c't FRITZBOX

Absichern · Erweitern · Tunen

Komfortabel telefonieren

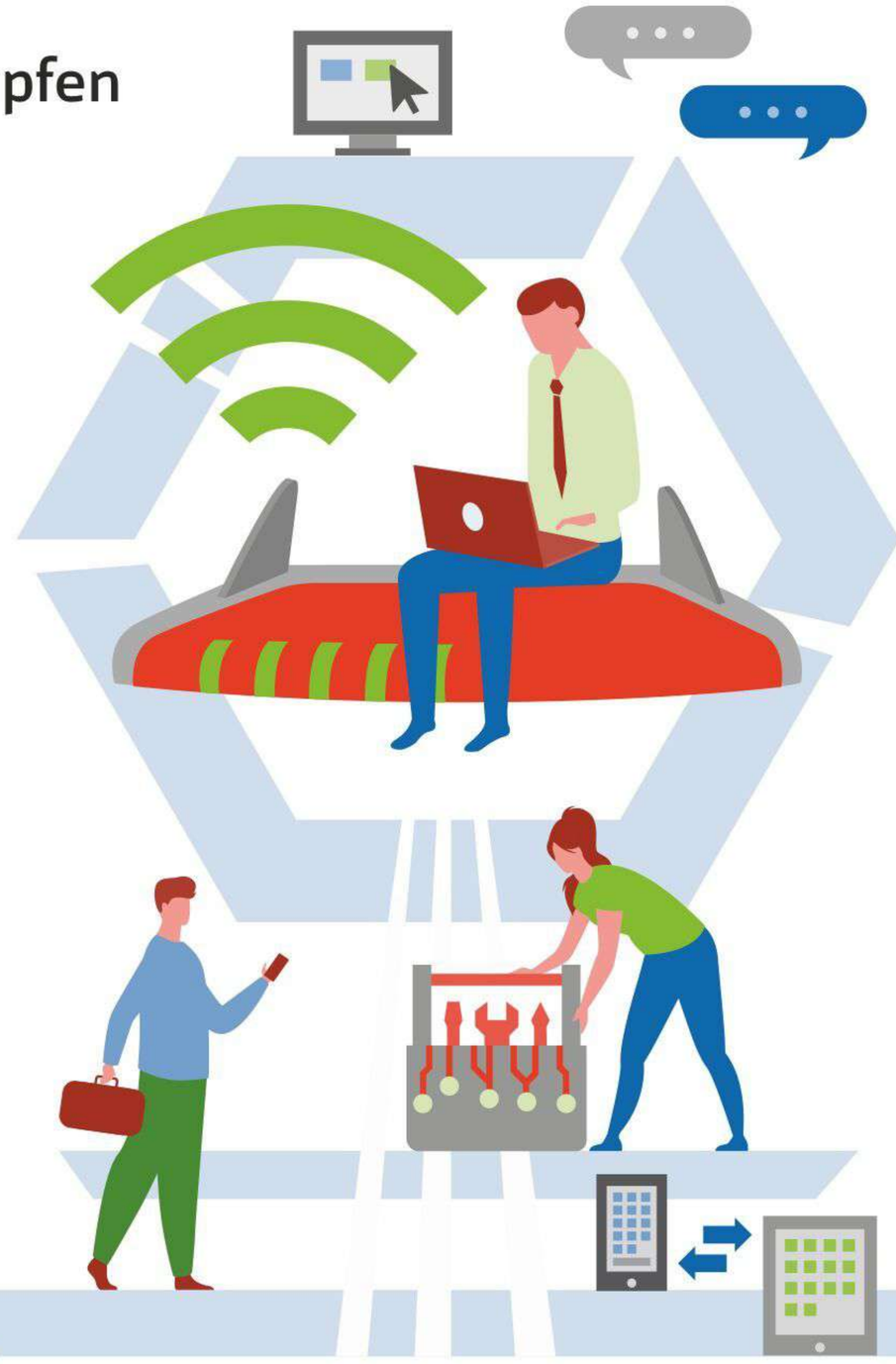
Gebrauchte Businesstelefone mit Fritzbox verknüpfen
Abhörsicher mit FritzOS telefonieren
Funklöcher stopfen mit Fritzbox und Raspi

WLAN ausreizen

Wie die Verbesserungen von Wi-Fi 6 wirken
Das bringt AVMs erster Repeater für Wi-Fi 6
Im Test: Fünf WLAN-Router gegen die Fritzbox
Mit WPA3 extrasicher funken

Optimal vernetzen

Was für Ihre nächste Fritzbox wichtig ist
Fritzbox: DynDNS mit IPv6 leicht gemacht
Internetausfällen vorbeugen



facebook.com/ctspecials

Fritzbox niet- und nagelfest

Heimnetz absichern · Tracking verhindern · Privatsphäre schützen
VPN trotz Kabelanschluss einrichten · Malware draußen halten

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

4 196982 314900 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

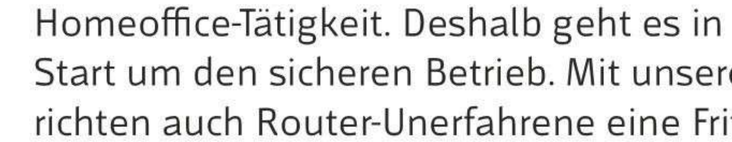
Liebe Leserin, lieber Leser,

als Technik-interessierter Anwender kann man leicht der Faszination des Neuen erliegen – und davon bieten die aktuelle Generation der Fritzbox-Router und ihr wieder einmal geglückt erweitertes FritzOS-Betriebssystem reichlich. Beispielsweise bildet der Router mit dem schnellen Wi-Fi 6, der WLAN-Verschlüsselung WPA3 und dem Privatsphärenschutz die Speerspitze der aktuellen Technologie-entwicklung ab.

Doch letztlich soll ein Router alle Ihre Netzwerkgeräte reibungslos ans Internet ankoppeln, vor allem im Licht der zunehmenden Homeoffice-Tätigkeit. Deshalb geht es in diesem Heft gleich zum Start um den sicheren Betrieb. Mit unseren praxisnahen Beiträgen richten auch Router-Unerfahrene eine Fritzbox unfallfrei ein, halten Möchtegern-Eindringlinge wirksam fern und schützen private Surfgewohnheiten vor fremden Augen und Telefonate vor fremden Ohren.

Fällt der Internetzugang aus, kann das zu erheblichen Behinderungen führen. Um Nachteile abzufedern, genügt aber ein einfacher Plan. Damit sind Sie mit Ihrer Fritzbox nervenschonend wieder online, noch bevor der Techniker „DSL-Leitungsanalysator“ buchstabiert hat.

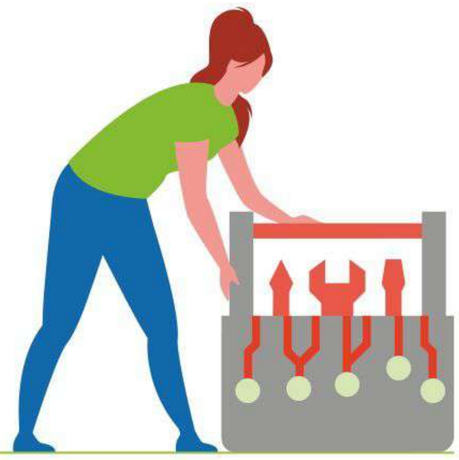
Doch auch ein „Alleskönner“ wie die Fritzbox kann in Wahrheit nicht alles. Lesen Sie, wie sich Business-Telefone günstig anbinden lassen oder wie Sie ein VPN trotz Kabelanschluss aufsetzen. Der Fritzbox kommt dabei der Mini-Computer Raspberry Pi zu Hilfe. Mit der Raspi-Fritzbox-Kombination führen Sie Mobilfunkgespräche mit jedem DECT-Telefon sogar im Keller, fernab von allen Mobilfunksignalen oder schützen Ihr ganzes Netz mit einem Adblocker vor in Anzeigen versteckter Malware.



Dušan Živadinović



Inhalt



HEIMNETZ ABSICHERN

Fritzboxen lassen sich dank vieler ab Werk eingebauter Funktionen leicht absichern. Die Grundlage bilden Verschlüsselungen und spezielle Einstellungen. Damit wehren Sie nicht nur Möchtegern-Eindringlinge ab, sondern schützen auch Ihre Privatsphäre.

6 Mehr Privatsphäre mit Fritzboxen
10 Beim Surfen die Privatsphäre schützen
16 DNS-over-TLS: Analyse mit Wireshark
20 Verschlüsseltes DNS für Pi-hole
28 AdGuard Home macht Pi-hole Konkurrenz
36 Raspi 4 als Fertig-VPN-Dongle
40 Fritzboxen sicher betreiben

WLAN AUSREIZEN

Mit Wi-Fi 6 bringen neue Fritzbox-Router und Fritz-Repeater die nächste WLAN-Entwicklungsstufe mit und flankieren sie mit der starken WPA3-Verschlüsselung. Die Vorgänger Wi-Fi 5 und WPA2 schlagen sich noch passabel, müssen aber mit baldiger Ablöse rechnen.

50 6 Router für Wi-Fi 6 im Test
60 Extrasicheres WLAN mit WPA3
66 AVM Fritz-Repeater 6000 mit Wi-Fi 6
68 Wie Wi-Fi 6 das WLAN beschleunigt

OPTIMAL VERNETZEN

Fritzboxen gibt es für alle üblichen Glasfaser-, DSL-, Kabel- und Mobilfunkzugänge. Dabei genügen oft auch die Netzwerk- und Internetdienste eines kleineren Modells, zumal sich alle sogar mit Bordmitteln gegen Internetausfälle absichern lassen.

76 Auswahlhilfe für den Router-Kauf
82 Strategien gegen Internetausfälle
88 Erste Hilfe bei Internetausfällen
94 Funkverlängerung gegen Internetausfall
102 Dateizugriff per SMB
112 DynDNS mit IPv6 leicht gemacht
116 Router für Glasfaser-Anschlüsse
117 Fritzchens Erleuchtung

KOMFORTABEL TELEFONIEREN

Geschäftliche Telefonate sind im Homeoffice unerlässlich. Dabei unterstützt eine Fritzbox vielfältig und nimmt mit ihrer Verschlüsselung eine Sonderstellung ein. Schnurlostelefone koppelt man mühelos an, mit etwas Zureden auch fremde Businesstelefone.

118 Verschlüsselt per VoIP telefonieren
124 Im Homeoffice komfortabel telefonieren
130 Fritzbox für Homeoffice-Telefonie
134 Unify-VoIP-Telefone an der Fritzbox
140 DECT-VoIP-Telefone bis 100 Euro
146 Telefon klingeln lassen mit Fritzconnection
148 Mobilfunk-Gateway



SPAREN MIT DER FRITZBOX

Gebrauchte Fritzboxen sind ein besonderer Spartipp; sie eignen sich für viele Anwendungen und bekommen lange Updates. Alternativ werden sie zum Ersatzrouter oder dienen nach Einzug von OpenWrt als mächtige Ergänzung für verschlüsseltes DNS, VPN & Co.

156 Fritzbox 7412 als Zweitrouter nutzen
160 Fritzbox 7520 ohne Einschränkungen
164 Fritzbox 7412 als OpenWrt-Kompagnon
167 Telefon als Türklingel nutzen
168 Fritzbox 7362 SL mit OpenWrt

ZUM HEFT

3 Editorial
170 Impressum

c't FRITZBOX
Absichern • Erweitern • Tunen

Komfortabel telefonieren
134 Gebrauchte Businesstelefone mit Fritzbox verknüpfen
118 Abhörsicher mit FritzOS telefonieren
148 Funklöcher stopfen mit Fritzbox und Raspi

WLAN ausreizen
68 Wie die Verbesserungen von Wi-Fi 6 wirken
66 Das bringt AVMs erster Repeater für Wi-Fi 6
60 Im Test: Fünf WLAN-Router gegen die Fritzbox
50 Mit WPA3 extrasicher funken

Optimal vernetzen
76 Was für Ihre nächste Fritzbox wichtig ist
112 Fritzbox: DynDNS mit IPv6 leicht gemacht
82 Internetausfällen vorbeugen

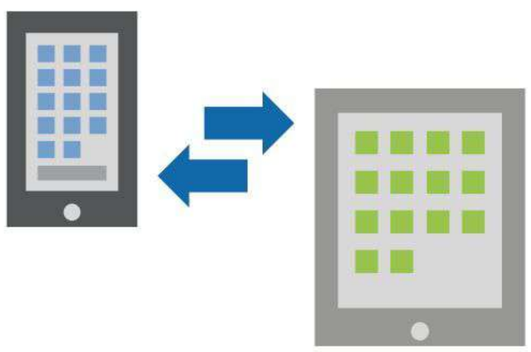
Fritzbox niet- und nagelfest
40, 6, 10 Heimnetz absichern • Tracking verhindern • Privatsphäre schützen
36, 28 VPN trotz Kabelanschluss einrichten • Malware draußen halten

facebook.com/ctspecials



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





facebook.com/ctspecials

Mehr Privatsphäre mit Fritzboxen

Lange Zeit war lediglich bekannt, wie vielfältig die Privatsphäre von Nutzern ausgespäht werden kann. Nun mehren sich aber die Gegenmittel. In aktuellen Fritzboxen lassen sich drei wichtige besonders einfach aktivieren.

Von **Dušan Živadinović**

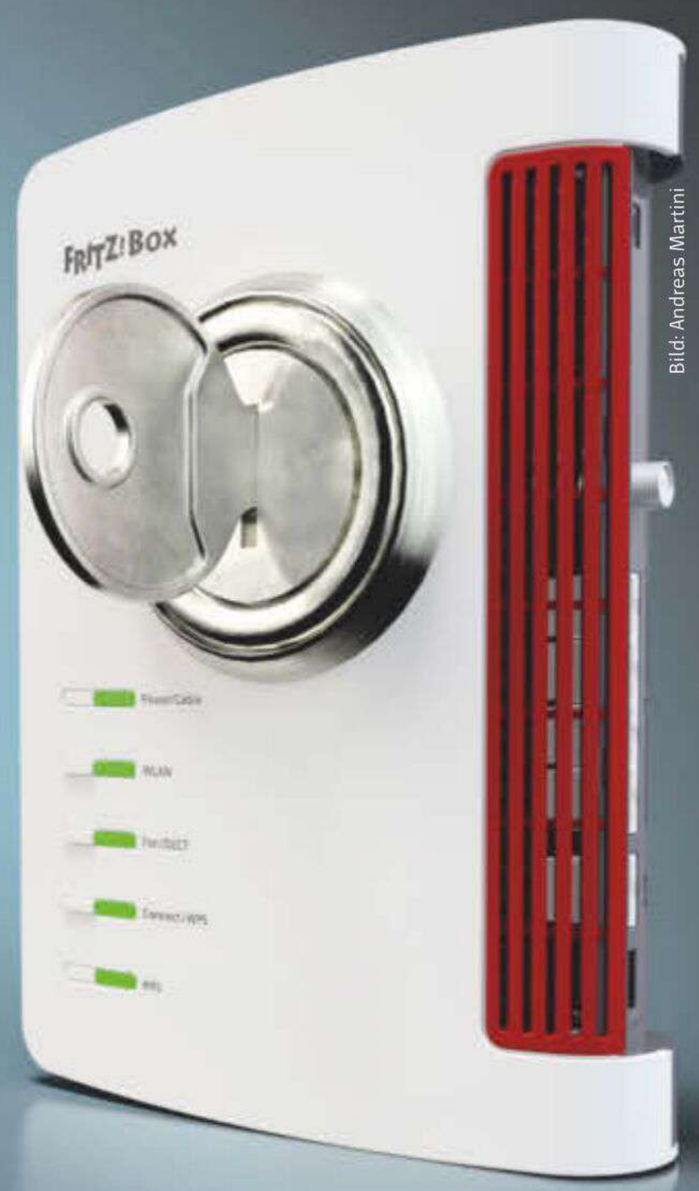


Bild: Andreas Martini

Mehr Privatsphäre mit Fritzboxen	6
Beim Surfen die Privatsphäre schützen	10
DNS-over-TLS: Analyse mit Wireshark	16
Verschlüsseltes DNS für Pi-hole	20
AdGuard Home macht Pi-hole Konkurrenz	28
Raspi 4 als Fertig-VPN-Dongle	36
Fritzboxen sicher betreiben	40

Seine Privatsphäre muss man selbst verteidigen, Konzerne und der Staat haben daran naturgemäß kein Interesse. Das ist soweit nichts Neues. Wie Sie Ihre PCs, Smartphones und andere Geräte ohne viel Aufwand konfigurieren, damit sie einen minimalen Fußabdruck im Internet hinterlassen, haben wir beispielsweise in c't 13/2020 zusammengefasst.

Doch für manche Lücken materialisieren sich die Gegenmittel nur verzögert. Beispielsweise ist die Telefonie per Voice over IP seit jeher ungeschützt. Obwohl erste Verschlüsselungen schon Anfang der 2000er-Jahre spezifiziert worden sind, ließen Provider, Telefon-, Tk-Anlagen- und Routerhersteller sie fast zwei Jahrzehnte lang links liegen. Derweil haben Messenger mit VoIP-Funktion davon profitiert. Signal, Wire, WhatsApp, iMessage und andere verschlüsseln Ende-zu-Ende und der Nutzer muss nicht einen Finger dafür rühren.

VoIP-Telefonie schützen

Höchste Zeit also, dass mit der Telekom ein großer Player im Markt wenigstens eine der vielen Methoden aufgreift und Routerhersteller wie AVM, Lancom oder Bintec-elmeg mitzieht. Denn Messenger sind nicht interoperabel und heute noch weniger verbreitet als Festnetztelefone.

Doch übliche VoIP-Gespräche, die auch grenzüberschreitend laufen können, lassen sich leicht massenhaft abhören, auch von fremden Nachrichtendiensten. Nicht zu vergessen die blank in den Hausverteilern zusammenlaufenden Telefonkabel: An Hausverteilern, die unbeachtet in Kellern stehen oder gar außen an Gebäuden, können Angreifer mit Notebook und DSL-Analysator oft unbehelligt alles mitschneiden, was über die DSL-Leitungen ins Internet geht. Und es soll ja Firmen geben, in denen man sich Passwörter oder auch Kreditkartendaten telefonisch durchgibt.

Die Geräteentwickler haben es allerdings nicht immer leicht, die Spezifikationen zur VoIP-Verschlüsselung umzusetzen. An manchen Stellen sind die Schriften zu knapp oder sie überlassen die genaue Implementierung dem Gespür der Programmierer. Das geht nicht immer gut und so haben wir auch für die Fritzbox Verbesserungsvorschläge. Unterm Strich muss man aber sagen: Der Einstieg in die VoIP-Verschlüsselung ist gelungen, auch wenn der hiesige Branchenprimus AVM zu wünschen übrig gelassen hat. Einzelheiten dazu finden Sie im Beitrag ab Seite 118.

WLAN absichern

Manche Sicherheitstechnik bekommt im Laufe der Zeit Risse. Bei der WLAN-Verschlüsselung kennt man das schon zur Genüge: Mit WEP und WPA sind schon zwei Methoden gekommen und (hoffentlich rückstandslos) gegangen. Nun sollte man für die dritte Methode, das aktuelle WPA2, den Abschied einläuten.

Zwar ist WPA2 nicht so grundlegend löchrig wie die WLAN-Steinzeittechnik WEP: WPA2-geschützte Funknetze lassen sich bisher nur über hartnäckiges Ausprobieren knacken (Brute Force). Aber Hochrechnungen, laut denen ein erwürfeltes 16-stelliges Passwort dem stumpfen Ausprobieren rund 19 Billionen Jahre lang standhalten soll, sind nun mal Hochrechnungen. Zudem gehen sie von aktuellen Methoden und aktueller Hardware aus. Doch WPA2 fehlt der Vertraulichkeitsschutz Perfect Forward Secrecy (PFS). Deshalb muss eine Attacke nicht zur Laufzeit des angegriffenen WLANs abgeschlossen sein, sondern kann auch aufgezeichnete Daten aufdecken. Falls man in einigen Jahren Quanten-Computer darauf ansetzen kann, sind Angreifer vermutlich weit schneller am Ziel als heute prognostiziert.

Je eher Sie also auf das bereits verfügbare WPA3 umsteigen desto besser. Die neue WLAN-Verschlüsselung ist zwar beileibe nicht perfekt. Aber zum Beispiel ist anders als bei WPA2 für jede Passworteingabe ein Wörterbuchangriff nicht möglich.



Stellt man aktuelle Fritzboxen auf das moderne WPA3 um, erhöht das die Sicherheit erheblich. WLAN-Clients, die sich nicht aufrüsten lassen, verwenden dann automatisch WPA2.

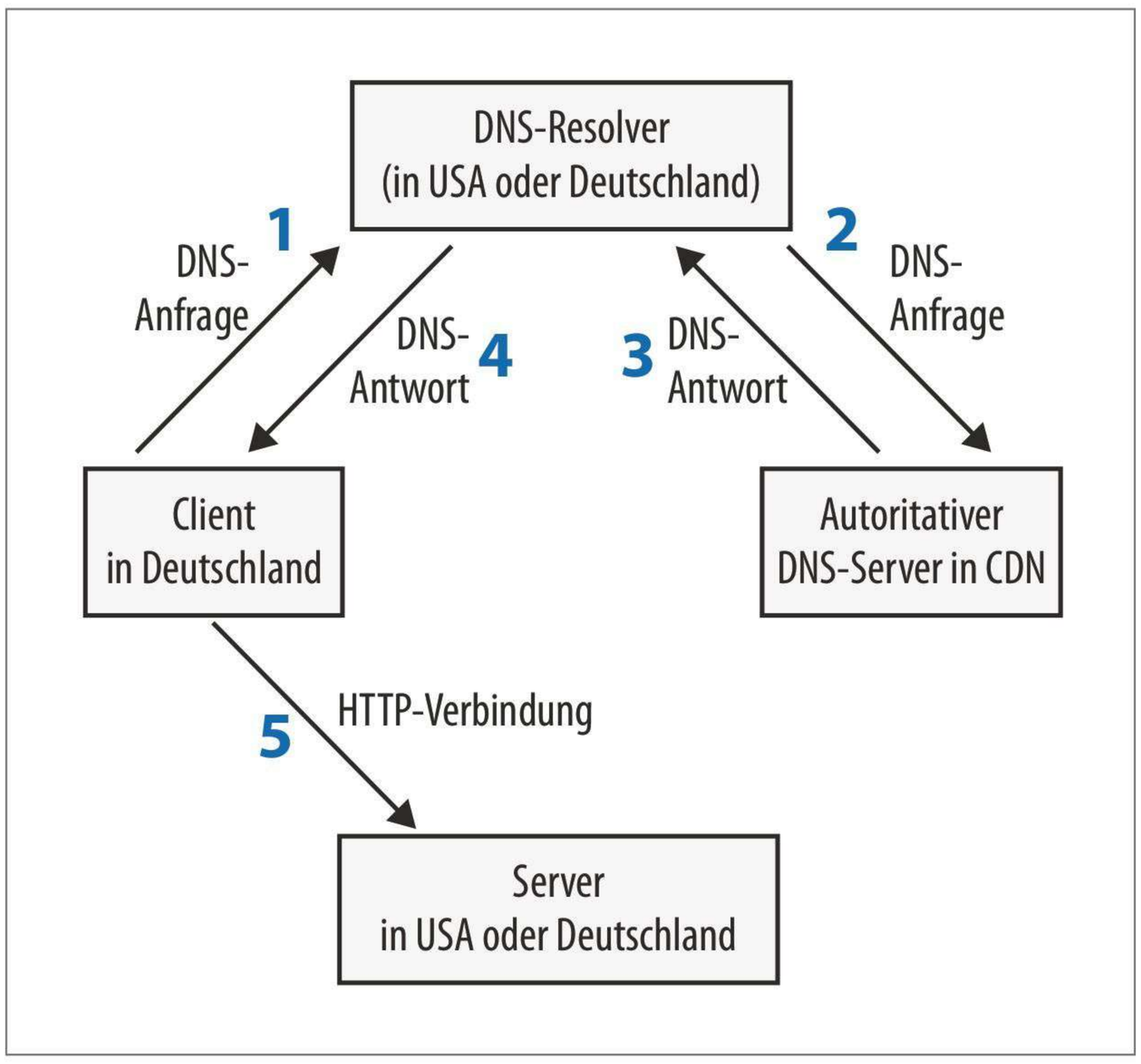
gabe ein neuer Verbindungsversuch erforderlich, sodass sich automatisierte Brute-Force-Angriffe auf eine WLAN-Basis derart in die Länge ziehen, dass sie aussichtslos sind. Zudem werten die Basisstationen zu viele misslungene Einbuchungsversuche als Angriffe und zögern ihre Antworten dann hinaus. Was WPA3 im Detail bringt, wie Sie es in Fritzboxen aktivieren und wie aktuelle Geräte im Test abschneiden, lesen Sie ab Seite 60.

DNS-Leckage stopfen

Für manche Privatsphären-Lecks müssen Gegenmittel komplett neu entwickelt und implementiert werden. Dazu zählt die Verschlüsselung der Kommunikation mit DNS-Resolvern, den „Telefonbüchern des Internet“. Denn alle Geräte sprechen Server im Internet anhand ihrer IP-Adresse an, die sie von Resolvern hauptsächlich im Klartext abfragen. Als die Technik Mitte der 1980er-Jahre entstand, hatte kein Entwickler auf dem Zettel, dass man anhand von DNS-Anfragen Nutzerprofile erstellen könnte. Auch kam später manche DNS-Erweiterung hinzu, die anderen Zwecken dienen sollte, aber nebenbei User-Tracking ermöglicht.

Dazu zählt insbesondere die Methode, mit der Provider die Betreiber von Content Delivery Networks (CDNs) informieren, wo auf der Welt sich der anfragende Client befindet (Geolocation). Damit können sie den Client zum nächstgelegenen Rechenzentrum leiten, was die Paketlaufzeit verkürzt (EDNS0-Option: edns-client-subnet, ECS). Große Content-Anbieter wie Apple, Microsoft oder Netflix nutzen CDNs, um Weitverkehrsstrecken zu entlasten. Daher ist ECS grundsätzlich von Vorteil.

Aber um Kinderschutzfilter zu implementieren, markieren Provider DNS-Anfragen vor der Weiterleitung – und auf den Strecken zu den Root-Servern und zum autoritativen Server können die Anfragen Dritte lesen (zum Beispiel am weltgrößten Inter-



Vom konfigurierten DNS-Resolver hängt wesentlich ab, welches Rechenzentrum etwa einen angefragten Netflix-Stream liefert und damit auch die Länge der Übertragungsstrecke. Leider plappern manche Resolver private Daten aus.

net-Drehkreuz DE-CIX in Frankfurt). Auch dagegen ist erst mal nichts einzuwenden. Man kann zum Markieren Hashes nutzen oder andere Merkmale, die keinem User direkt zugeordnet werden können.

User-Tracking geschenkt

Doch manche Provider nutzen die MAC-Adresse, den Usernamen oder andere Daten, die eine Identifizierung (Fingerprinting) hinter einem Router leicht machen. Wenn Lauscher diese Daten mit dem HTTP(S)-Verkehr korrelieren, sehen sie, welche Seiten Sie sich in der Freizeit ansehen und welche, wenn Sie beruflich aktiv sind.

Anhand solcher tageszeit- und wochentagabhängigen Profile lässt sich ein User sowohl auf Desktop- als auch auf Mobilgeräten identifizieren. So lässt sich grob ableiten, wo sich ein User gerade befindet (zu Hause oder unterwegs). Einzelheiten dazu finden Sie über ct.de/wdd4 im RFC 7626 sowie in einem Vortrag der Sicherheitsspezialistin Sara Dickinson.

Die Internet Engineering Task Force kommentiert die Situation so: Die weitaus meisten Webseiten sind zwar öffentlich (anonyme Alkoholiker, BitTorrent-Tracker, Suchmaschinen, Beratungsseiten etc.), aber die Daten darüber, wer welche Webseiten besucht, sollten weder öffentlich sein noch gesammelt werden können. Daher entwickelte die Organisation Verschlüsselungsmethoden für DNS-Abfragen: DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT). Beide schützen die Privatsphäre nur bis zum Resolver und verhindern den Datenabfluss über die ECS-Technik nicht. Aber wer einen nicht-protokollierenden Resolver nutzt, kann einer Resolver-Petze entgehen. AVM baut in seine Fritzboxen DoT ein. Wie man die Technik aktiviert und wie gut sie im Test funktionierte, lesen Sie ab Seite 10.

Jedoch ist AVM nicht der erste Hersteller, der DoT in Routern integriert. Beispielsweise bringt das Router-Betriebssystem pfSense DoT seit 2018 mit. Auch die Turris-Router der tschechischen Registry CZ.NIC, das freie Routerbetriebssystem OpenWrt und die Firewall-Distribution IPFire können DNS-Anfragen verschlüsseln.

Was DoT nicht macht

DoT ist ein wichtiger Baustein beim Schutz der Privatsphäre, aber nur einer von vielen. Die Technik verschlüsselt nur die Strecke vom Client zum Resolver. Der Resolver löst den Namen der angefragten Domain weiterhin im Klartext auf (er kommuniziert unverschlüsselt mit DNS-Root-Servern und autoritativen Servern).

Wer also den Verkehr eines Resolvers langfristig erfasst, kann im Datenstrom der vielen Nutzer, die diesen Resolver verwenden, vermutlich unterschiedliche Profile erkennen. Fachleute meinen, es sei nicht Privacy-relevant, ob zum Beispiel irgendein Telekom-Kunde die Webseite der Deutschen Aids-Hilfe besuchen wollte. Trotzdem gibt es Pläne, auch die restliche DNS-Kommunikation abzusichern.

DNS-Ratschläge

Über die DNS-Verschlüsselung hinaus hilft eine Handvoll einfacher Faustregeln, die Privatsphäre zu verbessern.

Meiden Sie kommerzielle VPN-Dienste. VPN-Anbieter betreiben eigene DNS-Server, um Kunden den Zugang zu Diensten zu ermöglichen, die ihnen das Geo-Blocking normalerweise vorenthält. Jedoch verrät man dabei seine Internet-Ziele dem VPN-Betreiber. Prinzipiell kann er diese Kenntnisse zu Geld machen, etwa durch Verkauf von Profilen an Werbetreibende.

Welchen DNS-Server Ihr aktuelles Gerät gerade benutzt (Smartphone, PC, Tablet, Smart-TV), verrät beispielsweise die Testseite Browserleaks (siehe ct.de/wdd4). Dort stehen im Bereich „DNS Leak Test“ die IP-Adressen der genutzten DNS-Resolver. Vor allem VPN-Anbieter unterhalten Webdienste zur DNS-Analyse, darunter „DNS leak test“ oder „Perfect Privacy“. Damit lässt sich prüfen, welche DNS-Informationen Streaming-Anbietern wie Netflix vorliegen, um etwa länderspezifische Zugänge zu ihren Videoangeboten durchzusetzen.

Prüfen Sie ab und zu, welchen Resolver Ihre Geräte befragen, denn es gab schon etliche Attacken auf Router, um darin den DNS-Server umzubiegen. Angreifer können so mitlesen, wer was tut oder DNS-Anfragen auf Werbeseiten umlenken, die für sie lukrativ sind – oder gleich Malware wie Erpressungstrojaner in den Browser schleusen.

Um Attacken auf Router möglichst kleine Angriffsflächen zu bieten, halten Sie deren Firmware aktuell. Sichern Sie das Webinterface mit einem individuellen, möglichst langen Passwort aus Groß-, Kleinbuchstaben und Sonderzeichen, schalten Sie Zugriffe aus dem Internet auf das Webinterface ab, nutzen Sie für die Fernwartung ein VPN. Verwenden Sie für das WLAN ein anderes, gleichfalls langes Passwort. Verweisen Sie Geräte von Besuchern ins Gastnetz. Bleibt uns noch eins für Ihre Internet-Surf-Unternehmungen zu wünschen: Mast- und Schotbruch! (dz) c't

Weitere Infos

ct.de/wdd4



Bild: Andreas Martini

Beim Surfen die Privatsphäre schützen

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

Von **Dušan Živadinović**

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

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

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

Internet-Tagebuch verschlüsseln

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

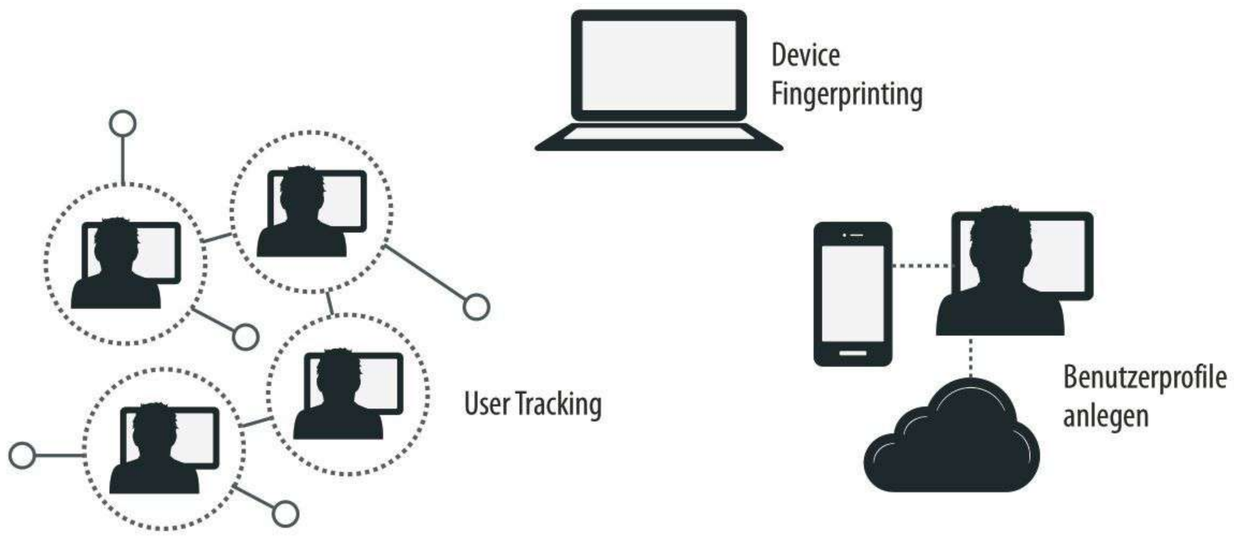
DoT und DoH sind noch junge Spezifikationen, verbreiten sich aber schneller als beispielsweise IPv6. In Smartphones ab Android 9 kann man DoT im Bereich „Private DNS Mode“ einschalten. Der DNS-Resolver in Linux-Systemd (Systemd-Resolved) eignet sich ebenfalls für DoT. Microsoft arbeitet daran, DoH in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

Weil es unpraktisch ist, mehrere Computer und Smartphones einzeln aufzurüsten und aktuell zu halten, richtet man verschlüsselnde DNS-Clients zum Beispiel auf dem DNS-Filter Pi-hole für sein komplettes Netz ein (siehe S. 20 und 28); dann sind auch IoT-Geräte, Medienreceiver, Webcams und sonstige Netzwerkgeräte geschützt, die sich nicht aufrüsten lassen. Einen Pi-hole oder AdGuard Home zu betreiben erfordert allerdings etwas Know-how und Pflegeaufwand. Beides hat AVM in Fritzboxen mit FritzOS 7.2x auf ein Minimum reduziert. Jedoch fehlt der Fritzbox ein Werbeblocker vom Schlage eines Pi-hole oder AdGuard Home.

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

Wie die DNS-Namensauflösung missbraucht werden kann

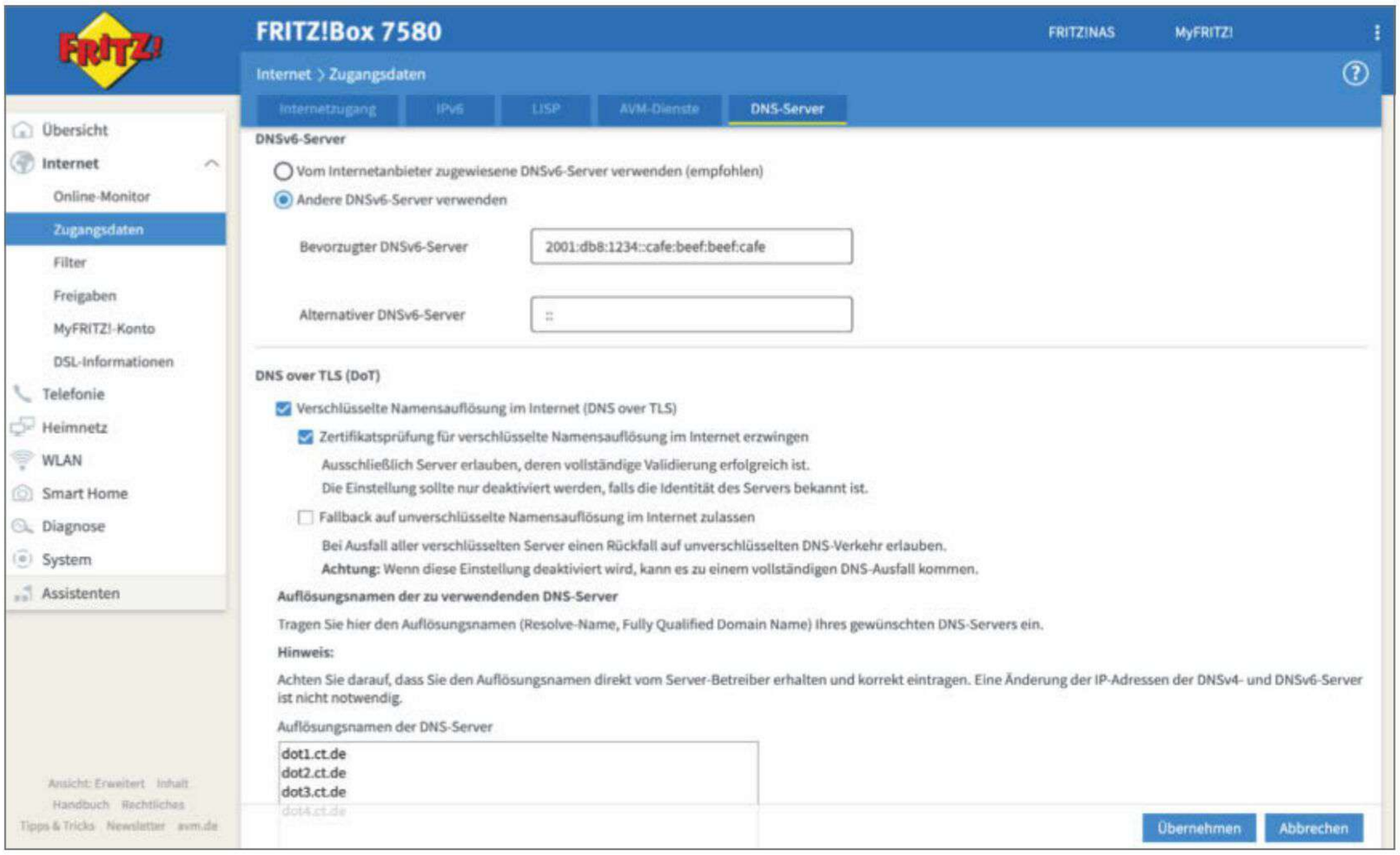
In unverschlüsselten DNS-Anfragen stecken vertrauliche Informationen, die sich vielfältig nutzen lassen, um Nutzerverhalten auszuleuchten.



Zwei DoT-Profile

Das zweite Profil „Opportunistic Privacy Profile“ ist weniger streng: Es gewichtet funktionierende DNS-Auflösung höher als den Privatsphärenschutz. Falls eine authentifizierte und verschlüsselte Verbindung scheitert, nimmt der Client auch mit einem Resolver vorlieb, den er nicht kennt oder der nicht verschlüsselt. Das zweite Profil bietet also begrenzten Schutz vor Spähern und manipulierten DNS-Informationen. AVM hat im aktuellen FritzOS beide DoT-Profile eingebaut.

Vor der Aktivierung der Funktion benötigen Sie mindestens einen, besser mehrere Domainnamen von DoT-Resolvern (zum Beispiel dns.quad9.net).



Einige Mausklicks genügen, um in Fritzboxen verschlüsselte DNS-Anfragen einzuschalten. Längst gibt es nicht nur experimentelle DoT-Resolver wie hier links unten im Screenshot abgebildet, sondern auch öffentlich zugängliche.

Eine Handvoll großer Resolver-Betreiber, darunter Cloudflare und Quad9 bieten öffentliche Namensauflösung via DoT an und validieren die DNS-Informationen auch. Validieren bedeutet: per DNSSEC sicherstellen, dass der Inhalt von DNS-Antworten nicht manipuliert ist und dass die Information ein vertrauenswürdiger Server gesendet hat. Ob Ihr aktueller Resolver DNS-Daten validiert, können Sie etwa mit dem „Connection Test“ auf internet.nl prüfen. Kandidatenlisten für DoT-Resolver finden Sie über ct.de/wvkk.

Die bei seinen Resolvern eingehenden DNS-Anfragen von Nutzern verwendet Cloudflare, um sein Content Distribution Network zu optimieren und Inhalte seiner Großkunden möglichst dort zu platzieren, wo sie oft nachgefragt werden. Wer sein Surf-Protokoll einem amerikanischen Konzern lieber nicht schenken möchte, findet über den Link am Ende des Artikels Listen kleinerer, offener DoT-Server mit „no logging“-Policy, darunter den Bielefelder Anbieter Digitalcourage (dns.digitalcourage.de).

Mal eben einschalten

Wenn Sie Ihre Resolver ausgewählt haben, öffnen Sie im Webinterface der Fritzbox das Menü Internet / Zugangsdaten / DNS-Server. Die Standardeinträge für unverschlüsselte DNS-Anfragen lassen Sie unverändert, damit Sie bei etwaigen DoT-Problemen Ihre ursprüngliche DNS-Konfiguration schnell reaktivieren können.

Setzen Sie im Abschnitt „DNS over TLS“ mindestens die ersten beiden Häkchen („Verschlüsselte Namensauflösung im Internet“ und „Zertifikatsprüfung für verschlüsselte Namensauflösung im Internet erzwingen“). Mit dem ersten aktivieren Sie DoT und mit dem zweiten stellen Sie sicher, dass der weiter unten eingetragene DoT-Resolver anhand seines TLS-Zertifikats authentifiziert wird. Dann können Sie sicher sein, dass tatsächlich der Resolver befragt wird, den Sie eingetragen haben (Strict Privacy Profile).

AVM merkt unter den zweiten Punkt an: „Die Einstellung sollte nur deaktiviert werden, falls die Identität des Servers bekannt ist.“ Das ist ein wenig zu knapp beschrieben. Gemeint ist: Wenn Sie einen DoT-Resolver nutzen, der nur ein selbstsigniertes Zertifikat liefert, dann lässt er sich nicht authentifizieren. Damit die Fritzbox auch diesen Resolver akzeptiert, muss der Haken weg.

Es ist empfehlenswert, mehrere Resolver zu verwenden, falls mal einer ausfällt. Auf Anfrage er-

klärte AVM, dass die Fritzbox die Wahl des „besten“ Servers anhand des Validierungsstatus und der Latenz trifft. Bei der Validierung prüft die Box die Zertifikatskette und die im Serverzertifikat eingetragenen Werte wie die IP-Adresse oder den DNS-Namen (Subject-Alternative-Name). Anschließend sortiert sie die Resolver nach absteigendem Validierungsstatus. Haben zwei oder mehr denselben Status, zieht die Box den Resolver mit der kürzesten Latenz vor.

Eigentlich möchte man Anfragen an mehrere Resolver streuen, um die Profilerstellung zu erschweren. Das sei aktuell aber nicht geplant, antwortete AVM auf Anfrage.

Nachteilig ist, dass die Box in der Resolverliste ausschließlich Domainnamen akzeptiert. So ist schon für die Verbindungsaufnahme eine erfolgreiche herkömmliche DNS-Auflösung nötig. Besser wäre eine Tabelle mit IP-Adressen und Domainnamen oder wenigstens wählbare Resolver für die DNS-Auflösung der verschlüsselnden Resolver (Bootstrap DNS-Resolver).

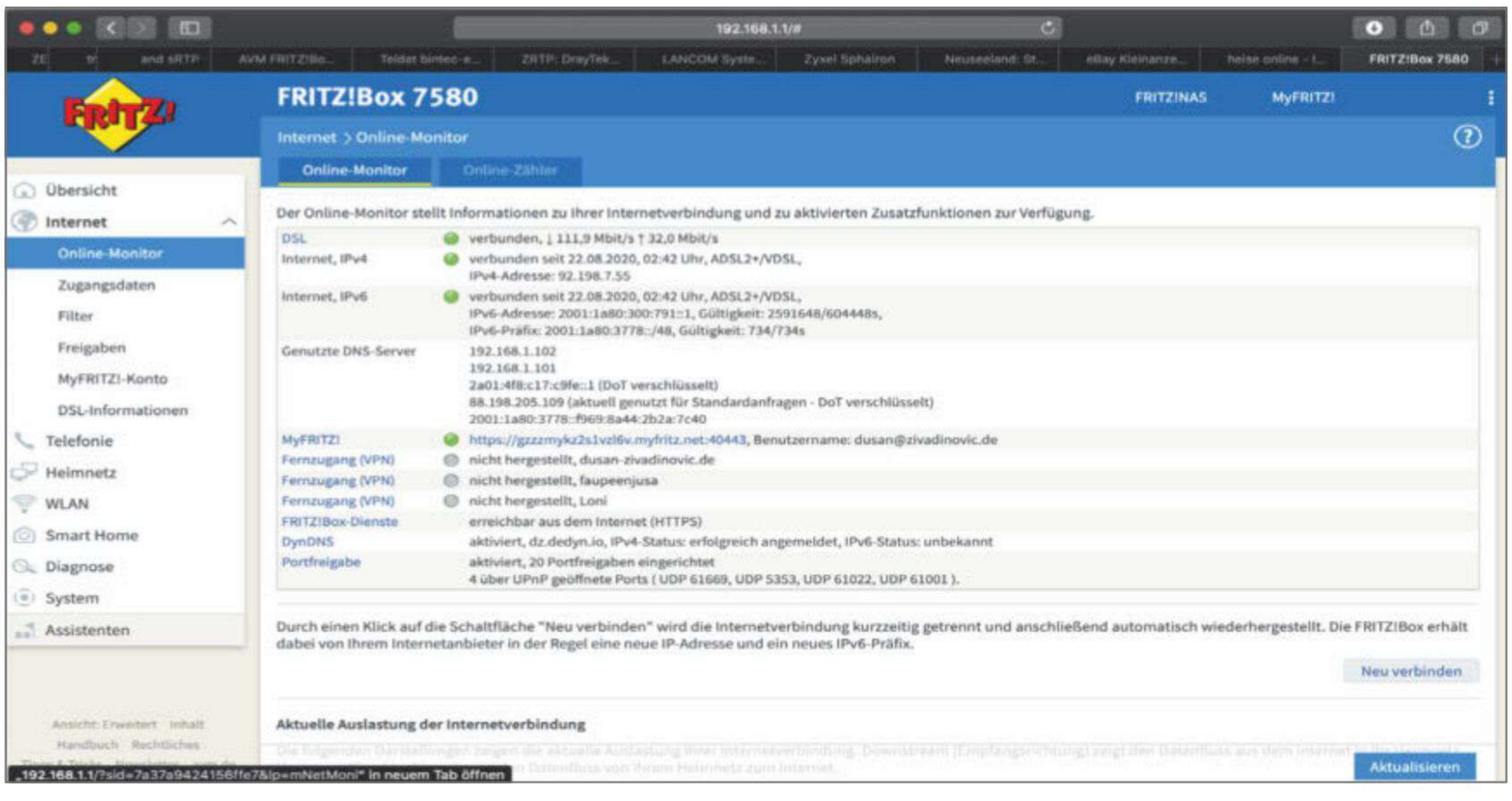
Mit der Option „Fallback auf unverschlüsselte Namensauflösung im Internet zulassen“ hat AVM das zweite DoT-Profil implementiert, das Opportunistic Privacy Profile. Schaltet man es ein, sendet die Box Klartext-DNS-Anfragen an einen der weiter oben eingetragenen Resolver, falls die Kommunikation mit dem DoT-Resolver scheitert. In sicherheitskritischen Bereichen sollte man diese Option nicht nutzen, denn Angreifer, die die DoT-Aushandlung blockieren, erzwingen unverschlüsselten DNS-Verkehr.

Wenn Sie Ihre Auswahl getroffen haben, speichern Sie die Änderungen mit „Übernehmen“ und legen Sie anschließend ein Backup der Fritzbox-Konfiguration auf Ihrem PC an (System / Sicherung / Sichern).

Dinge bedenken

Im Menü Internet / Online-Monitor sollten alle konfigurierten Resolver zu sehen sein (Genutzte DNS-Server). Zum neu eingerichteten DoT-Resolver sollte dort stehen: „aktuell genutzt für Standardanfragen - DoT verschlüsselt“.

Nun können Sie wie üblich surfen. Die netzinterne DNS-Auflösung, etwa für Ihre Drucker oder Dateiserver, funktioniert wie zuvor. Es gibt jedoch einige Dinge zu bedenken: Der DoT-Client kommuniziert standardmäßig über den TCP-Port 853. Somit können etwa Provider oder auch Angreifer den DoT-Verkehr leicht per Firewall-Regel unterbinden. Aktuell kennen wir für Deutschland zwar keinen solchen Fall, aber manche Staaten sperren Internetzugriffe anhand von DNS-Verkehrsanalysen, sodass sie DoT blockieren, um Klartext-DNS zu erzwingen. Russland plant ein Gesetz, das unter anderem DoT und TLS 1.3 verbietet.



In Fritzboxen lassen sich mehrere DNS-Resolver (DNS-Server) konfigurieren. Im Monitorbereich kann man nachschlagen, welcher gerade in Verwendung ist.

Prinzipiell kann man DoT-Clients und -Resolver auch auf anderen Ports betreiben, beispielsweise auf Port 443, der normalerweise HTTPS-Verkehr vorbehalten ist. DoT und HTTPS lassen sich nur mit erheblichem Aufwand und damit teuer unterscheiden (Deep Packet Inspection), sodass DoT auf Port 443 nicht blockiert wird.

Leider kann man in der Fritzbox den Zielport nicht einstellen und es gibt kaum DoT-Resolver, die über Port 443 ansprechbar sind. Ein Beispiel ist dns.cmrg.net, den Daniel Kahn Gillmor betreibt, der Entwickler des zugehörigen Multiplexers hddmux für HTTPS und DoT. Unterm Strich bedeutet das: Sollte der DoT-Verkehr einer Fritzbox providerseitig gesperrt sein, muss man sie auf Klartext-DNS zurückstellen. Wer weiterhin eine DNS-Verschlüsselung benötigt, kann ersatzweise einen eigenen DoH-Server auf einer Linux-Maschine einrichten.

Auch DoT-Server können ausfallen. Es gibt aber Webseiten, die darüber informieren, ob einer der dort erfassten Server läuft oder nicht (siehe ct.de/wvkk). Ist dort ein Eintrag grün markiert und er für Sie dennoch nicht erreichbar, blockiert vermutlich eine Firewall die Kommunikation – wenn Sie dieses Verhalten auch mit anderen Servern beobachten, ist das ein Beleg für einen DoT-Filter.

Geheimnisse und Schwächen

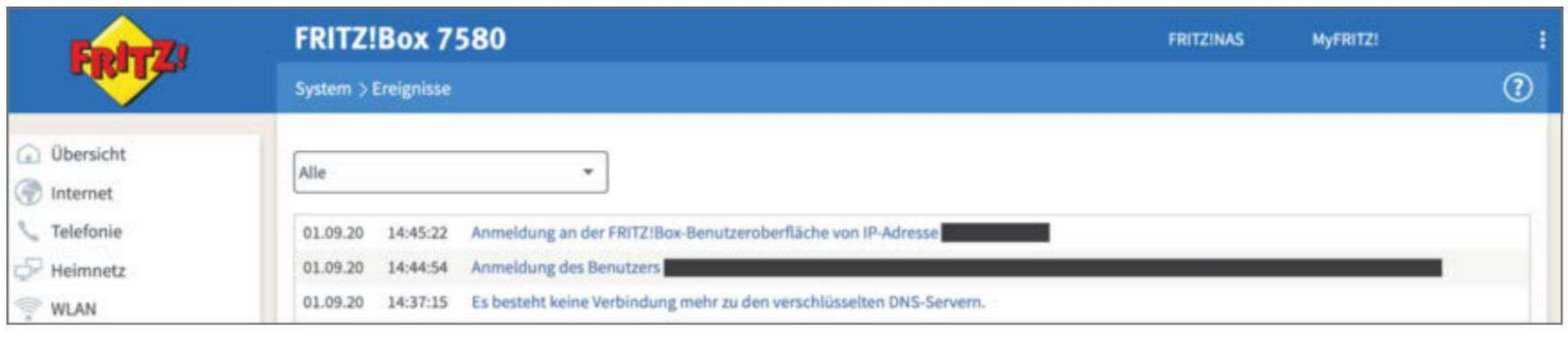
DoT-Clients verschlüsseln den Verkehr per TLS und müssen dafür das Transmission Control Protocol nutzen (TCP). Beide zusammen, TCP und TLS, erfordern etwas mehr Zeit für den Verbindungsaufbau als unverschlüsselter DNS-Verkehr, der über das schlanke User Datagram Protocol abläuft (UDP). Als Faustregel gilt aber: Je schneller die DNS-Auflösung, desto schneller der Aufbau von komplexen Webseiten, weil dafür besonders viele DNS-Anfragen erforderlich sind.

Deshalb versuchen DoT-Clients über eine einmal geöffnete TLS-Verbindung mehrere DNS-Abfragen abzuwickeln. Mit TLS-Version 1.2 verbleiben dennoch messbare Einbußen. Erst TLS 1.3 bringt Optimierungen mit, die DoT nahe an die Geschwindigkeit des klassischen DNS heranbringen (0-RTT, asynchrone Kanäle, TCP Fast Open, TCP Connection Re-Use, Pipelining).

Ob auch die Fritzbox davon Gebrauch macht, lässt sich noch nicht sagen. Zwar zeigen unsere Protokollanalysen, dass sie schon TLS 1.3 und den Verschlüsselungsschutz Perfect Forward Secrecy (PFS) nutzt; beides ist vorbildlich. Doch wenn PFS aktiviert ist, kann man den TLS-Verkehr selbst dann nicht entschlüsseln, wenn man den Server-Key besitzt; man braucht zusätzlich die Session-Keys des Clients. Diese lässt sich die Fritzbox bisher nicht entlocken.

Kurzer Servertest

Die Fritzbox notiert im Menü System/Ereignisse, falls es bei der DoT-Kommunikation mal knirscht. In unserem mehrmonatigen Testzeitraum mit eigenem DoT-Server ist das nur zwei Mal vorgekommen. Aus dem Eintrag im Fritzbox-Journal geht die Fehlerursache aber nicht hervor (Client-Fehler, Port-Blockade oder Server-Fehler). Um Licht ins Dunkel zu bringen, kann man die konfigurierten DoT-Server auf einem PC mit dem Tool `kdig` befragen. Auf gängigen Linux-Distributionen gehört `kdig` zu den Paketen Knot-Resolver und Knot-Server; beide gibt es auch für Macs. Den Knot-Resolver kann man über den macOS-Paketmanager Homebrew beziehen und den Knot-Server über den Paket-Manager MacPorts. Ein Beispielbefehl sieht so aus:



Wenn „das Internet kaputt“ ist, schaut man im Log der Fritzbox nach (System/Ereignisse). In seltenen Fällen kann das Symptom nämlich auch ein ausgefallener DNS-Server (Resolver) bewirken.

```
kdig @dns.digitalcourage.de ct.de +tls
```

Damit befragt `kdig` den Resolver von Digitalcourage nach der IP-Adresse der Domain ct.de. Mit der Option `+tls` lässt man sich Einzelheiten über die Verschlüsselung anzeigen. In der Ausgabe steht dann beispielsweise „TLS 1.3“, wenn `kdig` eine solche Verbindung aufgebaut hat. Darunter folgt die IP-Adresse der angefragten Domain (193.99.144.80).

Verkehrsanalyse

Um zu prüfen, ob die Fritzbox DNS-Anfragen tatsächlich verschlüsselt, ist mehr Aufwand erforderlich. Trennen Sie zunächst alle Geräte bis auf einen PC von der Fritzbox, damit Sie nur den DNS-Verkehr der Fritzbox aufzeichnen. Andernfalls können zum Beispiel Smart-TVs oder IoT-Geräte Verwirrung stiften, wenn sie direkt mit Resolvern kommunizieren.

Schalten Sie die Verkehrsaufzeichnung in der Fritzbox ein (über fritz.box/support.lua im Abschnitt Paketmitschnitte), surfen Sie mit dem PC einige Webseiten an und stoppen Sie die Aufzeichnung. Nun können Sie die übrigen Netzwerkgeräte wieder anschließen. Öffnen Sie das von der Fritzbox an den PC geschickte PCAP-File im Protokollanalysator Wireshark und dort im Menü Statistics die Option DNS. Dann öffnet Wireshark ein Fenster mit diversen Einzelheiten. In der ersten Spalte sind Rubriken wie „Total packets“, „Service Stats“ und „Query Stats“ aufgeführt. In der Spalte Count steht die Anzahl der Pakete zur jeweiligen Rubrik. Wenn in der gesamten Count-Spalte nur Nullen stehen, hat die Fritzbox keine Klartext-DNS-Anfragen verschickt – also ausschließlich DoT genutzt.

Weitere Infos

ct.de/wvkk

Um zu prüfen, wie die Fritzbox auf Resolver-Ausfälle reagiert, haben wir das mit einem eigenen DoT-Resolver simuliert. Clients, die auf die DNS-Auflösung der Fritzbox angewiesen waren, konnten dann keine Webseiten öffnen. Leider lieferte die Box in dieser Testreihe auch nach zehn Minuten keine DoT-Fehlermeldung (FritzOS 7.20 auf Fritzbox 7590). Im realen Einsatz erschwert das die Fehlersuche. Nach Reaktivieren des DoT-Resolvers klappte die Auflösung über die Fritzbox nicht umgehend wieder. Erst nachdem wir DoT kurz aus- und wieder einschalteten, funktionierte die sichere Namensauflösung.

Seit den ersten Versionen hat AVM aber an seiner DoT-Implementierung gefeilt und ab FritzOS 7.25 einiges verbessert. Im Log notiert die Box zuverlässiger: „Es besteht keine Verbindung mehr zu den verschlüsselten DNS-Servern“, wenn die Kommunikation scheitert. Schrittweise hat AVM auch die Robustheit verbessert. Ebenfalls ab FritzOS 7.25 gibt der DoT-Client nicht mehr auf, wenn der DoT-Resolver vorübergehend wegen Überlastung nicht erreichbar war, sondern stellt die Verbindung wieder her, sobald möglich.

Fazit

Unterm Strich konnte die DoT-Implementierung der Berliner im Dauertest weitgehend überzeugen, zumal nach dem sehr einfachen Einschalten das gesamte (W)LAN mit einem Schlag von den verschlüsselten DNS-Anfragen profitiert. Diese Technik in Fritzboxen zu haben, ist ein Gewinn. Weitere kommerzielle Routerhersteller sollten das als Ansporn nehmen und nachziehen. (dz) c't

Make:
KREATIV MIT TECHNIK

DAS KANNST DU AUCH!





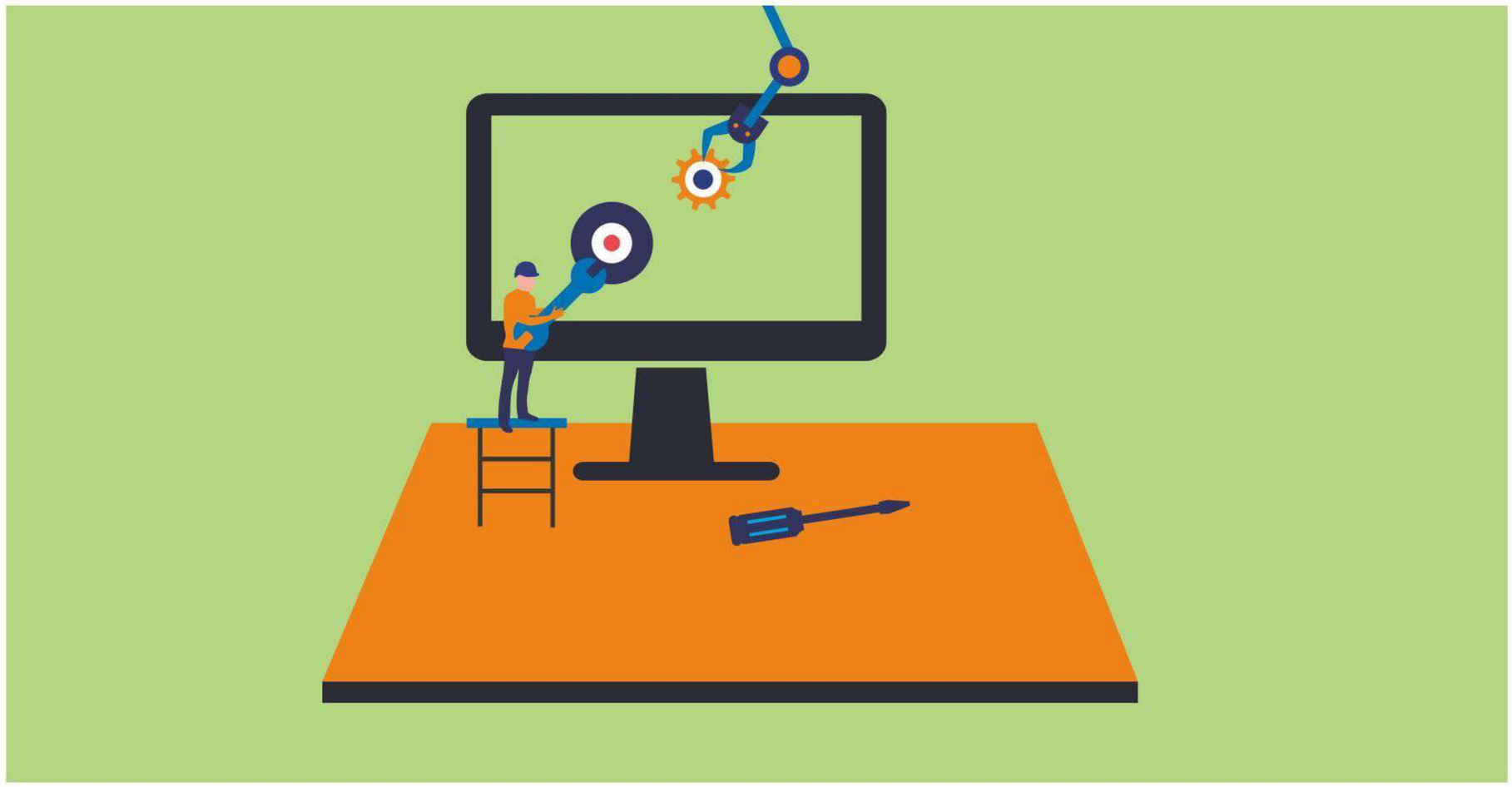
2 × Make testen
und 6 € sparen!

