den Internetzugang lohnt sich also nicht nur für DSL-Nutzer. (ea) c't

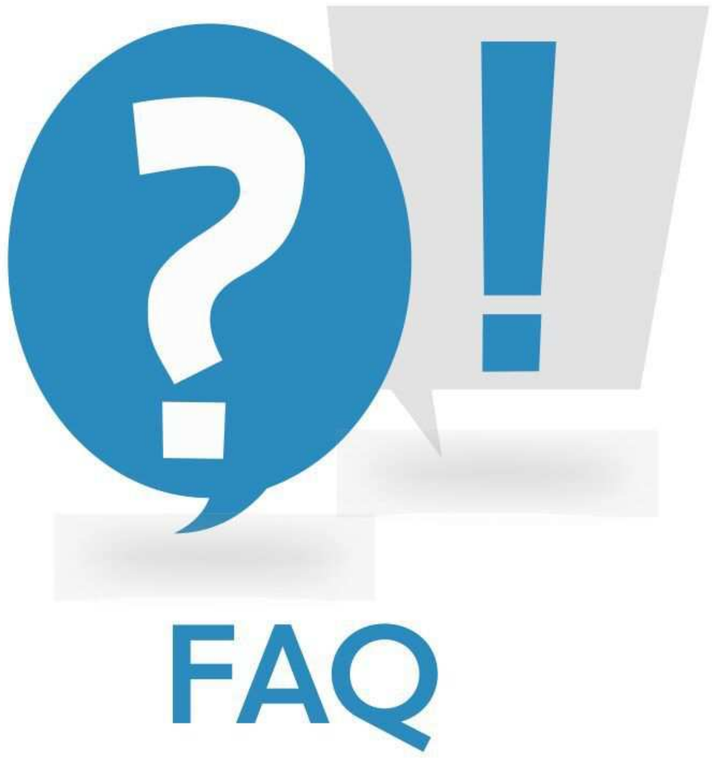
Literatur

[1] Ernst Ahlers, **Glas-Fritz**, Fritzbox 5530 mit Wi-Fi 6 für Glasfaser-Internetanschlüsse, c't 7/2021, S. 70

Energiebedarf Netzkomponenten

ct.de/wbtp

Per Glasfaser ans Internet



Praktisch alle Geräte im Heimnetz koppelt man entweder per elektrischem Ethernet-Kabel ans Internet oder drahtlos per WLAN. Wie finden die Internet-Daten den Weg zur Glasfaser? Und wie kommt die Glasfaser ins Haus?

Von **Dušan Živadinović**

Glasfaserarchitekturen

Was bedeuten FTTC, FTTB oder FTTH?

Es gibt diverse Glasfaserarchitekturen, je nachdem, wo die Faser aus Sicht des Netzbetreibers endet: im Straßenverteiler am Bordstein (Fiber-to-the-Curb, FTTC), im Gebäude (Fiber-to-the-Building, FTTB), in der Wohnung (Fiber-to-the-Home, FTTH) oder gar am Schreibtisch (Fiber-to-the-Desk, FTTD). Beim aktuell forcierten Glasfaserausbau für Privatkunden handelt es sich um FTTH-Anschlüsse.

Erdrakete zum Hausverteiler

Wie kommt die Glasfaser in meine Wohnung?

Während in vielen anderen Ländern Glasfaserleitungen oberirdisch geführt werden dürfen, müssen sie in Deutschland so wie Strom-, Gas- und Wasserleitungen unterirdisch zu den Teilnehmern laufen. Die erforderlichen Grabungsarbeiten bremsen das Ausbautempo und erhöhen den Aufwand. Es muss aber nicht die gesamte Strecke zum Haus aufgegraben werden: oft bahnt eine Erdrakete die letzten Meter vom Gehweg bis in den Keller. Dann folgt in der Regel ein Leerrohr und darin schließlich die Glasfaser bis zum Hausübergabepunkt (HÜP, auch Hausanschlusspunkt, HPL, genannt).

Von diesem Kunststoffkasten geht dann das Endstück zur Glasfaserdose im Haus (Glasfaser-Teilnehmeranschluss, GF-TA). Der GF-TA ist aus Sicht des Netzbetreibers der Endpunkt. Er kann bis zu 20 Meter vom HÜP entfernt sein (30 Meter bei Mehrfamilienhäusern); vor der Installation müssen etwaige Bohrungen oder Leerrohre vom HÜP zum GF-TA bereits angebracht sein.

Recht auf freie Routerwahl

Mein Betreiber hat keine Glasfaserdose installiert – wo schließe ich nun meinen Glasfaserrouter an?

Manche Netzbetreiber installieren keinen GF-TA, sondern montieren an einen proprietären Anschlusspunkt gleich ein Glasfasermodem (Optical Network Termination, ONT) ihrer eigenen Wahl. Damit verletzen sie das Recht auf Routerfreiheit, weil Kunden das Modem nicht selbst aussuchen können und weil man an solchen Anschlüssen keine Router mit eingebautem Glasfasermodem betreiben kann.

In solchen Fällen kann man zumindest vorübergehend auf Breitband-Router oder auf bestimmte DSL-Router ausweichen. Mehr dazu finden Sie im Abschnitt „Router ohne Glasfasermodem“.

Das Recht auf freie Wahl des Routers ist seit 2018 im Telekommunikationsgesetz festgeschrieben (siehe ct.de/w78n). Falls Sie einen GF-TA benötigen, weisen Sie Ihren Netzbetreiber freundlich darauf hin. Geben Sie ihm eine Chance, die Dose anzubringen – manche sind tatsächlich nicht im Bilde über das TKG oder beanspruchen für sich nicht-existente Ausnahmeregeln. Protokollieren Sie die Kommunikation mit dem Netzbetreiber und falls alles Bitten nicht fruchtet, reichen Sie eine Beschwerde bei der

Bundesnetzagentur ein. Die Grundlage für die Routerfreiheit hat die Agentur im Kontaktformular „Kundenschutz Telekommunikation“ zusammengefasst, auch hält sie ein Formular zum Einreichen von Beschwerden bereit (siehe ct.de/w78n).

Bei Streitigkeiten mit Telekommunikations- oder Post-Anbietern kann die BNetzA ein Schlichtungsverfahren einleiten. Dafür müssen Sie darlegen, dass Sie im Vorfeld versucht haben, eine Einigung zu erzielen.

Von der Dose zum Modem

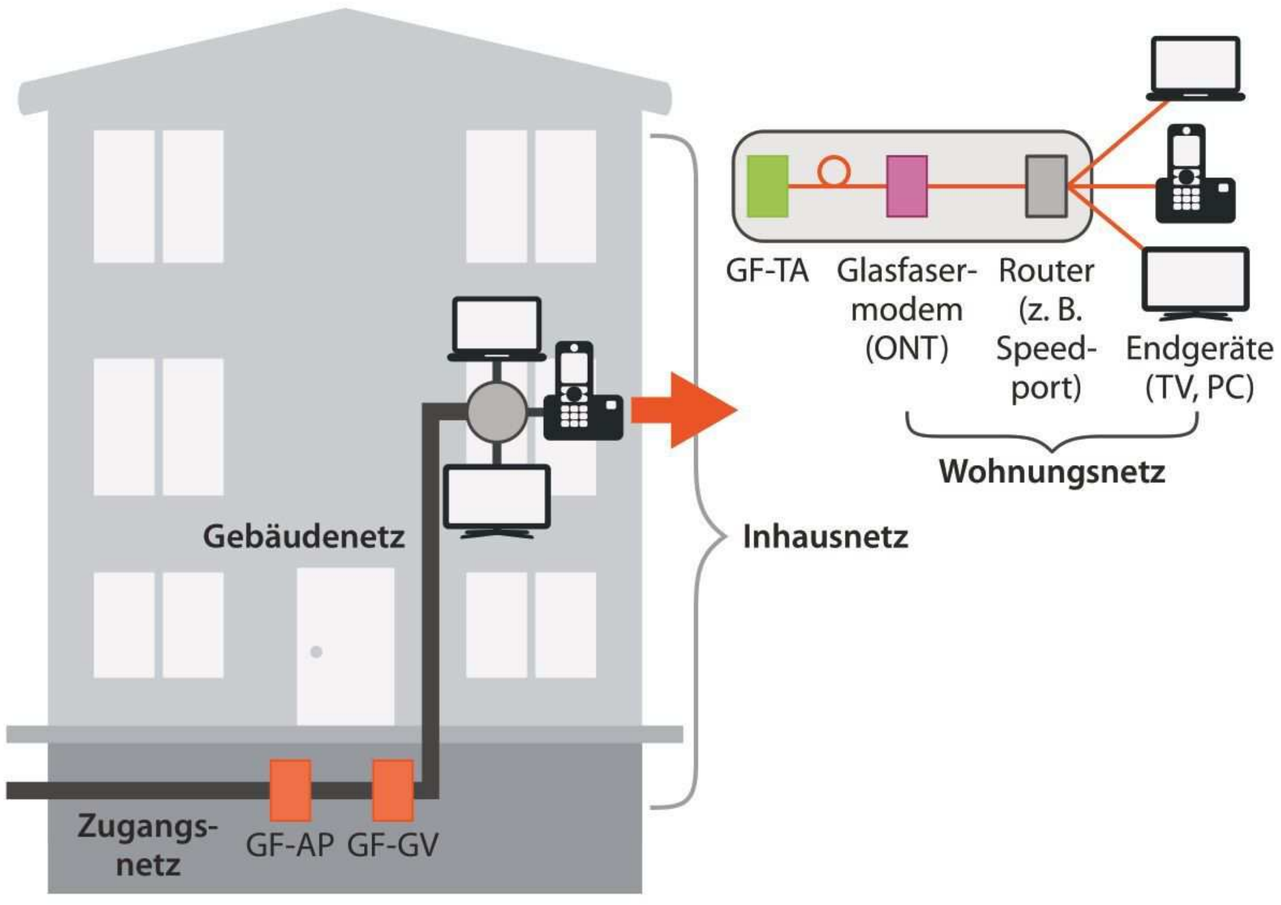
? Welches Gerät schließe ich an die Glasfaserdose an?

! Das letzte Element der Glasfaserinfrastruktur ist ein Glasfaser-Modem (Optical Network Termination, ONT). Es wird an die Glasfaserdose (GF-TA) angeschlossen. Üblicherweise stellt der Netzanbieter das Modem zur Verfügung. Ab dem ONT läuft der Internetverkehr normalerweise über das übliche, elektrische Ethernet zum Router, der den Zugang dann per Ethernet-Kabel im LAN oder per WLAN weiterverteilt.

Seit einiger Zeit gibt es aber auch Router mit eingebautem Glasfasermodem. Man schließt sie direkt an die Glasfaserdose an, was den ONT und eine Steckdose zu dessen Stromversorgung erspart.

Glasfaserinfrastruktur

Netzbetreiber wie die Telekom führen die Glasfaser zunächst von ihrem eigenen Zugangsnetz bis zum Glasfaserabschlusspunkt am Gebäude (GF-AP). In Mehrfamiliengebäuden führen separate Leitungen vom Glasfasergebäudeverteiler (GF-GV) zu den einzelnen Wohnungen. Den Endpunkt bildet die Glasfaserdose (Glasfaser-Teilnehmeranschluss, GF-TA). Dort bindet ein ONT (Optical Network Termination) oder ein Glasfaserrouter das Heimnetz über herkömmliches, elektrisches Ethernet an.



Faser statt Kabel

? Was ist beim Umgang mit Glasfaserkabeln zu beachten?

! Glasfaser-Patchkabel sind viel dünner als Ethernet-Patchkabel, sodass sie weniger auffallen. Jedoch sind sie viel weniger robust, sodass man sich vor dem Verlegen über den maximalen Biegeradius informieren sollte. Und klar: Knicke sind unbedingt zu vermeiden, weil die Fasern spröde sind und daher brechen können.

Überhaupt gilt es, die dünnen Kabelchen mit Samthandschuhen anzufassen und auch, die Schutzkäppchen aufzubewahren – die sollten Sie umgehend nach dem Abstöpseln von einer Buchse aufsetzen, um Verschmutzung zu vermeiden. Andernfalls können kleinste Staubkörnchen den Lichtübertritt zum Beispiel vom Glasfaser-Router zur Glasfaserdose bremsen. Dann ist es Glückssache, ob das Signal noch für eine stabile Verbindung ausreicht.

Die Anschlusstechniken GPON, XGS-PON und AON

? Kann ich einen beliebigen Glasfaserrouter oder ein beliebiges ONT anschließen?

! Nein, denn über die Glasfaserdose kommunizieren Modems je nach Infrastruktur des Betreibers auf unterschiedliche Weise. Verbreitet sind die GPON- und die AON-Technik (Gigabit Passive Optical Network und Active Optical Network). Manche Provider setzen in Feldversuchen XGS-PON ein. Ein ONT ist aber immer nur für eine der Techniken ausgelegt.

Bei GPON teilen sich alle an einem Verzweiger angeschlossenen Teilnehmer die Downstream-Kapazität von 2,5 GBit/s und 1,25 Gbit/s in Gegenrichtung (Upstream). Üblicherweise versorgt ein Knoten maximal 32 Anschlüsse. Die neuere passive Variante, XGS-PON oder auch 10G-PON, liefert maximal 10 GBit/s in beide Richtungen. In Deutschland betreibt die Telekom in Darmstadt ein erstes XGS-PON-Netz.

Beim aufwändigeren AON sind die Teilnehmer über separate Leitungen angeschlossen, sodass jedem die volle Bandbreite des Anschlusses zur Verfügung steht (bis zu 10 GBit/s); wie viel die Leitung dann tatsächlich durchlässt, hängt aber, wie an allen Anschlüssen, vom gewählten Tarif ab. Einige AON-Betreiber klemmen den ONT direkt an die Glasfaser an, installieren also keine Glasfaserdose. Kunden können den ONT an solchen Anschlüssen nicht selbst wechseln und auch keinen Router mit eingebautem ONT betreiben.

Das passende Glasfasermodem

? Welche Glasfasermodems eignen sich für meinen Anschluss?

! Wer keinen Glasfaserrouter direkt an der Dose betreiben kann oder will, braucht für die Umsetzung der Signale von der Glasfaser auf das übliche elektrische Ethernet ein externes Glasfasermodem (Optical Network Termination, ONT), sofern der Netzbetreiber es nicht selbst liefert. Es gibt diverse Hersteller von ONTs, die Preise starten bei rund 30 Euro (siehe ct.de/w78n).

Vor dem Kauf sollte man den Betreiber um eine detaillierte Schnittstellenbeschreibung bitten. Aus der sollte klar hervorgehen, ob es sich um einen AON-, GPON- oder XGS-PON-Anschluss handelt. Beispielsweise veröffentlicht die Telekom ihre Schnittstellenbeschreibungen, sodass man sich daran orientieren kann. Andernfalls kann der Betrieb eines ONT an Kleinigkeiten wie der Registrierung beim Provider scheitern. In dieser Hinsicht gehört das Glasfasermodem 2 von der Telekom (GPON-Technik, erhältlich ab rund 40 Euro) zu den interessanteren Kandidaten, weil es genau auf die Anforderungen des magenta Riesen abgestimmt ist und sich komfortabel per Smartphone registrieren lässt.

Der passende Router

? Wofür brauche ich überhaupt einen Router?

! Prinzipiell könnte man einen Glasfaseranschluss mit einem einzigen PC nutzen, den man per Ethernet-Kabel am ONT anschließt. Der PC baut dann die Internet-Verbindung zum Netzbetreiber auf. In den weitaus meisten Fällen kommt das aber nicht infrage, weil man mehr als ein Gerät über den Hausanschluss ins Internet bringen will. Diese Vermittlungsfunktion übernimmt ein Router, an den man alle Geräte des Heimnetzes wahlweise per Ethernet-Kabel oder per WLAN koppelt.

Im Router wird auch der Internetzugang mitsamt den Zugangsdaten konfiguriert. Viele Betreiber nutzen für den Transport des Internetverkehrs das im DSL-Bereich übliche PPPoE (Point-to-Point Protocol over Ethernet), manche stattdessen DHCP (Dynamic Host Control Protocol) oder noch andere Varianten – Einzelheiten finden Sie in den Einwahlunterlagen, die Ihnen der Provider zuschickt.

Wenn eine Dose bereits vorliegt, kann man daran spezielle Router für Glasfaseranschlüsse anstecken. Dazu gehören die Fritzbox 5530 Fiber [1] und die umfangreicher ausgestattete Fritzbox 5590 Fiber (siehe Test auf S. 72). Beide Modelle eignen sich für GPON und AON. Dafür enthalten sie einen SFP-Steckplatz, in den man je nach Bedarf das mitgelieferte GPON- oder AON-Modul steckt. Von dort führt dann ein Glasfaser-Patchkabel zur Faserdose (GF-TA).

Ausschließlich für GPON eignen sich die Fritzbox 5491 und der TP-Link TX-VG1530. In anderen Ländern sind in der Regel Router anderer Hersteller verbreitet, darunter etwa Modelle mit eingebautem Glasfaseranschluss von Nokia oder Sagem. Von solchen Routern raten wir ab, weil offen ist, ob sie sich für die in Deutschland üblichen Anschlüsse und Kommunikationsprotokolle eignen. Zudem kann bei manchen Nokia-Modellen nur der Netzbetreiber auf die essenziellen Einstellungen zugreifen (per TR069-Protokoll aus der Ferne).

Manche Netzbetreiber haben frühzeitig mit dem Glasfaserausbau begonnen und vor einigen Jahren auf die AON-Technik gesetzt (z. B. der Berliner Provider ediscom). In manchen Ländern ist AON weiterhin verbreitet, darunter etwa in Österreich. Für AON-Anschlüsse braucht man Router mit AON-Schnittstelle.

Router ohne Glasfasermodem

? Welche Router eignen sich für den Anschluss an den ONT?

! Wenn der Netzbetreiber einen ONT ohne Steckdose (GF-TA) am Hausverteiler angekoppelt, also das Gesetz der Routerfreiheit missachtet hat, können Sie es dauerhaft dabei belassen – oder Sie bitten den Betreiber, eine Dose zu setzen und leben einige Wochen mit dem unerwünschten ONT.

Wie Sie vorgehen, um eine Glasfaserdose nachträglich setzen zu lassen, haben wir im Abschnitt „Recht auf freie Routerwahl“ beschrieben.



Bild: AVM

Moderne Router wie die Fritzbox 5590 Fiber lassen sich ohne Umweg über einen ONT an eine Glasfaserdose anschließen. Dafür bringen sie einen SFP-Steckplatz mit (der helle Anschluss ganz links am Gehäuse).

Bis die Dose gesetzt ist, brauchen Sie einen Router, der per WAN-Port an den ONT angeschlossen wird (Breitband-Router). Ein guter, weil leistungsfähiger Kandidat ist die Fritzbox 4060 [2]. Auch das deutlich preisgünstigere Vorgängermodell 4040 eignet sich und daneben diverse Mesh-Sets wie die eero-Router.

DSL-Router kommen ebenfalls infrage, wenn man einen ihrer Ethernet-Anschlüsse als WAN-Port konfigurieren kann. Dabei liegt das DSL-Modem brach. Man koppelt sie ebenfalls per üblichem elektrischem Ethernet an den ONT. DSL-Fritzboxen wie die 7590 eignen sich ebenfalls für diese Betriebsart. Manche Glasfaseranbieter vermieten sogar solche Modelle.

Was sich beim Umstieg von DSL ändert

? Ich möchte meine Netzwerkgeräte weiterhin fernwarten können. Geht das auch, wenn ich von DSL auf Glasfaser wechsle?

! Prinzipiell geht das an jeder Anschlussart, nicht nur an DSL-, sondern auch an Glasfaser- oder gar Kabelanschlüssen. Je nach Netzbetreiber kann es aber neue Hürden geben.

Zunächst braucht man für den Zugang zum Heimnetz aus der Ferne eine öffentliche IP-Adresse direkt am eigenen Anschluss. Bei DSL-Anschlüssen der Telekom ist das beispielsweise grundsätzlich der Fall, es handelt sich um eine öffentliche IPv4-Adresse (auch WAN-IP-Adresse genannt). Sie ist lediglich nicht fest, sondern wechselt immer mal. Um sie nicht jedes Mal telefonisch abzufragen, richtet man am besten im Router einen DynDNS-Dienst ein, der die wechselnden IP-Adressen immer derselben DynDNS-Domain zuweist, anhand der man dann von unterwegs etwa auf den PC im Heimnetz per Port-Weiterleitung zugreift. Öffentliche IPv4-Adressen hat aber nur die Deutsche Telekom zur Genüge, die meisten anderen Provider kamen so spät auf den Markt, dass sie vom ohnehin kleinen IPv4-Adresskuchen nur Krümel abbekamen. Deshalb bringen solche Provider und auch Anbieter von Glasfaseranschlüssen viele ihrer Kunden per DS-Lite-Technik ins Internet. Dabei bekommt der Anschluss keine öffentliche IPv4-Adresse, sondern eine private und muss über die CG-NAT-Technik ins Internet (Carrier-Grade Network Address Translation). Mit CG-NAT spart der Provider IPv4-Adressen, indem er den IPv4-Verkehr vieler Kunden gleichzeitig über eine einzige öffentliche Adresse ins Internet leitet. Deshalb kann man das Heimnetz über solche Anschlüsse nicht per IPv4 erreichen, sondern nur über globale IPv6-Adressen.

An Privatkundenanschlüssen werden auch die globalen IPv6-Adressen dynamisch zugewiesen, weshalb man auch damit auf DynDNS zurückgreift. Die Handhabe ist geringfügig aufwendiger, weil bei IPv6 nicht nur der Router eine globale Adresse erhält, sondern auch jeder Host im Heimnetz, sodass es gilt, auch den jeweiligen DynDNS-Hostnamen immer mit der aktuellen IPv6-Adresse zu verknüpfen. Einzelheiten dazu finden Sie im Literaturhinweis [3].

Falls Sie beim selben Provider bleiben und von ihm aktuell für DSL eine öffentliche IPv4-Adresse erhalten, fragen Sie ihn vor dem Wechsel, ob Sie diese behalten können. Manche bieten öffentliche IPv4-Adressen bei besonderen Tarifen an, in der Regel aber mindestens für Geschäftskunden. (dz) c't

Literatur

[1] Ernst Ahlers, **Glas-Fritz**, Fritzbox 5530 mit Wi-Fi 6 für Glasfaser-Internetanschlüsse, c't 7/2021, S. 70

[2] Ernst Ahlers, **VPN-Express**, Fritzbox 4060: Rasanter Breitband-WLAN-Router im Test, c't 5/2022, S. 74

[3] Peter Siering, **V6-Fritz**, Portfreigaben, IPv6 und DynDNS-Namen auf Fritzboxen nutzen, c't 23/2021 S. 150

Formulare der BNetzA, Router-Tests

ct.de/w78n



Fritzbox 5590 für Glasfaser-Internet

AVMs Fritzbox 5590 bringt das Internet über einen schnellen Glasfaseranschluss in die Wohnung und verteilt es mit modernem Wi-Fi-6-WLAN weiter. Das kann die billigere Vorgängerin 5530 auch, aber die neue Box hat in einigen Sparten die Nase vorn, teils sogar mit großem Abstand.

Von **Ernst Ahlers**

Die jüngst erschienene Fritzbox 5590 hat von vielen im Heimnetz nützlichen Dingen mehr als ihre kleine, seit dem Frühjahr 2021 erhältliche Schwester 5530 [1]: vier statt zwei MIMO-Streams im Wi-Fi-6-WLAN auf beiden Funkbändern, vier statt zwei Gigabit-LAN-Ports, zwei statt einen Anschluss für Analogtelefone und zwei statt keine USB-Ports. Schon damit hätte sie das Etikett Glasfaser-Topmodell verdient.

Doch das wichtigste Merkmal ist ihr rasanter Router-Prozessor. In der 5590 erledigt ein Qualcomm IPQ8072A mit vier 2 Gigahertz flotten Cortex-A53-Kernen den Datenumschlag. Das merkt man nicht nur oberflächlich an den viel zügiger vom Browser aufgebauten Konfigurationsseiten, sondern auch deutlich beim Fritz-VPN.

Wir maßen im Roadwarrior-Szenario (Host im Internet greift via VPN auf Server im Fritzbox-LAN zu)

je nach Datenrichtung 300 oder 440 Mbit/s. Die 5530 mit ihrem veralteten CPU-Kern (MIPS32-Quadcore mit 800 MHz) schaffte in derselben Situation gerade mal 6 und 21 Mbit/s. Wir sind sehr gespannt, ob sich beide Geräte mit dem neuen WireGuard-VPN annähern [2].

Zukunftsgerichtet

Wie bei der 5530 ist der Glasfaseranschluss der 5590 als SFP+-Slot ausgeführt: Man steckt je nach Zugangsart (AON: Active Optical Network, GPON: Gigabit Passive Optical Network) eines der beiden mitgelieferten SFP-Optikmodule ein. Damit sollte die Box an allen hierzulande üblichen Glasfasernetzen funktionieren. Zurzeit bekommt man per GPON maximal 2,5 Gbit/s im Downstream, doch über XGS-PON sind auch 10 Gbit/s möglich. Dafür ist nur ein Modultausch nötig, kein neuer Router.

Fremde SFP+-Module akzeptierte die Fritzbox in einem kurzen Test nicht, sodass wir den NAT-Durchsatz nur über den Ethernet-WAN-Port mit seinen maximal 2,5 Gbit/s messen konnten. Mit zwei LAN-Hosts – was nicht unser Standard-Test-Setup ist – reichte die 5590 tatsächlich knapp 2 Gbit/s im IP-zu-IP-Modus durch, die Tabelle zeigt die Werte für einen Client. Bei dem beispielsweise im Netz der Deutschen Telekom gebräuchlichen PPPoE begrenzte unser Testserver die Datenrate. 1 Gbit/s – das Maximum des derzeit buchbaren – sollte die 5590 locker hergeben.

Übers Wi-Fi-6-WLAN kam vom Gigabit bei einem AX200-Client in der Nähe auf dem 5-GHz-Band fast alles an, über 20 Meter durch Wände immerhin noch ein großer Teil (siehe Tabelle).

Flott gespeichert

Die Rasanz der Router-CPU merkt man auch beim NAS-Durchsatz: Große Dateien lieferte die 5590 mit fast 140 MByte/s von einer USB-SSD über ihren bis zu 2,5 Gbit/s schnellen Ethernet-Port ins LAN. Die potente Hardware des Routers fordert freilich mit rund 12 Watt ein Quäntchen mehr Leistung als etwa eine xDSL-Fritzbox 7590 (10 Watt).

Interessanterweise gibt es auf der 5590er-Platine einen freien Chip-Bestückungsplatz sowie in der Buchsenleiste eine freie Stelle. Anscheinend hatte AVM ursprünglich einen ISDN-S0-Port vorgesehen, doch von dieser veralteten Technik hat man sich inzwischen endgültig verabschiedet. Als letzte Fritzbox bekam ein Modell der 7590AX den S0-Port [3].

Fazit

Wer als Fritz-Fan einen flinken Glasfaseranschluss in der Wohnung oder im Büro hat und schnelles VPN fürs Homeoffice braucht, der bekommt mit der Fritzbox 5590 den passenden Router. Dafür ist ein Hunderter mehr fällig als für die kleine Schwester 5530, was aber – nicht nur für die USB-Ports der 5590 – gut angelegtes Geld ist. (ea) c't

Literatur

[1] Ernst Ahlers, **Glas-Fritz**, Fritzbox 5530 mit Wi-Fi 6 für Glasfaser-Internetanschlüsse, c't 7/2021, S. 70

[2] Ernst Ahlers, **VPN-Turbo**, WireGuard verdoppelt VPN-Geschwindigkeit bei Fritzbox 7590, c't 4/2022, S. 35

[3] Ernst Ahlers, **Fritzbox 7590 AX mit und ohne ISDN**, ct.de/-6659823

AVM Fritz!Box 5590 Fiber

WLAN-Router für Glasfaseranschlüsse	
Hersteller, URL	AVM, avm.de
WLAN	2 × Wi-Fi 6 (4) = IEEE 802.11ax-1200 / ax-2400, simultan dualband, WPA3, WPS, DFS
Anschlüsse	1 × SFP+, 5 × RJ45 (1 × NBase-T bis 2,5 Gbit/s, 4 × 1 Gbit/s), 2 × USB 3.2 Gen 1 (5 Gbit/s), 2 × RJ11 (Fon1/2), 1 × TAE (Fon1), DECT-Basis für max. 6 Schnurlostelefone
Bedienelemente	5 Statusleuchten, 3 Tasten
Getestete Firmware	FritzOS 7.29
NAT-Perf. PPPoE (DS / US)	782 / 825 Mbit/s
IP-zu-IP (DS / US)	950 / 949 Mbit/s
WLAN 2,4 GHz nah / 20 m[1]	416 / 256–331 Mbit/s
5 GHz nah / 20 m[1]	932 / 231–269 Mbit/s
VPN-Durchsatz (DS / US)	442 / 302 Mbit/s (Fritz-IPsec, Roadwarrior)
NAS-Durchsatz große Dateien	103 / 139 MByte/s (Schreiben / Lesen)
Leistungsaufnahme[2]	12,4 Watt (25,3 VA)
Jährliche Stromkosten[2]	44 €
Preis	289 €

[1] gegen Intel AX200 [2] idle, bei Dauerbetrieb, 40 Cent/kWh, gerundet

Raus aus der Abhängigkeitshölle

In modernen Applikationen fußt Software Schicht um Schicht auf anderer Software. Muss man sich das wie ein fest gefügtes Mauerwerk oder mehr wie einen wackeligen Stapel vorstellen, der jeden Moment die ganze Firma begraben kann? Wer das nicht weiß, lebt gefährlich! Gegen das Unwissen helfen Werkzeuge, um die eigenen Abhängigkeiten aufzudecken und ihre Zuverlässigkeit zu beurteilen.