Ihre Vorteile:
- ✓ **GRATIS dazu:** Arduino Nano
- ✓ **Zugriff auf Online-Artikel-Archiv***
- ✓ **NEU:** Jetzt auch im Browser lesen!
- ✓ Zusätzlich digital über iOS oder Android lesen

Für nur 15,60 Euro statt 21,80 Euro.

* Für die Laufzeit des Angebotes.

Jetzt bestellen:
make-magazin.de/miniabo



DNS-over-TLS: Analyse mit Wireshark

Fritzboxen können ihren DNS-Verkehr neuerdings verschlüsseln und so helfen, die Privatsphäre aller Nutzer im Netzwerk zu schützen. Aber was genau passiert auf Ebene der Datenpakete? Aufschluss gibt eine Untersuchung mit dem Analysewerkzeug Wireshark.

Von **Jasper Bongertz**

Alle Geräte, die Internet-fähig sind, ermitteln mit DNS-Anfragen die IP-Adressen von Servern, um diese ansprechen zu können. Das ist etwa der Fall, wenn ein Browser die Domain ct.de ansteuert – der konfigurierte DNS-Resolver, meist der des Providers, liefert dann die IP-Adresse 193.99.144.80. Diese ruft dann der Browser auf, um eine HTTP-Verbindung zum Server aufzubauen. Weil die Geräte solche Anfragen unverschlüsselt und täglich vielfach an Resolver versenden, können fremde Nachrichtendienste oder Spione Profile von Nutzern erstellen.

DNS-over-TLS (DoT) gehört zu den Protokollen, die das unterbinden. Ein DoT-Client baut zunächst eine TLS-verschlüsselte Verbindung zum konfigurierten DoT-Resolver auf und kommuniziert mit diesem durch den TLS-Tunnel. Das ist auch bei Fritzboxen der Fall; sie schützen damit alle daran angekoppelten WLAN- und LAN-Clients. Auf Seite 10 haben wir ausführlich über Einrichtung, Monitoring und Testergebnisse mit FritzOS 7.2x berichtet.

Um genauer zu untersuchen, wie die Fritzbox bei der DoT-Kommunikation vorgeht, schaut man sich üblicherweise Paketmitschnitte an. Aufzeichnungen

ihres Internetverkehrs liefert die Box praktischerweise selbst, sofern es sich nicht um ein Provider-Modell von Vodafone oder anderen handelt (fritz.box/support.lua, Abschnitt „Paketmitschnitte“). Sie kopiert den Datenfluss der gewählten Schnittstelle zum Browser, der sie am Ende auf dem lokalen PC als PCAP-Datei speichert (z. B. fritzbox-vcc0_31.09.20_1824.pcap). Ist Wireshark installiert, genügt ein Doppelklick auf diese Datei, um sie zu öffnen.

Wir kommentieren im Weiteren einen Mitschnitt, den wir anlässlich eines Tests für den Beitrag auf Seite 10 angelegt haben. Die Fritzbox kommuniziert dabei mit dem für DoT eingerichteten DNS-Server Unbound. Für DoT-verschlüsselte Anfragen nutzt sie ausschließlich den dafür reservierten TCP-Port 853. Das kann man sich zunutze machen, um in Wireshark anhand eines Display-Filters allen übrigen Verkehr auszublenden (`tcp.port == 853`).

Eine der spannendsten Fragen rund um die Fritzbox und DoT ist: Welche TLS-Version verwendet sie? TLS 1.3 wäre wünschenswert, weil nur diese Version ein Chiffrat erzeugt, das Angreifer auch dann nicht dechiffrieren können, wenn sie den Schlüssel des Servers erbeuten. Das verhindert TLS 1.3 mit der Methode Perfect Forward Secrecy (PFS), bei der Client und Server geheime Sitzungsschlüssel aushandeln. Der für den Test verwendete Unbound-Server eignet sich jedenfalls für das moderne TLS 1.3 und das ältere 1.2.

Auf den ersten Blick sieht in Wireshark alles wie erwartet aus: Klickt man zum Beispiel auf das Paket „Client Hello“, führt Wireshark in der Spalte Protocol TLS 1.3 auf.

Versions-Entwirrung

Sieht man sich den Inhalt des Client Hello genauer an, findet man aber widersprüchliche Angaben. In der Schicht „Transport Layer Security“ steht im Versionsfeld „TLS 1.0“ und weiter unten, im Bereich „Handshake-Protokoll“ immerhin schon „TLS 1.2“.

Diese Widersprüche gehen auf ältere TLS-Server mit unvollständig implementierten Protokollaushandlungen zurück. Um diese zu kompensieren, werden einige Felder, in denen der Client TLS-Versionen aufführt, mit festgelegten Inhalten befüllt (siehe RFC 8446 in ct.de/wpse).

So wird das erste Versionsfeld der Schicht „Transport Layer Security“ nicht für TLS 1.3 genutzt. Stattdessen dürfen Clients dort nur TLS 1.0 oder TLS 1.2 eintragen (0x301 oder 0x0303). Im „Handshake Protocol“ muss das Versionsfeld grundsätzlich 0x0303 ent-

```
> Frame 15: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)
> Ethernet II, Src: JuniperN_51:69:ca (3c:61:04:51:69:ca), Dst: AVMAudio_65:39:c7 (e0:28:6d:65:39:c7)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 7
> PPP-over-Ethernet Session
> Point-to-Point Protocol
> Internet Protocol Version 6, Src: 2a01:4f8:c17:c9fe::1 (2a01:4f8:c17:c9fe::1), Dst: p200300c08fff2109e2286dfffe6539c3.dip0.t-ipconnect.de (2003:c0:8fff:2109:e228:6dff:fe65:39c3)
> Transmission Control Protocol, Src Port: 853, Dst Port: 46777, Seq: 655410809, Ack: 641459401, Len: 1420
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: 0427140157e63713f10c58f2fc9c636d4aa376dae7fbbb36…
        Session ID Length: 32
        Session ID: 06c6daa410b1ef34e50a5ce7d2dc962d6427bd2cdcb4c32d…
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 46
      v Extension: supported_versions (len=2)
          Type: supported_versions (43)
          Length: 2
          Supported Version: TLS 1.3 (0x0304)
      v Extension: key_share (len=36)
          Type: key_share (51)
          Length: 36
        > Key Share extension
  > TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  > TLSv1.3 Record Layer: Application Data Protocol: dns
```

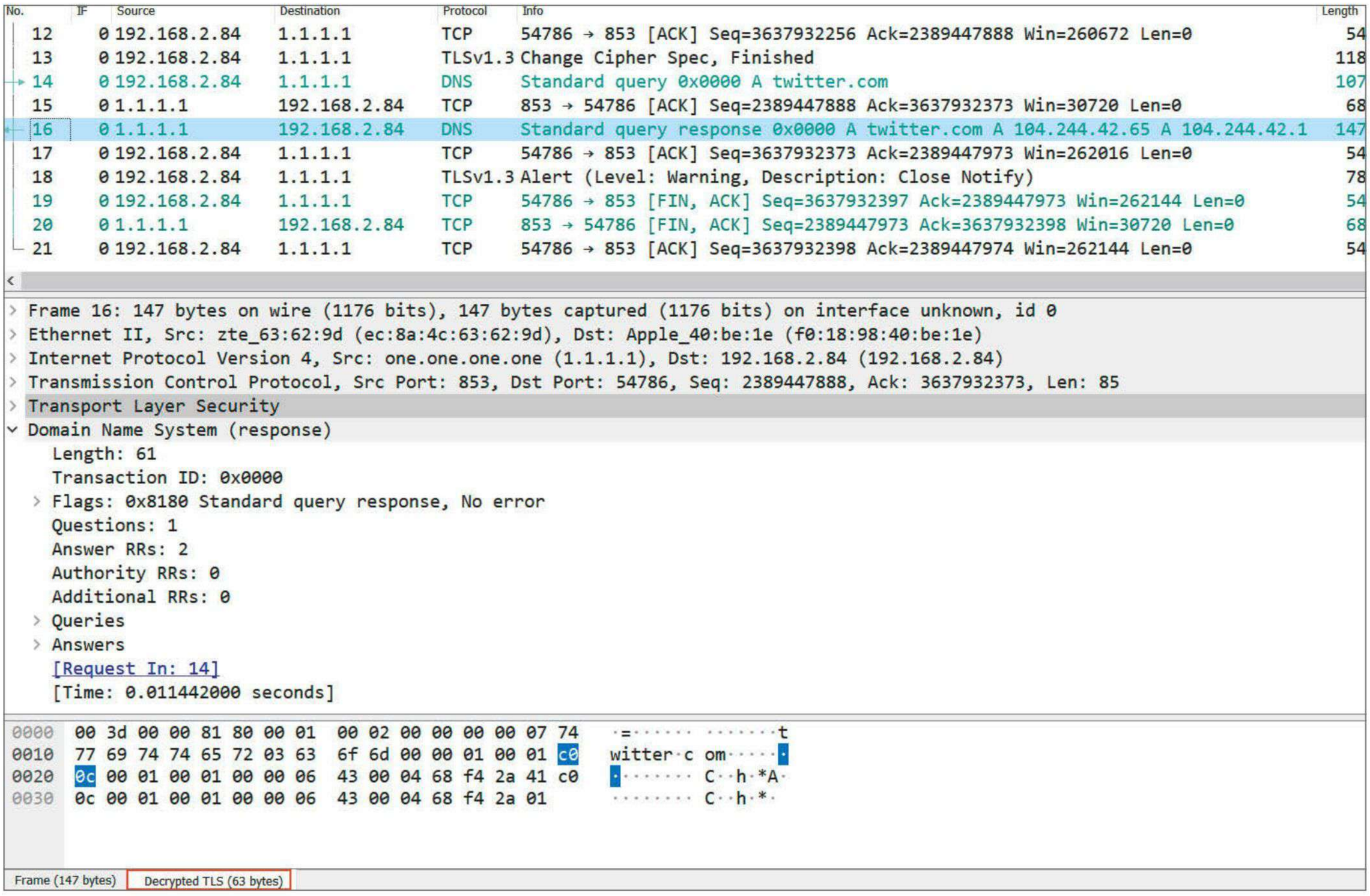
Auf den ersten Blick ist unklar, welche TLS-Version die Fritzbox für DNS-over-TLS verwendet. Tatsächlich wertet der Server aber nur eine von insgesamt drei Angaben des Clients aus.

halten. Für die tatsächliche Aushandlung nutzt der Client das erst später folgende Extension-Feld „supported_versions“. Dort können mehrere Versionen angegeben sein; für „TLS 1.3“ muss dort `0x0304` stehen.

Der Server meldet in seinem „Server Hello“-Paket im Versionsfeld ebenfalls provisorisch `0x0303` (TLS 1.2). Erst im Extension-Feld „supported_versions“ gibt er die Version an, die er verwenden möchte. Die Fritzbox hat im Client-Hello TLS 1.3 und 1.2 zur Wahl gestellt, der Server hat sich für TLS 1.3 entschieden (`0x0304`).

Ein Knoten bleibt noch zu entwirren, denn Wireshark führt in der Protokollspalte des Client-Hello durchaus schon TLSv1.3 an, obwohl zu diesem Zeitpunkt des Verbindungsaufbaus noch offen ist, welche Version der Server wählen wird. Deshalb müsste dort „TLSv1“ stehen. Dieser Widerspruch erklärt sich daraus, dass Wireshark die Spalteninhalte erst darstellt, nachdem es alle Pakete eines Mitschnitts bereits analysiert hat – dann weiß Wireshark schon, worauf sich die beiden Partner verständigt haben und führt das gleich so auf.

Wer sich vom korrekten Inhalt des Client-Hello-Pakets überzeugen will, kann das PCAP-File mit dem Kommandozeilen-Werkzeug `tshark` untersuchen. Wenn man nicht möchte, dass `tshark` die Datei so wie Wireshark analysiert, lässt man beim Aufruf einfach den sonst üblichen Parameter `-2` weg. Dann findet man im Client Hello (hier das Paket mit der laufenden Nummer 12) tatsächlich TLSv1:



So könnte ein entschlüsselter Mitschnitt der Fritzbox aussehen. Aber bisher behält sie die dafür erforderlichen TLS-Secrets für sich, sodass man für den Einstieg in die DoT-Analyse einen speziell modifizierten Linux-Client nutzt.

```
12 1.980112 2003:c0:8fff:2109:e228:↵
↳6dff:fe65:39c3 - 2a01:4f8:c17:c9fe:↵
↳:1 TLSv1 615 Client Hello
```

PFS oder nicht?

Im selben Paket führt der Client auch die Chiffren (Cipher Suites) auf, die er beherrscht. Die Fritzbox nennt hier insgesamt sogar 31 Chiffren. Alle, die die Kürzel „ECDHE“ oder „DHE“ enthalten, werden für Perfect Forward Secrecy verwendet.

Aus dem Chiffrenangebot wählt der Server einen Eintrag und teilt ihn im Paket „Server Hello“ mit. Im hier analysierten Mitschnitt hat Unbound „TLS_AES_128_GCM_SHA256“ gewählt. Das verwundert, denn es handelt sich nicht offensichtlich um eine PFS-Chiffre, obwohl für TLS 1.3 PFS verpflichtend ist. Die Auflösung lautet: In diesem Fall handeln Client und Server die Einzelheiten über den ebenfalls für die PFS-Aushandlung erlaubten Parameter „key_share“ aus.

Entschlüsselung abgewehrt

Weiter kann man in Wireshark anhand der Abfolge und der Paketgrößen grob rückschließen, in welchen Paketen sich DNS-Anfragen verbergen müssten. Denn diese haben eine TCP-Nutzlast größer Null und sind von der Client-IP aus versendet worden. Die Antwort liefert dann die Server-IP.

Aber um mehr zu sehen – etwa, ob ein Client einen TLS-Tunnel mehrfach nutzt, um die Antwortzeiten zu verkürzen –, müsste man die TLS-1.3-Verbindung entschlüsseln. Prinzipiell geht das, wenn man Wireshark die Session Keys mitgibt (TLS-Secrets). Speziell konfigurierte Clients können diese in Dateien ablegen. Ein solches Verfahren ist seit längerem schon für Browser wie Chrome erhältlich (siehe ct.de/wpse). Für DoT-Clients ist das noch die absolute Ausnahme und für Fritzboxen zumindest außerhalb der Labore des Herstellers bisher nicht erhältlich.

Mitschnitt und TLS-Analyse-Infos

ct.de/wpse

Ein PCAP zum Üben

Jedoch hat sich mit dem Thema DNS-over-TLS auch Wireshark-Core-Developer Peter Wu beschäftigt, genauer: Mit dem Linux-Client systemd-resolved, der sich ebenfalls für DoT eignet. Wu hat den Client so modifiziert, dass dieser die Keys exportiert und uns freundlicherweise einen Mitschnitt zur Verfügung gestellt, der sich für Übungszwecke eignet.

Für die weitere Analyse muss der Mitschnitt mit den Keys ergänzt werden. Wir haben sie mit dem Wireshark-Befehl `editcap inject-secrets` in einen dafür vorgesehen Datenblock der PCAP-Datei geschrieben. So entschlüsselt Wireshark die Pakete automatisch und zeigt die DNS-Anfragen und -Antworten im Klartext an.

Damit sind im Trace von Wu tatsächlich entschlüsselte DNS-Pakete zu sehen (14 und 16) und unterhalb der Bytes-Ansicht findet man den zusätzlichen Reiter „Decrypted TLS“: Der Client sendet eine DNS-Anfrage für die Domain twitter.com an einen Resolver von Cloudflare (1.1.1.1). Mit dem Paket 16 erhält er die Antwort mit den IP-Adressen. Das ist nicht gerade viel, aber wer erste Gehversuche mit DoT, TLS 1.3 und PFS unternehmen will, kann das als Einstieg nutzen. Sie finden den Mitschnitt mitsamt den Keys und diversen weiterführenden Infos über den c't-Link. (dz) c't



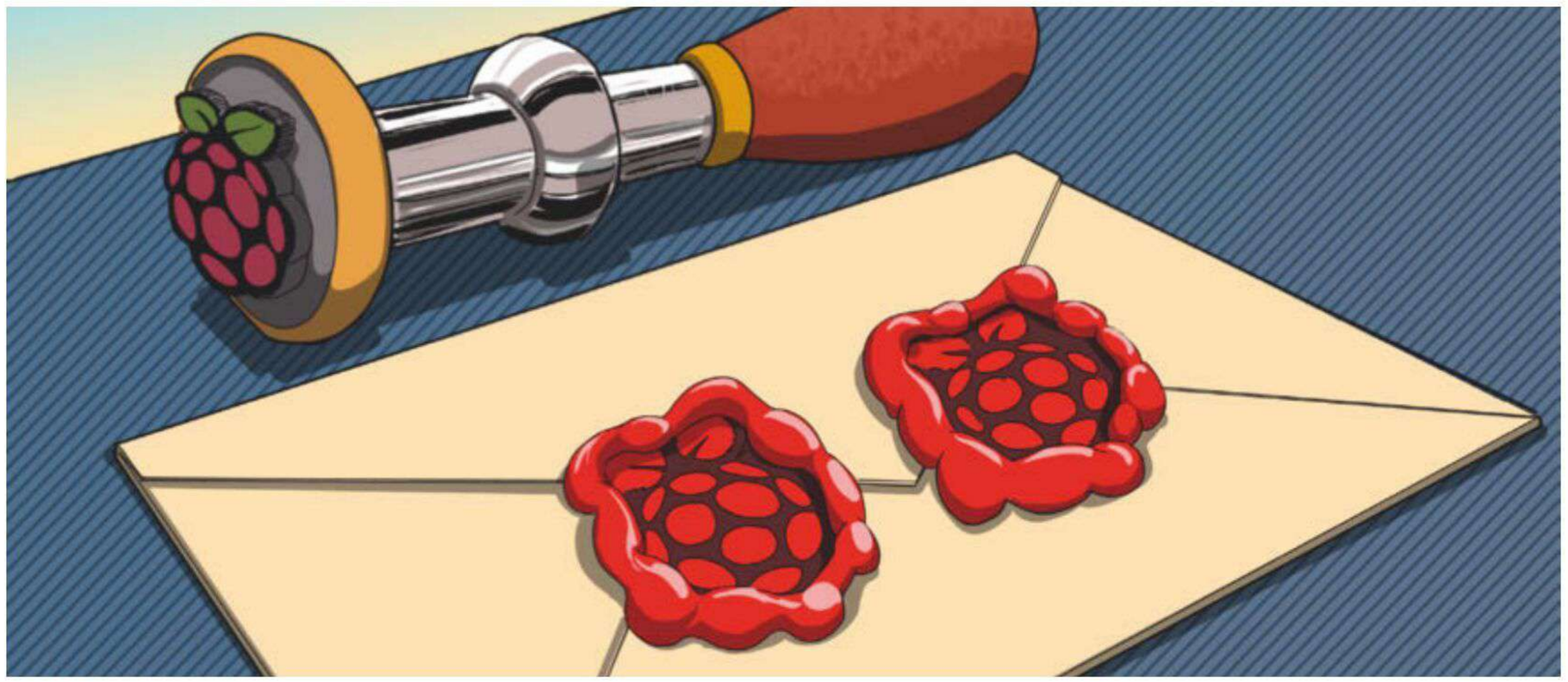


Bild: Thorsten Hübner

Verschlüsseltes DNS für Pi-hole

Mit der DNS-Verschlüsselung kann man sich davor schützen, dass Dritte aus Metadaten Erkenntnisse darüber sammeln, welche Webseiten man besucht. Router mit DNS-Verschlüsselung sind bisher aber selten. Ein Raspberry Pi mit dem DNS-Filter Pi-hole und gleich zwei verschiedenen DNS-Verschlüsselungen springt in die Bresche und erhöht nebenbei die Ausfallsicherheit.

Von **Dušan Živadinović**

An jedem Internetanschluss fließen Metadaten in Form unverschlüsselter DNS-Informationen unerkannt ab und zwar praktisch bei jedem Internet-Zugriff – zum Beispiel beim Surfen, beim Messaging oder beim Streamen. Geheimdienste und auch Internetprovider nutzen das zur Massenüberwachung. Besonders skrupellose Provider verkaufen Ihre Surf-Profile an Werbetreibende.

Mit einer DNS-Verschlüsselung kann man das Auslesen von Metadaten, das etwa am weltgrößten Internet-Drehkreuz in Frankfurt im großen Stil möglich ist, unterbinden. Seitdem die Internet Engineering Task Force vor wenigen Jahren die Verschlüsselungsmethoden DNS-over-TLS (DoT) und DNS-over-HTTPS (DoH) spezifiziert hat, sind etliche verschlüsselnde Clients für Linux, macOS, Windows, Android, iOS und andere Betriebssysteme entstanden. Wie man sie einrichtet, haben wir gezeigt (online abrufbar über ct.de/wr7d). Nachteilig daran ist, dass man sie auf jedem Gerät installieren muss, das man schützen will.

Diese Mühe kann man sich mit aktuellen Fritzboxen sparen, auf denen FritzOS ab Version 7.2x läuft; sie bringen einen DoT-Client mit. Der Großteil der übrigen Router lässt dieses Feature vermissen; auch fehlt es auf älteren Fritzboxen, wenn FritzOS 7.2x dafür nicht zu haben ist.

Als elegante Lösung bietet sich an, den Mikrorechner Raspberry Pi in Verbindung mit dem be-

liebten DNS-Filter Pi-hole und dem DoT-Client Stubby im Heimnetz nachzurüsten. Wie das geht, haben wir ebenfalls schon gezeigt, aber seitdem hat sich das Betriebssystem Raspberry Pi OS weiterentwickelt. Daher folgt hier eine aktualisierte und stark erweiterte Anleitung.

Grundsätzlich könnte sie viel knapper ausfallen, wenn Pi-hole einen DNS-Client verwenden würde, der die DNS-Daten selbst verschlüsselt. Doch aus Gründen der Ressourcensparsamkeit greifen die Pi-hole-Entwickler auf Dnsmasq zurück, das bisher konzeptionell nicht für die DNS-Verschlüsselung ausgelegt ist. Hilfsweise installiert man daher einen zusätzlichen lokalen Resolver, der verschlüsseln kann.

Der DoT-Client Stubby eignet sich dafür sehr gut, weil er ebenfalls nur wenige Ressourcen beansprucht. In sehr seltenen Fällen kann Stubby jedoch abstürzen. Wer sich gegen solche Ausfälle wappnen will, kann im LAN einen weiteren Raspi mit Stubby einrichten und hat sich damit auch gegen den Ausfall eines Raspi abgesichert. Zur Einrichtung muss man nur die Konfiguration des ersten Raspi auf die SD-Karte des zweiten kopieren.

Alternativ kann man einen gänzlich anderen DNS-Proxy verwenden – wahlweise auf dem zweiten Raspi oder auf demselben, auf dem Stubby läuft. Dieses zweite Szenario – zwei lokale Resolver auf einem Raspi – spielen wir mit dem DNSCrypt-Proxy durch. Er verschlüsselt je nach befragtem externen Resolver mit seinem eigenen dnscrypt-Protokoll oder mit DNS-over-HTTPS. Optional kann er die DNS-Anfragen so wie Stubby auf mehrere externe Resolver verteilen, was die Privatsphäre noch besser schützt.

Pi-hole installieren

Diese Anleitung geht von einem Raspberry Pi mit aktuellem OS aus und setzt nur geringe Linux-Kenntnisse voraus. Um Pi-hole einzurichten, öffnen Sie ein Terminal und aktualisieren zunächst die Paketverwaltung:

```
sudo apt update
sudo apt dist-upgrade
```

Mit dem zweiten Befehl ist das System auf den aktuellen Softwarestand gebracht. Falls sich dabei viele Pakete geändert haben, starten Sie den Raspi mit `sudo reboot` sicherheitshalber neu. Pi-hole lässt sich nun am einfachsten mit dem folgenden Befehl installieren:

```
curl -sSL https://install.Pi-hole.net↵
↳| bash
```

Nach der Installation öffnet sich ein Dialog, der diverse Dinge abfragt. Übernehmen Sie die Vorschläge und richten Sie erst mal provisorisch einen der DNS-Resolver ein, die Pi-hole vorschlägt, zum Beispiel Quad9. Übernehmen Sie auch die Vorschläge zu Blacklisten, IP-Protokollen, zur IP-Adresse des Raspi und des Gateways (Ihres Routers) sowie zum Web-Interface Lighttpd und Log Queries. Notieren Sie am Ende das Admin-Passwort für das Webinterface.

Schlagen Sie mit dem Kommandozeilenbefehl `ip` nach, welche IP-Adresse der Raspi bekommen hat und geben Sie diese in die Adresszeile Ihres Browsers ein, um das Webinterface von Pi-hole zu öffnen (zum Beispiel `http://192.168.178.22`). Binden Sie im Router, an den der Raspi angeschlossen ist, dessen MAC-Adresse an eine feste IP-Adresse, also beispielsweise an 192.168.178.22.

Bereiten Sie nun Pi-hole für den Betrieb mit den lokalen Resolvern Stubby und DNSCrypt-Proxy vor. Legen Sie dafür fest, dass der im Pi-hole eingebaute DNS-Resolver Dnsmasq beim Start nicht alle Netzwerk-Interfaces für sich beansprucht, sondern nur drei. Dazu bearbeiten Sie dessen Konfigurationsdatei mit einem Editor wie pico:

```
sudo pico /etc/dnsmasq.d/99-my-config.conf
```

Fügen Sie in die leere Datei die folgende Zeile ein:

```
listen-address=::1,127.0.0.1,192.168.178.22
```

Ersetzen Sie `192.168.178.22` mit der IP-Adresse Ihres Raspi. Die Adressen `::1` und `127.0.0.1` sind die IPv6- und IPv4-Loopback-Interfaces, über die Dnsmasq auf DNS-Anfragen antwortet, die von lokalen Anwendungen kommen. Damit sind die Vorarbeiten erledigt und es geht weiter mit der Installation des DNS-Resolvers Stubby:

```
sudo apt install stubby
```

Damit startet der Dienst auch schon, aber die Konfiguration muss noch angepasst werden. Stoppen Sie ihn daher und passen Sie die Konfiguration an:

```
sudo systemctl stop stubby
sudo pico /etc/stubby/stubby.yml
```

Zunächst ist die für Sie passende ECS-Einstellung auszuwählen (EDNS-Client-Subnet). Schaltet man diese Option ein (1), verschweigt Stubby das Subnetz Ihres Anschlusses und Sie erhöhen den Schutz der Privatsphäre. Schaltet man die Option aus (0), können Streaming-Anbieter wie Netflix anhand der Subnetzangabe besser zuordnen, woher die DNS-Anfrage kommt, und leiten Ihre Anfrage an das nächstliegende Rechenzentrum, das den Stream ausliefern kann. Das entlastet Internet-Weitverkehrsstrecken und senkt die Wahrscheinlichkeit für Übertragungsfehler. In den Grundeinstellungen ist ECS aus, also Privacy an:

```
edns_client_subnet_private : 1
```

Auch gut für die Privacy ist die Einstellung `round_robin_upstreams: 1`. Dabei verteilt Stubby die DNS-Anfragen reihum an alle konfigurierten entfernten Resolver und erschwert so Rückschlüsse auf das Verhalten der Nutzer eines Resolvers. Wenn diese Variable auf `0` steht, dann wird immer nur ein Upstream-Resolver in der Liste benutzt. Erst wenn der nicht mehr antwortet, kommt der nächste zum Zug.

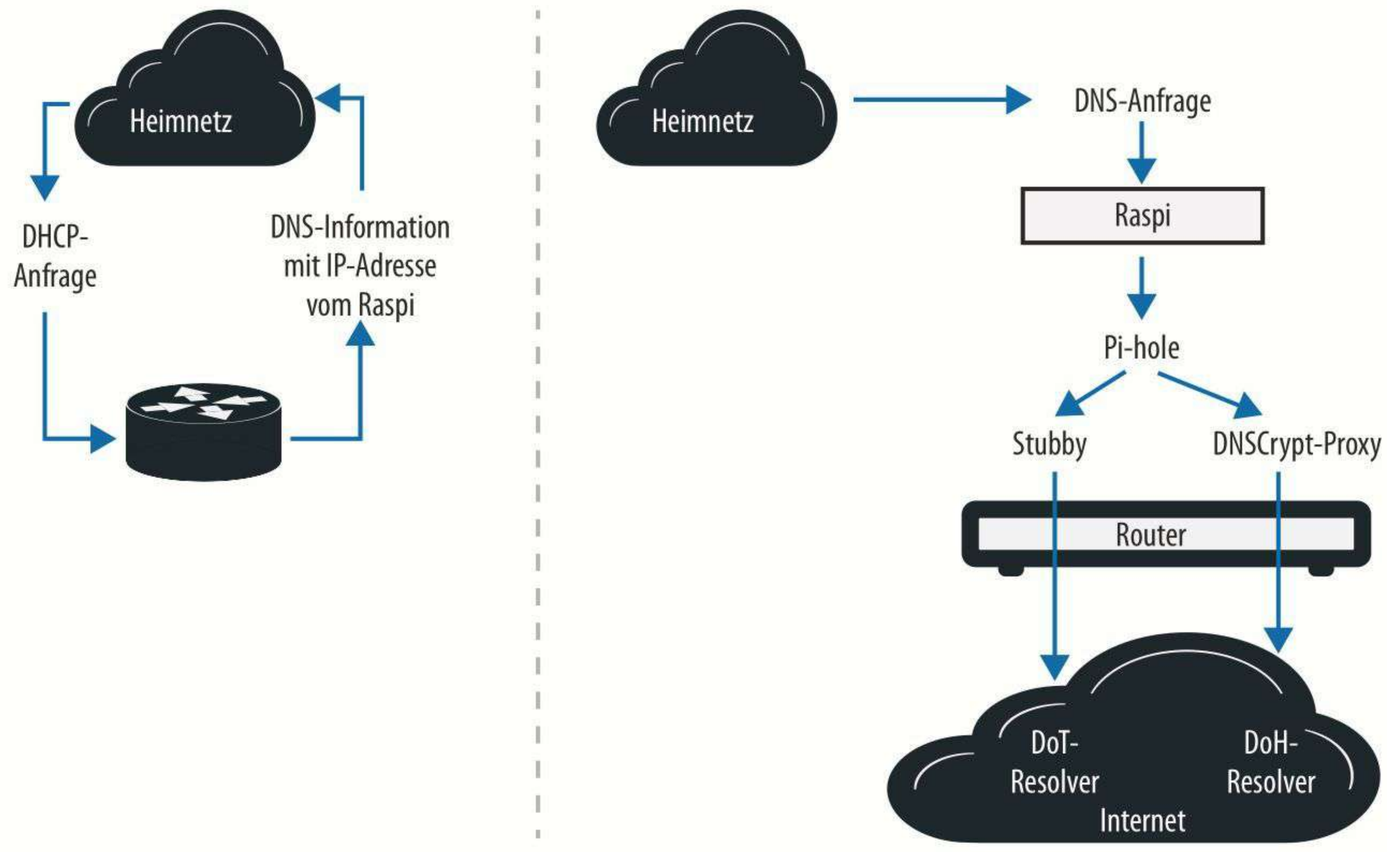
Der nächste wichtige Parameter ist die Listen-Address. Sie darf nicht `127.0.0.1:53` lauten, weil diese schon Dnsmasq belegt. Port `5353` darf es auch nicht sein, weil der für die lokale Multicast-DNS-Auflösung mittels Avahi reserviert ist; der Port 10053 eignet sich aber gut. So sieht ein Beispiel aus:

```
listen_addresses:
  - 127.0.2.2@10053
```

Lassen Sie die Loopback-Adresse für IPv6 weg (::1), denn damit gelang es nicht, Stubby und Dnsmasq auf unterschiedlichen Ports zu betreiben. Der nächste bedeutsame Punkt betrifft die Sicherheitsfunktion DNSSEC. In seltenen Fällen kann die Auf-

Verschlüsseltes DNS schützt Heimnetz

Rüstet man einen Raspi mit Pi-hole und lokalen Resolvern aus, kann man auf einen Schlag die Privatsphäre für das ganze Heimnetz verbessern. Damit die Anfragen bei Pi-hole landen, genügt es, die DHCP-Einstellungen des Routers anzupassen, sodass er Heimnetzgeräte mit der IP-Adresse des Raspis versorgt (links).



lösung mancher Domains bei eingeschaltetem DNSSEC scheitern. Wir empfehlen aber, DNSSEC zu nutzen und es allenfalls vorübergehend abzuschalten, wenn es mal knirscht.

Lassen Sie die übrigen Einstellungen zunächst unverändert, also auch die Parameter zu den DoT-Resolvern, die in der Stubby-Konfiguration bereits eingetragen sind. Wir zeigen später, wie Sie andere nutzen können. Speichern Sie die Änderungen mit Strg+X,Y. Wenn Sie DNSSEC aktiviert haben, kontrollieren Sie, ob diese Datei vorhanden ist:

```
ls /usr/share/dns/root.key
```

Ohne sie scheitert die DNS-Auflösung. Dann hilft es, Stubby neu zu starten, was aber nach Konfigurationsänderungen ohnehin erforderlich ist:

```
sudo systemctl restart stubby
```

Um testen zu können, ob Stubby DNS-Anfragen auflöst, installieren Sie das Paket `dnsutils`:

```
sudo apt install dnsutils
```

Ein Bestandteil dieses Pakets ist das Monitoring-Werkzeug `dig`. Mit dem folgenden Befehl lässt sich testen, ob Stubby DNS-Anfragen auflöst:

```
dig @127.0.2.2 -p 10053 ct.de
```

Die Antwort sollte die IP-Adresse von ct.de enthalten, also 193.99.144.80. Um zu prüfen, ob Stubby die Anfragen an die konfigurierten Upstream-Resolver weitergibt, kann man in einem Terminal-Fenster Stubby mit der Option `-v7` starten:

```
sudo stubby -v7
```

Öffnen Sie dann auf dem Raspi ein zweites Terminalfenster und geben Sie

```
dig @127.0.2.2 -p 10053 ct.de
```

ein. Im ersten Fenster sollten nun die IP-Adressen der entfernten Upstream-Resolver erscheinen, die in `/etc/stubby/stubby.yml` stehen. Um zu prüfen, ob Stubby ECS-Informationen sendet, geben Sie diesen `dig`-Befehl ein:

```
dig @127.0.2.2 -p 10053 edns-client-sub.net↵
↳ TXT +short
```

Wenn Ihr System ECS-Daten sendet, sollte in der Ausgabe „ecs_payload“ und nach der Variablen „ip“ Ihr Client-Subnet aufgeführt sein, also etwa „92.199.5.0“. Andernfalls steht am Anfang der Zeile „ecs False“.

Mehrere DoT-Resolver

Man kann mit Stubby diverse DoT-Resolver verwenden. Listen mit zahlreichen Resolvern finden Sie über ct.de/wr7d. Dort ist auch aufgeführt, nach welchen Richtlinien die Resolver arbeiten (z. B. mit oder ohne DNSSEC). Wenn Sie mehr als einen DoT-Server nutzen wollen (empfehlenswert wegen höherer Ausfallsicherheit und weil die Anfragen dann per Round-Robin-Verfahren verteilt werden), sollten Sie die Kandidaten gemäß Ihrer Ansprüche an DNSSEC, Filterung und ECS in Gruppen einteilen und dann nur solche Resolver eintragen, die zu einer Gruppe gehören. Also zum Beispiel „mit DNSSEC, ECS und ungefiltert“ oder „ohne DNSSEC, ohne Filter, ohne ECS“.

Wenn Sie neue DoT-Server prüfen, kommentieren Sie die alten vorübergehend aus (setzen Sie # an den Anfang der Zeile) und tragen Sie nur einen neuen ein. Speichern Sie die Änderungen und starten Sie den Dienst neu:

```
systemctl restart stubby
```

Prüfen Sie die neue Konfiguration:

```
dig @127.0.2.2 -p 10053 ct.de
```

Wenn Stubby nun eine Antwort liefert, ist die Konfiguration okay und man kann auf Wunsch die zuvor auskommentierten Server wieder hinzunehmen.

Ein Problem bei DoT-Servern ist, dass deren Zertifikate unabwendbar irgendwann ablaufen und dann vom Betreiber getauscht werden. Dann stimmt der Parameter `tls_pubkey_pinset` in /etc/stubby/stubby.yml nicht mehr, den Stubby zur Zertifikatsvalidierung verwendet. Das passiert bei DoT-Servern, die Let's-Encrypt-Zertifikate verwenden, mehrmals pro Jahr, weil die Zertifikate maximal 90 Tage gelten. Beispielsweise verwendet der DoT-Server dns2.digitalcourage.de ein Let's-Encrypt-Zertifikat.

Wenn also die DNS-Auflösung von Stubby einige Zeit lang funktioniert und dann plötzlich scheitert, ist vielleicht ein TLS-Zertifikat abgelaufen und durch ein neues ersetzt worden. Ob das der Fall ist, kann man mit Tools wie `kdig` testen. Der `kdig`-Befehl ist Bestandteil des Pakets `knot-dnsutils`, das Sie mit folgendem Befehl installieren:

```
sudo apt install knot-dnsutils
```

Das Befehlsmuster sieht so aus:

```
kdig @dns2.digitalcourage.de ct.de +tls
```

Falls `kdig` eine korrekte Antwort liefert (für ct.de sollte sie 193.99.144.80 lauten), aber Stubby nicht, spricht einiges dafür, dass `tls_pubkey_pinset` nicht aktuell ist. Den aktuellen können Sie mit folgendem Befehl auslesen:

```
echo | openssl s_client -connect↵
↳ 'dns2.digitalcourage.de:853' 2>/dev/null↵
↳ | openssl x509 -pubkey -noout ↵
↳ | openssl pkey -pubin -outform der ↵
↳ | openssl dgst -sha256 -binary ↵
↳ | openssl enc -base64
```

Setzen Sie statt `dns2.digitalcourage.de` die Domain des DoT-Resolvers ein, den Sie prüfen wollen.

Falls Stubby mal abstürzt, scheitert die DNS-Auflösung. Damit er möglichst umgehend wieder am Start ist, editieren Sie die Datei `/lib/systemd/system/stubby.service`:

```
sudo pico /lib/systemd/system/stubby.service
```

Setzen Sie die folgenden zwei Zeilen an das Ende des Abschnitts `Service`:

```
Restart=on-failure
RestartSec=1
```

Speichern Sie die Änderungen mit Strg+X,Y und starten Sie Stubby neu:

```
sudo systemctl daemon-reload
sudo systemctl restart stubby
```

DNSCrypt-Proxy

Der DNSCrypt-Proxy ist in Version 2.x ebenfalls als Paket erhältlich. Zu beachten ist, dass ECS erst ab Version 2.0.45 funktioniert, die bis zur Drucklegung dieses Sonderhefts im Paketbereich stable noch nicht erhältlich war (nur in sid/unstable). Man kann aber bereits mit der Version 2.019 starten und bei Verfügbarkeit auf 2.045 aktualisieren. DNSCrypt-Proxy wird mit einem einzigen Befehl installiert:

```
sudo apt install dnscrypt-proxy
```

Weil die Installationsroutine den Dienst starten will, aber die dafür angepeilte Loopback-Adresse Dnsmasq belegt, meldet die Installation am Ende den Fehler: „Job for dnscrypt-proxy.socket failed“. Das ließe sich normalerweise beheben, indem man in die Konfigurationsdatei `/etc/dnscrypt-proxy/dnscrypt-proxy.toml` eine freie Loopback-Adresse einträgt, etwa `127.0.2.3:10053`. Auf unseren Testsystemen wirkte diese Änderung aber ohne ersichtlichen Grund nicht. Ersatzweise trägt man die Einstellung in der System-Unit ein:

```
sudo pico /lib/systemd/system/↵
 ↳dnscrypt-proxy.socket
```

Ändern Sie dort die Listen-Adresse und den Port im Bereich Socket, damit sie wie folgt lauten:

```
[Socket]
ListenStream=127.0.2.3:10053
ListenDatagram=127.0.2.3:10053
```

Starten Sie anschließend den Daemon und den DNSCrypt-Proxy-Service neu:

```
sudo systemctl daemon-reload
sudo systemctl restart dnscrypt-proxy.socket
```

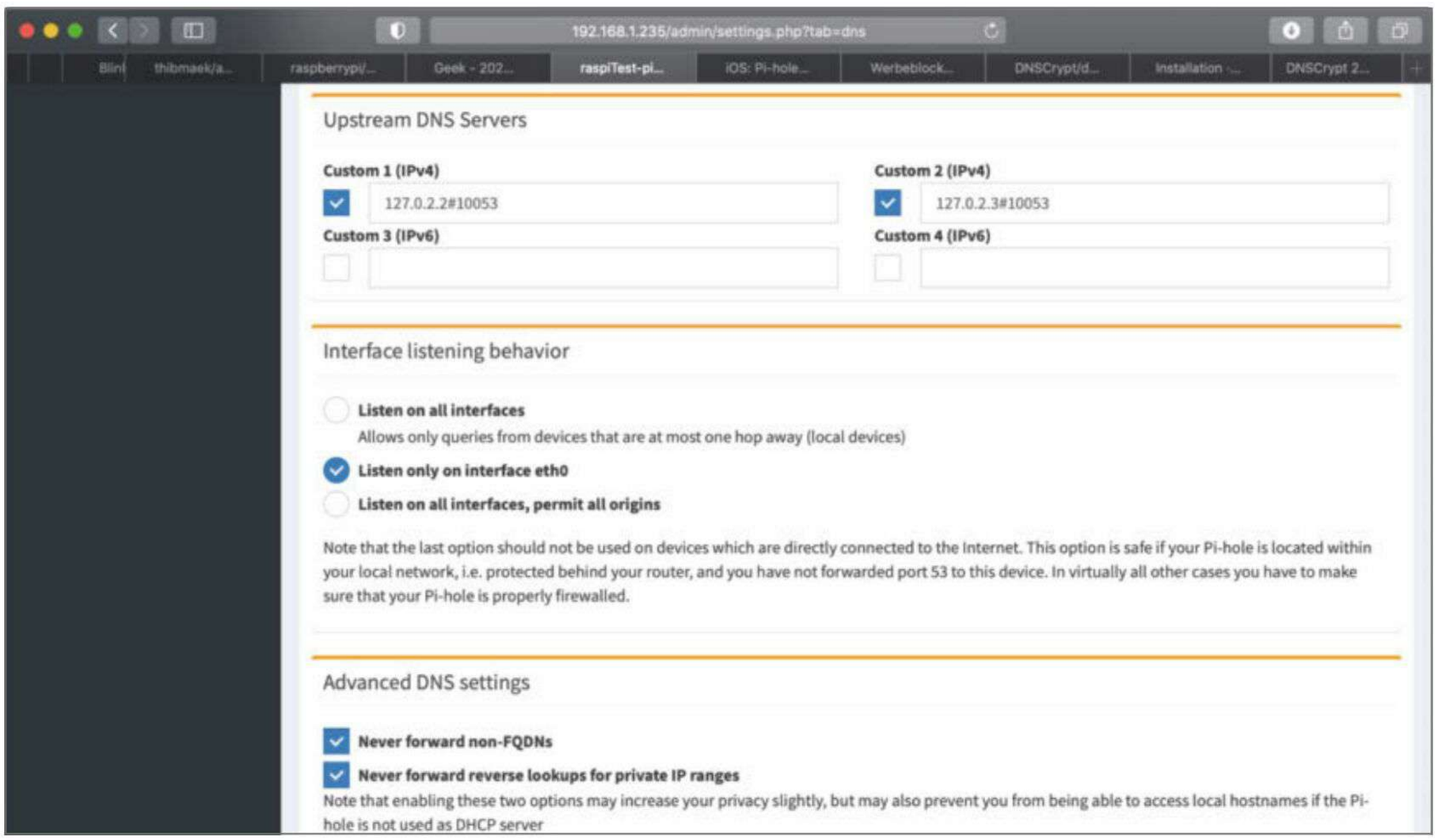
Der Dienst sollte nun einwandfrei laufen. Das kann man zum Beispiel mit dem Befehl

```
sudo systemctl status dnscrypt-proxy.socket
```

prüfen.

Nun geht es um die Konfiguration der Upstream-Resolver. Es gibt dafür im Prinzip zahlreiche Kandidaten (derzeit etwa 70 Hosts). Übersichten dazu finden Sie auf GitHub oder auch auf den Seiten des DNSCrypt-Projekts (siehe ct.de/wr7d). Allerdings aktualisiert DNSCrypt-Proxy 2.x seine Resolverliste auch selbstständig, und zwar in der Voreinstellung in 4-Stunden-Intervallen. Seine Standardstrategie fürs Load-Balancing heißt „p2“ und ist das, was man nutzen möchte, um Anfragen zu verteilen: Er nutzt dann die zwei schnellsten Server und bewertet die Latenz bei jeder Anfrage neu.

Wer argwöhnt, dass immer dieselben Resolver gewinnen, stellt auf die Strategie „ph“ um (schnellere Hälfte des Pools), um seine Anfragen weiter zu streuen und lebt damit, dass ein Teil der Queries nicht binnen 10 bis 15 Millisekunden beantwortet ist, sondern mal 20 bis 30 Millisekunden braucht.



Der DNS-Filter Pi-hole kann seine DNS-Anfragen an beliebige Resolver senden. Das kann man sich zu Nutze machen, um Pi-hole mit verschlüsselnden lokalen Resolvern zu erweitern.

Den Auswahlprozess kann man im Syslog beobachten.

Öffnen Sie die Datei `dnscrypt-proxy.toml` und stellen Sie die Konfiguration gemäß Ihrem Bedarf ein:

```
sudo pico /etc/dnscrypt-proxy/dnscrypt-proxy.toml
```

Im folgenden Beispiel ist das Loadbalancing auf `p2` eingestellt, DNSSEC eingeschaltet und es werden nur solche Resolver befragt, die laut Policy nicht protokollieren und nicht filtern:

```
lb_strategy = 'p2'
require_dnssec = true
require_nolog = true
require_nofilter = true
```

Falls Sie bestimmte Resolver nutzen wollen, schlagen Sie die Namen in den Resolverlisten nach und tragen Sie die gewünschten ohne die führenden Doppelkreuze (`##`) in die Variable `server_names` ein. Ein Beispiel sieht wie folgt aus:

```
server_names = ['bcn-dnscrypt', 'ams-doh-nl']
```

Ob mit expliziter Serverwahl oder mit automatischem Loadbalancing, starten Sie nun den Dienst neu:

```
sudo systemctl restart dnscrypt-proxy.socket
```

Ob der DNSCrypt-Proxy funktioniert, fördert

```
dig @127.0.2.3 -p 10053 ct.de
```

zu Tage. Welche DNS-Anfragen er erhält und beantwortet, notiert der Proxy in seiner Log-Datei, deren jüngste Einträge Sie beispielsweise mit `tail` ausgeben können:

```
sudo tail -f /var/log/dnscrypt-proxy/query.log
```

Pi-hole anpassen

Nun geht es um die Pi-hole-Konfiguration. Melden Sie sich dafür am Webinterface von Pi-hole an, öffnen

Sie über die linke Menüleiste die Einstellungen (Settings) und dort den Bereich DNS. Schalten Sie die zuvor aktivierten Upstream-Resolver ab und tragen Sie auf der rechten Seite die IP-Adressen und Ports Ihrer beiden Custom DNS-Resolver ein – nämlich `127.0.2.2#10053` für Stubby und `127.0.2.3#10053` für DNSCrypt-Proxy.

Schicken Sie Pi-hole nun einige DNS-Anfragen:

```
dig @localhost ct.de
dig @localhost dingsda.de
dig @localhost esrappeltimkarton.de
```

Öffnen Sie das Pi-hole-Webinterface und dort den Bereich Query Log. Pi-hole sollte nun in der Spalte Status aufführen, an welchen Upstream-Resolver die Anfrage geschickt wurde – zum Beispiel: „forwarded to 127.0.2.3#10053“.

Falls Sie länger beobachten wollen, an welchen Resolver die Anfragen gehen, ist das Webinterface unhandlich, denn es aktualisiert den Inhalt nicht automatisch. Stattdessen empfiehlt es sich, den IP-Verkehr des Loopback-Interfaces einfach eine Weile lang mit dem Befehl `tcpdump` mitzuschneiden. Installieren Sie dafür tcpdump:

```
sudo apt-get install tcpdump
```

Mit dem folgenden Befehl landet der Mitschnitt in der Datei dns-test.txt:

```
sudo tcpdump -vv -i lo >dns-test.txt
```

Um Anfragen zu senden, gibt man in einem anderen Fenster `dig`-Befehle ein:

```
dig @127.0.2.3 -p 10053 ct.de
dig @127.0.2.3 -p 10053 dingdong.de
dig @127.0.2.3 -p 10053 rapunzel.de
dig @127.0.2.3 -p 10053 fiedeldei.de
```

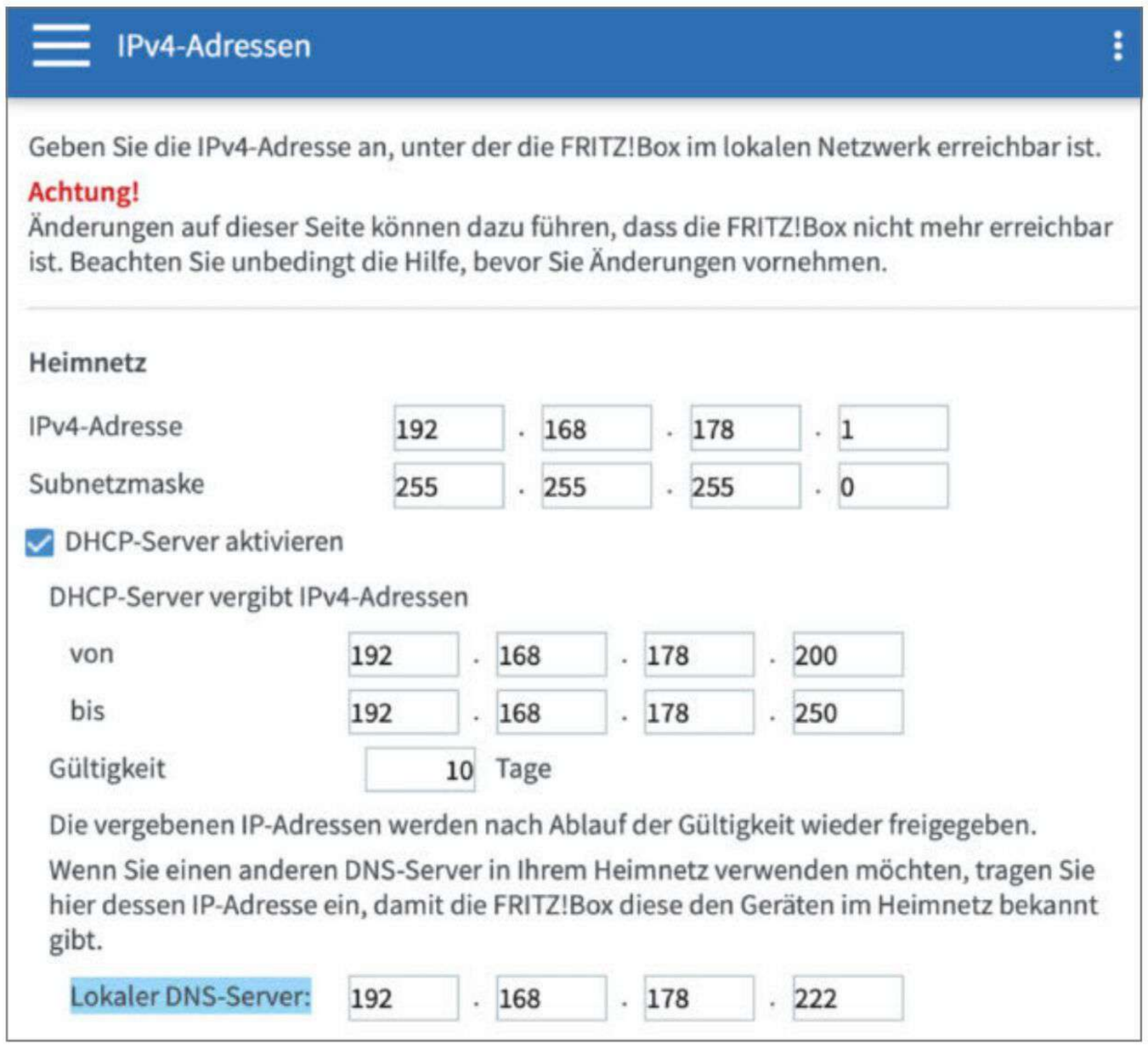
Nachdem Sie den Mitschnitt beendet haben (Strg+C), lassen Sie sich den Inhalt anzeigen:

```
less dns-test.txt
```

Neben den irreführenden Fehlermeldungen („bad udp cksum“) sollten in der Ausgabe die IP-Adressen der angefragten DNS-Resolver nebst verwendetem Port stehen, zum Beispiel „127.0.2.3.10053“. Der Prüfsummenfehler, den der Befehl tcpdump moniert, rührt daher, dass die Pakete nur intern übertragen werden und gar nicht bis zur Ethernet-Schnittstelle kommen, die erst die Prüfsumme berechnet und dann in die Pakete einträgt.

2020-12-07 10:06:15	A	time.apple.com	fritz.box	OK (forwarded to 127.0.2.2#10053)	CNAME (210.1ms)	Blacklist
2020-12-07 10:05:45	A	media-router-api1.prod.media.g05.yahoodns.net	fritz.box	OK (forwarded to 127.0.2.2#10053)	IP (185.4ms)	Blacklist
2020-12-07 10:05:45	AAAA	media-router-api1.prod.media.g05.yahoodns.net	fritz.box	OK (cached)	NODATA (0.1ms)	Blacklist
2020-12-07 10:05:45	A	weather-ydn-yql.media.yahoo.com	fritz.box	OK (forwarded to 127.0.2.3#10053)	CNAME (241.1ms)	Blacklist
2020-12-07 10:05:45	AAAA	weather-ydn-yql.media.yahoo.com	fritz.box	OK (forwarded to 127.0.2.3#10053)	CNAME (130.5ms)	Blacklist
2020-12-07 10:03:03	A	p19-btmmdns.icloud.com.akadns.net	fritz.box	OK (forwarded to 127.0.2.3#10053)	IP (345.2ms)	Blacklist
2020-12-07 10:02:58	A	p26-btmmdns.icloud.com.akadns.net	fritz.box	OK (forwarded to 127.0.2.3#10053)	IP (68.5ms)	Blacklist

An welchen Resolver Pi-hole eine DNS-Anfrage abgeschickt hat, kann man sich im Menü Query Log und dort in der Spalte Status anzeigen lassen. Im obigen Bild sind Beispiele für zwei lokal eingerichtete Resolver zu sehen, 127.0.2.2 und 127.0.2.3.



Aktuelle Fritzboxen können DNS-Anfragen zwar verschlüsseln, aber wer den Adblocker Pi-hole nutzen will, konfiguriert in den DHCP-Einstellungen den Raspi als DNS-Server für das Heimnetz.

Router einrichten

Probieren Sie Pi-hole zusammen mit den beiden lokalen Resolvern einige Tage lang mit einem PC aus. Tragen Sie dafür im PC die IPv4- und IPv6-Adresse (beginnt mit fe80:) des Raspi in die DNS-Einstellungen des PC ein. Prüfen Sie, ob sich darüber Ihre üblichen Webseiten öffnen lassen, also etwa ob das Streaming wie gewohnt klappt. Insbesondere das Streaming hoch aufgelöster Filme kann hakeln, wenn der Resolver keine ECS-Daten verrät, denn bei dieser Einstellung können die Anbieter nicht korrekt zuordnen, aus welchem Teilnetz die Anfrage kommt, und leiten daher bestenfalls ab und zu zum nächstgelegenen Rechenzentrum um, meist aber zu irgendeinem entfernten.

Als Faustregel gilt aber: Je länger die Strecke, desto mehr Backbone-Router sind beteiligt und desto höher ist die Wahrscheinlichkeit, dass einer davon überlastet ist und für Ihren Stream nur ungenügende Kapazität hat. Dann hilft es, erst mal alle entfernten Resolver in den beiden Konfigurationen zu deaktivieren und nur einen zu aktivieren, der definitiv ECS-Daten weitergibt. Sollte sich das Streaming bessern, ist das ein Beleg dafür, dass Sie nur solche Resolver in Stubby und DNSCrypt-Proxy konfigurieren sollten, die ECS-Daten melden.

Wenn Pi-hole schließlich zur Zufriedenheit läuft, richten Sie ihn als Adblocker und DNS-Resolver für das ganze LAN ein, indem Sie dessen IPv4- und IPv6-Adresse im Router in dessen DHCP-Einstellungen eintragen. Weiter unten haben wir beispielhaft für DrayTek- und Fritzbox-Router aufgeführt, wie man die DNS-Einstellungen ändert. Wie Sie bei anderen Routern vorgehen, finden Sie im Handbuch des jeweiligen Modells.

Auf DrayTek-Routern finden Sie die DNS-Einstellungen im Bereich „LAN/General Setup“. Setzen Sie dort unter dem Abschnitt „DNS Server IP Address“ ein Häkchen, um manuelle Einstellungen eintragen zu können (Force DNS manual setting). Geben Sie dann im Feld „Primary IP Address“ die IP-Adressen Ihres Raspi ein, auf dem Pi-hole läuft und speichern Sie die Änderungen.

Auf den verbreiteten Fritzboxen finden Sie die DNS-Einstellungen im Menü „Heimnetz/Netzwerk/Netzwerkeinstellungen/weitere Einstellungen/IPv4-Konfiguration“. Tragen Sie die IPv4-Adresse des Raspi im Feld „Lokaler DNS-Server“ ein und speichern Sie die Änderung. Wechseln Sie dann in das benachbarte Menü zur IPv6-Konfiguration und tragen Sie dort die IPv6-Adresse Ihres Raspi ein.

Die Netzwerkgeräte übernehmen die neuen DHCP-Einstellungen, wenn sie sich das nächste Mal am Router anmelden, also etwa nach Trennen und Anstöpseln des Netzwerkkabels.

Erfahrungen

Zwei jeweils per Hand auf die obige Weise eingerichtete Raspis liefen bei uns in mehrwöchigen Tests reibungslos; die DNS-Auflösung fiel dabei nicht aus. Interessant war zu beobachten, dass Pi-hole seine DNS-Anfragen nicht im stetigen Wechsel an Stubby und DNSCrypt-Proxy schickt, sondern einen der beiden eine Zeit lang bevorzugt und dann wechselt. Das variiert die Streuung der Anfragen und kommt der Wahrung der Privatsphäre zugute. (dz) c't

Entfernte verschlüsselnde Resolver

ct.de/wr7d



Bild: Rudolf A. Blaha

AdGuard Home macht Pi-hole Konkurrenz

Adblocker sind beliebt, weil sie nicht nur Werbung blockieren können, sondern auch Malware draußen halten und arglose Spaziergänge zu verseuchten Webseiten unterbinden. Dem beliebten Pi-hole ist mit AdGuard Home starke Konkurrenz erwachsen.

Von **Dušan Živadinović**

Unter den Adblockern nimmt Pi-hole auf der Beliebtheitsskala seit Längerem einen der vorderen Plätze ein. Aber einen wichtigen Entwicklungszweig berücksichtigen die Pi-hole-Entwickler bisher nicht: Der DNS-Dienst pihole-FTL beziehungsweise der zugrunde liegende Server Dnsmasq kommuniziert nur unverschlüsselt mit der Außenwelt – genauer: mit DNS-Resolvern, die angefragte Domainnamen zu IP-Adressen auflösen und damit den Weg zu gesuchten Zielen im Inter-

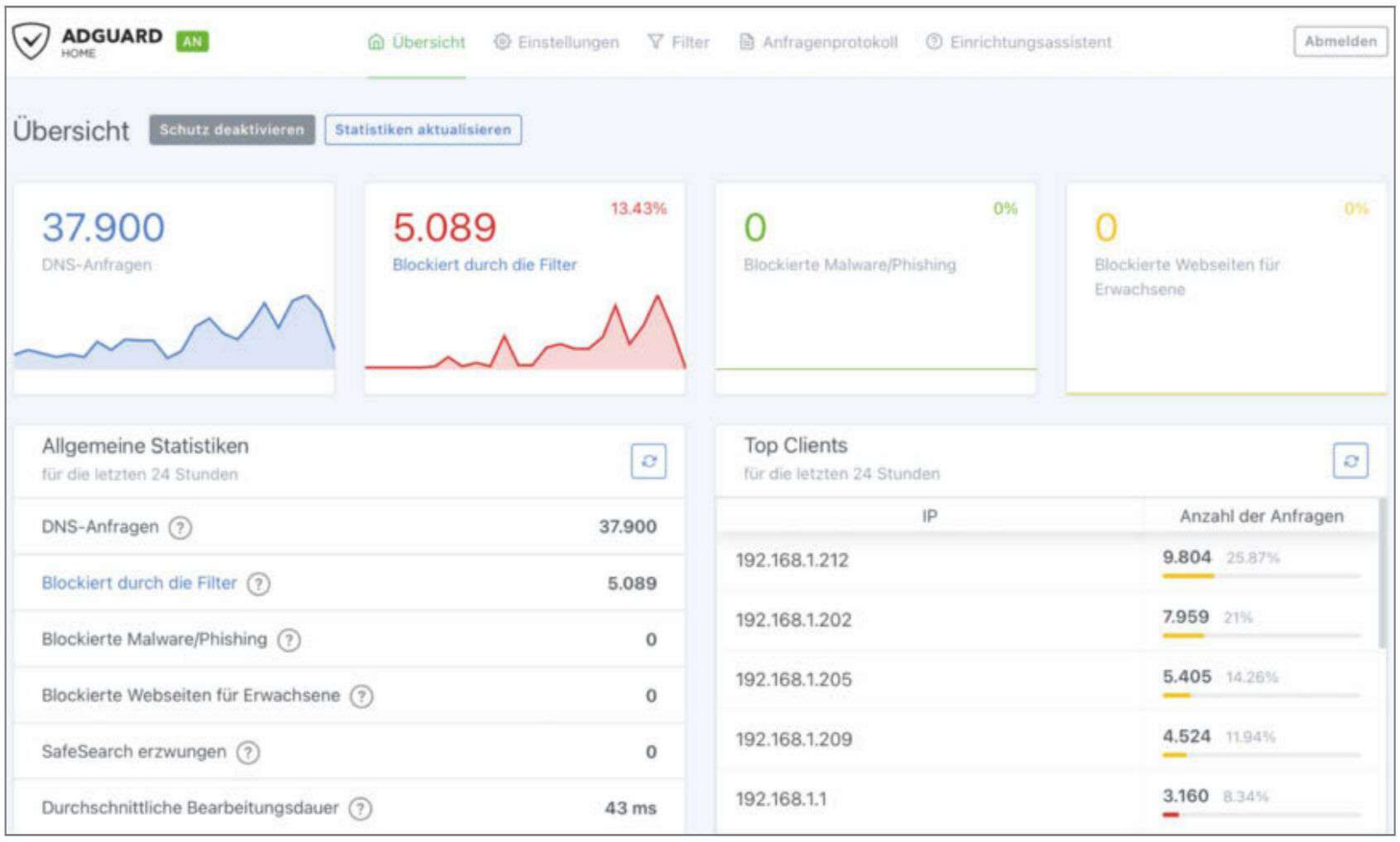
net weisen. Daher können Dritte die Pi-hole-Anfragen manipulieren und belauschen, beispielsweise am weltgrößten Internet-Drehkreuz DE-CIX in Frankfurt.

Dagegen helfen Protokolle zur verschlüsselten Kommunikation mit dem Domain Name System (DNS). Bisher üblich sind DNS-over-TLS (DoT), DNS-over-HTTPS (DoH) und DNSCrypt. DNS-over-QUIC (DoQ) gewinnt langsam an Fahrt und mehrere Arbeitsgruppen weltweit entwickeln weitere Protokolle. Pi-hole-Nutzer behelfen sich, indem sie verschlüsselnde Proxies wie Stubby oder DNSCrypt-Proxy davorschalten (siehe Seite 20).

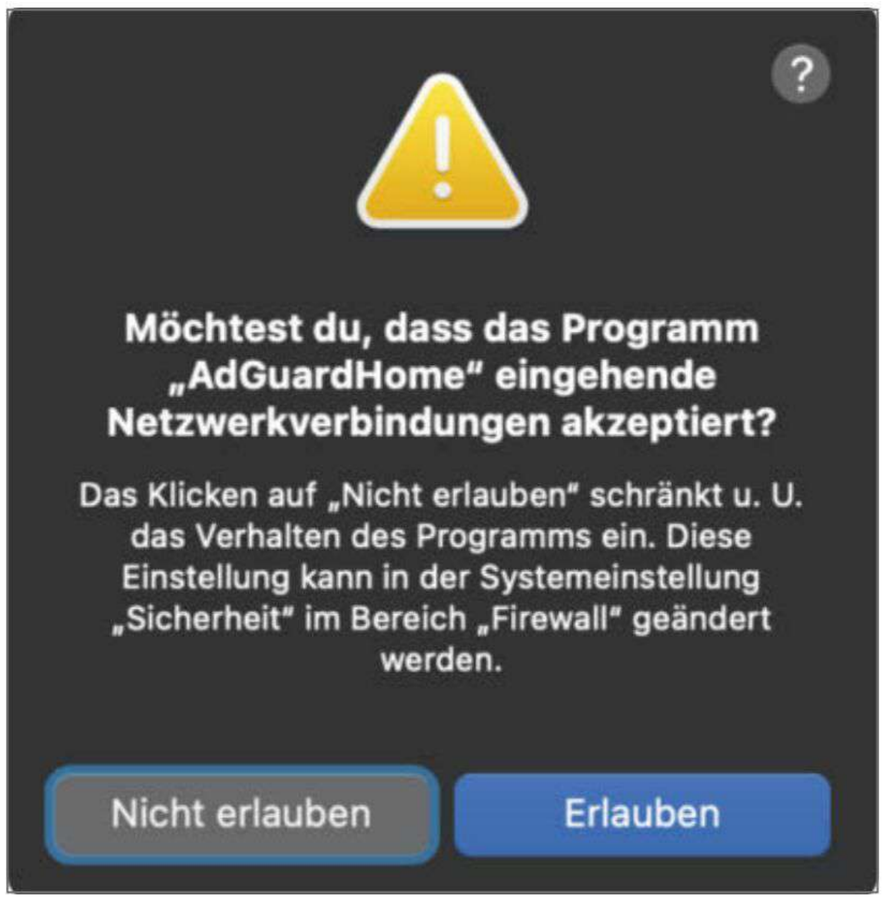
Im AdBlocker AdGuard Home stecken DoT, DoH, DNSCrypt und DoQ schon drin. Den auf GitHub veröffentlichten Quellcode finden Sie ebenso wie alle übrigen Querverweise zu diesem Artikel über ct.de/w46x. Die Firma AdGuard wurde 2009 in Moskau gegründet und hat ihren Sitz 2018 nach Zypern und damit in die EU verlegt. Sie verdient ihr Geld mit kommerziellen DNS-Filtern und AdBlockern.

AdGuard Home macht einen sehr übersichtlichen Eindruck. Anders als bei Pi-hole, der aus mehreren Programmen besteht, stecken bei AdGuard Home sämtliche Funktionen in einem nur rund 20 MByte großen Binary: ein lokaler DNS-Server (Stub-Resolver) zur Kommunikation mit externen DNS-Servern (rekursive Resolver), ein AdBlocker und ein Server zur Konfiguration per Webinterface. Die komplette Konfiguration liegt in einer Datei. Das Programm lässt sich im Handumdrehen installieren und auch deinstallieren.

AdGuard Home erfasst zudem die Antwortgeschwindigkeit der befragten Resolver, sodass man schnell erkennen kann, ob die Resolver-Wahl gut oder weniger gut war. Ab Werk bringt AdGuard Home eine eigene DNS-basierte Filterliste zum Blockieren von Malware und Werbung mit, weitere kann man wie bei Pi-hole in einem einfachen User-Interface definieren. Individuelle Sperr- und Freigabelisten lassen sich in AdGuard Home ebenfalls anlegen, jedoch nicht ganz so komfortabel wie in Pi-hole. Falls was schiefläuft, lässt sich die AdBlocker-Funktion per Mausklick abschalten. Einige Funktionen machen AdGuard Home auch für Umgebungen mit hohen Sicherheitsanforderungen interessant: Der Dienst kann auch mit Clients verschlüsselt kommunizieren und sein Webinterface per HTTPS ausliefern. All das verlockt, AdGuard Home auszuprobieren.



Der AdBlocker und Malware-Filter AdGuard Home liefert ähnlich übersichtliche Statistiken wie Pi-hole. Zusätzlich führt er aber auch die Bearbeitungszeit auf, was man zur Optimierung der Konfiguration nutzen kann.



Damit AdGuard Home auf Macs DNS-Anfragen von Clients annehmen kann, muss die Firewall diese durchlassen.

Weil DNS-Server den Port 53 exklusiv belegen, kann auf einem System immer nur ein Resolver laufen. Um AdGuard Home auf einem Raspi auszuprobieren, auf dem schon Pi-hole arbeitet, muss man also Pi-hole deaktivieren (z. B. mit dem Befehl `sudo systemctl stop pihole-FTL`). Man erleichtert sich das Leben aber, wenn man AdGuard Home eine eigene SD-Karte spendiert und das Raspberry Pi OS von Grund auf neu darauf einrichtet.

AdGuard Home läuft außerdem auf diversen anderen Linux-Distributionen und auch auf macOS (auf Macs mit der M1-CPU zunächst als x86-Code in Rosetta-Emulation, aber auch eine ARM-Anpassung ist in Arbeit). Eine komplette Übersicht über die vorausgesetzten CPU-Plattformen haben die Entwickler auf GitHub veröffentlicht. In diesem Beitrag spielen wir die Installation und Konfiguration für Raspberry Pi OS (Buster) und für macOS (High Sierra und Big Sur) durch; die Unterschiede sind minimal und zum Nachkochen dieser Anleitung genügen Grundkenntnisse. Gute Nachrichten für Terminal-Allergiker: Die Kommandozeile wird nur sporadisch bemüht.

Für die Installation von AdGuard Home setzen wir einen bereits eingerichteten Raspi voraus; es spielt keine Rolle, ob mit Desktop-Umgebung oder ohne. Wir haben die Modelle Raspberry Pi 3B+ und Raspberry Pi 4 erfolgreich ausprobiert. Die macOS-Einrichtung haben wir auf einem Intel-basierten Mac Mini Jahrgang 2011 (macOS 10.12.6) und einem taufrischen MacBook Pro mit M1-CPU von Apple durchgespielt (macOS 11.2.1).

Installation

Öffnen Sie ein Terminal und laden Sie das Installations-Skript für AdGuard Home mit dem `curl`-Befehl herunter; es wird automatisch an die Shell zum Ausführen weitergegeben:

```
sudo curl -sSL https://raw.↵
↳githubusercontent.com/↵
↳AdguardTeam/AdGuardHome/master/↵
↳scripts/install.sh | sh
```

Auf Macs geben Sie auf Nachfrage das Administrator-Passwort ein, der Raspi fragt nicht danach. Der Vorgang ist im Nu erledigt und AdGuard Home läuft dann schon. Die macOS-Firewall fragt dann, ob Sie für AdGuard Home eingehende Netzwerkverbindungen genehmigen wollen. Erlauben Sie das.

Das Skript führt unter anderem auf, in welchem Ordner AdGuard Home residiert (z. B. auf Linux in `/opt/AdGuardHome`, auf macOS 11 in `/Applications/AdGuardHome`). Notieren Sie diesen Ordner, um AdGuard Home bei Bedarf deinstallieren zu können. Neben der Einrichtung des Programms werden sowohl auf Linux als auch auf macOS Skripte zum automatischen Start nach dem Booten eingerichtet.

Ob der Dienst läuft, prüfen Sie auf dem Raspi so:

```
systemctl status AdGuardHome
```

Auf macOS geben Sie ein:

```
launchctl list | grep -i AdGuard
```

Der Dienst lässt sich einfach per Kommandozeile verwalten. Mit „Installation“ und „Deinstallation“ meinen die Entwickler aber nur das Aktivieren und Deaktivieren des Dienstes. Um das Programm komplett zu entfernen, löscht man einfach dessen Verzeichnis (z. B. `rm -rf /opt/AdGuardHome`).

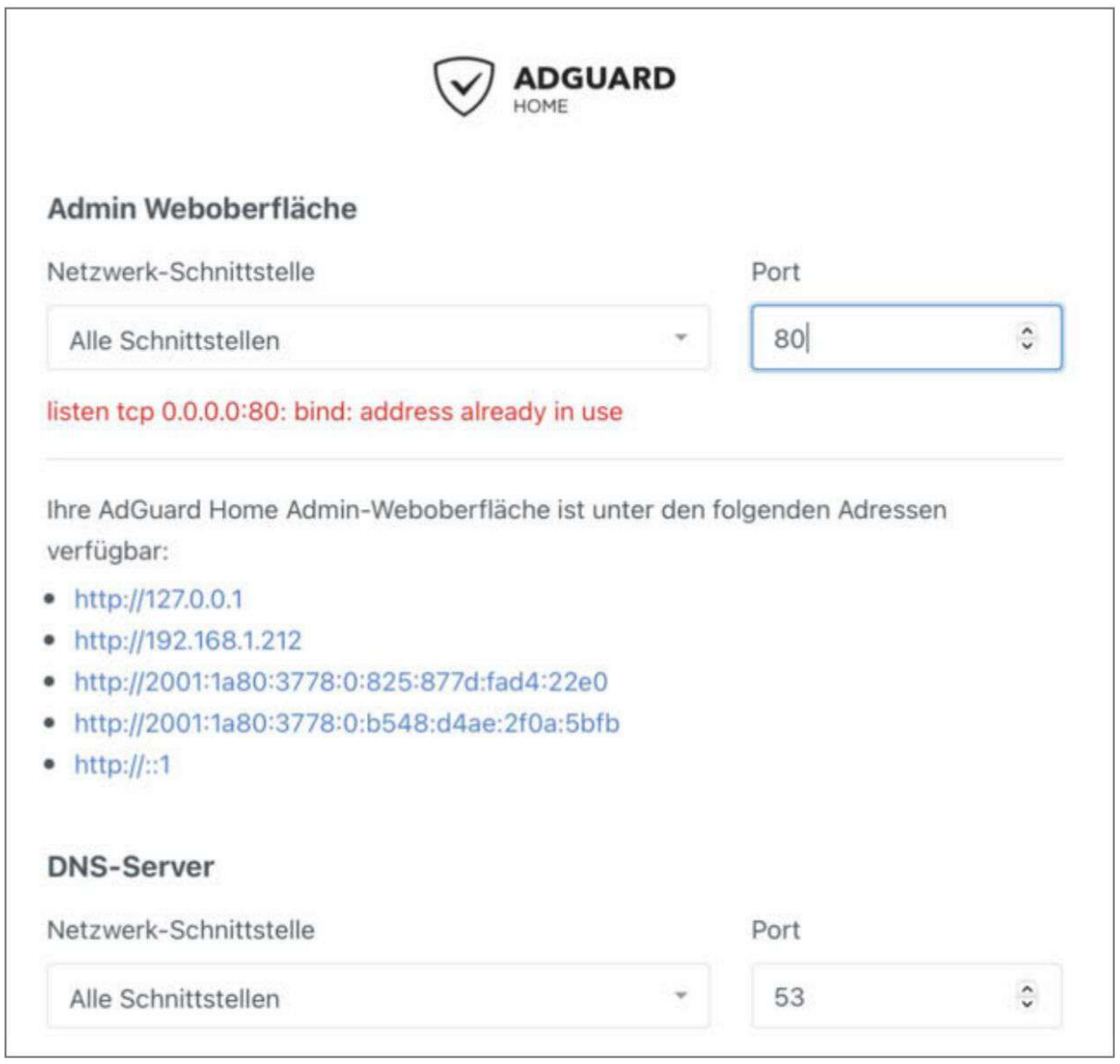
Konfiguration

Wenn Sie auf dem Raspi ein Desktop-System installiert haben, öffnen Sie dort im Browser die URL

http://127.0.0.1:3000. Falls nicht, ermitteln Sie mit dem Befehl `ip a` die LAN-IP-Adresse des Raspi und geben Sie diese im Browser eines beliebigen Rechners ein, der in Ihrem LAN läuft (z. B. http://192.168.178.101:3000). Auf Macs ist mindestens der Safari-Browser vorinstalliert, sodass sich AdGuard Home dort lokal konfigurieren lässt (http://127.0.0.1:3000).

Durch den ersten Teil der Konfiguration führt das Webinterface mit fünf einfachen Schritten. Klicken Sie auf der Startseite rechts unten aufs Menü, schalten Sie auf Deutsch um und laden Sie die Seite im Browser neu. Klicken Sie dann auf „Anfangen“.

Auf der zweiten Seite stellt man die Schnittstellen und den Port ein, über den der Webserver und der DNS-Server angesprochen werden. Nach Ende der Konfiguration ist der Webserver nicht mehr über den Port 3000 erreichbar, sondern über den jeweils eingestellten.



Die Einrichtung von AdGuard Home ist so einfach wie das Brezelbacken. Auf etwaige Adresskollisionen weist die Software selbstständig hin; man kann sie im Vorbeigehen beseitigen.

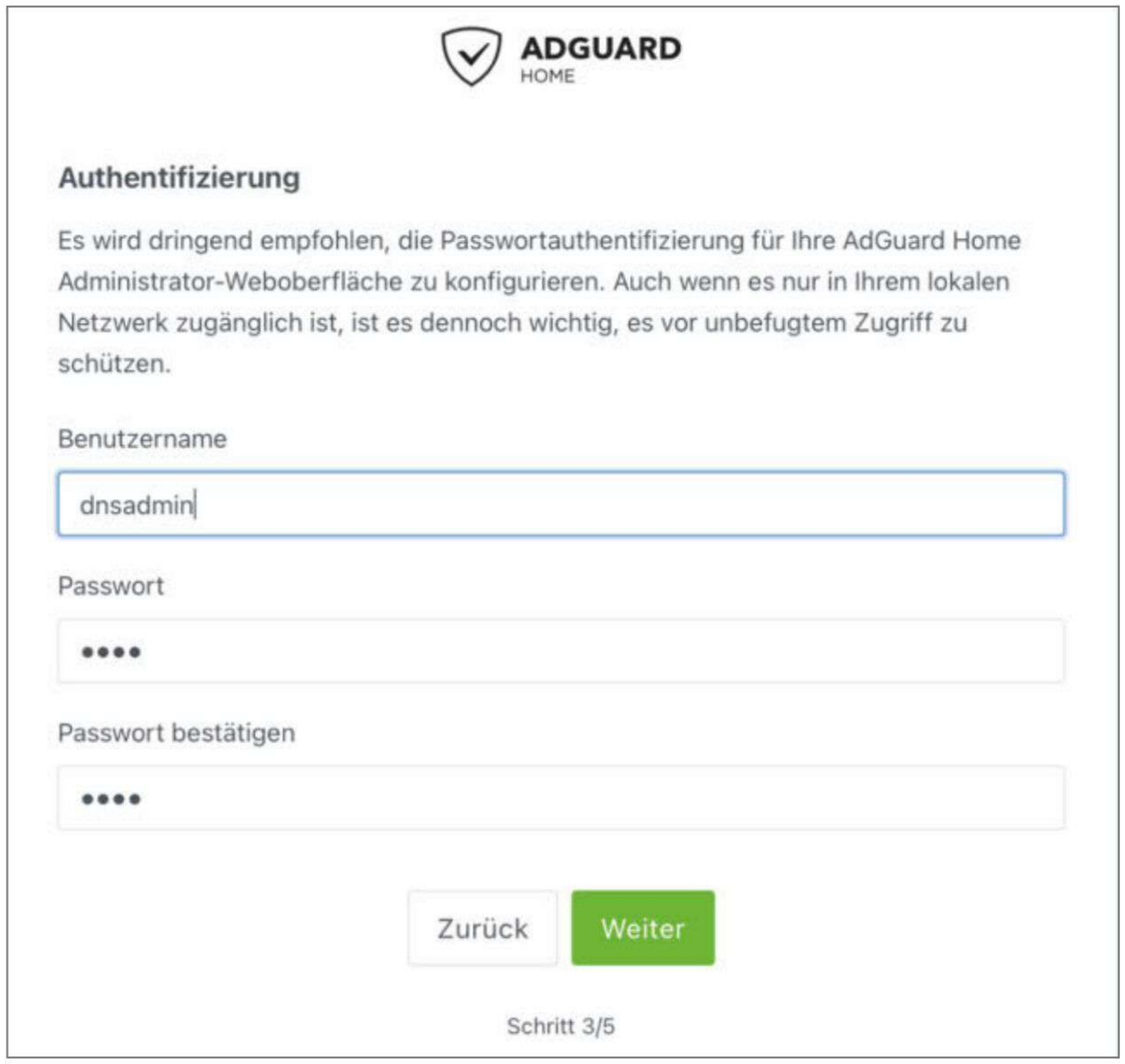
Normalerweise kann man für beide Server die Voreinstellung übernehmen. Falls aber auf demselben Rechner ein anderer Webserver den Port 80 nutzt, meldet der Assistent eine Adresskollision (address already in use). Am einfachsten ist es dann, dem Webserver von AdGuard Home einen anderen Port zuzuweisen, zum Beispiel 8080 oder 10080. Jedenfalls: Die nächste Seite des Einrichtungsassistenten lässt sich nur öffnen, wenn keine Kollision vorliegt.

Unterhalb der Schnittstellen- und Portwahl sind alle lokalen Adressen zu sehen, unter denen der Webserver erreichbar ist. Wenn Sie auf das Webinterface aus dem Heimnetz zugreifen wollen, sprechen Sie es am besten über die LAN-IP-Adresse an, also etwa 192.168.178.101, wenn das die IP-Adresse des Geräts ist, auf dem AdGuard Home läuft. Falls Sie den Webserver von AdGuard Home auf einem anderen als dem Standardport 80 betreiben, etwa 8080, sprechen Sie ihn so an: http://192.168.178.101:8080.

Die Voreinstellungen für den DNS-Server kann man normalerweise ebenfalls übernehmen. Für den Fall, dass der Standardport 53 von einem anderen DNS-Server belegt ist, meldet AdGuard Home ebenfalls eine Adresskollision. Prinzipiell kann man den DNS-Dienst so wie den Webserver auf einen anderen Port legen. Dagegen spricht aber, dass viele DNS-Clients nur für den Standardport ausgelegt sind.

Deshalb empfiehlt es sich, den anderen DNS-Server für die Dauer des Tests abzuschalten. Auf Macs kann der Port 53 durch einen Resolver wie Stubby belegt sein, auf Linux durch Dienste wie `systemd-resolved`. Um Stubby zu stoppen, öffnen Sie den Stubby-Manager und klicken Sie dort auf „Stop“. Um `systemd-resolved` auf einem Linux-System zu stoppen, klicken Sie auf den Button „Fix“, den AddGuard Home neben der Fehlermeldung einblendet.

Am Ende der zweiten Konfigurationsseite empfehlen die AdGuard-Home-Entwickler, den DNS-Dienst bereits jetzt für das gesamte Heimnetz einzurichten. Schieben Sie diesen Schritt besser auf, bis Sie sichergestellt haben, dass er zur Zufriedenheit läuft. Fahren Sie stattdessen mit der Zuweisung einer festen lokalen IP-Adresse für den Rechner fort. Auf den verbreiteten Fritzboxen öffnet man dazu das Menü „Heimnetz/Netzwerk“, klickt auf das Bearbeiten-Symbol des jeweiligen Geräts und schaltet die Funktion „Diesem Netzwerkgerät immer die gleiche



Den ersten Teil der Einrichtung unterteilt das Webinterface in fünf Schritte. Auf den meisten Systemen kann man die Vorgaben übernehmen und muss nur die Zugangsdaten festlegen.

IPv4-Adresse zuweisen“ ein. Auf anderen Routern hilft gegebenenfalls die Anleitung des Herstellers weiter.

Klicken Sie anschließend auf „Weiter“, tragen Sie einen Benutzernamen und ein Passwort ein und öffnen Sie die vierte Konfigurationsseite. Nun blendet AdGuard Home eine Anleitung zum Einrichten des Dienstes auf diversen Geräten ein. Lassen Sie diese Seite einstweilen offen und gehen Sie zurück zum Terminal, um den Dienst zunächst mit dem Befehl `dig` zu testen. Dig gehört auf macOS zur Grundausstattung, muss aber auf dem Raspi nachinstalliert werden; er steckt im Paket `dnsutils`.

```
sudo apt update
sudo apt install dnsutils
```

Prüfen Sie, ob der neu installierte Server DNS-Anfragen auflöst:

```
dig @localhost ct.de
```

Dig sollte die IP-Adresse `193.99.144.80` melden. Ist das der Fall, dann konfigurieren Sie AdGuard Home zunächst für nur ein Gerät, beispielsweise einen Windows-PC oder Mac. Kurzanleitungen dazu finden Sie, indem Sie im Webinterface unterhalb der Adressen auf eines der Symbole klicken – überspringen Sie aber den „DNS-Datenschutz“, weil von dort kein Weg zurück zum Assistenten führt. Stattdessen empfiehlt es sich, jedes der anderen Symbole anzuklicken und die dort vorgehaltenen Kurzanleitungen für späteren Bedarf in eine Textdatei zu kopieren.

Wenn Sie einen Testrechner für die Nutzung des AdGuard-Home-Dienstes konfiguriert haben, ist die Grundkonfiguration erledigt. Klicken Sie auf Weiter und dann auf „Übersicht öffnen“. Geben Sie dann im Authentifizierungsdialog die zuvor definierten Zugangsdaten ein. Anschließend öffnet AdGuard Home die Übersicht (Dashboard).

Im Prinzip kann man AdGuard Home so betreiben und zum Beispiel auf Stabilität testen – das Tool

nutzt zur DNS-Auflösung den Resolver dns10.quad9.net und filtert bereits Zugriffe auf Domains. Um seine volle Leistung zu nutzen, sollte man aber die Einstellungsmöglichkeiten zumindest grob überfliegen.

Klicken Sie dazu auf das Menü „Einstellungen/Allgemeine Einstellungen“. Mit der Option „Domains durch Filter und Host-Dateien sperren“ schaltet man den AdBlocker nach Bedarf ein und aus. Die AdGuard-Dienste zum Schutz vor verseuchten Webseiten, der Kinderschutzfilter und SafeSearch sind empfehlenswert. Bei allen vier Optionen gilt aber: Falls später auf Ihrem Testrechner Internet-Programme verzögert öffnen oder YouTube-Streams und andere Dienste unvollständig laden, empfiehlt es sich, die Filter testweise abzuschalten. Auch sind Protokolle und Statistiken nützlich bei der Fehlersuche, sodass man sie eingeschaltet lassen sollte.

Klicken Sie nun auf „Einstellungen/DNS-Einstellungen“. Im Feld Upstream-DNS-Resolver steht zu Beginn nur ein Eintrag. Zumindest um die Ausfallsicherheit zu erhöhen, ist es aber nützlich, dort mehrere Resolver einzutragen. AdGuard bietet dafür unter der Adresse kb.adguard.com/en/general/dns-providers eine große Sammlung an. Auch eine gute Quelle für DoH- und DNSCrypt-Resolver ist die Seite dnscrypt.info/public-servers. Um die Adresse eines DoH-Servers zu ermitteln, klickt man dort links in der Spalte „Name“ auf einen Eintrag und kopiert den Domain-Anteil aus der Zeile „Addresses“ in das Webinterface von AdGuard Home (z. B. spricht man den Resolver von dnshome-doh mit AdGuard Home anhand der Domain dns.dnshome.de an – Details dazu stehen im Abschnitt „Resolver eintragen“).

Resolver-Wahl

Mit der Wahl der Resolver stellt man die Weichen für die Sicherheit und Privatsphäre. Zunächst ist zu beachten, dass jeder Resolver-Betreiber DNS-Anfragen und Quell-IP-Adressen protokollieren kann. Ob er das tut, hängt von seiner Motivation ab. Manche bieten Resolver eigens für den Schutz der Privatsphäre und sichern zu, keine Protokolle anzulegen (no-logs). Andere versuchen, ihre Dienste zu Geld zu machen und arbeiten mit Werbetreibenden zusammen.

Prinzipiell könnte man der Protokollierung entgehen, indem man einen rekursiven Resolver vom Schlage des Quad9-Dienstes selbst betreibt. Dafür hält man die Root-Zone lokal zum Beispiel auf einem DNS-Server wie Unbound vor (Hyperlocal Root), damit dieser direkt mit DNS-Root-Servern und autoritativen Servern kommunizieren kann. Doch das geht bisher nur unverschlüsselt, sodass die Privatsphäre futsch ist.

Deshalb nutzt man besser einen externen Resolver, den auch viele andere Anwender verwenden, weil dessen Kommunikation mit der Root-Zone und den autoritativen Servern nicht den IP-Adressen der Heimrouter zugeordnet werden kann. Deshalb sind Resolver, welche die Provider den Heimroutern bei der Einwahl zuteilen, keine schlechte Wahl. Jedoch unterhält bisher kaum ein Provider verschlüsselnde Resolver. Immerhin hat die Deutsche Telekom Anfang Februar einen DoH-Resolver im offenen Feldversuch gestartet.

Doch wer nicht gerade Telekom-Kunde ist und der Firma vertraut, steckt in einer Zwickmühle, wenn er seinen DNS-Verkehr verschlüsseln will – denn die Vertrauenswürdigkeit der meisten Anbieter ist unklar. Immerhin sichern manche Resolver-Betreiber in ihren AGBs zu, die Privatsphäre zu wahren.

Bei US-Unternehmen sollte man generell vorsichtig sein, weil diese verpflichtet sind, Daten ihrer Nutzer auf staatliche Weisung herauszugeben. Immerhin hat Quad9 seinen Hauptsitz erst Mitte Februar in die Schweiz verlegt, die zugesichert hat, keine Daten von Quad9-Nutzern einzufordern (siehe ct.de/w46x).

Gute Kandidaten sind die Server der Schweizer Digitalen Gesellschaft und der Bielefelder Institution Digitalcourage. Zu beachten ist aber, dass durch Spenden finanzierten Projekte der Last der Anfragen nicht immer gewachsen sind. Deshalb beantwortet der Resolver von Digitalcourage pro Quell-IP-Adresse maximal 20 DNS-Anfragen pro Sekunde. Gegen solche Engpässe hilft es, mehrere Resolver zu konfigurieren.

Vor der Auswahl sollte man festlegen, welche Funktionen man vom Resolver erwartet, also ob er mit oder ohne Security-Blocklist, DNSSEC oder ECS arbeitet (Extension Mechanisms for DNS Client-Subnet, kurz ECS). Security-Blocklisten sperren Zugriffe auf Webseiten mit Malware (empfehlenswert). Die Sicherheitstechnik DNSSEC schützt vor Manipulation von DNS-Auskünften (empfehlenswert).

Per ECS-Funktion teilt der Resolver dem Betreiber der Zieldomain mit, aus welchem Subnetz die DNS-Anfrage stammt. Falls der Betreiber der angefragten Domain, zum Beispiel Netflix oder Amazon Prime, seine Dienste weltweit über verschiedene Rechenzentren anbietet (Content Delivery Network, CDN), kann er die Nutzerin oder den Nutzer zum nächstgelegenen Rechenzentrum leiten. Das entlastet Weitverkehrsstrecken im Internet, senkt die Wahrscheinlichkeit für Überlastungen und verkürzt die Signallaufzeit, sodass es prinzipiell empfehlenswert ist.

Weil die Resolver oft nur kleine Subnetzgrößen nennen (z. B. für maximal 256 User), können Lauscher aus den Anfragen nach einer Weile unterschiedliche Userprofile ableiten. Je nach Provider können in den ECS-Informationen aber auch weitere private Daten stecken (z. B. die komplette IP-Adresse), wovon Nutzer nichts erfahren.

Die Entwickler von AdGuard Home und DNSCrypt führen in ihren Resolver-Listen den ECS-Support nur sporadisch bis gar nicht auf. Beispielsweise ist bei Googles Resolvern ECS aktiviert, aber in der AdGuard-Liste fehlt diese Kennzeichnung. Für viele Resolver muss man also direkt beim Anbieter recherchieren, ob sie die ECS-Funktion nutzen.

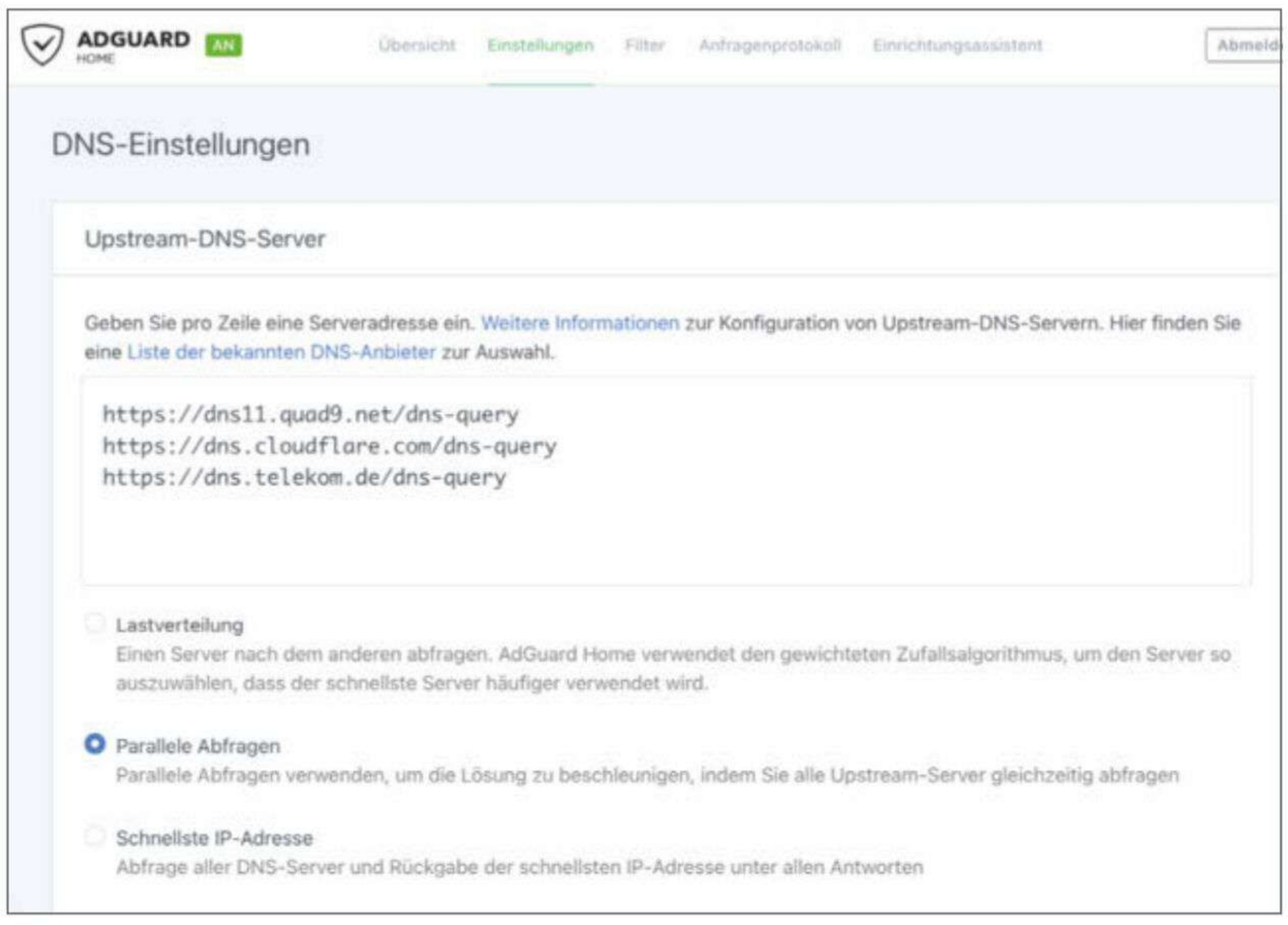
Resolver eintragen

Mit dem vorangestellten `https://` legt man fest, dass AdGuard Home für die Kommunikation mit dem Resolver das verschlüsselnde Protokoll DoH verwendet. DoT, DNSCrypt und DoQ leisten im Prinzip dasselbe und es ist dem Betreiber überlassen, welche der Methoden er nutzt oder ob sein Resolver überhaupt verschlüsselt. Vor allem große Resolver-Betreiber wie Cloudflare bieten sowohl unverschlüsselte als auch verschlüsselte DNS-Kommunikation an. Um mit AdGuardHome einen Resolver per DoT anzusprechen, setzt man der Domain `tls://` voran, also etwa `tls://dns3.digitalcourage.de`. Bei manchen DoH-Resolvern muss man der Domain noch den Pfad /dns-query anfügen, also zum Beispiel `https://dns.dnshome.de/dns-query` – da ist etwas Experimentierfreude gefragt.

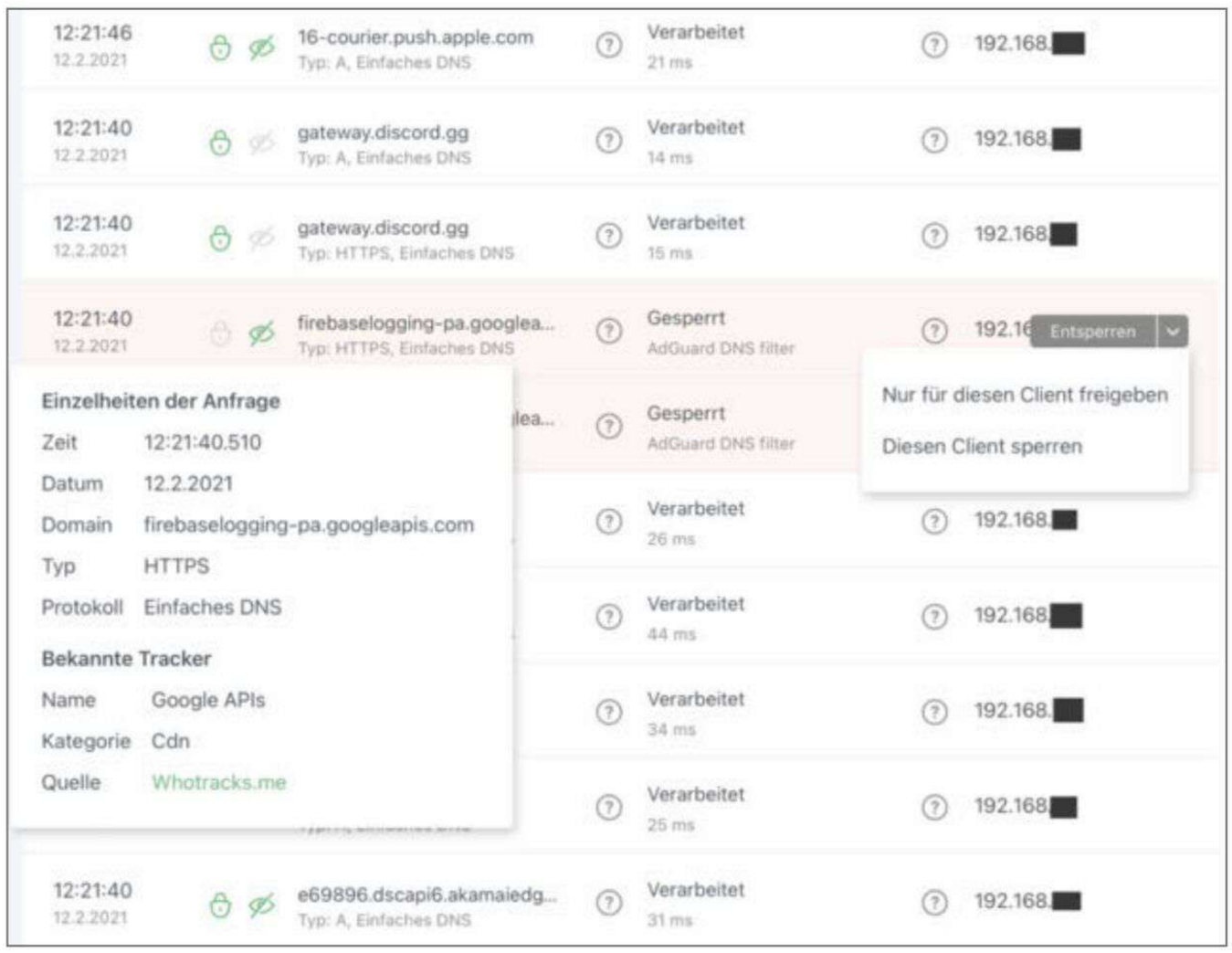
Wenn Sie Ihre Resolver-Kandidaten eingetragen haben, scrollen Sie ein Stück nach unten und klicken Sie auf „Upstreams testen“. AdGuard Home gibt dann gleich bekannt, ob die Kommunikation geklappt hat und führt auch auf, wenn er einen Resolver nicht erreicht hat. Prüfen Sie dann, ob die URL korrekt ist. Wenn ja, dann ist der nicht erreichbare Server vermutlich gerade außer Betrieb. Solange AdGuard Home mindestens einen Resolver ansprechen kann, wird dessen Dienst funktionieren. Einige Spezialfunktionen stehen aber nur dann zur Verfügung, wenn Sie mehrere funktionierende Resolver eingetragen haben.

Dann kann AdGuard Home DNS-Anfragen an mehrere Resolver streuen (Lastverteilung), alle Resolver auf einmal befragen (parallele Abfragen; sie beschleunigen den Webseitenaufbau) oder immer nur den schnellsten Resolver befragen. Welche der Methoden Sie nutzen, hängt davon ab, ob Sie die Geschwindigkeit oder die Privatsphäre höher gewichten. Wenn Sie die Resolver-Einstellungen erledigt haben, klicken Sie auf Anwenden.

Die Adressen der Bootstrap-Server lassen Sie am besten unverändert. Diese benötigt AdGuard Home,



AdGuard Home bietet für die Abfrage externer Resolver drei Methoden. Je nach Bedarf kann man die Geschwindigkeit oder den Schutz der Privatsphäre höher gewichten.



In AdGuard Home kann man den Zugriff auf gesperrte Webseiten einzelnen Clients freigeben. So lässt sich leicht testen, ob die Sperrung einer Domain unerwünschte Auswirkungen auf Internetdienste hat.

um die IP-Adressen der eingetragenen Resolver zu finden. Im Bereich DNS-Serverkonfiguration empfiehlt es sich, den Begrenzungswert höherzustellen. Voreingestellt sind maximal 20 Anfragen pro Client pro Sekunde. Wenn Ihr AdGuard-Home-Rechner keine weiteren Aufgaben hat, können Sie dort 0 eintragen, um beliebig viele Anfragen zu erlauben und so Verzögerungen auszuschließen.

Lassen Sie IPv6 eingeschaltet, weil das einfach gute Netzwerkpraxis ist. Für den Inhalt der DNS-Kommunikation spielt es aber keine Rolle, ob die Anfrage per IPv4 oder per IPv6 gestellt wurde – sie wird auf demselben Weg beantwortet, wie sie eingegangen ist.

Im Bereich DNS-Zwischenspeicher (Cache) sollte man die Voreinstellungen übernehmen. Allenfalls die Größe des Zwischenspeichers könnte man erhöhen, damit sich AdGuard Home mehr DNS-Antworten merken kann. Geräte mit kleinem Arbeitsspeicher kann man aber leicht überfordern, sodass man die Cache-Größe nur vorsichtig erhöhen sollte.

Resolver-Listen und Infos

ct.de/w46x

Alle übrigen Voreinstellungen sollte man zunächst übernehmen. Surfen Sie eine Weile wie gewohnt auf Ihrem Testrechner. In der Regel laufen schon nach wenigen Minuten hunderte von DNS-Anfragen auf. Klicken Sie dann auf „Übersicht“ und prüfen Sie die durchschnittliche Bearbeitungsdauer. Als Faustregel gilt: je kürzer, desto besser. In unseren Tests erreichte AdGuard Home mit einigen Resolvern bei parallelem Abfragemodus Latenzen um 40 Millisekunden herum. Mit weit entfernten oder hoch belasteten Resolvern dehnte sich die Latenz aber leicht auf 160 Millisekunden aus.

Kommandozeile

AdGuard Home lässt sich auch über die Kommandozeile verwalten, etwa um die Konfiguration auf Fehler zu prüfen (`AdGuardHome --check-config`). Man kann auch dem Webserver eine neue IP-Adresse oder einen neuen Port zuweisen. Eine Übersicht über die Optionen liefert dieser Befehl:

```
AdGuardHome --help
```

Die Konfigurationsdatei finden Sie im Stammverzeichnis von AdGuard Home im Unterordner data. Sie heißt AdGuardHome.yaml. Man kann sie mit einem Texteditor bearbeiten, muss dann aber den Dienst manuell beenden und neu starten, um die Änderungen zu übernehmen.

Monitoring

Statusmeldungen soll die Software eigentlich in die Datei `/var/log/AdGuardHome.stdout.log` schreiben. Diese Datei ließ AdGuard Home aber auch nach 12 Wochen Dauerbetrieb unangetastet. Nützliche Meldungen fanden wir aber in `/var/log/AdGuardHome.stderr.log` (`AdGuardHome.err` auf dem Raspi).

Dort notiert AdGuard Home, auf welcher IP-Adresse und welchem Port der Dienst auf Anfragen wartet (z. B. `udp://192.168.1.99:53`) oder auch, ob und wann der AdBlocking-Filter aktualisiert worden ist (z. B. Filter 1 has been updated: 742569 bytes, 38908 rules).

Im Log tauchten vereinzelte Fehlermeldungen auf (failed to create file, too many open files). Das hatte auf den Betrieb keine sichtbaren Auswirkungen. AdGuard Home lief mehrere Monate lang reibungslos und hinterließ im Vergleich mit anderen Adblockern und Malware-Filtern einen geschmeidigen Eindruck. (dz) c't



Bild: Andreas Martini

Raspi 4 als Fertig-VPN-Dongle

Damit Beschäftigte zu Hause arbeiten können, sind VPN-Lösungen meist unverzichtbar. Die Einrichtung ist aber oft aufwendig. Mit einem Raspberry Pi 4 als USB-Dongle sind die Rechner im Homeoffice binnen Minuten im Firmennetz und vollständig vom Heimnetz isoliert.

Von **Mirko Dölle**

Homeoffice-Arbeitsplätze mit VPN-Tunnel ins Firmennetz sind für Admins riskant: Angreifer können die mitunter schlecht gesicherten Heimnetze ausnutzen, um die Rechner als Brückenkopf zum Angriff auf interne Firmensysteme zu missbrauchen. Auch die Einrichtung der VPN-Tunnel ist nicht jedem Anwender zuzumuten. Der Raspberry Pi ist eine günstige und gleichzeitig einfache Alternative, um Arbeitsrechner im Homeoffice mit dem Firmennetz zu verbinden und gleichzeitig vom Heimnetz des Mitarbeiters zu isolieren.

Die von uns entwickelte Lösung des Raspi als „VPiN“ nutzt aus, dass der Mini-Rechner über den USB-C-Anschluss nicht nur Strom aufnimmt, sondern auch Daten gemäß USB 2.0 überträgt. Damit kann der Raspi 4 verschiedene USB-Peripheriegeräte emulieren, wenn Sie ihn an einen PC oder an ein Notebook anschließen. Sollte im Einzelfall die Stromversorgung über einen USB-Anschluss des Rechners nicht genügen, können Sie mit einem Y-Kabel wie dem DeLock 83176 zwei USB-Ports gleichzeitig anzapfen.

Sie benötigen lediglich einen Raspberry Pi 4 mit 2 GByte RAM und einem Gehäuse, das lüfterlos für eine ausreichende Kühlung sorgt – etwa das „Aluminiumgehäuse mit Kühlfunktion“ von Joy-it für 12

bis 15 Euro. Zusammen mit einer 16 GByte großen MicroSD-Karte kommt man so auf etwa 60 bis 70 Euro. Sie benötigen nicht einmal ein Netzteil. Man steckt im einfachsten Fall das Netzwerkkabel des Arbeitsrechners an den Raspi und schließt den Raspi als USB-Netzwerk-Adapter an.

Damit sich der Raspi 4 beim angeschlossenen Rechner als USB-Ethernet-Adapter ausgibt, müssen Sie bei Raspberry Pi OS das Device Tree Overlay `dwc2` zusätzlich laden lassen, indem Sie an die Datei /boot/config.txt folgende Zeile anfügen:

```
dtoverlay=dwc2
```

Zusätzlich muss Raspberry Pi OS bei jedem Start das Modul `libcomposite` laden. Tragen Sie es deshalb in der Datei /etc/modules ein. Die eigentliche Initialisierung und Konfiguration als USB-Gadget erfolgt im Verzeichnis /sys/kernel/config/usb_gadget und ist in [1] und [2] ausführlich beschrieben. Wir haben Ihnen unter ct.de/w7t6 eine angepasste Variante des Initialisierungs-Skripts `initusbc` zum Download bereitgestellt, das den Raspi 4 als USB-Ethernet-Adapter mit der Bezeichnung „VPiN“ konfiguriert. Kopieren Sie es nach /usr/local/bin und machen Sie es ausführbar. Damit das Skript künftig nach jedem Neustart wieder ausgeführt wird, tragen Sie es vor der Zeile `exit 0` in der Datei /etc/rc.local ein.

Die Netzwerkkonfiguration erfolgt über die Datei /etc/network/interfaces.d/usb0, wir haben Ihnen die Konfigurationsdatei unter ct.de/w7t6 zum Download bereitgestellt – so wie alle anderen Konfigurationsdateien, die Sie für dieses Projekt benötigen. Sie verwendet das IPv4-Subnetz 192.168.255.0/24. Sollte das Subnetz im Homeoffice des Anwenders bereits belegt sein, müssen Sie ein anderes verwenden.



Ein Aluminiumgehäuse in Form eines Kühlkörpers sorgt für lautlose Kühlung des Raspi-VPN-Dongle, die Stromversorgung übernimmt allein der Arbeitsrechner. Die MicroSD-Karte lässt sich außedem leicht mit einem Siegel versehen.

Adressverteiler

Um Anwendern die Netzwerkkonfiguration zu ersparen, soll der VPiN über die emulierte USB-Ethernet-Schnittstelle auch als DHCP-Server arbeiten – sich aber per Ethernet oder WLAN automatisch auch eine Adresse aus dem Heimnetz besorgen. Deshalb müssen Sie die Netzwerkschnittstelle `usb0` für den DHCP-Client sperren, indem Sie folgende Zeile am Ende der Datei `/etc/dhcpcd.conf` anfügen:

```
denyinterfaces usb0
```

Als DHCP-Server empfehlen wir `dnsmasq` und `radvd`. Beide Pakete müssen Sie nachinstallieren. Die zugehörigen Konfigurationsdateien `/etc/dnsmasq.d/usb0` und `/etc/radvd.conf` finden Sie ebenfalls im Download-Bereich. Da sich der VPiN als NAT-Router ins Firmennetz einbuchen soll, fehlen noch die Weiterleitungs- und MasqueradingEinstellungen. Dazu bearbeiten Sie die Datei `/etc/sysctl.conf` und fügen dort folgende Zeilen ein:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

Außerdem installieren Sie das Paket `iptables-persistent`, lassen die aktuellen Regeln jedoch nicht speichern – stattdessen kopieren Sie die Dateien `rules.v4` und `rules.v6`, die wir bereitgestellt haben, in das Verzeichnis `/etc/iptables-persistent`.

Geheimniskrämer

Die Einrichtung von Wireguard auf dem Raspi setzt voraus, dass Sie bereits einen entsprechenden Server als Gegenstelle aufgesetzt haben. Dabei orientieren sich die nachfolgenden Beispiele und Kommandos an dem in [3] beschriebenen Setup: Als Subnetze für das VPN dienen 192.168.24.0/24 respektive fd00:42::0/64, der Wireguard-Server hat die IP-Adresse 192.168.24.1 und der erste Client erhält die Adresse 192.168.24.100. Außerdem benötigen Sie den Public Key des Servers und den Private Key des Clients – wie Sie diese erzeugen und abrufen, ist ebenfalls in [3] genau beschrieben.

Bei Redaktionsschluss gab es Wireguard noch nicht in den Standard-Repositories von Raspberry

Pi OS, weshalb Sie sich die Pakete aus dem Debian-Backports-Repository besorgen müssen. Dazu legen Sie als Root im Verzeichnis `/etc/apt/sources.list.d` die Datei `backports.list` an und tragen dort folgende Zeile ein:

```
deb http://httpredir.debian.org/↵
↳debian buster-backports main contrib non-free
```

Damit Apt die Echtheit der Debian-Pakete verifizieren kann, müssen Sie außerdem die Debian-Schlüssel importieren:

```
apt-key adv \
--keyserver keyserver.ubuntu.com \
--recv-keys 04EE7237B7D453EC \
648ACFD622F3D138
```

Danach aktualisieren Sie die Paketlisten und installieren anschließend das Paket `wireguard-tools`.

Unter ct.de/w7t6 finden Sie ein Template für die Datei `/etc/wireguard/wg0.conf`, in der Sie die Schlüssel von Client und Server sowie Hostnamen und Port des VPN-Servers nachtragen müssen. Sie sollten außerdem die DNS-Einstellungen anpassen und dort den internen DNS Ihres Unternehmens eintragen, damit die Mitarbeiter etwaige Intranet-Dienste und -Server wie gewohnt ansprechen können. Der Dateiname `wg0.conf` ist übrigens mit Bedacht gewählt: So heißt das zugehörige Netzwerk-Device später ebenfalls `wg0`. Auch das Skript `wg-quick`, das die VPN-Verbindung auf- und abbaut, nutzt den Dateinamen ohne Erweiterung, um die Konfigurationsdatei zu finden.

Für den automatischen Aufbau der VPN-Verbindung nach dem Start haben wir uns für einen Systemd-Service entschieden, der den Tunnel 30 Sekunden nach Aufbau der Internetverbindung per `wg-quick` aufbaut. Kopieren Sie die heruntergeladene Datei `wgtunnel.service` nach `/etc/systemd/system` und aktivieren Sie den Dienst:

```
systemctl enable wgtunnel
```

Die Karenzzeit ist erforderlich, weil das Systemd-Target `network-online.target` unmittelbar dann ausgelöst wird, wenn eine Netzwerkverbindung steht – ohne zu prüfen, ob es sich tatsächlich um eine funktionierende Internetverbindung handelt. Ohne die Verzögerung hatten wir häufig den Fall, dass Wireguard den Namen des VPN-Servers im ersten Anlauf nicht auflösen konnte. Da `wg-quick` auch dann alle Daten inklusive Namensauflösung auf den Tunnel umlenkt, wenn der Tunnel noch gar nicht steht, scheitern alle weiteren Versuche, die IP-Adresse des VPN-Servers zu ermitteln. Die Alternative wäre, die Clients mit einer statischen IP-Adresse zu konfigurieren oder auf `wg-quick` zu verzichten und das Routing sowie die Paketweiterleitung durch den VPN-Tunnel manuell zu konfigurieren.

Ins Netz gegangen

Ideal ist es, wenn der Arbeitsrechner per Ethernet vernetzt ist. Dann muss man lediglich das Ethernet-Kabel des Rechners an den Raspi anschließen und den Raspi per USB mit dem Arbeitsrechner verbinden. Schon arbeitet der VPiN als transparenter USB-Netzwerkadapter. Unter Windows müssen Sie zuvor den Android-Treiber von Samsung installieren, der auf ct.de/w7t6 verlinkt ist.

Die WLAN-Konfiguration ist komplizierter und birgt mehr Fehlerquellen. Beispielsweise ist es wichtig, dass die Anwender die Verbindung zum heimischen WLAN abschalten, bevor sie den VPiN anschließen, weil es andernfalls zu Komplikationen beim Routing kommen kann. Außerdem sollen VPN-Nutzer ihr privates WLAN-Passwort nicht an die Admins im Betrieb weitergeben müssen. Voraussetzung dafür ist aber, dass die Admins vorab etwa per `raspi-config` die Ländereinstellung vorgenommen oder diese Einstellung manuell in der Datei `/etc/wpa_supplicant/wpa_supplicant.conf` eingetragen haben.

Damit Anwender das WLAN selbst konfigurieren können, haben wir Ihnen das Shell-Skript `wlansetup` mit Textmenüs auf Basis von `dialog` zum Download bereitgestellt. Es dient als Standard-Shell für den neu anzulegenden Benutzer `wlan`. Anwender müssen sich dann nur noch per SSH, etwa mittels PuTTY unter Windows, auf der IP-Adresse 192.168.255.1 einloggen und dem Dialog folgen – anschließend startet der VPiN neu und arbeitet dann als VPN-Router.

Das Paket `dialog` gehört unter Raspberry Pi OS nicht zur Standardinstallation, weshalb Sie es nachinstallieren müssen. Außerdem haben wir die WLAN-Konfiguration auf mehrere Skripte aufgeteilt, damit `wlansetup` nicht mit Root-Rechten arbeiten muss. Konkret müssen Sie neben `wlansetup` noch die Skripte `wlanadd` und `wlanremove` installieren sowie die Sudo-Konfiguration `sudowlan` unter `/etc/sudoers.d` ablegen, damit der Benutzer `wlan` die nötigen Rechte für die WLAN-Konfiguration erhält. Anschließend legen Sie den Benutzer `wlan` an und setzen ein Login-

Damit niemand sein privates WLAN-Passwort an die Admins der Firma herausgeben muss, erfolgt die WLAN-Einrichtung via SSH über ein einfaches Textmenü durch die Anwender selbst.



Passwort, das Sie später an den Anwender weitergeben müssen:

```
useradd -d /tmp -g nogroup \
-M -N -s /usr/local/bin/wlansetup \
-u 999 wlan
passwd wlan
```

Das WLAN-Setup-Skript ist einfach gehalten. Es sucht per `iwlist wlan0 scan` nach drahtlosen Netzen und bietet sie als Liste zur Auswahl an. Anschließend erfragt es das Passwort und hängt die Daten an die Datei `/etc/wpa_supplicant/wpa_supplicant.conf` an. Anschließend erfolgt ein `reboot`. Außerdem bietet das Skript an, eine WLAN-Konfiguration wieder zu löschen, wobei dann sämtliche `network`-Blöcke aus der Datei `wpa_supplicant.conf` entfernt werden – auf diese Weise lässt sich jederzeit auf Ethernet-Betrieb zurückschalten, ohne dass Konflikte mit einer fortbestehenden WLAN-Verbindung entstehen.

Unkaputtbar

Ein großes Problem von Raspi-Appliances ist, dass das Dateisystem auf der MicroSD-Karte schnell kaputt geht, wenn man den Mini-Rechner vor dem Ausschalten nicht ordentlich herunterfährt. Für einen Raspi als VPN-Dongle ist das ein Showstopper, würde es doch vom Anwender verlangen, den Raspi erst herunterzufahren, bevor er seinen Arbeitsrechner ausschaltet und so dem Raspi die Stromversorgung via USB kappt. Die Lösung ist, die Mount-Optionen des Root- und des Boot-Dateisystems auf Read-Only zu ändern und dem Linux-System eine Reihe von RAM-Disks bereitzustellen, damit es weiterhin die nötigen Dienste starten kann. Dazu tauschen Sie die Dateien `/boot/cmdline.txt` und `/etc/fstab` gegen die von uns zum Download bereitgestellten Versionen aus – booten aber noch nicht neu.

Damit Sie später bei Bedarf noch Änderungen am System vornehmen können, sollten Sie die Skripte `rw` und `ro` aus unserer Skriptesammlung installieren. Sie enthalten jeweils zwei `mount`-Aufrufe mit der Option `remount` für das Root- und das Boot-Dateisystem. Die Skripte sollten nur für den Root-Benutzer – respektive über `sudo` – ausführbar sein. Die Sudo-Konfiguration für den Benutzer `wlan` enthält bereits eine entsprechende Freigabe.

Bevor Sie neu starten und den Konfigurationsstand damit zementieren, müssen Sie unbedingt einen lokalen DNS-Resolver einrichten, der die `/etc/resolv.conf` dynamisch bereitstellt. Dazu installieren und aktivieren Sie den NetworkManager und, ganz entscheidend, legen den symbolischen Link für `resolv.conf` an:

```
apt-get install network-manager
systemctl enable \
--now NetworkManager
ln -sf /run/NetworkManager/\
resolv.conf /etc/resolv.conf
```

Der Standard-Resolver von Raspberry Pi OS hinterlegt den DNS-Server, den er etwa vom DHCP-Server mitgeteilt bekommt, nämlich direkt in der Datei `/etc/resolv.conf`. Ist das Root-Dateisystem und damit auch `/etc` nicht mehr beschreibbar, funktioniert das nicht mehr – der DNS bliebe dann auf ewig derjenige, den Sie bei der Einrichtung verwendet haben. Damit findet der VPiN den WireGuard-Server jedoch nicht, kann kein VPN aufbauen und ist somit nutzlos. Der NetworkManager hingegen arbeitet mit einem eigenen Resolver und speichert die DNS-Konfiguration in der Datei `resolv.conf` im Verzeichnis `/run/NetworkManager`, die künftig auf einer RAM-Disk liegt und dementsprechend weiterhin beschreibbar ist.

Fazit

Fertig konfiguriert und mit einem unkaputtbaren Dateisystem eignet sich der VPiN bestens, um auch Anwendern ohne Vorkenntnisse Zugang zum Firmennetz zu verschaffen – einfach, indem sie Ihr Netzwerkkabel vom PC an den Raspi umstecken und den Raspi am Arbeitsrechner anschließen. Die automatische Weiterleitung des gesamten Netzwerkverkehrs ins Firmennetz bringt einen großen Sicherheitsgewinn, da die Arbeitsplatzrechner im Homeoffice so vollständig vom potenziell unsicheren heimischen Netz isoliert sind. (mid) c't

Literatur

[1] Thomas Koch und Mirko Dölle, **Voll aufgebohrt**, Raspberry Pi 4 ausnutzen, c't Raspi 2020, S. 68

[2] Thomas Koch und Mirko Dölle, **Neue beste Freunde**, Raspberry Pi 4 am iPad Pro, c't Raspi 2020, S. 74

[3] Peter Siering, **Schutz ausrollen**, VPN-Server mit dem Raspi, c't Raspi 2020, S. 100

Skripte und Konfigurationsdateien

ct.de/w7t6

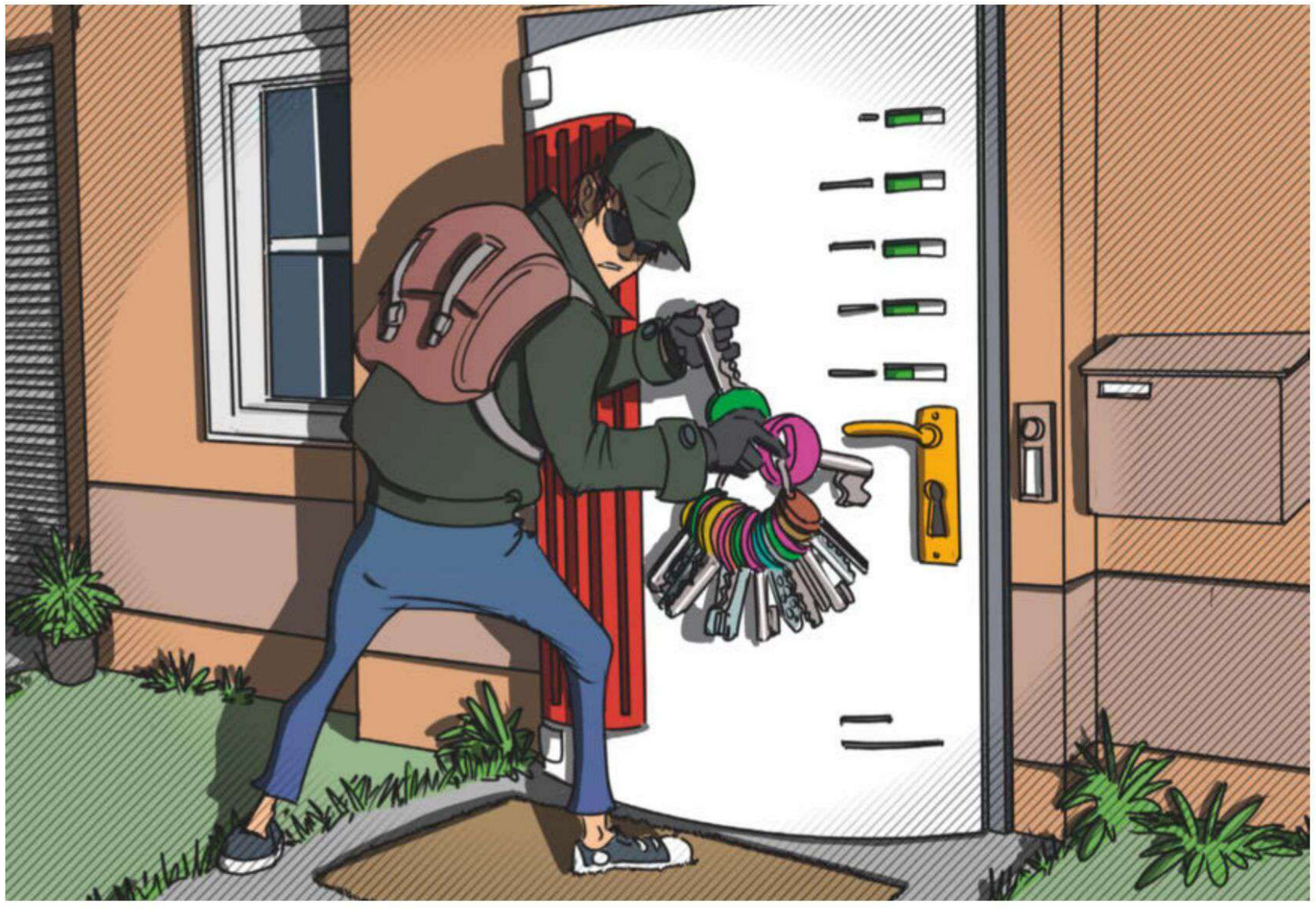


Bild: Thorsten Hübner

Fritzboxen sicher betreiben

Gescheiterte Anmeldeversuche am Webinterface der Fritzbox zeigen, dass Cyber-Schurken massenhaft versuchen, die Kontrolle über schlecht gesicherte AVM-Router zu übernehmen. Mit wenigen Handgriffen schützen Sie sich vor diesen und weiteren Angriffen.