Von **Sylvester Tremmel**



Bild: Albert Hulm

Wie abhängig sind wir?	74
Ein Framework unter der Lupe	76
Abhängigkeiten erkennen	82
Sicherheitsvorfälle in Logs aufspüren	88

Sieben Terrassen hat der Läuterungsberg in Dantes Göttlicher Komödie. Auf Terrasse Nummer vier des Fegefeuers büßen die Faulen in immerwährender Hetze. Irgendwo dort werden sich vielleicht auch die Programmierer einfinden müssen, die gedankenlos Abhängigkeiten anhäufen, um zwei oder drei Zeilen Code zu sparen – wenn sie Glück haben.

Wenn sie Pech haben, holen ihre Sünden sie noch in diesem Leben ein. So dürften sich im Dezember 2021 viele IT-Mitarbeiter gefühlt haben, als sie von Abteilung zu Abteilung hetzten. Es galt zu verhindern, dass ihr Betrieb einer Sicherheitslücke in Log4j zum Opfer fällt – vor allem aber mussten sie erst mal herausfinden, an wie vielen Stellen man die Java-Bibliothek Log4j überhaupt nutzte. „Schnell, schnell, daß nicht die Zeit verlorengehe“, hätten sie zusammen mit Dantes Büßern schreien mögen.

Daraus darf man aber nicht den Schluss ziehen, Open Source zu verteufeln oder ganz auf Bibliotheken zu verzichten. Die Zeiten, in denen man jedes Projekt als frei stehenden Haufen Assembler- oder C-Code implementieren konnte, sind vorbei: Anwendungen sollen im Browser laufen oder auf virtuellen Maschinen, die Bytecode interpretieren, und sie sollen möglichst architektur- und betriebssystemübergreifend funktionieren.

Zum anderen wird aus der krampfhaften Vermeidung von Abhängigkeiten allzu leicht das „Not invented here Syndrom“. Dabei erfindet jeder Entwickler jedes Rad neu – noch dazu oft mit mehr Ecken, als ein Rad haben sollte. Das ist nicht nur ineffizient, sondern auch ineffektiv: Das globale Software-Ökosystem blüht und gedeiht genau deshalb so prächtig, weil man auf Vorhandenes aufbaut, kooperiert und wechselseitig die Arbeit anderer nutzt. Ganz besonders gilt das für Open-Source-Projekte.

Es ist also gut und richtig, dass Log4j in Unmengen von Java-Projekten steckt: Fast jede Software sollte Log-Dateien schreiben und wer auf eine vorhandene Bibliothek setzt, der profitiert, wenn andere die Bibliothek verbessern. Weniger gut und richtig ist, wie unkoordiniert und versteckt die Abhängigkeiten oft wuchern und wie gedankenlos sie in Projekte geladen werden.

Wucherungen

Dieser Wildwuchs nimmt mitunter absurde Ausmaße an, man könnte vom „Already invented there Syndrom“ sprechen: NPM ist ein Katalog für JavaScript-Pakete, nach eigener Aussage das weltgrößte Softwareverzeichnis – und ein Schauplatz solcher pathologischen Abhängigkeiten. Immer wieder fallen auch große Projekte auf die Nase, weil sie sich indirekt und blind auf irgendein kleines Trivialpaket verlassen.

Im März 2016 traf es zum Beispiel den JavaScript-Transpiler Babel, der modernen JavaScript-Code in älteren Code für ältere Browser übersetzt. Babel nutzte das Paket left-pad, dessen frustrierter Entwickler es im Zuge eines Namensstreits depublizierte. Das brachte Babel ins Straucheln, ebenso wie viele andere Projekte, die left-pad nutzten, zahllose weitere Projekte, die Babel nutzten, und so weiter.

left-pad ist keine hilfreiche Bibliothek, die komplizierte Arbeit abnimmt, sondern besteht aus einer Handvoll Zeilen Code. Damit kann man Zeichenketten auf der linken Seite bis zu einer bestimmten Länge auffüllen. Diese Trivialität war eine Abhängigkeit, auf die sich alle möglichen Projekte blind verließen.

Auf Seite 76 lesen Sie, worauf man stößt, wenn man die Abhängigkeiten des Frontend-Frameworks Vue.js beforscht: ein wichtiges Projekt, das zahlreiche Größen der IT-Branche benutzen. Hinter Vue.js selbst steht aber keine solche Größe und mit dem Projekt alleine ist es auch nicht getan. Denn Vue benötigt zum Beispiel das erwähnte Kompatibilitätstool Babel. Und was ist mit den Projekten, auf die wiederum Babel aufbaut? Hinter jeder neuen Abhängigkeit kann sich eine Perle der Open-Source-Kultur, der Morast von verwahrlostem Code oder der Wahnwitz sinnloser Minimalpakete verbergen.

So interessant diese Überraschungen für NPM-Forschungsreisende sind: In eigenem Code will man sie nicht haben. Auf Seite 82 zeigen wir Ihnen deshalb, wie SBOMs helfen, den Überblick zu bewahren. In so einer „Software Bill of Materials“ finden sich alle Abhängigkeiten fein säuberlich aufgelistet. Und ab Seite 88 stellen wir SIEM-Werkzeuge vor („Security Information and Event Management“), die Sie schnell warnen, wenn akute Probleme auftreten. Mit solchen Tools wissen Sie immer, auf welchen Säulen ihre Systeme ruhen – und welche dieser Säulen eventuell bröckeln.

Wenn dann eine Sicherheitslücke entdeckt wird oder ein Projekt den Geist aufgibt, versinken Sie nicht in hektischem Chaos, sondern wissen gleich, welche Bereiche betroffen sind und was Sie beruhigt ignorieren können. Schnell reagieren müssen Sie im Fall der Fälle immer noch, aber Sie haben einen Plan und büßen weder im Diesseits noch im Jenseits für Ihre Trägheit. (syt) c't



Bild: Albert Hulm

Ein Framework unter der Lupe

Große Open-Source-Projekte sind ein Zusammenspiel vieler Komponenten, die wiederum aus Komponenten bestehen. Eine beispielhafte Reise in die Tiefen des Frameworks Vue.js verrät, auf wessen Schultern die meiste Last großer Projekte ruht, wer hinter Benutzer- und Organisationsnamen steckt und was ein komplexes Open-Source-Gebilde ins Wanken bringen kann.

Von **Jan Mahn**

Banken nutzen sie, Versicherungen, Autohersteller, Start-ups und Weltkonzerne. Den großen Frontend-Frameworks wie Angular, Vue.js und React begegnet man überall dort, wo Websites mehr tun sollen, als nur statische Informationen darzustellen. Die Frameworks betreiben interaktive Bestell- und Konfigurationsseiten, Kunden- und Mitarbeiterportale, Admin-Oberflächen und Onlinebankingseiten. Veröffentlicht ist der Code der Frameworks unter Open-Source-Lizenz, einsetzen darf man sie auch kommerziell ohne Lizenzkosten.

Um zu verstehen, was so große Open-Source-Projekte zusammenhält, ist ein genauerer Blick angebracht. Auf den nächsten Seiten graben Sie sich mit

uns anhand eines Beispielprojekts durch die Schichten aus Abhängigkeiten und stoßen zum Kern der Frage vor, wem Webentwickler die gut gepflegten, dokumentierten und nützlichen Werke wirklich zu verdanken haben – und wo die Probleme liegen, wenn Projekte auf zu wenigen Schultern lasten. Auf dem Weg werden Ihnen große und bekannte Akteure begegnen, unbekannte Einzelkämpfer und lose Grüppchen. Und Sie werden auf menschliche Schicksale und individuelle Karrierepfade stoßen, auf unternehmerische Probleme und die Auswirkungen der großen Weltpolitik auf harmlosen JavaScript-Code.

Von hinten aufgerollt

Als Forschungsobjekt haben wir uns das drittgrößte unter den Frontend-Frameworks vorgenommen: Vue.js (github.com/vuejs/core). Das wird bei GitHub gehostet, eingesetzt wird es unter anderem von dessen Mitbewerber GitLab. In der Liste der Unternehmen, die mit Vue.js arbeiten, finden sich außerdem Schwergewichte wie Facebook, Netflix, Nintendo und Adobe. Bevor Missverständnisse aufkommen: Das bedeutet nicht, dass diese Unternehmen direkt alle ihre Websites mit Vue.js gebaut haben – das Framework kann auch in internen Admin-Oberflächen oder kleinen Anwendungen stecken.

Vue.js unterscheidet sich in einem nicht unwesentlichen Detail von Angular und React: Dahinter steckt kein Weltkonzern. Erfinder und bis heute Maintainer ist Evan You, ein Softwareentwickler Anfang 30. Nach dem Studium wurde Google auf seine JavaScript-Basteleien im Internet aufmerksam und kontaktierte ihn. Zwei Jahre lang bezahlte das Unternehmen You dafür, dass er im „Creative Lab“ Prototypen für neue Bedienkonzepte in JavaScript entwickelte. Weil Googles Angular nicht so recht zur Art seiner Projekte passte, entstand bei You langsam die Idee, selbst

Glossar: Software im Team entwickeln

Contributor: Wer etwas zu einem Projekt beiträgt, darf sich Contributor nennen. Selbst wenn er nur einen Tippfehler in der Dokumentation beseitigt hat – für viele ist genau das der Einstieg in Open-Source-Projekte. Die Einstiegshürde ist niedrig, die meisten Softwareprojekte werden heute bei GitHub oder GitLab verwaltet. Mit einem Account dort kann jeder, der einen Fehler findet, beim Verbessern helfen.

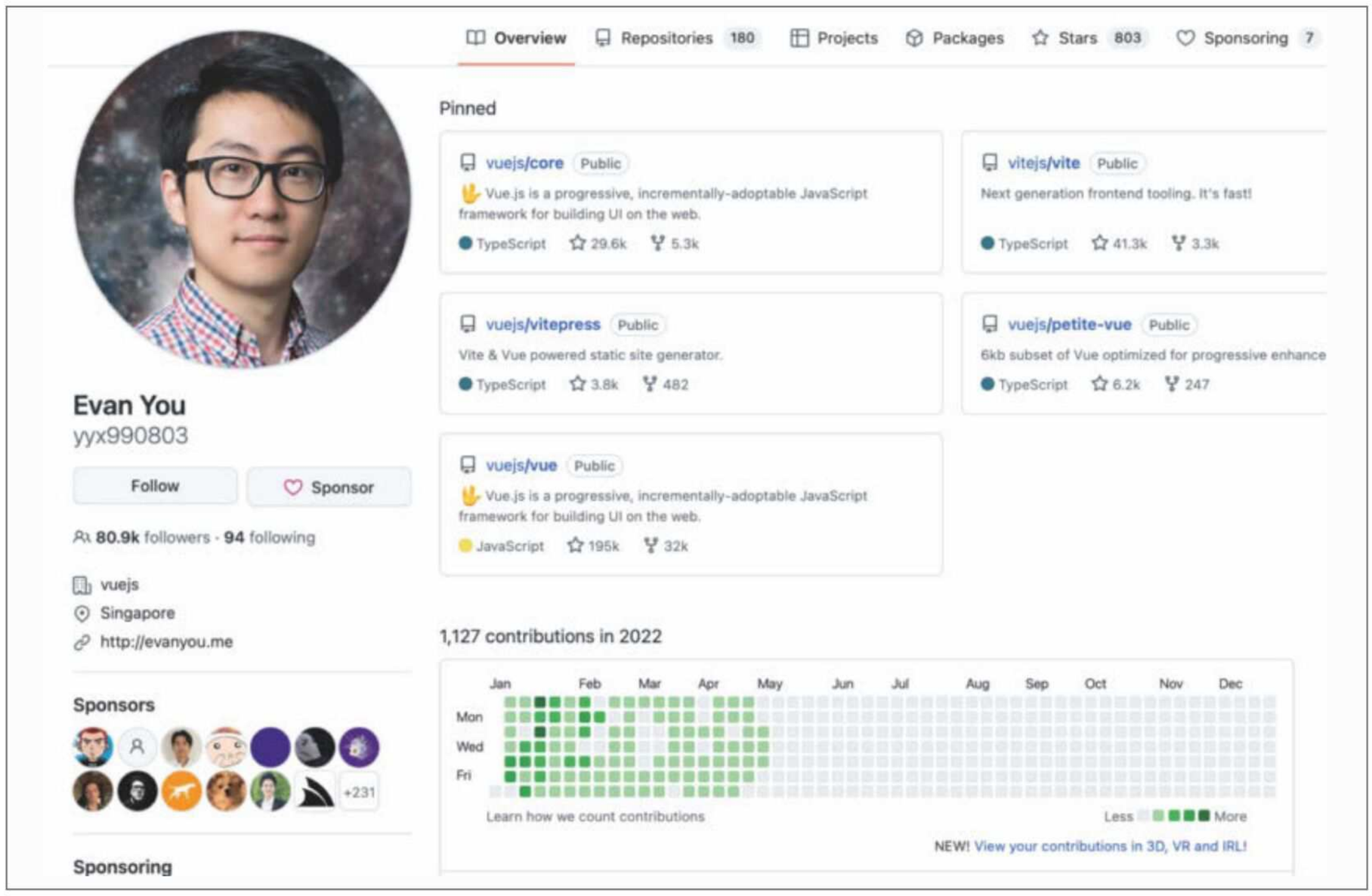
Maintainer: Nicht jeder, der etwas am Code ändern will, kann Änderungen direkt vornehmen. Jedes Projekt braucht einen oder mehrere Maintainer, die die Berechtigung haben, eingereichte Änderungen zu akzeptieren und in den Code aufzunehmen. Maintainer kümmern sich auch darum, die geplanten Funktionen für eine neue Version festzulegen und steuern, wohin sich das Projekt entwickelt.

Pull Request und **Merge Request:** Auf den Softwareverwaltungsplattformen GitHub und Bitbucket heißen sie Pull Request, GitLab nennt sie Merge Request. Gemeint ist dasselbe. Wer Änderungen an einer Software plant, legt zunächst einen sogenannten **Fork** an, eine Kopie der Code-Basis. Darin schreibt er all seine geplanten Änderungen und testet sie gründlich. Wenn er überzeugt ist, dass die Änderungen das Projekt voranbringen, stellt er einen Request mit diesen Änderungen an das Originalprojekt. Ein Maintainer prüft die Änderungen und entscheidet, ob sie reif für die Übernahme sind.

Commit: Ein Block aus Änderungen in der Versionsverwaltung Git heißt Commit. Er kann Änderungen in mehreren Dateien enthalten. Bestenfalls teilt man Commits so, dass sie immer nur ein Problem angehen und gibt ihnen präzise Beschreibungen. Das erleichtert später die Nachverfolgung von Änderungen.

Issue: Zum guten Stil in Projekten gehört es, nicht blind loszulaufen und die Community mit einem Pull Request zu überraschen. Erster Schritt ist ein Issue – die Übersetzung „Problem“ greift zu kurz, Issues können auch Wünsche oder Ideen sein. Meist werden sie erst diskutiert, bevor sich jemand an neue Entwicklungen macht und schließlich einen Pull Request anlegt.

Code Review: Bevor Maintainer Code in ihre Software übernehmen, prüfen sie ihn gründlich in einer Code Review. In einigen Projekten passiert das auch mehrstufig, bevor die Maintainer des Gesamtprojekts zustimmen, schauen sich Spezialisten für eine Baustelle den Code an und erstellen eine Review. Wenn dabei Probleme auftreten, kann der Code auch noch mal an den Ersteller gehen.



Evan You erfand Vue.js für den Eigenbedarf, heute spielt es in einer Liga mit Angular und React. Code für sein Projekt schreibt er immer noch.

ein eigenes kleines Framework zu erschaffen. Den ersten Commit bei GitHub veröffentlichte er im Juli 2013.

In Interviews spricht You immer wieder über seine damalige Motivation, die prototypisch für Open-Source-Projekte ist: Bei seinem Arbeitgeber Google fehlte ihm ein Projekt, in dem echte Menschen seine Entwicklungen nutzten. Mit Vue.js bekam er schnell, was er vermisste: Kollegen und immer mehr Fremde begannen, die Software auszuprobieren und einzusetzen. Der große Durchbruch kam 2014 mit einem Tweet von Taylor Otwell, seines Zeichens Erfinder und Maintainer des populären PHP-Backend-Frameworks Laravel. Otwell war unzufrieden mit seinen zähen Angular-Lernfortschritten und verkündete per Twitter, jetzt Vue.js zu lernen. Damit stand das kleine Framework schlagartig im Rampenlicht. Die schon damals große Laravel-Community gab Vue.js eine Chance, und die Nutzerzahlen stiegen rasant.

Beide Hände im Code

Auch 2022 ist Evan You noch Maintainer des Vue-Projekts, mittlerweile nicht mehr allein, sondern mit einem Core-Team aus insgesamt 19 Entwicklern. Ein Unternehmen oder eine andere Organisation steht bis heute nicht hinter dem Projekt, unter der Website vuejs.org steht weiterhin „Copyright © 2014-2022 Evan You“. You selbst hat keinen Arbeitgeber im klassischen Sinn, er arbeitet Vollzeit als Vue-Maintainer ohne klassischen Arbeitsvertrag. Um sein Auskommen muss man sich aber wohl keine Sorgen machen, immerhin zählt er auf seiner Homepage Uhrensammeln als Hobby auf. Bezahlt wird er über Firmen, die im Vue-Kontext unterwegs sind und ihr Logo gern unter „Sponsors“ auf der Projektseite sehen. Das sind vor allem Agenturen, die mit Vue.js Projekte für Kunden entwickeln und Anbieter von Vue-Trainings. Außerdem gibt es Vue-Konferenzen auf der ganzen Welt, die das Kernprojekt und dessen Verantwortliche finanziell unterstützen.

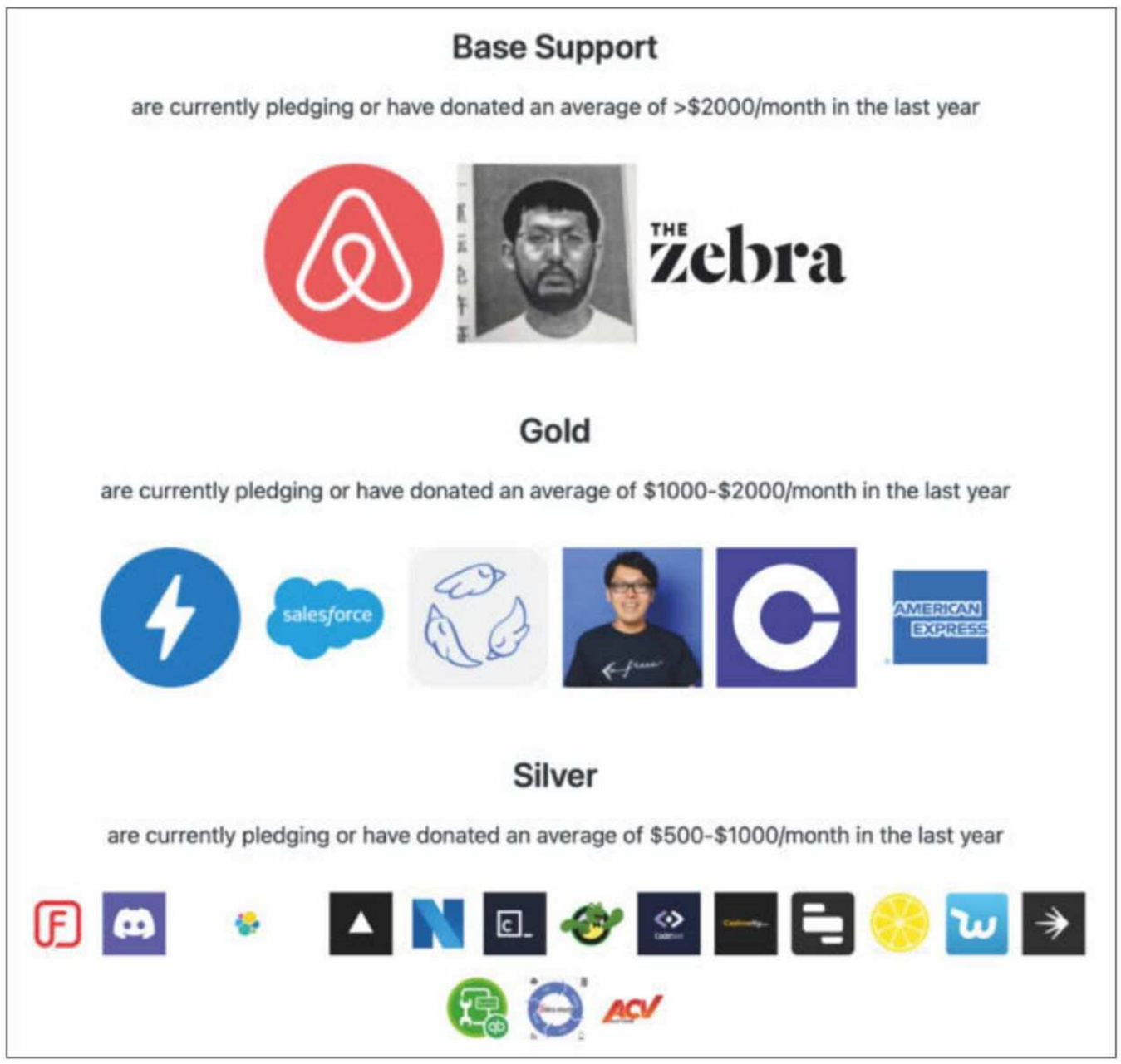
Die meisten weiteren Maintainer neben You dagegen arbeiten für andere Unternehmen, darunter zum Beispiel GitLab. Bei einem genaueren Blick auf Evan Yous GitHub-Profil (Benutzername yyx990803) sticht sofort seine regelmäßige Arbeit ins Auge – es vergeht kaum ein Tag ohne Beitrag. Und anders als andere Maintainer, deren Projekte so groß geworden sind, sieht You seine Aufgabe bis heute im Programmieren: Im laufenden Jahr 2022 sind 92 Prozent seiner

GitHub-Beiträge Commits, also eigener Code, nur ein Prozent machen Code Reviews aus.

Dass You selbst so aktiv und eine zentrale Figur ist, kann – wie jede One-Man-Show – langfristig zum Problem werden. Ein gesundheitsbedingter Ausfall wäre ein ernstes Problem für das Projekt. Die Tatsache, dass keine Firma hinter dem Projekt steht, ist dagegen eher kein Problem – wenn auch ungewohnt für Deutsche, die in einem solchen Fall mindestens einen eingetragenen Verein erwarten.

Und darunter?

Auf dem nächsten Teil der Reise gehts von der oberen Ebene des Projekts zu den Abhängigkeiten. Bei JavaScript-Projekten, die den Paketmanager NPM nutzen, findet man sie in Dateien mit dem Namen package.json. Einen besseren Überblick bekommt man mit programmiersprachenunabhängigen Software-Teilelisten, sogenannten SBOMs. Wie die funktionieren und wie man sie auswertet, lesen Sie ab Seite 82. Mithilfe des dort vorgestellten Werkzeugs Dependency-Track haben wir uns auch die Abhängigkeiten von Vue.js angesehen.

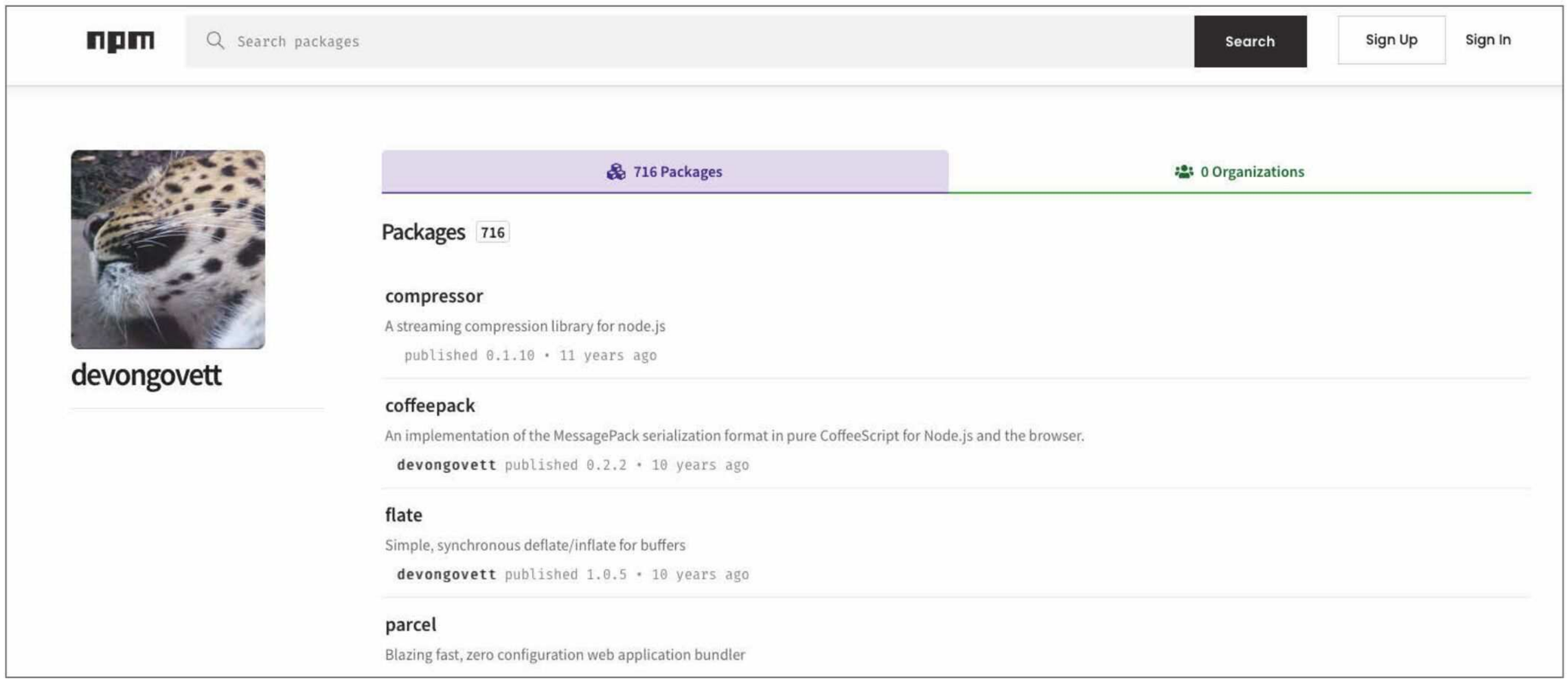


Obwohl große Akteure wie Salesforce und Airbnb monatlich Geld an Babel zahlen, meldete das Projekt 2021 finanzielle Probleme. Die Maintainer zahlen sich ein überschaubares Gehalt aus.

Eine kaum zu übersehende Säule, auf der Vue.js steht, sind die zahlreichen Pakete aus dem Babel-Projekt. Babel (babeljs.io) übersetzt modernen und effizienten ECMAScript-Code, eine syntaktisch verbesserte JavaScript-Variante bei Bedarf in alte JavaScript-Syntax, die auch alte Browser verstehen. So können Entwickler alle Annehmlichkeiten der modernen Sprache nutzen, ohne den untoten Internet Explorer 11 abzuhängen oder sich um kleine Unterschiede zwischen Browsern kümmern zu müssen. Perspektivisch könnte Babel irgendwann gänzlich obsolet werden, wenn die Browserhersteller die kleinen Unterschiede beseitigt haben.

Auch hinter Babel steht kein Unternehmen und wie bei Vue gibt es auch keine natürliche Person und keine Rechtsform. Am ehesten kann man das Projekt als „nicht-eingetragenen internationalen Verein ohne festen Sitz“ beschreiben. An dieses Organisationsmodell muss man sich in diesen Teilen der Open-Source-Welt gewöhnen. Die Aufgabe eines Vereinsregisters übernehmen GitHub (für den Code) und die Plattform Open Collective (opencollective.com), auf der die Finanzierung des „Vereins“ verwaltet wird. Damit andere Unternehmen solchen losen Zusammenschlüssen Geld zukommen lassen können, gibt es dort das Modell des sogenannten „Fiscal hosting“: Eine zwischengeschaltete Organisation, in diesem Fall das „Open Source Collective“ nimmt das Geld an, verwahrt es und lässt es dem Projekt zukommen – nach Abzug von Verwaltungskosten. Die Sponsoren bekommen von der in den USA registrierten gemeinnützigen Organisation eine Bescheinigung für ihre Unterlagen.