Von **Ronald Eikenberg**

Mit zunehmender Häufigkeit erreichen uns Zuschriften von Lesern, denen beunruhigende Aktivitäten im Ereignis-Log Ihrer Fritzboxen auffallen. Ein zufälliges ausgewähltes Beispiel: „Seit drei Tagen sind in der Logdatei meiner Fritzbox vermehrt Einbruchversuche von der IP-Adresse 185.232.52.55 zu verzeichnen. […] Auch wenn ich ein starkes Passwort einsetze, ist es doch ein komisches Gefühl.“ Unbekannte versuchen demnach, sich am Webinterface der Fritzboxen anzumelden – und das immer wieder, oft über einen langen Zeitraum. Häufig gehen diese Anmeldeversuch von

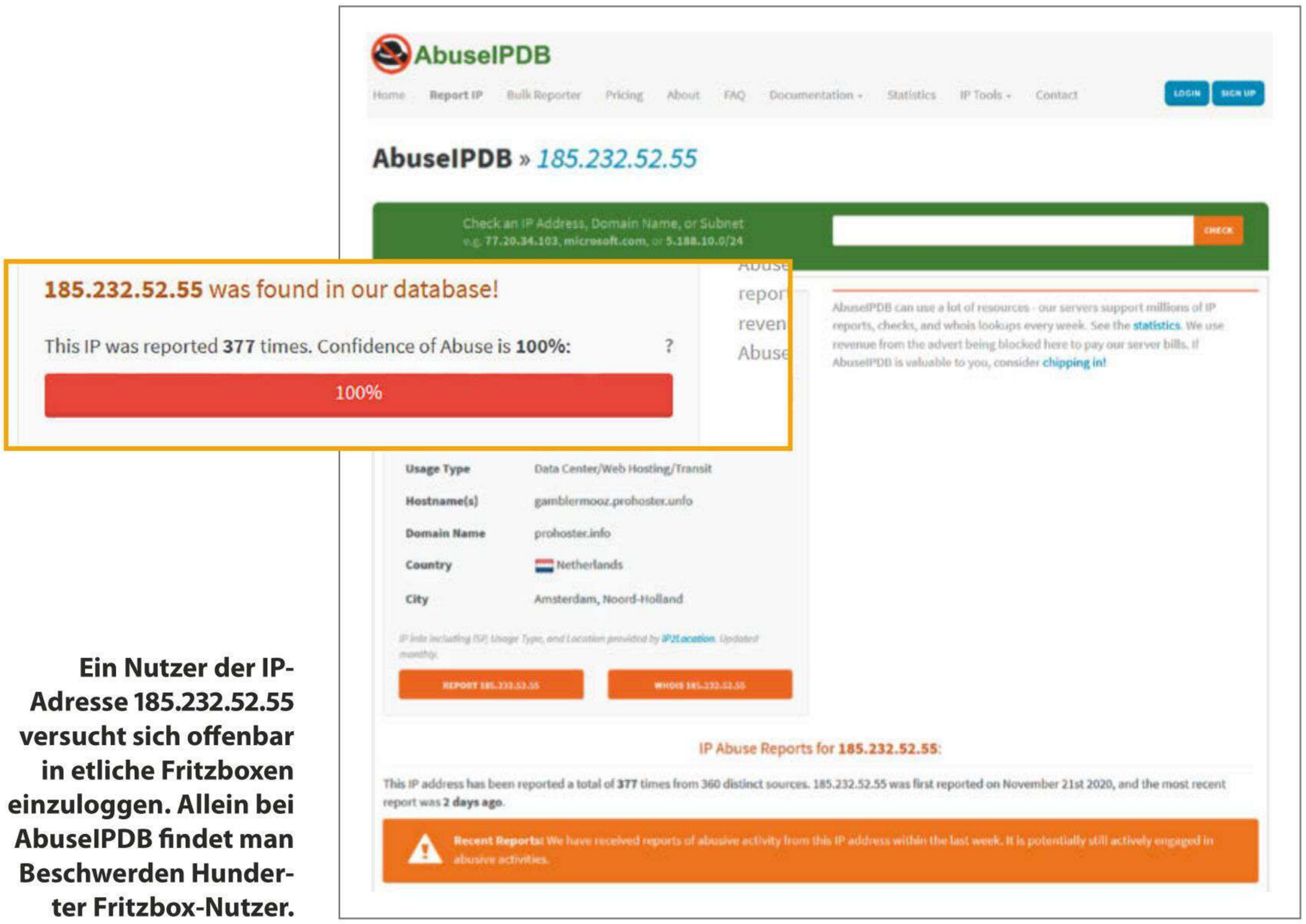
der gleichen IP-Adresse aus, bei mehreren Lesern versuchte sich etwa ein Nutzer der IP-Adresse 185.232.52.55 etliche Male einzuloggen.

Gibt man diese Adresse bei Google ein, landet man schnell bei AbuseIPDB, einer Website, auf der man IP-Adressen melden kann, die sich auffällig verhalten. Zu 185.232.52.55 findet man dort bereits Hunderte Beschwerden. Die meisten kommen von Nutzern aus Deutschland und betreffen Vorkommnisse der Kategorien Hacking und Brute-Force. Zumeist wird die Fritzbox als Angriffsziel genannt. Recherchiert man weiter, zeigt sich auffälliges Verhalten, das von der IP-Adresse bereits seit Sommer 2020 ausgeht und AVM-Router zum Ziel hat.

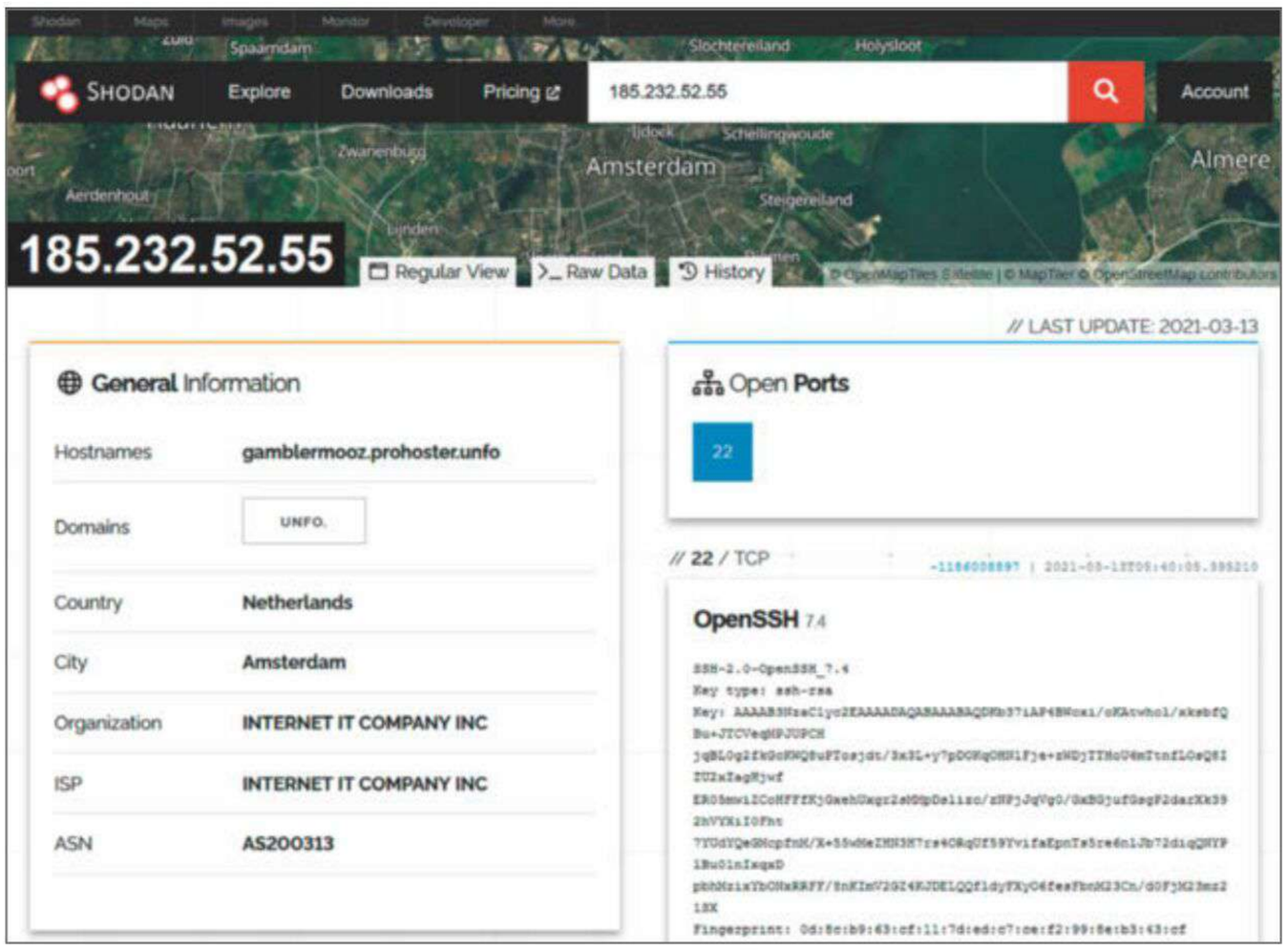
Aber wer steckt dahinter? Laut einer Whois-Abfrage gehört die IP-Adresse zu einem Unternehmen namens „Internet IT Company Inc.“, das offenbar auf den Seychellen angemeldet wurde. Als Abuse-Kontakt ist eine Freemail-Adresse bei Yandex.ru angegeben – nicht gerade vertrauenerweckend. Etwas mehr verrät der Portscan-Dienst Shodan: Er verortet die Adresse in Amsterdam und ordnet ihr die Domain gamblermooz.prohoster.unfo zu.

Laut Shodan ist unter der IP-Adresse lediglich ein OpenSSH-Server erreichbar. Das spricht dafür, dass dahinter nicht etwa ein infizierter Desktop-Rechner steckt, sondern eher ein Serversystem in einem Rechenzentrum. Da die OpenSSH-Version mit 7.4 reichlich alt ist und Sicherheitslücken enthält, erscheint denkbar, dass es sich um einen vergessenen Server-Zombie handelt, der übernommen wurde und nun fremdgesteuert wird.

Wer auch immer dahintersteckt, man muss davon ausgehen, dass er keine redlichen Absichten hegt. Denn eine Fritzbox ist ein hochattraktives Angriffsziel. Die Täter gehen bei der Wahl ihrer potenziellen Opfer anscheinend wahllos vor; vermutlich scannen sie stumpf weite Teile des deutschen Internets nach Fritzboxen, deren Webinterface von außen erreichbar ist. Offenbar haben es die Angreifer vornehmlich auf den HTTPS-Standardport 443 abgesehen. Als Benutzernamen probieren sie unter anderem zahl-



Ein Nutzer der IP-Adresse 185.232.52.55 versucht sich offenbar in etliche Fritzboxen einzuloggen. Allein bei AbuseIPDB findet man Beschwerden Hunderter Fritzbox-Nutzer.



Der Internetscanner Shodan vermutet hinter den Angriffen einen Server aus Amsterdam.

lose Mailadressen durch, meist mit .de-Endung. In einem uns bekannten Fall geht aus dem Ereignisbericht der Fritzbox hervor, dass eine Liste mit Mailadressen deutscher Kleinunternehmer zum Einsatz kam (kontakt@[domain].de). Unklar bleibt, ob die Adressen aus öffentlichen Quellen stammen oder irgendwo mit dazu passenden Passwörtern entwendet wurden.

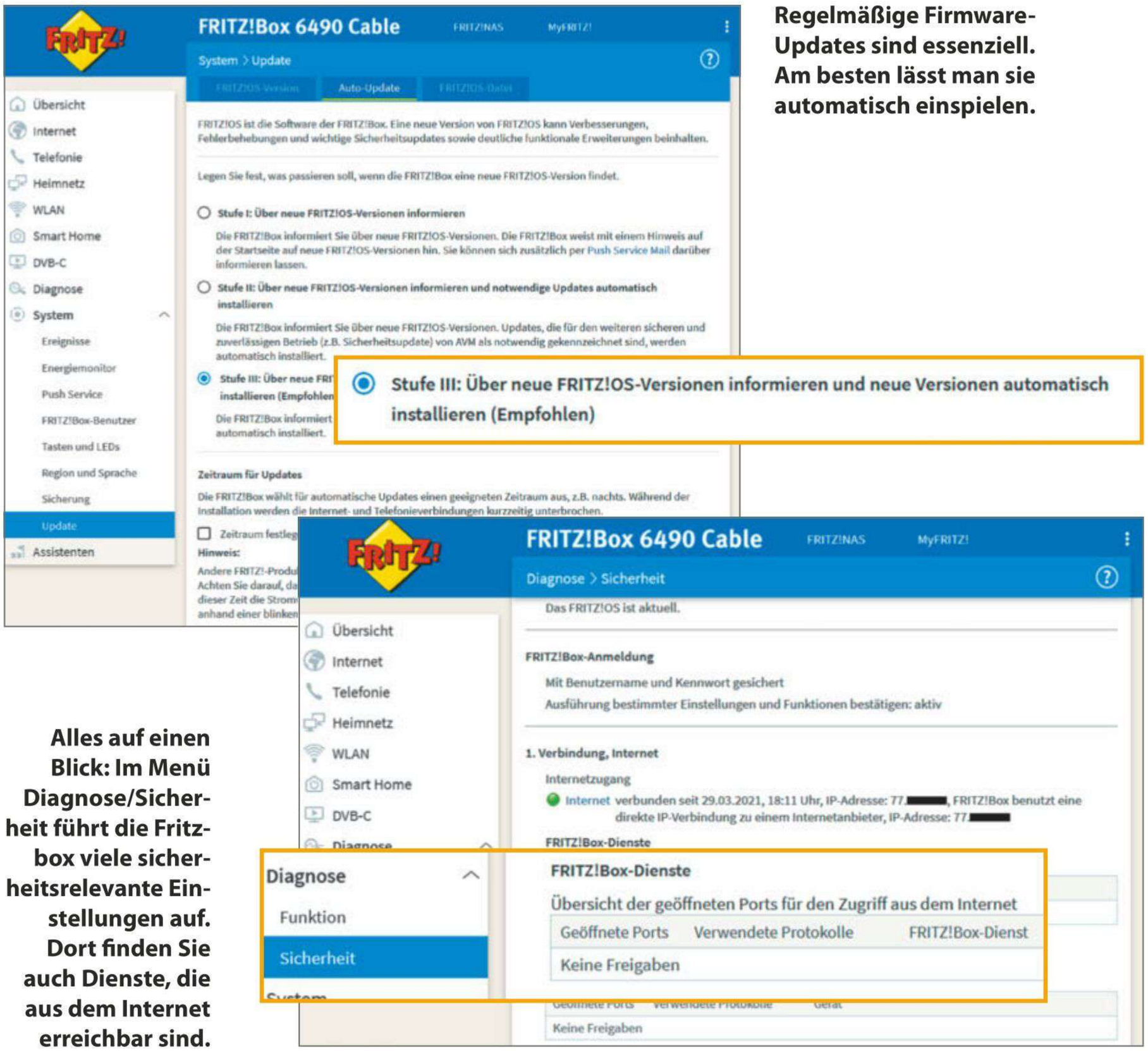
Wer solche Login-Versuche in seinem Fritzbox-Log entdeckt, sollte nicht gleich in Panik verfallen. Es handelt sich erst mal nur um gescheiterte Anmeldungen. Die Situation ist vergleichbar mit einem Einbruchsversuch, bei dem ein Angreifer vor Ihrer Haustür steht und auf gut Glück einen großen Bund mit Schlüsseln durchprobiert. Passt keiner der vielen Schlüssel, zieht der Möchtegern-Einbrecher unverrichteter Dinge weiter. Das ist ohne jede Frage unangenehm, doch noch nicht gefährlich – schließlich bleibt in diesem Fall die Haustür verschlossen.

Einbruchschutz

Damit das auch so bleibt, sollten Sie die Einbruchsversuche zum Anlass nehmen, Ihr Schutzkonzept zu überprüfen und zu verbessern. Denn spätestens, wenn der Einbrecher vor Ihrer Tür steht, kann man nicht mehr von einer theoretischen Gefahr sprechen. Sie ist sehr konkret. Im besten Fall sorgen Sie dafür, dass ein potenzieller Einbrecher das Login-Formular – und damit das gesamte Webinterface der Fritzbox – gar nicht erst erreichen kann. Wenn Sie ohnehin nicht von unterwegs auf Ihren Router oder dessen Dienste zugreifen, dann besteht kein Grund, ihn aus dem Internet erreichbar zu machen.

Bevor Sie mit dem Sicherheits-Check loslegen, sollten Sie sicherstellen, dass das Fundament stabil ist: Öffnen Sie die Weboberfläche des Routers, die Sie aus Ihrem Netz über http://fritz.box erreichen und stellen Sie im Menü System / Update sicher, dass die aktuelle Firmware (FritzOS) installiert ist. Klicken Sie unten rechts auf „Neues FRITZ!OS suchen“, um die Update-Suche anzustoßen. Falls es ein Update gibt, sollten Sie es gleich einspielen. Der Grund ist simpel: Firmware-Updates können nicht nur neue Funktionen und Bugfixes mitbringen, sondern auch Sicherheits-Patches, die Schwachstellen im Router-Betriebssystem beheben.

Statten Sie auch der Unterseite Auto-Update einen Besuch ab und aktivieren Sie mindestens die „Stufe II: Über neue FRITZ!OS-Versionen informieren und notwendige Updates automatisch installieren“, damit Ihr Router automatisch Updates einspielt, die der Hersteller als sicherheitsrelevant einstuft. Darunter können Sie bei „Zeitraum für Updates“ eine



Regelmäßige Firmware-Updates sind essenziell. Am besten lässt man sie automatisch einspielen.

Alles auf einen Blick: Im Menü Diagnose/Sicherheit führt die Fritzbox viele sicherheitsrelevante Einstellungen auf. Dort finden Sie auch Dienste, die aus dem Internet erreichbar sind.

Startzeit für die automatischen Updates einstellen, um sicherzustellen, dass Sie von den Aktualisierungen nicht tagsüber aus dem Videocall mit dem Chef gerissen werden.

Eine Übersicht der Firmware-Versionen für die aktuellen Fritzbox-Modelle finden Sie unter ct.de/wggy. Falls Sie den AVM-Router von Ihrem Provider erhalten haben, dann können Sie Firmware-Updates möglicherweise nicht selbst installieren. Dies ist beispielsweise bei den Providern von Internet per TV-Kabel der Fall. In diesem Fall können Sie nur abwarten, bis Ihr Provider das Update einspielt.

Wenn Ihr Fritzbox-Modell nicht länger mit Firmware-Updates versorgt wird, dann ist es schon recht alt. Denken Sie in diesem Fall über eine Neuanschaffung nach. Eine moderne Fritzbox ist dank der aktuellen Firmware nicht nur sicherer, sondern durch die neuere Hardware auch flotter. Es muss nicht zwangsläufig das aktuelle und teure Spitzenmodell sein. Je nach Anforderungen reicht auch das gebrauchte Top-Modell von vor zwei Jahren für einige Zeit aus.

Fenster und Türen verschließen

Steht das Firmware-Fundament, dann können Sie sich einen Überblick über die allgemeine Sicherheitslage verschaffen. Öffnen Sie im Webinterface

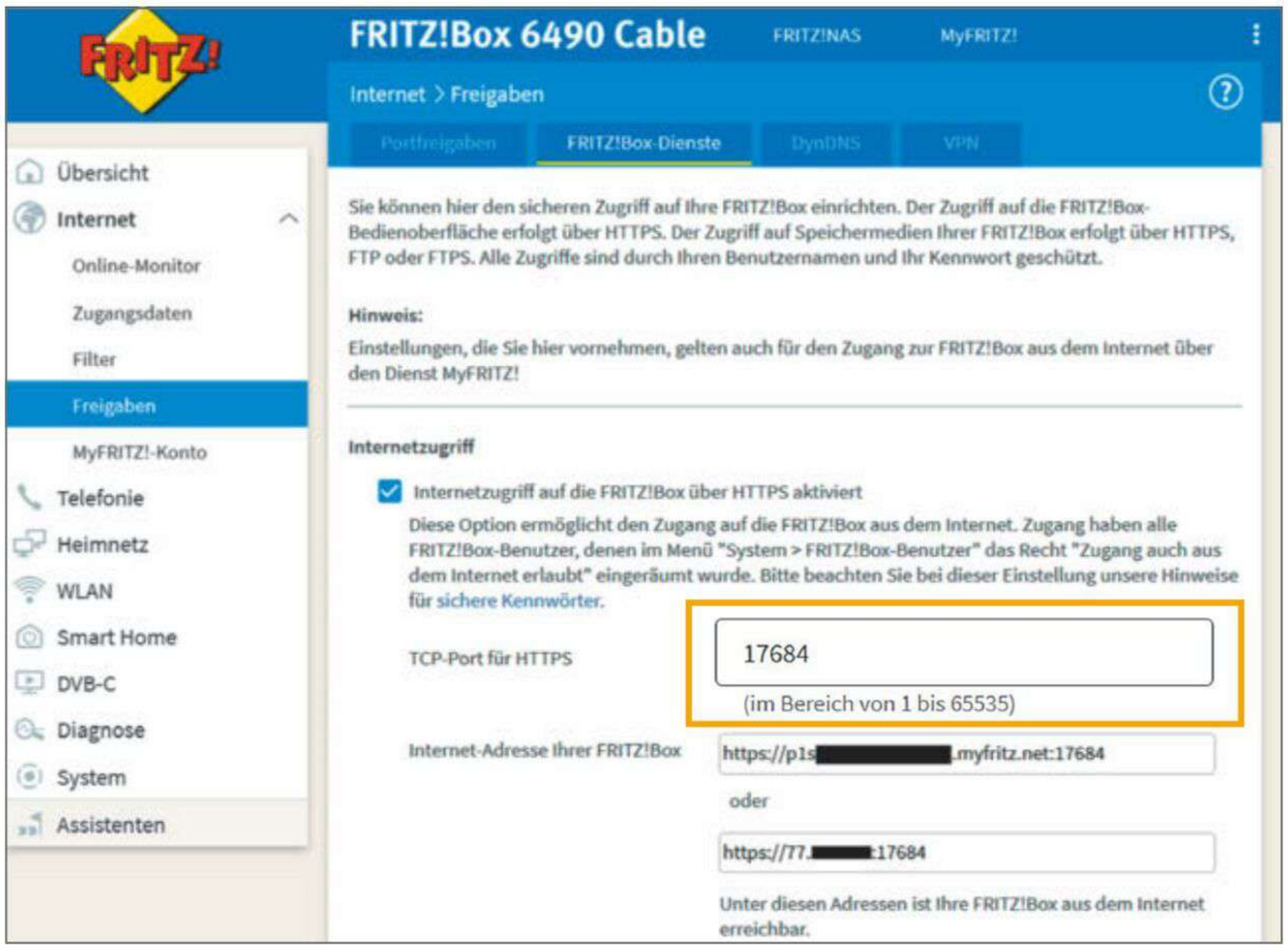
im Menü Diagnose / Sicherheit den Sicherheitsbericht, der die relevanten Einstellungen übersichtlich zusammenfasst. Die aus dem Internet erreichbaren Dienste finden Sie gleich oben, etwa unter „1. Verbindung, Internet“: Bei FRITZ!Box-Dienste führt der Router eigene Dienste auf, die für Zugriffe aus dem Internet erreichbar sind und unter „Portfreigaben auf Heimnetzgeräte“ erfahren Sie, welche Dienste anderer Geräte im Heimnetz von außen zugänglich sind.

Im Idealfall sind beide Listen leer, denn jeder öffentlich erreichbare Dienst ist ein Angriffsziel. Sind Dienste direkt aus dem Internet zugänglich, werden sie zwielichtige Gestalten eher früher als später attackieren, um etwaige Zugangsbeschränkungen wie Passwortabfragen zu brechen oder Sicherheitslücken auszunutzen. Schlimmstenfalls hat der Angreifer anschließend nicht nur den attackierten Dienst im Griff, sondern Ihr gesamtes Heimnetz.

Wenn Sie von unterwegs auf Ihr Heimnetz zugreifen möchten, nutzen Sie stattdessen besser eine verschlüsselte VPN-Verbindung [1]. Falls Sie doch einmal Dienste direkt von außen erreichbar machen wollen oder müssen, dann sollten Sie darauf achten, dass diese auf dem aktuellen Software-Stand sind und zudem auf eine sichere Authentifizierung setzen: starke, lange Passwörter sowie Zwei-Faktor-Authentifizierung, wenn möglich.

Falls Sie überflüssige Dienstefreigaben im Sicherheitsbericht der Fritzbox entdecken, sollten Sie diese im Menü Internet / Freigaben deaktivieren. Im Bereich Portfreigaben finden Sie die Weiterleitungen ins interne Netz und unter FRITZ!Box-Dienste die öffentlich erreichbaren Dienste der Fritzbox. Wenn Ihnen die eingangs beschriebenen Zugriffsversuche im Ereignis-Log der Fritzbox (System / Ereignisse) aufgefallen sind, dann haben Sie das Webinterface und / oder den FTP-Dateiserver des Routers für Zugriffe aus dem Internet freigegeben. Falls das unbeabsichtigt geschah, dann machen Sie es rückgängig, indem Sie bei den Fritzbox-Diensten im Bereich Internetzugriff die Häkchen bei „Internetzugriff auf die FRITZ!Box über HTTPS aktiviert“ und „Internetzugriff auf Ihre Speichermedien über FTP / FTPS aktiviert“ entfernen und die Konfigurationsänderungen übernehmen.

Falls Sie auf einen oder beide Dienste nicht verzichten können, sollten Sie zumindest sicherstellen, dass nicht die Standardports 443 für HTTPS und 21 für FTP eingestellt sind. Damit verhindern Sie die unbefugten Zugriffsversuche zwar nicht, sie werden aber seltener, da Angreifer häufig nur die Standardports abklopfen – das aber bei sehr vielen IP-Adressen. Nur wenn es jemand wirklich auf Sie abgesehen hat, wird er sich die Mühe machen, andere Ports zu scannen, etwa solche im fünfstelligen Bereich.



Ändert man die Ports der Fritzbox-Dienste auf hohe, zufällig gewählte, klopft ungebetener Besuch deutlich seltener an.

Der Portbereich reicht bis 65535. Seit FritzOS 7.10 schlägt die Fritzbox automatisch einen zufälligen Port für HTTPS vor, wenn Sie den Fernzugriff aktivieren. Überprüfen Sie die Einstellung insbesondere dann, wenn die Funktion schon längere Zeit aktiv ist oder gar noch eine ältere FritzOS-Version läuft. Um Angreifern das Auffinden offener Ports nicht leichter als nötig zu machen, sollten Sie in Internet / Filter / Listen / Globale Filtereinstellungen die Option „Firewall im Stealth Mode“ einschalten. Das erschwert den Angreifern die erforderlichen Portscans sehr, weil die Fritzbox nun nicht mehr mit einem Lebenszeichen reagiert (Zugriff verweigert), sondern stumm bleibt.

Sicherheitsschloss installieren

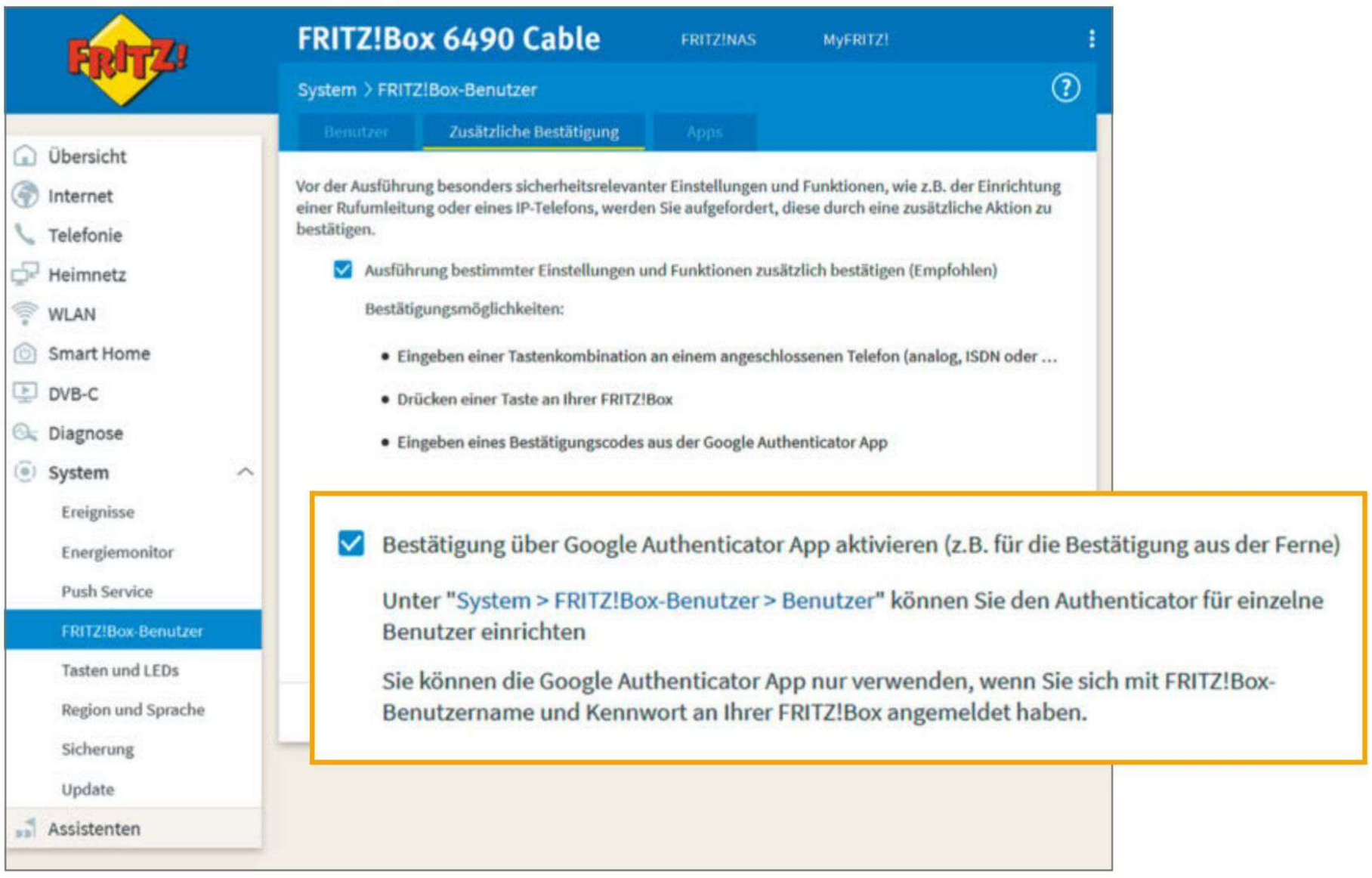
Falls ein Angreifer das Webinterface auf dem exotischen Port entdeckt, wird er mit einem Login-Dialog konfrontiert, in das er einen Benutzernamen und ein Passwort eingeben muss. Nur wenn beide Angaben stimmen, bekommt er Zugang zur Fritzbox.

Machen Sie es ihm so schwer wie möglich, indem Sie sowohl einen individuellen, schwer zu erratenden Usernamen als auch ein sicheres Passwort einstellen. Wechseln Sie hierzu in das Menü System / FRITZ!Box-Benutzer. Anschließend können Sie einen Benutzereintrag ändern oder einen neuen anlegen. Sowohl beim Benutzernamen als auch beim Kennwort können Sie Ihrer Kreativität freien Lauf lassen – je länger, desto besser. Wichtig ist nur, dass Sie die korrekte Zeichenfolge beim späteren Fernzugriff auf die Fritzbox parat haben. Der Einsatz einer Gedächtnisstütze ist ratsam, etwa in Form eines Passwortmanagers oder eines Zettels im Portemonnaie.

Gehen Sie alle angelegten Benutzer durch und misten Sie gründlich aus. Das Häkchen bei „Zugang auch aus dem Internet erlaubt“ sollte, wenn überhaupt, nur bei Konten mit individuellem Benutzernamen und starkem Passwort gesetzt sein. Bei dieser Gelegenheit sollten Sie auch die Berechtigungen überprüfen. Es ist eine gute Idee, den Nutzern nur jene Berechtigungen zu erteilen, die sie wirklich brauchen und alle übrigen Rechte zu entziehen. Sinnvoll ist auch, mit mehreren Konten für verschiedene Zwecke zu arbeiten: So muss etwa der Nutzereintrag, mit dem Sie auf den Netzwerkspeicher der Fritzbox zugreifen, nicht gleichzeitig die Router-Einstellungen ändern dürfen.

Stellen Sie auf der Unterseite „Zusätzliche Bestätigung“ sicher, dass die Option „Ausführung bestimmter Einstellungen und Funktionen zusätzlich bestätigen (Empfohlen)“ eingeschaltet ist. Dann müssen Sie beim Ändern folgenreicher Einstellungen gesondert bestätigen, dass Sie vor Ort und somit wahrscheinlich dazu berechtigt sind. Hierzu drücken Sie einfach eine Taste am Router oder tippen einen vorgegebenen Code ins Festnetztelefon ein.

Recht neu ist die Möglichkeit, wichtige Änderungen aus der Ferne zu bestätigen. Das ist sehr nützlich, wenn Sie die Router-Konfiguration von unterwegs ändern möchten. Hierzu setzt AVM auf das bewährte OTP-Verfahren (One Time Password): Sie verknüpfen einen OTP-Generator wie die Google-Authenticator-App oder andOTP per QR-Code-Scan mit der Fritzbox und können anschließend kurz gültige Einmalcodes generieren, mit denen Sie sicherheitskritische Einstellungen aus der Ferne ändern dürfen. Der Einmalcode ersetzt den Knopfdruck am Router. Leider ist es noch nicht möglich, schon das



Zum Ändern wichtiger Einstellungen, etwa von Rufumleitungen, sollte eine zusätzliche Bestätigung erforderlich sein – etwa durch das Drücken einer Taste am Router oder per OTP-App.



Hinter dem Push-Service Änderungsnotiz verbirgt sich eine äußerst nützliche Benachrichtigungsfunktion, die den Fritzbox-Besitzer per Mail über sicherheitsrelevante Änderungen an den Einstellungen sowie über Anmeldungen an der Bedienoberfläche informiert.

Einloggen am Webinterface der Fritzbox mit diesem Zweitfaktor zu schützen.

Wenn Sie schon mal den Bereich FRITZ!Box-Benutzer offen haben, sollten Sie dort im Bereich Apps nicht länger genutzten Anwendungen die Zugriffsrechte entziehen. Klicken Sie dazu neben einem Eintrag auf das rote X.

Alarmanlage scharfschalten

Um über verdächtige Aktivitäten auf dem Laufenden zu bleiben, sollten Sie von Zeit zu Zeit das Ereignis-Log im Menü System/Ereignisse kontrollieren. Setzen Sie den Filter oben auf System, um Anmeldeversuche an den Fritzbox-Diensten zu inspizieren; mit dem Filter Alle bekommen Sie unter anderem auch WLAN-Anmeldeversuche mit.

Über System / Push Service kann die Fritzbox per Mail über diverse Ereignisse informieren. Sie müssen zunächst unter Absender ein Mailkonto konfigurieren, das die Fritzbox zum Versand nutzen soll. Legen Sie für diesen Zweck am besten ein separates Konto an, damit Sie nicht das Kennwort Ihres primär genutzten Mailzugangs in der Fritzbox hinterlegen müssen. Schalten Sie dann den Push-Service Änderungsnotiz ein und abonnieren Sie „Über Anmeldungen an der Benutzeroberfläche informieren“, um keine erfolgreiche Anmeldung zu verpassen. Stöbern Sie nach weiteren Ereignissen, die Sie interessieren – Ihre Fritzbox kann Sie per Mail zum Beispiel auch über die Verfügbarkeit neuer Firmware benachrichtigen.

Netzwerkcheck

Um den Erfolg der getroffenen Schutzmaßnahmen zu überprüfen, können Sie zum Beispiel den Netzwerkcheck von heise Security benutzen (siehe ct.de/wggy): Er scannt Ihre aktuelle Internet-IPv4-Adresse nach offenen Standard-Ports und warnt, sollte er fündig werden. Damit versetzen Sie sich in die Perspektive eines Angreifers, der nach Schlupflöchern sucht. Wenn Sie alle Dienste nach außen gekappt haben, sollte der Netzwerkcheck keine oder nur sehr wenige Ports entdecken. Es gibt wenige Ports, die die Fritzbox selbstständig nach außen offenhält, damit Router-eigene Dienste wie die VoIP-Telefonie laufen. Laut AVM-Dokumentation sind dies: TCP-Port 21 (FTP/FTPS), TCP-Port 443 (Fernzugriff auf Weboberfläche, wenn mit alter FritzOS-Version aktiviert), UDP-Port 500 und 4500 (VPN), TCP- und UDP-Port 5060 (VoIP), UDP-Port 7078-7109 (VoIP) sowie TCP-Port 8089 (TR-069).

Sollten diese Ports in den Ergebnissen des Netzwerkchecks stehen, gibt es dafür also einen guten Grund. Die ersten Ports für FTP(S), Weboberfläche und VPN stehen dort nur, wenn Sie die zugehörigen Fritzbox-Funktionen aktiviert haben, die Telefonie-Ports nur, wenn VoIP eingerichtet ist. Beachten Sie, dass der Netzwerkcheck von heise Security derzeit nur IPv4-Adressen abklappert. Bei Fritzboxen darf man davon ausgehen, dass die Ergebnisse auch für deren aktuelle globale IPv6-Adresse gelten.

Ungebetene Besucher aus dem Internet sind nicht nur eine Gefahr, vor der Sie Ihren Router schützen müssen. Auch die Funkstrecke muss abgesichert

Perspektivwechsel: Mit dem Netzwerkcheck von heise Security begeben Sie sich in die Rolle eines Angreifers und überprüfen, ob Dienste über Ihre IPv4-Adresse auf den Standardports erreichbar sind.



werden, damit sich Ihre Nachbarn nicht in Ihrem Heimnetz umschauen oder ungefragt über Ihren Anschluss surfen und Dinge tun, für die später Sie den Kopf hinhalten müssen.

Die gute Nachricht ist, dass Sie damit nur wenig Arbeit haben. Stellen Sie unter WLAN / Sicherheit / WPA-Verschlüsselung am besten „WPA 2 + WPA3“ (WPA3-Mixed-Mode) ein, damit moderne Geräte, die bereits WPA3 verwenden, die bestmögliche Verschlüsselung einsetzen. Ältere Geräte wählen dann automatisch die WPA2-Verschlüsselung, die weiterhin ausreichend sicher ist. Wenn Sie diesen Modus wählen, sollte unter „Weitere Sicherheitseinstellungen“ die Option „Unterstützung für geschützte Anmeldungen von WLAN-Geräten (PMF) aktivieren“ aktiv sein. Einen ausführlichen Hintergrundartikel über die Vor- und Nachteile von WPA3 finden Sie ab Seite 60.

Einige alte Geräte haben im WPA3-Mixed-Mode möglicherweise Probleme mit dem Verbindungsauf-

Lernen Sie Ihre Box noch besser kennen



Stephan Brey
Mein Heimnetzwerk mit der FRITZ!Box
Alle Funktionen einer aktuellen FRITZ!Box, aufgebaut wie der Konfigurationsbereich der FRITZ!Box selbst: einfacher kann ein Ratgeber nicht sein! Internet, Telefon, Heimnetzwerk, WLAN, Selbsthilfe, Apps und Hacks.
ISBN 9783645606608
30,00 € ›



Wolfram Gieseke
Die ultimative FRITZ!Box-Bibel
Das umfassende Praxisbuch zu den AVM-Routern in der 4. aktualisierten Auflage, Juni 2021: alle aktuellen Geräte ausführlich dargestellt, Einrichtung, Konfiguration, Absicherung, Mesh-Verbindungen und vieles mehr.
ISBN 9783959822732
19,95 € ›

› 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
shop.heise.de/fritzbox ›

bau, zum Beispiel alte iPads, die Apple seit Jahren nicht mehr mit iOS-Updates versorgt. Statt für solche Problemfälle die Sicherheit Ihres Haupt-WLANs und damit aller Geräte zu reduzieren, können Sie einfach das Gastnetz der Fritzbox mit der Verschlüsselung WPA2 (CCMP) aufspannen und die betroffenen Geräte dort einbuchen. Sie finden es unter WLAN / Gastzugang. Das vom Hauptnetz separierte Gastnetz ist auch der richtige Ort für alle Clients, denen Sie nicht über den Weg trauen sowie für Ihre Gäste, denen Sie zwar Internetzugriff spendieren möchten, die aber nicht aufs Heimnetz zugreifen sollen.

Falls Sie das WLAN-Passwort aushändigen, sollten Sie es von Zeit zu Zeit ändern, um die Kontrolle über die Nutzung zu behalten. Unter „Weitere Einstellungen“ können Sie noch etwas Feintuning betreiben: Aktivieren Sie zum Beispiel den Push-Service, um ein Protokoll über die An- und Abmeldungen am Gastnetz per Mail zu erhalten. Unter „Geräte im Gastzugang oder Hotspot“ sollte die Option „WLAN-Geräte dürfen untereinander kommunizieren“ ausgeschaltet und „Internetanwendungen beschränken“ eingeschaltet sein, damit Ihre Gäste nur surfen und mailen können.

Nutzen Sie für Ihre Funknetze möglichst lange Passwörter (WLAN-Netzwerkschlüssel), um es Angreifern schwer zu machen. Das voreingestellte Passwort sollten Sie ändern, da es lediglich aus Ziffern besteht. Nutzen Sie einen mindestens 16 Zeichen langen Mix aus Groß- und Kleinbuchstaben sowie Ziffern. Durch den Einsatz von Sonderzeichen können Sie die Komplexität erhöhen.

Achten Sie jedoch darauf, dass Sie das Passwort auf allen Geräten gut eintippen können – auch mit der Fernbedienung des Smart-TV und dem Controller der Spielekonsole. Auf allzu exotische Sonderzeichen sollten Sie deshalb besser verzichten, machen Sie das Passwort stattdessen lieber etwas länger. Auch sich optisch ähnelnde Zeichen wie 1, l und I sowie 0 und O erhöhen lediglich das Frustrationspotenzial.

Das Gastnetz sollten Sie unbedingt mit einem anderen Passwort schützen als Ihr Hauptnetz. Darüber hinaus sollten Sie in WLAN / Sicherheit / WPS-Schnellverbindung die Komfortfunktion WPS (Wi-Fi Protected Setup) abschalten, da sich Ihre Gäste ansonsten einfach per Knopfdruck am Router mit Ihrem Hauptnetz verbinden und sogar dessen WLAN-Passwort einsehen können. Sie können die Funktion bei Bedarf vorübergehend wieder aktivieren, etwa wenn Sie neue Geräte mit dem Router verbinden möchten, ohne immer wieder das Passwort eingeben zu müssen.

Hintertüren absichern

Damit Ihr Schutzwall nicht gleich wieder eingerissen wird, sollten Sie abschließend noch einen Blick auf UPnP werfen: Über das UPnP-Protokoll können Geräte in Ihrem Heimnetz Ihre Fritzbox nicht nur finden, sondern auch umkonfigurieren. Das kann gefährlich werden: Wenn es ganz schlecht läuft, dann ist die neue WLAN-Kamera von Discounter nicht nur unsicher vorkonfiguriert, sie richtet sich über UPnP auch noch eine Portweiterleitung im Router ein. Dann ist sie fortan für die ganze Welt erreichbar und mit Pech auch noch als DDoS-Server und andere Angriffe dienstbar – ganz ohne Ihr Zutun.

In Heimnetz / Netzwerk / Netzwerkverbindungen spüren Sie Geräte auf, die via UPnP an der Fritzbox-Konfiguration schrauben dürfen. Klicken Sie bei Ihren Geräten auf das Stift-Symbol, um die jeweiligen Einstellungen zu öffnen. Hier sollte die Funktion „Selbstständige Portfreigaben für dieses Gerät erlauben“ ausgeschaltet sein, damit die Geräte nicht eigenmächtig Port-Weiterleitungen im Router einrichten. Unter Internet / Freigaben / Portfreigaben können Sie ganz unten über den Deaktivieren-Knopf die selbstständige Portfreigabe zudem für alle Geräte deaktivieren, die bisher keine Freigaben angelegt haben.

Falls Sie Ihre Fritzbox ausschließlich über das Webinterface konfigurieren und zudem keine AVM-Apps wie FRITZ!App Fon nutzen, können Sie unter „Heimnetz / Netzwerk / Netzwerkeinstellungen / weitere Einstellungen“ die Funktion „Zugriff für Anwendungen zulassen“ abschalten. Damit verhindern Sie, dass Ihre Fritzbox über das TR-064-Protokoll gesteuert wird. Da TR-064 eine Authentifizierung voraussetzt, ist das davon ausgehende Sicherheitsrisiko allerdings überschaubar, sofern Sie Ihre Fritzbox-Accounts mit starken Passwörtern schützen. Beachten Sie, dass Sie damit auch einige Drittanbieter-Apps und Skripte aussperren, welche die Box über TR-064 steuern.

Mehr Privatsphäre

Nicht nur in puncto Sicherheit können Sie bei der Fritzbox allerhand einstellen und optimieren, insbesondere beim Datenschutz hat sich jüngster Zeit viel getan. Beispielsweise haben wir ausführlich beschrieben, wie Sie mit der Fritzbox verschlüsselt über VoIP telefonieren (siehe S. 118) und Ihre Privatsphäre beim Surfen verbessern, indem Sie DNS-Anfragen verschlüsselt über DNS-over-TLS, kurz DoT, abwickeln (siehe S. 10). (rei) c't

Literatur

[1] Urs Mansmann, **Tunnel durchs Internet**, Mobile Geräte mit VPN sicher ins Netz bringen, c't 3/2016, S. 126

Firmware-Versionen & Netzwerkcheck

ct.de/wggy

Make: Projects

SMART HOME CHALLENGE

präsentiert von FRITZ!



DU HAST DAS SCHLAUESTE SMART HOME IM GANZEN LAND?

- Gestalte dein Smart Home
- Verknüpfe Sensoren und Aktoren
- Nutze WLAN zur Kommunikation
- **Gewinn:**
  10 x einen 500,- € Maker-Einkaufsgutschein!

Die ersten tollen Projekte wurden schon eingereicht.

MACHST DU AUCH MIT?!

makeprojects.com/de/smart-home-challenge

6 Router für Wi-Fi 6 im Test

Mit Wi-Fi 6 soll das WLAN reibungslos funken. Fünf Router der 150-Euro-Klasse zeigen im c't-Labor, wie flott sie Wi-Fi-6-Stationen bedienen, wo es noch hakt und wie weit sie hinter einem Gerät der Oberklasse zurückbleiben.

Von **Ernst Ahlers**

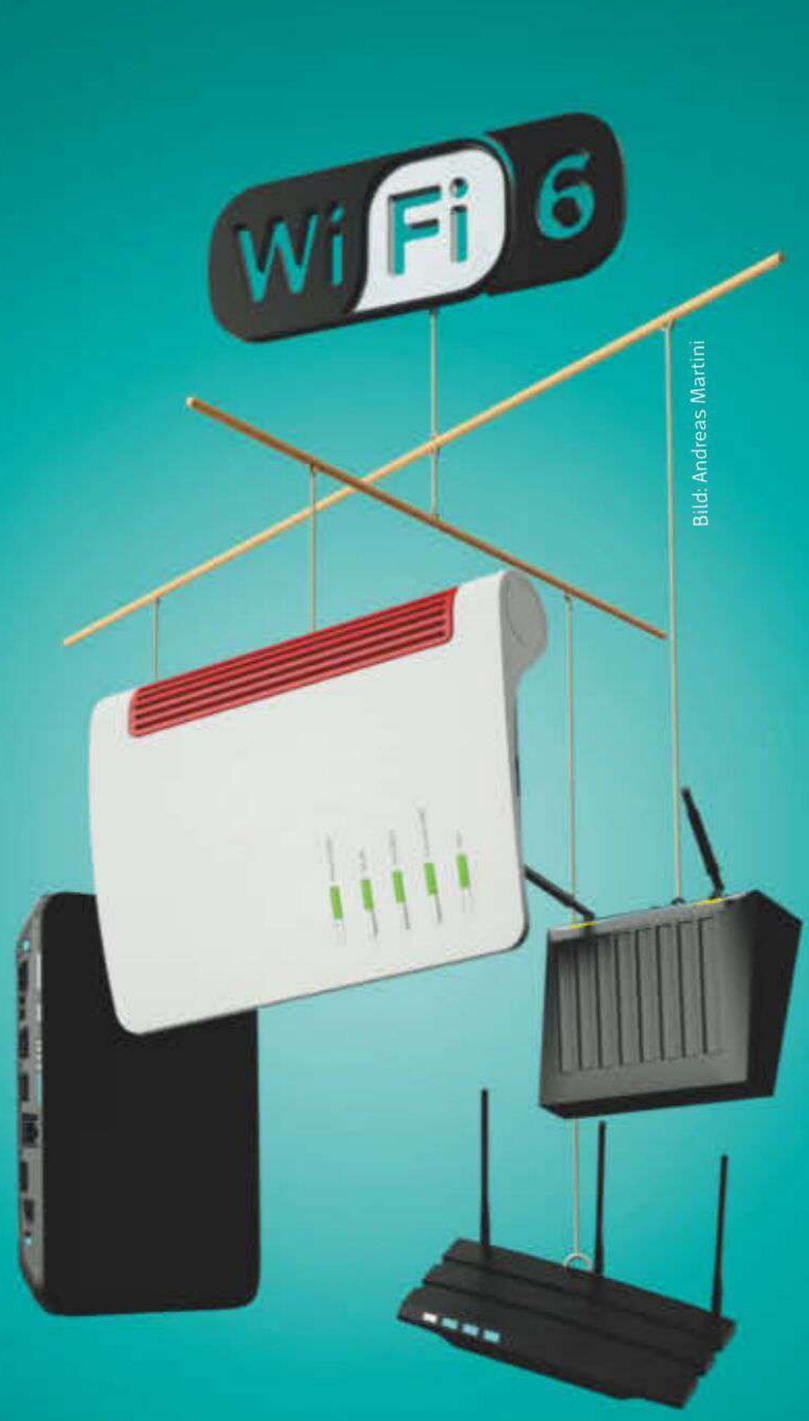


Bild: Andreas Martini

6 Router für Wi-Fi 6 im Test	50
Extrasicheres WLAN mit WPA3	60
AVM Fritz-Repeater 6000 mit Wi-Fi 6	66
Wie Wi-Fi 6 das WLAN beschleunigt	68

Wenn das WLAN beim Upgrade des Internetanschlusses nicht mehr mithalten kann, liegt der Griff zu einem neuen Router und damit zur jetzt aktuellen WLAN-Generation Wi-Fi 6 nahe. c't hat ein halbes Dutzend Geräte ins Labor gebeten, wobei wir für die Auswahl zwei Pflichtmerkmale setzten: DFS und WPA3. Nur mit Dynamic Frequency Selection – automatischem Kanalwechsel bei Radarerkennung – darf ein Router im 5-GHz-Band sämtliche Kanäle nutzen. So kann er Nachbar-WLANs besser ausweichen, was dem Durchsatz beider Netze zugutekommt.

Die WLAN-Verschlüsselung WPA3 (siehe S. 60) schützt WLAN-Clients besser als das alte WPA2, unter anderem mit Protected Management Frames (PMF) und Perfect Forward Secrecy (PFS). PMF verhindert, dass ein Angreifer Clients mit gefälschten Steuerpaketen von der Basis abmelden und auf einen eigenen Honeypot umleiten kann. PFS sorgt dafür, dass aufgezeichneter chiffrierter Verkehr auch mit Kenntnis des WLAN-Passworts nicht nachträglich entschlüsselt werden kann.

Die getesteten Router sollten höchstens 200 Euro kosten und Wi-Fi-6-WLAN (siehe S. 68) in beiden Funkbändern anbieten. Geräte, die DFS oder WPA3 nicht beherrschten, flogen aus dem Testfeld wieder heraus. Zuerst traf es den RAX40 von Netgear. Er konnte zwar DFS, scheiterte aber an WPA3. In den Versionshinweisen der bei Testbeginn aktuellen Firmware 1.0.3.88 fanden wir: „This firmware version does not support OFDMA, WPA3, and Smart Connect." Das kann man angesichts der auf dem Karton zugesagten OFDMA-Fähigkeit nur als enttäuschend bezeichnen. Der Edimax BR-6473AX und der TP-Link Archer AX50 mussten sich verabschieden, weil ihnen DFS *und* WPA3 fehlten.

So blieben fünf Router verschiedener Marken übrig. Vier davon sind Breitband-Router, die man an ein Modem anschließt. Die Fritzbox 7530 AX hat eines für Supervectoring-VDSL integriert. Dazu gesellt sich mit dem Speedport Pro Plus ein opulent ausgestattetes Gerät, das der Provider Deutsche Telekom anbietet. Es soll den Ausblick geben, was man für mehr Geld an Mehrwert bekommt. Schließlich haben wir zum Generationenvergleich noch einen älteren Router mitgemessen: Die Ergebnisse der Fritzbox 7580, unseres Referenzgerätes für Wi-Fi-5-Messungen mit Notebooks, sind im Balkendiagramm enthalten.

„Einfach nur Internet" erwies sich als leicht, das schafften alle, auch per PPPoE am Telekom-VDSL, wobei manche etwas Nachhilfe bei der VLAN-Konfiguration brauchten [1]. Spannend wird es bei weitergehenden Ansprüchen, etwa wenn man einen eigenen Cloud-Server wie das Familien-NAS per IPv4 und IPv6 aus dem Internet erreichbar machen will. Die dafür nötigen IPv6-Dienstfreigaben beherrschen längst nicht alle Router so sauber wie AVMs Fritzwboxen. Meist bleibt einem nur, die IPv6-Firewall ganz auszuschalten, falls das überhaupt geht; dann müssen sich aber alle (W)LAN-Hosts IPv6-seitig selbst schützen.

Setup-Hürdchen

Vor dem ungebremsten Surfspaß steht die Einrichtung. Bei der Konfiguration hilft bei allen getesteten Routern ein Assistent im Browser, der aber leider

Wi-Fi-6-Router: Leistungswerte

	NAT-Durchsatz		WLAN-Durchsatz			
	PPPoE	IP/IP	2,4 GHz nah	20 Meter	5 GHz nah	20 Meter
	besser ▶	besser ▶	besser ▶	besser ▶	besser ▶	besser ▶
Asus RT-AX58U	904	950	332	305	737	347
AVM Fritzbox 7530AX	884	950	346	213	706	226
D-Link DIR-X1860	901	950	421	297	695	216
Huawei WiFi AX3 (WS7200)	187	948	382	276	893	283
Linksys MR7350	849	949	322	256	691	309
Telekom Speedport Pro Plus	nicht messbar	nicht unterstützt	403	322	898	371
AVM Fritzbox 7580[1]	**882**	**949**	**204**	**189**	**848**	**309**

alle Werte in MBit/s, NAT-Performance Downstream, WLAN gegen Intel AX200[1] zum Vergleich, [1] erst mit späterer Firmware (Asus), dann nur via Alexa oder Google-Assistant



Asus RT-AX58U

Asus' RT-AX58U ist vollgestopft mit Funktionen und mit vier Betriebsarten (Router, AP, Repeater, Bridge) flexibel einsetzbar. Aber hier und da gibts kleine Ungereimtheiten: Direkt via Modem am Telekom-VDSL in der WAN-Betriebsart PPPoE ließ sich das Multicast-IPTV zwar nutzen, in einer Kaskade mit DHCP als WAN-Protokoll hinter einer Fritzbox 7590 jedoch nicht.

Wem die anderen Asus-Spezialitäten (AiCloud für Fernzugriff auf Einstellungen und NAS-Funktion, Alexa / IFTTT-Einbindung, zwei VPN-Typen zur Wahl) wichtiger sind, wird über solch eine Macke hinwegsehen und sich über guten WLAN-Durchsatz freuen. Besuchergeräte sind dabei im Gastnetz ebenfalls per WPA2+3 schützbar.

- **guter WLAN-Durchsatz**
- **WPA2+3 fürs Gastnetz**
- **MC-IPTV nicht in allen Modi**



AVM Fritzbox 7530 AX

Erstaunlicherweise brachte AVM als xDSL-Erstling für Wi-Fi 6 keinen Nachfolger des Wi-Fi-5-Topmodells 7590 heraus, sondern dem Anschein nach eine aufgebohrte Variante von dessen kleiner Schwester 7530: ISDN-Fans werden den S0-Bus vermissen, NAS-Anwender einen USB-3.0-fähigen Port für den Massenspeicher.

Die erste Firmware des Neulings ist schon so weit gereift wie die der älteren Geschwister: Am Telekom-VDSL sind wie bei anderen Providern nur wenige Schritte nötig, bis das Internet inklusive IPv6 und dem optionalen Multicast-IPTV läuft. Dazu gibts die von AVM gewohnten Extras (siehe Tabelle auf Seite 56). Wer schon von Fritzboxen überzeugt ist, muss sich nun nur fragen: Warten auf die hypothetische „7690" oder schon jetzt zugreifen?

- **viele Funktionen**
- **reife Firmware**
- **durchschnittliches WLAN**

auch bei allen Geräten mehr oder weniger gravierende Lücken lässt. Beispielsweise sollte man stets das voreingestellte Konfigurationspasswort ändern, weil es bei den Geräten aufs Typenschild am Geräteboden oder unter einem Deckel gedruckt ist. Tut man das nicht, kann sich ein Besucher per Abfotografieren des Schildes und nach der bequemen WLAN-Kopplung per WPS-PBC – dazu gleich mehr – in der Routerkonfiguration umgucken. Wenigstens boten alle Router-Assistenten an, die voreingestellten WLAN-Zugangsdaten (Funknetzname und Passwort) zu ändern. Diese Gelegenheit sollte man ergreifen.

Auch auf weitere Einstellungen lohnt ein Blick, etwa auf die Konfiguration der Systemzeit, damit eventuell eingerichtete Internetsperren in beiden Halbjahren tatsächlich zu den vorgegebenen Zeitpunkten greifen. Das Aktivieren der „Airtime Fairness" sorgt dafür, dass auch ältere Clients besser bedient werden, wenn mehrere WLAN-Geräte gleichzeitig Daten empfangen, von denen einer eine besonders schwache Funkverbindung hat. Der wird



D-Link DIR-X1860

Mit dem DIR-X1860 hat D-Link einen Preiskracher im Sortiment. Viel günstiger kommt man zurzeit kaum an einen Wi-Fi-6-Router, aber dafür gibts auch nur eine Ausstattung mit dem Nötigsten und kleine Macken: Die WLAN-Kopplung per Tastendruck (WPS-PBC) scheiterte wiederholt mit unserem Testnotebook. Auf der Haben-Seite verbucht der DIR-X1860 die funktionierende IPv6-Präfixdelegation in sein (W)LAN, wodurch man Router nachschalten kann, die dann eigene IPv6-Subnetze aufspannen. Leider fanden wir hier weitere trübe Stellen: Im Gast-WLAN wurde IPv6 zwar angeboten, aber es führte nicht ins Internet. Das Live-TV per Multicast lief einwandfrei im 2,4-GHz-Band, eigenartigerweise aber nicht über 5 GHz. Solche Fehler hinterließen bei uns den Eindruck: nicht fertig entwickelt.

- **preisgünstig**
- **kann IPv6-Kaskadierung**
- **mehrere Firmware-Macken**



Huawei WiFi AX3 (WS7200)

Huaweis Router ist in zwei Varianten im Handel: Das Modell WS7100 hat einen etwas langsameren Prozessor und keine NFC-Kopplung, weswegen wir das WS7200 vorzogen. Sein Preis schwankt stark: Zeitweise wurde er über Amazon für 50 Euro feilgeboten, bei einer großen Elektronikkette waren zwischendurch 100 Euro fällig. Die NAT-Performance mit PPPoE fiel ungewöhnlich niedrig aus, vielleicht wegen unseres Messverfahrens. Denn über ein Modem am Supervectoring-Anschluss lieferte der Router die erwarteten 260 MBit/s; Huawei hat im Labor knapp 1000 MBit/s gemessen. Die Wi-Fi-6-Option TWT für verbessertes Energiemanagement in Mobilgeräten muss man per Hand aktivieren, ebenso den optionalen Betrieb mit einem 160 MHz breiten Signal (ax-2400 statt ax-1200).

- **WLAN-Kopplung per NFC**
- **guter Durchsatz**
- **Wi-Fi-6-Optionen ab Werk aus**

dann etwas ausgebremst, was die Nettodatenrate der besser angebundenen überproportional hebt.

Weitere Punkte, die Sie als Router-Admin prüfen sollten: Aktivieren der Mixed-Mode-Verschlüsselung WPA2+3, Einschalten von IPv6, Aktivieren des optionalen 160-MHz-Betriebs fürs WLAN, Konfigurieren des Gast-WLANs für Besucher. Diese Optionen per Browser zu überprüfen ist auch dann wichtig, wenn Sie den Router per Smartphone-App eingerichtet haben. Die Wartung per App ist zwar bequemer, aber der Funktionsumfang fällt je nach Modell größer oder kleiner aus; meist sieht man dort nicht alle Optionen.

WLAN-Sicherheit

Bietet ein Router WPA3 an, bedeutet das nicht automatisch, dass ein WPA3-fähiger Client auch immer eine WPA3-gesicherte Verbindung aufbaut: Bei der Kopplung per Tastendruck (WPS-PBC, Wi-Fi Protected Setup Push-Button Configuration) kam im Test immer nur ein WPA2-Link zustande. Erst nach manueller



Linksys MR7350

Die Belkin-Marke Linksys hat seit dem Wi-Fi-3-Urahn WRT54G, aus dem die quelloffene Firmware OpenWrt entstand, einen guten Klang. Leider kann sie mit dem Wi-Fi-6-Nachfolger MR7350 daran nicht anknüpfen, denn seine Firmware zeigte sich in Details noch unausgereift: IPv6 funktionierte am Telekom-VDSL erst, als wir die IPv6-Verbindungsart manuell auf PPPoE umstellten. Multicast-IPTV gabs zwar im LAN, aber im WLAN liefen die Streams nicht an. Im Gastnetz starteten sie hingegen und es wurde klar, wo es hakt: Dem Router fehlt die Multicast-to-Unicast-Umsetzung, wodurch die MC-Streams ruckeln und klötzeln. Hinter eine Fritzbox geschaltet reichte der MR7350 das Multicast-IPTV gar nicht weiter.

- **guter WLAN-Durchsatz**
- **IPv6 erst mit Nacharbeit**
- **untauglich für MC-IPTV**



Telekom Speedport Pro Plus

Seit Herbst 2020 besetzt der Speedport Pro Plus den Spitzenplatz im Telekom-Angebot: Mit vier Internetoptionen – Supervectoring-Modem, LTE-Funkmodul, SFP-Slot für Glasfasermodule, Ethernet-WAN-Port – ist er auf alle Eventualitäten vorbereitet, inklusive der Hybridzugänge, die in hauseigener Technik DSL und Mobilfunk bündeln. Messwerte zur NAT-Leistung müssen wir schuldig bleiben: DHCP für IP-zu-IP unterstützt der Router nicht, PPPoE funktionierte in unserem Mess-Setup nicht.

Intern gibt es WLAN mit 4 und 8 MIMO-Streams, was dem Router beim Multiuser-Benchmark den höchsten Durchsatz im Test bescherte. Aber dafür saugt er auch deutlich kräftiger an der Steckdose als die anderen Prüflinge. TWT fürs WLAN will die Telekom per Firmware-Update nachreichen.

- **extraflottes WLAN**
- **flexibler Internetzugang**
- **sehr stromhungrig**

Eingabe des WLAN-Passworts entstand eine WPA3-Verbindung.

Bei den Routern von Asus, AVM, D-Link und der Telekom kann man mit Kamera ausgestattete WLAN-Clients durch Scannen eines QR-Codes koppeln: Bei der Fritzbox 7530 AX und dem Speedport Pro Plus lässt man sich das schachbrettartige Muster im Browser anzeigen. Bei den anderen Geräten kann man es zurzeit *nur*, bei der Fritzbox *auch* in der vom Hersteller bereitgestellten App anzeigen lassen. Das erleichtert besonders Besuchern das Koppeln ihrer Smartphones mit dem Gastnetz, falls der Router eines anbietet.

Schließlich boten zwei Probanden – Huawei WiFi AX3 und Telekom Speedport Pro Plus – noch eine besonders einfache Art der Kopplung: Bei ihnen genügt es, ein Mobilgerät mit aktivierter NFC-Schnittstelle (Near Field Communications, WPS-NFC) ein paar Sekunden an den Router zu halten. Weil darüber aber wie bei WPS-PBC die Zugangsdaten fürs

Haupt-WLAN ausgetauscht werden, sollte man die Funktion – genauso wie WPS-PBC – nach dem Koppeln der eigenen Geräte ausschalten, damit sich Besucher nicht einen Zugang ins interne Netz erschleichen können. Bei Huawei gibt es zum Abschalten einen separaten Menüpunkt, bei der Telekom ist NFC an WPS-PBC gebunden.

Funkgeschwindigkeit

Wir maßen mit dem Benchmark-Tool iperf3 den Nettodurchsatz, also wie schnell die Router Daten in der Praxis an ein Wi-Fi-6-Notebook schicken (Asus VivoBook 14 mit nachgerüstetem WLAN-Modul Intel AX200). Anders als in [2] geschildert testen wir seit Anfang 2020 mit unbeschränkter TCP-Windowsize, also ohne den iperf-Parameter `-w256k`, der vorher für die Vergleichbarkeit mit älteren WLAN-Generationen sorgte. Dadurch können Wi-Fi 5 und Wi-Fi 6 auch mit einem TCP-Datenstrom schon weit aufdrehen und gewinnen mit mehreren parallelen TCP-Strömen nur noch wenig hinzu.

Der erzielbare Durchsatz hängt direkt von der Bruttodatenrate auf dem Funkkanal ab und die wiederum von mehreren Dingen: Der wichtigste Parameter ist die Zahl der genutzten Antennen (zwei bei den meisten Geräten, zwei oder drei je nach Funkband bei der Fritzbox 7530 AX, vier oder acht beim Speedport Pro Plus).

Dabei spielt der Client mit: Wenn er nur zwei Antennen hat wie die meisten Notebooks und bessere Smartphones, gehen auch nur zwei parallele Datenströme (MIMO-Streams) rüber. So ergeben sich im 5-GHz-Band mit der dort üblichen Signalbreite von 80 MHz bei Wi-Fi 6 auf kurze Distanz maximal 1200 MBit/s brutto. Bei Wi-Fi 5 sind es unter denselben Bedingungen bis zu 867 MBit/s. Bei größeren Strecken sinkt die Funkdatenrate wegen der zunehmenden Streckendämpfung und der damit abnehmenden Empfangssignalstärke.

Ein extrabreiter 160-MHz-Funkkanal verdoppelt im 5-GHz-Band die Bruttorate, ist bei der 7530 AX aber nicht einschaltbar, weil sich ihr Chipsatz anscheinend nicht dafür eignet; die vom Hersteller genannten 1800 MBit/s beziehen sich auf drei MIMO-Streams. Bei der zum Vergleich mitgemessenen Fritzbox 7580 ist die 160-MHz-Option ab FritzOS 7.2x nicht mehr abschaltbar. So kam es, dass der ältere Router in diesem Test mit den Neulingen noch gut mithalten konnte (siehe Balkendiagramm auf Seite 51). Im 2,4-GHz-Band blieb er gegenüber der neuen Technik indes deutlich zurück. Anders ausgedrückt: Ihre Wi-Fi-6-Clients gewinnen, wenn sie im 2,4-GHz-Band verbunden sind und Sie Ihren Wi-Fi-5-Router ersetzen.

Um eine zufriedenstellende WLAN-Note zu erreichen, musste ein Router auf Entfernung diesmal mindestens 125 MBit/s liefern. Beim Doppelten – dem Maximaldurchsatz eines Supervectoring-Downstreams – gab es ein „Gut“. Mit noch mal 100 MBit/s mehr ist Reserve für noch schnellere Anschlüsse da und es gab dafür eine sehr gute Note.



Wi-Fi-6-Router – Technische Daten und Testergebnisse

Modell	Asus RT-AX58U	AVM Fritzbox 7530 AX	D-Link DIR-X1860	Huawei WiFi AX3 (WS7200)	Linksys MR7350	Telekom Speedport Pro Plus
mitgelieferte Extras (außer Patchkabel)	–	TAE-Kabel	–	–	–	TAE-Kabel, TAE-Kupplungen
getestete Firmware-Version	3.0.0.4.384_10177	FritzOS 7.21	1.03b07	10.0.5.27	1.1.4.202174	120141.3.5.020.0
Quelltexte verfügbar	✓ (ältere Version)	auf Anfrage	✓ (ältere Version)	–	auf Anfrage	auf Anfrage
Anschlüsse / Hardware						
WAN / LAN / xDSL	1 / 4 / –	0 (1) / 4 (3) / 1	1 / 4 / –	1 / 3 / –	1 / 4 / –	0 (1) / 4 (3) / 1
USB / weitere Ports	1 × 5 GBit/s / –	1 × 480 MBit/s / –	– / –	– / –	1 × 5 GBit/s / –	2 × 5 GBit/s / SFP, SIM, µSD
Bedienelemente	Ein, Reset, WPS	WLAN, DECT, Connect/ WPS	Ein, Reset, WPS	Ein, Reset, WPS	Ein, Reset, WPS	Anmelden/WPS, WLAN, Neustart, Reset
Statusanzeigen / abschaltbar	8 / ✓	5 / ✓	4 / ✓	1 / –	10 / –	7 / –
Konfiguration						
Browser-Oberfläche deutsch / brauchbare Hilfe / Assi	✓ / (✓) / ✓	✓ / ✓ / ✓	✓ / – / ✓	✓ / ✓ / ✓	✓ / – / ✓	✓ / ✓ / ✓
Konfigurationshelfer übergeht	IPv6, IPTV, WPA2+3, Sommerz., Wi-Fi-6-Opt., Gastnetz	Änderung Admin-Pass-wort, Gastnetz, WPA2+3	VLAN-Tagging, WPA2+3, DFS-Kanäle	WPA2+3, Sommerzeit, Wi-Fi-6-Opt., Gastnetz, IPTV	WPA2+3, Gastnetz, Änderung Admin-Pass-wort	Änderung Admin-Pass-wort, Wi-Fi-6-Opt., Gastnetz
Fernwartung per App / HTTPS / ab Werk aus / Port änderb.	–[1] / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / – / – / –	✓ / – / – / –	i. V. / – / – / –
Fernüberwachung per SNMP / Syslog / E-Mail	– / ✓ / –	– / – / ✓	– / ✓ / ✓	– / – / –	– / – / –	– / – / ✓
NTP-Server frei einstellbar / Sommerzeit korrekt	✓ / ✓	✓ / ✓	✓ / ✓	– / ✓	– / ✓	– / ✓
andere Betriebsarten	AP, Repeater, Bridge	AP, Repeater (i. V.)	–	AP, Repeater	AP, Repeater, Bridge	–
Besonderheiten	Mesh-fähig (AiMesh), Alexa- und IFTTT-Einbindung, NAS-Funktion, AiCloud 2.0, Internet per USB-Mobilfunk-Stick	Mesh-fähig (Fritz-Mesh), HD-Telefonie, NAS-Fkt., Smart-Home-Funktionen, Dyndns-Dienst (IPv4 und IPv6), Hotspot-Modus, USB-Fernanschluss, Internet per LTE-Stick	–	Mesh-fähig (HiLink), NFC-Kopplung	Mesh-fähig (Velop), NAS-Funktion	Hybrid-fähig (LTE+DSL), Mesh-fähig (Speed Home Wifi), HD-Telefonie, NFC-Kopplung, NAS-Funktion, Magenta-Smart-Home
WAN						
IPv4-Protokolle (außer PPPoE)	DHCP, PPTP, L2TP	DHCP, statische IP, DS-Lite	DHCP, statische IP, PPTP, L2TP, DS-Lite	DHCP, statische IP	DHCP, statische IP, PPTP, L2TP	–
IPv6-Modi	DHCPv6, statische IP, Passthrough, Tunnel (6in4, 6to4, 6rd)	DHCPv6, statische IP, DS-Lite, Tunnel (6in4, 6to4, 6rd)	DHCPv6, PPPoE, statische IP, Tunnel (6rd)	SLAAC, DHCPv6	Auto, PPPoE, Pass-through, Tunnel (6rd)	Nativ
T-VDSL-kompatibel / IPv6 / Multicast-IPTV	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓[2]	✓ / ✓ / ✓
Multicast-Proxy	✓[3]	✓	✓	✓	✓[3]	✓
DynDNS-Dienste / beliebiger Server (Protokoll) / per URL-Eingabe / LE-Zertifikat	9 / – / – / ✓	7 / – / ✓ / ✓	2 / ✓ (k. A.) / – / –	2 / – / – / –	2 / – / – / –	4 / ✓ (Dyndns2) / – / –
VPN-Server / VPN-Client	beides: OpenVPN, IPsec	beides: IPsec	QuickVPN / –	– / L2TP	–	IPsec / –
Telefonie						
SIP-Nebenstellen intern / extern / SIP-Trunking	– / – / –	✓ / ✓ / ✓	– / – / –	– / – / –	– / – / –	– / – / –
DECT-Telefonie / Analoge Telefone (Buchse)	– / –	✓ / 1 (TAE/RJ12)	– / –	– / –	– / –	✓ / 2 (TAE)
ISDN-S0-Bus	–	–	–	–	–	✓
LAN						
DHCP: IP nach MAC / DHCP-Server abschaltbar	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Portweiterleitungen: Portwechsel / Bereiche / Triggering	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / –	✓ / – / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
UPnP-Status / UPnP-Portfreigaben / default aus	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	✓ / – / ✓
IPv6-Kaskadierung (delegierte Präfixgröße)	–	✓ (/62)	✓ (/60)	–	–	–

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden i. V. in Vorbereitung k. A. keine Angabe

[1] erst mit späterer Firmware (Asus), dann nur via Alexa oder Google-Assistant [2] nur im LAN, nicht im WLAN [3] MC-IPTV nicht in Kaskade per DHCP [4] gegen Intel AX200 unter Windows 10
[5] 1 WAN-/DSL- und 1 LAN-Port belegt, kein Datenverkehr, Dauerbetrieb, 30 Cent/kWh, Kosten gerundet

Wi-Fi-6-Router – Technische Daten und Testergebnisse

Modell	Asus RT-AX58U	AVM Fritzbox 7530 AX	D-Link DIR-X1860	Huawei WiFi AX3 (WS7200)	Linksys MR7350	Telekom Speedport Pro Plus
WLAN						
2,4 GHz / 5 GHz (MIMO-Streams)	Wi-Fi 6 (2) / Wi-Fi 6 (2)	Wi-Fi 6 (2) / Wi-Fi 6 (3)	Wi-Fi 6 (2) / Wi-Fi 6 (2)	Wi-Fi 6 (2) / Wi-Fi 6 (2)	Wi-Fi 6 (2) / Wi-Fi 6 (2)	Wi-Fi 6 (4) / Wi-Fi 6 (8)
alias IEEE 802.11	ax-574 / ax-2400	ax-574 / ax-1800	ax-574 / ax-1200	ax-574 / ax-2400	ax-574 / ax-1200	ax-1150 / ax-4800
Gastnetz / mit WPA2+3	✓ / ✓	✓ / ✓	✓ / –	✓ / –	✓ / –	✓ / ✓
Roaming-Funktionen 11k / 11v / 11r	– / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –
Wi-Fi 6: BSS Coloring / Spatial Reuse (SRP) / TWT	✓ / – / ✓	✓ / – / ✓	✓ / – / ✓	✓ / – / ✓	✓ / – / ✓	✓ / – / i. V.
Firewall						
bei IPv4 / IPv6 abschaltbar / IPv6-FW folgt dyn. Präfix	✓ / ✓ / –	– / – / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	– / – / –
Regelsätze für IPv4+IPv6 getrennt / gemeinsam	✓ / –	✓ / ✓	✓ / –	– / –	✓ / –	– / –
Pakete nach Dienst / Quelle / Ziel filtern	✓ / ✓ / ✓ (nur IPv4)	✓ / ✓ / ✓	✓ / ✓ / ✓	– / – / –	– / – / –	– / – / –
Exposed Host IPv4 / IPv6	✓ / –	✓ / ✓	✓ / –	✓ / –	✓ / –	– / –
Messwerte						
Max. NAT-Durchsatz PPPoE Down/Upstream	904 / 905 MBit/s	884 / 868 MBit/s	901 / 897 MBit/s	187 / 168 MBit/s	849 / 823 MBit/s	nicht messbar
IP/IP Down/Upstream	950 / 949 MBit/s	950 / 949 MBit/s	950 / 949 MBit/s	948 / 948 MBit/s	949 / 949 MBit/s	DHCP nicht unterstützt
WLAN-Durchsatz 2,4 GHz nah / 20 m[4]	332 / 181–305 MBit/s	346 / 157–213 MBit/s	421 / 155–297 MBit/s	382 / 145–276 MBit/s	322 / 147–256 MBit/s	403 / 254–322 MBit/s
5 GHz nah / 20 m[4]	737 / 255–347 MBit/s	706 / 184–226 MBit/s	695 / 136–216 MBit/s	893 / 254–283 MBit/s	691 / 207–309 MBit/s	898 / 238–371 MBit/s
Summendurchsatz 5 GHz nah+nah / nah+fern[4]	554 / 535 MBit/s	539 / 401 MBit/s	600 / 410 MBit/s	867 / 586 MBit/s	780 / 367 MBit/s	942 / 618 MBit/s
Leistungsaufnahme[5]	5,6 Watt (13 VA)	6,9 Watt (14 VA)	4,7 Watt (10 VA)	5,2 Watt (9 VA)	5,4 Watt (11 VA)	19 Watt (36 VA)
jährliche Stromkosten[5]	15 €	18 €	12 €	14 €	14 €	50 €
Bewertung						
Ausstattung	⊕	⊕	○	○	○	⊕⊕
Funktionen	⊕	⊕⊕	⊕	○	○	⊕
NAT-Durchsatz PPPoE / IP-zu-IP	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	○ / ⊕⊕	⊕⊕ / ⊕⊕	k. A.
WLAN-Durchsatz 20 m 2,4 / 5 GHz	⊕ / ⊕⊕	○ / ○	⊕ / ○	⊕ / ⊕	⊕ / ⊕	⊕ / ⊕⊕
Preis	144 €	179 €	96€	59 €	94 €	320 € (Miete: 10 €/ Monat)

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden i. V. in Vorbereitung k. A. keine Angabe

[1] erst mit späterer Firmware (Asus), dann nur via Alexa oder Google-Assistant [2] nur im LAN, nicht im WLAN [3] MC-IPTV nicht in Kaskade per DHCP [4] gegen Intel AX200 unter Windows 10
[5] 1 WAN-/DSL- und 1 LAN-Port belegt, kein Datenverkehr, Dauerbetrieb, 30 Cent/kWh, Kosten gerundet

Einen Latenz-Unterschied konnten wir nicht ausmachen: Die mittlere Ping-Zeit (Laufzeit für Hin- und Rückweg) über die WLAN-Verbindung unterschied sich bei den Routern nur minimal. Sie lag bei allen Probanden, einschließlich des älteren Wi-Fi-5-Modells, gerundet zwischen 2 und 4 Millisekunden.

WLAN für viele

Schließlich überprüften wir mit zwei gleichzeitig im 5-GHz-Band angebundenen Notebooks, wie gut Wi-Fi 6 sein Versprechen einlöst, mehrere Clients gleichzeitig besser zu bedienen als Wi-Fi 5. Zwei Router konnten uns im ersten Szenario – beide Notebooks nahe bei der Basis – überraschen: Beim MR7350 und dem Speedport Pro Plus war der Summendurchsatz höher als der eines einzelnen Laptops.

Beim Speedport Pro Plus wäre womöglich noch mehr durchgegangen, wenn er Multigigabit-LAN-Ports für 2500 MBit/s hätte. Die im Multiuser-Szenario „nah+nah“ gemessenen 948 MBit/s entsprechen bis auf Krümelchen dem maximal über Gigabit-Ethernet (1000 MBit/s) möglichen Nettodurchsatz (950 MBit/s).

Erwartetermaßen sank der Summendurchsatz, als wir ein Notebook weiter entfernten, am wenigsten beim Asus RT-AX58U (–3 Prozent). Sonst ging die Gesamtdatenrate um 30 bis 50 Prozent zurück, genauso wie beim Wi-Fi-5-Router. Einen klaren Vorteil für Wi-Fi 6 können wir hier nicht erkennen; vielleicht

WLAN-Ausblick

Die sechste WLAN-Generation baut mit einer Normerweiterung auf den WLAN-Standard IEEE 802.11 auf. Im Dezember 2020 hat das international tätige Normungsgremium „Institute of Electrical and Electronics Engineers“ den achten Entwurf (D8.0) von 802.11ax intern als final erklärt und wird ihn wohl noch 2021 endlich als Standard veröffentlichen.

Damit ist die Entwicklung aber nicht am Ende: Der Entwurf für den Nachfolger Wi-Fi 7 (IEEE 802.11be) hatte zum gleichen Zeitpunkt schon die Version 0.2 erreicht. Bis der zu einer Spezifikation gereift ist, auf die man Chips bauen kann, werden wohl noch zwei Jahre vergehen und einige mehr, bis Wi-Fi-7-Hardware erschwinglich und verbreitet ist.

Wer sein WLAN heute mit Wi-Fi 6 modernisieren will, muss also nur erwägen, wie wichtig die voraussichtlich ab Sommer 2021 in der EU verfügbare Erweiterung Wi-Fi 6E ist [3]: Damit soll WLAN rund 500 MHz mehr Spektrum bekommen, dessen Nutzung aber neue Basen *und* Clients voraussetzt.

braucht die Firmware der getesteten Geräte noch etwas Optimierung.

Wi-Fi-6-Optionen

Eine der für dicht besiedelte Gegenden wichtigsten Wi-Fi-6-Funktionen (siehe S. 68) ist Spatial Reuse: Die Router dürfen damit trotzdem senden, wenn auf demselben Kanal gerade ein Nachbarnetz aktiv ist, dessen Signal aber unter einer vorgegebenen Schwelle liegt. Das steigert die Spektrumseffizienz. Um fremden Verkehr beim Kanalzugriff schneller zu erkennen (OBSS-PD, Overlapping Basic Service Set Preamble Detection), müssen Wi-Fi-6-Basen ihre Zellen mit BSS Coloring markieren, was alle Prüflinge taten. Die ausgefeiltere Variante mit Spatial-Reuse-Parametern (SRP) zum Bilden von SR-Gruppen fanden wir noch nirgends.

Wichtiger als SRP ist Unterstützung für Target Wait Time. TWT soll Mobilgeräten längere Deep-Sleep-Phasen ermöglichen, was die Akkuladung schont. Die Telekom will beim Speedport Pro Plus die TWT-Funktion per Firmware-Upgrade nachrüsten. Bei anderen Geräten muss man sie manchmal erst aktivieren.

Die Leistungsaufnahme der Router haben wir wie üblich gemessen, aber nicht benotet, weil Modelle sehr unterschiedlicher Klassen im Test sind: Eines enthält ein xDSL-Modem, ein anderes besonders aufwendige WLAN-Schnittstellen. Da fällt es den Routern ohne solche Extras naturgemäß leichter, mit weniger Strom auszukommen.

Fazit

Wer eine gut funktionierende WLAN-Installation hat, muss den alten Router nicht sofort rauswerfen: Eine ältere Wi-Fi-5-Basis bediente unsere Test-Clients durchsatzmäßig im 5-GHz-Band ebenso gut wie die Neulinge. Der Schritt zur nächsten WLAN-Generation wird deshalb erst dann unumgänglich, wenn sich mehr Wi-Fi-6-Clients – Smartphones, Tablets, Notebooks – im Funknetz versammeln.

Wenn Sie Ihren Internetanschluss über ein separates Modem betreiben, lassen sich die hier getesteten Breitband-Router bei einem Provider- und Technikwechsel leicht weiter nutzen. Manche der Geräte zeigten noch kleinere Macken, die hoffentlich kommenden Firmware-Upgrades ausbügeln.

All-in-one-Geräte wie die Fritzbox 7530 AX und der zum Vergleich mitgetestete Telekom Speedport Pro Plus haben hingegen alles für xDSL-Anschlüsse an Bord. Letzterer zeigt, was heute WLAN-mäßig geht, kommt mit vielen Anschlusskombinationen (xDSL, LTE, Glasfaser) im Telekom-Netz zurecht, ist aber kein Sonderangebot und zudem stromhungrig. AVMs nicht mal halb so teure Fritzbox 7530 AX muss ihm beim WLAN-Durchsatz den Vortritt lassen. Ihre flexiblere Firmware macht die Box aber nicht nur für Heimserverbetreiber interessanter. (ea) c't

Literatur

[1] Ernst Ahlers, **Assistenten-Nachhilfe**, Was Router-Wizards übersehen und wie man das nachholt, c't 20/2019, S. 132

[2] Ernst Ahlers, **WLAN: Antworten auf die häufigsten Fragen**, c't 2/2019, S. 134

[3] Jennifer Li, **Von 540 auf 1040**, Wie Wi-Fi 6E das WLAN-Spektrum verdoppelt, c't 1/2021, S. 48



Herbstcampus

Wissen, Inspiration und Praxisrelevanz

15. September 2021 – Online

Bis 31. Juli für nur 49 € buchen!

Die gewohnt kommunikative Konferenz für Unternehmensentwickler mit:

- mehr als 20 Vorträgen
- Themenclustern aus drei Vorträgen und interaktiven Diskussionen
- Themen: Softwarearchitektur, Containerisierung, Java, APIs, Infrastructure as Code, Teamwork & Weiterentwicklung
- Diskussionsrunden per Chat und Video
- virtuellem Get-together am Abend

www.herbstcampus.de

Veranstalter

iX · heise Developer · dpunkt.verlag

Silber-Sponsor

infoteam software



Bild: Andreas Martini

Extrasicheres WLAN mit WPA3

Einer der großen Fortschritte in FritzOS 7.2x ist die verbesserte WLAN-Verschlüsselung WPA3. Sie stopft nicht nur die in WPA2 in den letzten Jahren entdeckten Lücken, sondern bringt auch nützliche neue Funktionen mit. WPA3 klappt auch schon mit vielen Geräten – und anderen Routern.

Von **Alfred Arnold, Ernst Ahlers**

Mit WPA3 ab FritzOS 7.2x liefert AVM eine Runderneuerung der WLAN-Verschlüsselung: Für den Anwender sieht alles mehr oder weniger wie gewohnt aus, aber er wird besser gegen Angriffe und Ausspähen geschützt. Im Folgenden schildern wir, wie WPA3 das schafft. Beim Verständnis hilft ein kurzer Rückblick, der nicht nur Fritzbox-Besitzern nutzt, sondern auch denen anderer Router und WLAN-Basen (Access-Points). Er schildert die WPA2-Ausgangslage und gibt Einrichtungstipps, unter anderem zu sicheren Passwortlängen und Optionen, mit denen man Geräte bequem koppeln kann. Wer das schon im Hinterkopf hat, kann zum Abschnitt „WPA3 endlich da“ vorspringen.

Bereits 2004 erschien die WLAN-Verschlüsselung WPA2. Sie verwendet den immer noch als sicher geltenden AES-Algorithmus (Advanced Encryption Standard) für das Chiffrieren der Daten. Sein Schutz hielt fast fünfzehn Jahre, eine in IT-Maßstäben sehr lange Zeit, in der sich die WLAN-Datenrate von 54 auf 1733 MBit/s brutto mehr als verdreißigfachte. Aber auch die besten Schlösser rosten.

Vor einigen Jahren stellte sich heraus, dass WPA2-Personal anfällig gegen Offline-Dictionary-Attacken ist: Ein Angreifer kann die notwendigerweise noch unverschlüsselte Anmeldung eines Clients, den sogenannten Key Handshake, mitschneiden und mithilfe eines Wörterbuchs durchprobieren, welches Passwort zu den dabei ausgetauschten kryptografischen Prüfsummen passt.

Die Hardware für solche Brute-Force-Angriffe wurde wie die fürs WLAN über die Jahre immer billiger und leistungsfähiger. 2016 stellte ein Forscherteam der Uni Wien auf einer internationalen Konferenz eine auf die Aufgabe spezialisierte Hardware vor: Die knapp 100.000 US-Dollar teure FPGA-Implementierung kann über 10 Millionen Passwörter pro Sekunde testen (siehe Link unter ct.de/wpgv) – so was gönnen sich Dienste mit dreibuchstabigen Abkürzungen für staatlich gedeckte Spionage.

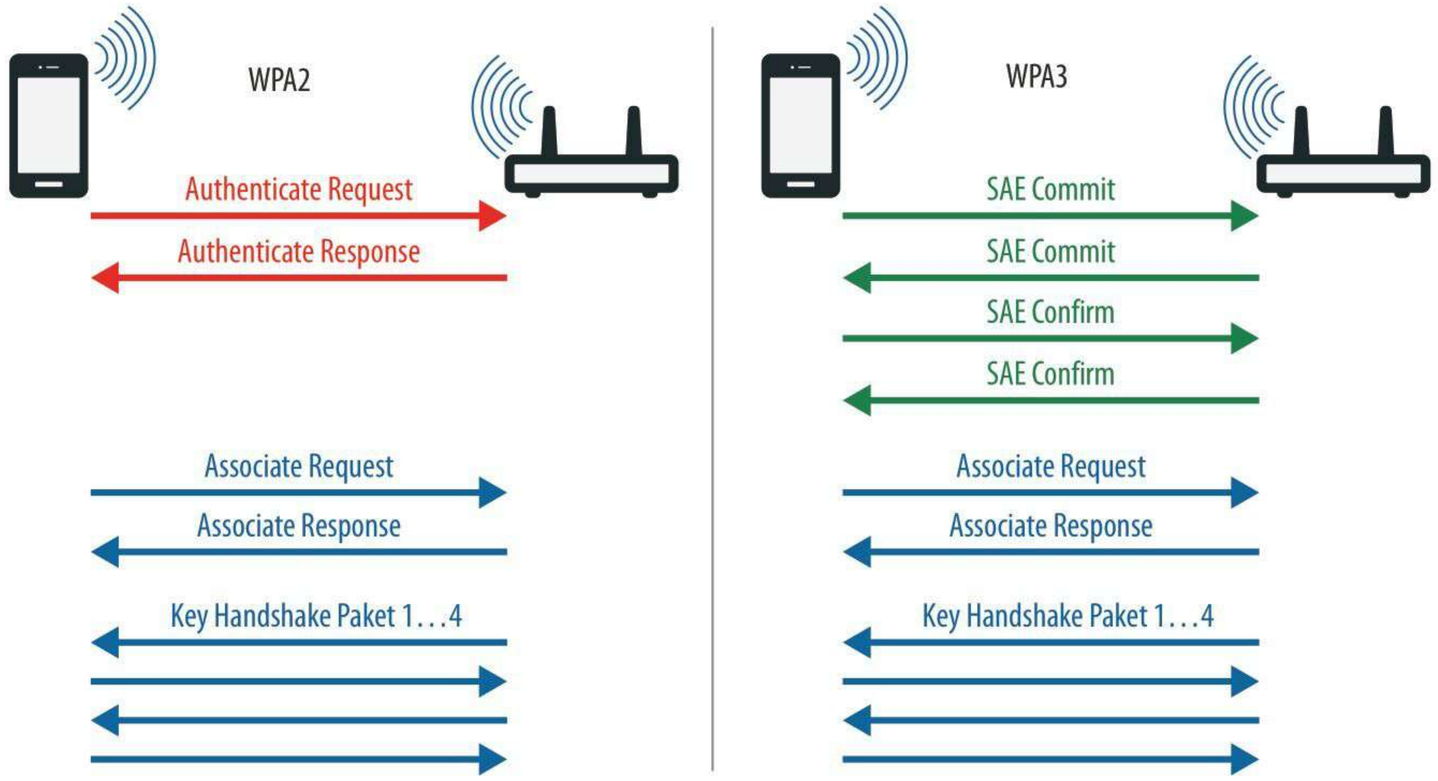
Bitte würfeln!

Falls Sie einen Router haben, der sich nicht für WPA3 eignet (etwa ältere Fritzboxen), prüfen Sie Ihren WPA2-Schlüssel: Dabei gilt der dringende Rat, möglichst lange und – besonders wichtig – erwürfelte Passwörter zu verwenden. Mit jedem weiteren Zeichen, das zufällig aus Buchstaben (groß und klein) sowie Ziffern gewählt wird, vergrößert sich der Suchraum um den Faktor 62.

Setzt man seit 2016 eine Vervierfachung der Hardware-Leistung an, dann würde ein solches 16-stelliges Passwort dem 100.000-Dollar-Knacker heute im Mittel immer noch rund 19 Billionen Jahre standhalten. Selbst wenn einem Aggressor die tausendfache Leistung zur Verfügung steht und noch eine kryptologische Abkürzung entdeckt wird, die den

WLAN-Anmeldung bei WPA2 und WPA3

Der Hauptunterschied zwischen den WPA-Varianten liegt am Anfang des Verbindungsaufbaus: Bei WPA3 machen die Stationen einen an Diffie-Hellman angelehnten Schlüsseltausch. Mit dem darüber vereinbarten temporären Schlüssel schützen sie den eigentlichen Key Handshake, was Angreifern die Grundlage für Wörterbuchattacken und das nachträgliche Dechiffrieren von Nutzerdaten entzieht (Perfect Forward Secrecy, PFS).



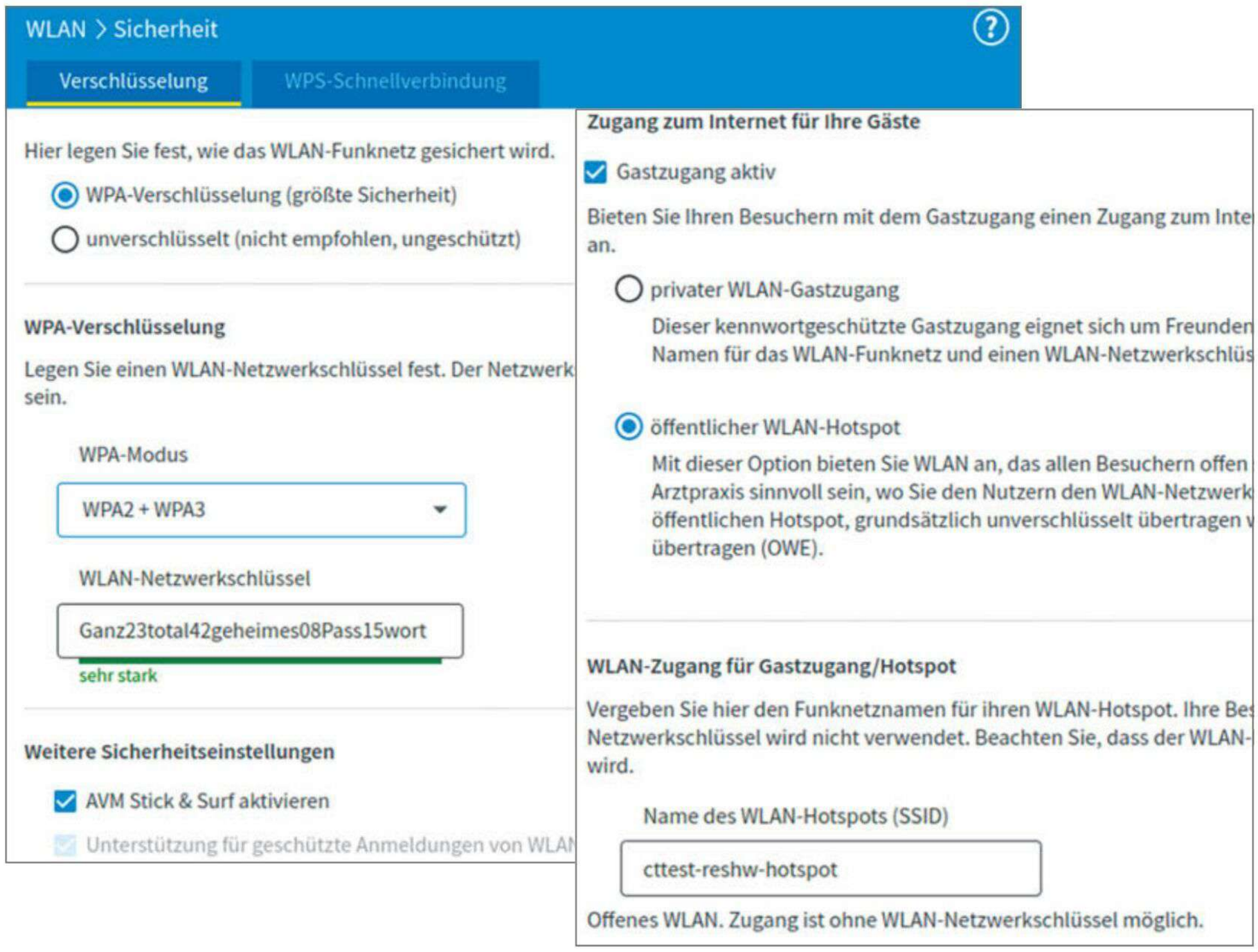
Aufwand auf ein Tausendstel reduziert, genügt WPA2-PSK mit einem so langen Passwort noch weiiiiit über Ihre Rente hinaus.

Um die zunehmende Sperrigkeit beim Eintippen zu umgehen, kann man WLAN-Clients per Knopfdruck (WPS-Taste) oder bei Smartphones und Tablets auch per Abfotografieren eines QR-Codes koppeln. Es gibt also keinen Grund, sichere Passwörter zu meiden.

Neben der Passwort-Problematik stellt aus heutiger Sicht der fehlende Vertraulichkeitsschutz Perfect Forward Secrecy (PFS) einen Mangel von WPA2-PSK dar: Hat ein Angreifer die WPA2-Passphrase in die Finger bekommen, kann er aufgezeichnete Daten nachträglich entschlüsseln. WPA2-Enterprise mit Zertifikaten ist da besser aufgestellt.

2017 kam der Paukenschlag. Ein Team von Sicherheitsforschern um Mathy Vanhoef veröffentlichte die von ihnen gefundene, auf den Namen KRACK getaufte Lücke: Die meisten WPA2-Implementierungen stellten sich als anfällig gegen eine Replay-Attacke heraus (c't 23/2017, S. 16). Mit der konnte ein Angreifer Clients dazu bewegen, verschiedene Pakete mit demselben Schlüssel zu chiffrieren – eine kryptografische Todsünde.

Zwar konnten die Hardwarehersteller die KRACK-Lücke mit Software-Updates schließen. Aber die Wi-Fi Alliance sah sich angesichts des öffentlichen Interesses unter Zugzwang und stellte kurzfristig die bereits in Arbeit befindliche WPA-Version 3 fertig – so schnell, dass eine ganze Weile kein Hersteller WPA3-fähige Geräte vorweisen konnte.



Schon das 2020 erschienene FritzOS 7.20 brachte die WPA3-Mixed-Mode-Verschlüsselung fürs Haupt- und fürs Gast-WLAN mit. Letzteres kann man alternativ im Hotspot-Modus betreiben, um Besuchern und Kunden einen verschlüsselten Internetzugang ohne Passworteingabe anzubieten.

WPA3 endlich da

Mittlerweile hat sich die Situation gewandelt und WPA3 ist nicht nur in die Firmware teurer Enterprise-Basen eingezogen, sondern ab Version 7.20 in AVMs FritzOS angekommen. Damit können nun viele Fritzbox-Besitzer von WPA3 profitieren.

Erfreulicherweise ändert sich auf den ersten Blick beim Einrichten der WLAN-Verschlüsselung nichts. Wie früher gewährt bei WPA3-Personal eine Passphrase den Zugang. So wird auch der mittelfristig unverzichtbare Mixed-Mode möglich: Die Funkzelle bietet WPA2 und WPA3 parallel an, damit ältere Clients weiterhin über WPA2 Verbindung bekommen. Denn bis die nicht WPA3-fähigen Smartphones, Tablets, Notebooks und PC-Adapter aus dem Markt verschwunden sind, wird es noch einige Jahre dauern.

Stellen Sie in der Router-Konfiguration unter WLAN / Sicherheit den Ausklapper WPA-Modus von WPA2 (CCMP) auf „WPA2 + WPA3“ um. Wenn sich nun ein WPA3-fähiger Client anmeldet, ist bei ihm der Sitzungsschlüssel gegen Abhören und einen folgenden Brute-Force-Angriff geschützt: Der Client lässt sich nicht mehr per Deauth-Paketen vom Fritz-WLAN abmelden, um ihn auf einen Fake-Hotspot umzulenken, und sein Datenverkehr ist nicht mehr nachträglich entschlüsselbar.

Auch für Hotspots

Als Bonus hat AVM auch das optionale Gastnetz mit WPA3 im Mixed-Mode versehen, sodass Ihre Besucher ebenfalls besser geschützt sind. Alternativ können Gastwirte und andere Selbstständige das Fritzbox-Gastnetz für ihre Kunden auf den WPA3-Hotspot-Modus Enhanced Open umstellen: Die dort mit dem alten Namen OWE (Opportunistic Wireless Encryption) bezeichnete automatische Verschlüsselung ist zwar auch nicht perfekt, weil sie Man-in-the-Middle-Attacken zulässt. Trotzdem schützt Enhanced Open die Kunden in Restaurants, Praxen oder Kanzleien weit besser gegen simples Abhören als unverschlüsselte Hotspots. Damit alte Clients nicht hinten runterfallen, läuft Enhanced Open im Transitional-Modus. Geräte, die sich nicht darauf verstehen, bekommen so wenigstens eine unverschlüsselte Verbindung und sind nicht komplett ausgeschlossen.

Auch bei WPA3-PSK gilt es, ein sicheres Passwort zu verwenden, das weder in einem Wörterbuch steht noch einfach zu erraten ist. Nun geht bei Ihnen gewiss die Frage im Kopf um, wo denn überhaupt die Vorteile von WPA3 liegen. Sie liegen im Detail und haben es in sich.

Zum einen verwendet WPA3 die Passphrase während der Anmeldung so, dass ein Angreifer allein durch passives Mithören nicht mehr in der Lage ist, eine Offline-Wörterbuch-Attacke auf das WLAN-Passwort zu führen. WPA3 verknüpft dazu die Passphrase mit einem Diffie-Hellman-artigen Schlüsselaustausch, über den sich die Stationen auf einen temporären Schlüssel einigen. Damit schützen sie den folgenden Key Handshake, mit dem sie den für die WLAN-Übertragungen genutzten Pairwise Key ermitteln. Das entzieht dem Angreifer einen wesentlichen Baustein, den er braucht, um ein Passwort zu erraten.

Wer Passwörter durchprobieren will, muss bei WPA3 folglich aktiv eine Verbindung zum AP aufbauen. Dabei lässt sich aber jedes Mal nur ein Passwort testen. Brute-Force-Attacken dauern so unrealistisch lange und fallen schnell auf. Die WLAN-Basen wehren sich dann mit verzögerten Antworten, was blindes Raten aussichtslos macht.

WLAN verteidigen mit PMF

Protected Management Frames (PMF) verhindern, dass Angreifer Ihren WLAN-Client mit einem gefälschten Steuerungspaket von der Basis trennen. Im besten Fall resultiert solch eine Attacke nur im Verbindungsabriss (Denial of Service, DoS). Für solchen WLAN-Vandalismus genügt schon ein billiges, als Smartwatch getarntes Spielzeug (Deauther Wristband V2, c’t Security 2020, S. 176).

Schlimmstenfalls gelingt es dem Angreifer aber, den WLAN-Client auf seinen Fake-Hotspot umzuleiten, sodass er sich als Man-in-the-Middle in Ihren Datenverkehr einklinken kann. Weil Basen und Clients bei einer WPA3-Verbindung PMF nutzen müssen, sind sie dagegen gefeit. Falls Ihre WLAN-Basis nur WPA2 spricht, aber die PMF-Option bietet, aktivieren Sie sie.

Entspannt zurücklehnen?

Die neue Schlüsselaushandlung erfüllt auch den PFS-Wunsch: Ist WPA3 auf den Stationen korrekt umgesetzt, dann verwerfen sie die Aushandlungsschlüssel nach der Verwendung. Spätestens beim Verbindungsende ist kein Material mehr vorhanden, anhand dessen sich mitgeschnittene Daten nachträglich dechiffrieren ließen, was Seitenkanal-Attacken vorbeugt.

Das dafür von WPA3 genutzte Verfahren ist weder neu noch eine Erfindung der Wi-Fi Alliance, sondern unter dem Namen Simultaneous Authentication of Equals (SAE) schon seit Langem Teil der WLAN-Norm IEEE 802.11: Es wurde einst für sichere Verbindungen zwischen den Nodes in Mesh-WLANs entwickelt (IEEE 802.11s).

Als Nutzer merkt man von all dem nichts: Der zusätzliche Rechenaufwand kostet nur Sekundenbruchteile. Außerdem ist er nur einmal beim Verbindungsaufbau fällig. Die Stationen können ihre paarweisen Schlüssel zwischenspeichern und bei späterer Wiederaufnahme der Verbindung einen Teil der Aushandlung überspringen. Das nützt besonders in verteilten WLANs für größere Gebäude, wo die Mobilgeräte häufig zwischen mehreren Basen hin und her springen, etwa einem Mesh-WLAN aus Fritzbox und Fritz-Repeatern. Mit dem kommenden SAE-FT (Fast Transition, IEEE 802.11r) klappt das künftig auch mit einer Anmeldung an einer Basis, die dann fürs ganze Netz gilt.

Leider nicht ganz …

Auch wenn SAE schon viele Jahre existiert, weckte es erst das Interesse von Sicherheitsforschern, als WPA3-fähige Geräte auf den Markt kamen. Wieder war es Mathy Vanhoef, der die ersten Ergebnisse präsentieren konnte (c't 18/2019, S. 44). Die fielen nicht unbedingt schmeichelhaft aus:

- Die Passphrase lässt sich zwar dank des Diffie-Hellman-artigen Schlüsselaustauschs nicht mehr ermitteln, aber ein Angreifer kann eine WLAN-Basis schon mit wenigen WPA3-Anmeldeversuchen pro Sekunde nahezu auslasten (Denial of Service, DoS). Der dagegen vorgesehene Anti-Clogging-Mechanismus hat sich als untauglich erwiesen.
- Ein Angreifer kann sich als Man-in-the-Middle in den Verbindungsaufbau einschleichen und den Client dazu bringen, einen WPA2-Verbindungsaufbau zu starten, obwohl die Basis WPA3 unterstützen würde. Zwar bemerken die Stationen das und unterlassen die Verbindung, aber es sind genug Pakete in WPA2-Manier gelaufen, dass der Angreifer eine Offline-Wörterbuchattacke darauf starten kann.
- Der Schlüsselaustausch findet auf Basis einer elliptischen Kurve statt. Dabei kann ein Angreifer Client und AP auf eine schwächere Kurve herunterzwingen, was den Schutz mindert.

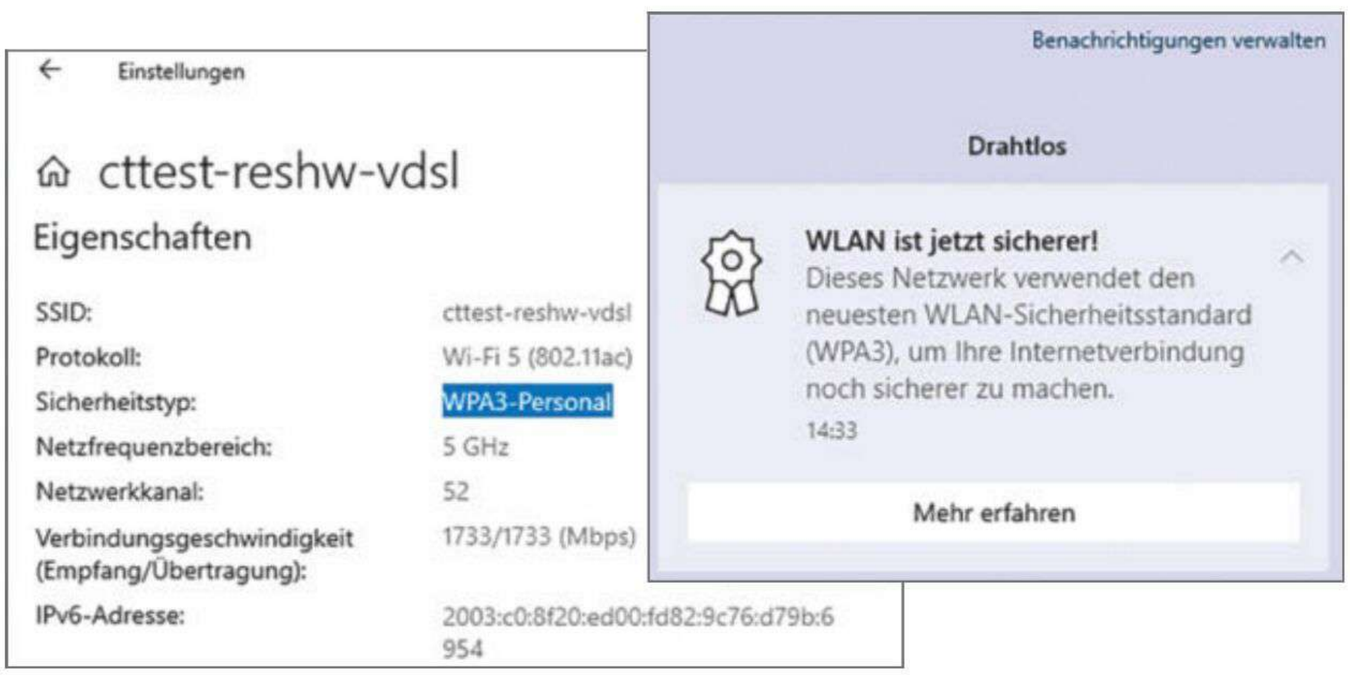
Diese drei Macken stellen WPA3 nicht insgesamt infrage, aber man darf sich schon wundern, wieso sie erst im Nachhinein aufgefallen sind. Anders als die KRACK-Lücke lassen sie sich nicht durch Workarounds in der Geräte-Firmware umgehen. Deshalb arbeitet die Wi-Fi Alliance an Erweiterungen und Korrekturen, die voraussichtlich in die Version 3 der WPA3-Spezifikation münden.

WPA3 aktivieren!

Wer nun zweifelt, ob er WPA3 schon nutzen sollte: Bitte unbedingt! Selbst Mathy Vanhoef hat zugestanden, dass es auch in seiner jetzigen imperfekten Form einen Fortschritt gegenüber WPA2 darstellt.

So setzt Apple WPA3 ab macOS 10.15 beziehungsweise iOS 13 ein und Google ab Android 10. Microsoft Windows 10 beherrscht WPA3 seit Build 1903, setzt aber Unterstützung im Treiber der WLAN-Hardware voraus.

Der auf Linux-Systemen übliche WPA-Supplicant kann seit Version 2.7 mit WPA3 umgehen. Das Tool ist aber nur der Unterbau auf Betriebssystemebene. Je nach Distribution und verwendetem Desktop



Beim ersten Verbinden meldet Windows 10, dass das neue WLAN WPA3 spricht und bietet Informationen dazu an. Wer sich später vergewissern will, klickt auf das WLAN-Tray-Symbol, öffnet die Verbindungseigenschaften und blättert herunter zum Sicherheitstyp.

(Gnome, KDE et cetera) bietet das nutzerseitige Werkzeug zum Verwalten und Anlegen vom WLAN-Profilen – etwa der GUI-Teil des NetworkManagers – WPA3 eventuell noch nicht an. Manchmal zeigt es ein WPA3-fähiges Netz mit „Unbekannter Sicherheitstyp“ an. Probieren Sie die Verbindung trotzdem, unter Kubuntu 20.04 klappte sie.

Nach welchem Verfahren ein Gerät die WLAN-Verschlüsselung ausgehandelt hat, zeigt die Fritzbox in der Liste aktiver Clients an (im Menü unter WLAN / Funknetz). Dort steht unter den Eigenschaften dann „WPA3“ oder „OWE“.

Es gibt auch Clients, die kein WPA3-Update bekommen, beispielsweise AVMs Fritz!WLAN-Sticks. Manche dieser Kandidaten werden sich, anstatt in einem Mixed-Mode-Netz (WPA2+3) auf WPA2 zurückzufallen, gar nicht mehr verbinden. Der Grund sind – wie meistens – Implementierungsfehler, die in einem reinen WPA2-Netz nicht auffielen. Wenn die Basis es unterstützt, kann man für solche Clients per Multi-SSID eine separate WPA2-only-Funkzelle aufspannen und mit einer eigenen Passphrase versehen. Das beherrschen Fritzboxen leider noch nicht. Sollte es in Ihrem Gerätepark Clients geben, die den Mixed-Mode nicht mögen, müssen Sie vorerst bei WPA2 bleiben.

Als Momentaufnahme haben wir bereits im Herbst 2020 eine Handvoll Geräte an zwei WLAN-Basen geprüft und durchwachsene Ergebnisse verzeichnet (siehe Tabelle). Neuere WLAN-Adapter (Wi-Fi 6: Intel AX200) werden offensichtlich besser gepflegt als ältere (Wi-Fi 5: Qualcomm QCA6174) und deren Windows-Treiber ebenso besser als die Linux-Varianten.

Beim riesigen Android-Hard- und Software-Zoo muss man mit Überraschungen rechnen: So verhielt sich unser vergleichsweise altes Android-8-Muster (Sony Xperia X Compact) kompatibler als ein Android-9-Beispiel (Nokia 5), das alle unsere WPA3-Funkzellen verschmähte. Der verschlüsselte Hotspot-Betrieb (Enhanced Open) klappte an der Fritzbox nur mit einem Client (Intel AX200 unter Windows 10).

WPA3-Hinweise von AVM und Microsoft

ct.de/wpgv

Fazit

Trotz seiner anfänglichen Hakeleien ist WPA3 ein großer und wichtiger Schritt zu mehr WLAN-Sicherheit. Auch wenn es noch etwas Zeit braucht, bis WPA3 in den meisten Netzen mit den meisten Clients reibungslos läuft, sollten es Fritzbox-Nutzer unbedingt aktivieren. Bei der erfahrungsgemäß langfristigen Firmware-Pflege von AVM stehen die Chancen gut, dass sich das wahrscheinlich noch 2021 erscheinende, weiter verbesserte WPA3 Release 3 nachrüsten lässt und man WLAN-sicherheitstechnisch eine Weile Ruhe hat. (ea) c't

WPA3-Kompatibilität

	Fritzbox-WLAN Mixed-Mode	Fritzbox-Gastnetz Mixed-Mode	Fritzbox-Hotspot (Enh. Open Trans.)	L822 Mixed-Mode	L822 WPA3 only	L822 Hotspot (Enhanced Open)	L822 Hotspot (Enh. Open Trans.)
Windows 10 (Wi-Fi-5: QCA6174)	WPA2	WPA2	unverschlüsselt	WPA2	keine Verbindung	keine Verbindung	unverschlüsselt
Windows 10 (Wi-Fi-6: AX200)	WPA3	WPA3	WPA3	WPA3	WPA3	WPA3	keine Verbindung
Linux (Kubuntu 20.04, QCA6174)	WPA3	keine Verbindung	unverschlüsselt	WPA3	WPA3[1]	keine Verbindung	unverschlüsselt
Linux (Kubuntu 20.04, AX200)	WPA3	keine Verbindung	unverschlüsselt	WPA3[1]	WPA3[1]	keine Verbindung	unverschlüsselt
macOS 10.15.6 (MBP 2015, A1502)	WPA3	WPA3	unverschlüsselt	WPA3	WPA3	keine Verbindung	unverschlüsselt
macOS 10.15.6 (MBP 2020, A2251)	WPA3	WPA3	unverschlüsselt	WPA3	WPA3	keine Verbindung	unverschlüsselt
Android 8 (Sony Xperia X Compact)	WPA2	WPA2	keine Verbindung	WPA2	keine Verbindung	keine Verbindung	unverschlüsselt
Android 9 (Nokia 5)	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung	keine Verbindung
Android 10 (Samsung S7+)	WPA3	keine Verbindung	unverschlüsselt	WPA3	WPA3	WPA2	unverschlüsselt
iOS 14 (iPhone X)	WPA3	WPA3	unverschlüsselt	WPA3	WPA3	keine Verbindung	unverschlüsselt

[1] nach manuellem Einrichten der Verbindung Fritzbox: AVM Fritzbox 7590 mit FritzOS 7.20, L822: Access-Point Lancom L822 mit Firmware 10.40.0291RU1

AVM Fritz-Repeater 6000 mit Wi-Fi 6

AVMs erster Repeater fürs aktuelle Wi-Fi-6-WLAN ist funktechnisch opulent ausgestattet. Das bringt Reserven für die Zukunft, aber er funkt auch mit Wi-Fi-5-Routern schon flott.

Von **Ernst Ahlers**



Der Fritz-Repeater 6000 ist AVMs neues Repeater-Topmodell. Wie sein Wi-Fi-5-Vorgänger Fritz-Repeater 3000 arbeitet der Neuling in drei Frequenzbereichen gleichzeitig, bei 2,4 GHz und in zwei 5-GHz-Blöcken. Eine 5-GHz-Schnittstelle dient der Mesh-Verbindung (Backbone) mit dem WLAN-Router, die andere bedient so wie die 2,4-GHz-Schnittstelle die Clients. Der 6000er nutzt Qualcomm-WLAN-Chips (PHY: QCN 5024/5054), das System-on-Chip konnten wir nicht zweifelsfrei identifizieren. Der restlichen Hardware nach müsste es ein IPQ8074A sein.

Der Repeater lässt sich wie gewohnt leicht ins Netz einbinden und übernimmt dabei die WLAN-Einstellungen der Fritzbox. Er soll sich laut AVM auch mit WLAN-Routern anderer Hersteller sowie jenen von Providern verstehen. Wir haben ihn mit den Fritzboxen 7530 AX und 7580 probegefahren. Mit der ausgelieferten Firmware 7.20 mochte der 6000er im Repeater-Modus in unserem Aufbau mit der 7530 AX keine Clients auf 2,4 GHz annehmen. AVM hat während des Tests eine verbesserte Beta-Ausgabe der nächsten Firmware-Version bereitgestellt, die den Bug beseitigt.

Gegen unseren Standard-Wi-Fi-6-Client Intel AX200 schaffte der Fritz-Repeater im optionalen Access-Point-Modus (Netzanbindung per LAN-Kabel) einen hohen Durchsatz, auch wenn der Downstream bei der 5-GHz-Schnittstellen im Nahbereich circa 45 Prozent langsamer war als der Upstream (501 zu 918 und 502 zu 922 MBit/s). Möglicherweise gleicht sich das bei kommenden Firmware-Updates an. Über die 20-Meter-Strecke durch Wände lagen die Richtungen ungefähr gleichauf.

Als Repeater war der Backbone-Durchsatz über die Mesh-Verbindung und 20 Meter mit maximal 340 MBit/s gegen die Fritzbox 7530 AX zufriedenstellend. Mit der älteren Wi-Fi-5-Fritzbox 7580 verstand sich der 6000er besser (bis 520 MBit/s). Am 26-Meter-Punkt bekam der AX200-Client von der 7530 AX über den Repeater hinweg dann 156 MBit/s (2,4 GHz) beziehungsweise 103 MBit/s (5 GHz) zu-

gespielt; auch hier war es mit der 7580 etwas mehr (193/138 MBit/s).

Laut Beacons bietet der 6000er-Repeater die üblichen Roaming-Helferfunktionen fürs Mesh (IEEE 802.11k, Radio Resource Measurement und 11v, BSS Transition) sowie die wesentlichen Wi-Fi-6-Funktionen (BSS Coloring: effizientere Spektrumsnutzung, Target Wait Time: erleichtertes Energiesparen in Mobilgeräten, Down- und Uplink-MU-MIMO für gleichzeitigen Datenverkehr mit mehreren Geräten).

Fazit

Der Fritz-Repeater 6000 ist eine interessante, wenn auch teure Option für Fritzbox-Besitzer, die schon mehrere Wi-Fi-6-Clients betreiben und ihr WLAN vergrößern möchten. An der Performance wird AVM mit kommenden Firmware-Verbesserungen gewiss noch feilen. Richtig aufdrehen dürfte der 6000er, wenn optimal zu ihm passende 4-Stream-Fritzboxen mit Wi-Fi 6 erscheinen. (ea) c't

AVM Fritz!Repeater 6000

WLAN-Repeater	
Hersteller	AVM, www.avm.de
WLAN (MIMO-Streams)	3 × Wi-Fi 6 (4) = IEEE 802.11ax-1200 / -2400 / -2400, WPA3, WPS, DFS
Bedienelemente	Connect-Taste, 2 Statusleuchten
Anschlüsse	2 × RJ45 (1 × Multigigabit-Ethernet bis 2,5 GBit/s, 1 × Gigabit-Ethernet)
Getestete Firmware	FritzOS 7.20 / 7.24 beta
WLAN 2,4 GHz nah / 20 m[1]	377 / 202–251 MBit/s
5 GHz I nah / 20 m[1]	710 / 145–220 MBit/s
5 GHz II nah / 20 m[1]	712 / 250–290 MBit/s
Backbone-Durchsatz 20 m[2]	226–338 MBit/s
Client-Durchsatz 26 m 2,4 / 5 GHz[2]	156 / 103 MBit/s
Leistungsaufnahme[3]	8,3 Watt / 18 VA
Jährliche Stromkosten[3]	22 €
Preis	205 €

[1] gegen Intel AX200 im Access-Point-Modus (LAN-Brücke, FritzOS 7.20)
[2] im Repeater-Betrieb (FritzOS 7.24 beta) mit Fritzbox 7530AX (FritzOS 7.22)
[3] Repeater ohne Ethernet-Links, idle, bei Dauerbetrieb, 30 Cent/kWh, gerundet

iX Workshop

WORKSHOPS 2021



31. Aug. - 01. Sept. 2021

DevSecOps: Automatisierte Sicherheitstest für die Web-App-Entwicklung



06. - 10. Sept. 2021

Powerkurs vSphere-Administration – mit GUI und Command Line (vSphere 7 und 6)



13. - 14. Sept. 2021

Parallele Programmierung mit Java: Effiziente Software für Multi-Core Systeme

Weitere Infos unter **www.heise-events.de/workshops**

iX Workshop



Bild: Andreas Martini

Wie Wi-Fi 6 das WLAN beschleunigt

Bei der jetzt aktuellen sechsten WLAN-Generation steht die Effizienz im Vordergrund: Wi-Fi 6 alias IEEE 802.11ax soll unter anderem mit schlauerem parallelen Bedienen der Clients den Summendurchsatz in Funkzellen hochtreiben. Ein kleiner Datenraten-Nachschlag ist da nur das Sahnehäubchen.

Von **Guido R. Hiertz und Sebastian Max**

Bei Wi-Fi 6 steht zum ersten Mal nicht die Geschwindigkeit des einzelnen Clients im Fokus der Entwicklung. Stattdessen bringt diese von der IEEE unter dem Namen 802.11ax spezifizierte Version unter anderem zentrale Koordination der Funkzelle, OFDMA und Coloring, die die Geschwindigkeit beim gleichzeitigen Betrieb vieler Geräte steigern sollen. Ein kurzer Rückblick hilft beim Verständnis.

Wie die Ur-Norm IEEE 802.11 von 1997 (max. 2 MBit/s brutto) behandelten auch der erste, weit verbreitete Standard 802.11b (max. 11 MBit/s) sowie die auf 54 MBit/s beschleunigten Fassungen 802.11g (im 2,4-GHz-Band) und 802.11a (5 GHz) alle Datenpakete

mit gleicher Priorität. Jede Station (STA) – Access-Point (AP) alias Basis versus mobile Clients – durfte pro Sendegelegenheit (TX Opportunity, TXOP) auch immer nur ein Paket abschicken.

Die zweite Epoche brachte einen schlauen Durchsatzturbo: 802.11n (max. 600 MBit/s) führte die Mehrantennentechnik MIMO ein (Multiple Input Multiple Output). Durch Kombinieren der Signale mehrerer Antennen kann ein Gerät mehrere Datenströme gleichzeitig senden. Das vervielfacht die Kanalkapazität, wobei die Seite mit weniger Antennen das Limit vorgibt: Ein 2-Stream-11n-Client kann höchstens mit 300 MBit/s empfangen, auch wenn ein 4-Stream-11n-AP 600 MBit/s senden kann.

Dort setzt 802.11ac (max. 6900 MBit/s bei 8 Streams) an: Eine Basis mit vielen Antennen kann mehrere Empfänger mit wenigen Antennen gleichzeitig bedienen (Downlink Multi-User MIMO, DL MU-MIMO). Im obigen Beispiel kann der AP zwei Clients idealerweise parallel mit 300 MBit/s versorgen, in der Summe also 600 MBit/s absetzen.

Brutto-Aufschlag

802.11ax folgt dem Vorbild seiner Vorgänger und steigert die maximale Bruttodatenrate nochmals, jedoch um nur knapp 40 Prozent auf 9600 MBit/s. Dabei setzt 802.11ax weiterhin auf die mit 802.11a und 11g eingeführte Übertragungstechnik OFDM (Orthogonal Frequency-Division Multiplexing), die den zur Verfügung stehenden Frequenzblock in viele Unterträger unterteilt. Jedem Unterträger werden Daten als einzelne Symbole aufmoduliert (zeitlich begrenzter Signalverlauf).

Bei 802.11ac dauert ein Symbol 3,6 µs und kann bis zu 8 Bit transportieren (256-QAM). Mit einem in 468 Unterträger eingeteilten 160-MHz-Block und einem fehlerkorrigierenden Code mit der Rate 5/6 ergibt dies einen Datenstrom von 468 × 8 Bit × 5/6 / 3,6 µs = 866 MBit/s pro Antenne.

802.11ax führt eine höherstufige Modulation mit 10 Bit pro Symbol ein (1024-QAM). Allein das steigert die Bruttodatenrate um 25 Prozent. Der restliche Gewinn gegenüber 11ac stammt hauptsächlich von weniger Hilfsträgern, die keine Daten transportieren. Außerdem verlängert 11ax die Symboldauer auf 13,6 µs, was eine effizientere Einteilung in 1960 Unterträger erlaubt. Somit ergibt sich eine maximale Bruttodatenrate von 1201 MBit/s pro Antenne.