Organisatorisch scheint Babel gut aufgestellt, sechs Maintainer teilen sich die Arbeit. Auf der Homepage erfährt man, dass zum Beispiel die Wohnungsvermittlerplattform Airbnb als „Base Supporter“ monatlich über 2000 US-Dollar an das Projekt überweist. Bis zu 2000 US-Dollar pro Monat ist das Projekt unter anderem Salesforce, Coinbase und American Express wert. Weitere Unternehmen zahlen kleinere Beträge. Was nach viel Geld klingt, ist aber offenbar nicht so rosig: Die Maintainer sollten Vollzeit von dem Geld bezahlt werden, doch dafür reichte plötzlich das Geld nicht mehr. Im Mai 2021 wandten sie sich mit einem Blogbeitrag an die Community: 333.000 US-Dollar, so rechneten sie vor, bräuchten



Viel vorgenommen: Der Entwickler Devon Govett hat 748 Pakete bei NPM veröffentlicht, darunter viele Basis-Funktionen, die von anderen Paketen benutzt werden.

sie, um sich überschaubare Gehälter von 2000 US-Dollar auszuzahlen – nicht gerade ein Vermögen für IT-Spezialisten. Nur knapp die Hälfte, also rund 150.000 US-Dollar kamen laut Blogbeitrag jährlich zusammen. Was zuerst stabil und solide aussieht, entpuppt sich leider bei genauerem Hinsehen als allzu bröckelige Säule des Webs.

Tausendsassa

Auf ein ganz anders gelagertes Problem stießen wir beim unauffälligen Paket mit dem Namen „brotli“. Das lädt Vue.js als Abhängigkeit für Entwicklungsumgebungen, es handelt sich um eine Implementierung des Brotli-Kompressionsalgorithmus, der 2014 bei Google erfunden wurde und in Schriftarten im „Web Open Font Format“ (WOFF2) zum Einsatz kommt. Geschrieben hat das Brotli-Paket der Entwickler Devon Govett mit dem NPM- und GitHub-Benutzernamen devongovett, im Hauptberuf Entwickler bei Adobe. Das Paket selbst hat nur eine eigene Abhängigkeit, eine kleine Base64-Bibliothek namens base64-js. Auch die stammt von einem Einzelentwickler, dem Amerikaner Jameson Little (beatgammit). Dessen Base64-Implementierung ist sowas wie der Sockel zahlreicher großer Säulen des JavaScript-Universums. Laut GitHub steckt sie in über 10 Millionen Projekten. Aber auch Devon Govetts brotli ist ein viel gefragtes Paket. Es verbirgt sich in 236 anderen NPM-Paketen und hat laut NPM ganze 1,7 Millionen wöchentliche Downloads. Für ein so bedeutendes Projekt ist es erschreckend schlecht aufgestellt. Vor ziemlich genau fünf Jahren, im Mai 2017 erschien die letzte Version (1.3.2). Das NPM-Paket liegt im privaten Account von Devon Govett, das zugehörige GitHub-Repository hat er auf die GitHub-Organisation foliojs übertragen – ein Projekt, das er mit seinem Kumpel Luiz Américo zusammen betreut. Kein großes Team und kein Unternehmen.

Govett scheint ein Händchen dafür zu haben, sich Arbeit aufzuhalsen: Unfassbare 748 NPM-Pakete hat er in seiner Karriere angehäuft, längst nicht alle bekommen Aktualisierungen, wobei man manches sicher als ausentwickelt betrachten kann. Doch die schiere Menge ist nicht genug – zielstrebig oder unfreiwillig hat er sich auch Programmierherausforderungen gesucht, die elementare Probleme lösen und heute Grundlagen für andere Bibliotheken sind, die wiederum Grundlage für andere sind. Neben der Brotli-Implementierung hat er sich Encoder und Decoder für Audio, Bilder und Videos sowie weitere Kompressionsalgorithmen heraus-

gepickt. Wer einen Beleg dafür sucht, auf welch wackligen Säulen manches in der heutigen Softwareentwicklung steht, wird bei Govett fündig. Von einem Tag auf den anderen zusammenbrechen kann aber auch dieses Gebilde nicht mehr, selbst wenn Govett im hypothetischen Fall die NPM-Welt brennen sehen wollte und bei allen Projekten den Stecker ziehen wollte: NPM verhindert mittlerweile immerhin, dass Projekte über Nacht depubliziert werden. Im schlimmsten Fall könnte er kaputte neue Versionen veröffentlichen, die alten blieben aber erhalten.

Weltpolitik und Code

Die letzte Etappe der Reise führt raus aus dem Unterbau von Vue.js in eine andere Ecke des Vue-Ökosystems. Bei der Recherche stießen wir auf eine besonders bedrückende Diskussion bei GitHub über das Projekt BootstrapVue. Das hat es sich zur Aufgabe gemacht, Komponenten aus dem CSS-Framework Bootstrap in Vue.js bereitzustellen. Die aktuell größte Aufgabe dieser Community: ihr Werk für das vergleichsweise neue Vue.js 3 und Bootstrap 5 vorzubereiten – ein umfangreiches Unterfangen. Und so war die Freude groß, als sich am 14. Dezember 2021 der GitHub-Nutzer xanf zu Wort meldete (zu finden über ct.de/wftd) und verkündete, dass er mit einem Maintainer-Team diese Herausforderung annehmen wolle. Hinter dem Benutzernamen steckt Illya Klymov, hauptberuflich Frontend-Entwickler bei GitLab. Es folgten immer wieder Status-Updates der Umbauarbeiten und der Umbau schien auf einem guten Weg. Am 1. März 2022 dann der Schock. Wieder meldete sich xanf zu Wort, diesmal mit einer nicht-technischen Nachricht: „Sorry, no deadlines atm – we have Russia invasion in our country (Ukraine) and I'm writing this post from a shelter in Kharkiv, which is under rocket attacka for a few days." Seitdem gibt es dennoch Fortschritte beim Projekt, und trotz der Umstände vermeldete der Entwickler zwischendurch, aktuell an der kompliziertesten Komponente, der für Tabellen, zu arbeiten. Auch BootstrapVue organisiert seine Sponsoren über Open Collective und bezahlt Klymov darüber. Der Fall zeigt aber leider, dass Finanzierung und Organisationsstruktur manchmal nicht alles sind. Am Ende stehen auch hinter Organisationsnamen engagierte Menschen mit eigenen Schicksalen und Problemen.

Dass Einzelkämpfer mit ihren privaten GitHub-Repositories das Web zusammenhalten, ist schlicht unvernünftig.

Zu groß zum Scheitern?

Was bleibt nach dieser Reise durch die JavaScript-Paketquellen? Zum einen die Erkenntnis, dass sich Open-Source-Projekte mittlerweile sehr professionell organisieren können und Wege finden, international zusammenzuarbeiten. Um Vue.js selbst muss man sich am wenigsten Sorgen machen, aber schon beim aktuell unverzichtbaren Babel sieht es finanziell problematisch aus. Projekte, die Grundlagentechnik im Verborgenen bauen, haben es auf dem Sponsorenmarkt nicht so leicht wie ein schillerndes Frontend – schließlich liegt es ja in ihrer Natur, dass sie nicht im Mittelpunkt stehen und man von ihrer Existenz bestenfalls nichts mitbekommt.

Richtig problematisch sind die Lebenswerke von Einzelkämpfern, die teils vor vielen Jahren sehr grundlegende Probleme gelöst haben. Die stützen heute mehr oder weniger unfreiwillig die Fundamente des Webs, ohne Kontrolle, ohne Organisationsstruktur und mit vielen offenen Fragen. Hier ist klar die ganze Community gefragt: Für grundlegende Funktionen bräuchte man eine starke und die Zeiten überdauernde Organisation wie die Linux-Foundation, die den Linux-Kernel organisatorisch betreut, oder deren Tochterorganisation, die OpenJS-Foundation, die sich um NodeJS kümmert.

Als Webentwickler mögen diese Zustände gruselig klingen und dazu verleiten, künftig Anwendungen ohne fremde Hilfe und ohne Abhängigkeiten schreiben zu wollen. Richtig zielführend ist aber auch das meist nicht – und keinesfalls automatisch besser oder sicherer. Angesichts der vielen großen Unternehmen auf Nutzerseite wären Sie immerhin nicht allein, wenn irgendwo existenzielle Probleme aufträten. Wichtig ist aber in jedem Fall, sich beim Laden neuer Pakete einen kritischen Blick anzugewöhnen und jederzeit einen Überblick zu haben. Mehr dazu auf den folgenden Seiten. (jam) c't

Projekte und Akteure

ct.de/wftd

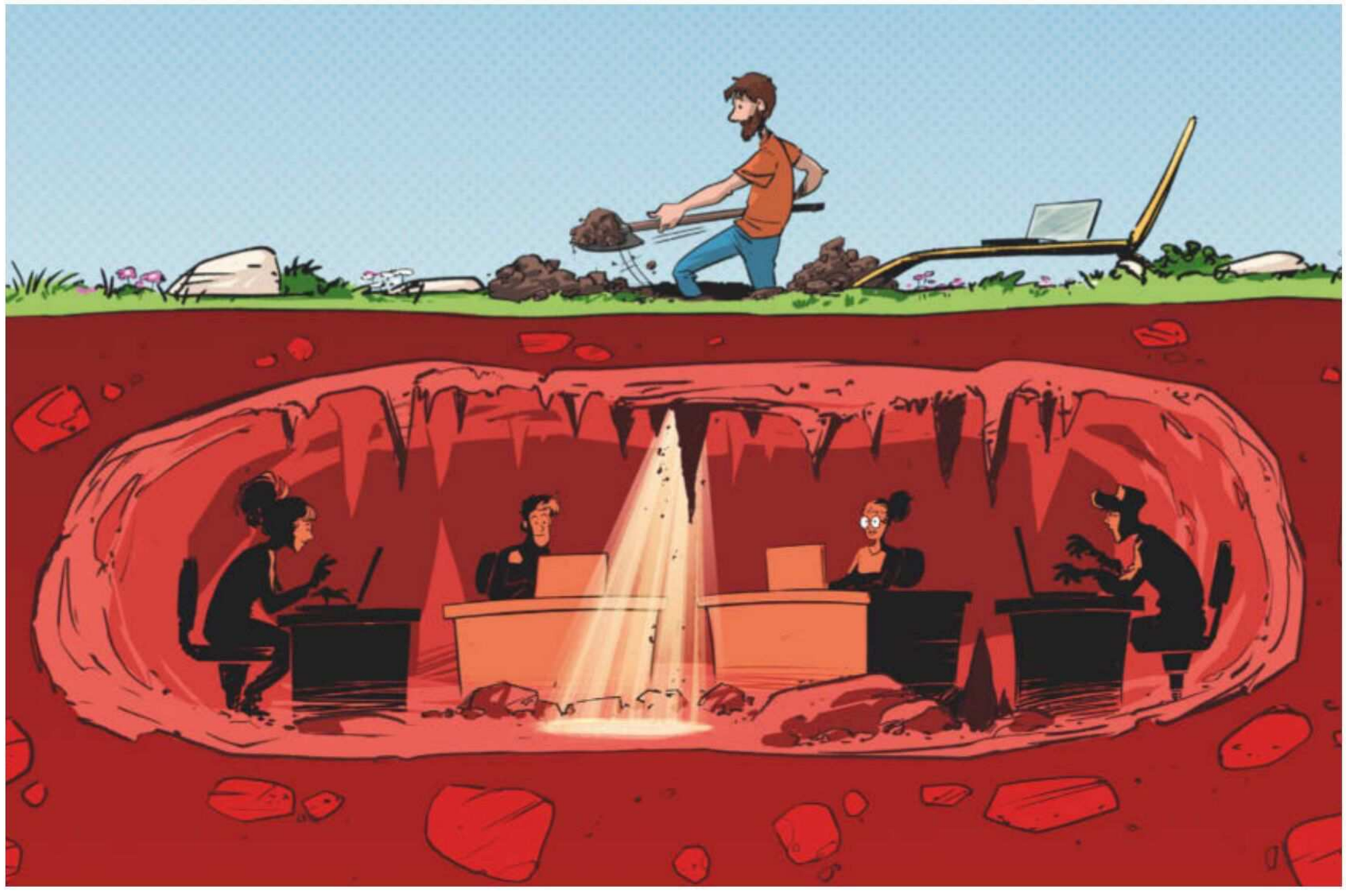


Bild: Albert Hulm

Abhängigkeiten erkennen

Fast jede Software hängt von anderen ab. Wer da den Überblick verliert, handelt sich massenweise Probleme etwa in Gestalt von Sicherheitslücken ein. Software-Teilelisten, sogenannte SBOMs, versprechen Einblicke. Die volle Kontrolle bekommen Admins und Entwickler – na klar – mit einem weiteren Werkzeug: Dependency-Track.

Von **Manuel Ottlik**

Die Sicherheitslücke in der Java-Log-Bibliothek Log4j löste Ende 2021 Schockwellen in vielen Unternehmen aus. Eine harmlose Logging-Bibliothek konnten Angreifer leicht dazu überreden, Schadcode aus dem Internet zu laden. Was Admins und Beobachter überraschte, war nicht nur, dass eine ziemlich leicht zu missbrauchende Funktion so lange in einer so verbreiteten Bibliothek wie Log4j überleben konnte. Überraschend war vor allem das Treiben in vielen IT-Abteilungen – hektisch wurden vieler-

orts per Hand Tabellen mit verwendeter Software zusammengetragen und auf den Suchbegriff „Java“ gefiltert. Dann begann eine mühsame Suche, bei eigener Software im Quellcode, bei gekaufter Software in Dokumentationen und mit Mails an den Hersteller. Die verzweifelten Fragen: „Wo zur Hölle könnte in unserem Netzwerk Log4j stecken? Haben wir vielleicht etwas übersehen?“ Probleme, die sich nicht auf Mittelständler mit Admin-Einzelkämpfern beschränkten. Unsere Redaktion erreichten auch Berichte, wie die IT-Abteilungen großer Konzerne mit der Frage umgingen. Selbst wenn es einen CISO (Chief Information Security Officer) und ganze Teams für IT-Sicherheit gab, gingen interne Mails an alle Abteilungen und ihre Leitungen. Die sollten schnellstmöglich prüfen und bestätigen, dass die eingesetzten Anwendungen frei von Log4j oder abgesichert seien.

Was sich all diese Softwarebetreiber in diesem Moment wünschten: eine zentrale interne Datenbank, die sämtliche Abhängigkeiten aller Anwendungen kennt. Am besten natürlich durchsuchbar und mit einer Anbindung an Sicherheitslückendatenbanken. In einer perfekten Welt hätte man nur „log4j“ in ein Suchfeld eintippen müssen, um sämtliche Vorkommen der betroffenen Bibliothek im eigenen Betrieb zu finden – feinsäuberlich aufgeschlüsselt nach Projekt und mit der jeweiligen Version. Für einzelne Programmiersprachen gibt es bereits Ansätze, die Abhängigkeiten eines Projekts auf Schwachstellen überprüfen. In der JavaScript-Welt greift man etwa zum Befehl `npm audit`. Doch damit ist einer IT-Abteilung, die außerdem noch Docker-Container, .NET, Java-Applikationen und Python-Skripte im Einsatz hat, nur bedingt geholfen. Kaum jemand wird ausschließlich Anwendungen in einer einzigen Programmiersprache nutzen und mit vielen fragmentierten Informationsquellen ist niemandem geholfen.

Software Bill of Materials

Man braucht etwas, das unabhängig von einer bestimmten Sprache oder einem Framework funktioniert. In anderen Industriezweigen gibt es das schon seit Langem: eine strukturierte Materialliste, eine „Bill of Materials“. So etwas gibt es auch für Software, die sogenannte „Software Bill of Materials“, kurz SBOM. Ähnlich wie bei der Zutatenliste auf dem Lieblingsmüsli enthält eine SBOM alle Komponenten, aus denen eine Software besteht – und zwar in einem standardisierten und maschinenlesbaren Datenformat. Darin stehen alle NPM-Pakete, die ein JavaScript-Frontend benötigt, und alle Pip-Pakete, die ein Python-Projekt voraussetzt.

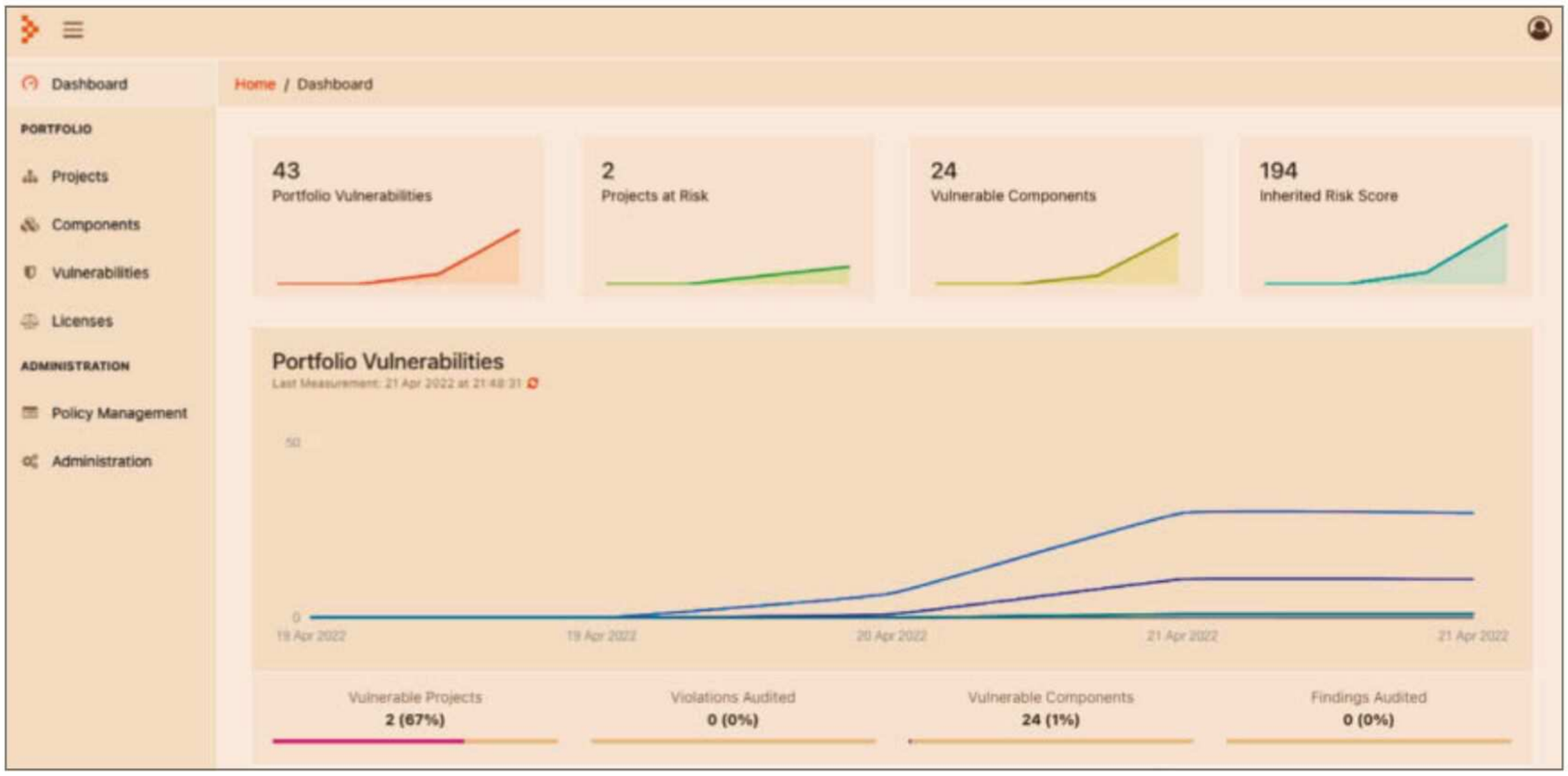
International steigt die Verbreitung von SBOMs aktuell: In den USA sind sie durch eine Executive Order des Weißen Hauses im Mai 2021 verpflichtend für alle Softwarehersteller geworden, die an Behörden liefern (siehe ct.de/wtw3) – im deutschen IT-Grundschutz-Kompendium ergibt die Suche nach „SBOM“ und ähnlichem aktuell dagegen keine Treffer.

Die populärste Spezifikation für SBOMs heißt CycloneDX, ein Open-Source-Projekt, hinter dem die in Sicherheitsfragen aktive OWASP Foundation steckt. CycloneDX spezifiziert eine Datei, die alle Bestandteile einer Software strukturiert auflistet. Sie kann in XML oder JSON verfasst werden und setzt auf bereits bestehenden Standards wie „Package URL“ (PURL) und „Common Platform Enumeration“ (CPE) auf, um die Komponenten selbst eindeutig zu identifizieren. Informationen zu beiden finden Sie über ct.de/wtw3. Mit dem CycloneDX-SBOM-Standard können Anwendungen, Container, Betriebssysteme und Firmware sowie Frameworks und Bibliotheken beschrieben werden. Außerdem gibt es im CycloneDX-Kosmos noch andere BOMs aus dem IT-Kontext, beispielsweise für Software-as-a-Service (SaaSBOM).

Ein simples CycloneDX-Dokument im JSON-Format sieht zum Beispiel wie folgt aus:

```
{
 "bomFormat": "CycloneDX",
 "specVersion": "1.2",
 "version": 1,
 "components": [
  {
   "name": "example-library",
   "group": "example-user",
   "type": "library",
   "version": "1.3.5",
   "description": "Just an example",
   "licenses": [
    { "license": {"id": "MIT"} }
   ],
   "purl":"pkg:composer\/example-user↵
            ↳\/example-creator@1.3.5"
  }
 ]
}
```

Es beginnt mit Metadaten, danach folgt unter dem Schlüssel `components` eine Liste von Bestandteilen. Für jede Komponente wird verpflichtend ein Name und ein Typ angegeben. Weitere Angaben zur Iden-



Mit einem Blick wissen Sie dank Dependency-Track, wie es um die Sicherheit Ihrer Systeme steht.

tifikation sind laut Standard optional, aber ratsam, damit Pakete später eindeutig und automatisch identifiziert werden können. Die PURL im obigen Beispiel verrät, dass es sich um ein Paket aus dem PHP-Paketmanager Composer handelt.

Neben Paketen darf eine SBOM auch externe Dienste auflisten, auf die die Software zugreift. Wenn Ihre Software also zum Beispiel Wetterdaten von einem externen API bezieht, würde sich diese Schnittstelle unter `services` wiederfinden. Ähnlich einer Lieferkette in der Industrie kann eine SBOM auch eine Baumstruktur mit weiteren indirekten Abhängigkeiten enthalten. Wenn bei der Erstellung der SBOM bereits Schwachstellen bekannt sind, können diese unter `vulnerabilities` abgelegt werden. Welche Datenfelder CycloneDX darüber hinaus noch bereithält, verrät die gut aufbereitete CycloneDX-Dokumentation (zu finden über ct.de/wtw3).

Übersicht mit Dependency Track

Falls Sie jetzt als Entwickler die Angst überkommt, künftig neben Programmcode, Unit Tests und Dokumentation auch noch SBOMs schreiben zu müssen, seien Sie beruhigt: Diese Fleißarbeit übernehmen Kommandozeilenwerkzeuge, die es für alle gängigen Programmiersprachen gibt. Dazu später mehr – zunächst zur Perspektive der Admins, die von ihren Softwareherstellern SBOMs bekommen haben. Dass Hersteller SBOMs bereitstellen, ist heute noch keinesfalls selbstverständlich und bisher haben sich auch keine zentralen Anlaufstellen wie ein „SBOM-Hub“ zum Download der Dokumente etabliert. Es bleibt nur ein Blick in die Dokumentation oder bei Kaufsoftware eine vertragliche Vereinbarung mit dem Hersteller. Je mehr Kunden es schaffen, ihre Hersteller zu überzeugen, desto schneller kann sich der Standard durchsetzen.

Mit den Dokumenten in JSON oder XML allein ist Ihnen aber auch noch nicht viel geholfen; Sie brauchen ein Werkzeug, das die SBOMs einliest, die Komponenten auf Schwachstellen analysiert und die Ergebnisse anschaulich darstellt. Genau das macht Dependency-Track: Für jede Software, die in einer Organisation verwendet wird, legt man künftig in Dependency-Track ein Projekt an, hinterlegt Software, Versionsnummer und SBOM und bekommt Übersichten über den aktuellen Zustand schön aufbereitet in einem Web-Frontend.

Dort finden Sie Tabellen zu verwendeten Bausteinen, deren Lizenzen sowie Baumstrukturen mit weiteren Abhängigkeiten. Die wichtigste Funktion ist aber die Analyse der Komponenten auf bekannte Schwachstellen. Abgeglichen wird einmal täglich gleich mit mehreren Schwachstellendatenbanken: der National Vulnerability Database (NVD), dem Sonatype OSS Index, den NPM Audit Advisories, der GitHub Advisory Database und optional auch mit dem kostenpflichtigen Dienst VulnDB. Alle Schwachstellen können Sie in einer Tabelle in Dependency-Track einsehen und erfahren auch direkt, welche Ihrer Projekte von der Schwachstelle betroffen sind.

Damit Sie im Ernstfall schnell informiert werden, kann die Software E-Mails oder Benachrichtigungen für Microsoft Teams, Slack oder sonstige Webhook-fähige Systeme versenden.

Dependency Track zeigt außerdem an, ob es für eine verwendete Komponente schon eine neuere Version ohne Schwachstelle gibt, die Sie verwenden könnten. Dafür werden die Paketmanager der unterschiedlichen Programmiersprachen abgefragt. Das funktioniert sogar für private Pakete, die Sie in Ihrer firmeninternen Paket-Registry liegen haben. Diese können Sie als zusätzliche Quelle in Dependency-Track hinterlegen.

Die Plattform gleicht eingesetzte Software nicht nur gegen externe Datenbanken ab, sondern erlaubt auch eigene Richtlinien (Policies) zu erstellen, die aus mehreren Bedingungen bestehen dürfen. So können Sie etwa überprüfen lassen, ob eine Anwendung Schwachstellen eines gewissen Schweregrads hat oder eine bestimmte Komponente in einer problematischen Version enthält. Auf dem Screenshot unten sehen Sie, wie Sie mit einer einfachen Policy alle Anwendungen identifizieren, die Log4j mit der berühmten Sicherheitslücke nutzen. Wenn die Bedingungen zutreffen, wird eine „Policy Violation“ an der Anwendung markiert. Jeder Policy können Sie dabei auch einen Schweregrad zuweisen, der bei Verstoß aufleuchtet. Das funktioniert nicht nur für Sicherheitsprobleme, sondern auch für Lizenz-Informationen, die an jeder Komponente in der SBOM vermerkt sind. So können Sie zum Beispiel erkennen, wenn eine Bibliothek oder Software ihr Lizenzmodell ändert und plötzlich zum Problem wird.

Live und in Farbe

Viele dieser Funktionen richten sich zweifelsohne an große Organisationen, die Mitarbeiter nur für solche Sicherheits- und Lizenzfragen beschäftigen können. Auch an LDAP-Anbindung und Berechtigungsverwaltung ist gedacht. Dass Dependency-Track so viele Funktionen mitbringt, sollte Sie aber auch in einer kleineren Umgebung nicht abschrecken, die Software auszuprobieren und zu nutzen. Installation und Einstieg sind nämlich denkbar einfach. In wenigen Minuten fahren Sie die Umgebung als lokale Umgebung mit Docker hoch (eine ausführliche Installationsanleitung finden Sie über ct.de/wtw3).

Die Dependency-Track-Entwickler bieten eine Docker-Compose-Datei an, mit der Sie die Plattform ausprobieren können. Laut Doku werden mindestens 4,5 GByte Arbeitsspeicher und zwei CPU-Kerne gefordert, im Test kamen die beiden Container aber auch mit deutlich weniger RAM klar. Laden Sie sich die Docker-Compose-Datei herunter (siehe ct.de/wtw3) und starten Sie die Software mit:

```
docker compose up -d
```

Unter der Adresse http://localhost:8080 finden Sie dann das Frontend. Mit dem Benutzernamen `admin` und dem initialen Passwort `admin` können Sie sich anmelden. Nachdem Sie das Passwort geändert haben, wählen Sie im Menü „Projects“ aus, erstellen mit dem Button „Create Project“ ein neues Projekt und tragen einen Namen und optional weitere Details des Projekts ein. Wenn Sie im Reiter „Components“



Keine Angst vor Log4j: Dependency-Track warnt aufgrund einer passenden Richtlinie vor problematischen Bibliotheksversionen in einer Anwendung.

unter „Upload BOM“ eine SBOM-Datei im CycloneDX-Format hochladen, wird sie anschließend analysiert.

Falls Ihre Softwarelieferanten noch keine SBOMs bereitstellen und Sie zum Ausprobieren von Dependency-Track auch keine selbst generieren möchten, finden Sie eine Auswahl an Beispielen zum Download über ct.de/wtw3. Mit einem geladenen BOM und echten Sicherheitsproblemen bekommen Sie schnell ein Gefühl, was mit Dependency-Track möglich ist und welche Funktionen Sie im Alltag nutzen möchten.

SBOMs generieren

Der folgende Abschnitt richtet sich an alle, die selbst Software entwickeln, vertreiben oder vermieten und SBOMs im CycloneDX-Format anbieten möchten oder sollen. Die gute Nachricht: Rund um das noch recht junge Format – CycloneDX 1.0 erschien im März 2018 – hat sich schnell eine große Open-Source-Gemeinschaft gebildet, die unter anderem SBOM-Generatoren für unterschiedlichste Programmiersprachen und Techniken bereitstellt. Die funktionieren nicht für jede Sprache identisch: Für Node.js-Projekte werden SBOMs über einen Kommandozeilenaufruf generiert, für Java-Projekte gibt es ein Maven-Plug-in, das Sie Ihrem Projekt hinzufügen müssen. Nicht alle Generatoren setzen den CycloneDX-Standard schon komplett um: Das CLI für Node.js unterstützt aktuell noch keine Dependency-Trees und das Werkzeug für PHP-Projekte hat gerade einmal 15 Sterne auf GitHub, steht also noch ganz am Anfang seiner Karriere. Beide erzeugen aber gültige SBOMs, die Dependency-Track auswerten kann. Wenn Sie auf der Suche nach einem Generator für Ihre Programmiersprache sind, ist das „Tool Center“ von CycloneDX, eine Übersicht über alle Projekte, die erste Anlaufstelle, zu finden unter cyclonedx.org/tool-center.

Generieren ganz praktisch

Um ein Gefühl zu bekommen, wie wenig Arbeit das Generieren von SBOMs macht, können Sie die Arbeitsschritte an einem Beispiel nachvollziehen. Dafür haben wir ein Projekt aus einem JavaScript-Artikel von Ende 2020 herausgesucht, der schon länger nicht aktualisiert wurde – die Chancen, Sicherheitslücken zu finden, stehen also gut. Den Code bekommen Sie über ct.de/wtw3 aus einem GitHub-Repository, die fertige Datei liegt da bereits unter 02-application/sbom.json. Über das Tool Center finden Sie schnell ein geeignetes Werkzeug für JavaScript, installiert wird es mit:

```
npm install -g @cyclonedx/bom
```

Laden Sie anschließend das Beispiel-Repository oder ein anderes JavaScript-Projekt herunter und navigieren auf der Kommandozeile in den Ordner, in dem die Datei package.json liegt. Den Generator starten Sie dann mit

```
cyclonedx-node --include-dev \
--include-license-text \
--type application \
--output bom.json
```

Die erzeugte Datei können Sie anschließend in Dependency-Track hochladen. Die Plattform verarbeitet die SBOMs aber asynchron – wundern Sie sich also nicht, wenn nicht augenblicklich die Alarmglocken schrillen. Nach ein paar Minuten zeigt Dependency-Track die Anzahl der Schwachstellen an, aufgeteilt nach Schweregrad. Im Tab „Audit Vulnerabilities“ sehen Sie eine Liste aller Schwachstellen, die Dependency-Track beim Abgleich mit den Datenbanken identifiziert hat.

Dependency-Track findet für das Beispielprojekt eine kritische Sicherheitslücke in der Bibliothek lodash. Wenn Sie in Zukunft immer direkt informiert werden wollen, wenn diese problematische Bibliothek irgendwo auftaucht, legen Sie sich eine Policy dafür an: Wechseln Sie dafür im Menü auf „Policy Management“ und klicken dort auf „Create Policy“. Vergeben Sie einen Namen und erstellen Sie anschließend eine Bedingung für die sogenannten „Coordinates“ (den vollen Namen einer Bibliothek), in diesem Fall „lodash > 4.0.0“. Weil auch die Policy Violations asynchron geprüft werden, müssen Sie ein paar Minuten warten – dann sehen Sie an dem erstellten Projekt unter dem Tab „Policy Violations“ sieben Verstöße gegen Ihre neue Richtlinie. Auf dem gleichen Wege können Sie Pakete auf deren Lizenz überprüfen: Erstellen Sie zum Beispiel eine Policy mit dem Namen „keine OS-Lizenz“, verändern Sie den Operator der Bedingungen auf „All“ und nehmen Sie in den Bedingungen mit „Licence / is not“ alle Lizenz-Arten auf, die Sie akzeptieren möchten. Für jede Komponente, die keine dieser Lizenzen verwendet, wird dann eine Violation generiert. Wenn Sie nicht auf das nächste Prüfintervall warten wollen, können Sie die SBOM einfach erneut hochladen – dann startet Dependency-Track die Analyse auch außerhalb des Intervalls.

Continuous Security Monitoring

Als Entwickler könnten Sie Ihre generierte SBOM jetzt irgendwo hochladen, wo Ihre Nutzer sie finden und bestenfalls auch per Skript herunterladen können; in der Dokumentation können Sie auf den Link verweisen. Vom CycloneDX-Projekt gibt es auch einen einfachen Repository-Server zum Selbsthosten, auf den Sie SBOMs hochladen können (zu finden im Tool Center). Es reicht aber auch ein beliebiger Webserver. Sobald Sie den Prozess der Bereitstellung einmal per Hand durchgespielt haben, sollten Sie die Schritte umgehend automatisieren. Das Generieren von SBOMs können Sie am besten einer CI/CD-Umgebung wie GitLab oder GitHub Actions überlassen. Dann können Sie sicher sein, dass die SBOM mit jeder Änderung am Code aktualisiert wird. Für CI/CD-Integrationen finden Sie auf der CycloneDX-Seite ebenfalls Projekte. Die sind aber teilweise noch etwas spärlich und unflexibel. Einfacher ist es meist, den Befehl für einen passenden Generator selbst in eine CI/CD-Aktion zu verpacken und auch den Upload auf Ihren Server einzubauen.

Wenn Sie als Softwarenutzer einen Weg finden, SBOMs automatisiert zu beziehen (bei eigener Software aus Ihrer CI/CD-Umgebung oder mit geskripteten Downloads von Herstellern) und diese vollautomatisch zu Dependency-Track hochladen, können Sie stolz erzählen, dass Ihre Organisation „Continuous Security Monitoring“ (CSM) umsetzt. Damit SBOM-Dateien automatisch bei Dependency-Track ankommen, nutzen Sie dessen HTTP-API. Die Plattform bietet dafür für jede Gruppe von Benutzern API-Schlüssel an, die man bei API-Aufrufen übermitteln muss. Diese Schlüssel erzeugen Sie in der Weboberfläche über „Administration/Access Management/Teams“. Der Upload frischer SBOMs ist dann nur noch ein einfacher HTTP-PUT-Befehl, die Dokumentation erklärt diesen Schritt ausführlich (siehe ct.de/wtw3) und zeigt auch, wie man ihn aus einer CI/CD-Umgebung absetzt.

Dokumentationen und Werkzeuge

ct.de/wtw3

Fazit

Eine Software Bill of Material (SBOM) und CycloneDX trennen die Beschreibung der Anwendung und ihrer Abhängigkeiten von einer konkreten Programmiersprache. Der Standard unterstützt alle gängigen Programmiersprachen, Docker-Container und weitere Artefakte wie Helm-Charts und sogar externe Dienste. Also vieles von dem, was Sicherheitslücken haben kann. Ohne eine Software wie Dependency-Track hat man an den JSON- oder XML-Dateien aber keine Freude. Sie bereitet die SBOMs visuell auf, prüft täglich die Sicherheitslage und pustet im Falle einer Sicherheitslücke Benachrichtigungen über diverse Kanäle raus.

Um SBOMs erfolgreich in einer Organisation einzuführen, sind aber auch nicht-technische Probleme zu lösen: Richtig sinnvoll ist das Unterfangen erst, wenn wirklich alle Anwendungen ohne Ausnahme erfasst werden. Davon muss man sowohl alle Entwickler eigener Anwendungen als auch Lieferanten weiterer Software überzeugen. Das ist aktuell harte Arbeit und ein langfristiges Projekt, das sich aber lohnen kann: Bei der nächsten großen Sicherheitslücke kennen Sie die Auswirkungen auf Ihre Organisation ohne panische Rundmails und hastig erzeugter Excel-Tabellen. Genug Arbeit wartet aber auch dann noch. Nachdem Dependency-Track Alarm geschlagen hat, muss man die Probleme schließlich noch abstellen. (jam) c't

Es gibt 10 Arten von Menschen.
iX-Leser und die anderen.



Jetzt Mini-Abo testen:
3 Hefte + Tastatur nur **19,35 €**

www.iX.de/testen

www.iX.de/testen
49 (0)541 800 09 120
leserservice@heise.de
iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

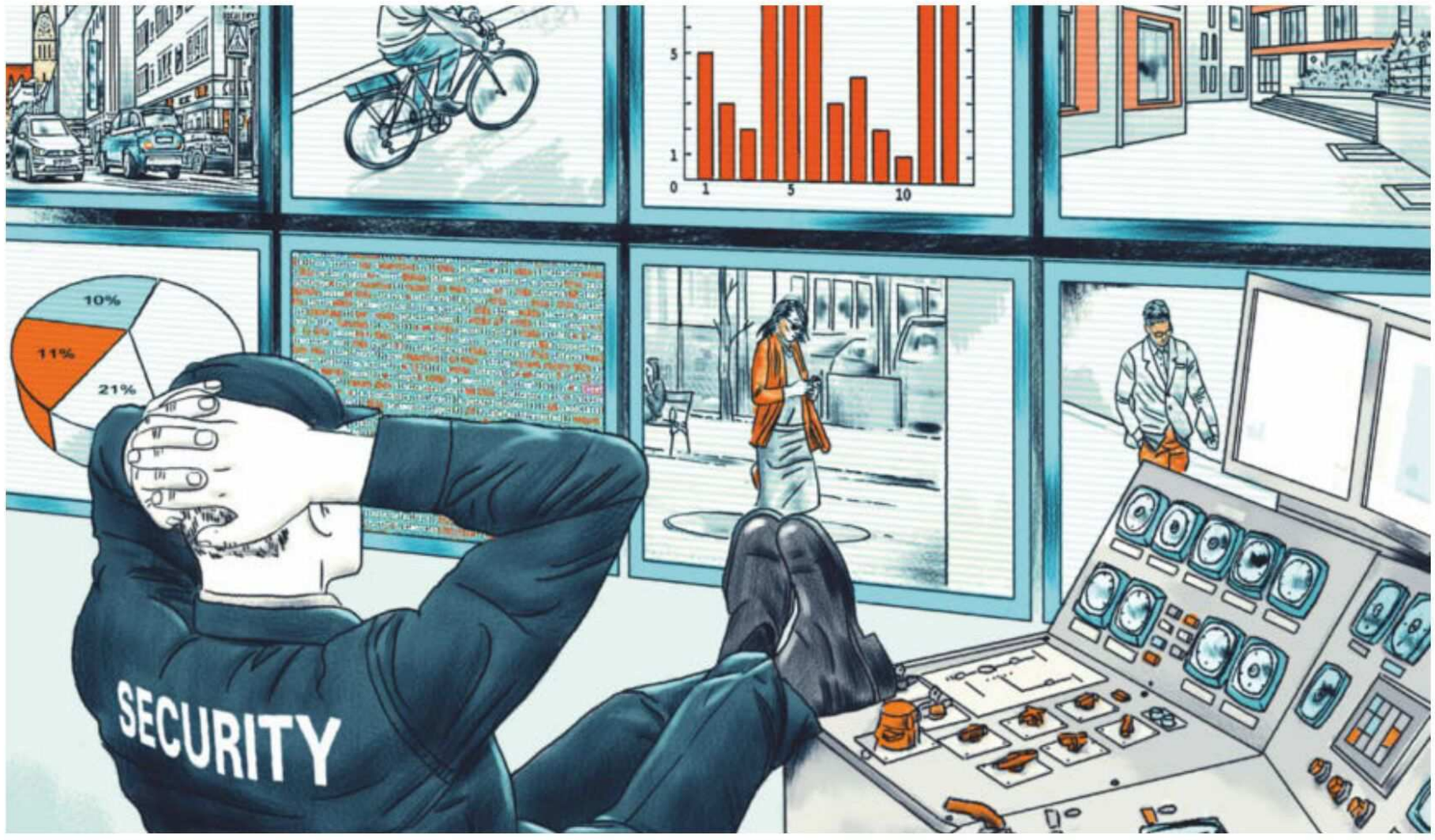


Bild: Thomas Kuhlenbeck

Sicherheitsvorfälle in Logs aufspüren

Logs helfen nicht nur beim Aufspüren von Fehlern, wenn es klemmt. Mit Elasticsearch und Kibana sammeln Sie Logs, bereiten diese auf und reagieren schneller auf sicherheitsrelevante Ereignisse.

Von **Jan Kopia**

Auf fast allen IT-Systemen liegen Log-Dateien, die von Betriebssystemen und Anwendungen produziert werden. Durch Log-Dateien kann ein Entwickler oder Administrator Fehlerzustände, Erfolge und Misserfolge einer Anwendung oder des IT-Systems erkennen und bewerten. Üblicherweise landen Logs als Datei in vorgegebenen Verzeichnissen, die dann versiertes IT-Personal manuell öffnen und einsehen kann. Leider wachsen Log-Dateien schnell auf viele Tausend Zeilen pro Tag an, sodass kaum jemand sie manuell sichtet. Weil es mühsam ist, schaut man meist erst bei Problemen in die Logs und kehrt mithilfe der Erkenntnisse zumindest die Scherben auf.

Was bei einer vollgelaufenen Festplatte ärgerlich, aber gerade noch vertretbar ist, wird problematisch, wenn es um Angriffe und Sicherheitsprobleme geht. Da gilt es, möglichst früh von Unregelmäßigkeiten zu erfahren, um den Angreifern einen Schritt voraus zu sein.

Security Information and Event Management (SIEM) heißt das Gebiet der Informationssicherheit, in dem alle zur Verfügung stehenden Informationen (also unter anderem Logs) systematisch gesammelt und Sicherheitsereignisse möglichst automatisch erkannt werden. SIEM-Werkzeuge sind in der Lage, große Mengen an Log-Quellen zu durchsuchen, zu analysieren, Bedrohungen zu erkennen und zu melden. Log-Auswertung ist der erste Schritt und die Grundvoraussetzung für das, was man als SIEM bezeichnet. Dieser Artikel beschreibt zunächst, was Sie mit SIEM für die Sicherheit in Ihrem Netz tun können und zeigt dann praktisch, wie Sie Ihre eigenen Logs systematisch auswerten.

Dass Log-Überwachung und SIEM keine Spielereien der IT-Abteilung sind, sehen immer mehr Organisationen ein – nicht zuletzt wegen immer häufigerer Angriffe. In einigen Bereichen kommt man gar nicht umhin, sich damit auseinanderzusetzen, weil die Compliance-Anforderungen eindeutig sind und die Einhaltung von ISO/IEC 27001 oder des BSI-IT-Grundschutzes fordern. Beide Dokumente verlangen, dass IT-Systeme zu überwachen und bezüglich Informationssicherheitsanforderungen zu analysieren sind.

Die gute Nachricht für alle, die ihre Logs systematisch auswerten wollen: Es gibt bereits gute Werkzeuge zum Auswerten auf dem Markt, viele sind Open-Source-Software. Eine beliebte Software-Kombination für diese Aufgabe heißt abgekürzt ELK, bestehend aus den Bausteinen Elasticsearch, Logstash und Kibana. Der Kern der Software ist quelloffen, wenn auch nicht mehr nach einer Lizenz, die von den Vertretern freier Software als Open-Source-Software eingestuft wird.

Das Folgende zeigt, wie Sie die drei Komponenten des ELK-Stack auf eigener Hardware in Docker-Containern betreiben und Logs aus Ihrer gesamten Infrastruktur einsammeln und auswerten. Das macht beim Einrichten etwas mehr Arbeit als ein gemietetes Angebot, dafür behalten Sie die volle Kontrolle über Ihre Daten, die durchaus sensibel sein können.

Bevor es ans Einrichten geht, müssen Sie anhand der Wichtigkeit Ihrer IT-Systeme entscheiden, welche Sie in die Log-Überwachung einbinden wollen. Zu viele Logs führen sonst schnell zu Chaos und überfordern die Auswerter. Unternehmen starten idealerweise mit den Kernanwendungen und den damit verbundenen IT-Systemen mit der Fragestellung: Welche Ereignisse wollen wir frühzeitig erkennen? Daran gekoppelt ist die Frage, zu welchen Ergebnissen die Log-Überwachung führen soll. Geht es lediglich um das Erkennen ungewöhnlicher Serverlasten oder sollen auch Angriffe oder andere Anomalien erkannt werden? Die Antworten auf diese Fragen sind nicht nur wichtig für die Art und Anzahl der Log-Quellen, sondern besonders für die Suchanfragen- und Alarm-Konfiguration.

Elasticsearch-Stack in Containern

Anstatt sich zu viele theoretische Gedanken zu machen, sollten Sie sich einen PC oder Server suchen, den ELK-Stack in Betrieb nehmen und mit eigenen Daten von einem zu überwachenden Gerät versorgen. Um das Vorgehen aus diesem Artikel nachvollziehen zu können, brauchen Sie einen Rechner mit Windows, macOS oder Linux und installiertem Docker mit der Compose-Erweiterung – eine von uns

Elastic und die Lizenzen

Das Unternehmen Elastic untersagt in seinen Lizenzbedingungen, die Software als Clouddienst zu vermieten. Ähnlich gehen mittlerweile mehrere Entwickler insbesondere von Datenbanken vor, um sich davor zu schützen, dass die großen Cloudprovider mit dem Vermieten der Anwendung Geld verdienen, ohne sich aktiv am Open-Source-Projekt zu beteiligen. Elastic selbst bietet stattdessen selbst komplett verwaltete Instanzen an. Der Nutzer wählt dabei nur den Cloudprovider seiner Wahl (zur Auswahl stehen Google Cloud, Microsoft Azure oder Amazon AWS) und Elastic richtet das Werkzeug automatisch ein. Anschließend muss man nur noch die notwendigen Log-Quellen anbinden und kann loslegen. Mit der Administration der ELK-Umgebung hat man dann keine Arbeit.

Ziele abstecken

Ob Log-Überwachung oder SIEM, vorab müssen Sie Ziele festlegen und sogenannte Anwendungsfälle definieren, die beschreiben, welche Ereignisse wie erkannt werden sollen und wie darauf reagiert wird. Anwendungsfälle werden vorab technisch und organisatorisch besprochen und niedergeschrieben, sodass sie mit einem hohen Automatisierungsgrad zügig ablaufen können. Ein Beispiel für eine solche Kette aus Ereignis und Reaktion: Ein fehlgeschlagener Administrator-Login-Versuch auf einem kritischen System löst automatisch eine Alarm-Nachricht für den IT-Support aus. Der Supportmitarbeiter hat dann eine vorgeschriebene Liste an Reaktionen abzuarbeiten, wodurch die Zeitspanne einer möglichen Bedrohung sehr klein ist. Um solche Anwendungsfälle zu definieren, müssen mindestens folgende Fragen geklärt werden:

Anwendungsfall für SIEM

Frage	Beispiele
Was sind besondere Risiken und welche Ereignisse sollen erkannt werden?	Einbruch in das IT-System durch Login auf eine bestimmte IP-Adresse
Für welche IT-Systeme/ Anwendungen soll dies erkannt werden?	Active Directory und Domänencontroller
Was sind die relevanten Log-Quellen zur Erkennung?	Log-Dateien in /var/logs oder Windows Security Log
Sind Schwellwerte oder Bedingungen zu beachten?	Logins vor 8 Uhr und nach 19 Uhr
Welche weiteren Informationen sind nötig?	Quell-IP-Adresse des Logins, die Nutzung von su oder root als Stichwort, eine Event-ID
Wie soll darauf reagiert werden?	per Alarm an den IT-Support und Dashboard-Anzeige
Welche Konsequenzen werden ergriffen?	tiefergehende Untersuchung durch IT-Administration oder Konto-Sperrung

regelmäßig aktualisierte Schritt-für-Schritt-Anleitung zur Docker-Installation auf allen Plattformen finden Sie über ct.de/waje.

Dieser Rechner mit Docker arbeitet als Auswertungsserver. Zum Ausprobieren können Sie auch Ihren Desktop-PC einsetzen (mindestens 4 GByte RAM vorausgesetzt), die Zusammenstellung können Sie später leicht auf einen Server verschieben. Außerdem brauchen Sie einen PC oder Server im selben Netzwerk, dessen Logs ausgewertet werden sollen. Haben Sie nur eine Maschine zur Hand, kann es auch die sein, auf dem die Container laufen. Als Beispiel im Artikel dient ein Windows-Server, der überwacht werden soll.

Den gesamten ELK-Stack, bestehend aus drei Containern, starten Sie am schnellsten mit Docker-Compose. Dazu brauchen Sie eine Datei mit dem Namen docker-compose.yml, die alle wichtigen Parameter für den Start der Container enthält und die Container untereinander bekannt macht. Eingerichtet werden die drei Container selbst, die einzubindenden Volumes (der Speicherort für persistente Daten), die Port-Freigaben auf der Netzwerkkarte des Gastgebers, die Netzwerkbezeichnung sowie Umgebungsangaben. Im Kasten rechts finden Sie die Yaml-Datei – abtippen müssen Sie die nicht, wir stellen sie über ct.de/waje zum Download bereit. Außerdem brauchen Sie vier Konfigurationsdateien, die Sie ebenfalls zum Download finden.

Legen Sie am besten einen neuen Ordner für das Projekt an und darin die Datei docker-compose.yml zusammen mit den Konfigurationsdateien ab. Navigieren Sie auf einer Kommandozeile in den Ordner. Mit dem Befehl `docker compose up -d` fahren die drei Container hoch. Zu den Schnellstartern gehören die in Java programmierten Programme nicht; bis sich Elasticsearch-Datenbank und Kibana-Weboberfläche berappelt haben, vergehen ein paar Minuten.

Ohne grafische Anzeigen ist jede Log-Überwachung schwer zu gebrauchen. Zentrale Komponente im ELK-Stack für den überwachenden Admin ist die Weboberfläche von Kibana, das für die Visualisierung verantwortlich ist. In Kibana bauen Sie Ihre Diagramme, Dashboards und Alarme. Sind die Container hochgefahren, ist die Oberfläche auf Port 5601 erreichbar. Diese finden Sie im Browser unter der Adresse http://localhost:5601. Beim ersten Besuch werden Sie gebeten, sich anzumelden. Haben Sie

Benutzername und Kennwort in der Konfiguration nicht verändert, lauten die Anmeldedaten „elastic“ und „verySecret“. Nach der Anmeldung begrüßt Sie eine Willkommensseite. Ohne Daten gibt es aber noch nicht viel zu sehen.

Ein Weg, über den Daten in der Elasticsearch-Datenbank landen, ist Logstash. Es sammelt Logzeilen, reichert sie an, formatiert sie und schickt sie anschließend an eine Datenablage. Ziel der aufbereiteten Logs kann Elasticsearch sein, die Ausgabeformate reichen aber von CSV bis zu kompatiblen Diensten wie Graphite, Kafka, Loggly oder Nagios. Dass ein System wie Logstash überhaupt nötig ist, liegt an den Ausgaben, die Anwendungen wie Nginx oder Apache ausspucken. Deren Logzeilen muss Logstash erst parsen, damit sie als strukturierte Daten gespeichert und später systematisch durchsucht werden können.

Mit Logstash kann man jede erdenkliche Software auswerten, die irgendwo Logs ablegt. Die Konfiguration einer Log-Verarbeitung mit Logstash besteht aus den drei Komponenten Input-Plug-ins, Output-Plug-ins und Filter. Input-Plug-ins binden Log-Quellen an, die zum Beispiel im Syslog liegen, per HTTP eingeliefert werden oder in einer Datei auf Auswertung warten. Filter-Plug-ins wandeln die eingesammelten Log-Dateien um. Filter verkleinern die Daten, reichern sie mit weiteren Informationen an oder zerpflücken sie mit Mitteln wie regulären Ausdrücken. Logs eines Webservers kann man zum Beispiel mit Geodaten zur IP des Besuchers anreichern. Mit Output-Plug-ins werden die aufbereiteten Daten-

```
version: "3.9"
services:
  elasticsearch:
    image: docker.elastic.co/elasticsearch/↵
↳elasticsearch:7.15.1
    volumes:
     - ./elastic/elasticsearch.yml:/usr/share/↵
↳elasticsearch/config/elasticsearch.yml
     - elastic:/usr/share/elasticsearch/data
    ports:
      - "9200:9200"
      - "9300:9300"
    environment:
      ES_JAVA_OPTS: "-Xmx256m -Xms256m"
      ELASTIC_PASSWORD: verySecret
      discovery.type: single-node
    networks:
      - elastic

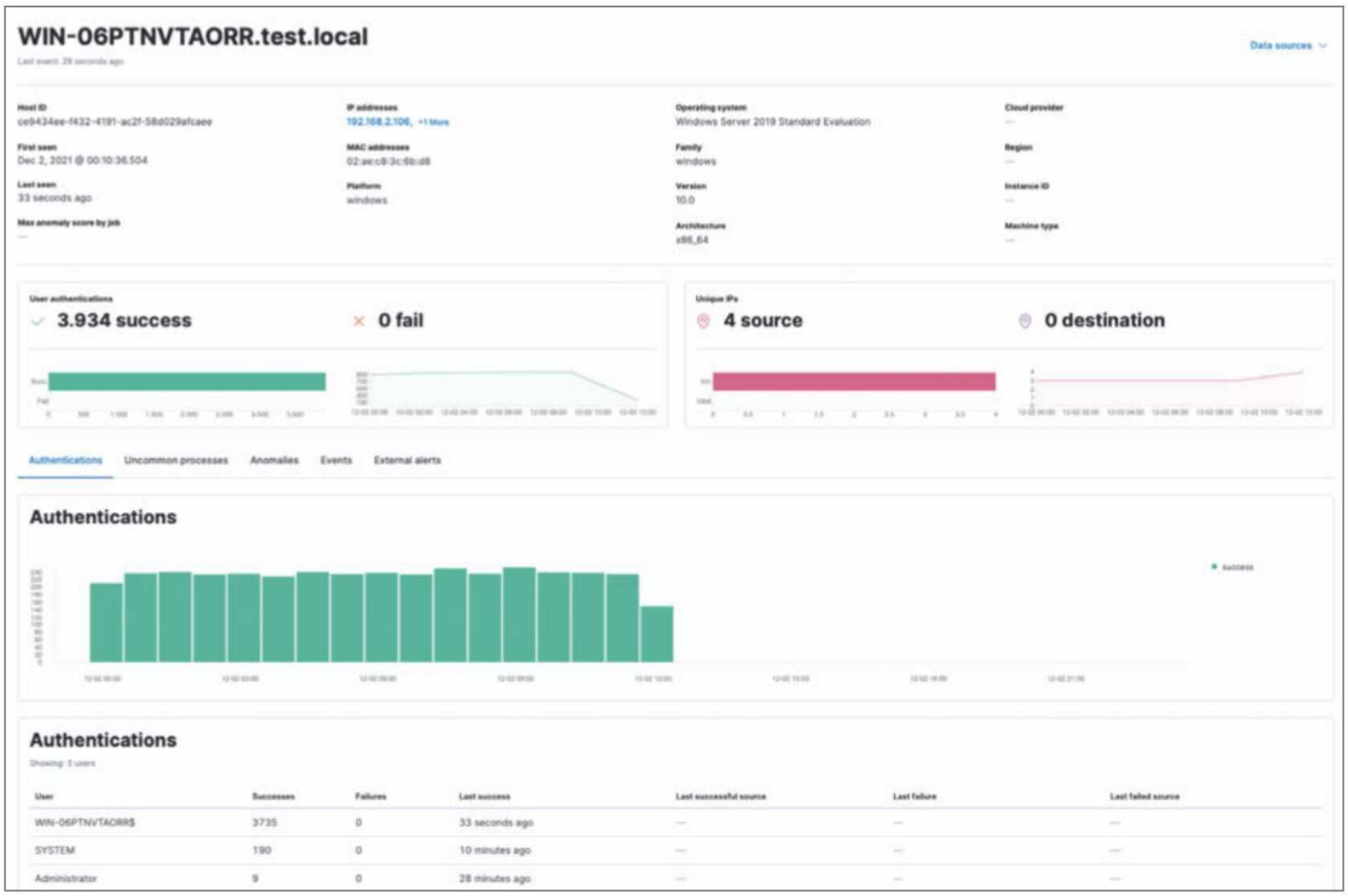
  logstash:
    image: docker.elastic.co/logstash/logstash:7.15.1
    volumes:
      - ./logstash/logstash.yml:/usr/share/↵
↳logstash/config/logstash.yml
      - ./logstash/pipeline:/usr/share/logstash/pipeline
    ports:
      - "5044:5044"
      - "5000:5000/tcp"
      - "5000:5000/udp"
      - "9600:9600"
    environment:
      LS_JAVA_OPTS: "-Xmx256m -Xms256m"
    networks:
      - elastic
    depends_on:
      - elasticsearch

  kibana:
    image: docker.elastic.co/kibana/kibana:7.15.1
    volumes:
      - ./kibana/kibana.yml:/usr/share/kibana/↵
↳config/kibana.yml
    ports:
      - "5601:5601"
    networks:
      - elastic
    depends_on:
      - elasticsearch

networks:
  elastic:
    driver: bridge

volumes:
elastic
```

Der ELK-Stack besteht aus Elasticsearch, Logstash und Kibana. In Containern ist die Zusammenstellung schnell gestartet.