Damit der Empfänger die in einem Symbol gesendeten 10 Bit fehlerfrei liest, muss das empfangene Signal allerdings um mindestens 60 dB (Leistungsfaktor eine Million) lauter als das Rauschen und die Nachbarsignale sein. Anders ausgedrückt: Der Empfänger muss für solche Datenraten schon direkt neben der WLAN-Basis stehen. Erschwerend kommt hinzu, dass die begrenzte Sendeleistung in einem breiten 160-MHz-Kanal weiter verteilt wird und ein Empfänger auch mehr Rauschen aufnimmt. Beides verkürzt die Reichweite. Wichtig ist 1024-QAM deshalb hauptsächlich für die Werbung, weil man so auch bei Geräten mit nur einer Antenne mit mehr als 1 GBit/s auf dem Karton prahlen kann.

Effizienter Parallelfunk

Die mit 802.11ac eingeführten, optional 160 MHz breiten Funkkanäle erlauben zwar, sehr viele Daten in einem Rutsch zu senden. Sie erhöhen aber auch die Wahrscheinlichkeit für gegenseitige Störungen mit Nachbarnetzen, die im selben oder teils überlappenden Frequenzbereich funken, sodass der WLAN-Datenstau wächst und nicht schrumpft.

So gab die High Efficiency WLAN Study Group (HEW SG) als Ziel vor, dass 11ax eine große Zahl von Geräten in verstopften Netzen viermal so schnell bedienen soll – was die Wi-Fi-6-Werber frech als generelle Regel verkaufen, die zu falschen Erwartungen führt: Viermal so schnell wie Wi-Fi 5 ist Wi-Fi 6 nur in seltenen Situationen.

Das Hauptargument für OFDMA (Orthogonal Frequency-Division Multiple Access) in 802.11ax dürfte gewesen sein, dass es auch ohne MU-MIMO parallele Übertragungen ermöglicht und im Verein mit MU-MIMO dessen Effizienz steigern kann.

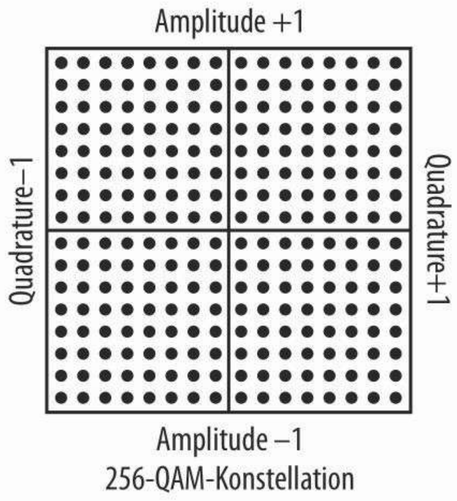
Bis hin zu 802.11ac belegt ein Datenpaket immer den gesamten Funkkanal. Weil aber jede Datenübertragung mit einer langsamen, also Sendezeit fressenden Startsequenz beginnt (Präambel), wird das Verhältnis zwischen deren Dauer und der Datenübertragung mit steigender Sendegeschwindigkeit immer ungünstiger.

Weniger Vorspann

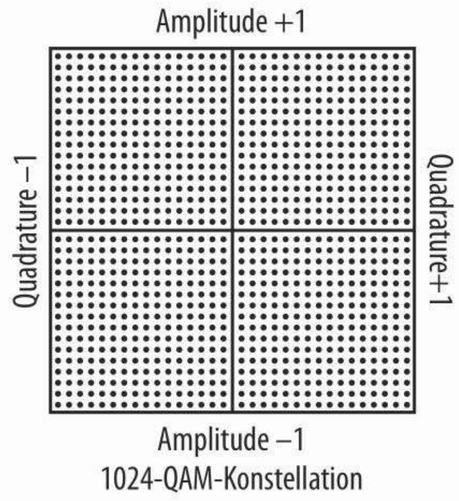
Da sich die Präambeln nicht beliebig verkürzen lassen, muss für mehr Effizienz ihre Häufigkeit sinken. Sendet man mehrere Datenpakete gleichzeitig in unterschiedlichen Bereichen des Funkkanals, genügt eine Präambel für alle, wodurch sich das Verhältnis von Nutz- zu Verwaltungsdaten verbessert. Bei OFDMA unterteilt die Basis den Funkkanal dazu in Resource-Units (RU) von 2, 4, 8, 20, 40 und 80 MHz.

Modulation

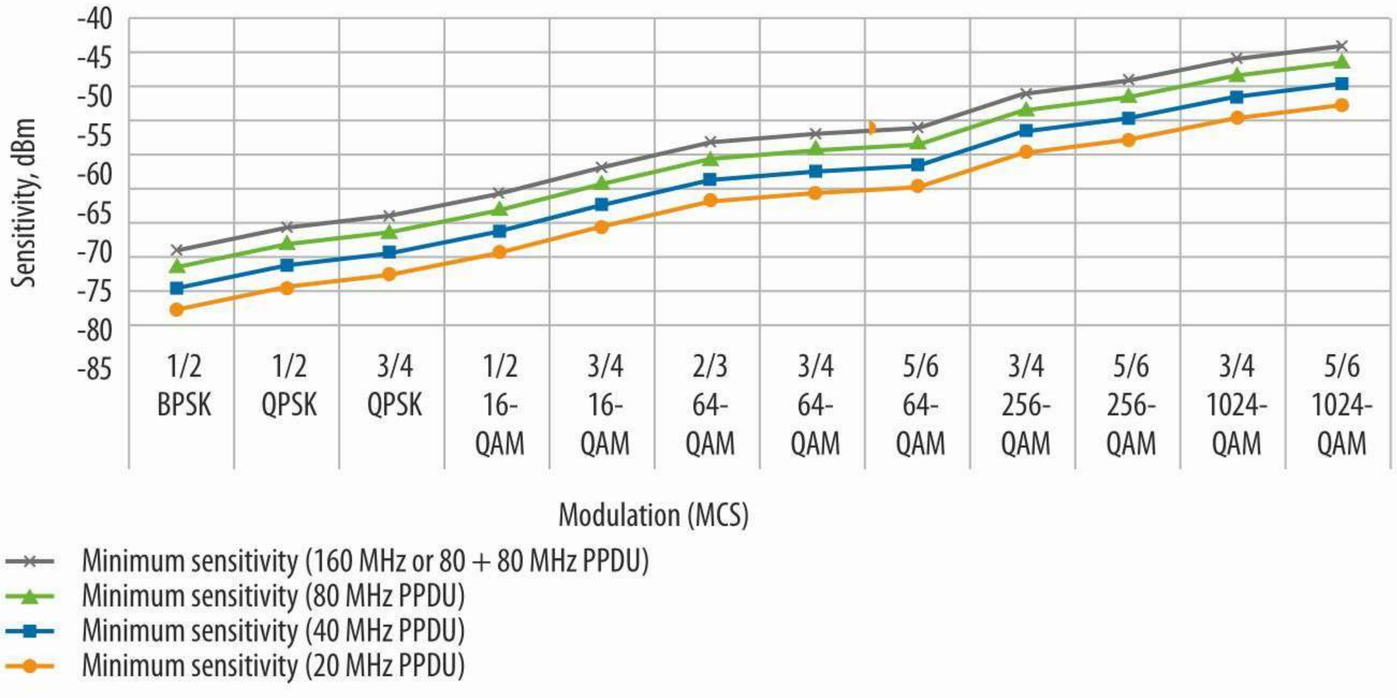
1024 mögliche Konstellationspunkte bei 1024-QAM in Wi-Fi 6 kodieren 10 statt 8 Bit (256-QAM) pro Symbol, erfordern aber auch ein deutlich stärkeres Signal. 25 Prozent mehr Durchsatz gibt es damit praktisch nur in unmittelbarer Nähe zur WLAN-Basis. Bei schlechter werdender Verbindung schaltet 11ax auf die robusteren Modulationen bis 16-QAM herunter.



256-QAM-Konstellation



1024-QAM-Konstellation



Ein 20-MHz-Kanal kann so aufgeteilt werden, dass die Basis beispielsweise eine Millisekunde lang gleichzeitig an fünf Clients sendet. Eine Station, die gerade einen großen Download zieht, bekommt dann etwa eine RU mit 8 MHz, eine zweite für ihren Videostream eine RU mit 4 MHz und die übrigen jeweils 2 MHz. Die restlichen 2 MHz gehen für Schutzabstände zwischen den RUs drauf.

Stationen, die per OFDMA parallel Daten empfangen, sollen diese bei 11ax auch gleichzeitig quittieren, statt wie früher nacheinander. Das erhöht den Zellendurchsatz ebenfalls.

Zentralsteuerung

Eine Wi-Fi-6-Basis soll OFDMA sowohl beim Senden als auch beim Empfangen nutzen. Dazu sammelt der AP zuerst Informationen zu der erwarteten Sendegeschwindigkeit der Clients und den in den Stationen wartenden Datenpaketen. Dann teilt er den Stationen die jeweiligen RUs mit Trigger-Frames zu.

So koordiniert die Basis den Zugriff auf den Funkkanal auch beim Empfangen. Alte WLAN-Hasen wird das an die im frühen IEEE-802.11-Standard definierte PCF erinnern (Point Coordination Function), die aber

nie praktische Anwendung fand. So wie eine Ampel verstopfte Kreuzungen verhindert, gewährleistet die zentrale Zuteilung bei vielen gleichzeitig aktiven WLAN-Teilnehmern eine flüssigere Übertragung, als wenn alle Stationen eigenständig um das Senderecht ringen.

Für Zufallszugriffe kennzeichnet die Basis außerdem Resource-Units in Trigger-Frames, um die die Stationen wie bei älteren WLAN-Verfahren konkurrieren: Sie warten eine zufällige Zahl dieser RUs ab und senden dann (Backoff). Damit sind Kollisionen zwar nicht sicher ausgeschlossen, aber der AP verringert sie durch das Vorgeben eines Intervalls für die Zufallszahl.

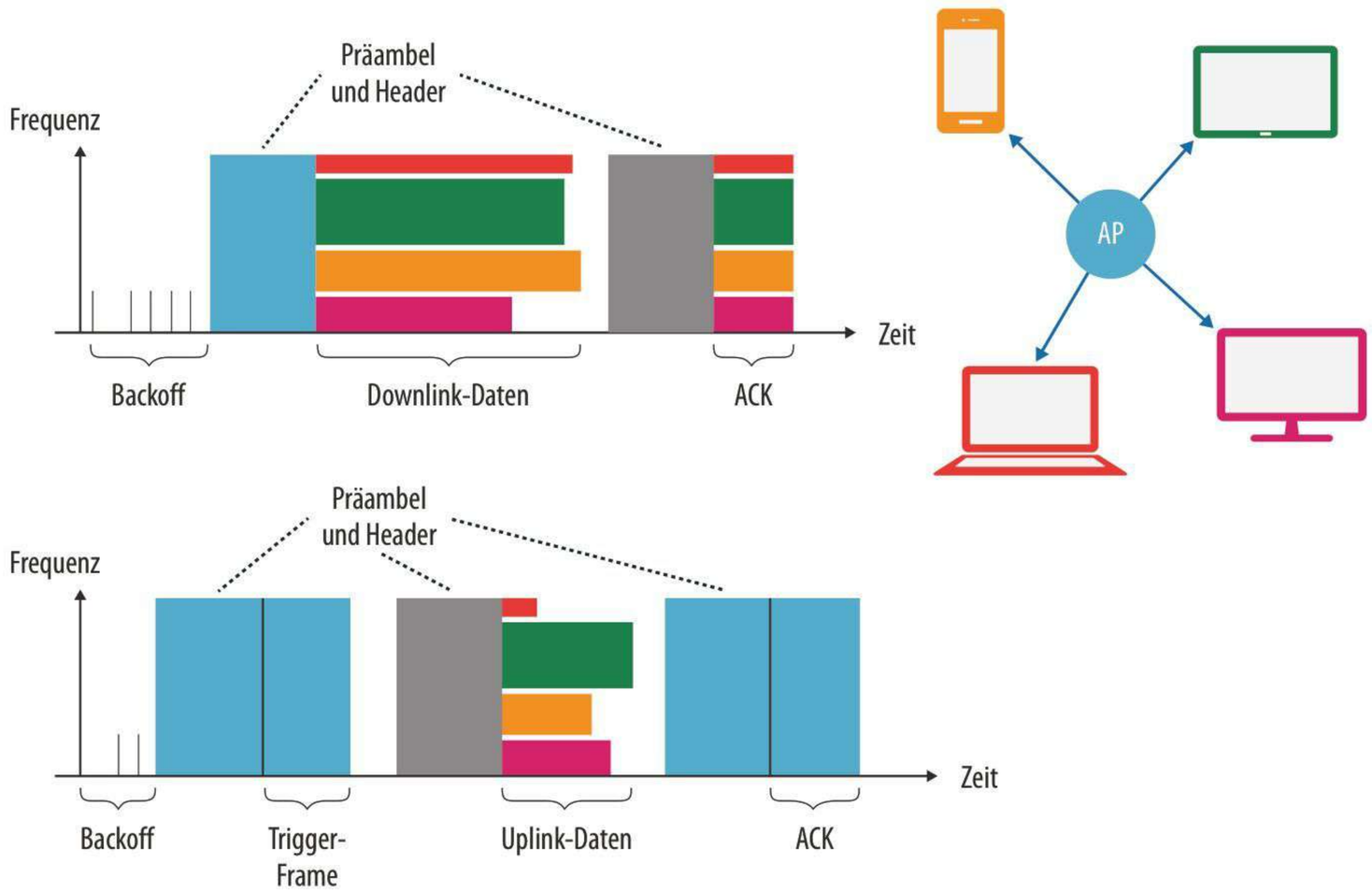
Dieser Zufallszugriff ist nicht nur wichtig, damit Stationen ihre Basis zwecks Planung der nächsten Trigger-Frames über die Menge der wartenden Daten informieren können: Auch brauchen ihn neue Stationen, um sich anzumelden.

Gewollte Lücken

Schließlich ermöglicht OFDMA einer WLAN-Basis auch, Frequenzblöcke auszublenden und so um störende Nachbarnetze „herumzufunken“. Im WLAN belegt der kleinste Funkkanal üblicherweise 20 MHz. Breitere Kanäle sind doppelt, viermal oder gar achtmal so groß und bieten damit eine entsprechend höhere Transportkapazität. Einen 80-MHz-Kanal darf eine Basis im Wi-Fi-5-Modus nur dann nutzen, wenn alle vier zusammengefassten 20-MHz-Blöcke frei sind. Wenn einer oder mehrere belegt sind, muss sie warten. 11ax kann aber zumindest die freien 20-MHz-Blöcke bündeln.

OFDMA-Downlink

Unterschiedliche Modulationsstufen auf den OFDM-Trägern ermöglichen bei Multi-User-MIMO, gleichzeitig Clients mit Daten zu versorgen, die die Basis verschieden gut empfangen (Downlink). Das steigert die Funkzelleneffizienz und soll bei der nächsten Gerätewelle (Wi-Fi 6 Wave 2) auch in umgekehrter Richtung funktionieren (Uplink)..



Bei parallelen Uplink-Übertragungen von mehreren Stationen könnte prinzipiell großer Verschnitt entstehen: Will etwa ein Client nur ein paar TCP-ACKs schicken, während ein anderer gerade ein Backup hochlädt, braucht Ersterer nur sehr kurz zu senden. Er müsste selbst in der schmalsten RU von 2 MHz viel Balast einsetzen (Padding), um auf die erforderliche Sendedauer zu kommen und dieselbe Uplink-TXOP nutzen zu können wie die Station, die das Backup sendet. Doch diese Bandbreitenverschwendung vermeidet 11ax durch variable Fragmentierung: Der zweite Client zerteilt seine Backup-Pakete vorübergehend in kleinere Häppchen, die besser zu den kurzen TCP-ACKs des ersten passen.

Ignorante Nachbarn

Das umstrittenste Thema in 11ax ist der „Spatial Reuse“: WLAN-Stationen sollen Nachbarnetze im selben Frequenzblock bewusst ignorieren, wenn die Verbindung zu ihrer Gegenstelle hinreichend gut ist. Das kann man sich wie die Gesprächsgrüppchen auf einer Party vorstellen: Alle reden innerhalb ihrer Gruppe, obwohl sie die Gespräche der anderen als Hintergrundrauschen wahrnehmen.

Entsprechend würde eine WLAN-Station also senden, obwohl sie nach dem herkömmlichen Zugriffsverfahren den Funkkanal als belegt ansehen und schweigen müsste (Listen before Talk). Dabei entscheidet die Station auch anhand des Signalpegels des fremden Netzes: Höhere Schwellen bedeuten kürzere Wiederverwendungsabstände.

Im mit rund 80 MHz vergleichsweise schmalen 2,4-GHz-Band hilft Spatial Reuse besonders. Selbst eine mäßige Verringerung des Wiederverwendungsabstands verbessert die Spektrumnutzung wesentlich, auch weil sich in den Lücken zwischen den WLAN-Signalen Bluetooth und Zigbee tummeln.

In der Praxis orientiert sich eine Station an zwei Schwellen: Kann sie die Präambel einer fremden Übertragung erkennen, gilt eine sehr niedrige Grenze, andernfalls eine hundertmal so hohe. Da der Präambelschwellwert so viel niedriger ist, sehen Stationen einen Kanal selbst dann als belegt an, wenn die Kommunikation weit entfernt von ihnen stattfindet. Das resultiert in einem sehr konservativen, großen Wiederverwendungsabstand und sequenziellen Übertragungen, obwohl genauso gut paralleler Betrieb möglich wäre.

Viele WLAN-Hersteller – darunter Cisco, HPE-Aruba, Huawei, Ruckus und Ubiquiti – haben schon länger proprietäre Funktionen in ihren APs untergebracht, um den Präambelschwellwert automatisch oder manuell auf beliebige, deutlich höhere Werte zu setzen. Der Preis für diese gleichzeitigen Übertragungen sind vermehrte Störungen zwischen den Nachbarn, die durch langsamere, robustere Modulation kompensiert werden. Weil die Funkzellen aber seltener aufeinander warten müssen, kann es sich dennoch lohnen.

Buntfunk

802.11ax definiert nun eine herstellerübergreifende Variante zum automatischen Setzen des Schwellwertes. Dazu bedient es sich beim Teilstandard 802.11ah (WLAN für IoT und Sensornetze unterhalb 1 GHz) und führt die „Färbung“ von Funkzellen ein (Coloring). Die Farbe ist eine 6-Bit-Kennung in der Präambel, die die WLAN-Basis zufällig setzt.

Weil die Kennung sehr früh in der Präambel erscheint, können 802.11ax-Geräte schnell entscheiden, ob die Sendung aus ihrem eigenen Netz kommt. Wenn nicht, heben sie ihre Präambelschwelle für die Belegt-Erkennung an. So können benachbarte Wi-Fi-6-Netze freie Kanäle häufiger identifizieren.

Gegenüber den proprietären Verfahren von Cisco & Co. hat Coloring den Vorteil, dass es auch für Clients funktioniert. Nachteilig ist hingegen, dass alte Geräte es nicht verstehen: Bei Sendungen an Wi-Fi-5- und ältere Stationen bleiben 802.11ax-Geräte aufgrund fehlender Farbe so konservativ wie eh und je. Außerdem passt sich der Mechanismus nicht den realen, sich ständig ändernden Funkbedingungen an. Bis auf den Coloring-Erfinder Broadcom sind die WLAN-Chip-Hersteller denn auch sehr vorsichtig bezüglich Aussagen zur Nützlichkeit des Verfahrens.

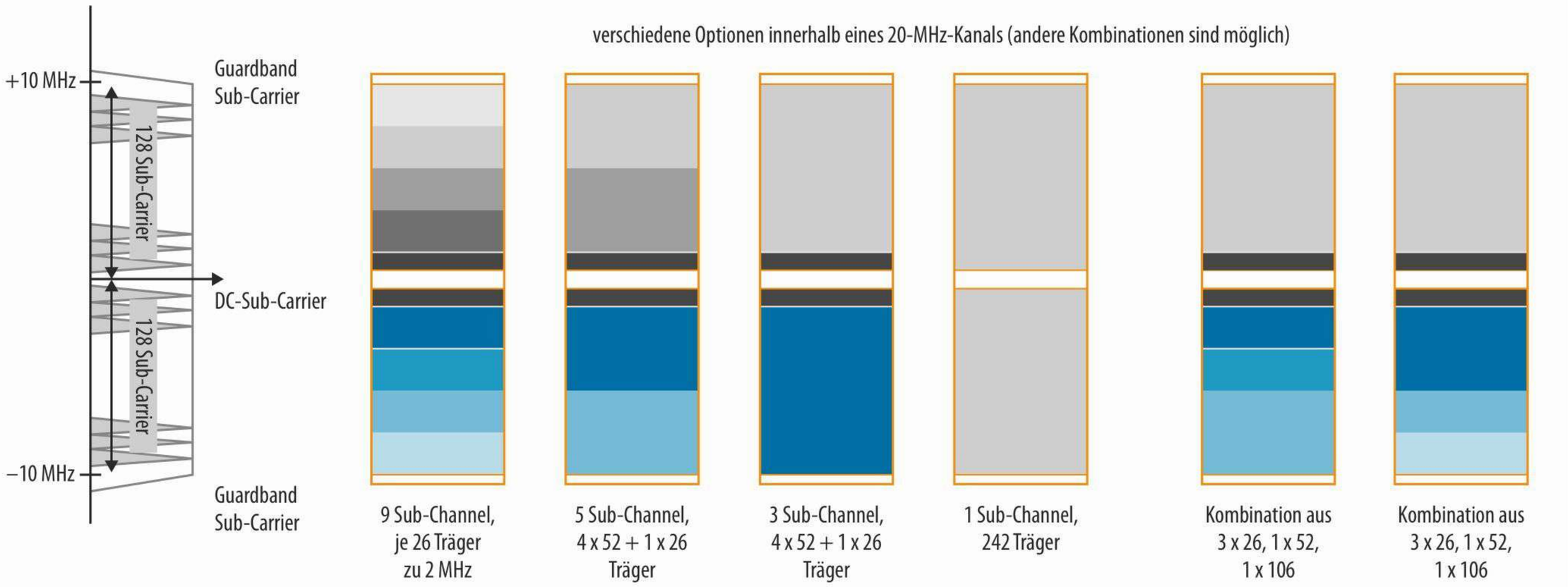
Eine andere Option für Spatial Reuse sieht vor, dass ein AP fremde Netze einladen kann, gleichzeitig zu senden. Dazu gibt der AP ein bestimmtes Maß an Störabstand vor, um dessen Einhaltung er bittet. Andere Netze können dann entscheiden, ob sie das Maß einhalten und gegebenenfalls parallel senden. Wenn sie ihre Sendeleistung verringern, dürfen sie im Gegenzug ihren Präambelschwellwert im gleichen Maß heraufsetzen: Wer leiser spricht, stört andere weniger und soll deshalb den Funkkanal leichter als frei behandeln dürfen.

Schlauer warten …

Ebenfalls aus 802.11ah hat Wi-Fi 6 ein Verfahren für verbessertes Energiesparen bei Clients übernommen: Target Wake Time (TWT). Ohne TWT müssen alle

Subträger-Verteilungen

256 Träger (Sub-Carrier) pro 20 MHz Kanalbreite erlauben bei OFDMA, die Datenraten pro Client feinstufig anzupassen. So kann Wi-Fi 6 etwa ein Smartphone genau zugeschnitten mit einem 10-MBit/s-Videostream bedienen und den Rest der Kanalkapazität einem Notebook zuschlagen, das ein großes VM-Image vom Server lädt. Die Aufteilung der Träger ändert sich von einer zur nächsten Sendegelegenheit abhängig davon, wie die jeweiligen MU-Clientgruppen zusammengesetzt sind.



Stationen, die sich bei der WLAN-Basis zum Energiesparen schlafend melden, regelmäßig aufwachen und prüfen, ob Daten bereitliegen. Der AP speichert diese nämlich zwischen und meldet das in seinen Beacon-Signalen, die er typischerweise rund zehnmal pro Sekunde sendet. In diesem festen Raster kommt es vor, dass viele Clients nach einem Beacon Daten bekommen. Bis die letzte Station versorgt wurde, muss sie aber unter Umständen akkuzehrend lange wach bleiben.

TWT führt Wachphasen für einen einzelnen Client oder eine Gruppe von Stationen unabhängig von den Beacons ein. Die Clients können so deutlich länger schlafen gehen. Ferner können Basis und Client die Wachphase individuell verhandeln, sodass ein akkubetriebenes Gerät viel seltener aufwachen muss als ein ans Stromnetz angeschlossenes. Außerdem begrenzt TWT die Anzahl der Stationen, die pro Durchgang Daten bekommen. Das verkürzt die Wachphase für den Listenletzten.

… mit Nickerchen

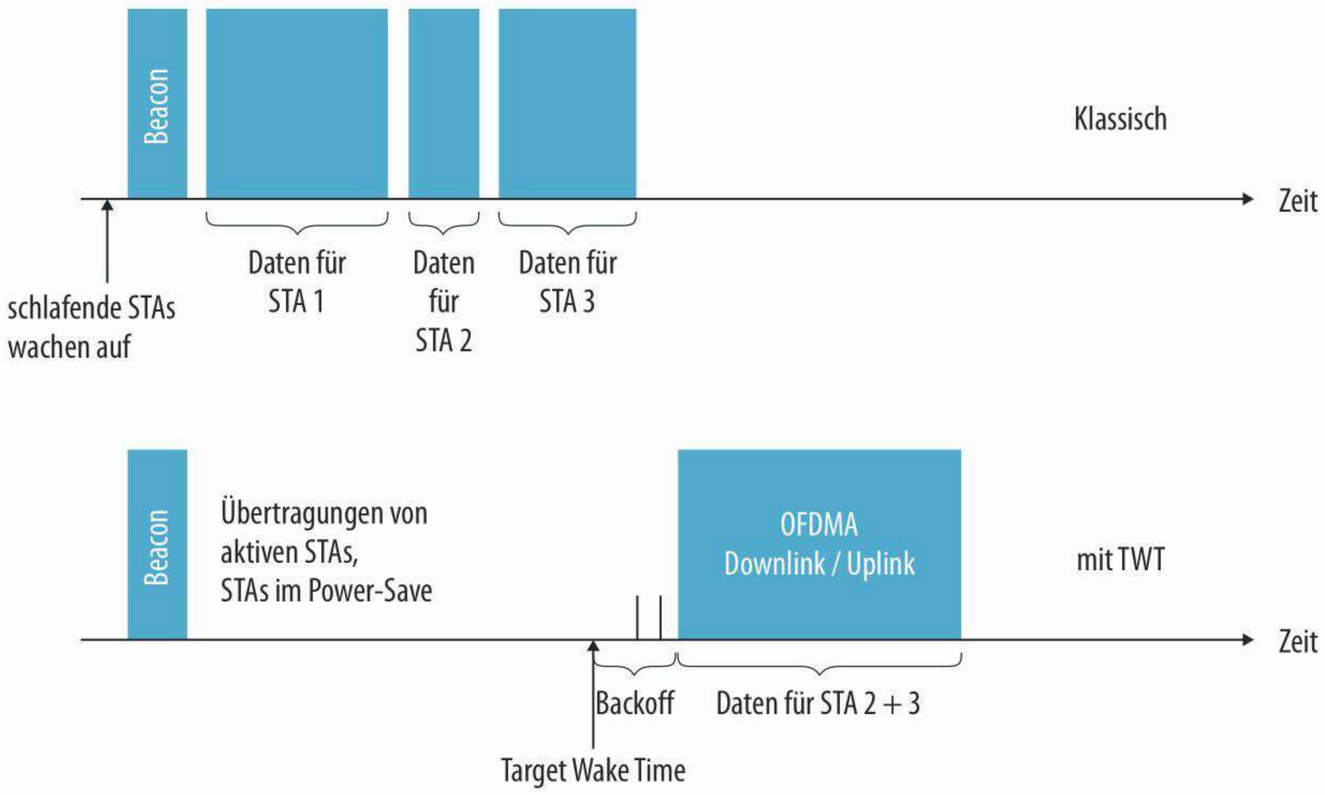
Schon bei Wi-Fi 5 enthält jeder WLAN-Frame neben den üblichen Adressinformationen einen Hinweis, welche Station angesprochen wird. Wi-Fi 6 verfeinert das so, dass Clients sehr kurz nach der Präambel erkennen, ob sie weiter zuhören müssen. Mit diesem Microsleep können Stationen schneller ins Stromsparen zurückfallen, wenn sie nichts erwarten.

Wi-Fi 6 bringt schließlich zwei Kniffe mit, die die Reichweite im Freien steigern sollen: 11ax-Geräte können größere Guard-Intervalle verwenden (Schutzabstand zwischen OFDM-Symbolen). Das senkt zwar den Bruttodurchsatz etwas, bewirkt aber auch, dass das System die im Freien typischerweise längeren Funkechos besser toleriert, die sonst aufeinanderfolgende Symbole stören.

Außerdem führt 802.11ax die Dual Carrier Modulation (DCM) ein: Damit teilt eine Station den Funkkanal in zwei Hälften und sendet auf jeder das glei-

Target Wake Time

Bisher mussten Stationen (STAs) passend zu den Beacons der WLAN-Basis aufwachen, schlimmstenfalls rund zehnmal pro Sekunde, um zu erfahren, ob Daten für sie vorliegen. Wi-Fi 6 lässt sie mit der Target Wake Time länger akkuschonend schlafen, um dann mehrere Clients in einem Rutsch zu bedienen (Multi-User-MIMO und OFDMA).



che Datenpaket mit doppelter Geschwindigkeit. Das ergibt zwar keinen Geschwindigkeitsgewinn, aber eine zuverlässigere Übertragung bei starken Interferenzen innerhalb des Funkkanals.

Effizientere VLANs

Admins bringt 802.11ax ein Geschenk, das zwar schon lange in der WLAN-Norm steht, bislang aber nicht verpflichtend war: Mit MultiBSSID kann ein Access-Point mehrere VLANs in einem Beacon ankündigen.

Wenn Firmen heute mehrere logisch getrennte Netze – intern, Gäste, IoT – per Multi-SSID auf einer Basis nutzen, muss der AP für jedes VLAN eigene Beacons senden. Das drückt den Zellendurchsatz enorm, denn die Beacons wurden im Laufe der Jahre durch neue WLAN-Features immer größer. Außerdem werden sie zeitfressend mit der langsamsten Funkdatenrate gesendet, damit alle Stationen sie sicher dekodieren können. Das Zusammenfassen per Multi-BSSID bringt also in Firmen besseren Durchsatz – sobald genug 11ax-Clients verbreitet sind, die das verstehen.

Was bringts?

Dass 802.11ax alias Wi-Fi 6 auf dem Papier nun auch in einfachsten Geräten mit nur einer Antenne das Gigabitlimit knackt, ist der WLAN-Industrie ein willkommener Werbegag. Aber auch mit potenteren Clients wird man gegenüber Wi-Fi 5 im heimischen WLAN kaum Verbesserungen bemerken, denn zu gering ist dort typischerweise die Anzahl tatsächlich gleichzeitig aktiver Geräte. Mit sinkenden Preisen werden am ehesten noch billige IoT-Sensoren und Aktoren von 802.11ax profitieren, die dank 2 MHz Kanalbandbreite größere Strecken überbrücken.

Seine Vorteile wird Wi-Fi 6 überall dort ausspielen, wo viele Clients auf engem Raum zusammenkommen, also in Stadien, Bahnhöfen, Konzertsälen, Schulen und Flughäfen – sobald genügend Geräte im Markt sind, die 802.11ax unterstützen.

Die Wi-Fi Alliance (WFA) zertifiziert 802.11ax schon seit 2019 als Wi-Fi 6, wobei die erste, Mitte 2019 erschienene Gerätegeneration die wichtigsten Funktionen von 802.11ax mitbringt und mit der besseren WPA3-Verschlüsselung bündelt.

Für das laufende Jahr 2021 darf man Wi-Fi-6-Geräte erwarten, die das geplante, unlizenzierte 6-GHz-Band nutzen (Wi-Fi 6E) und so das zu erwartende Gedränge im 5-GHz-Band mildern.

Anno 2023 dürfte Wi-Fi 6 Wave 2 als zweite 11ax-Generation erscheinen, was heute noch optionale Features zur Pflicht macht, beispielsweise MU-MIMO im Uplink.

Ausblick

802.11ax kämpft noch mit Anlaufschwierigkeiten, obwohl die WFA-Zertifizierung „Wi-Fi 6“ eigentlich den Grundstein für herstellerübergreifende Kompatibilität legen sollte. So schaltet ein führender Chip-Produzent viele Wi-Fi-6-Funktionen nur dann frei, wenn auch in der Gegenstelle Bausteine von ihm zum Einsatz kommen.

Wi-Fi 6 ist mit seinen neuen Funktionen wie den Trigger-Frames und TWT deutlich komplexer als seine Vorgänger. Berichte über Sicherheitslücken in Firmware und Treibern von 11ax-Chips werden so sicher kommen wie das Amen in der Kirche.

Dennoch arbeitet das IEEE bereits am Nachfolger: Neue Funktionen wie Distributed MIMO in 802.11be bauen auf der zentralen Koordination von 802.11ax auf. Damit sollen mehrere Access-Points gleichzeitig an mehrere Stationen senden, sodass quasi eine virtuelle, verteilte WLAN-Basis mit Antennen an unterschiedlichen Orten entsteht. Damit das funktioniert, müssen die Access-Points auf das OFDM-Symbolraster bezogen zeitlich koordiniert arbeiten, also auf weit unter eine Mikrosekunde Unterschied synchronisiert sein. Es wird spannend, ob der Gewinn den Aufwand rechtfertigt.

Auch wenn heute schon mit 160 MHz überbreite Funkkanäle in der Praxis selten nutzbar sind, wird 802.11be bis zu 320 MHz breite Kanäle definieren. Die dürften sich nur im hoffentlich bald verfügbaren 6-GHz-Band nutzen lassen.

Dass Wi-Fi-7-APs eines Tages gar mit 16 Antennen (MIMO-Streams) erhältlich sein werden, ist hingegen unabhängig vom Frequenzspektrum nützlich. Weil Clients nimmer Platz für 16 Antennen haben werden, bringt das abermals hauptsächlich in dicht besetzten Szenarien spürbaren Nutzen. (ea) c't

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



Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur nur **16,50 €**

www.iX.de/testen

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

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Was für Ihre nächste Fritzbox wichtig ist

Nach einiger Zeit im Homeoffice und Arbeiten in der Cloud kann schon mal der Wunsch nach mehr Internet-Geschwindigkeit wachsen. Mit einem schnelleren Anschluss muss meist auch ein neues Zugangsgerät her, was oft eine Fritzbox ist. Wir zeigen, welches Modell wo am besten passt und wie man den Boxen neue Tricks beibringt.

Von **Ernst Ahlers**

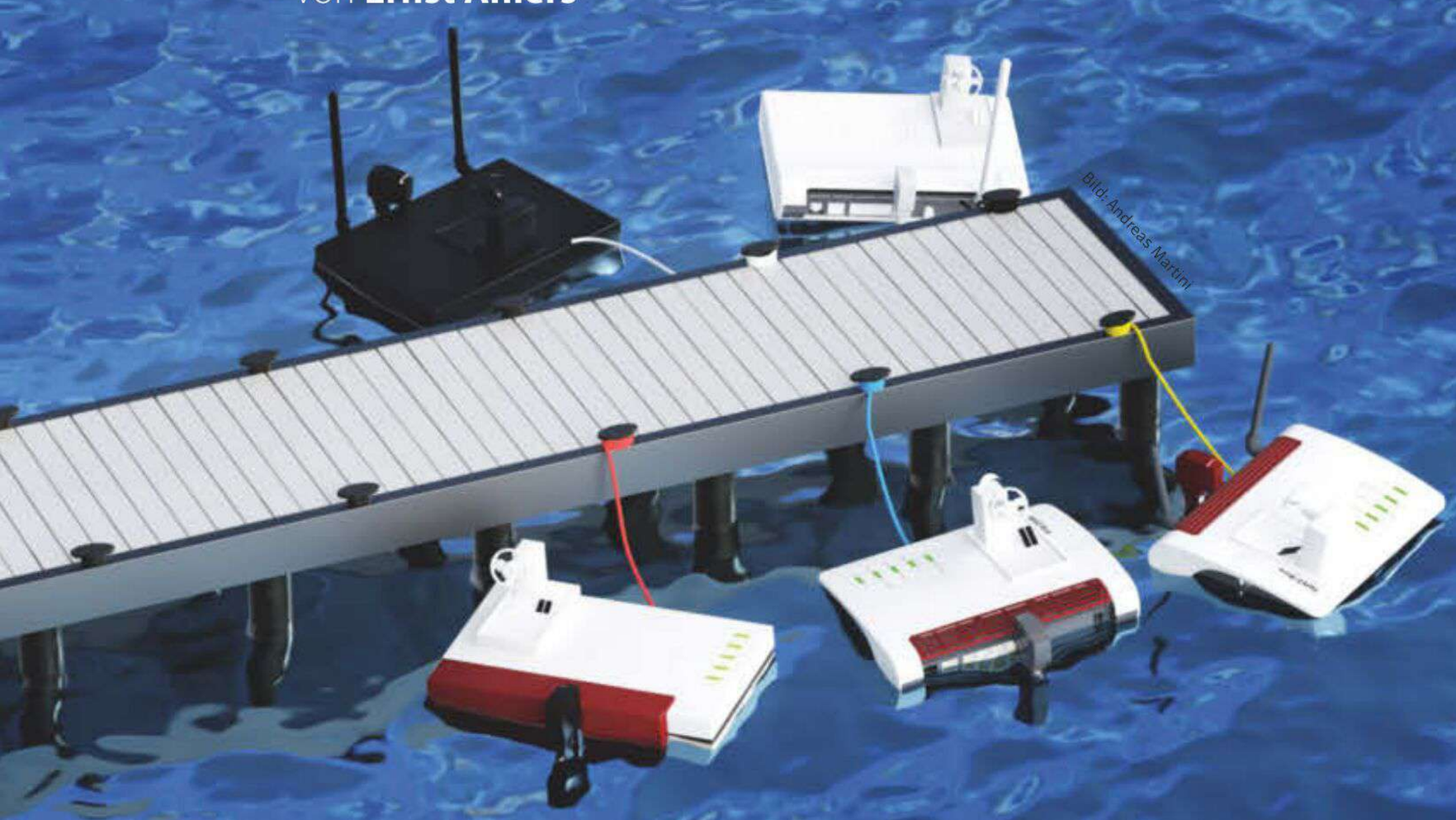


Bild: Andreas Martini

Auswahlhilfe für den Router-Kauf	76
Strategien gegen Internetausfälle	82
Erste Hilfe bei Internetausfällen	88
Funkverlängerung gegen Internetausfall	94
Dateizugriff per SMB	102
DynDNS mit IPv6 leicht gemacht	112
Router für Glasfaser-Anschlüsse	116
Fritzchens Erleuchtung	117

AVM, die Mutter der zu Recht verbreiteten, oft geliebten Fritzboxen, macht auch nicht alles auf Anhieb richtig, aber mehr richtig als viele andere Routerhersteller. Wer etwa die Vorteile des IPv6-Protokolls – jeder Rechner ist prinzipiell von überall her erreichbar – nutzen will, hat praktisch nur die Auswahl zwischen einer Fritzbox oder teureren Geräten für den Unternehmenseinsatz von Firmen wie Bintec, Draytek oder Lancom Systems. Denn bei IPv6 scheiterten in bisherigen c't-Tests viele Router anderer, im Small-Office / Home-Office-Segment (SOHO) tätiger Hersteller immer wieder an fehlenden oder falsch programmierten Optionen (zum Beispiel bei Dienstfreigaben unter wechselndem IPv6-Präfix).

Beim Internet per TV-Kabel – da wird IPv6 besonders wichtig, weil es kaum „richtiges" IPv4 mehr gibt – steht AVM ohnehin allein auf weiter Flur, wenn man sich nicht auf das vom Internetversorger angebotene Gerät verlassen will. Denn die Provider ordern gerne bei Fernost-Fabrikanten Modelle, die „einfach nur Internet" liefern. So sparen sie Kosten und hoffen, ihren Supportabteilungen das Leben zu erleichtern.

Fehler in der Betriebssoftware der Router, also der Firmware, werden bei den Providergeräten durchaus behoben. Aber so häufige Updates wie bei AVMs FritzOS, die auch Funktionserweiterungen – also einen Mehrwert – mitbringen, gibt es anderswo nicht. Kurzum, wer am Kabelanschluss sein Recht auf freie Wahl des Routers ausüben will, kommt an den Fritzboxen kaum vorbei.

Typische Datenraten

Anwendung	Datenrate (MBit/s)
Chat / Messaging	0,01
Telefonie[1]	0,05 – 0,20
Audiostreaming[1]	0,06 – 0,26
Videokonferenz-Upstream (HD)[1]	1 – 4
Videostreaming (Full HD)[1]	4 – 10
4K-Video (UHD)[1]	10 – 30
Dateitransfer (Bilder bei Chats etc.)	was die Leitung hergibt

[1] je nach App, Codec und Kompressionsgrad

Wir geben auf den folgenden Seiten Ratschläge, worauf Sie bei der Anschaffung der zu Ihrem neuen Internetanschluss passenden Fritzbox achten müssen und schauen außerdem auf Optionen, die zurzeit besonders wichtig sind (VPN zwischen Homeoffice und Fritzbox in der Firma) beziehungsweise jetzt relevant werden, also schnelles (W)LAN mit NBase-T alias Multigigabit-Ethernet und Wi-Fi 6. Wo es passt, führen wir die aktuell erhältlichen Modelle mit ihrer Nummer auf.

Providerauswahl

Welche Fritzbox Sie brauchen, hängt in erster Linie davon ab, für welches Internetangebot von welchem Provider Sie sich entscheiden. Denn der gibt die Wide-Area-Network-Zugangstechnik (WAN) vor: DSL/G.fast per Telefonkabel, DOCSIS übers TV-Kabel,



Fünf Fritzboxen bieten Auswahl für die drei wichtigsten Zugangsarten: DSL (7590 und 7530), TV-Kabel (6660 und 6591) und LTE-Mobilfunk (6890 LTE).

Mobilfunk oder Glasfaser. Zwar lassen sich die verschiedenen Fritzboxen-Typen über externe Modems prinzipiell auch an anderen Zugängen betreiben, aber das hat gleich mehrere Nachteile: höhere Stromkosten, mehr Geraffel auf dem Sideboard, eine weitere Fehlermöglichkeit, wenn „das Internet kaputt“ ist.

Dieser Weg ist jedoch unumgänglich, wenn der Provider eine Zugangstechnik einsetzt, für die es keine Fritzbox mit internem Modem gibt. Dann kommt beispielsweise das Modell 4040 infrage. Als Faustregel bleibt: Falls Ihr neuer Provider keine Fritzbox als Router bereitstellt, vergewissern Sie sich bei seinem Support, welche Modelle passen.



Das Modell 6660 ist die erste Fritzbox mit beschleunigtem Ethernet: Ihr LAN-Port 1, die abgesetzte gelbe Buchse, transportiert bis zu 2,5 GBit/s.

Flotte Auffahrt

Beim Internet per Telefonkabel (DSL) scheint mit Supervectoring-VDSL2 (7590, 7583, 7530, 6890 LTE) das Ende der Fahnenstange erreicht zu sein: Viel mehr als 250 MBit/s im Downstream und 40 MBit/s in Gegenrichtung geben die alten Leitungen nicht her, wohlgemerkt auch nur auf vergleichsweise kurzen Kabelstrecken von 150 bis 200 Meter. Darüber wirds weniger. Doch selbst 100 MBit/s dürften zumindest für die nächsten paar Jahre für die allermeisten Anwendungen genügen, sogar in Wohngemeinschaften, wenn drei 4K-Videostreams parallel laufen.

Außerhalb der Ballungszentren sind solche Geschwindigkeiten selten zu haben. Immerhin liefern stationäre Mobilfunkrouter wie die Fritzbox 6890 LTE per 4G-Technik Spitzenraten bis 100 MBit/s – wenn man eine auf 800 MHz sendende Basisstation in der Nähe und für sich allein hat. Doppelt so schnellen Landfunk bietet Vodafone in seinen jüngsten Ausbaugebieten, wo der Betreiber zusätzlich auf 700 MHz sendet. Da kommt noch keine Fritzbox mit, man braucht Vodafones GigaCube 5G.

Lediglich Heimarbeiter, die ständig viele große Dateien wie Ordner voller hochaufgelöster Raw-Bilder oder Images virtueller Maschinen hoch- und runterladen müssen, profitieren von Gigabit-Anschlüssen. G.fast (7583), das als Zubringer für die letzten Meter vom Glasfaseranschluss im Gebäudekeller (Fiber to the Building, FTTB) übers Telefonkabel in die Wohnung eingesetzt wird, hat da gegenüber VDSL2 einen Vorteil: Seine Bruttokapazität von 1000 beziehungsweise 2000 MBit/s, je nach Spezifikation, lässt sich flexibel auf die beiden Übertragungsrichtungen aufteilen. Heimarbeiter könnten also – falls der Provider mitspielt – auch symmetrische 500 MBit/s bekommen, immerhin etwas über 60 MByte/s brutto in beide Richtungen.

Internet per Koaxkabel

Bis die Glasfaser den Weg ins Wohnzimmer gefunden hat (Fiber-to-the-Home, FTTH), könnte sie längst vom Internet per TV-Kabel überholt sein: Anschlüsse, die mit dem Standard DOCSIS 3.0 laufen (Fritzbox 6490, 6430), geben jetzt schon 1000 MBit/s her, was bei Downloads über 100 MByte/s entspricht. Das will im Heimnetz erst mal verdaut sein, siehe folgend unter „Interne Beschleunigung“.

DOCSIS 3.1 (6591, 6660), das die Kabelprovider vielerorts schon ausbauen, legt eine Schippe drauf: Es definiert bis zu 10 GBit/s im Downstream und 1 GBit/s in Gegenrichtung. Bei letzterer gibt es in Kabelnetzen aber zurzeit trotzdem höchstens 50 MBit/s (6,3 MByte/s), und die nur in teuren Tarifen. Vodafone bietet für kleines Geld bei manchen langsameren Tarifen eine „Upload Option“ an, die aus 25 immerhin 50 MBit/s macht. Angesichts der schon bei DOCSIS 3.0 für den Upstream definierten 200 MBit/s wird ein TV-Kabelanschluss für Heimarbeiter damit zwar auch kein Renner, aber immerhin ein Quäntchen schneller als Supervectoring.

Die dürftige Uplink-Situation dürfte sich mit dem im März 2020 veröffentlichten DOCSIS-Standard 4.0 ändern: Er spezifiziert den Vollduplex-Betrieb mit paralleler Übertragung in beide Richtungen auf denselben Frequenzblöcken. So werden bis zu 6 GBit/s schnelle Uploads möglich – sobald die Kabelprovider ihre Netze dafür ertüchtigt haben. Das schließt die Glasfaser-Anbindungen der lokalen Kabelkonzentratoren (CMTS) ein. Denn die erweisen sich vielfach

vorgetragener Klagen zufolge in Stoßzeiten als Flaschenhals, sodass man dann den extraschnellen Anschluss nicht ausschöpfen kann.

Internet aus der Luft

Fritzboxen für Internet per Mobilfunk (6890, 6820) nehmen eine Sonderstellung ein, die sie beispielsweise fürs Wochenendhäuschen interessant machen: Die Mobilfunkanbieter deckeln den Datenverkehr übers LTE-Netz in den meisten Tarifen. Bei Überschreiten des für den Abrechnungszeitraum erlaubten Volumens bremsen sie den Zugang so drastisch, dass der Anschluss nur noch für langsames Websurfen und E-Mail taugt.

Möglicherweise ändert sich das mit dem Ausbau des 5G-Netzes, das wesentlich höhere Geschwindigkeiten als LTE verspricht. Im Lauf des Sommers 2021 will AVM endlich seine schon 2019 angekündigte, dazu passende Fritzbox 6850 5G auf den Markt bringen. Das Gerät soll im 5G-Mobilfunknetz bis zu 1,3 GBit/s übertragen können, aber auch in älteren LTE- und sogar UMTS-Netzen noch funktionieren.

Internet per Licht

Wenn das Internet schon per Glasfaser ankommt, hängt meist ein Glasfaser-Modem (genauer: ein Medienwandler) des Providers an der Wand. Daran kann man prinzipiell alle Router anschließen, die Ethernet als WAN-Zugang nutzen. Hat eine Fritzbox keinen separaten Port dafür, dann kann man ihren LAN1-Anschluss dahingehend umkonfigurieren. Wichtig ist, dass der Router das vom Provider verwendete Zugangsprotokoll verwendet (PPPoE oder DHCP), und zwar für beide Internet-Protokollvarianten, IPv4 und IPv6.

Manche Router – etwa die Fritzboxen 5490 und 5491 – haben ein integriertes, die neue 5530 sogar ein wechselbares Glasfasermodul. Sie können daher ohne externes Modem an die Faserdose angeschlossen werden. Das senkt den Energiebedarf etwas,



muss vom Provider in seinen Nutzungsbedingungen aber zugelassen sein.

Interne Beschleunigung

Die in den kommenden Jahren zu erwartende Internetbeschleunigung über 1 GBit/s hinaus wird zur Herausforderung fürs interne Netz, denn hier sind bislang Gigabit-Ethernet (940 MBit/s netto übers LAN-Kabel) und WLAN gemäß Wi-Fi 5 üblich, das bei typischen Clients bestenfalls im Nahbereich 500 MBit/s netto transportiert.

Das 2012 als IEEE 802.11ac erschienene Wi-Fi 5 ist trotzdem noch nicht veraltet, denn sein sich jetzt ausbreitender Nachfolger Wi-Fi 6 (IEEE 802.11ax) liefert bei gleichen Randbedingungen (Funkkanalbreite, Antennenzahl) bestenfalls 40 Prozent mehr Datenrate. Dafür kann es in Funknetzen mit vielen Clients Vorteile ausspielen (siehe Seite 68).

Entscheidend ist bei beiden die Anzahl der parallel genutzten Antennen: 4-Stream-MIMO, etwa bei der 7590, liefert eine höhere Summendatenrate als 2-Stream-MIMO (7530). Mehr Streams werden wichtig bei vielen gleichzeitig aktiven Clients (MU-MIMO) und wenn man das Funknetz mit Repeatern ausdehnen will. Kombinieren Sie dann idealerweise 4-Stream-Repeater mit 4-Stream-Routern. Künftig wird AVM seiner Fritzbox 6660, der ersten mit Wi-Fi 6, gewiss weitere Modelle zur Seite stellen. Die senden dann wahrscheinlich auch mit mehr als zwei MIMO-Streams.

Beim LAN-Kabel breitet sich langsam das Multigigabit-Ethernet namens NBase-T aus: Es geht über die Stufen 2,5 und 5 GBit/s bis zu 10 GBit/s hoch. Außer in einzelnen Routern wie der Fritzbox 6660 steckt NBase-T auch schon in neueren Mac-PCs. Es lässt sich bei Windows- und Linux-Rechnern per Steckkarte und USB-Adapter nachrüsten. Leider sind Ethernet-Switches mit mehr als zwei NBase-T-Ports immer noch einige hundert Euro teuer, aber das dürfte sich mittelfristig ändern.

Begrenzter Fernzugang

Eine viel genutzte Fritzbox-Funktion ist ihr VPN (Virtual Private Network mit dem IPsec-Protokoll), also die verschlüsselte Vernetzung beispielsweise von einem Notebook aus einem fremden Netz mit dem eigenen. Wir haben bei einer Auswahl aktueller Router an einem Supervectoring-Anschluss mit einer Kapazität von 250/40 MBit/s gemessen, welche VPN-Datenrate sie mit der im April 2020 aktuellen Firmware liefern (siehe Balkendiagramm unten). Dabei nutzten wir ein aktuelles Windows-10-Notebook im Verlagsnetz (mit 1 GBit/s symmetrisch ans Internet angebunden) und konfigurierten es wie von AVM in der Fritz-VPN-Anleitung für Windows empfohlen (ct.de/w48q).

Wer aus dem Homeoffice mit einem separaten VPN-Client auf dem Firmen-Notebook aufs Firmen-Netzwerk zugreift, für den ist die VPN-Leistung der Boxen belanglos. Denn in dieser Konstellation muss

VPN-Durchsätze gängiger Router

Modell	Firmware-Version	Downstream (1 × TCP) [MBit/s]	Upstream (1 × TCP) [MBit/s]	Downstream (6 × TCP) [MBit/s]	Upstream (6 × TCP) [MBit/s]	RTT (Ping-Mittelwert) [ms]	Leerlaufleistung [W]
		besser ▶	besser ▶	besser ▶	besser ▶	◀ besser	◀ besser
Fritzbox 7590	7.12	23	17	22	18	8,7	8,5
Fritzbox 7530	7.14	18	15	19	16	8,2	5,5
Fritzbox 7490	7.12	9,5	8,1	9,4	8,3	11,5	7,6
Fritzbox 6890 LTE	7.13	23	19	23	19	9,4	8,3[3]
Fritzbox 6660[1]	7.14	22	30	24	31	8,8	13,9
Fritzbox 6591[1]	7.13	18	36	21	35	9,1	12,5
Fritzbox 6590[1]	7.12	23	19	24	19	8,6	11,6
Fritzbox 4040[2]	7.14	19	14	18	15	8,3	3,5
Asus DSL-AC68VG	5.00.08-272	32	28	33	28	9,1	10,8
Draytek Vigor 2865	4.0.6	218	42	252	42	6,8	6,1
Netgear RAX120[2]	1.0.1.118	64	42	63	42	7,4	14,1[4]

OpenVPN bei Asus und Netgear, sonst IPsec
[1] als Exposed Host über Draytek Vigor 165 als Supervectoring-Router [2] mit Draytek Vigor 165 als Supervectoring-Modem [3] nur xDSL, kein LTE-Link [4] nur Router

der Router den bereits vom Laptop verschlüsselten VPN-Verkehr ja nur durchleiten, was keine zusätzliche Rechenleistung erfordert.

Läuft die Fritzbox hingegen im Büro einer Kfz-Werkstatt oder einer kleinen Anwaltskanzlei als VPN-Gateway und muss man häufiger von zu Hause aus aufs dortige Netz zugreifen, dann setzt die Box die Grenze: Selbst über unsere flotten Anschlüsse gingen bei der Fritzbox 7590 bestenfalls 23 MBit/s durch, also nur knapp 3 MByte/s. Die zum Vergleich herangezogene 7490, ein älteres, aber noch weit verbreitetes Modell, blieb mit knapp 10 MBit/s sogar noch deutlich dahinter.

VPN-Beschleunigung

Eine Besserung gibt es ab FritzOS 7.20: AVM hat nach eigenen Worten im Labor „deutlich über 60 MBit/s“ gemessen, an einem realen Anschluss praktische Werte bis „über 30 MBit/s“.

50 Prozent mehr VPN-Datenrate für Fritzboxen allein durchs Firmware-Update sind erfreulich, aber andere können VPN noch besser: Der Netgear RAX120, ein Breitband-Router ohne Modem, aber mit dem derzeit leistungsfähigsten WLAN (Wi-Fi 6 mit 8 MIMO-Streams, c’t 19/2019, S. 88), lieferte mit OpenVPN immerhin 64 MBit/s – und das, obwohl OpenVPN notorisch langsamer ist als das dem Fritz-VPN zugrunde liegende IPsec (ct.de/w48q). Jedoch schluckt der RAX120 deutlich mehr kostentreibenden Strom im Leerlauf (13,5 Watt) als die Fritzbox 7590 (8,5 Watt).

Drayteks Vigor 2865 hingegen – ein DSL-Router ohne WLAN und Telefonie für Firmen – schaffte es per IPsec-VPN sogar bei weniger Leistungsbedarf, den Supervectoring-Anschluss komplett auszulasten (252 MBit/s).

Alternativ-VPN

Zwar hat AVM die IPsec-VPN-Konfiguration laiensicher gestaltet und dokumentiert, womit auch ein Hobby-Admin sie zu bewältigen vermag. Problematisch bleibt aber vor allem für Kabel-Internet-Kunden, dass sich das Fritz-VPN immer noch nicht auf IPv6 als Trägerprotokoll versteht: Wer sein Netz an einem DS-Lite-Anschluss ohne öffentliche IPv4-Adresse betreiben muss, kann es nicht über das Fritzbox-VPN von außen erreichen.

Abhilfe ist – mit ein wenig Geld und Mühe – möglich, indem man der Fritzbox ein VPN-Gateway zur Seite stellt und dabei auf WireGuard als moderneres VPN-Protokoll wechselt. Wie OpenWrt und WireGuard auf eine Fritzbox-basierte „Schwesterkiste“ kommen, steht in c’t 10/2019, Seite 28. Spezielle Handreichungen für WireGuard auf mobilen Geräten finden Sie in c’t 10/2020, Seite 160.

Die in diesem c’t-Projekt verwendete Fritzbox 4040 schaffte mit WireGuard unter OpenWrt einen Verschlüsselungsdurchsatz von rund 480 MBit/s (c’t 17/2019, S. 72). Da sehen die auf der 4040 mit dem (zugegeben etwas ältlichen) FritzOS 7.14 und IPSec gemessenen 19 MBit/s dürftig aus.

FritzOS-Zukunft

Neben den üblichen kleinen Verbesserungen ist die moderate VPN-Beschleunigung nicht die einzige wesentliche Neuerung ab FritzOS 7.2x: Das WLAN erhält die verbesserte Verschlüsselungstechnik WPA3 (siehe Seite 60). Die muss man künftig so lange im Mischbetrieb mit WPA2 nutzen, bis nur noch WPA3-fähige Clients unterwegs sind. Das normalerweise per Passwort geschützte Gastnetz können beispielsweise Bistrobetreiber zum Hotspot umkonfigurieren, der dann die Sicherungstechnik OWE / Enhanced Open anbietet, also verschlüsselte WLAN-Verbindungen ohne Passwort.

Bei der Dateifreigabe (Windows-Shares) von an die Fritzbox angeschlossenen Massenspeichern kann man dank der dann angebotenen Protokolle SMB2 und SMB3 endlich das unsichere SMB1 hinter sich lassen. Ferner kommt verschlüsselte Telefonie (per TLS oder SRTP gesicherte SIP-Verbindungen) mit ausgewählten VoIP-Providern. DNS over TLS kann die Internet-Domainnamen-Auflösung verschlüsseln, was die Privatsphäre schützt.

Welche wählen?

Wer einen DSL-Anschluss nutzt, sieht sich zurzeit immerhin vier Fritzbox-Modellen gegenüber, Gebrauchtangebote einmal außen vor gelassen. Doch auch bei den anderen Zugangsarten gibt es Auswahl. Wenn es weniger aufs Geld ankommt, greifen Sie zum Topmodell. Das wird noch lange Zeit, wenn auch nicht ewig, FritzOS-Updates bekommen. Es hat in ein paar Jahren noch einen guten Wiederverkaufswert, falls Sie mit dem Provider auch die Zugangstechnik wechseln. Alle anderen greifen eher zum günstigsten Neugerät. Das ist zwar sparsamer ausgestattet, wird aber lange halten. Des Autors erste Fritzbox von 2013 läuft immer noch störungsfrei bei den Schwiegereltern. (ea) c't

VPN-Konfiguration, -Protokollvergleich, Firmware-Support

ct.de/w48q



Bild: Rudolf A. Blaha

Internetausfälle: Beste Strategien

Ob eigener Router oder Gegenstück beim Provider: Gelegentlich stirbt ein Stück Elektronik, das Netz ist weg und der Techniker muss anrücken. Die Zwangspause lässt sich mit wenig Aufwand von Tagen oder gar Wochen auf Minuten verkürzen.

Von **Ernst Ahlers**

Spätestens, wenn vor dem Homeoffice ein Bagger anrückt, um den Fußweg oder die Straße aufzureißen, sollten Sie sich wappnen: Bei Bauarbeiten beschädigte Kommunikationskabel können gleich ganze Wohnblöcke vom Internet abschneiden. Oft sind Netzausfälle aber weit weniger augenfällig und breitflächig, denn jede Elektronik verschleißt irgendwann, auch die von Netzbetreibern.

Ende 2017 brach des Autors Internetzugang zusammen: Der DSL-Router funktionierte, bekam aber kein Signal mehr von der Gegenstelle. Laut Techniker war unser Port in der Linecard im Konzentrator tot und auch kein anderer Port frei. Deshalb konnte er die Leitung nicht kurzerhand umklemmen. Bis eine Ersatzkarte aufgetrieben und installiert war, dauerte es rund zwei Wochen.

Glücklicherweise ließ sich die Wartezeit mit einem Mobilfunkrouter überbrücken, der als Testgerät samt Daten-SIM gerade in der Redaktion stand. So wurde die Misere zur Chance: Es entstanden zwei Praxisartikel, die schildern, wie man den heimischen Cloudserver trotz Provider-NAT aus dem Internet erreichen kann [1, 2].

Zwei Wochen lange Ausfälle sind gewiss selten. Doch auch wenn Ihre nächste Unterbrechung nur zwei Tage dauern sollte, kann sie hinderlich sein. Um bei einem Internetausfall im Handumdrehen wieder online zu kommen, müssen Sie aber nicht bei c't arbeiten, sondern sich nur mit ein paar Schritten vorbereiten: Zugangsdaten dokumentieren, mit dem Nachbarn sprechen, einen Zweitweg ins Internet planen und dafür eventuell etwas Hardware anschaffen.

Der Beitrag auf Seite 88 leitet zur Prüfung an, ob Sie das Problem vielleicht selbst beheben können, und schildert, wie Sie Umwege ins Internet schaffen, bis der Hauptanschluss wieder funktioniert. Ein Umweg führt oft über ein Mobilfunknetz, was mit einem begrenzten und teuren Datenvolumen einhergeht. Damit das Kontingent nach einem morgendlichen Ausfall nicht schon am Abend ausgeschöpft ist, muss man heimlichen Saugern vorübergehend die Datengier abgewöhnen, also an allen Geräten automatische Betriebssystem- und App-Updates vorübergehend ausschalten.

Was vor dem Ausfall zu tun ist

Falls Sie übers Festnetz telefonieren, prüfen Sie, ob die Zugangsdaten zu Ihrem Provider-Portal beziehungsweise Kundencenter funktionieren und fordern Sie sie gegebenenfalls neu an. Dann können Sie bei einem Netzausfall die Festnetznummern aufs Smartphone umleiten, wenn die Internettelefonie über Ihr Backup nicht zuverlässig funktioniert.

Es schadet auch nicht, die Zugangsdaten für den Internetanschluss sowie die Internettelefonie parat zu haben. Damit können Sie bei einem Defekt Ihres Routers ein Ersatzgerät in Betrieb nehmen, ohne erst beim Provider anfragen zu müssen. Sichern Sie die Einstellungen Ihres Routers gelegentlich, damit Sie sie beim Gerätetausch gegen ein identisches Modell einfach wieder einspielen können. Wer sich einen gebrauchten Router desselben Typs in den Schrank legt, ist dann binnen Minuten wieder online.