Im Security-Bereich von Kibana findet man die Funktionen, um mit SIEM loszulegen. Neben Übersichten findet man hier auch Dialoge zum Einrichten von Alarmen, damit man schnell auf Ereignisse reagieren kann.

objekte schließlich in verschiedenen Formaten zur Verfügung gestellt, damit eine Zielanwendung wie Elasticsearch sie speichern kann.

Einfacher mit Beats

Logstash ist das Schweizer Taschenmesser zum Verarbeiten von Logs, aber nicht der einsteigerfreundlichste Weg, um an strukturierte Logs und brauchbare Dashboards zu kommen. Für viele der gängigen Betriebssysteme und Serverdienste gibt es einen kürzeren Weg zum Ziel: sogenannte Beats. Das sind Programme, die Elastic entwickelt und die als Dienst auf dem zu überwachenden System laufen, dort Daten sammeln und direkt an Elasticsearch schicken. Bei deren Einrichtung assistiert die Kibana-Oberfläche und legt auch direkt passende Dashboards für die zu erwartenden Daten an.

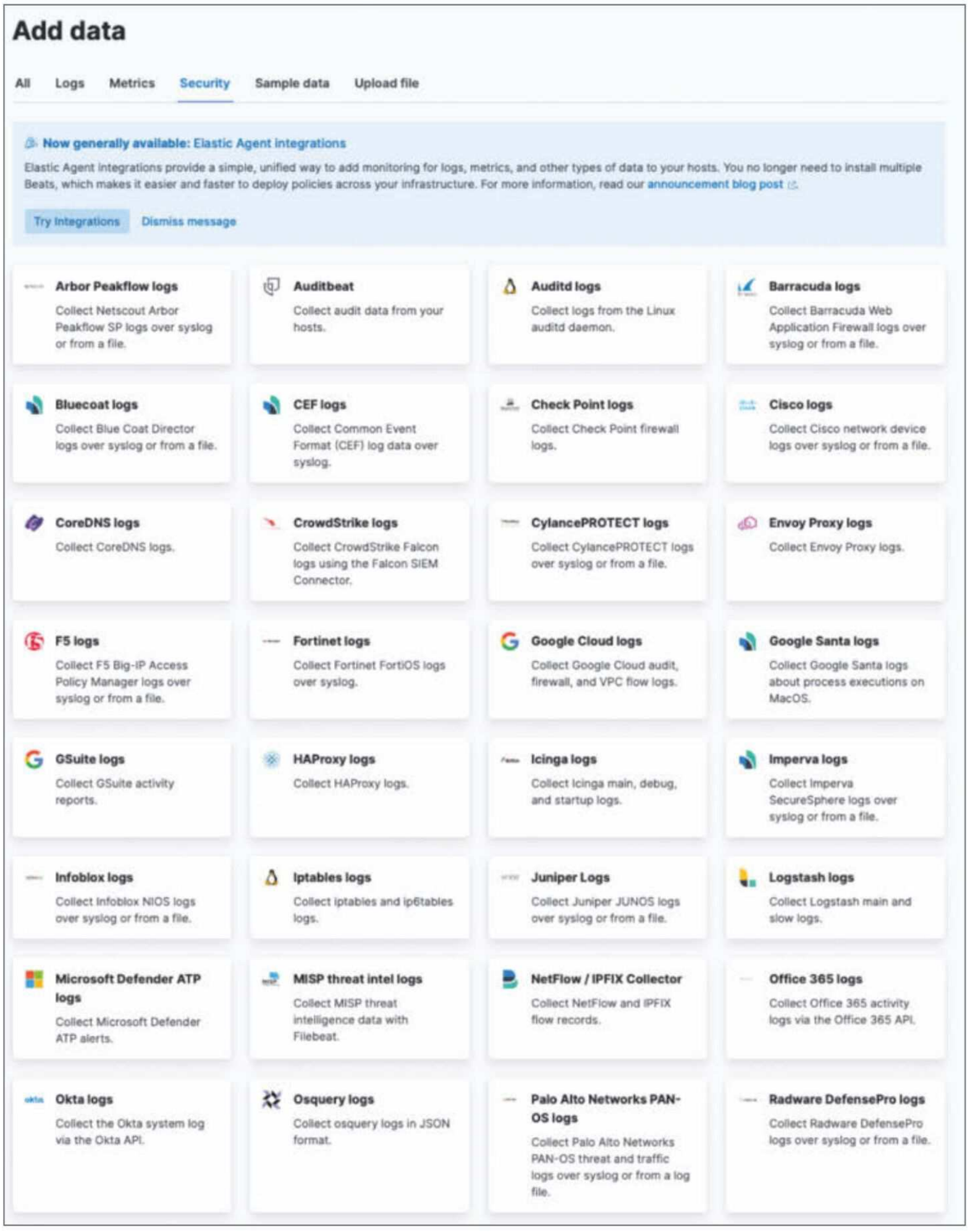
Um einen Windows-PC zu überwachen, klicken Sie auf dem Kibana-Dashboard auf „Add your data“ und suchen in der Übersicht nach „Windows Event Log“. Kibana schickt Sie zunächst zum Download der Anwendung Winlogbeats. Laden Sie die Zip-Datei herunter und entpacken sie auf der Windows-Maschine im Ordner „C:\Program Files“. Benennen Sie anschließend den Ordnernamen mit der Versionsnummer in Winlogbeat um und öffnen eine PowerShell-Sitzung mit administrativen Rechten in diesem Ordner. Mit folgendem Befehl registrieren Sie Winlogbeat als Windows-Dienst (die Ausführung von PowerShell-Skripten auf dem Gerät muss erlaubt sein):

```
.\install-service-winlogbeat.ps1
```

Bevor Sie den Dienst starten, öffnen Sie die Datei winlogbeat.yml und ändern Sie die IP-Adresse auf die Ihrer Maschine mit Docker. Damit die Übertragung funktioniert, müssen die Ports 9200 und 5601 in deren Firewall freigegeben sein. Anpassen müssen Sie folgende Zeilen:

```
output.elasticsearch:
  hosts: ["<IP Ihres Servers>:9200"]
  username: "elastic"
  password: "verySecret"
setup.kibana:
  host: "<IP Ihres Servers>:5601"
```

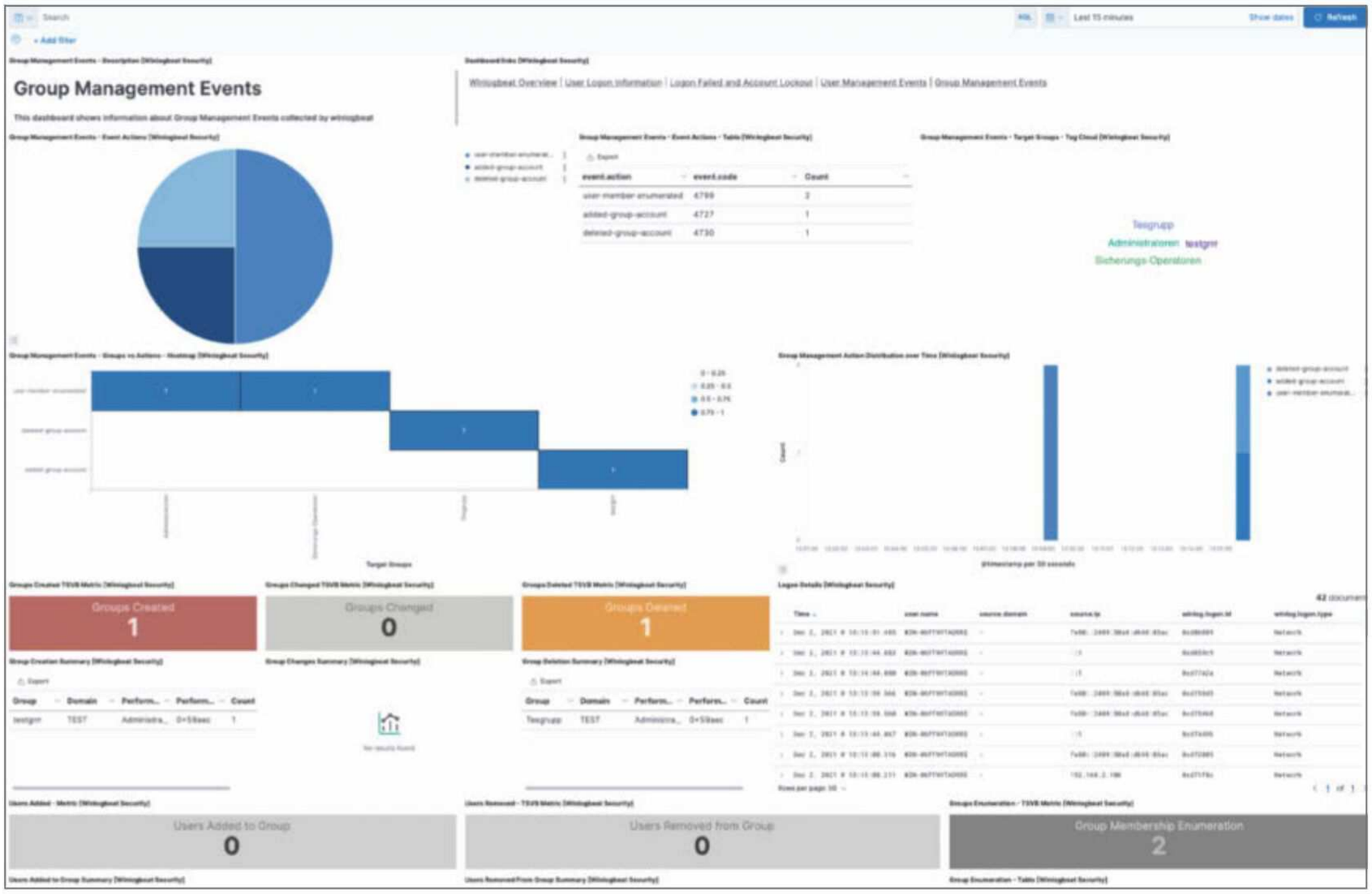
Beats sind die erste Wahl, um Logs und Metriken in Kibana zu bringen. Die kleinen Programme laufen als Dienst auf der zu überwachenden Maschine. Bei der Installation hilft die Kibana-Oberfläche.



Anschließend führen Sie folgende Befehle in der PowerShell-Sitzung aus:

```
.\winlogbeat.exe setup
Start-Service winlogbeat
```

Zurück in Kibana prüfen Sie unten rechts mit „Check Data“, ob Daten angekommen sind. Standen netzwerkseitig keine Hürden im Weg, sollten Sie eine Erfolgsmeldung sehen. Der Button „SIEM App“ führt Sie direkt in Ihren neuen Security-Kontrollraum. Dort gibt es viel zu entdecken: Links im Menü finden Sie den Punkt „Hosts“ und dort direkt Übersichten über erfolgreiche und fehlgeschlagene Login-Versuche auf der Windows-Maschine. Neben dem Security-Bereich, einer recht neuen Kibana-Funktion, sollten



Viel Arbeit ist nicht nötig, um Einblicke ins Geschehen eines Active Directory zu bekommen. Auf dem Domaincontroller läuft der Dienst Winlogbeat und sendet Ereignisse, das Dashboard liefert Kibana fertig eingerichtet mit.

Sie auch einen Blick in die Dashboards werfen, die beim Einrichten von Winlogbeat angelegt wurden: Navigieren Sie oben links auf das Menü und wählen dort unter „Analytics“ den Punkt „Dashboards“. Werfen Sie einen Blick auf die Dashboards, deren Name mit „Winlogbeat“ beginnt. So sollten Sie einen guten Eindruck bekommen, was Sie mit Elasticsearch und Kibana aus Ihren Daten herausholen können – mit den mitgelieferten Dashboards kommt man schon sehr weit. Um zum Kibana-Profi zu werden, müssen Sie sich aber früher oder später mit der Kibana Suchsyntax „Kibana Query Language“ (KQL) auseinandersetzen, damit Sie eigene Abfragen, Dashboards und Alarme entwickeln können.

Beginn der Reise

Nachdem Sie die ersten Daten in Kibana gesehen haben, beginnt die Arbeit erst: Weitere Windows-Maschinen überwachen Sie, indem Sie auch dort Winlogbeat wie oben beschrieben installieren und aktivieren. Einblick ins Geschehen anderer Dienste (etwa Ihrer Nginx- oder Apache-Webserver) bekommen Sie, indem Sie sich nach einem passenden Beat für diese Anwendungen umschauen. Zur Installationsanleitung gelangen Sie über den Schriftzug „elastic“ ganz oben links in Kibana und den Button „Add your data“. Je nach Beschaffenheit Ihres Dienste-Zoos können Sie sich dort passende Beats zum Ausprobieren und Kennenlernen aussuchen. Für Windows gibt es neben Winlogbeat zum Beispiel noch Metricbeat, der Informationen zur Auslastung übermittelt. Mit dem dritten Baustein des ELK-Stacks, Logstash, müssen Sie sich erst auseinandersetzen, wenn für Ihre Anwendung kein Beat zur Verfügung steht.

Dieser Artikel liefert nur einen Einstieg in die Materie – was Kibana noch alles auf Lager hat, entdecken Sie am besten Stück für Stück anhand eigener Daten. Wenn Sie ein Gefühl dafür bekommen haben, was technisch möglich ist, sollten Sie sich strategische Gedanken machen und die Ziele der Überwachung in Form von Anwendungsfällen (siehe Kasten auf Seite 90) bestimmen. Der ELK-Stack ist auch mit der kostenlosen Lizenz geeignet, um eine professionelle Log-Überwachung und SIEM aufzubauen und die Sicherheit im Netzwerk durch schnelle Reaktion zu verbessern. (jam) c't

Docker-Zusammenstellung

ct.de/waje

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.heise.de

Leserbriefe und Fragen zum Heft:
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Jobst-H. Kehrhahn (keh)
(verantwortlich für den Textteil)

Konzeption: Dušan Živadinović (dz), Jan Mahn (jam)

Koordination: Pia Ehrhardt (piae), Angela Meyer (anm)

Redaktion: Ernst Ahlers (ea), Jan Mahn (jam), Urs Mansmann (uma), Angela Meyer (anm), Andrijan Möcker (amo), Sylvester Tremmel (syt), Dušan Živadinović (dz)

Mitarbeiter dieser Ausgabe: Jan Kopia, Manuel Ottlik, Markus Stubbig

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Cathrin Kapell, Martina Lübke, Steffi Martens, Marei Stade, Matthias Timm, Ninett Wagner

Digitale Produktion: Christine Kreye (Ltg.), Melanie Becker, Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Fotografie: Andreas Wodrich, Melissa Ramson

Illustration: Thorsten Hübner, Berlin; Albert Hulm, Berlin; Thomas Kuhlenbeck, Münster; Andreas Martini, Wettin; Moritz Reichartz, Viersen; Michael Vogt, Berlin

Titel: Steffi Martens, www.freepik.com

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: Andre Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 22.11.2022

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlages in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2022 by
Heise Medien GmbH & Co. KG

Das Active Directory im Windows-Netzwerk

Wer mehr als nur ein paar Computer pflegen muss, wünscht sich eine zentrale Verwaltung, anstatt von Rechner zu Rechner zu eilen. In Windows-Netzwerken setzen Administratoren seit zwei Jahrzehnten auf das Active Directory. Microsofts Computer- und Benutzerverwaltung lohnt sich nicht nur für große Unternehmen.

Von **Jan Mahn**



Bild: Thorsten Hübner

Das Active Directory	96
Windows mit GPOs steuern	104
Redundante Domaincontroller	110

Ein Arbeitsplatzrechner in einem Büro hilft seinem Nutzer nicht nur bei der täglichen Arbeit, er verursacht nebenbei auch neue Arbeit – und zwar beim Administrator, der sich um die Verwaltung des PCs kümmern muss: Updates ausführen, Einstellungen anpassen, Programme installieren und aktuell halten. Sobald man vor der Aufgabe steht, in einer größeren Umgebung – etwa in Unternehmen, Behörden, Schulen oder Universitäten – zahlreiche Arbeitsplätze zu verwalten, wünscht man sich einen Weg, über den man Einstellungen auf vielen Geräten gleichzeitig platzieren kann. Eine zentrale Verwaltung muss her.

Für Windows-Admins gibt es das Active Directory (AD), das tief in die Desktop- und Serverausgaben von Windows integriert ist. Dieser Artikel liefert einen Einstieg in diese Grundlagentechnik, die maßgeblich zum Erfolg von Windows in großen Netzwerken beigetragen hat.

Eine der Kernfunktionen des Active Directory sind Gruppenrichtlinien. Solche erstellen Admins an zentraler Stelle und legen damit Einstellungen fest, die sie sonst zum Beispiel in der Systemsteuerung finden. Die Gruppenrichtlinien wenden sie dann mit wenigen Klicks auf Gruppen von Computern an. Wenn zum Beispiel alle Mitarbeiter das Firmen-Intranet als Startseite im Browser bekommen sollen, ist das schnell eingerichtet. Spätestens nach einem Neustart der Clients sind die Einstellungen angekommen. Mit einer solchen Infrastruktur ist es dem Admin egal, ob er 10 oder 10.000 Computer konfigurieren muss. Vor Ort besuchen muss man einen im Active Directory verwalteten PC bestenfalls nur noch, wenn Kabel lose oder Batterien in der Funktastatur leer sind.

Universalverzeichnis

Kern des AD ist eine Datenbank, die Objekte in einer hierarchischen Struktur verwaltet (anders als etwa eine SQL-Datenbank). Objekte können alles Mögliche sein – zum Beispiel Computer, Benutzer und

Das Active Directory: Microsofts Zugpferd

Seit Windows 8, spätestens aber seit Windows 10, steht Windows für seine Datenschutz-Fehltritte in der Kritik: Telemetrie kann man nur noch in der Enterprise-Edition abklemmen, Cortana wurde angeboten wie Sauerbier, die Suche in der Startleiste und der Store sprechen fleißig mit Microsoft-Servern und ein frisch installiertes Windows Pro ist schon voll mit Spiele-Apps, die im Unternehmensnetz nichts verloren haben. Alles Gründe, die Admins dazu bringen könnten, sich nach Alternativen etwa in der Linux-Welt umzusehen.

Doch von einer massenhaften Abwanderung ist nichts zu sehen. Dass Windows in Organisationen noch immer so populär ist, liegt nicht an Bequemlichkeit oder Microsoft-Hörigkeit, wie es Open-Source-Vertreter gerade Behörden gern vorwerfen. Maßgeblich verantwortlich für die Bedeutung von Windows ist das Active Directory – bis heute ein sehr komfortabler und flexibler Werkzeugkasten für homogene Windows-Netze und solche mit hohem Windows-Anteil.

Viele Teilprobleme kann man durchaus auch mit Linux als Desktop- und Server-Betriebssystem lösen (zum Beispiel mit der Open-Source-AD-Alternative Samba), die Integration von weiteren Diensten (Fileserver, Druckserver, Deployment per WDS, Updates per WSUS, Zertifikatsdienste) und das Zusammenspiel aller Komponenten in einem Windows-Netzwerk mit Active Directory sind aber einfach, funktional und über Jahrzehnte erprobt. Und: Viele dieser Dienste, etwa WSUS, gibt es eben nur als Dienst auf einem Windows-Server.

Dass das Active Directory noch immer die Basis des Erfolgs von Windows ist, hält Microsoft nicht davon ab, sein eigenes Produkt mit Missachtung zu strafen. Seit Windows Server 2012 gab es am Active Directory und seinen Verwaltungswerkzeugen keine nennenswerten Neuerungen. Bei den großen Keynotes von Microsoft-Chef Satya Nadella wird dieser Geschäftszweig einfach totgeschwiegen.

Stattdessen versucht der Konzern immer wieder, Anbindungen an seine Azure-Cloud zu verkaufen: Das lokale Active Directory kann man etwa mit dem Azure Active Directory synchronisieren. Nutzer können sich dann mit ihren AD-Benutzerdaten online bei Microsoft anmelden. Diese Synchronisierung des lokalen ADs mit der Cloud ist Voraussetzung, um Dienste wie Office 365 und Microsoft Teams im Unternehmen einzuführen.

Gruppen. Die Hierarchie kann man sich wie eine Baum- oder Ordnerstruktur vorstellen. Das Wurzel-Objekt, das alle weiteren Objekte enthält, heißt Domäne. Die trägt einen Namen in Form eines DNS-Namens. Das kann, muss aber nicht derselbe Domainname sein, den die Organisation auch im Internet benutzt, zum Beispiel example.org.

Als Benutzer ohne Administrationsauftrag sind Sie vielleicht schon einmal über den Begriff der Domäne gestolpert, weil Ihnen ein Dialog in Windows oder einer anderen Software die Option „stattdessen an einer Domäne anmelden“ vorgeschlagen hat. Gemeint ist dann die Domäne eines Active Directory.

In einer Domäne werden die Objekte in sogenannten Organisationseinheiten (Organisational Units, OU) sortiert. Darin können weitere Organisationseinheiten oder die Objekte selbst liegen – vergleichbar mit Ordnern und Dateien in einem Dateisystem. Jedes Objekt bekommt in der Hierarchie eine eindeutige Adresse, den sogenannten „distinguishedName“. Der beginnt mit dem „commonName“ (`CN=`), bei Personen ist das zum Beispiel der Vor- und Nachname, dann folgt eine Aufzählung der Hierarchie der Organisationseinheiten (`OU=`) und schließlich die Komponenten des Domänenamens (`DC=`). Ein distinguishedName kann zum Beispiel wie folgt aussehen:

```
CN=Kalle Knacker,OU=Admins,↵
↳OU=Benutzer,DC=test,DC=local
```

Der Nutzer im Beispiel heißt Kalle Knacker, ist in der Organisationseinheit Admins. Diese ist ein Kinder-Element der OU mit dem Namen Benutzer. Die wiederum liegt auf oberster Ebene in der Domäne test.local. Wie Sie Ihr Active Directory strukturieren, ist Ihnen weitestgehend selbst überlassen – mit der Ordnerstruktur bilden Sie möglichst die Struktur Ihrer Organisation ab. Sinnvoll kann eine Sortierung nach Standorten, Unternehmensbereichen oder Abteilungen sein.

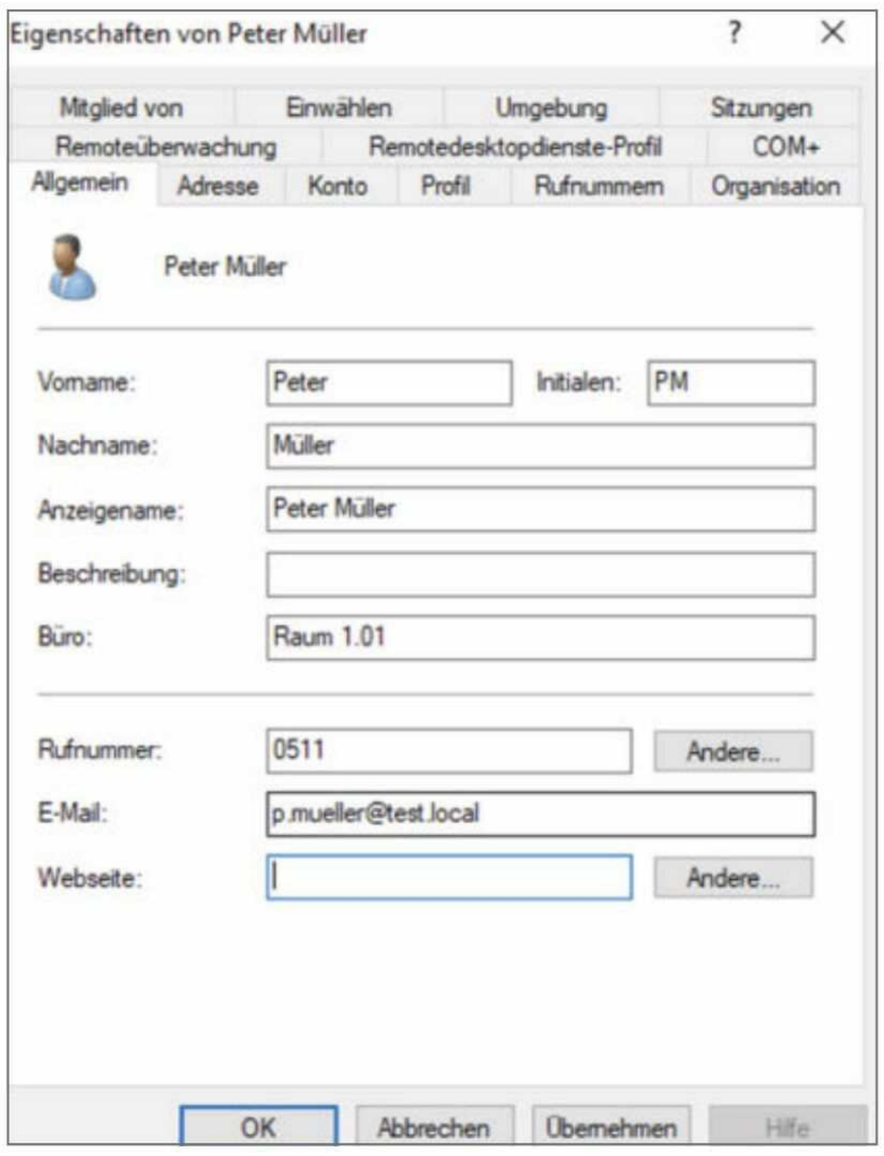
Ähnlich wie in einem Dateisystem dürfen in einer OU nicht zwei Objekte mit demselben Namen liegen – sonst wäre der distinguishedName nicht eindeutig. Wenn also zwei Mitarbeiter mit exakt demselben Namen in einer Organisationseinheit liegen, müssen Sie sich bei der Benennung etwas einfallen lassen.

Theoretisch könnte man beliebige Objekte aus der realen Welt im Active Directory verwalten. Wenn es Ihnen nützlich erscheint, könnten Sie zum Beispiel die Autos des Unternehmensfuhrparks hier ablegen (das ist kein Praxis-Tipp, sondern nur ein theoretisches Beispiel; meist gibt es einfachere Alternativen). Jedes Objekt trägt Attribute, also Felder, in denen man Daten speichern kann.

Objektschablonen

Welche Objekte existieren und welche Attribute diese tragen, legen Schablonen fest, sogenannte Schemata. Microsoft liefert ein Active Directory schon mit vorgefertigten Schemata aus, Sie müssen also nicht bei null anfangen und zuerst die Attribute eines Nutzers definieren. Computer, Gruppen und Benutzer sind bereits angelegt und meist kommen Sie lange ohne Schema-Erweiterungen durchs Admin-Leben. Solche Erweiterungen brauchen Sie erst dann, wenn Sie eine Software nutzen, die eng mit einem Active Directory verzahnt arbeitet. Microsofts Mailserver Exchange ist ein Beispiel für eine Anwendung, die eine Schema-Erweiterung bei der Installation durchführt und das Schema für das Nutzerobjekt mit weiteren Attributen ausstattet.

Auch Schemata sind hierarchisch sortiert und haben einen distinguishedName. Das mitgelieferte Schema für Benutzer heißt mit vollem Namen



Das Active Directory dient nicht nur als zentraler Anmeldedienst, es kann auch ein Organisations-Telefonbuch bereitstellen.

Glaubensfrage Domänenbenennung

Die Frage nach dem „richtigen“ Namen für eine AD-Domäne ist eine wahre Glaubensfrage. Einige plädieren dafür, den Namen der schon existierenden Internetdomain zu nutzen. Das macht es einfacher, zum Beispiel Zertifikate für Dienste zu beschaffen, die von externen Clients akzeptiert werden. Vieles spricht aber gegen diese Strategie – allen voran das Argument, dass die Domäne möglichst einige Jahrzehnte halten sollte, wohingegen sich Unternehmensnamen durchaus ändern können. Dann sind die Mitarbeiter genervt, wenn weiterhin der alte Name verwendet wird. Eine Umbenennung einer Domäne ist kein Vergnügen! Gut fährt man mit einem kurzen Domänennamen, der vergleichsweise unabhängig vom Unternehmensnamen ist, zum Beispiel eine Abkürzung. Am besten sucht man eine Adresse, die im Internet noch nicht vergeben ist und bucht sie direkt. Das Unternehmen Example Inc. könnte statt example.org seine Active-Directory-Domain etwa exi.de nennen und diese zur Sicherheit gleich bei einem Domain-Hoster mieten.

Von der Top-Level-Domain .local, die man früher gern eingesetzt hat, wird für produktive Domänen heute abgeraten. Ersatzweise empfiehlt sich .lokal, das nicht durch die mit Windows 11 eingeführte Namensauflösung mDNS belegt ist.

```
CN=Person,CN=Schema,CN=Configuration,DC=test,
DC=local
```

Solche Benutzer-Objekte tragen neben einem Namen (bestehend aus Vor- und Nachname sowie Initialen) noch weitere Datenfelder, etwa für die Büronummer und Telefonnummern. Wenn Sie diese Werte gewissenhaft im Active Directory pflegen, fallen dabei nützliche Nebenprodukte wie ein firmeninternes Telefonbuch ab. Viele Telefonanlagen und IP-Telefone können das Active Directory befragen und durchsuchen und Sie sparen sich eine doppelte Datenhaltung mit einer weiteren Datenbank. Software, die auf das Verzeichnis des Active Directory zugreifen soll, muss über das „Lightweight Directory Access Protocol“ (LDAP) kommunizieren.