Alternativ-Wege

In vielen Wohnungen gibt es zwei Medien, die den Zugang zum Internet aufbauen können: die Telefonleitung (DSL) und das TV-Kabelsystem (DOCSIS). Davon nutzt man in der Regel nur eines. Das andere lässt sich leider nicht mal eben in Betrieb nehmen, denn es fehlt zumindest am Versorgungsvertrag mit



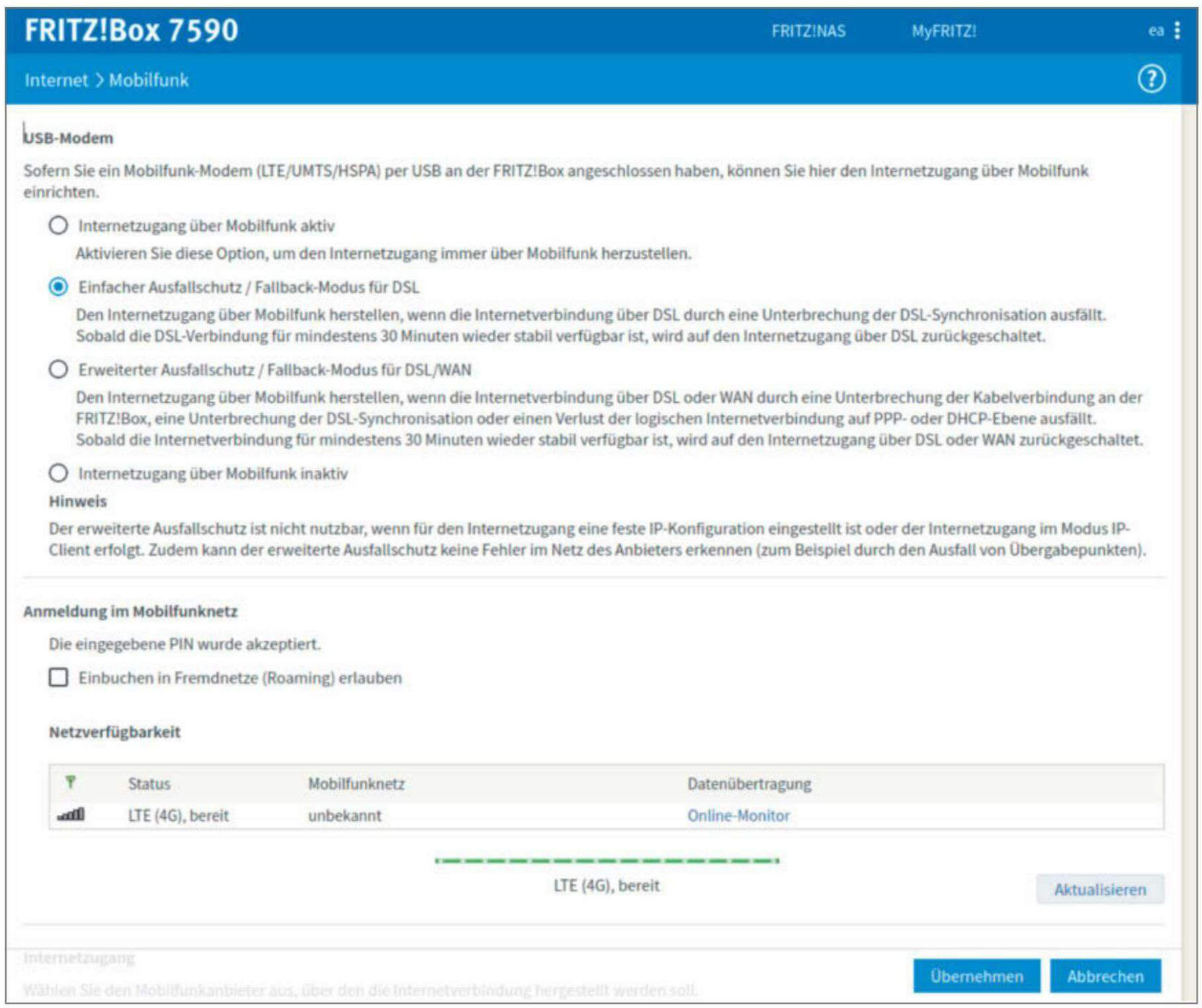
Ein USB-Mobilfunk-Stick (links) beziehungsweise ein LTE-Router (Mitte) schaffen einen zweiten Internetzugang, auf den dazu fähige WLAN-Router beim Ausfall des Hauptweges automatisch umschalten. Als Luxusvariante nutzt ein Load-Balancer (rechts) mehrere Zugänge per Lastverteilung, was nicht nur die Ausfallsicherheit erhöht, sondern auch die Internetgeschwindigkeit fürs lokale Netz.

einem Provider, oft auch am geeigneten Modem oder Router.

Wer einen besonders zuverlässigen Internetzugang möchte und nicht auf den Euro schauen muss, kann beide Wege mit einem speziellen Router kombinieren (Multi-WAN, Wide Area Network, dazu gleich mehr). Alle anderen haben zwei Ausweichmöglichkeiten: beim Nachbarn anklopfen, um vorübergehend dessen WLAN als Internetquelle anzuzapfen oder oben erwähnten Mobilfunkumweg selbst bauen.

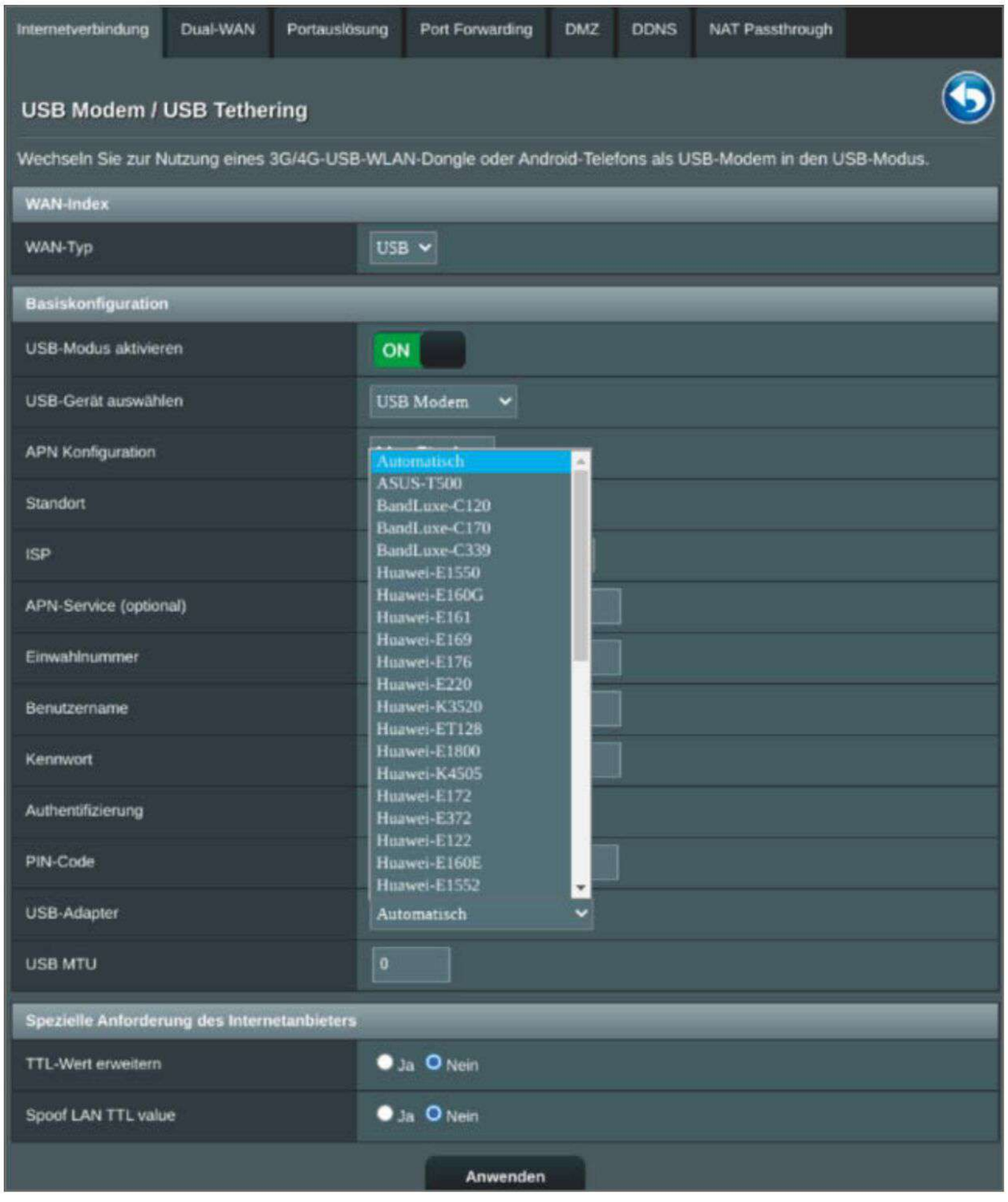
Beides kann ohne Investition in zusätzliche Hardware klappen: Manche Internet-Router können statt ihres Haupt-WAN-Zugangs (DSL, DOCSIS, Glasfaser) ihre WLAN-Schnittstelle als alternativen Internet-Uplink nutzen. Die Möglichkeit existiert allerdings nur, wenn Sie vollen Zugriff auf die Browser-Konfigurationsseiten eines eigenen Geräts haben – also keinen Provider-Router nutzen – und wenn das Modell diese Option beherrscht. Das ist beispielsweise bei AVMs Fritzboxen gegeben. Beherrscht Ihr Router den WLAN-Uplink nicht, hat aber einen Ethernet-WAN-Port für den alternativen Internetzugang, dann können Sie ihm einen WLAN-Client mit Ethernet-Ausgang vorschalten. Das kann auch ein WLAN-Repeater mit LAN-Port oder eine billig erstandene, gebrauchte Fritzbox wie das Modell 4020 sein.

Für den WLAN-Uplink bitten Sie Ihren Nachbarn um den Namen und das Passwort seines Gastnetzes sowie darum, darin alle Internetanwendungen freizugeben. Denn manche Router beschränken die Anwendungen im Gastnetz beispielsweise auf Surfen und Mailen, wodurch beispielsweise der VPN-Zugang zur Firma scheitert.



Fritzboxen können die meisten USB-Mobilfunk-Sticks als automatisches Internet-Backup nutzen. Bei Steuerung über den AT-Befehlssatz baut dann die Fritzbox die Internetverbindung selbstständig auf, wenn die Hauptleitung ausfällt.

Erkennt ein WLAN-Router den USB-Mobilfunk-Stick nicht automatisch, muss man bei manchen Routern aus einer Liste manuell wählen und hoffen, sein Modell dort zu finden. Wer sich solch ein Internet-Reserverad anhängen will, sollte vor dem Kauf recherchieren, mit welchen Sticks der Router harmoniert.



Mag der Nachbar nicht teilen, müssen Sie auf eine Funktion Ihres Smartphones zurückgreifen: Alle aktuellen Geräte können ihren Mobilfunk-Internetzugang per WLAN-Hotspot teilen. Aktivieren Sie den Hotspot und tragen Sie seine Zugangsdaten beim WLAN-Uplink Ihres Routers ein. So versorgt das Smartphone Ihr ganzes Netz, ohne dass Sie dessen WLAN-Clients auf den Smartphone-Hotspot um- und später wieder zurückkonfigurieren müssten. Falls Sie das Smartphone nicht entbehren können oder schlicht keines nutzen, bietet sich in USB-Mobilfunksticks ein Ausweg.

Schauen Sie dann, ob Ihr Mobilfunkprovider eine zubuchbare Daten-Dayflat anbietet und ordern Sie diese – falls die Störung länger als ein paar Stunden anhält, an jedem Morgen neu. Beispielsweise gibt es bei Prepaid-Angeboten der großen Mobilfunker wie Vodafone CallYa oder O2 my Prepaid für 5 Euro ein für eine vierköpfige WG gerade so brauchbares Tagesvolumen von 10 beziehungsweise 25 GByte. Andere Provider bieten auch bei diesem Vertragstyp unbegrenzte Dayflats an, beispielsweise Telekom DayFlat unlimited für 6 Euro.

Wer ein einfaches Smartphone mit Prepaid-Karte als Notfallreserve für die Familie vorhält, nimmt lieber dieses statt seines persönlichen Geräts. Denken Sie zum Schluss noch daran, das Handy an einen Ort mit gutem Mobilfunkempfang innerhalb der

WLAN-Reichweite des Routers zu legen, etwa auf die Fensterbank, und schließen Sie es per Ladegerät an die Steckdose an.

Reserve-Rat

Die oben geschilderten Wege setzen bei einem Internetausfall voraus, dass jemand vor Ort ist und den Router umkonfigurieren kann. Wenn das nicht gegeben ist, beugen Sie einem Internetausfall vor, indem Sie einen Router mit Failover-Funktion zu einem zweiten Zugang installieren. Solch eine Funktion steckt nicht nur in Routern für Firmenkunden, sondern auch in einigen für kleine Netze, unter anderem in Fritzboxen oder Asus-Geräten.

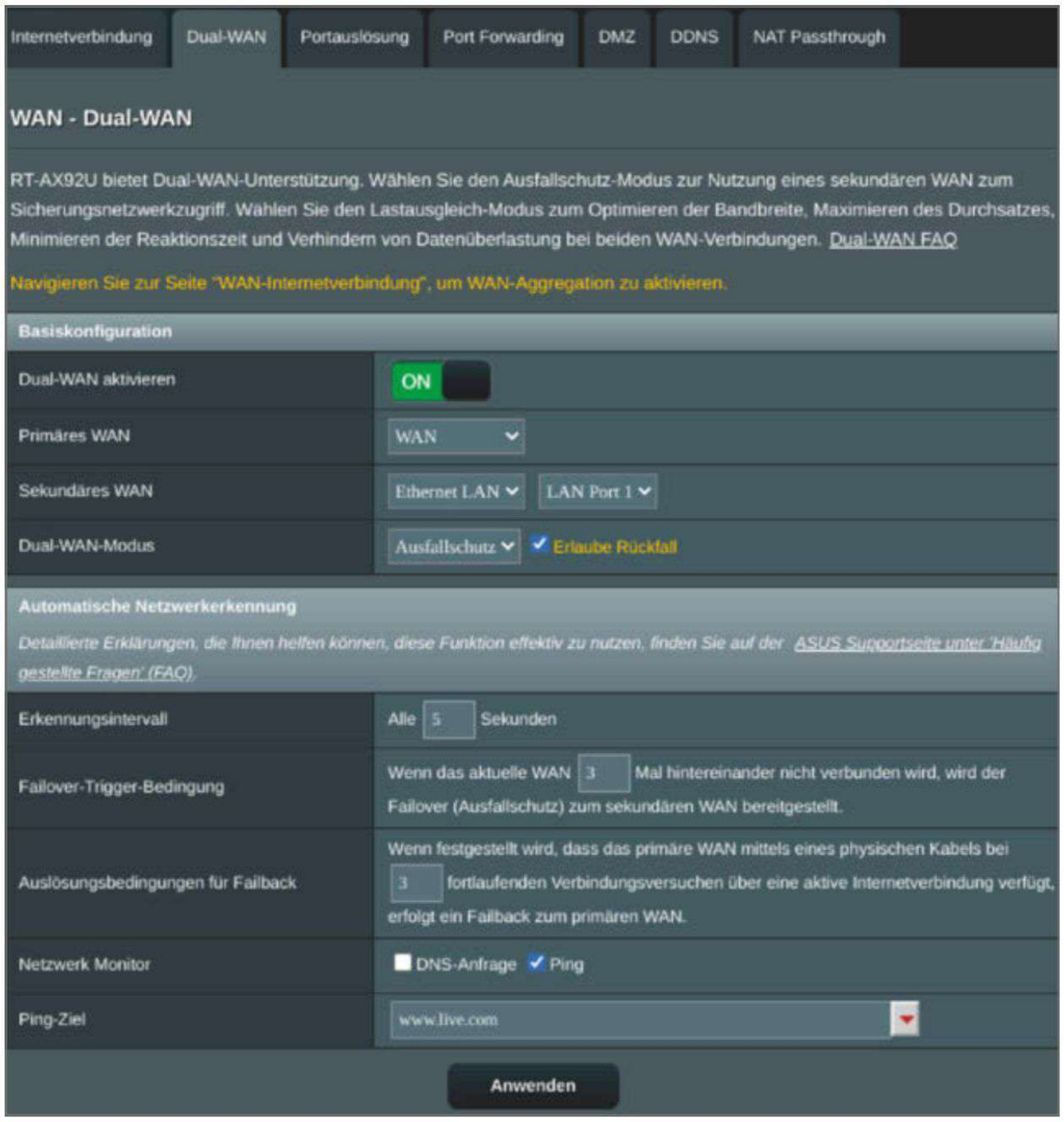
Der zweite Zugang wird meist per Mobilfunk aufgebaut, entweder über einen separaten USB-Stick oder einen Mobilfunk-Router mit 4G- oder 5G-Technik. Die Fritzbox 6890 LTE für Supervectoring-Anschlüsse (Test in c't 26/2017, S. 44) enthält bereits ein 4G-Modem. Zum Mobilfunk-Stick oder -Router brauchen Sie eine Daten-SIM-Karte (jüngste Tarif-Übersicht in c't 4/2020, S. 94).

Für 4G/LTE genügt ein USB-Stick vom Gebrauchtmarkt. Wenn der am PC funktioniert, ist aber noch lange nicht klar, dass er es auch am Router tut. Prüfen Sie das vor dem ersten Internetausfall. Erkennt Ihr Router den Stick nicht automatisch, können Sie meist aus einer kleinen Auswahl manuell wählen. Am besten recherchieren Sie vor dem Kauf in Internetforen, welche Sticks sich für Ihren Router eignen.

Legen Sie sich mit dem Stick auch ein USB-Verlängerungskabel mit drei bis fünf Metern Länge bereit: Oft ist der Mobilfunkempfang am Standort des Routers schwach. Mit der Verlängerung können Sie den Stick näher am Fenster positionieren. Das verbessert die Funksituation und erhöht die Internetgeschwindigkeit. Mit einer speziellen Adapterbrücke lassen sich auch Ethernetkabel als USB-Verlängerung nutzen. Bessere Adapter überbrücken so auch 50 Meter. Einzelheiten dazu finden Sie ab Seite 94.

Wer Unwägbarkeiten bezüglich der Kompatibilität von Router und Mobilfunkstick vermeiden will, kann sich alternativ einen günstigen stationären Mobilfunkrouter zulegen, der per LAN-Kabel als Ausweichverbindung an den Hauptrouter kommt. Solche Geräte gibt es neu für deutlich unter 100 Euro, beispielsweise den TP-Link TL-MR100. Ein älteres Exemplar wie Zyxels LTE-4506 – das weiße Tönnchen im Bild auf Seite 83 – findet man gelegentlich auch schon für unter 60 Euro. Wichtig beim Gebrauchtkauf: Lassen Sie sich keinen veralteten 3G-Router (HSPA, HSPA+) andrehen. Die Mobilfunk-Provider schalten nämlich nach und nach ihre UMTS-Netze ab. Der Internetzugang über GSM/Edge (2G) funktioniert zwar weiter, ist aber für heutige Ansprüche bei Weitem zu langsam.

Für Ausflüge oder Dienstreisen sind akkubestückte 4G- oder 5G-Router im Zigarettenschachtelformat als Hotspot beliebt. Auch solche Geräte lassen sich am heimischen Router als Backup nutzen. Das geht am einfachsten, wenn der Taschenrouter einen Ethernet-Port hat und dauerhaften Betrieb bei angeschlossenem Ladegerät erlaubt. Letzteres ist keine Selbstverständlichkeit: Schauen Sie vor dem Kauf ins Datenblatt oder in das Handbuch.



Bei Asus-Routern kann man die Reaktionszeit beim Internetausfall für den Übergang zur Ersatzleitung und zurück nach eigenen Vorstellungen anpassen. Außerdem beherrschen die Geräte nicht nur dieses Failover, sondern auch die Lastverteilung auf mehrere Festnetzverbindungen (Load-Balancing).

Literatur

[1] Ernst Ahlers, **Server-Umleitung**, Heimserver hinter DS-Lite oder CG-NAT erreichbar machen, c't 2/2018, S. 138

[2] Mark Liebrand, **UDP-Helfer**, Per UDP ins Heimnetz trotz CG-NAT und DS-Lite, c't 6/2018, S. 152

[3] Markus Stubbig, **Softe Datenverteiler**, Stabileres Internet mit Multi-WAN-Routern, c't 24/2016, S. 122

[4] Markus Stubbig, **Multi-WAN-Bau**, pfSense als Load-Balancer, c't 24/2016, S. 128

[5] Andrijan Möcker, **Freigekauft**, Router für OpenWrt: Von Komplettpaket bis Spartipp, c't 5/2021, S. 104

Gürtel und Hosenträger

Wer wegen häufiger Ausfälle des Internetzugangs immer wieder aus der Arbeit gerissen wird, sollte überlegen, ob sich eine zweite Festnetzverbindung lohnt: Bei der Lastverteilung (Load-Balancing) etwa über DSL und TV-Kabel bekommt man nicht nur höhere Down- und Upload-Geschwindigkeiten (in Summe für die Gruppe), sondern auch erhöhte Verfügbarkeit, weil beim Ausfall einer Verbindung der Verkehr automatisch über die verbliebene weiterläuft.

Zwei Anschlüsse kosten normalerweise mehr als einer und man braucht zusätzlich zu den Provider-Routern beziehungsweise -Modems einen Multi-WAN-Router mit Load-Balancing-Funktion. Aber diese Investition kann sich bei kleinen Firmen und Selbstständigen im Homeoffice schnell bezahlt machen. Und auch die restliche Familie profitiert vom zuverlässigeren Internet.

Multi-WAN-Router gibt es vorwiegend für den Firmeneinsatz und in zahlreichen Ausstattungsvarianten von vielen Herstellern, beispielsweise Cisco, Draytek, Lancom, Mikrotik, Peplink oder Zyxel. Auch der Selbstbau ist bei vergleichsweise bescheidenem Kapitaleinsatz mit Router-Betriebssystemen wie pfSense oder OpenWrt möglich [3, 4, 5].

Den Multi-WAN-Betrieb findet man ebenfalls in WLAN-Routern von Asus als zuschaltbares „Dual-WAN“, wahlweise über einen zum zweiten WAN-Port umzuwidmenden LAN-Port oder per optionalem Mobilfunk-USB-Stick. Auch hier hat man die Wahl zwischen Failover und Load-Balancing.

Besonders geschickt lässt sich das in einem Mesh-System etwa mit dem Asus RT-AX92U (Test in c't 13/2019, S. 86) hinter zwei Provider-Routern umsetzen: Der Mesh-Router bündelt deren Zugänge per Load-Balancing und leitet den so beschleunigten Internetzugang in sein LAN und Mesh-WLAN weiter.

Üben und wachsam bleiben

Für welchen der oben geschilderten Internetumwege Sie sich auch entscheiden: Probieren Sie Ihre Lösung aus, und zwar nicht nur beim Einrichten, sondern auch danach immer mal wieder. Falls Ihr Internet-Backup übers Mobilfunknetz führt, achten Sie bei Prepaid-Daten-SIMs auf zwei Dinge: erstens, dass genug Guthaben aufgebucht ist, um bei Bedarf eine Dayflat zu aktivieren, und zweitens, dass Sie die Daten-SIM wenigstens einmal im Jahr kurz benutzen, damit der Provider sie nicht wegen Inaktivität abschaltet. Lassen Sie sich gegebenenfalls vom Smartphone daran erinnern.

Mit den Tipps im folgenden Artikel können Sie sich weiter vorbereiten, bevor der eingangs erwähnte Bagger seine Schaufel schwingt. Erwischt diese statt des Kommunikationskabels aber die Energieversorgung, ist es Zeit für einen laaangen Spaziergang. (ea) c't

Ein Breadboard ist für Sie kein Schneidebrett?

Dann sind Sie bereit für den Einstieg in die Elektronik!

Make Elektronik Special

Make Elektronik Special bietet einen einfachen und praxisorientierten Einstieg in Transistorschaltungen, die Maker in eigenen Projekten einsetzen können. Das mitgelieferte Experimentierset inkl. Breadboard, Kabeln und 45 Elektronikbauteilen enthält alles, um die gezeigten Schaltungen sofort nachbauen und testen zu können. Dabei machen die speziellen Adapterplatinen den Aufbau zum Kinderspiel. Jede Menge Projekte zum Nachbauen sind ebenfalls dabei. Also – sofort loslegen!

shop.heise.de/make-elektronik21

Heft + Experimentierset für nur 44,95 € ›



Inklusive Experimentierset

Exklusiv im heise shop!

heise shop

shop.heise.de/make-elektronik21 ›

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



Bild: Rudolf A. Blaha

Internetausfälle: Erste Hilfe

Wenn die Internetverbindung ausfällt, bedeutet das merkliche Einschnitte. Doch anstatt auf die Hotline zu bauen oder auf die Reanimationskunst eines Technikers, können Sie mit ein wenig Vorbereitung die Ausfallzeit verkürzen und bestimmte Probleme mit etwas Know-how selbst beseitigen.

Von **Andrijan Möcker**

Die Abhängigkeit vom Internetzugang ist enorm. Umso ärgerlicher, wenn er ausfällt. Das passiert öfter, als man denken mag, denn gerade bei DSL – der Technik, die oft Jahrzehnte alte Telefonleitungen nutzt – sind die Übertragungswege gar nicht für derart breitbandige Anwendungen gedacht und auch DOCSIS- und Glasfaserverbindungen bleiben nicht von technischen Fehlern und Wartungsausfällen verschont. Die Lösung: Wissen zur Selbsthilfe und ein einfacher Plan für den Ernstfall.

Wenn der Router die Internetverbindung bereits verloren hat und auch nach 10 Minuten nicht selbst-

ständig wieder aufgebaut hat, sollten Sie zunächst den genauen Punkt in der Verbindungsstrecke identifizieren, der ausgefallen ist: Stellen Sie der Reihe nach sicher, dass Ihr Rechner mit dem Router verbunden ist, der Router noch Lebenszeichen zeigt (LEDs an) und dass alle erforderlichen Stecker eingesteckt sind.

Melden Sie sich dann über das Webinterface am Router an. Das klappt mit jedem üblichen Browser anhand der IP-Adresse des Routers http://<IP-Adresse>. Wenn Sie sie nicht geändert haben, finden Sie die IP-Adresse in der Anleitung.

Die Webinterfaces der Router variieren stark, die meisten enthalten aber eine Seite, die den Verbindungsstatus des Übertragungsmediums (DSL, DOCSIS, Glasfaser) anzeigt. Fritzboxen führen diese Information im Ausklappmenü „Internet“ auf. Der „Online-Monitor“ blendet „DSL-“ beziehungsweise „Kabel-Informationen“ als Untermenüs ein, die zeigen, ob der Router verbunden ist und ob ihm der DSLAM beziehungsweise die Kabelkopfstelle des Providers eine IP-Adresse zugewiesen hat; Fehler im Kernnetz des Providers können beispielsweise dazu führen, dass das im Router eingebaute Modem durchaus mit der Gegenstelle synchronisiert (unterste Verbindungsschicht, Layer 1) , aber der PPPoE-/DHCP-Server des Providers keine IP-Adresse zuweist oder Datenpakete einfach nicht geroutet werden. Andere Router führen den Verbindungsstatus beispielsweise in „Systeminformationen“ getauften Menüs – im Zweifel hilft die Anleitung.

Funktioniert die Verbindung auf der untersten Schicht und die IP-Kommunikation scheitert, liegt das Problem zwar oft an einem Baustein des Netzbetreibers, aber gelegentlich streikt auch die Software des Routers, die zu selten versucht, die IP-Verbindung neu aufzubauen. Starten Sie den Router neu und prüfen Sie, ob danach die Daten wieder fließen. Wenn nicht, können Sie zunächst mit Ihrem Smartphone im heise iMonitor und auf Allestörungen (verlinkt über ct.de/wgwq) prüfen, ob derzeit eine Großstörung vorliegt. Bringt das keine Antwort, kontaktieren Sie Ihren Anbieter und melden die Störung.

Zeigt die Router-Oberfläche hingegen, dass die Verbindung über das Medium abgebrochen ist – also etwa keine DSL-Synchronisierung besteht –, haben Sie schon deutlich bessere Selbsthilfeoptionen als auf Netzebene: Starten Sie den Router in der Hoffnung neu, dass er die Verbindung danach neu aufbaut. Hilft das nicht, fragen Sie zunächst Ihren Anbieter, ob eine Störung an der Vermittlungsstelle vorliegt, an der Sie angeschlossen sind. Wenn nicht, lohnt es sich, einige Optionen in Abhängigkeit der verwendeten Übertragungstechnik einmal selbst durchzugehen.

Erste Hilfe: DSL

DSL nutzt Telefonleitungen, wie sie weltweit seit über 120 Jahren verwendet werden. Viele Komponenten wurden seitdem mehrfach ausgetauscht, viele Kabel neu verlegt, trotzdem ist Telefoninfrastruktur an vielen Stellen mehrere Jahrzehnte alt und eigentlich nur für schmalbandige analoge Übertragungen gedacht; dementsprechend anfällig ist DSL. Fällt es ohne Fehler beim Netzbetreiber aus, können Sie an mehreren Stellen ansetzen: Kontrollieren Sie zunächst das Kabel vom Router zur Teilnehmer-Anschluss-Einheit (TAE), der Telefonwanddose; die Zuleitung ist meist sehr dünn und Haustiere oder neugierige Kinder können diese durch Knabbern oder mutwilliges Zerren beschädigen. Ersatz finden Sie eventuell daheim: Sowohl im TAE-Stecker als auch im RJ45-Stecker ist die Belegung standardisiert, sodass Sie auch Kabel von alten DSL-Geräten verwenden können. Gelegentlich liegt Routern auch ein TAE-RJ45-Adapter mit der Beschriftung „DSL“ bei. Damit können Sie ein Netzwerkkabel als DSL-Zuleitung verwenden.

Wenn die Router-Verkabelung keinen Fehler zeigt, lohnt ein kurzer Blick hinter die Abdeckung der Dose: Kupfer ist ein weiches Metall und lockere angebrachte Adern können die Dämpfung erhöhen, die DSL entweder ganz oder sporadisch ausfallen lässt. Prüfen Sie vorsichtig, ob die Adern fest in der Klemmstelle sitzen und ziehen Sie die Schrauben gegebenenfalls nach. Nehmen Sie danach den Router bei offener TAE-Dose in Betrieb und warten Sie ab, ob Besserung eintritt. Wenn nicht, können Sie die Adern lösen und auf Korrosion prüfen. Korrodierte Aderenden sollten Sie mit einem Seitenschneider abtrennen und neu abisolieren, sofern genug Kabel aus der Wand kommt. Von der Dose sollte zudem nur ein Adernpaar abgehen, angeschlossen an den ersten beiden Klemmstellen von links – Rot (andere Farbe möglich) auf a (1), Rot-Schwarz auf b (2).

Einst übliche Kaskadenschaltungen, um mehrere Telefone an einem Anschluss zu betreiben, können zu störenden Reflexionen führen, wenn der Router nicht am Ende angeschlossen wird oder Abzweige vorhanden sind; sie sind an b2 (5) und a2 (6) angeklemmt. Das Komplizierte daran: An der nächsten

Dose liegen die Adern wieder an a und b, sodass Sie nicht unbedingt erkennen können, an welcher Buchse die Zuleitung des Providers ankommt. Entweder Sie klemmen selbst an allen Dosen b2 und a2 ab und prüfen, an welcher TAE Ihr Router eine DSL-Verbindung aufbaut oder Sie melden die Ausfälle Ihrem Provider und schildern dem Techniker Ihre Beobachtung, der die Installation dann anpasst – beispielsweise, indem er überzählige Dosen entfernt und die Leitung bis zur gewünschten TAE brückt. Grundsätzlich gilt für DSL: Je kürzer das Kabel und je weniger Klemmstellen, desto besser das Signal und desto stabiler die Verbindung.

Haben Sie bei der Fehlersuche an den TAE-Dosen keinen Erfolg, wartet die Antwort vielleicht im Flur oder im Keller: In Mehrfamilienhäusern gibt es oft mehrere Übergabepunkte, die über mehrpaarige Leitungen mit dem APL (Abschlusspunkt Linientechnik) – der Verteilerstelle, an der das Erdkabel von der Straße auf die Hausverkabelung übergeht – verbunden werden und auf Etagenebene oder an mehreren Stellen im Keller die einzelnen Teilnehmeranschlussleitungen in die Wohnungen versorgen. Nicht selten hängen diese offen in den Fluren und wenn jemand daran hängen bleibt, ist die Leitung schnell aus dem Kasten gezogen. Entdecken Sie das, bleibt Ihnen zunächst nur, einen Techniker zu bestellen, damit dieser die korrekte Zuleitung identifizieren und wieder auflegen kann. Versuchen Sie auf keinen Fall selbst an der Verteilung zu arbeiten, wenn Sie die Klemmtechnik oder die korrekten Leitungen nicht kennen. An den Leitungen hängt eventuell wichtige Infrastruktur, deren Ausfall Sie auf keinen Fall verursachen sollten; die Konsequenz könnte im schlimmsten Fall eine Geld- oder gar Gefängnisstrafe sein. Allerdings können Sie dem Techniker bei der Fehlerbehebung über die Schulter schauen und Ihre Leitungen für spätere Fälle markieren, die Verantwortung und das Risiko bleibt aber.

Gleiches gilt für den Abschlusspunkt Linientechnik: Offiziell darf daran nur die Telekom arbeiten und insbesondere in Mehrfamilienhäusern sollten Sie die Finger davon lassen. In Ihrem (unvermieteten) Eigentum können Sie natürlich schalten und walten, wie Sie wollen, müssen sich dann jedoch vor genervten Mitbewohnern und Ihrem Bankkonto rechtfertigen, denn den Techniker, der Ihre Fehler behebt, zahlen Sie selbst. Meist lohnt es sich, alte Verteilertechnik zu entfernen und die TAE möglichst nah und direkt mit dem APL zu verbinden, die Zweidrahtleitung bis zum DSL-Router also sehr kurz zu halten. So holen Sie „alles“ aus der Leitung heraus und



Die Teilnehmer-Anschluss-Einheit (TAE) ist für Telefonanschlüsse seit mehreren Jahrzehnten üblich, sitzt oft an den verrücktesten Stellen und hat nicht selten ebenso viele Jahrzehnte hinter sich. Man sollte sie deshalb genau unter die Lupe nehmen, wenn DSL-Probleme auftreten; Korrosion, Feuchtigkeit oder Dreck erhöhen die Dämpfung.

minimieren Störeinflüsse durch parallel verlaufende Leitungen anderer Systeme. Falls dadurch die Ethernetstrecke vom Router zu Ihrem Switch oder zu Ihren PCs länger wird, ist das meist kein Problem. Schon gängige Cat-5-Kabel befördern Gigabit-Signale bis zu 100 Meter weit.

Abgesehen von passiver Verteilertechnik wird immer öfter aktive DSL-Technik in den Kellern von Mehrfamilienhäusern eingebaut: Micro Digital Subscriber Line Access Multiplexer (DSLAM) hängen per Glasfaser am Kernnetz und verkürzen so die Telefonleitungen auf wenige Meter. Das ist die Voraussetzung für extraschnelles Internet per VDSL oder G.fast. Sie hängen jedoch meist am allgemeinen Strom des Hauses und wenn der bei Bauarbeiten abgeschaltet wird, ist die Verbindung weg – dann hilft nur Rücksprache mit den Arbeitern vor Ort.

Erste Hilfe: DOCSIS

Die „Data Over Cable Service Interface Specification“ (DOCSIS) nutzt ursprünglich für Rundfunk verlegte Koaxialkabel zur Datenübertragung. Fällt die Ver-

bindung ohne ersichtlichen Grund an Ihrer Anschlussdose oder der Netztechnik des Anbieters aus, sollten Sie zunächst den Hausanschlussverstärker kontrollieren. Er ist in Häusern installiert, um das Eingangssignal der Erdleitung zu verstärken, sodass es auf viele weitere Buchsen aufgeteilt werden kann. Das Gerät sitzt meist im Keller und ist entweder ein kleines, mit der Steckdose und mehreren Koaxialkabeln verbundenes Kästchen oder ein abgeschlossener Schrank.

Fällt für den Verstärker der Strom aus, reicht der Pegel hinter dem Verstärker durch die vielen Abzweige meist nicht mehr für eine reibungslose Internetverbindung aus. Der Grund kann, wie auch beim Micro-DSLAM, der abgestellte Allgemeinstrom des Mehrparteienhauses sein. Und wenn der Verstärker nicht stromlos ist, kann er dennoch die Problemquelle sein: Während er den Bereich zwischen 65 und 860 MHz in Empfangsrichtung verstärkt, muss er den Bereich unter 65 MHz für die Senderichtung, also die Uplink-Kanäle durchlassen. Das kann auch bei Verstärkern klappen, die nicht dafür gedacht sind.



Bild: Merlin Schumacher

Hausanschlussverstärker sind beim Internet per TV-Kabel in Mehrfamilienhäusern essenziell, weil das Signal bei vielen Abzweigdosen andernfalls zu stark abfällt. Sie hängen jedoch meist mit am Allgemeinstrom des Hauses; wird dieser bei Bauarbeiten abgestellt, ist die Internetverbindung weg.

Die DOCSIS-Verbindung ist dann aber unter Umständen holprig oder der Uplink langsam. Die Beschriftung „Rückkanal 5-65 MHz“ verrät, ob sich der Verstärker für DOCSIS eignet. Moderne, professionelle Installationen mit abgeschlossenem Verteilerkasten sind dafür ausgelegt.

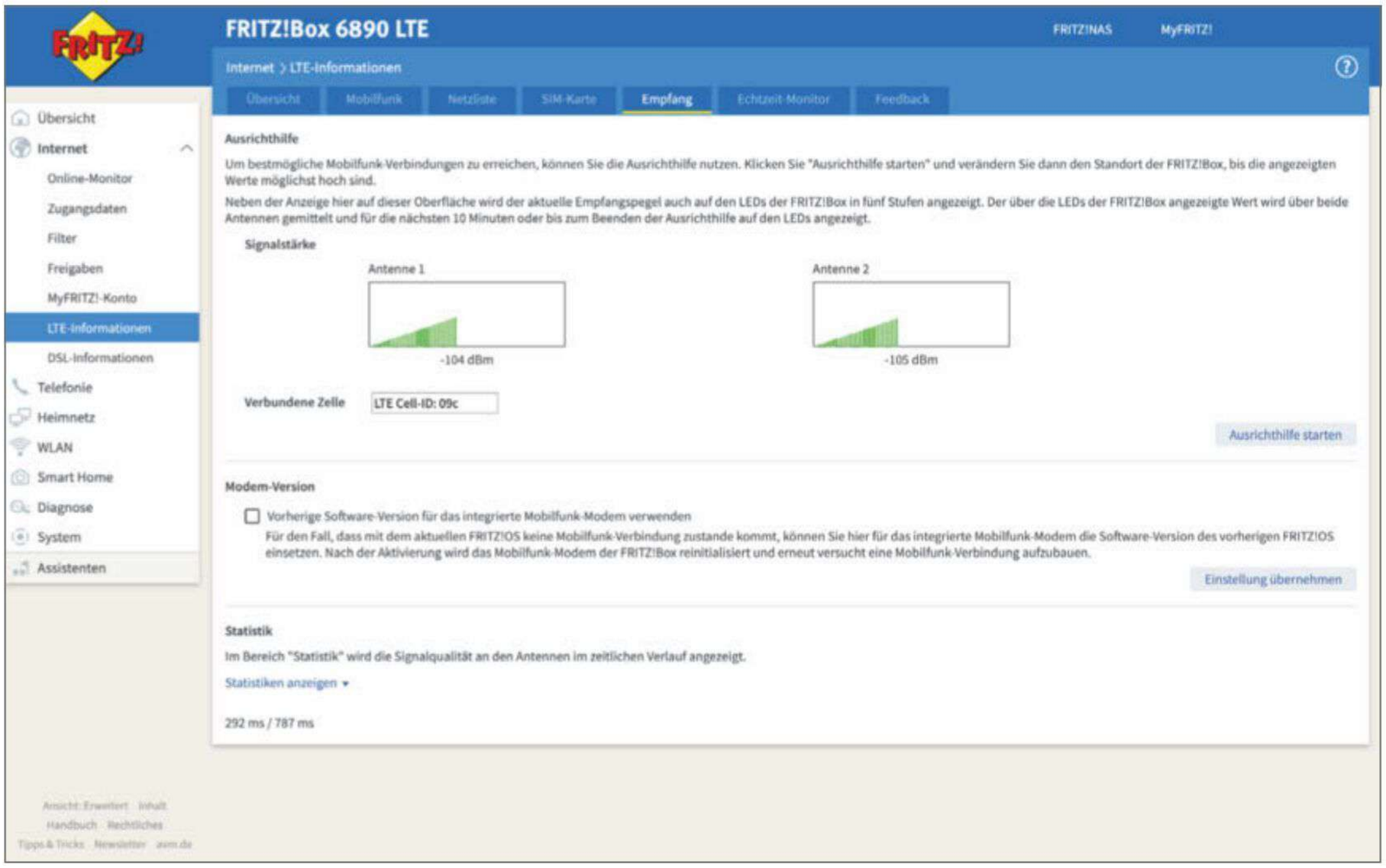
Entdecken Sie hingegen einen alten oder defekten Verstärker, weisen Sie Ihren Vermieter auf das Problem hin, damit er einen Fernsehtechniker beauftragt. Als Eigentümer können Sie den Verstärker einfach selbst tauschen und zudem präventiv einen Ersatzverstärker im Schrank vorhalten oder ein Kupplungsstück, um den Hausanschluss im Falle eines Verstärkerdefekts direkt mit der Zuleitung zum Modem zu verbinden, bis Ersatz da ist. Auch ein Ersatzkabel für die Verbindung vom Router zur Buchse kann nicht schaden; der verwendete Steckerstandard ist IEC 60169-24, bekannt als „F-Stecker“.

Deformierte Stecker, beschädigte Kabel oder auch defekte Empfangsgeräte im Hausnetz können Kurzschlüsse verursachen, die andere Geräte beeinträchtigen. Das gilt nicht nur für die Anschlüsse in Ihrer Wohnung, sondern auch für die von Nachbarn. Ist die Anzahl der Nachbarn überschaubar, lohnt es sich nachzufragen, ob diese ein neues Gerät angeschlossen haben oder sich an der Installation einer Anschlussdose versucht haben.

Erste Hilfe: Glasfaser

Glasfaser gilt als moderne und schnelle Anschlusstechnik. Die Installation erfordert aber vergleichsweise teures Werkzeug und ohne Vorbereitung können Nutzer wenig selbst tun. Indikatoren dafür, dass das Problem auf Ihrer Seite der Verbindungsstrecke liegt, können abgeknickte Glasfaserleitungen, stark verdreckte oder abgebrochene Glasfaserstecker sowie ein lebloser Medienkonverter sein (das Glasfaser-Modem). Kein Drama, denn Netzbetreiber terminieren Glasfasern meist einmal im Keller und gegebenenfalls ein weiteres Mal in der Wohnung in einem geschützten Anschlusskasten, von dem ein standardisiertes Kabel abgeht. Wie auch bei den anderen Zugangsarten gilt: Aus Verteilern gerissene Leitungen in Fluren oder im Keller sind ein schlechtes Zeichen und bedürfen der Zuwendung eines Technikers.

Wenn Sie sich für einen Ausfall aufgrund eines Medienkonverterdefekts oder einer beschädigten Router-Zuleitung wappnen wollen, sprechen Sie Ihren Anbieter an: Die verwendeten Geräte sowie Stecker- und Kabelstandards variieren von Anbieter



Hybrid-Router mit eingebautem DSL- und Mobilfunkmodem sind speziell zur Erhöhung der Internetverfügbarkeit gedacht. Mit den Monitoring-Funktionen der Fritzbox 6890 LTE lässt sich das vor Ort beste Mobilfunknetz leicht finden und der Router optimal zur Basisstation aufstellen.

zu Anbieter und die Unterschiede sind nicht unbedingt offensichtlich. Eventuell kann Ihnen der Anbieter passende Ersatzteile verkaufen. Verdreckte Stecker lassen sich mit in Alkohol getränkten fusselfreien Tüchern reinigen. Mehr zum Thema Glasfaser haben wir für Sie in [1] aufgeschrieben.

Failover

Wenn nur der Techniker des Providers das Problem lösen kann, dauert der Ausfall länger. Ihr Smartphone kann trotz geringem Inklusivvolumen womöglich erste Hilfe leisten: Viele Mobilfunkprovider bieten Tagesflatrates ohne Volumenbeschränkung als Optionen zur Buchung per App oder im Kundenportal an. Ihr Heimnetz können Sie dann entweder direkt über die Hotspot-Funktion Ihres Smartphones versorgen, indem Sie SSID und Schlüssel wie an Ihrem Router einstellen und das Router-WLAN vorerst deaktivieren. Der Hotspot-Betrieb benötigt viel Strom, lassen Sie das Smartphone also am Ladeanschluss.

Manche Router, Fritzboxen etwa, können Sie als WLAN-Clients (WISP-Modus) mit dem Internet verbinden, beispielsweise den Smartphone-Hotspot. In FritzOS steckt diese Option im Bereich der Zugangsdaten („weiterer Internetanbieter / vorhandener Zugang über WLAN“). Einmal verbunden, können alle Geräte im Heimnetz wieder ins Internet – nur vermutlich spürbar langsamer. Gleichermaßen können Sie auch das Gast-WLAN der befreundeten Nachbarn einbinden und umgekehrt Ihres anbieten – idealerweise sind Sie dafür nicht bei demselben Provider wie Ihre Nachbarn.

Eine höhere Internetverfügbarkeit und mit automatischem Wechsel zu einer Ersatzverbindung bekommen Sie bei einigen Routern über ein USB-Mobilfunkmodem. FritzOS etwa blendet beim Anstecken eines geeigneten Modems die Unterseite „Mobilfunk“ ein und bietet dort an, auf die Mobilfunkverbindung umzuschalten, wenn die Verbindung auf IP-Ebene ausfällt oder erst, wenn die Hauptleitung keine Verbindung mehr hat.

O2 bietet dafür derzeit einen interessanten Tarif an: „my Internet-to-go“ hat keine Grundgebühr. Tages-, Wochen- und Monatstarife mit unbegrenztem Datenvolumen kosten 5, 20 beziehungsweise 50 Euro zur Buchung per App. Die Einrichtung kostet einmalig 50 Euro, wobei der erste Flatrate-Monat enthalten ist; wer etwa für den Urlaub bucht, kann das aus-

nutzen und die Daten-SIM danach als Backup am heimischen Router einsetzen. O2 behält sich vor, den Tarif nach 12 Monaten ohne Buchung zu kündigen, womit der Dienst jährlich mindestens fünf Euro kostet (eine Tagesflat mindestens pro Jahr). Die jährlichen Erhaltungsbuchungen sollten Sie zudem für einen Test der Failover-Funktion Ihres Routers nutzen, in dem Sie die Hauptleitung vom Router trennen und beobachten, ob er in erwarteter Zeit eine Mobilfunkverbindung herstellt.

Mobilfunkmodems bekommen Sie günstig gebraucht über einschlägige Kleinanzeigenportale. Verzichten Sie bei der Auswahl nicht auf LTE-Fähigkeit, denn der Vorgängerstandard UMTS (3G) geht in Rente. Beispielsweise kosten Telekom Speedsticks (ohne SIM-Lock) etwa 15 Euro und stammen von Huawei, deren Modems weit verbreitet sind und an nahezu allen Routern mit Mobilfunkmodem-Unterstützung laufen. Die Kombination aus Ausfallsicherung und Urlaubs-WLAN erzielen Sie mit einem Mobilrouter, etwa der Magenta Speedbox oder dem Magenta Schnellstart [2]. Für erstere muss Ihr Router die Internetverbindung über einen normalen Ethernet-Port aufbauen können; zweiter stellt ein virtuelles Ethernet-Interface per USB bereit.

Noch besser auf DSL-Ausfälle sind Hybrid-Router mit eingebauten DSL- und LTE-Modems vorbereitet. Die Fritzbox 6890 LTE hilft mit einem durchdachten Echtzeitmonitor, das beste Mobilfunknetz und die optimale Position für die LTE-Versorgung leicht zu finden. Mit dem Hybrid-Router Speedport Pro und der Tarifoption „Hybrid LTE“ ist man zwar auf die Infrastruktur der Telekom angewiesen, bekommt dafür aber eine gleichzeitige Internetversorgung über DSL und LTE. Der Hybrid-Router leitet die Daten über den gerade besseren Weg oder nutzt automatisch den verbliebenen, falls einer der beiden ausfällt. Hybrid LTE bietet die Telekom für alle MagentaZuhause-Tarife für 4,95 Euro monatlich. Der Speedport Pro kostet allerdings rund 390 Euro.

Benachbarte Leidensgenossen können sich alternativ über Freifunk zu einer Netzgemeinschaft vereinen: Freifunkrouter vernetzen sich untereinander, bemerken, wenn Wege zu den Freifunk-Servern wegbrechen und wählen automatisch eine alternative Route. Fällt ein Anschluss aus, kann man sich einfach mit der Freifunk-Infrastruktur verbinden und weitersurfen. Dauert der Ausfall länger, stellen Sie Ihren üblichen Router auf „Internet per Ethernet“ um und stecken ihn auf einen der Client-Ports Ihres Freifunkrouters. Router, die sich für den Freifunkbetrieb eignen, etwa den TP-Link Archer C6, gibt es gebraucht sehr günstig; mehr verrät die Seite Ihrer lokalen Freifunk-Community [3]. (amo) c't

Literatur

[1] Jan Mahn, Urs Mannsmann, **Schnelle Fasern**, Glasfasern fürs lokale Netz und fürs Internet, c't 18/2020, S. 68

[2] Andrijan Möcker, **Sparrepertoire**, Gebrauchte Netzwerkhardware 2021, c't 9/2021, S. 116

[3] Andrijan Möcker, **Freifunk**: Das größte Bürgernetz Deutschlands, c't 17/2019, S. 66

02-Tarif

ct.de/wgwq

WILLKOMMEN IN DEN GUTEN ALTEN ZEITEN...

Testen Sie Retro Gamer mit 30 % Rabatt!

2 Ausgaben als Heft oder digital + Geschenk nach Wahl

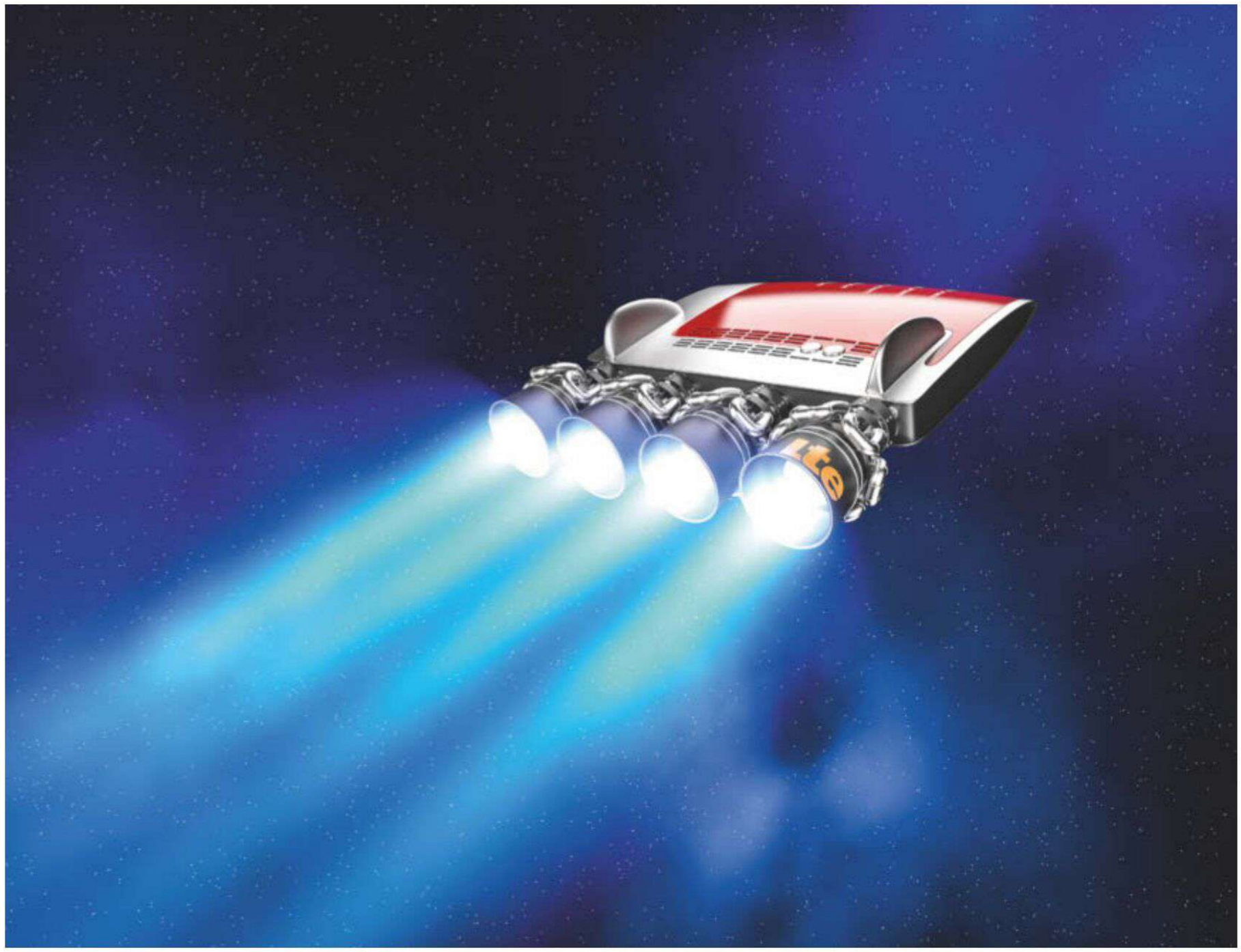




Jetzt bestellen:

www.emedia.de/rg-mini

(0541) 800 09 126 leserservice@emedia.de eMedia Leserservice, Postfach 24 69, 49014 Osnabrück



Kabelbrücken

Fritzboxen können bei einem DSL-Ausfall stationäre LTE-Router, Smartphones oder LTE-Sticks als Ersatzweg zum Internet nutzen. Allerdings steht der Router selten dort, wo der Empfang gut ist. Wir haben einige Methoden ausprobiert, um das Funkzubehör mit Verlängerungen an den optimalen Standort zu bringen.

Von **Dušan Živadinović**

Wer eine Fritzbox braucht, die sich per LTE oder UMTS ins Internet einbucht, wenn der Bagger das Kabel getrennt hat, kann sich natürlich gleich mit dem Modell 6890 LTE wappnen: Diese Box bringt ein Mobilfunkmodem mit und lenkt den Verkehr automatisch darauf um, wenn die Hauptleitung ausfällt (Fallback). Das und die Loadbalancing-Funktion, mit der sie DSL und LTE gleichzeitig nutzt, macht sie für kleine Unternehmen attraktiv.

Im Fallback-Modus lassen sich mit den von Mobilfunkern normalerweise zugeteilten IP-Adressen Server-Dienste nicht nutzen, aber immerhin kann man

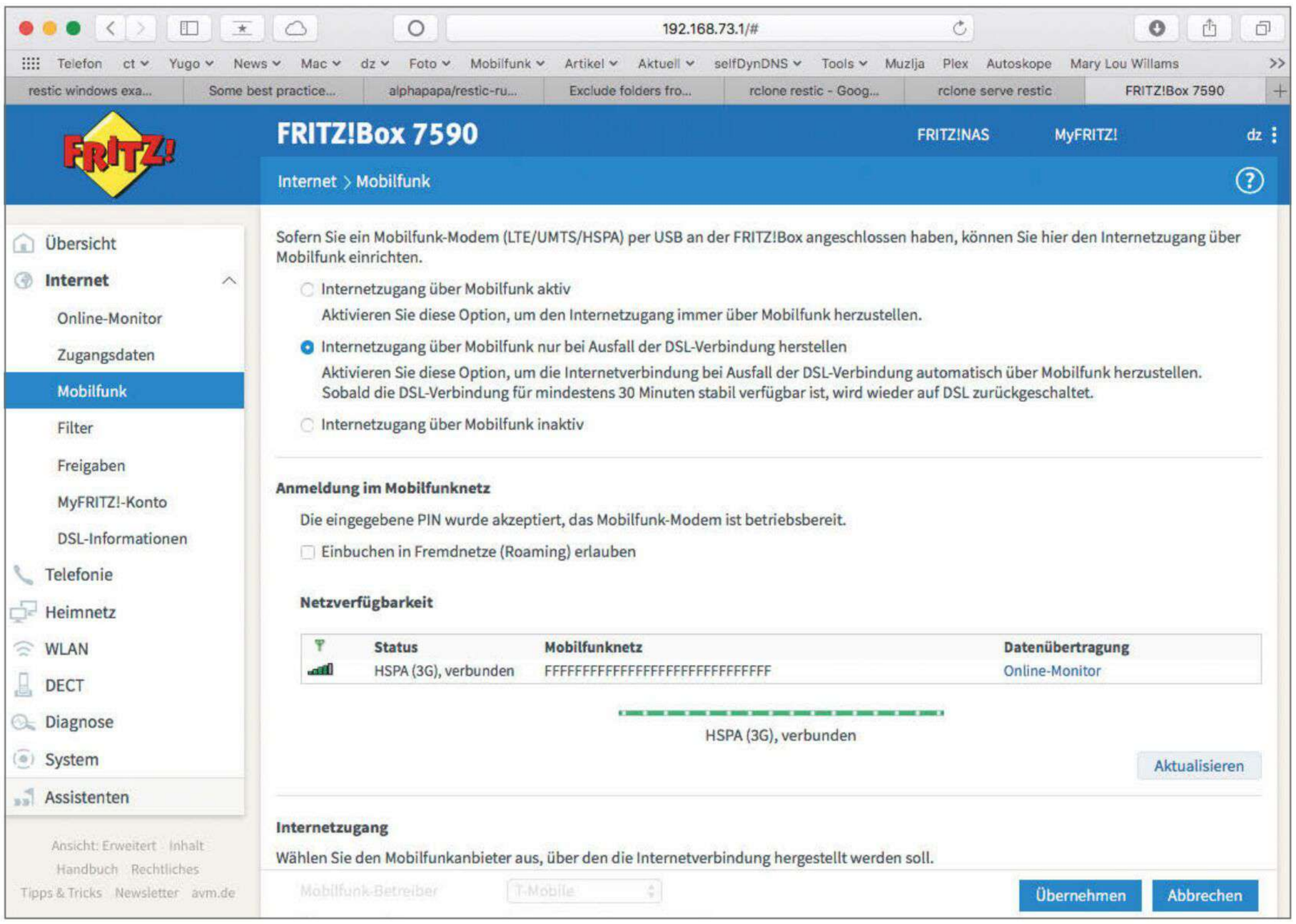
darüber sämtliche ausgehenden Internetanwendungen verwenden (Surfen, Chatten, Streamen, Mailen etc.). Auch alle übrigen an der Fritzbox angeschlossenen Geräte haben dann Zugang zum Internet per Mobilfunk. Dafür genügt eine billige Prepaid-SIM-Karte, zum Beispiel in Kombination mit einem Tagestarif, wie ihn diverse Provider für unter fünf Euro anbieten (z. B. O2 Day Pack Unlimited, Kaufland mobil DayFlat oder AldiTalk Internet-Flatrate S).

Kehrt die DSL-Verbindung zurück, schaltet die 6890 LTE automatisch darauf um (Fallforward). Sehr nützlich ist der Monitor-Modus der Box. Damit hilft sie, den optimalen Standort und die beste Ausrichtung zur Basisstation zu finden. Dabei kommen ihr auch die zwei externen Mobilfunkantennen zugute.

Kein anderes Fritzbox-Modell erreicht ihre Funktionalität, aber man kann andere Modelle immerhin mit externen Mobilfunkmodems nachrüsten. Dafür kommen die Modems von stationären Mobilfunkroutern, Mobilfunksticks oder Android-Smartphones infrage. Stationäre LTE-Router koppelt man per Ethernet an die Fritzbox, Sticks und Android-Smartphones über USB. Prinzipiell eignen sich auch iOS-Geräte, aber Fritzboxen können sie bisher nicht über USB steuern. Seit FritzOS 7.10 docken sie immerhin per WLAN an deren „Persönlichen Hotspot“ an. Dafür muss die Fritzbox ihren WLAN-Gastzugang abschalten.

Internetumleitung per Zweit-Router

Ein Ethernetsegment darf für Gigabit-Ethernet je nach Konfektionierung bis 100 Meter lang sein. So lässt sich eine Fritzbox im Keller leicht mit einem



Fritzboxen können etliche verschiedene USB-Sticks ansteuern. Darunter sind auch alte Schätzchen wie hier der Huawei E270. In diesem Beispiel lässt nur die Anzeige des Mobilfunknetzes zu wünschen übrig – es heißt nicht „FFFFF...“, sondern „Telekom“.



Der stationäre LTE-Router Netgear LB2120-100PES lässt sich auch über Ethernet mit Strom versorgen (PoE), sodass man am Standort nicht unbedingt eine Steckdose braucht.

LTE-Router unterm Dach verbinden. Zur Überbrückung von kurzzeitigen DSL-Ausfällen genügt schon ein älterer Mobilfunkrouter. Zum Beispiel bekommt man den Huawei B390s-2 alias Telekom Speedport LTE800 gebraucht schon ab rund 20 Euro. Wunderdinge sollte man freilich nicht erwarten – das LTE-Modem liefert maximal 50 MBit/s, die LAN-Ports maximal 100 MBit/s (Fast-Ethernet).

Neue Einstiegsmodelle gibt es für unter 100 Euro. Beispielsweise bietet der Mobilfunkprovider Ortel ein einfaches Modell für 40 Euro. Immerhin bekommt man für 30 Euro Guthaben aktuell 90 GByte Übertragungsvolumen mit einer Laufzeit von 28 Tagen – ohne Mindestlaufzeit und Kündigungsfrist. Ähnliche Angebote haben auch die Telekom, O2 Telefónica und Vodafone in petto. Eine Fritzbox 6820, die ausschließlich ein Mobilfunkmodem an Bord hat, bekommt man ab rund 130 Euro. Die etwas besser bestückte Fritzbox 6850 LTE kostet rund 170 Euro.

Manche LTE-Router lassen sich per Power over Ethernet (PoE) mit Strom versorgen, sodass sie am Aufstellungsort ohne Stromsteckdose auskommen. Das trifft zum Beispiel auf den Netgear LB2120-100PES zu. Er ist für PoE gemäß IEEE 802.3af ausgelegt (max. 13 W). Aber Achtung: Das Modell LB2120-100EUS bringt kein PoE mit. Zwar hat AVM bisher keine Fritzbox für PoE ausgelegt, aber einen LB2120 kann man mit einem PoE-Injektor wie dem TP-Link TL-POE150S oder dem Digitus DN-95102-1 speisen (gibts in der Elektronik-Grabbelkiste für rund 20 Euro).

Für die Kopplung steckt man ein Ethernetkabel in den LAN-Port eines LTE-Routers. Das andere Kabelende führt man dem WAN-Port der Fritzbox zu. Manchen Modellen hat AVM einen festen WAN-Port spendiert, etwa den Modellen 7580 und 7590. Man schaltet ihn im Menü „Internet / Zugangsdaten / vorhandener Zugang über WAN“ ein. Bei anderen Fritzboxen muss man per Hand zwischen DSL und LAN1 umschalten.