Die eingebauten Standard-Objekte dienen nicht nur als Datenspeicher für ein Firmentelefonbuch und ein PC-Inventar, sie sind auch die Grundlage für eine zentrale Authentifizierung (Anmeldung) und eine zentral steuerbare Autorisierung (Berechtigungsprüfung). Alle Benutzer im Active Directory haben einen Benutzernamen und ein Kennwort. Computer können Mitglied der Domäne werden und bekommen intern ein Computerkonto. Domänen-Nutzer dürfen sich an ihnen mit ihren Zugangsdaten anmelden, sofern sie dafür freigeschaltet sind. Der Vorteil eines zentralen Benutzermanagements liegt auf der Hand: Niemand muss lokale Benutzerkonten auf allen Rechnern anlegen und man kann zum Beispiel zentral festlegen, dass sich alle Mitarbeiter der Buchhaltung mit ihren Anmeldedaten an anderen PCs derselben Abteilung anmelden dürfen (so, dass sie keine fremden Daten sehen können).

Während die Organisationseinheiten für Ordnung sorgen, können Sie Computer und Nutzer in Gruppen zusammenfassen, unter anderem, um Berechtigungen zu vergeben. Weil alles hierarchisch organisiert ist, dürfen Gruppen auch ineinander verschachtelt werden. So kann man jeden Mitarbeiter zum Beispiel in eine Gruppe für seine Abteilung stecken und alle Abteilungsgruppen in die Gruppe Mitarbeiter.

Schaltzentrale Domaincontroller

Eine Windows-Domäne wird von sogenannten Domaincontrollern bereitgestellt. Das sind (virtuelle) Maschinen, auf denen Windows Server (ab Windows Server 2000) installiert ist. Microsoft empfiehlt dringend, auf dieser Server-Instanz nebenbei keine weiteren Dienste zu betreiben – wenn etwas den Domaincontroller blockiert, steht die Arbeit im Netzwerk still. Nur in sehr kleinen Umgebungen kann man von dieser Regel auch mal abweichen.

Mit diesem Grundwissen über den Aufbau von Domäne und Verzeichnis ausgestattet, können Sie

ein Active Directory zum Ausprobieren selbst einrichten. Alles, was Sie dafür brauchen, ist eine Virtualisierungsplattform Ihres Vertrauens (wie Hyper-V oder VMware) und die ISO-Datei mit einem aktuellen Windows Server (2019 oder 2022). Den Link zur Evaluation-Version von Server 2022 finden Sie über ct.de/wngx (siehe auch [1]).

Die dürfen Sie 180 Tage lang für Experimente benutzen – Microsoft hat aber eine Tücke eingebaut: Nachdem Sie einen Server in der Evaluation-Version zum Domaincontroller ernannt haben, können Sie Windows Server nicht mehr durchs Eingeben eines Lizenzschlüssels zu einer Vollversion umwandeln.

Richten Sie eine virtuelle Maschine mit einem aktuellen Windows Server mit grafischer Oberfläche (Standard, nicht Datacenter) ein, geben Sie ihr einen Computernamen wie „dc01“ und am besten eine statische IP-Adresse (man kann einen Domaincontroller technisch durchaus per DHCP betreiben, das ist aber definitiv nicht empfohlen). Wenn Sie später auch das Zusammenspiel der Domäne mit einem Desktop-Windows testen wollen, installieren Sie eine zweite VM mit Windows 10 Professional, Enterprise oder Education und geben auch ihr einen sprechenden Namen wie „PC-Test-01“. Aktivieren müssen Sie weder den Server noch das Desktop-Windows. Stecken Sie beide VMs in ein gemeinsames virtuelles Netzwerk, das auch Kontakt zum Internet hat – wenn die Maschinen sich gegenseitig per Ping erreichen, ist Ihre Testumgebung startklar.

Ein Windows-Server wird zum Domaincontroller, indem man eine Rolle installiert. Mit dem Aktivieren von Rollen bestimmt man, welche Aufgaben ein Windows-Server übernimmt. Öffnen Sie dazu den Server-Manager und klicken oben rechts auf „Verwalten/Rollen und Features hinzufügen“. Klicken Sie sich durch den Assistenten, bis Sie neue Rollen auswählen können. Setzen Sie dort den Haken bei „Active Directory-Domänendienste“ (nicht zu verwechseln mit den „Active Directory Lightweight Directory Services“, das ist nur ein nackter LDAP-Server) und setzen den Assistenten fort. Windows wird Ihnen automatisch ein paar Features vorschlagen, die Sie mit installieren sollen. Lassen Sie diese Vorschläge unverändert. Es handelt sich um die Werkzeuge mit grafischen Oberflächen.

Beginn einer Ära

Ist die Rollen-Installation erledigt, ist der Server bereit, um zum Domaincontroller hochgestuft zu werden. Früher startete man den Vorgang feierlich mit dem Befehl `dcpromo` auf der Kommandozeile. Ein denkwürdiger Moment, der in einer Admin-Karriere nicht allzu oft vorkam – eine Domäne ist eine Einrichtung für die Ewigkeit und kann gut Jahrzehnte überdauern. Mit Server 2012 hat Microsoft `dcpromo` abgeschafft und die Funktion unnötig kompliziert im Server-Manager versteckt. Oben rechts im Server-Manager sollten Sie nach der abgeschlossenen Rolleninstallation ein gelbes Warndreieck sehen, dahinter verbirgt sich der Hinweis, dass die AD-Rolle konfiguriert werden möchte. Klicken Sie dort auf „Server zu einem Domänencontroller heraufstufen“.

Im ersten Schritt des Assistenten werden Sie gefragt, in welche Gesamtstruktur Sie den Domaincontroller integrieren wollen. Eine Domäne ist nämlich nicht die oberste Ebene in einem Active Directory. Ihr übergeordnet ist eine sogenannte Gesamtstruktur. In vielen kleinen und mittleren Unternehmen enthält eine Gesamtstruktur nur genau eine Domäne. Die Gesamtstruktur braucht man erst, wenn die Organisation wirklich groß ist: Internationale Konzerne können sich zum Beispiel dazu entscheiden, für jeden Kontinent eine Domäne anzulegen und alle in einer Gesamtstruktur zusammenzufassen.

Wählen Sie für Ihre erste Domäne „Neue Gesamtstruktur hinzufügen“ und geben ihr einen Namen, zum Beispiel test.local. Im zweiten Schritt fragt der Assistent, welche Funktionsebene Domäne und Gesamtstruktur haben sollen. Das ist ein nichtssagender Begriff, den man besser mit „Active-Directory-Generation“ übersetzt hätte. Mit fast jeder Windows-Server-Version kamen kleinere Neuerungen zum AD hinzu. Wenn Sie die Struktur auf „Windows Server 2016“ einstellen, bekommen Sie die neuesten Funktionen, können später aber keine Domaincontroller mit älteren Server-Versionen hinzufügen (wohl aber ältere Server und Desktops als Domänenmitglieder). Mit Server 2019 und 2022 kamen keine neuen Funktionen hinzu, wählen Sie also 2016.

Außerdem verlangt der Assistent ein Wiederherstellungskennwort (DSRM-Kennwort, Directory Services Restore Mode). Das ist der Zugang für absolute Notfälle kurz vorm Totalschaden. Für eine Produktivumgebung vergeben Sie ein möglichst langes Kennwort und verwahren es an mindestens einem sehr sicheren Ort, am besten auch außer Haus. Lassen Sie die anderen Optionen unverändert, insbesondere der Haken für den DNS-Server muss aktiv sein. Setzen Sie anschließend den Assistenten fort. Den nächsten Schritt, der nach DNS-Delegierung fragt, können Sie überspringen. Auch dem NetBIOS-Namen Ihrer Domäne müssen Sie keine große Auf-

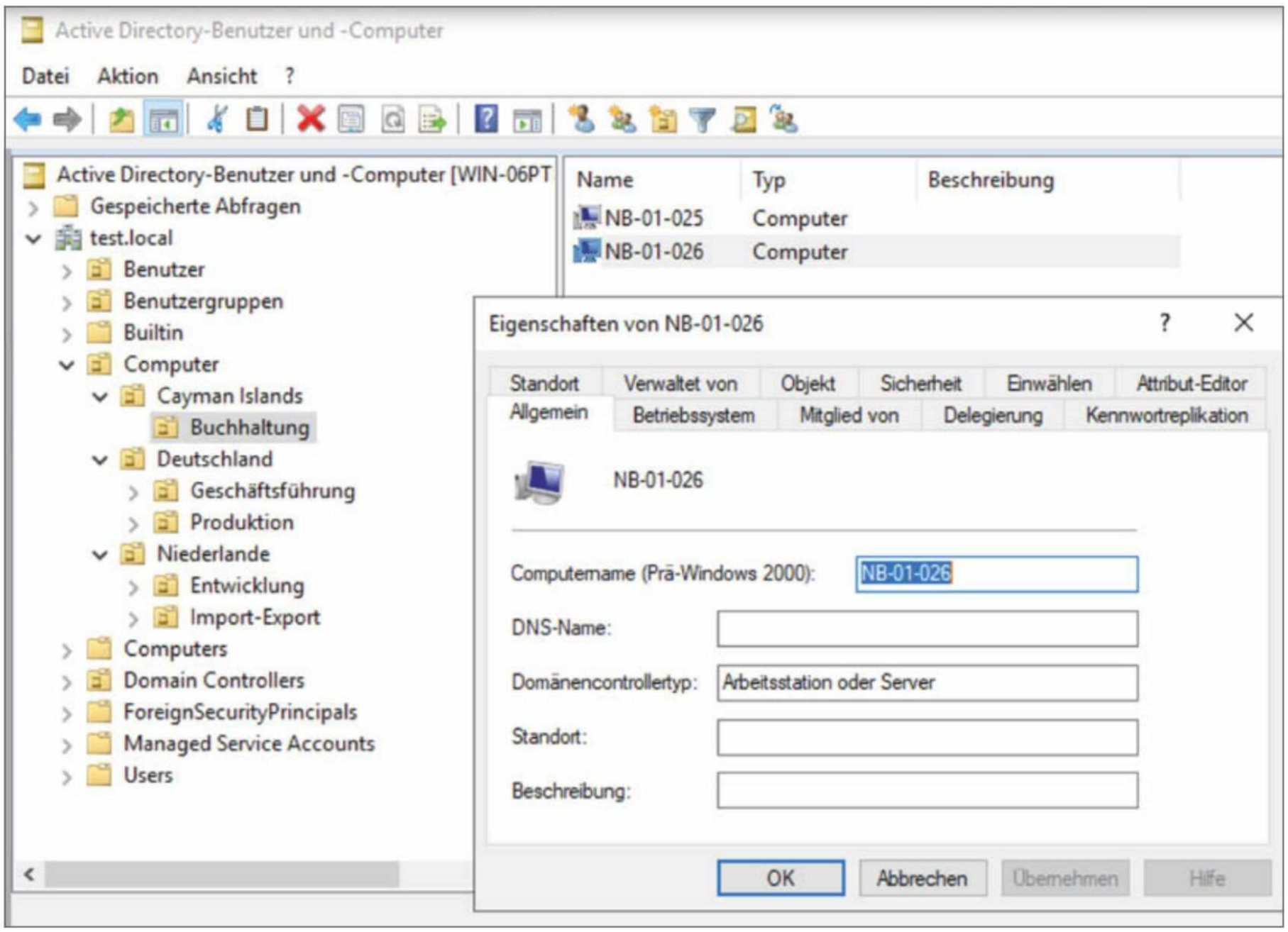
merksamkeit schenken, der Assistent unterbreitet Ihnen einen Vorschlag. Für die Domäne test.local nehmen Sie einfach „TEST“. Das ist ein historisches Relikt, das die Nutzer aber noch vergleichsweise oft zu sehen bekommen, zum Beispiel bei der Anmeldung.

Im nächsten Schritt können Sie drei Pfade anpassen: zunächst den Datenbankordner (NTDS, benannt nach dem AD-Vorgänger NT Directory Services). In diesen legt der Server seine hierarchische Datenbank ab. Außerdem brauchen Sie einen Ordner für die Protokolldateien und einen für die Freigabe SYSVOL. In diesem per SMB im Netzwerk freigegebenen Ordner liegen später die Gruppenrichtlinienobjekte mit Einstellungen, die von den Clients eingelesen und verarbeitet werden. Die Best-Practice-Empfehlung lautet, diese drei Ordner auf einen separaten Datenträger zu legen. Für eine Experimental-Domäne belassen Sie es bei den Vorgaben und klicken den Assistenten bis zum Ende durch. Am Ende wird der Server neu gestartet und ist ab diesem Zeitpunkt Domaincontroller.

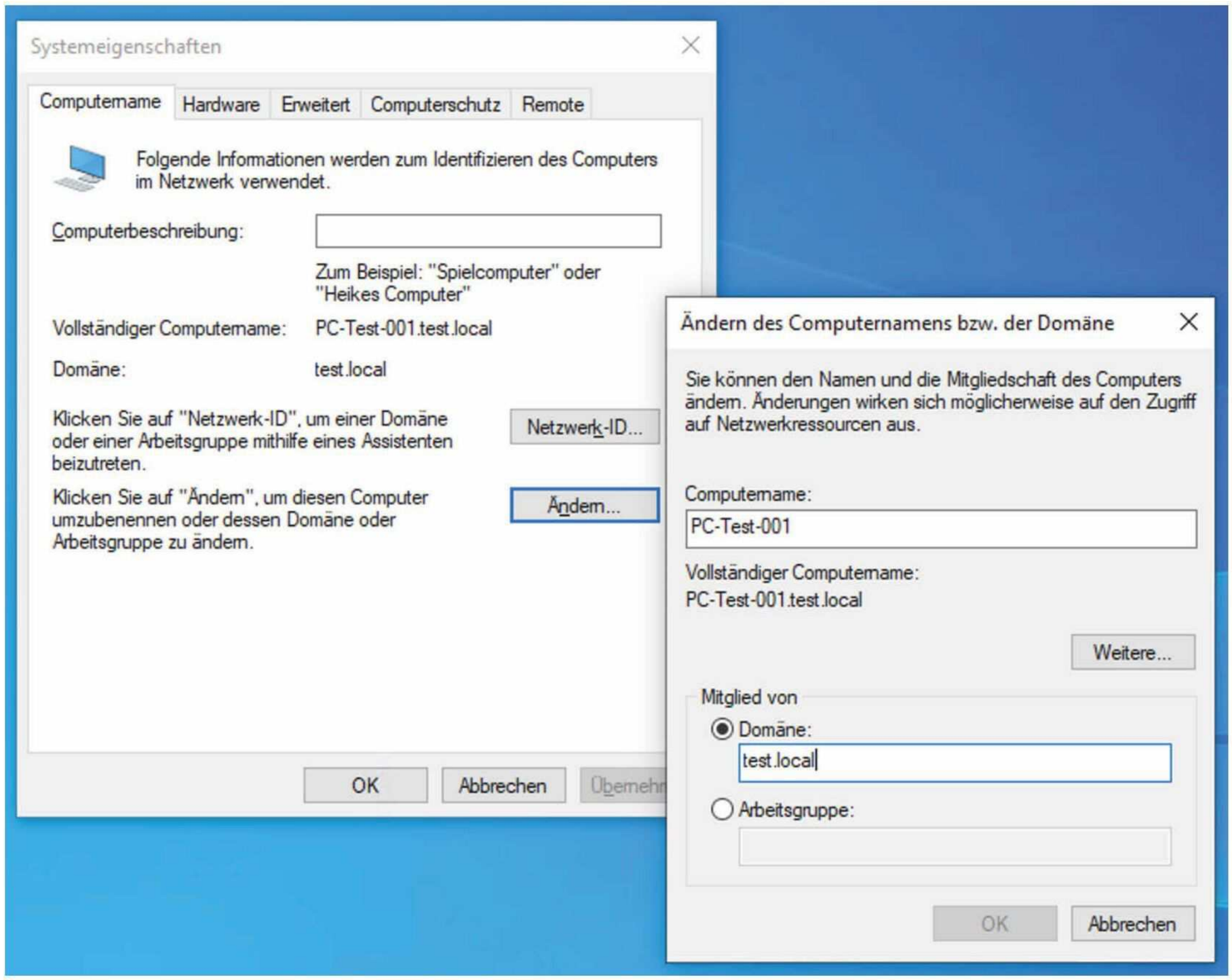
Willkommen zu Hause

Dieser Wandel ist unverkennbar nach dem Neustart: In der Anmeldemaske wird jetzt zusätzlich der NetBIOS-Name Ihrer Domäne angezeigt und Ihr bisheriger lokaler Administrator-Account auf diesem Server hat den Aufstieg zum Domänen-Account mit dem Namen Administrator hinter sich. Melden Sie sich mit seinem gewohnten Kennwort an. Nach der etwas zähen Erstanmeldung können Sie Ihre neue Domäne in Augenschein nehmen. Die grafische Oberfläche zur Verwaltung finden Sie, wenn Sie „Active Directory-Benutzer und -Computer“ in die Suche eintippen – dieses Werkzeug sollten Sie direkt auf den Desktop legen.

Es zeigt Ihnen links die noch sehr leere Baumstruktur an – diese mit Leben zu füllen, bleibt Ihnen überlassen. Am besten lassen Sie die vordefinierten Benutzerobjekte in ihrer Organisationseinheit Users und legen eine neue OU mit dem Namen „Benutzer“ an. Klicken Sie dafür links auf den Namen Ihrer Domäne und dann oben auf das Symbol, das wie



Die Benutzer- und Computerverwaltung für das Active Directory kommt im Windows-2000-Layout daher, ist aber bis heute funktional und schnell verstanden.



Mit wenigen Klicks wird ein Windows-10-PC (Pro, Enterprise oder Education) zum Domänenmitglied. Danach können sich Domänen-Nutzer an ihm anmelden und Admins ihn fernverwalten.

„Neuer Ordner“ aussieht. Damit erstellen Sie eine neue OU. Hier können Sie schon mal Ihren ersten Nutzer platzieren – öffnen Sie die OU und klicken dann oben auf das Nutzer-Symbol. Der kleine Assistent ist selbsterklärend. Ihr Nutzer bekommt Vor- und Nachname sowie ein Kennwort und einen Benutzernamen.

Unterwerfung

Ausgestattet mit Domäne und Benutzer können Sie jetzt Ihren ersten Client-PC zum Mitglied machen. Jeder Windows-Desktop mit einer Pro-, Education- oder Enterprise-Edition (und jeder Windows Server) kann Mitglied einer Domäne werden. Damit das reibungslos klappt, ist noch eine Änderung am Netzwerk fällig: Ihr Domaincontroller arbeitet seit der Installation auch als DNS-Server und löst Anfragen für die Domain test.local auf. Die AD-DNS-Integration ist einerseits technisch nötig, damit der Domaincontroller gefunden wird, andererseits enorm praktisch, weil jeder PC sofort einen internen Subdomain-Eintrag bekommt. Der Computer mit dem Hostname PC-Test-01 bekäme den Eintrag pc-test-01.test.local. In sehr großen Organisationen kann man Domaincontroller und DNS auch trennen, in kleinen und mittleren Umgebungen ist das aber nicht nötig.

Damit Sie einen Rechner in die Domäne aufnehmen können, muss der als DNS-Server den Domaincontroller verwenden. Vorher sollten Sie aber sicherstellen, dass Ihr DNS-Server alle Anfragen, die nicht zu test.local gehören, an einen anderen DNS-Server im Internet weiterleitet. Geben Sie auf dem DC in die Suchleiste „DNS“ ein und öffnen Sie den DNS-Manager. Klicken Sie links auf den Namen des Servers, dann auf Weiterleitungen. Wenn hier noch nichts steht, tragen Sie einen öffentlichen DNS-Server Ihres Providers, 1.1.1.1 (von Cloudflare) oder

8.8.8.8 (von Google) ein. Wechseln Sie dann zur Windows-10-Maschine und tragen in den Netzwerkeinstellungen die IP-Adresse Ihres Domaincontrollers als DNS-Server ein. Zum Test können Sie dort anschließend die Auflösung mit `nslookup test.local` prüfen.

Öffnen Sie jetzt den Dialog zum Ändern des Computernamens. Den hat Microsoft mit Windows 10 in der Einstellungen-App unter System/Info ganz unten hinter dem Link „Diesen PC umbenennen (fortgeschritten)“ versteckt (nicht verwechseln mit „Diesen PC umbenennen“). Zügig kommen Sie zum Dialog über den Befehl `sysdm.cpl` auf der Kommandozeile. Klicken Sie im Dialog unten auf „Ändern“.

Tragen Sie dort den Namen Ihrer Domäne ein. Zum Ändern der Domänenmitgliedschaft müssen Sie lokaler Administrator auf dem PC sein und werden dann aufgefordert, die Zugangsdaten eines Administrators der Domäne einzugeben. In einem produktiven System sollten Sie unbedingt weitere Admin-Accounts mit beschränkteren Rechten einrichten; für eine Testumgebung ist es vertretbar, den Account „Administrator“ zu nutzen.

Mit diesem Akt unterwirft sich der PC vollständig den Spielregeln der Domäne. Per Richtlinie kann ein Domänen-Admin jetzt zum Beispiel dafür sorgen, dass der bisherige lokale Administrator seine Rechte oder sein Kennwort verliert. Eine Domänenmitgliedschaft ist daher nicht das geeignete Verfahren, um Bring Your Own Device (BYOD) in Unternehmensnetzen umzusetzen: Privatgeräte gehören nicht in die Domäne.

Wenn die Aufnahme in Ihre Domäne geklappt hat, verabschiedet sich der Client zum Neustart. Anschließend dürfen Sie sich mit den Nutzerdaten eines Domänen-Nutzers anmelden. Klicken Sie im Anmeldebildschirm unten links auf „Anderer Benutzer“ und melden sich mit dem Benutzernamen an. Dass es sich um eine Domänen-Anmeldung handelt, ist schon voreingestellt. Um sich mit einem lokalen Konto an einem Domänen-PC anzumelden, setzen Sie ein \ vor den lokalen Benutzernamen.

Der Anfang ist gemacht

Ihre Domäne in einer minimalen Konfiguration ist einsatzbereit. Für den produktiven Einsatz fehlen aber noch einige Einrichtungsschritte. In den beiden folgenden Artikeln erfahren Sie, wie Sie Ihre Windows-10-PCs mit Gruppenrichtlinien verwalten und wie Sie mehrere Domaincontroller redundant im Verbund betreiben. (jam) c't

Literatur

[1] Jan Mahn, **Wohin des Weges?**, Was Windows Server 2022 Neues bringt, c't 13/22, S. 156

Dokumentation und Downloads:

ct.de/wngx





Bild: Thorsten Hübner

Windows mit GPOs steuern

Das Active Directory verwaltet nicht nur Benutzer und Gruppen. Mit Gruppenrichtlinien steuern Administratoren, wie sich Windows-PCs verhalten sollen. An den Geräten selbst muss man dann kaum noch Hand anlegen.

Von **Jan Mahn**

Schon auf einem einzigen privat genutzten Windows-PC gibt es viel einzustellen, wenn man ihn in Betrieb nimmt: Cortana-, Telemetrie- und Energiespareinstellungen, Standardbrowser, Startseite, Desktop-Hintergrund, Standarddrucker und vieles mehr. Die meisten Einstellungen nimmt man am privaten PC im Laufe der Zeit vor, wenn etwas fehlt oder stört. In großen Netzwerken von Firmen, Schulen, Unis und Behörden ist das keine Option: Als Administrator möchte man jenen, die vor den PCs sitzen, das Einrichten nicht nur abnehmen, sondern es ihnen sogar verbieten. Die eigene Katze als Desktop-Hintergrund will man ihnen vielleicht noch gestatten, sie von Energiespareinstellungen, Gerätemanager und anderen Browsern aber tunlichst fernhalten.

Alle Windows-Einstellungen per Hand vorzunehmen und den Rechner danach zu vernageln, ist ver-

geudete Zeit – nur eine zentrale Steuerung verspricht einen vergnüglichen Admin-Alltag. Genau diese Steuerung bekommt man mit Microsofts Active Directory, der zentralen Benutzer-, Geräte-, und Gruppenverwaltung über die sogenannten Gruppenrichtlinien.

Voraussetzung, um die Schritte aus diesem Artikel nachstellen zu können, ist eine Testumgebung aus mindestens einem Windows-Server als Domain-Controller und einem Windows-10-Client als Domänen-Mitglied. Wie Sie eine Domäne einrichten sowie Benutzer und Windows-Clients hinzufügen, haben wir ausführlich ab Seite 96 beschrieben. Auch wenn Sie bereits eine Domäne im produktiven Einsatz haben, kann es nie schaden, eine davon unabhängige Testumgebung zur Hand zu haben.

Gruppenrichtlinien und ihre Objekte

Bevor es mit der Arbeit losgehen kann, ist etwas Begriffsklärung notwendig. Gesteuert werden die Clients über sogenannte **Gruppenrichtlinienobjekte** (Group Policy Objects, GPO). Ein Gruppenrichtlinienobjekt enthält eine Sammlung von Anweisungen an Windows-Clients. Die Anweisungen unterteilen sich in solche für **Computer** und solche für **Benutzer.** Ein einzelnes Gruppenrichtlinienobjekt kann beide Formen enthalten. Diese Unterteilung entspricht derjenigen, die Windows-Kenner aus der Registry kennen [1].

Innerhalb eines GPO können zwei Formen von Arbeitsanweisungen an die Clients verpackt werden: **Richtlinien** und **Einstellungen**. Einstellungen sind vorwiegend solche Änderungen, die man auf einem lokalen Computer über die Systemsteuerung (control.exe) vornehmen würde. Dort kann man Drucker einrichten, Energiesparpläne anlegen sowie Geräte, Benutzer, Netzwerkverbindungen, Freigaben und geplante Aufgaben verwalten. Außerdem kann man über Einstellungen Ordner, Dateien und Registry-Einträge an die Clients verteilen.

Der zweite große Hebel zur Verwaltung sind Richtlinien – die sind immerhin namensgebend für das Konzept der Gruppenrichtlinien. Solche Richtlinien enthalten klare Anweisungen wie „Alle Desktopsymbole ausblenden und deaktivieren“. Richtlinien kann man aktivieren, deaktivieren oder unkonfiguriert lassen – wobei die letzten beiden Optionen nicht automatisch dasselbe bedeuten und man immer das Kleingedruckte lesen muss. Einigen Richtlinien kann man zusätzlich noch Parameter übergeben, etwa einen Dateipfad oder eine von mehreren Optionen aus einem Drop-down-Menü.

Richtlinien sind Gebote und Verbote an Computer und Benutzer. Über sie entfernen Sie zum Beispiel den Ruhezustandsknopf im Startmenü, sperren den Zugriff auf die Systemsteuerung, oder schalten den Start-Sound von Windows ab. Für viele Dinge, die Ihnen unter Windows schon immer ein Dorn im Auge waren, gibt es Richtlinien. Für das Umsetzen auf dem Client ist keine schwarze Magie nötig, auch das geschieht intern mit bekannten Bordmitteln: Die Richtlinien enthalten Anweisungen, welche Einträge an der Windows-Registry vorzunehmen sind. Alle Einstellungen könnten Sie also auch mit regedit.exe per Hand vornehmen.

Dass Sie als Administrator, ohne die Registry-Schlüssel zu kennen, einen Schalter wie „Cortana zulassen“ auf „deaktiviert“ umlegen können, verdanken Sie administrativen Vorlagen (ADMX-Dateien) und zugehörigen Sprachdateien (ADML-Dateien). Im XML-Format ist darin festgelegt, welche Registry-Schlüssel wie befüllt werden sollen, wenn Sie die Richtlinie konfigurieren, und welche Parameter es gibt. Für Einstellungen an Windows und Windows-Komponenten werden diese Vorlagen direkt beim Einrichten der Domäne auf dem Domain-Controller installiert. Grundsätzlich kann aber jeder Softwareanbieter, der Einstellungen in der Registry ablegt, eigene Vorlagen im ADMX-Format bereitstellen. Zum Beispiel gibt es für Google Chrome und mittlerweile auch für Mozilla Firefox solche Vorlagen zum Download von den Entwicklern (siehe ct.de/w21j). Mit der Veröffentlichung von Windows 11 hat Microsoft auch passende ADMX-Dateien zum Nachinstallieren bereitgestellt (siehe ct.de/w21j).

SYSVOL

Wenn Sie ein Gruppenrichtlinienobjekt mit Richtlinien und Einstellungen geschnürt haben, landet es als Ordner auf einer Netzwerkfreigabe, die unter dem Namen SYSVOL auf allen Domain-Controllern bereitgestellt wird. Wenn Sie mehrere Domain-Controller betreiben, werden die Inhalte automatisch repliziert. Hat man den Pfad bei der Einrichtung der Domäne nicht verändert, liegt der Ordner auf dem Domaincontroller unter C:\Windows\SYSVOL\sysvol\<Name der Domäne>.

Gruppenrichtlinienobjekte gelten nicht für alle Computer und alle Benutzer – dann wären sie reichlich unpraktisch. Ein GPO muss, damit es angewendet wird, mit einem Standort, einer Domäne oder

einer Organisationseinheit (OU) verknüpft werden. Dann wirkt es auf alle Objekte, die in der Hierarchie unterhalb liegen, es wird also vererbt. Ein GPO, das auf der Ebene der Domäne verknüpft ist, wirkt sich auf alle Computer und Nutzer in allen Organisationseinheiten aus.

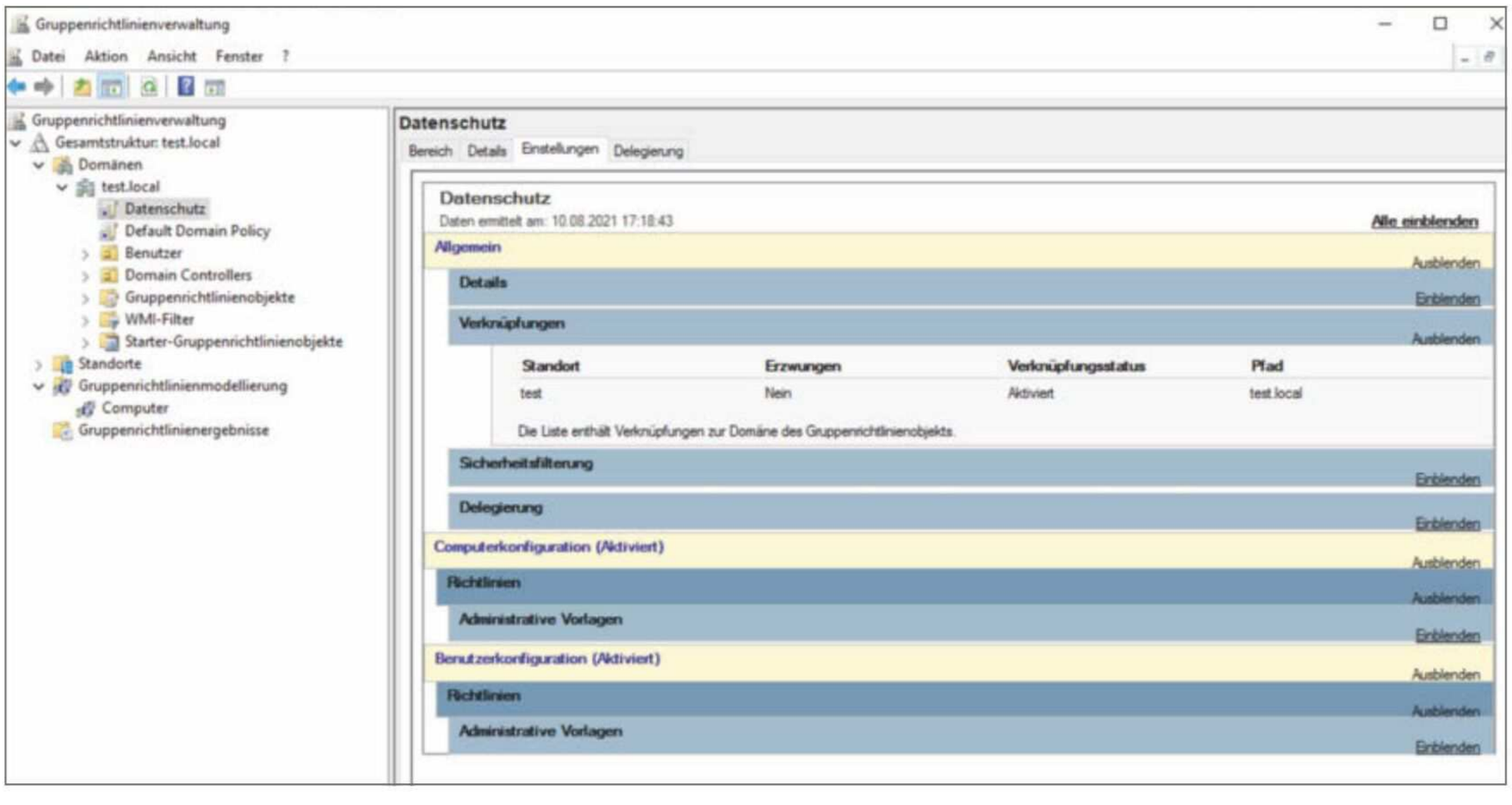
Dieselbe Richtlinie können Sie auch auf verschiedenen Ebenen mehrfach konfigurieren: Einmal für die Domäne und einmal für eine untergeordnete OU. Dann gilt die Grundregel, dass eine spezielle Richtlinie die allgemeine überschreibt. Ein GPO für eine OU überschreibt also eins für die gesamte Domäne (Standorte und mehrere Domänen spart dieser Artikel aus). Zunutze machen kann man sich diese Verarbeitungsreihenfolge immer dann, wenn einzelne Bereiche von einem globalen Standard abweichen sollen: Wenn alle Nutzer grundsätzlich das Firmenlogo als Hintergrundbild bekommen sollen, nur die Mitarbeiter im Foyer ein anderes, würden Sie dieselbe Richtlinie einmal auf Domänen- und einmal auf OU-Ebene für die OU „Foyer“ aktivieren. Eine Warnung für den Einstieg: Halten Sie die Struktur von Beginn an so einfach wie möglich. Gerade am Anfang denkt man oft zu kompliziert und arbeitet mit zu vielen Regeln auf zu vielen Ebenen, weil man es zu gut meint. Ein Großteil Ihrer Regeln wird für fast alle Ihrer Computer und Nutzer gelten.

Zu guter Letzt gibt es noch eine weitere Stufe der Komplexität: Nicht immer wollen Sie, dass alle Computer oder Nutzer innerhalb einer Organisationseinheit von einer Richtlinie betroffen sind. Dann kommen, zusätzlich zur Verknüpfung an eine OU oder Domäne, Filter zum Einsatz. Der gebräuchlichste Filter ist der sogenannte **Sicherheitsfilter**. Der Begriff weist etwas in die falsche Richtung – gemeint ist ein Filter auf Sicherheitsgruppen, also Gruppen von Personen oder Computern im Active Directory. Wenn Sie eine Teilmenge einer OU in eine solche Gruppe stecken, können Sie ein GPO darauf einschränken. Auch hier gilt: Setzen Sie Filter sparsam ein, um den Überblick nicht zu verlieren.

Der zweite Filtertyp kommt seltener zum Einsatz. Über den **WMI-Filter** (Windows Management Instrumentation) können Sie vor dem Anwenden einer Richtlinie Eigenschaften einer Windows-Installation abfragen und darauf filtern. Das braucht man zum Beispiel, wenn ein GPO nur für ein bestimmtes Betriebssystem oder eine Prozessorarchitektur gelten soll.

Erstkontakt

Dieses theoretische Wissen ist nötig, um sich in der grafischen Oberfläche für die GPO-Verwaltung nicht



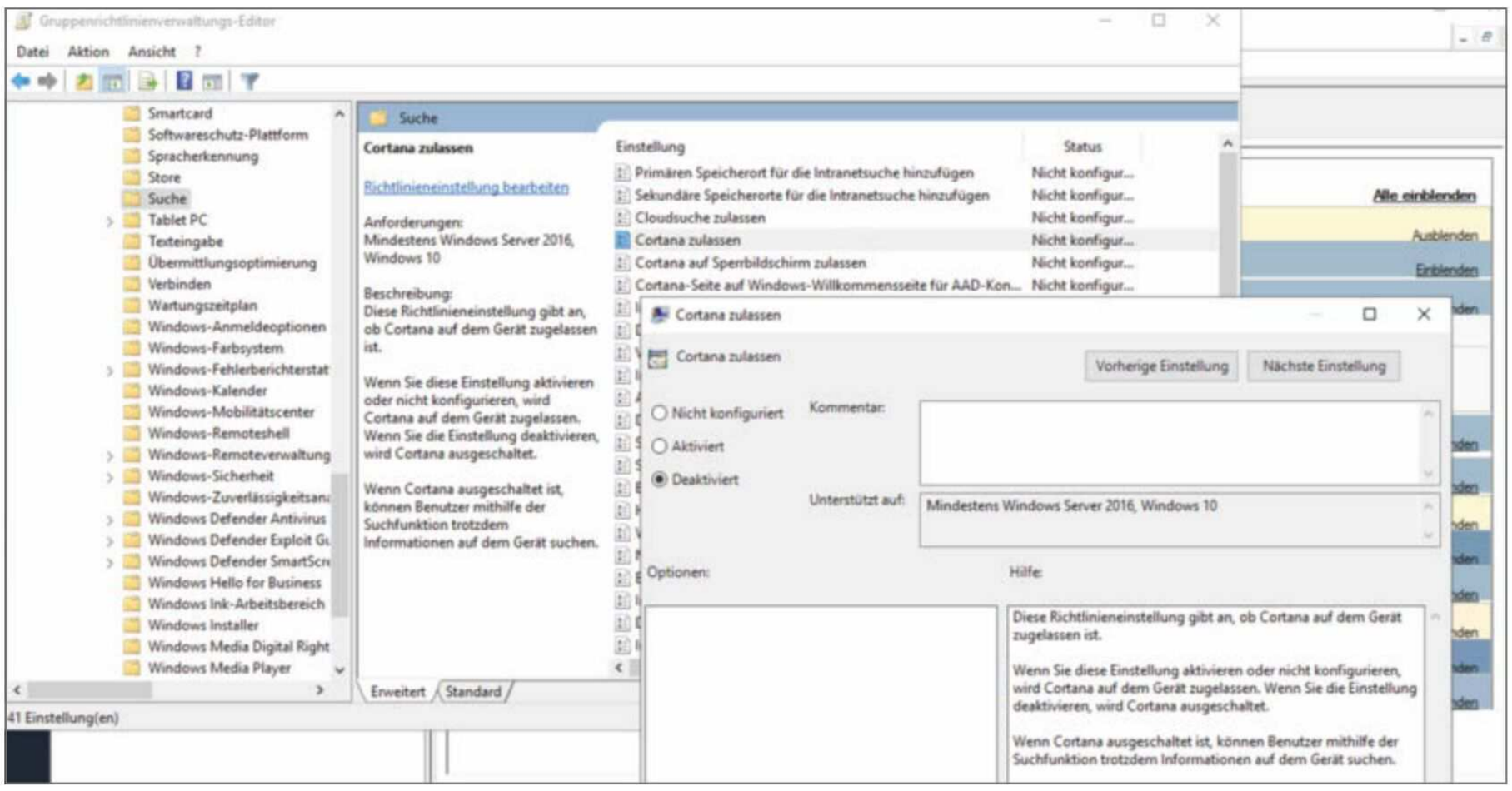
Nicht gerade intuitiv. In der blau-gelben Ansicht sehen Sie eine Übersicht eines Gruppenrichtlinienobjekts. Per Rechtsklick kommen Sie zum Editor, über den Sie Richtlinien und Einstellungen hinzufügen.

komplett zu verlieren. Auf dem Domänen-Controller finden Sie das grafische Werkzeug mit dem Namen Gruppenrichtlinienverwaltung (`gpmc.msc`). Dessen Oberfläche ist, vorsichtig formuliert, gewöhnungsbedürftig und mehr als überarbeitungswürdig. Selbst wenn man das Prinzip verstanden hat, bleiben die Schritte unintuitiv. Microsofts Interesse, das zu ändern, hält sich aber in Grenzen. Mit dem „Advanced Group Policy Management“ (AGPM) hat das Unternehmen eine weitere Oberfläche im Programm, die mehr Funktionen mitbringt: zum Beispiel eine Versionierung von Änderungen und ein Check-out-System, das parallele Bearbeitung und Konflikte durch mehrere Admins verhindert. Das AGPM ist aber Kunden von Microsofts Software Assurance vorbehalten.

Öffnen Sie zum Anlegen der ersten Richtlinien die Gruppenrichtlinienverwaltung. Links in der Baumstruktur finden Sie die Gesamtstruktur und darin die Domänen – am Anfang gibt es derer nur eine. Unterhalb können Sie die Organisationseinheiten Ihres Active Directory anlegen. Widerstehen Sie der Versuchung, die komplette Struktur bis in alle Ebenen nachzubauen. Richten Sie die Verschachtelung erst ein, wenn Sie irgendwann eine spezialisierte Richtlinie auf eine OU brauchen. Per Rechtsklick auf den Domänennamen finden Sie den Menüpunkt, über den Sie eine OU hinzufügen.

Für die Experimente in diesem Artikel brauchen Sie keine OUs; Sie richten ein GPO für die ganze Domäne ein. Rechtsklicken Sie auf den Domänennamen, dann auf „Gruppenrichtlinienobjekt hier erstellen und verknüpfen …“ Als Beispiel sollen Windows im Folgenden ein paar der ärgsten Datenschutz-Zumutungen abgewöhnt werden. Nennen Sie Ihre Richtlinie daher zum Beispiel „Datenschutz“. Wenn Sie in der Baumstruktur darauf klicken, sehen Sie eine Ansicht mit vier Reitern. Im Reiter „Bereich“ finden Sie die Sicherheits- und WMI-Filter. Beide lassen Sie zunächst unverändert. Im zweiten Reiter „Details“ gibt es nur eine Einstellung. Dort können Sie ein GPO ganz deaktivieren (wenn es zum Beispiel temporär nicht gebraucht wird). Interessanter ist die Möglichkeit, nur die Benutzer- oder die Computer-Einstellungen zu deaktivieren. Wenn ein GPO nur eine der beiden Kategorien enthält, sollten Sie die andere hier abschalten. Das spart bei der Abarbeitung später Zeit, wenn Ihre Domäne viele GPOs enthält.

Auf dem Reiter „Einstellungen“ finden Sie den Kern des GPO. Diese Darstellung fällt optisch komplett aus dem Rahmen von Windows-Werkzeugen und wird technisch noch immer vom Internet Explorer dargestellt. Wenn Sie ein Warnhinweis davon abhält, diese Seite anzuzeigen, müssen Sie in diesem eine Ausnahmeregel hinzufügen. Sie sehen



Per Richtlinie bekommt Cortana Schweigen verordnet und auch die Telemetrie schränken Sie mit wenigen Klicks organisationsweit ein. Die Nutzer können solche Anordnungen dann nicht mehr überschreiben.

Gruppenrichtlinien für mehr Datenschutz

Typ	Ort[1]	Name	Empfohlene Einstellung
Computerkonfiguration	/AV/Windows-Komponenten/ Datensammlung und Vorabversionen	Telemetrie zulassen	Aktiviert (Stufe 0)
Computerkonfiguration	/AV/Windows-Komponenten/ Datensammlung und Vorabversionen	Übermitteln des Gerätenamens in Windows-Diagnosedaten zulassen	Deaktiviert
Computerkonfiguration	/AV/Windows-Komponenten/Suche	Cloudsuche zulassen	Aktiviert (Cloudsuche deaktivieren)
Computerkonfiguration	/AV/Windows-Komponenten/Suche	Websuche nicht zulassen	Aktiviert
Computerkonfiguration	/AV/Windows-Komponenten/Store	Store-Anwendung deaktivieren	Aktiviert
Computerkonfiguration	/AV/Windows-Komponenten/OneDrive	Verwendung von OneDrive für die Dateispeicherung verhindern	Aktiviert
Computerkonfiguration	/AV/System/Benutzerprofile	Werbe-ID deaktivieren	Aktiviert

[1] AV = Richtlinien/Administrative Vorlagen

eine Ziehharmonika-Struktur und dort ganz unten die Computer- und die Benutzerkonfiguration. Um Regeln zu definieren, klicken Sie irgendwo auf der Seite mit der rechten Maustaste, dann auf „Bearbeiten“. Es öffnet sich ein weiteres Werkzeug, der Gruppenrichtlinienverwaltungs-Editor.

Los geht es mit dem Abschalten der Telemetriedatenübermittlung an Microsoft. Die Richtlinie finden Sie unter „Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Datensammlung und Vorabversionen“. Klicken Sie dort doppelt auf „Telemetrie zulassen“. Zunächst müssen Sie die Richtlinie oben aktivieren, dann können Sie darunter die Telemetrie-Stufe auswählen. Die Details zu den Auswirkungen einer Richtlinie stehen im Dialog unten rechts. In Kurzform: Wenn Sie Stufe 0 wählen, sendet Windows Enterprise gar keine Daten, die anderen Versionen (Pro und Education) möglichst wenig. Speichern Sie mit OK.

Wenn Sie das Prinzip einmal ausprobiert haben, sind Sie bereit für die Konfiguration Ihrer Clients und der Rest der Arbeit ist reine Fleißarbeit. In der Tabelle „Gruppenrichtlinien für mehr Datenschutz“ finden Sie einige (nicht alle) Datenschutzrichtlinien und empfehlenswerte Konfigurationen.

Wenn Sie alle Richtlinien für das GPO konfiguriert haben, schließen Sie den Gruppenrichtlinienverwaltungseditor einfach. Das fühlt sich komisch an, aber es gibt keinen Knopf zum Speichern oder Übernehmen. Danach sehen Sie zunächst wieder die leere Ziehharmonika-Ansicht. Auch das ist nicht gerade nutzerfreundlich gemacht: Um Ihre Änderungen zu sehen, klicken Sie wieder irgendwo rechts und dann auf „Aktualisieren“. Ihr GPO ist in diesem Moment aber bereits aktiv.

Richtlinienverarbeitung

GPOs werden zu zwei festen Zeitpunkten verarbeitet: Computerrichtlinien beim Booten, bevor Sie den Anmeldeschirm sehen. Meldet sich dann ein Domänennutzer an, beginnt die Abarbeitung der für ihn eingerichteten Benutzerrichtlinien. Außerdem werden die Richtlinien regelmäßig nach 90 Minuten im Hintergrund aktualisiert. Wenn Ihnen dieses Intervall zu lang oder zu kurz ist, können Sie es ändern – ebenfalls per Gruppenrichtlinie. Die Einstellung finden Sie in den administrativen Vorlagen für Computer unter System/Gruppenrichtlinie unter dem Namen „Gruppenrichtlinien-Aktualisierungsintervall für Computer festlegen“. Gerade in der Phase, in der Sie an Ihrer Test-VM Gruppenrichtlinien optimieren, wollen Sie vermutlich nicht so lange warten. Per Hand stoßen Sie die Verarbeitung aller neuen und geänderten Richtlinien auf der Kommandozeile des Clients mit dem Befehl `gpupdate` an. Empfehlenswert ist in der Experimentierphase der Parameter `/force`. Dann werden alle Richtlinien noch einmal angewendet:

```
gpupdate /force
```

Weil manche Richtlinien eine erneute Anmeldung erfordern, können Sie noch `/logoff` anhängen. Wenn es nötig ist, wird der aktuelle Nutzer dann abgemeldet. Melden Sie sich in Ihrer Test-Domäne an einem

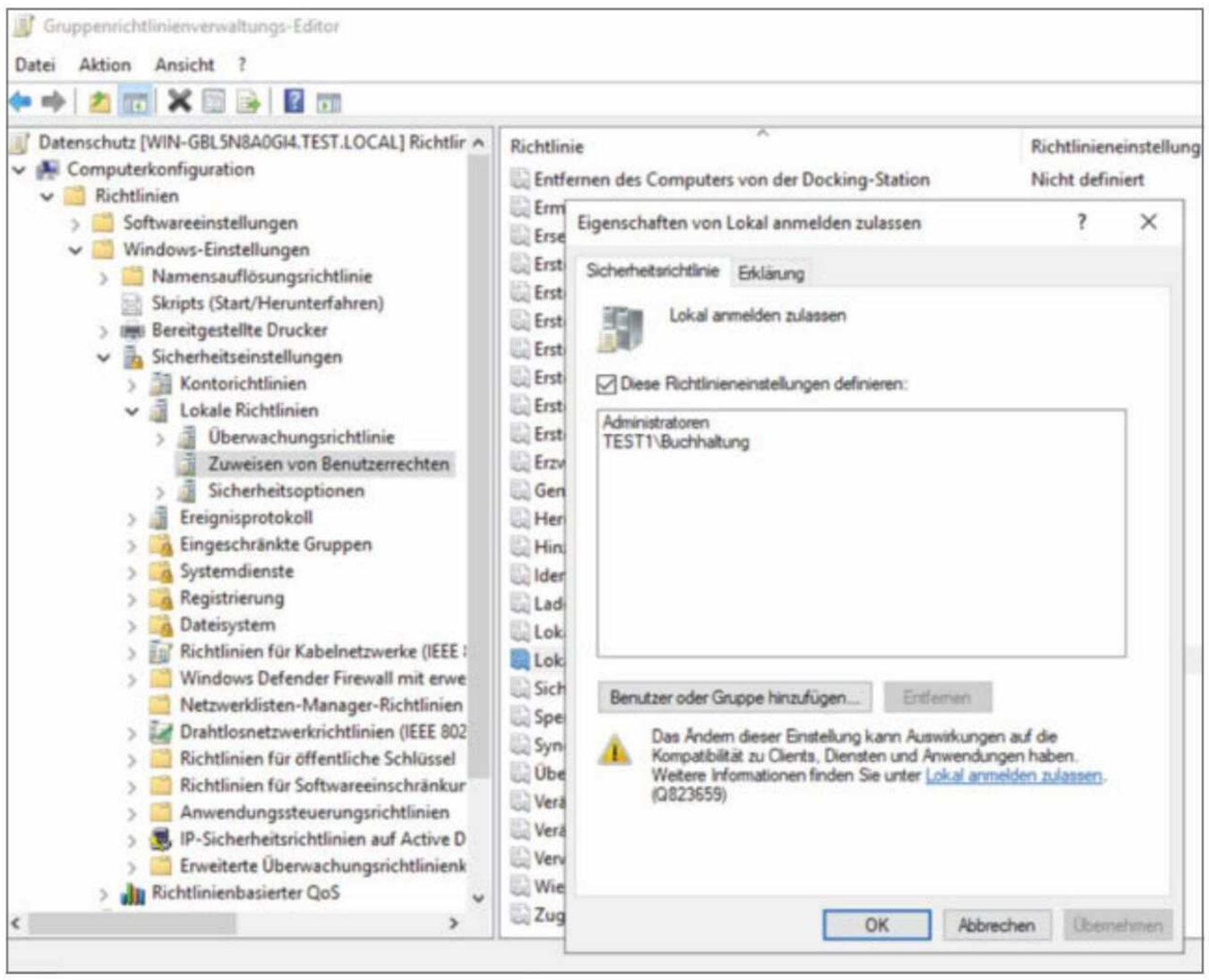
Windows-Client an und sehen Sie nach, ob die Telemetrie-Stufe erfolgreich angepasst wurde.

Was Sie per Richtlinien alles konfigurieren können, erfahren Sie am besten, wenn Sie in einer ruhigen Minute die administrativen Vorlagen für Benutzer und Computer durchstöbern, besonders die Ordner System und Windows-Komponenten sind sehr ergiebig. Nach einem Streifzug durch die Ordner haben Sie eine grobe Vorstellung, was möglich ist. Wenn Ihnen später ein Problem begegnet, das Sie gern per Richtlinie abstellen würden, hilft am besten eine Suche in einer Suchmaschine zusammen mit dem Begriff „GPO“. Im Internet gibt es außerdem einige Listen, die von Freiwilligen gepflegt werden (siehe ct.de/w21j). Nicht alle Pfade zu allen Richtlinien auswendig zu kennen, ist keine Schande und die Sortierung ist nicht immer sofort einleuchtend.

Richtlinien ohne Vorlage

Auch außerhalb des Ordners „Administrative Vorlagen“ gibt es Richtlinien – diese werden ein bisschen anders konfiguriert. Eine solche Richtlinie brauchen Sie für eine ganz alltägliche Aufgabe: Standardmäßig kann sich jeder Nutzer an jedem Windows-Desktop in der Domäne anmelden. Das ist vielleicht in manchen Großraumbüros ohne feste Plätze sinnvoll, in den meisten Unternehmen aber nicht erwünscht.

Um festzulegen, dass sich an Rechnern der Organisationseinheit „Buchhaltung“ nur Mitglieder der Nutzergruppe „Buchhaltung“ anmelden dürfen, legen Sie in der Gruppenrichtlinienverwaltung zuerst die Organisationseinheit an der Stelle an, an der sie auch im Active Directory liegt. Verknüpfen Sie dort eine neue Gruppenrichtlinie mit einem sprechenden Namen wie „Anmelden Buchhaltung“ und wechseln Sie in den Gruppenrichtlinienverwaltungseditor. Biegen Sie dort unter Computerkonfiguration/Richtlinien nicht wie gewohnt in die administrativen Vorlagen ab, sondern zu „Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrollen“. Dort finden Sie die Richtlinie „Lokal anmelden zulassen“. Aktivieren Sie diese Richtlinie und fügen Sie die Namen von Gruppen hinzu, die sich anmelden dürfen. Damit Sie den vollständigen Namen der Gruppe nicht eintippen müssen, wählen Sie „Durchsuchen“, geben in die Suche den Anfang des Gruppennamens ein und lassen nach der Gruppe suchen. Anschließend werden Sie noch per Warnhinweis daran erinnert, dass Sie sich nicht selbst aussperren sollen: Eine Gruppe mit Administratoren müssen Sie immer zusätzlich angeben.



Wer sich an Computern in Ihrer Domäne anmelden darf, steuern Sie per Richtlinie. Eine Administratorengruppe muss immer in der Liste enthalten sein.

Weitere Forschung

Mit diesem Wissen sind Sie bereit, Ihre Computer auf eigene Faust mit Richtlinien zu steuern und sich das Leben einfacher zu machen.

Wenn Sie mit den Grundfunktionen von Active Directory und GPOs vertraut sind, sollten Sie sich im nächsten Schritt mit den Sicherheitsproblemen vertraut machen, die aus allzu lax konfigurierten Active Directories resultieren. In den Standardeinstellungen machen Sie es Angreifern und Erpressern nämlich zu leicht, Ihr System zu kapern. Insbesondere allmächtige Admin-Accounts, die sowohl in der Domäne als auch auf allen Clients frei walten dürfen, haben in einer produktiven Umgebung nichts zu suchen. Um lokale Admin-Konten über das AD zu verwalten, gibt es ein vergleichsweise neues Verfahren, das per GPO gesteuert wird [2]. Das einzurichten, ist ein lohnenswerter nächster Schritt. (jam) c't

Literatur

[1] Hajo Schulz, **Registratur**, Was Sie über die Windows-Registry wissen müssen, c't 17/2021, S. 144

[2] Jan Mahn, **Passwort-Auswürfler**, Lokale Admin-Passwörter in der Windows-Domäne verwalten, c't 14/2019, S. 158

Listen und Downloads

ct.de/w21j

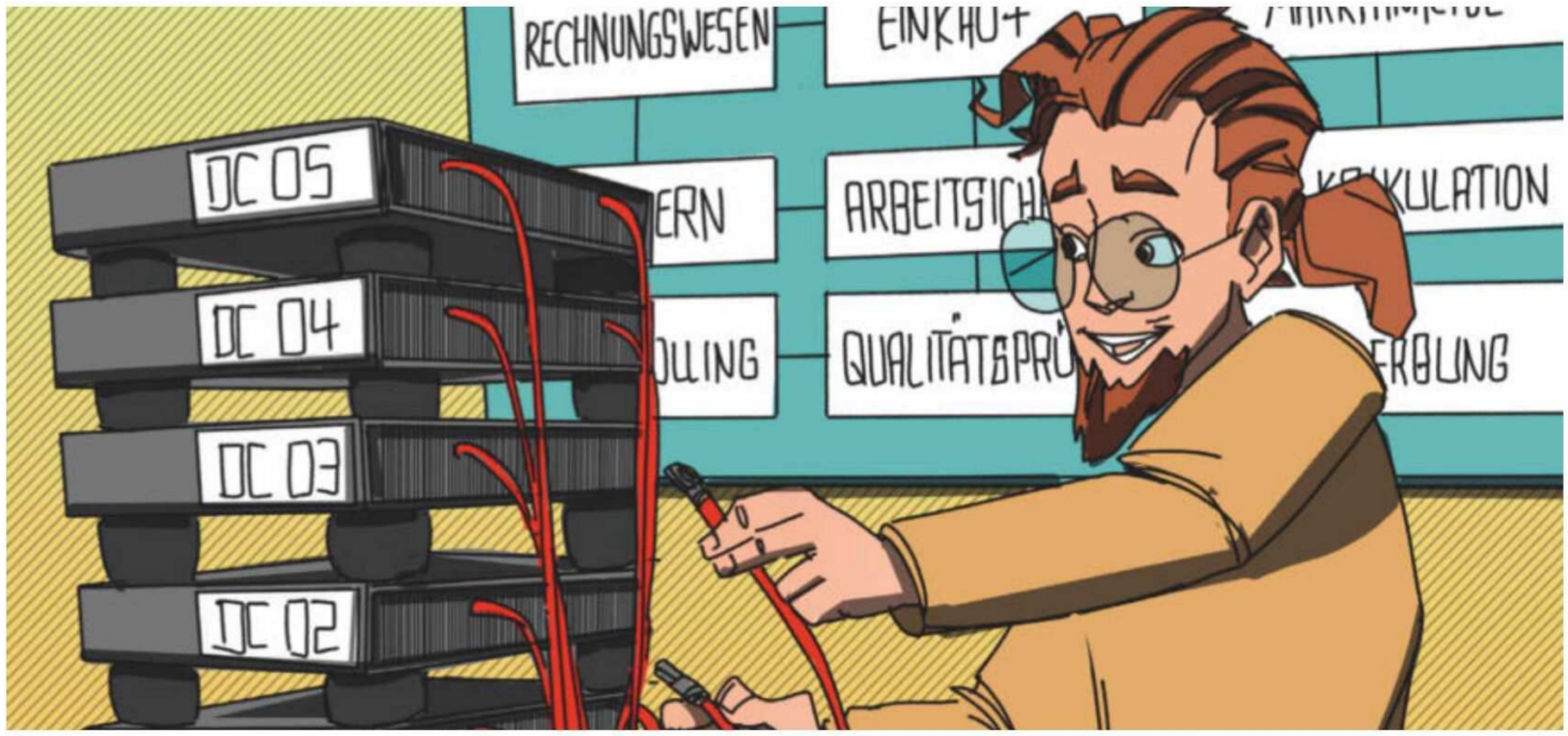


Bild: Thorsten Hübner

Redundante Domaincontroller

Microsofts Active Directory ist die Schaltzentrale in vielen großen Netzwerken, sodass selbst kurze Ausfälle den gesamten Betrieb lahmlegen und Geld kosten. Daher sollten immer mehrere Server als Domaincontroller im Team arbeiten.

Von **Jan Mahn**

Admins von Organisationen, die viele Benutzer, Gruppen und Windows-Computer verwalten müssen, schätzen die Funktionen des Active Directory, das tief in Windows Server und die Desktop-Windows-Ausgaben integriert ist. Nachdem eine Domäne mit Benutzern und Gruppen eingerichtet ist (siehe S. 96), sind Gruppenrichtlinienobjekte (Group Policy Objects, GPO) der nächste Schritt zum zentral verwalteten Netzwerk (siehe S. 104).

So praktisch eine zentrale Steuerung auch ist: Fällt der Domaincontroller (DC) aus, geht schlagartig vieles nicht mehr. Eine Domäne läuft zwar grundsätzlich auch auf einem einzelnen DC, das ist aber alles andere als empfehlenswert. Schon ein Neustart des DC nach einem Windows-Update würde Ausfälle für alle Nutzer bedeuten. Deshalb gilt es, jegliche Unterbrechungen beim Betrieb des Active Directory zu vermeiden, was nur funktioniert, wenn man sich nicht auf einen einzelnen DC verlässt.

Rudeltiere

Mit der Anforderung, das Active Directory (AD) auf mehrere Schultern zu verteilen, sind Sie bei Weitem nicht allein. Die Microsoft-Entwickler haben sich ein komplexes Verfahren ausgedacht, um das AD redundant zu betreiben. Die Datenbank mit Nutzern, Computern und Gruppen wird dann auf mehreren Servern synchron gehalten (repliziert). Gleichzeitig haben die Erfinder berücksichtigt, dass Organisationen sehr

groß werden und Niederlassungen überall auf dem Globus betreiben können. Sobald man so dezentral organisiert ist und nur per Internet (über ein VPN) mit dem Rest des Unternehmens verbunden ist, wird jede Replikation zwangsläufig kompliziert – bestenfalls soll das lokale Netz auch dann weiter funktionieren, wenn die Verbindung zur Konzernzentrale temporär ausfällt.

Bevor Sie mit der Einrichtung mehrerer Domaincontroller loslegen, brauchen Sie einen Überblick, welche Aufgaben jeder Server übernehmen kann. Damit die Replikation für möglichst viele Gegebenheiten sinnvoll eingerichtet werden kann, hat sich Microsoft nämlich insgesamt fünf Rollen ausgedacht, von denen jeder Domaincontroller mehrere ausfüllen kann. Solange Sie ein AD nur auf einer Maschine betreiben, ist das einfach: Alle Rollen liegen dann auf diesem Server. Sobald der zweite Server dazu kommt, kann die Arbeit aufgeteilt werden.

Bei Microsoft heißt dieses Prinzip „Flexible Single Master Operations“ (FSMO) und die Bezeichnung FSMO-Rolle ist in Adminkreisen recht verbreitet. Das Wort „Master“ verrät, dass es trotz replizierter Informationen stets eine Autorität gibt, die Auskünfte über die derzeit geltende Wahrheit geben kann, ohne sich mit anderen abzustimmen. Wer den Master fragt, bekommt jederzeit schnell eine gültige Antwort. Jede Master-Rolle ist dabei für einen Themenbereich zuständig.

Auf Ebene der Gesamtstruktur gibt es zwei solcher Rollen, die jeweils nur ein Server gleichzeitig haben kann. Recht unspektakulär ist der Domain-Naming-Master (Domänenbenennungs-Master). Der Server mit dieser Rolle stellt sicher, dass niemand eine Domäne einrichtet, deren Name in der Gesamtstruktur schon vergeben ist. Nur er kann zuverlässig sagen, ob ein gewählter Domänenname schon in Benutzung ist. Kontakt zu einem Server mit dieser Rolle braucht man also immer, wenn man eine neue Domäne anlegen will, also selten. Etwas häufiger gefragt ist der Schema-Master. Dieser verwaltet die Schemas der Objekte und wird immer gebraucht, wenn man diese Objektschablonen verändert. Das kommt zum Beispiel vor, wenn man eine Software installiert, die tief ins Active Directory integriert ist, neue Datenfelder braucht und während ihrer Installation Schemaerweiterungen platziert (wie etwa Microsofts Exchange). Auch den Schema-Master gibt es nur einmalig in einer Gesamtstruktur.

In einer kleinen Umgebung liegen diese beiden Rollen auf einem der DC. Unternimmt man nichts, auf dem zuerst eingerichteten, und bestenfalls muss man sich nie wieder damit beschäftigen, dass es die Rollen überhaupt gibt. Fällt der erste DC mit diesen Rollen unrettbar aus, muss man die Rollen von einem anderen übernehmen lassen – dazu später mehr. Eine solche Rettung ist aber nicht dringend, einen Ausfall bemerkt zunächst kein Nutzer bei der täglichen Arbeit, Anmeldungen und GPO-Verarbeitung laufen ohne einen Server mit diesen Rollen weiter.

In großen Unternehmen, die mit mehreren Domänen an ihren Standorten arbeiten, liegen die beiden Gesamtstrukturrollen auf einem zentralen Server, zum Beispiel im Rechenzentrum der Firmenzentrale. Es reicht, wenn die DC in den Niederlassungen ihn durch ein VPN über das Internet erreichen. Weil die Rollen nur selten angefragt werden, bremst die Internetverbindung das Tagesgeschäft nicht und temporäre Internetausfälle stören nicht.

Domänenrollen

Drei weitere Master-Rollen existieren in jeder Domäne. In kleinen Umgebungen, zum Beispiel mit drei DC und nur einer Domäne in der Gesamtstruktur, ist die Aufteilung weiterhin unspektakulär und auch diese Rollen können zusammen mit den beiden Gesamtstruktur-Rollen auf dem ersten DC liegen.

Für das Anlegen von Objekten wichtig ist der RID-Master. Jeder Computer, jede Gruppe und jeder Benutzer bekommen im Active Directory einen eindeutigen Bezeichner, den Security Identifier (SID). Dieser ist tief in Windows verwurzelt und wird dort unter anderem für Berechtigungen genutzt. Benutzername, Anzeigename und Position im Active Directory können sich ändern, die SID bleibt erhalten. Eine SID sieht zum Beispiel folgendermaßen aus: S-1-5-21-3623811015-3361044348-30300920-1234. Der Block „-21-“ zeigt an, dass es sich um einen Domänen-Account handelt. Es folgt ein Bezeichner für die Domäne. Der letzte Block, hier „-1234“, ist der Relative Identifier (RID). Er wird bei jedem neuen Objekt inkrementiert und muss in der Domäne einmalig sein. Damit mehrere DCs neue Objekte anlegen können, ohne sich mit allen anderen darüber beraten zu müssen, welche RID zuletzt vergeben wurde, teilt der RID-Master allen Domaincontrollern seiner Domäne vorab Blöcke zu, aus denen sie sich bedienen können. Einen Ausfall des RID-Masters bemerkt man also erst, wenn ein DC seinen Block aufgebraucht hat und neue RIDs bestellen will. In den Standardeinstellungen bekommt jeder DC 500 RIDs vom RID-Master zugeteilt und weitere 500,

wenn er die Hälfte seines Kontingents verbraucht hat. In der typischen Domäne eines mittelständischen Unternehmens, in der im Monat wenige neue Mitarbeiter einen Account bekommen sollen, kommt man demnach lang ohne einsatzbereiten RID-Master aus.

Regelmäßig gefragt ist der PDC-Emulator. Die Abkürzung PDC (Primary Domain Controller) stammt noch aus grauer NT4-Domänen-Vorzeit, als der PDC der einzige Server war, der Änderungswünsche an Objekten entgegennehmen konnte. Die anderen Domaincontroller hießen „Backup Domain Controller“, bekamen nur Kopien der Datenbank und konnten lediglich lesende Anfragen beantworten. Mit dem FSMO-Konzept ist damit Schluss, alle Server nehmen Schreibaufträge an und replizieren die Änderungen.

Der PDC-Emulator hat aber unter den DCs weiterhin ein paar Sonderrollen: Zunächst ist er fürs Abgleichen der Uhren seiner Kollegen zuständig – eine gemeinsame Zeitbasis ist beim Replizieren unerlässlich. Außerdem bekommt er immer als erster eine Nachricht, wenn ein anderer DC eine Kennwortänderung angenommen hat. Bis sich diese bei allen DCs rumgesprochen hat, kann es schlimmstenfalls ein paar Minuten dauern. Versucht sich in diesem Zeitfenster ein Benutzer an einem anderen DC anzumelden und bemerkt dieser ein falsches Kennwort, fragt er umgehend beim PDC-Emulator nach, ob es eine Kennwortänderung gab und probiert es damit erneut. Dieses Konstrukt ist also ein Kompromiss aus Benutzerfreundlichkeit und Lastenteilung. Ein kurzer Neustart des PDC-Emulators ist zu verschmerzen; sofern möglich legt man das Wartungsfenster aber außerhalb der Hauptnutzungszeit. Sollte der Server mit der PDC-Emulator-Aufgabe unrettbar defekt sein, muss man zügig handeln und die Aufgabe einem anderen Server zuweisen.

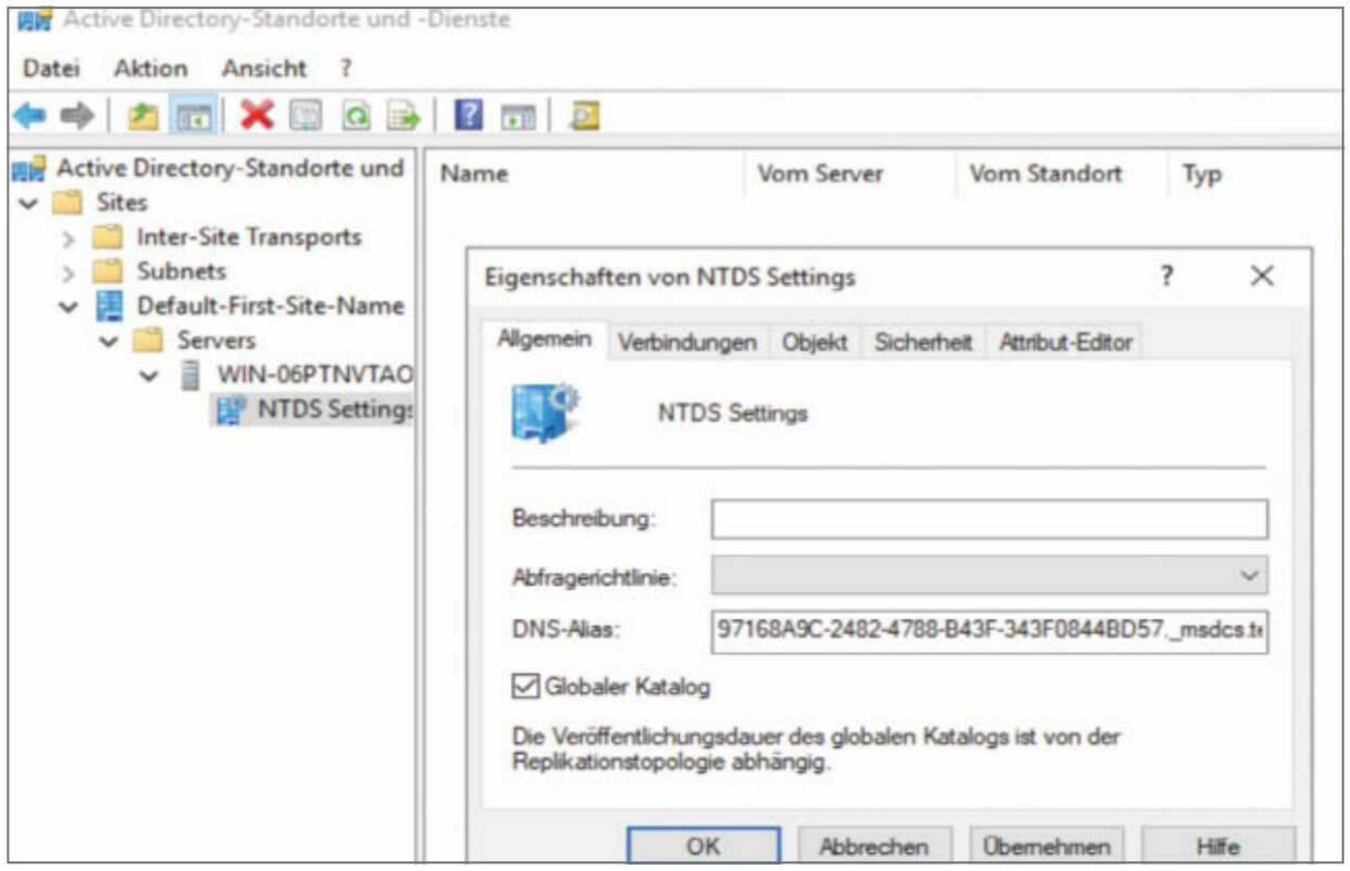
Der Infrastruktur-Master ist nur dann gefragt, wenn es in einer Gesamtstruktur mehrere Domänen gibt. Dann ist es nämlich möglich, dass Nutzer Mitglied in Gruppen anderer Domänen sind und nötig, dass Namen von Nutzern aus anderen Domänen aufgelöst werden. Hierfür gibt es den Globalen Katalog (Global Catalog, GC). Er enthält eine Kopie mit den grundlegenden Informationen sämtlicher Objekte der Gesamtstruktur. Verständlich wird das am Beispiel eines Unternehmens, das drei Standorte in Europa hat. An jedem arbeiten einige hundert Mitarbeiter, und jeder Standort hat eine eigene Domäne (berlin.example.org, wien.example.org und bern.example.org). In jedem der drei Netze stehen drei Domaincontroller, die zunächst nur die Datensätze ihrer eigenen Domain verwalten und replizieren – das ist ja der Sinn der Domänenaufteilung. Einer der drei Server an jedem Standort hält je eine Kopie des Globalen Katalogs. Er wird im internen Netz zum Beispiel befragt, wenn in Berlin in einer Gruppenliste der Vor- und Nachname eines Mitarbeiters aus Wien dargestellt werden muss. Die lokale Katalogkopie spart viele Anfragen, die quer durch Europa geschickt werden müssten. Theoretisch kann man jeden DC einer Domäne zum Katalogserver ernennen – das erhöht aber den Speicherplatz- und Replikationsbedarf und damit den Netzwerkdurchsatz. Eine Kopie des GC pro Standort ist meist die beste Wahl.

Wie Sie die FSMO-Rollen verschieben, lesen Sie im Abschnitt „Bist du nicht willig“, den Globalen Katalog können Sie per grafischer Oberfläche auf einem Server aktivieren. Der Dialog ist aber gut versteckt: Öffnen Sie auf dem Domaincontroller die Anwendung „Active Directory-Standorte und -Dienste“ (in die Suche eintippen). Hangeln Sie sich dort in der Baumstruktur über den Namen Ihres Standortes, den Punkt „Servers“ und Ihren Servernamen zu „NTDS Settings“ durch. Mit einem Rechtsklick darauf erreichen Sie „Eigenschaften“ und können dort den Haken für den Globalen Katalog setzen. Die Replikation kann sich je nach Netzwerkverbindung und Organisationsgröße über Stunden ziehen.

Katalogverwalter

Die Rolle des Infrastruktur-Masters ist eng verbunden mit dem Globalen Katalog. Seine Aufgabe: Unterschiede zwischen Globalem Katalog und seinem eigenen Datenbestand erkennen und lokal in der Domäne umsetzen. Er würde es zum Beispiel mitbekommen, wenn ein Nutzer, der in einer organisationsweiten Gruppe steckt, im Globalen Katalog gelöscht wurde, und ihn in seiner eigenen Domain aus dieser Gruppe entfernen. Diese Änderung würden die anderen DCs per Replikation mitbekommen und ihn auch tilgen – so bleiben die Server synchron.

Die Infrastruktur-Master zu positionieren, ist nicht ganz trivial, grundsätzlich gilt: Bei mehreren Domänen braucht jede einen Infrastruktur-Master. Es gibt zwei Möglichkeiten, aus denen Sie für jede Domäne einzeln auswählen: Haben Sie sich dafür entschieden, dass in einer Domäne alle DCs den Globalen Katalog führen, ist es unerheblich, welcher die Infrastruktur-Master-Rolle bekommt. Sobald auch nur einer der DCs einer Domäne den Globalen Katalog nicht führt (was ja durchaus empfohlen ist), gilt für



Gut versteckt: Den Globalen Katalog weist man über das Werkzeug „Active Directory-Standorte und -Dienste“ einem oder mehreren Domaincontrollern zu.

diese Domäne eine Sonderregel: Der Infrastruktur-Master darf dann nicht gleichzeitig eine Kopie des Globalen Katalogs haben. Um die Regel zu verstehen, muss man etwas um die Ecke denken und vor allem wissen, dass der Globale Katalog keine separate Datenbank ist, sondern zusammen mit den eigenen AD-Objekten gespeichert wird. Hat ein Server den Globalen Katalog, liegen fremde Objekte (wenn auch nur als Teilkopie) stets aktuell in seiner Datenbank. Der Infrastruktur-Master ist technisch so umgesetzt, dass er Abweichungen zwischen Globalem Katalog und eigener Datenbank erkennt und an die anderen DCs weitergibt – hat ein Server beide Funktionen, würde er immer seine eigenen Daten mit sich selbst vergleichen und demnach niemals eine Änderung bemerken, die er an die Kollegen weitergeben müsste. Opfer dieser Informationslücke wären daher die DCs in der Domäne, die weder Globalen Katalog noch Infrastruktur-Master-Rolle haben. Sobald Sie eine dezentrale Infrastruktur haben, müssen Sie die Infrastruktur-Master-Rolle an jedem Standort auf einen freien DC verschieben – dazu später mehr.

Keine Panik

Wenn Sie angesichts der Komplexität der FSMO-Rollen die Lust verloren haben, das AD redundant zu betreiben, gibt es gute Nachrichten: In einem Unternehmen mit einem Standort und einer Domäne ist die Welt vergleichsweise einfach. Wenn Sie aktuell nur einen DC in Betrieb haben, installieren Sie eine weitere Maschine mit Windows Server und geben ihr über den Server-Manager die Active-Directory-Rolle (wie ab S. 96 beschrieben). Der grafische Assistent, über den Sie den Server im Anschluss zum DC hochstufen, fragt Sie im Verlauf, ob Sie eine neue Gesamtstruktur oder Domäne anlegen oder ihn zu einer bestehenden Domäne hinzufügen wollen. Wählen Sie letztere Option, dann ist Ihr Active Directory mit wenigen Klicks redundant und Ihre Windows-Clients befragen ab sofort auch den neuen Server. Windows-Updates installieren Sie am besten nacheinander und beginnen auf den anderen DCs. Der zuerst eingerichtete DC ist Rolleninhaber aller FSMO-Rollen und zuletzt dran, wenn Sie sich sicher sind, dass das Windows-Update auf den anderen DCs keine schweren Nebenwirkungen hatte. Bestenfalls starten Sie ihn nach Feierabend neu.

Einblick in die Rollenverteilung brauchen Sie entweder, wenn Ihre Umgebung größer wird, neue Standorte und Domänen hinzukommen, wenn Sie einen FSMO-Rolleninhaber für längere Zeit (Stunden oder Tage) für Wartungsarbeiten abschalten müssen – oder wenn er den Dienst verweigert.

Bist du nicht willig

Wie fast immer in Windows gibt es mehrere Wege, um auf eine Einstellung zuzugreifen. Auch die FSMO-Rollen kann man per Kommandozeile, per PowerShell und teilweise per grafischer Oberfläche verwalten. Am schnellsten kommen Sie auf der Kommandozeile zu einer Liste aller aktuellen Rolleninhaber:

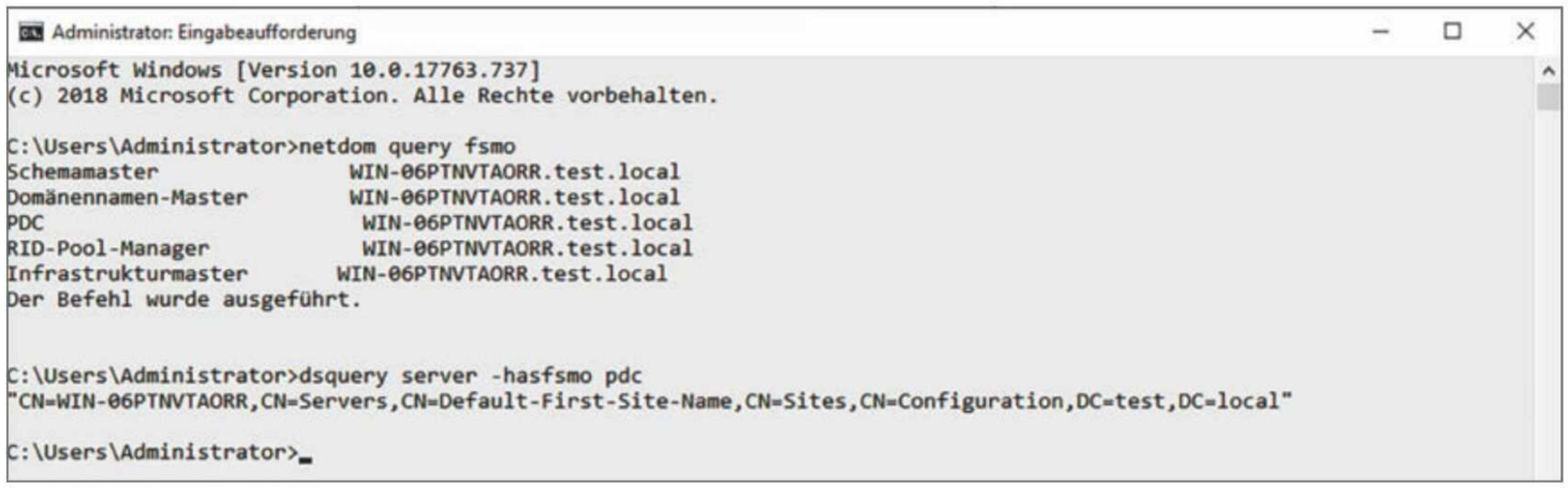
```
netdom query fsmo
```

Wenn Sie den vollen DistinguishedName eines Rolleninhabers brauchen, kommen Sie mit `dsquery` zum Ziel:

```
dsquery server -hasfsmo pdc
```

Den letzten Parameter können Sie gegen `pdc`, `rid`, `infr`, `name` und `schema` tauschen, um die anderen Rolleninhaber zu sehen. PowerShell-Fans, die die Informationen für Skripte und Reports brauchen, kommen mit `Get-ADDomain` und `Get-ADForest` an die Rolleninhaber von Domäne und Gesamtstruktur.

Rollen können auf zwei Wegen den Besitzer wechseln: per Übergabe oder per Übernahme. Klingt



Der Befehl netdom in der Eingabeaufforderung listet alle Rolleninhaber auf. Braucht man den DistinguishedName, hilft dsquery.

spitzfindig, ist aber entscheidend. Eine Übergabe ist ein einvernehmlicher Akt, bei dem beide Server (bisheriger und neuer Inhaber) online und intakt sind. Wenn man plant, etwas an der Struktur zu optimieren, wählt man immer dieses Mittel. Nicht nötig ist es, vor jedem Neustart und jeder Update-Installation per Hand die FSMO-Rollen zu übergeben. Das wäre in den allermeisten Fällen übertrieben.

An einer Übernahme sind nicht beide Server beteiligt. Sie ist das letzte Mittel, wenn der bisherige Rolleninhaber unrettbar offline ist. Bei einer Übernahme ermächtigen Sie einen anderen Server, diese Rollen zukünftig zu bekleiden. Entscheidend dabei: Der bisherige Inhaber darf danach nie wieder im Netzwerk auftauchen, nicht heute und nicht in ein paar Jahren versehentlich. Selbst wenn Sie es später schaffen sollten, beispielsweise die defekte virtuelle Maschine doch noch zu booten – nach der Übernahme der Rollen ist der Zug abgefahren. Zwei Server in einer Domäne, die sich zum Rolleninhaber derselben Rolle erklären, sind der sichere Weg ins Chaos: Alte Daten, längst geänderte Kennwörter und unangenehme Replikationsprobleme sind die Folge. Schlimmstenfalls endet das mit langwierigem Gefummel im ADSI-Editor.

Eine friedliche Übergabe starten Sie am bequemsten per PowerShell (mit administrativen Rechten) auf einem der DC. Empfehlenswert ist es in jedem Fall, zunächst mal in einer Experimentierumgebung die Befehle auszuprobieren, bevor Sie sich an die produktive Domäne machen. Zuständig für die Rollenverschiebung ist der PowerShell-Befehl `Move-ADDirectoryServerOperation`. Um zum Beispiel die Rollen des Betriebsmasters und des PDC-Emulators auf einen Server mit dem Namen DC02 zu verschieben, setzen Sie folgenden Befehl auf einem der DCs (oder einer anderen Maschine, auf der die AD-Verwaltungswerkzeuge RSAT installiert sind) ab:

```
Move-ADDirectoryServerOperation↵
↳MasterRole -Identity "DC02" ↵
↳-OperationMasterRole,PDCEmulator
```

Wer nicht gern viel tippt, schreibt nur `move-add`, betätigt zweimal die Tab-Taste und lässt die PowerShell den Befehl automatisch vervollständigen. Mehrere Rollen können Sie per Komma an den Befehl anhängen, die Werte für die fünf Rollen heißen `PDCEmulator`, `RIDMaster`, `InfrastructureMaster`, `DomainNamingMaster` und `SchemaMaster`. In dieser Reihenfolge haben die Rollen auch Nummern von 0 bis 4, die Sie statt der langen Namen einsetzen können.

Sofern beide Server online und bereit sind, meldet der PowerShell-Befehl schnell Vollzug und die Operation ist erledigt. Gelingt das nicht, verabschieden Sie sich vom alten Rolleninhaber, fahren ihn für immer herunter (verbannen die virtuelle Festplatte mit einem Sicherheitshinweis versehen ins Archiv, damit niemand den Server später startet) und hängen den Parameter `-Force` an den PowerShell-Befehl an. Dass die Übernahme erfolgreich war, zeigt ein erneuter Aufruf von `netdom` oder `dsquery`.

Einfacher als gedacht

Ein redundantes Active Directory sollte weder Schmerzen noch schlaflose Nächte bereiten. Im Gegenteil – auf mehrere Schultern verteilt, läuft das System zuverlässiger, und auch Updates mit Neustarts sind kein Problem. Hat man die Aufgaben der fünf FSMO-Rollen und des Globalen Katalogs einmal verstanden, verlieren auch diese Funktionen ihren Schrecken. Dann steht auch großen Umgebungen mit mehreren Domänen nichts mehr im Weg, in denen an jedem Standort nur die Objekte liegen, die dort auch gebraucht werden. (jam) c't

Die volle Ladung



Auch als Heft + PDF mit 29 % Rabatt

Dieses c't-Sonderheft räumt auf mit Mythen rund ums E-Auto und schafft einen realen Überblick zu Vor- und Nachteilen der E-Mobilität

- ► Leitfaden zum Kauf eines E-Autos
- ► Kostenvergleich: Storm vs. Sprit
- ► Fahrberichte und Tests
- ► Den Akku richtig nutzen und laden
- ► Überschussladen – Strom aus Photovoltaik nutzen
- ► Auch als Bundle mit Buch „E-Autos einfach erklärt“ vom dpunkt-Verlag erhältlich!

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

shop.heise.de/ct-eautos22

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

M·net

Jetzt beraten lassen!

Wir vernetzen ihr Business

Mit den leistungsstarken Vernetzungslösungen von M-net.

- Zukunftsfähige Glasfaser-Technologie
- Für jede Unternehmensgröße

m-net.de/geschaeftskunden/vernetzung

M-net ist klimaneutral*

* Bereits erreicht und noch viel vor: m-net.de/klimaneutral