Sind Box und Router verbunden und eingeschaltet, weist der LTE-Router der Box per DHCP eine private IP-Adresse aus seinem Subnetz zu (z. B. 192.168.5.x beim Netgear). Welche das ist, zeigt die Fritzbox auf der Startseite ihrer Weboberfläche an. Öffnen Sie dann im Browser das Webinterface des LTE-Routers (z. B. 192.168.5.1) und konfigurieren Sie ihn. Tragen Sie also, falls erforderlich, die PIN der SIM-Karte ein und bauen Sie die Mobilfunkverbindung zum Internet auf – damit ist die Internet-Umleitung per Mobilfunkrouter fertig.



USB-Brücke über Ethernet: Damit lässt sich eine Fritzbox im Keller leicht mit einem Mobilfunkstick unterm Dach verbinden. Aber nicht jede Brücke funktionierte im Test und schon gar nicht jede mit jedem Stick (links: Digitus, oben: 2-Tech, rechts: LogiLink.

Sticks and Stones

Falls es ein Mobilfunkstick sein soll: Die weitaus meisten Modelle sind nur mit dem älteren USB 2.0 bestückt, das nicht mehr als 480 MBit/s befördert. Doch auch damit haben Sie für den Mobilfunkzugang zum Internet genügend Reserven, weil deren Modems nicht über 150 MBit/s hinauskommen (LTE-Kategorie 4). Selbst die schnelleren liefern allenfalls 300 MBit/s (Kategorie 6). Ähnliches gilt für Android-Smartphones.

Mit passiven USB-2.0-Verlängerungen kommt man nur einige Meter weit. Das kann genügen, um einen Stick außerhalb des Funkschattens aufzustellen, etwa in Fensternähe. Die Güte der erhältlichen USB-Verlängerungen streut aber stark, so dass man unter Umständen mehrere ausprobieren muss. Aktive USB-Verlängerungen frischen das USB-Signal an den Kabelenden auf und kommen so auf größere Reichweiten. Ein Beispiel dafür ist das Set USB2AAEXT20M von StarTech, das zurzeit rund 80 Euro kostet. Damit überbrückt man aber nur zehn Meter.

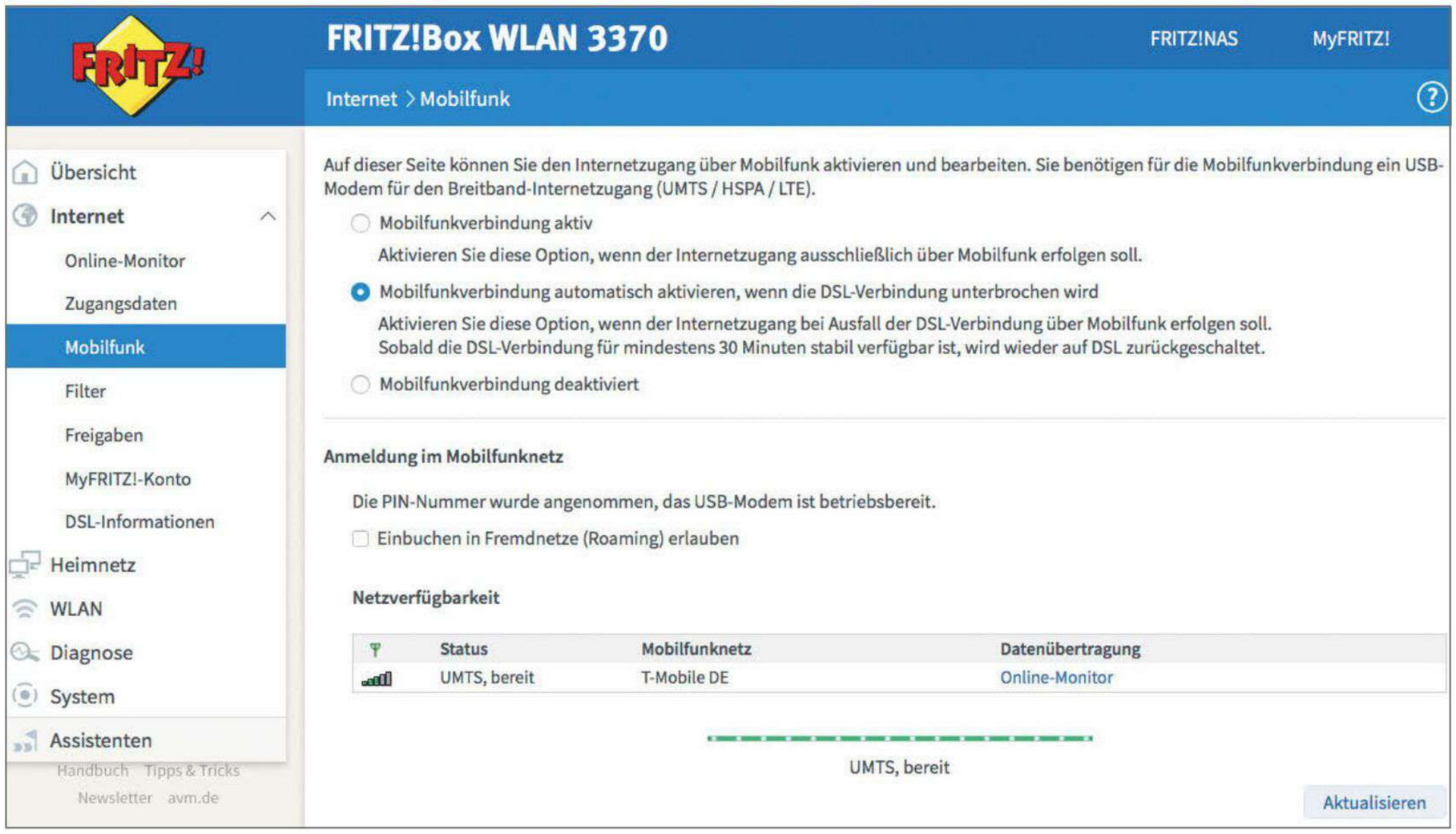
Viele LTE-Sticks und -Router sind mit Buchsen für externe Antennen ausgerüstet (meist TS-9-Format). Wir raten von externen Antennen jedoch ab, denn jeder Millimeter Antennenkabel verschlechtert das Mobilfunksignal, das im Modem ankommen soll. Diese Einbußen erspart man sich, wenn man das Modem gleich so aufstellt, dass es optimal versorgt wird, und überbrückt die Entfernung zur Fritzbox per USB oder Ethernet.

USB über viele Meter

Wenig bekannt ist, dass sich USB-Signale auch mittels Extendern über Ethernetkabel übertragen lassen. Dabei profitiert man von der höheren Güte und Verbreitung der Ethernetverkabelung – in vielen Häusern liegt diese Infrastruktur schon vor und Verlegekabel gibt es schon ab 20 Cent pro Meter.

Mit USB-Ethernet-Brücken kann man solche Infrastruktur preisgünstig auch für den Anschluss von USB-Webcams, -Druckern oder -Scannern nutzen. Dabei gibt es zwei Gruppen von Brücken: Die aufwendigen kapseln USB-Pakete in IP-Frames und liefern sie an einen PC, der sie dort mit passender Software ausliest und der Anwendung zuführt. Beispielsweise bietet der Bielefelder Hersteller SEH solche Brücken.

Für die Verlängerung einer USB-Strecke von einem Router zu einem LTE-Stick braucht man aber Brücken, die beidseitig in Hardware aufgesetzt sind. Sie bestehen aus einem Sende- und einem Emp-



Alt, aber funktioniert: Vodafones UMTS-Stick K4505-Z spielt nicht nur an einer ähnlich alten Fritzbox 3370, sondern auch an einer modernen 7590.

fangsteil (Tx und Rx). Das Sendeteil stöpselt man an PC oder Router typischerweise per USB-Type-A-Stecker an und verbindet es mit einem Ethernetkabel (RJ45-Buchse). Das andere Ethernetende führt zum Empfangsteil der Brücke, an deren USB-Type-A-Buchse schließlich der LTE-Stick angesteckt wird.

Viele solcher USB-Brücken stammen von chinesischen oder taiwanischen Herstellern und sind für deutlich unter 50 Euro zu haben. Wir haben keine gefunden, die explizit für Mobilfunksticks ausgelegt ist, sondern nur für Tastatur, Maus, Webcam, Drucker oder Scanner.

Probeweise haben wir drei Modelle von Assmann Electronic (Digitus DA-70141), 2-Tech (USB-Repeater) und LogiLink (UA0207) geordert und mit elf Mobilfunksticks ausprobiert, und zwar an einer älteren Fritzbox 3370 mit FritzOS 6.54 und einer Fritzbox 7590 mit FritzOS 7.10. Alle drei Brücken sind für maximal 50 Meter Ethernet ausgelegt (Cat-5, Cat-5e oder Cat-6).

Prinzipiell kommt auch der StarTech USB 2.0 Ethernet Extender infrage. Laut Hersteller überbrückt dieser Extender sogar bis zu 100 Meter Ethernet. Er ist aber erst ab 400 Euro zu haben – dafür bekommt man leicht mehrere LTE-Router, sodass er für dieses Szenario nicht infrage kommt.

Alle drei getesteten Extender mussten die USB-Signale durch ein 48 Meter langes Ethernetkabel schicken. Es besteht aus drei Segmenten: Das Hauptsegment ist ein 40 Meter langes Verlegekabel in Cat-5e-Ausführung, beidseitig mit RJ45-Dosen bestückt. Damit entspricht es einem Stück Hausverkabelung. Von den RJ45-Dosen führen ein fünf und ein drei Meter langes Stück in den Raum.

Die beiden Empfangsteile der Brücken von Digitus und LogiLink sind für eine externe Stromversorgung ausgelegt. So kompensieren sie den Spannungsabfall über längere Ethernetstrecken. Davon profitieren insbesondere die älteren, stromdurstigen Mobilfunksticks mit UMTS-Modem. Digitus legt seiner Brücke ein passendes Netzteil bei, dem LogiLink fehlt es. In Kombination mit einer Fritzbox braucht man für das LogiLink also ein Netzteil (5V, 2A) oder einen PoE-Injektor. Dieser dürfte sich aber nur lohnen, wenn Sie die LogiLink-Brücke bereits besitzen – in unserem Szenario funktionierte die LogiLink-Bridge nur mit dem in Ehren ergrauten UMTS-Stick Huawei E169G.

Die meisten Sticks funktionierten mit der Digitus-Brücke an der Fritzbox 7590 mit FritzOS 7.10. Die Ergebnisse haben wir in der Tabelle auf Seite 100 zusammengefasst. Von der einfachen 2-Tech-Brücke raten wir ausdrücklich ab. Beispielsweise stürzte die Fritzbox ab, als wir darüber den UMTS-Stick Vodafone K4505-Z angeschlossen haben – möglicherweise, weil alle Bausteine zusammen zu viel Strom vom USB-Port der Fritzbox gezogen haben. Mit einem zwischengeschalteten USB-Hub stürzte die Fritzbox zwar nicht ab, aber sie konnte den Stick über diese Brücke dennoch nicht ansprechen.

Mini-Router im Stick

Bei der Ansteuerung der Sticks muss man zwei Gruppen unterscheiden: Herkömmliche Mobilfunksticks enthalten ein simples Modem, das auf AT-Befehle hört. In neueren Modellen stecken komplette Mini-Router, die man über ein eigenes Webinterface konfiguriert. Die Fritzbox koppelt an solche Sticks über USB im Tethering-Modus an, verhält sich also wie ein DHCP-Client an einem externen Router. Manche dieser Sticks enthalten auch ein WLAN-Modul mit Hotspot-Funktion.

Den Tethering-Modus über USB nutzen Fritzboxen auch für die Anbindung an Android-Smartphones. Da sich die DHCP-Kommunikation in diesem Szenario auf den Bezug von IP-Adressen beschränkt, muss die Fritzbox jegliche Konfiguration, Steuerung und Statusmeldungsanzeige dem Smartphone oder dem Stick überlassen.

Im Test haben wir zunächst alle Sticks und das Android-Smartphone Samsung Galaxy S5 direkt an den beiden Fritzboxen ausprobiert. Die Einrichtung ist einfach: Man steckt Stick oder Smartphone an einen USB-Port der Fritzbox an. Die Sticks starten dann erst und brauchen eine Weile, bis sie gebootet haben. Ist das erledigt, stellt man in der Fritzbox im Menü „Internet / Mobilfunk“ die gewünschte Betriebsart ein: Im Grundzustand ist der Internet-Zugang über Mobilfunk abgeschaltet. Auf Wunsch kann man ihn dauerhaft einschalten oder automatisch darauf umschalten lassen, wenn die Hauptleitung ausfällt (Fallback inklusive Fallforward).

Im Grundzustand trennt die Fritzbox die Mobilfunkverbindung, wenn 60 Sekunden lang keine Daten übertragen werden. Das spart ein wenig Strom. Die Frist lässt sich im Menü „Mobilfunk“ ändern und das Verhalten ebendort auch abschalten. Wenn wieder Bedarf ist, dauert es nur rund fünf Sekunden, bis die Mobilfunkschnittstelle wieder IP-Pakete verschickt.

Das Fallforward, also das automatische Zurückschalten auf DSL, könnte AVM etwas flexibler gestalten. Aktuell muss die Leitung mindestens 30 Minuten stabil gewesen sein, bevor die Box das Fallforward auslöst. Das finden wir bei Weitem zu lang und wünschen uns eine einstellbare Frist. Um einen Fallforward zu erzwingen, muss man die Box entweder per Hand neu starten oder im Menü „Internet/Zugangsdaten“ auf „Übernehmen“ klicken.



Unter den LTE-Sticks gibt es mehrere, die einen kompletten Router im Mini-Format enthalten. An diese dockt eine Fritzbox über USB als DHCP-Client an.

Android-Brücke

Android-Smartphones sind sehr verbreitet. Außerdem gibt es Gebrauchtgeräte in sehr brauchbarem Zustand schon ab 20 Euro. Deshalb erscheinen sie zunächst als bester Ausweg bei DSL-Ausfällen. Zur Kopplung des Smartphones an die Fritzbox kommen WLAN und USB infrage. Beide haben Vor- und Nachteile.

Für die WLAN-Anbindung eignen sich nur Fritzboxen ab FritzOS 7.1. Sie koppeln damit als WLAN-Clients an einen Hotspot an. Weiteres Zubehör

braucht man dafür nicht, aber die WLAN-Reichweite in Gebäuden ist wegen Wänden und Gegenständen im Funkweg klar kürzer als die, die man mit USB-Ethernet-Brücken erzielen kann. Auch hat AVM den WLAN-Client-Modus nicht für automatisches Fallback ausgelegt – man kann den WLAN-Zugang zum Internet nur per Hand einschalten (Menü „Internet / Zugangsdaten / Internetanbieter“). Nach dem Umstellen auf „vorhandener Zugang über WLAN“ blendet die Fritzbox die Namen der WLANs in Reichweite ein. Zur Anmeldung wählen Sie Ihren WLAN-Hotspot aus (also etwa den des Android-Geräts) und geben dort das eingerichtete Passwort ein – fertig.

Für USB-Tethering muss auf dem Smartphone der Datensparmodus abgeschaltet sein (siehe Einstellungsmenü „Datennutzung“). Ist das sichergestellt, koppeln Sie das Smartphone per USB an die Fritzbox. Aktivieren Sie dann das USB-Tethering im Menü „Netzwerk & Internet“ und zwar im Bereich „Tethering und mobiler Hotspot“.

Wenn alles klappt, zeigt die Box auf der Startseite im Bereich „Übersicht / Verbindungen“ über welchen Netzbetreiber (z. B. Telekom) und welches Smartphone die Internetverbindung hergestellt ist (z. B. SAMSUNG_Android USB-Tethering).

Nachteilig ist, dass das Smartphone das Tethering abschaltet, wenn es die Verbindung zur Fritzbox verliert, also etwa nach einem Stromausfall. Das ist unpraktisch, wenn gerade dann niemand vor Ort ist. Hilfsweise kann man immerhin Automati-

Fritzbox, Mobilfunksticks und USB-Ethernet-Brücken

Fritzbox / USB-Stick	Steuerung	USB direkt an Fritzbox	Fallback/Fallforward	USB-Extender (Fallback/Fallforward)[1]
3370 / FritzOS 6.54				
Android-Smartphone	Router / Tethering	✓	✓/✓	✓/✓,–/–,–/–
4G Systems XSStick W1208	Modem / AT-Befehlssatz	–	–/–	–/–,–/–,–/–
Huawei E169G	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,✓/✓
Huawei E270	Modem / AT-Befehlssatz	–	–/–	–/–,–/–,–/–
Huawei E3372h	Modem / AT-Befehlssatz	–	–/–	–/–,–/–,–/–
Kuwfi	Router / Tethering	–	–/–	–/–,–/–,–/–
Novatel Wireless Ovation MC996D	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,–/–
Vodafone K4505-Z	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,–/–
Vodafone K5005	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,–/–
Vodafone K5006-Z	Modem / AT-Befehlssatz	–	–/–	–/–,–/–,–/–
ZTE MF79	Router / Tethering	✓	✓/✓	✓/✓,–/–,–/–
ZTE MF710	Router / Tethering	✓	✓/✓	✓/✓,–/–,–/–
7590/FritzOS 7.10				
Android-Smartphone	Router / Tethering	✓	✓/✓	✓/✓,–/–,–/–
4G Systems XSStick W1208	Modem / AT-Befehlssatz	✓	–/–	✓/✓,–/–,–/–
Huawei E169G	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,✓/✓
Huawei E270	Modem / AT-Befehlssatz	✓	–/–	✓/✓,–/–,–/–
Huawei E3372h	Modem / AT-Befehlssatz	✓	–/–	✓/✓,–/–,–/–
Kuwfi	Router / Tethering	–	–/–	–/–,–/–,–/–
Novatel Wireless Ovation MC996D	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,–/–
Vodafone K4505-Z	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,–/–
Vodafone K5005	Modem / AT-Befehlssatz	✓	✓/✓	✓/✓,–/–,–/–
Vodafone K5006-Z	Modem / AT-Befehlssatz	–	–/–	–/–,–/–,–/–
ZTE MF79	Router / Tethering	✓	✓/✓	✓/✓,–/–,–/–
ZTE MF710	Router / Tethering	✓	✓/✓	✓/✓,–/–,–/–

[1] Extender 1: Digitus, 2: 2-Tech, 3: LogiLink ✓ funktioniert – funktioniert nicht



Die weitaus meisten Mobilfunk-Sticks steuert eine Fritzbox über den AT-Befehlssatz selbst. Deshalb kann sie auch den Verbindungsauf- und abbau selbst regeln.

sierungstools wie Tasker nutzen, um das USB-Tethering auf dem Smartphone automatisch einschalten zu lassen.

LTE-Sticks

Um LTE-Sticks an der Fritzbox zu nutzen, schaltet man die Fritzbox am besten aus, stöpselt den Stick (bei Bedarf über die USB-Brücke) an und schaltet sie dann ein. Zwar sind Stick, Box und Brücken für Hotplug ausgelegt (Anstecken und Entfernen ohne auszuschalten), aber wenn man mehrere Sticks oder Brücken nacheinander ausprobiert, kommt die Fritzbox gelegentlich aus dem Tritt. Dann kann sie schon mal bei der Initialisierung des Sticks scheitern, das Umschalten von Tethering- zum AT-Modus vergessen und auch schon mal abstürzen. Ursache sind in den meisten Fällen Kombinationen von USB-Extendern und Sticks, nicht die Fritzbox selbst.

Je nach Stick kann es einige Minuten dauern, bis ihn die Box erkannt und initialisiert hat – oder einfach nur meldet, dass sie das angesteckte Stück nicht verwenden kann. Manche Sticks brauchen mehr als eine Minute zum Booten. Geben Sie also nicht gleich auf, wenn die Box nicht umgehend anzeigt, ob sie den Stick verwenden kann.

Wenn sie ein geeignetes Modem erkannt hat, meldet sie das im Menü „System / Ereignisse“ und blendet es im Menü „Internet / Mobilfunk“ ein. Dort kann man bei Bedarf auch die PIN der SIM-Karte eingeben und den Empfangspegel (RSSI) sowie den Verbindungsstatus einsehen.

Steckt man eine USB-Brücke zwischen Stick und Box, meldet sie im Menü „Heimnetz / USB“ einen USB-Hub. Zusätzlich sollte sie dort auch ein Modem aufführen. Ist das nicht der Fall, obwohl das Modem bei direktem Anschluss an der Fritzbox funktioniert, liegt es daran, dass die Brücke den Spannungsabfall über die Ethernet-Strecke nicht kompensiert, also die USB-Signale unleserlich in der Fritzbox ankommen. Wenn Sie eine solche Brücke eigens für die Verlängerung zum LTE-Stick angeschafft haben, können Sie sie getrost umgehend zum Verkäufer zurückschicken. Im Test half in solchen Situationen selbst eine unterstützende Stromversorgung per USB-Hub nicht.

Beide Fritzboxen lösen das Fallback automatisch aus, wenn das DSL-Signal drei bis vier Minuten fehlt. Das entspricht den Angaben von AVM. Allerdings wünscht man sich auch hier eine einstellbare Frist.

Die elf probeweise eingesetzten USB-Sticks kann man in zwei Gruppen aufteilen: Huawei E169G, Huawei E270, Novatel Wireless Ovation MC996D sowie Vodafone K4505-Z haben mehrere Jahre in einer gut gehüteten Schublade überdauert. Sie sind maximal für UMTS ausgelegt. Wir haben sie eigens für die ältere Fritzbox 3370 mit FritzOS 6.54 ausgegraben. Sie spielen aber auch an der neuen Fritzbox 7590.

Die übrigen Sticks sind neueren Datums, allesamt auch für LTE geeignet und stammen von einem kleinen Fischzug durch Gebrauchtbörsen. Alle waren für deutlich weniger als 50 Euro erhältlich. Nur der Vodafone K5006-Z und der KuWfi-Stick funktionierten an keiner der beiden Fritzboxen. Aber auch da sind Hopfen und Malz noch nicht verloren: Wenigstens den KuWfi, der einen Router und ein WLAN-Modul enthält, können immerhin Fritzboxen ab FritzOS 7.10 als WLAN-Hotspot verwenden. (dz) c't



Bild: Andreas Martini

Dateizugriff per SMB

Wer regelmäßig größere Datenmengen zwischen Computern austauschen muss, landet zwangsläufig bei dem, was im Volksmund als Windows-Freigabe bekannt ist. Längst können auch Macs, Linux-PCs, NAS-Büchsen und sogar Mobiltelefone und Tablets auf diese zugreifen. In der Praxis scheitert das jedoch oft an Details, die dieser Beitrag klärt.

Von **Peter Siering**

Bevor sich dieser Artikel an konkrete Hilfestellungen macht, bereitet er Sie mit einem Exkurs auf typische Probleme vor: Grundlage der Windows-Freigaben ist eine Protokollfamilie mit dem Namen „Server Message Block“ (SMB), die vorübergehend auch mal unter „Common Internet File System“ (CIFS) firmierte. Typisch für SMB ist die klare Rollenverteilung in Server und Client. Der Server stellt Freigaben bereit, der Client greift darauf zu. Als Protokollfamilie bezeichnet man sie, weil es verschiedene Spielarten gibt – was zunächst nicht weiter schlimm ist, weil Server und Client beim Aufbau einer Verbindung die Version absprechen.

Der Grundgedanke des Protokolls ist, dass hinter einem Client eine Identität steckt, meist ein realer Benutzer. Für sie ist auf dem Server (oder einer übergeordneten Verwaltungsinstanz, sprich Domäne) ein Name und ein Passwort hinterlegt. Dateien, die ein Client anlegt, gehören diesem Benutzer. Das Dateisystem auf dem Server und die dort hinterlegten Rechte spielen ebenfalls eine Rolle. Es genügt also nicht, dass ein Benutzerkonto Zugriff auf eine Freigabe erhält, auch die Rechte im Dateisystem hinter der Freigabe müssen passen.

Nickligkeiten

Stete Quelle großer Fehlersuchorgien sind die Annahmen, die vor allem Windows-Clients hinsichtlich des Benutzernamens und der Passwörter treffen. Windows schickt im ersten Anlauf den Namen des aktuell lokal angemeldeten Benutzers an den Server, wenn es auf eine Freigabe zugreift. Kennt der Server den Benutzer und passt das bei der lokalen

Anmeldung angegebene Passwort nicht, bittet der Server um Eingabe desselben. Kennt der Server den Nutzer nicht, fragt er sowohl den Namen als auch das Passwort ab. Der Zugriff auf Freigaben gelingt unter Windows obendrein nur mit Konten, für die auf der Server-Seite ein Passwort vergeben worden ist.

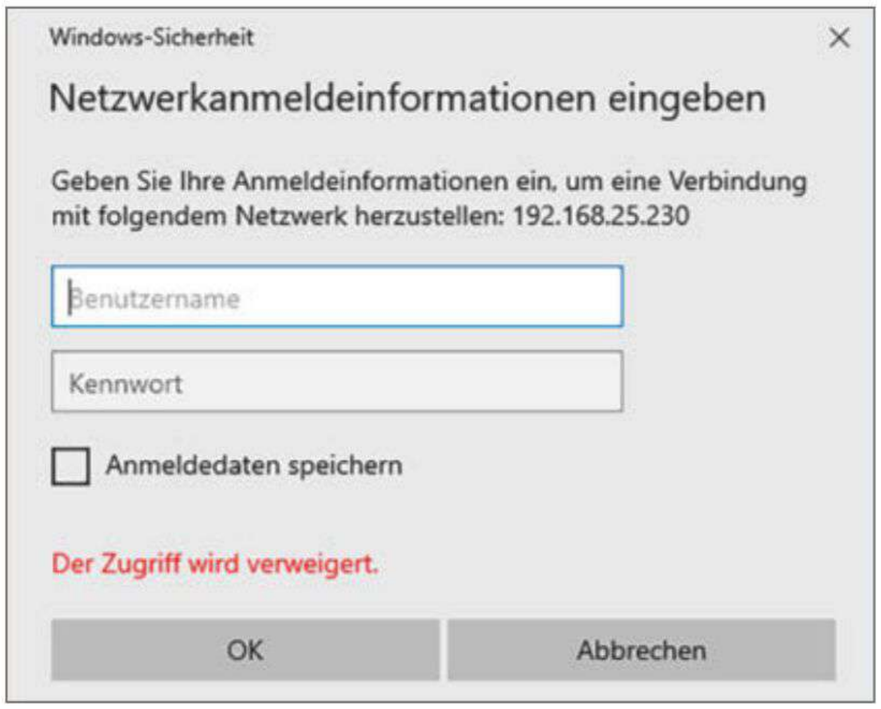
Windows überträgt zusammen mit dem Benutzernamen gern auch den Namen des Rechners, also nicht nur „peter“, sondern „meinpc\peter“. Nicht jeder Server verwirft den fremden Rechnernamen; die Anmeldung scheitert dann. Egal mit welchem Client kann ein leerer Rechnername in der Angabe des Benutzers helfen, etwa „\peter“ oder der Name des Servers selbst „server\peter“. In letzter Verzweiflung ist auch die alternative Schreibweise „peter@server“ einen Anlauf wert. Das klappt aber nur, wenn ein System überhaupt den Namen des Nutzers erfragt.

Der gut gemeinte Komfort vieler SMB-Clients, hauptsächlich der von Windows, die Anmeldeinformationen, also Name des Nutzers und Passwort für die angesprochene Freigabe lokal zu speichern, kann nach hinten losgehen: Wer beim Versuch, auf eine Freigabe zuzugreifen, partout ein „Zugriff verweigert“ erntet, sollte sich die gespeicherten Anmeldeinformationen ansehen. Vielleicht enthalten sie noch ein altes Passwort, das längst auf dem Server geändert wurde. Die folgenden plattformspezifischen Hinweise zeigen, wo Sie nachschauen müssen.

Eine letzte vornehmlich Windows-Clients zuzurechnende Eigenschaft rührt von der Abstammung als Einbenutzersystem her: Ein an Windows angemeldeter Benutzer kann standardmäßig nur unter einer Identität Verbindung zu einem Server aufnehmen. Hat sich der Nutzer „peter“ also mit dem Server „nas“ und der Freigabe „musik“ verbunden (in der typischen Schreibweise „\nas\musik“), kann er sich mit „\nas\videos“ auch nur als „peter“ verbinden.

Ein Server-Betreiber kann die Differenzierung von Möglichkeiten auf Freigaben also nicht mit verschiedenen Identitäten lösen, sondern muss dazu auf Rechte für Freigaben, Rechte im Dateisystem und Gruppen von Benutzern zurückgreifen – jedenfalls dann, wenn er mit verschiedenen Freigaben für diverse Benutzer arbeiten will. Das wird allerdings dank sich stapelnder Access Control Lists (ACLs) in Windows und modernen NAS schnell undurchsichtig.

Seine Krönung erfährt das Ganze dann, wenn man als regulärer Windows-Nutzer ein Laufwerk verbunden hat und dann aus Gründen eine Eingabeaufforderung mit Admin-Rechten öffnet. Auch wenn der Benutzer zum Beispiel „\nas\musik“ als Laufwerk M: verbunden hatte, sieht man das in der Admin-Eingabeaufforderung nicht – das kann irritierend sein, wenn man als Admin Dateien anderer Nutzer aufs NAS kopieren will.



Windows sendet beim Verbinden zu einer Freigabe automatisch zuerst den Namen des angemeldeten Benutzers. Wenn der oder das Passwort nicht passt, fragt es diese Daten ab.

Wer von diesen Eigenarten bisher nichts gehört hat, wird früher oder später bei Versuchen, Dateien über Freigaben durch die Gegend zu kopieren, daran scheitern – es sei denn, er hat Glück oder Intuition. Manche dieser Nickligkeiten bilden Clients anderer Couleur nach, etwa Anmeldedaten zu einem Server für eine Freigabe für andere Freigaben desselben Servers zu recyceln. Aber macOS und Linux ergänzen durchaus auch eigene Schrullen.

Marotten

Kopfschmerzverstärkend wirkt, wie die beteiligten Systeme Passwörter behandeln. SMB-Server und -Clients speichern und versenden die schon ewig nicht im Klartext, sondern schicken sie durch Hash-Funktionen und vergleichen zur Überprüfung die Hashes. Unix-Systeme verwenden dazu traditionell andere Verfahren als Windows. Dadurch muss man, wenn Linux- oder macOS als Server dienen, für jeden Benutzer, der via SMB zugreifen soll, ein Extra-Passwort festlegen. Eine automatische Synchronisierung mag möglich sein, setzt aber aktive Konfigurationsarbeit voraus [1].

So wie Windows typischerweise davon ausgeht, dass nur ein einzelner Nutzer einen PC interaktiv verwendet, ist die Linux-Welt eher so ausgerichtet,

dass mehrere Nutzer gleichzeitig auf einem PC aktiv sein können. Der Zugriff auf Dateien, egal ob lokal oder im Netz, wird über eine systemweite Konfigurationsdatei (/etc/fstab) geregelt. Das passt nicht so recht zu einer Sichtweise aus Nutzerperspektive. Das wird auf Linux-Client-PCs jedoch gern genutzt, um persönliche SMB-Freigaben außerhalb der grafischen Bedienoberfläche etwa in der Shell erreichbar zu machen.

Spätestens hier wird klar, welchen großen Dienst die zahlreichen NAS-Hersteller ihren Kunden erweisen: Nicht nur verbergen sie die nervigen Unterschiede der Passwortbehandlung. Sie schaffen es auch, die Verwaltung der Benutzer und die Vergabe von Rechten im Dateisystem und auf Freigabeebene hinter einer mehr oder minder gelungen vereinfachten Weboberfläche zu verbergen. Wer mehr will, kann das mit dem freien Datei- und Druckdienst Samba selbst zusammenschrauben [1].

Nicht nur Windows, auch viele andere Systeme benutzen die veraltete Version von SMB (SMB1) nicht mehr freiwillig, weil es Clients und Server dazu nötigt, zu viele vertrauliche Informationen im Netzwerk preiszugeben und für Eindringlinge eine leichte Beute ist. Heute sind SMB2 oder 3 Standard und bieten unter anderem bessere Performance. Aber es gibt durchaus Server, die es nicht besser können, etwa noch populäre ältere Fritzboxen, alte Netzwerk-

Gemeinsamer Nenner

Wichtig für erfolgreiche Versuche, Dateien via SMB auszutauschen, ist, dass das Netzwerk darunter einwandfrei funktioniert: Client und Server sollten im gleichen IP-Subnetz stecken, also IP-Adressen haben, die aus demselben Netz stammen, etwa 192.168.178.100 und 192.168.178.109 bei einer Netzmaske von 255.255.255.0; die Zahlen vor dem letzten Punkt dürfen also nicht variieren. In diesem Fall sollte in einer Kommandozeile auf dem Rechner mit der Adresse 192.168.178.109 ein `ping 192.168.178.100` Antworten des Rechners mit der 100 am Ende der Adresse erbringen. Oft klappt dann auch die lokale Auflösung von Namen, etwa ein `ping nas`.

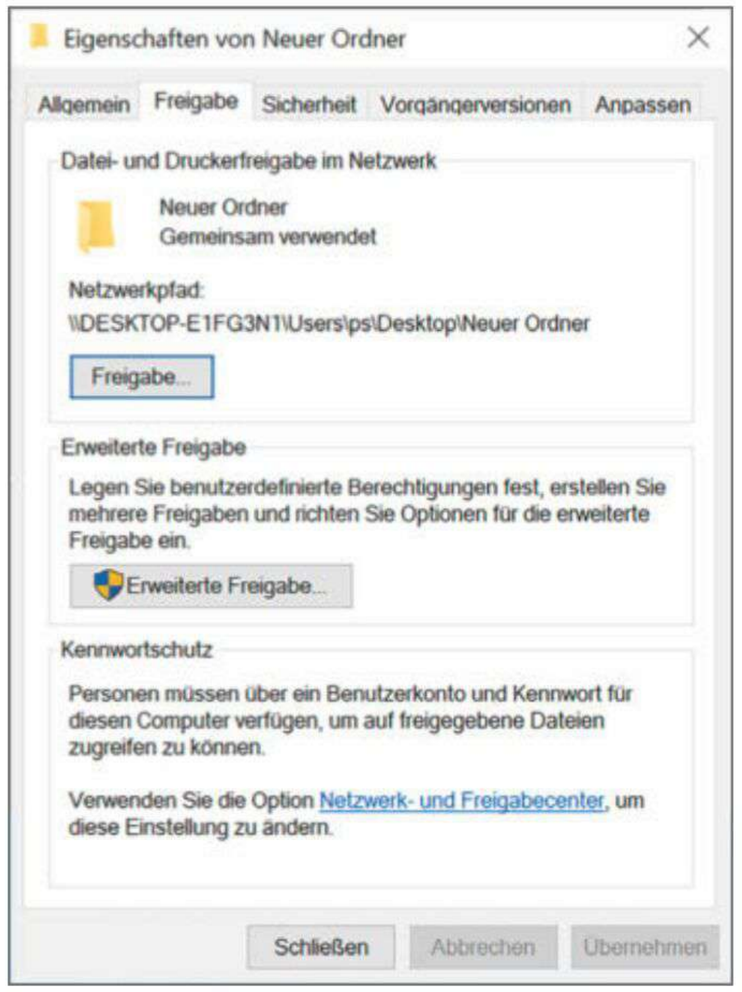
Wenn es sich um unterschiedliche Netze handelt, kann man mit `ping` prüfen, ob die Rechner einander grundsätzlich erreichen. Eine Aussage, ob sich deren Verbindung für SMB eignet, lässt sich daraus nicht ableiten. Eine zwischen ihre Netze geschaltete Firewall könnte das Pingen zulassen, SMB aber verbieten. Je öffentlicher eines der beiden Netze ist, desto größer ist die Wahrscheinlichkeit. Auch große WLAN-Installationen verbieten oft die Kontaktaufnahme von Clients untereinander. Sie sollten zusätzlich überprüfen, ob Regeln der geräteeigenen Firewall Ihnen vielleicht einen Strich durch die Rechnung machen.

Ein Wort noch zur Namensauflösung in SMB-Netzen: Ohne weitere Hilfestellung durch spezielle Nameserver fanden die Rechner einander im selben IP-Netz über Rundrufe (Broadcasts). Früher war es zudem üblich, dass sie aus ihrer Mitte einen auserkoren haben, der die Annoncen von Namen sammelt und den anderen bereitstellt (Browser genannt). Unter anderem mit dieser Hilfe füllte sich die Windows-Netzwerkumgebung auf dem Desktop, die allerdings nie als besonders zuverlässig galt. Das heute gängige SMB2 und 3 ersetzen derlei Verfahren durch neuartige „Web Service Discovery“-Dienste.

Wer auf den Zugriff via Namen besteht und die beteiligten Geräte dauerhaft betreiben will, sollte auf feste IP-Adressen sowie einen funktionierenden lokalen DNS-Nameserver setzen. Sollen Samba-Server in einem solchen Szenario auch in der Netzwerkumgebung sichtbar sein, hilft es, auf ihnen einen Web Service Discovery Daemon zu betreiben, den es als freie Implementierung gibt (siehe ct.de/wj6v). Für die Ad-hoc-Vernetzung tut man sich einen großen Gefallen, mit den IP-Adressen vorliebzunehmen. In Heimnetzen genügt meist der Namensdienst des Routers, der lokale Namen registriert und auflöst, den beispielsweise eine Fritzbox anbietet.



Die Freigaben eines PCs mit einer aktuellen Version von Windows 10 tauchen auf anderen PCs im Explorer unter dem Netzwerksymbol nur auf, wenn Sie zustimmen, dass der PC von anderen im Netz gefunden werden kann.



Die einfache „Freigabe“ trifft im Unterschied zu „Erweiterte Freigabe“ einige Annahmen über das Ansinnen des Nutzers und veröffentlicht nicht nur das Verzeichnis „Neuer Ordner“ im Benutzerprofil des Nutzers „ps“, sondern gleich den ganzen Ordner „c:\Users“.

scanner oder Spezialgeräte, deren Anschaffungspreis in fünfstelligen Regionen liegt. Wer partout nicht umhin kommt, kann SMB1 erlauben, sollte das aber nur in einem vollständig separierten Netzwerk tun.

Womit man auch stets rechnen muss, wenn man plattformübergreifend Dateien austauschen möchte, sind unterschiedliche SMB-Implementierungen. Besonders Apple geht dabei gern eigene Wege. So gab es zwischenzeitlich sogar Software, mit deren Hilfe sich ein regulärer Samba-Server auf macOS einrichten ließ. Mit den neueren Versionen von macOS klappt das aber nicht mehr.

Windows als Server

Soweit zu den Gemeinsamkeiten, jetzt zu den einzelnen Protagonisten: Eine reguläre Windows-Installation auf dem Desktop-PC dient erst dann als Server, wenn sie dazu angehalten worden ist, dem lokalen Netzwerk zu vertrauen, dieses Netzwerk also als „privat“ einstuft. Andernfalls beißt man sich die Zähne aus. Beim Einrichten einer Freigabe vergewissert sich Windows, in welchen Netzen es Freigaben anbieten soll und offeriert, den aktuellen Zustand geeignet anzupassen (also von öffentlich auf privat umzustellen). Das kann man auch von Hand tun, indem man das Startmenü mit der Windows-Taste öffnet und nach „Freigabe“ suchen lässt. Windows bietet dann „Erweiterte Freigabeeinstellungen verwalten“ an.

Wenn Sie den Zugriff nicht für Ihr eigenes, ohnehin schon vorhandenes Konto erlauben wollen, müssen Sie eines dafür anlegen. In der Pro-Ausgabe von Windows 10 führt der mit Abstand einfachste Weg zu einem neuen Konto immer noch über die „Computerverwaltung“ (im Windows+X-Menü) und dort den Bereich „Benutzer und Gruppen“. Wenn Sie es stattdessen über die Einstellungen versuchen (Windows+I), versucht Windows, Ihnen sofort ein Microsoft-Konto unterzujubeln – und das ist für Netzwerkzugriffe nicht hilfreich. Unter Home gelingt das Anlegen von Nutzern am schnellsten in der Eingabeaufforderung mit `net user`.

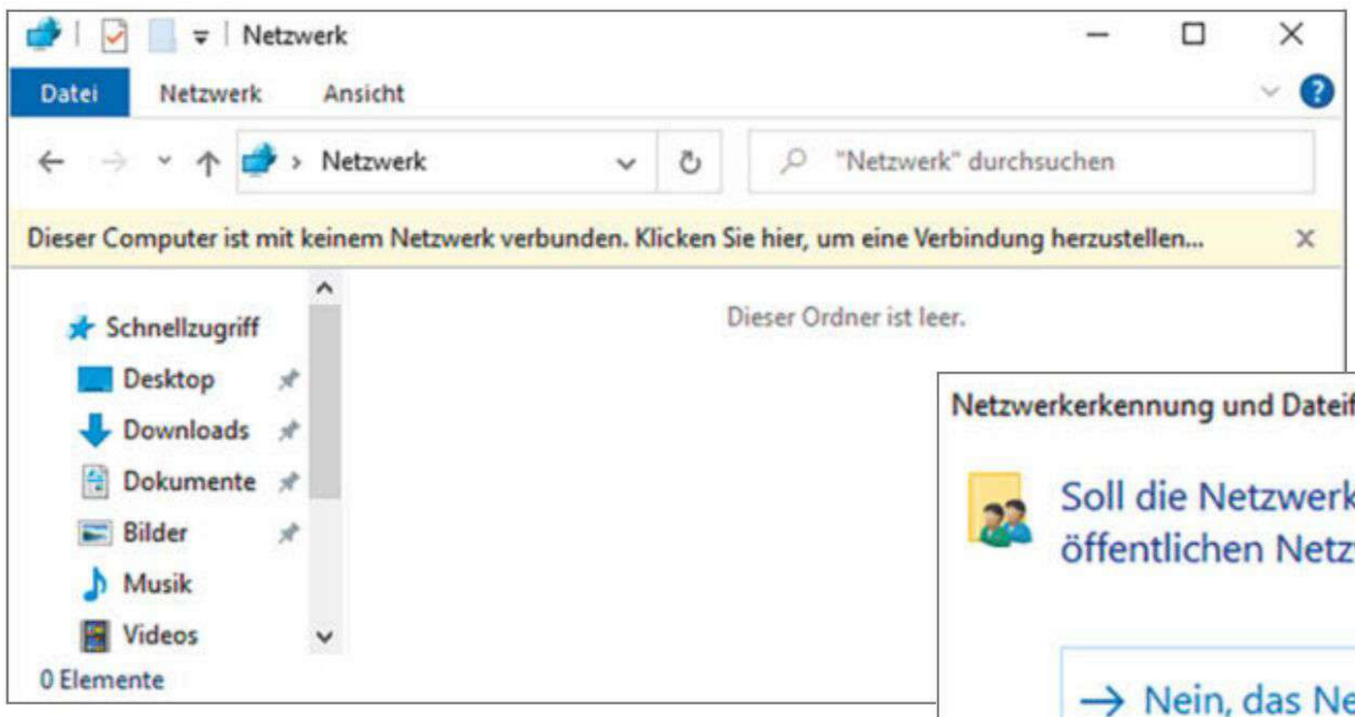
Die einfache Freigabefunktion, die Sie über die Eigenschaften eines Ordners unter Freigabe oder über das Kontextmenü mit „Zugriff gewähren auf“ erreichen, legt ein besonderes Verhalten an den Tag: Wenn das freizugebende Verzeichnis unterhalb eines Nutzerprofiles liegt, also unterhalb von c:\Users beziehungsweise c:\Benutzer, und zum Beispiel ein Verzeichnis auf dem Desktop eines Nutzers oder ein Unterverzeichnis seiner Dokumente ist, stellt Windows c:\Users komplett ins Netz. Wenn die Dateirechte in dieser Verzeichnishierarchie abweichend gesetzt sind, könnten andere Zugriff auf private Daten übers Netz erhalten.

Um solche Automatiken zu meiden, empfiehlt sich die „Erweitere Dateifreigabe“, die Sie ebenfalls als Knopf im Eigenschaftsdialog von Ordnern oder Dateien finden. Wenn man sie bemüht, um ein Verzeichnis freizugeben, interpretiert Windows diesen Wunsch nicht, sondern gibt genau das gewünschte Verzeichnis frei, egal wo es im Dateisystem liegt. Man muss dann allerdings etwas mehr Arbeit investieren, die Besucher aussuchen und die Rechte unterhalb des Verzeichnisses so anpassen, dass die zugelassenen Nutzer dort auch lesen, schreiben und was auch immer dürfen – diesen Teil der Arbeit nimmt die einfache Dateifreigabe klickfaulen Nutzern ab.

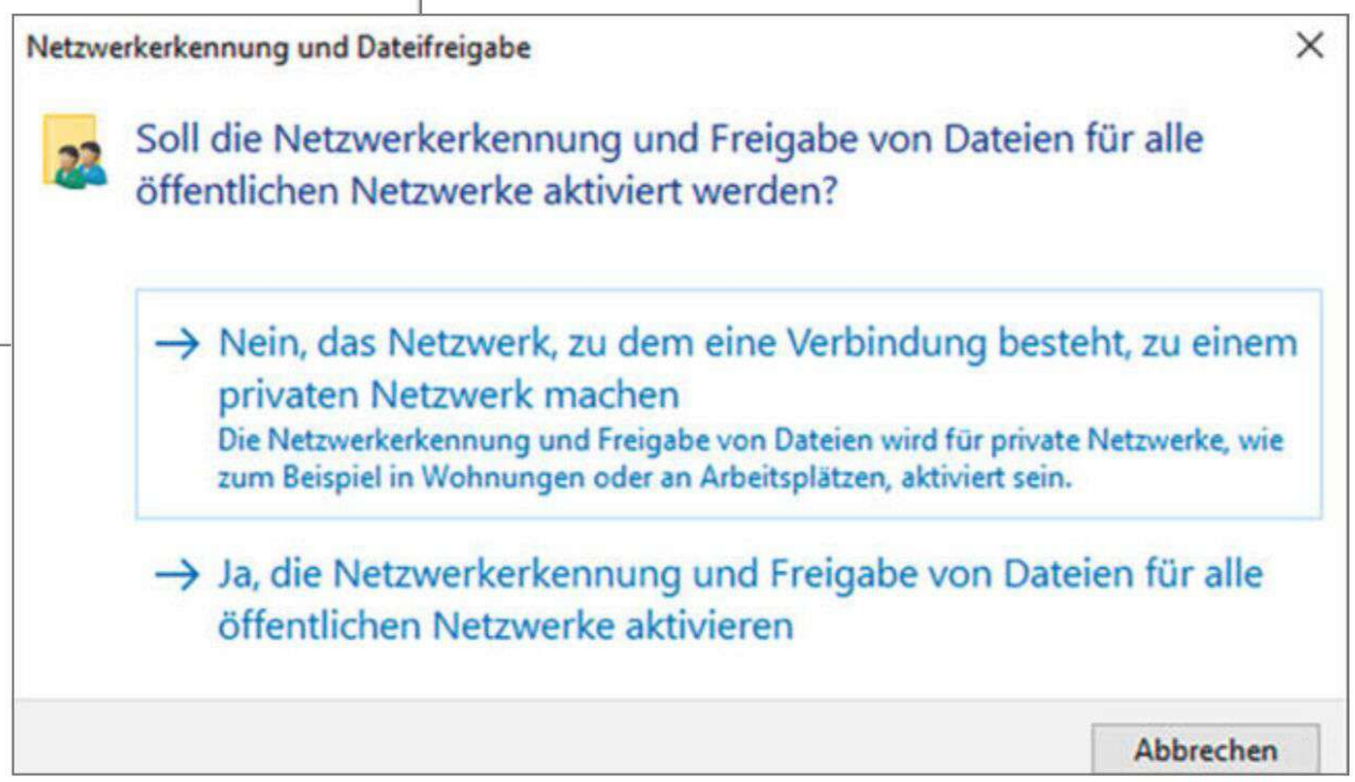
Windows als Client

Auch ein Windows-Client möchte freiwillig und sinnvollerweise nur in einem privaten Netz auf Freigaben zugreifen. Wenn Sie im Explorer das erste Mal auf „Netzwerk“ klicken, erscheint am oberen Rand eine gelbe Zeile mit einem Hinweis. Sie können Windows darüber erlauben, im lokalen Netz zu suchen und gleichzeitig auffindbar zu sein. Folgen Sie gegebenenfalls der Empfehlung, das aktuelle Netz zu einem privaten zu machen, wenn es denn Ihr eigenes und vertrauenswürdig ist. Sollten Sie das Angebot nicht erhalten, hilft auch auf dem Client die Suche, um „Erweiterte Freigabeeinstellungen verwalten“ aufzurufen.

Der Zugriff auf Freigaben ist auch ohne diese Zustimmung möglich. Geben Sie dazu in einem Explorer-Fenster in der Adresszeile den Namen einer Netzwerkressource oder deren IP-Adresse ein. Beim Zugriff auf die erste Freigabe eines Servers fragt

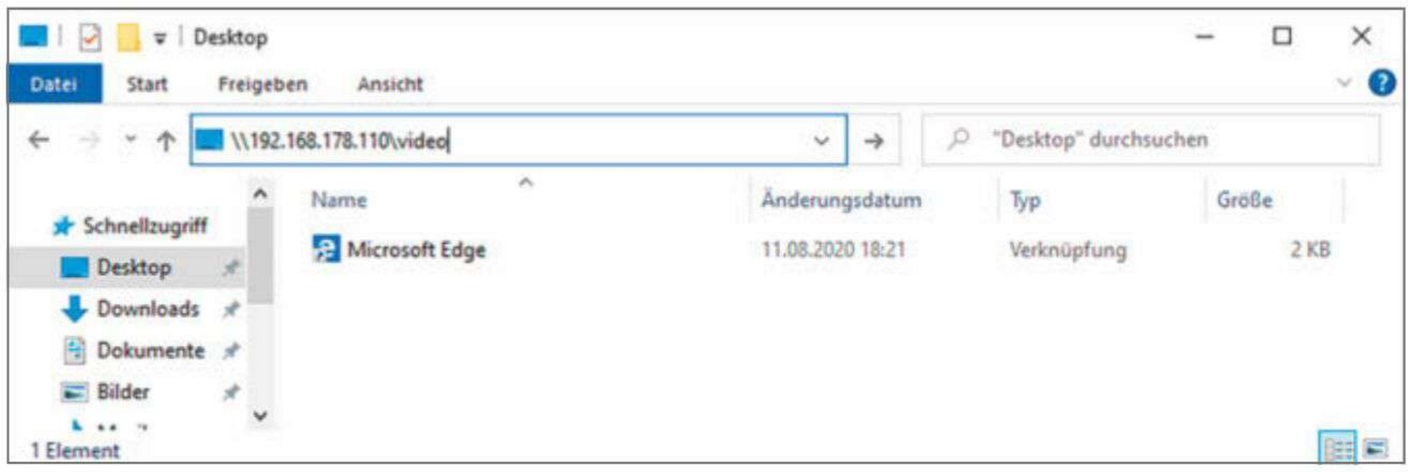


Beim ersten Klick auf das Netzwerksymbol im Explorer mangelt es meist nicht an einer Netzwerkverbindung, sondern Windows möchte nur, dass Sie ...



... auch für den Client festlegen, wie vertrauenswürdig das Netzwerk ist. Freigaben sollten im öffentlichen Netz nie erlaubt sein.

Wenn Sie eine Freigabe nicht über den Namen des Servers erreichen, probieren Sie es stattdessen mit der IP-Adresse – das sollte immer klappen.



Windows bei Bedarf Benutzernamen und Passwort ab. Es bietet bei dieser Gelegenheit an, diese Daten zu speichern. Sie können diesen Speicher über eine Suche im Startmenü nach „Anmeldeinformationen“ einsehen und bearbeiten oder das auf der Kommandozeile erledigen: `cmdkey /list`.

Wenn der für die lokale Anmeldung verwendete Benutzername auf der Gegenseite bekannt ist, aber nicht verwendet werden soll, müssen Sie die Automatik überstimmen: Das geht ohne viel Federlesen auf der Kommandozeile mit dem `net use`-Befehl. Mit `net use * \\nas\freigabe /user:hans` schickt Windows direkt den Benutzernamen „hans“ und erfragt das Passwort. Das Überstimmen des Namens klappt allerdings nur, wenn noch keine Verbindung zum Server besteht.

Der Stern in dem Befehl sorgt direkt dafür, dass die Freigabe mit dem nächsten unbenutzten Laufwerksbuchstaben verbunden wird. Sie können stattdessen auch einen Laufwerksbuchstaben vorgeben. Es geht aber auch ganz ohne. Gibt man nach erfolgreich hergestellter Verbindung (mit `net use` können Sie die aktuell verbundenen Freigaben sehen) den Pfad \\nas\freigabe in die Adresszeile des Explorer ein, zeigt Windows ohne weitere Rückfragen die Inhalte der Freigabe, nutzt dafür aber den zuvor mit `/user:` festgelegten Nutzernamen.

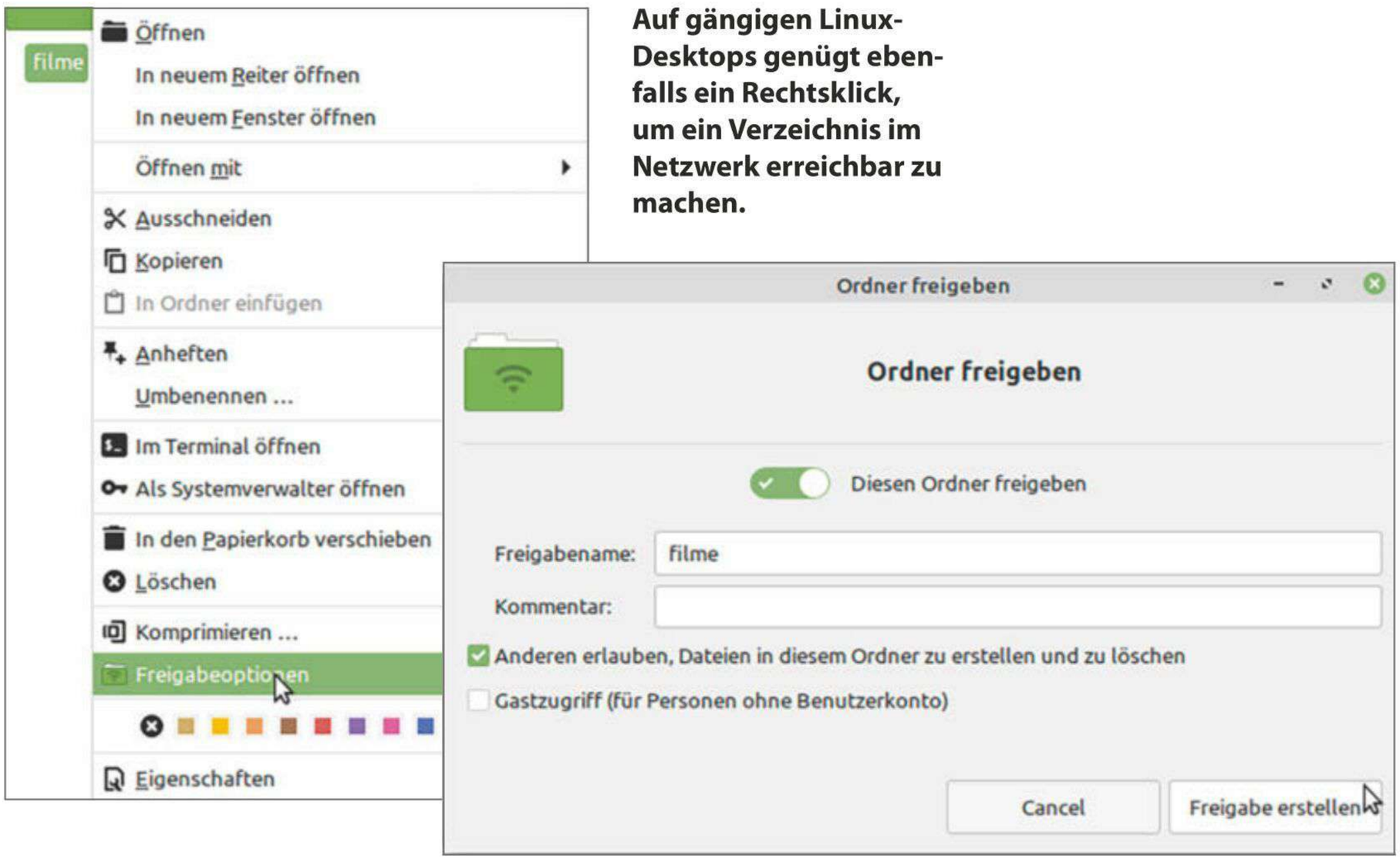
Ob Windows auf diese Weise auf einen Windows-Server, einen Mac, ein NAS oder ein anderes Unix-System mit Samba zugreift, spielt keine Rolle. Wenn der Zugriff über den Namen nicht gelingt, probieren Sie es mit der IP-Adresse. In größeren Netzen kann es nötig sein, statt des nackten Namens den vollqualifizierten Namen zu nehmen, also statt nur \\server\freigabe einzugeben \\server.ct.heise.de\freigabe. Wenn ein korrekter Benutzername keinen Zugriff erlaubt, stellen Sie Server, Rechner und eventuell Domain-Namen mit Backslash voran, etwa „server\hans“.

Linux als Server

Über den Betrieb von Linux als SMB-Server kann man dicke Bücher schreiben. Das liegt daran, dass die dafür zuständige freie Software Samba in der Lage ist, Windows-Server vollständig zu ersetzen. Seit Version 4 kann man mit ihrer Hilfe sogar den Windows-eigenen Verzeichnisdienst Active Directory betreiben. Nahezu jedes NAS verwendet heute Samba für SMB-Freigaben. Ungewöhnlich ist, wie Samba auch dann zum Einsatz kommt, wenn ein Linux-Client Dateien im Netz freigibt – diesen Teilaspekt betrachtet dieser Artikel im Detail. Wenn Sie weitere Samba-Ambitionen hegen, hilft unter anderem [1].

Ein voll ausgestatteter Linux-Desktop erlaubt normalerweise per Rechtsklick auf einen benutzereigenen Ordner das Einrichten einer Freigabe. Fehlt die Option, sind einige Pakete nachzuinstallieren. Deren Namen hängen vom verwendeten Desktop und seinem integrierten Dateimanager ab. In der Regel handelt es sich um Pakete wie nemo-share, nautilus-share oder caja-share. Zusätzlich erwarten die, dass auch das Paket samba eingerichtet ist. Im Freigabedialog erscheint ein Hinweis, wenn Samba noch fehlt. Eine Grundkonfiguration von Samba ist nicht nötig – nutzen Sie die Standardvorgaben.

Beim Einrichten einer Freigabe im Desktop wird Samba instruiert, eine Freigabe einzurichten. Dazu gibt es ein spezielles Modell, die sogenannten User-Shares. Sie lassen sich über das Samba-eigene `net`-Kommando verwalten. Nach Einrichten einer Freigabe gibt `net usershare list` eine Liste aus oder zeigt mit passenden Optionen unter anderem Details einer Freigabe an. Das ist unterm Strich sehr bequem, um mal eben Dateien mit einem Windows-PC übers Netz auszutauschen. Die Freigabe besteht nur, wenn der freigebende Benutzer auch angemeldet ist. Für dauerhaft laufende Server eignet sich das nicht.



Auf gängigen Linux-Desktops genügt ebenfalls ein Rechtsklick, um ein Verzeichnis im Netzwerk erreichbar zu machen.

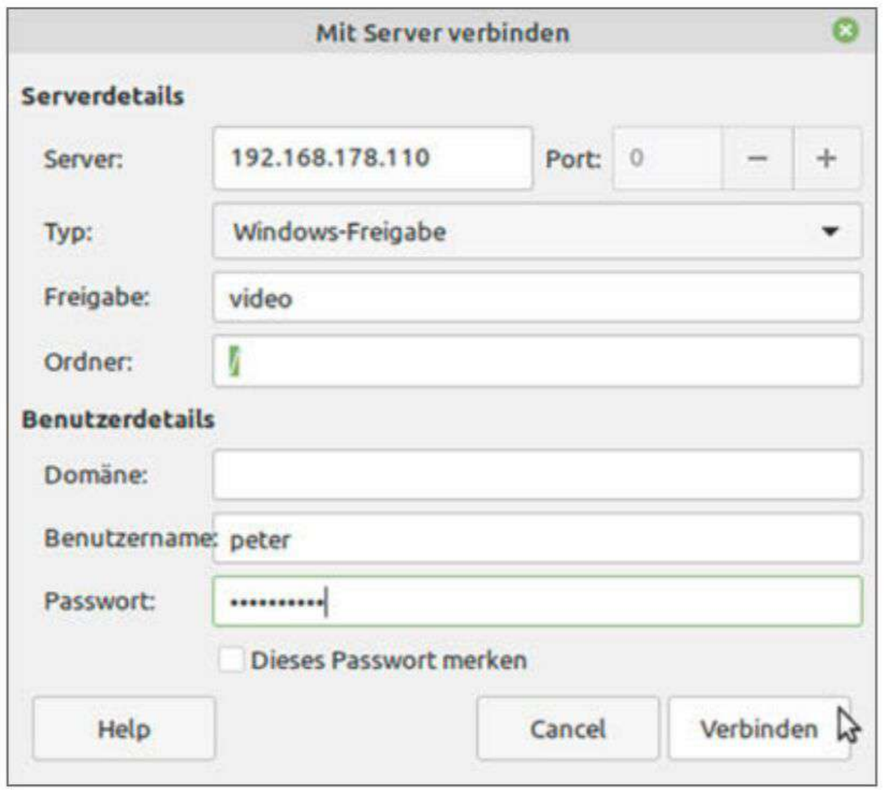
Die Optionen für die Freigabe fallen eher spärlich aus. Für einen passwortgeschützten Zugriff ist es notwendig, auf der Kommandozeile noch Kennwörter für die Nutzer zu setzen.

Wenn Sie eine solche Freigabe schützen, also nicht für jeden offen stehen lassen wollen, müssen Sie für jeden Nutzer einen Extrahandgriff ausführen. Wie im Einstieg erläutert, kann Samba bei einem Zugriff mitgeschickte Passwortdaten nicht mit den für Unix-Nutzer hinterlegten Kennwörtern abgleichen. Sie müssen für jeden vorhanden Unix-Nutzer, der zugreifen dürfen soll, mit `smbpasswd -a <name>` ein Kennwort setzen – dies wird passend für Samba gehasht. Eine Liste der gesetzten Kennwörter liefert das Kommando zum Bearbeiten von Samba-Passwortdatenbanken: `pdbedit -L`. Mit `pdbedit -x -u <name>` können Sie gesetzte SMB-Kennwörter auch wieder entfernen.

Linux als Client

Der Zugriff auf SMB-Server vom Linux-Desktop aus ist längst keine Hexerei mehr. Die üblichen Verdächtigen, die auch beim Freigeben von Verzeichnissen helfen, übernehmen auch den Client-Part, sprich die Desktop-Umgebungen. Sie nutzen dazu aber weder Samba als Software noch greifen Sie auf die Fähigkeiten des Linux-Kernels zurück, SMB-Freigaben als Dateisystem in den Dateibaum einzuhängen. Die SMB-Fähigkeiten erlernen Gnome-artige Oberflächen über das Gnome Virtual File System (GVfs). Darin stecken noch viele weitere Backends, etwa für Apples Netzwerkprotokoll AFP, WebDAV und SFTP. KDE bemüht dafür analog seine KIO-Slaves.

Der Benutzer gibt in der Adresszeile des Dateimanagers „smb://nas/video“ ein, um auf die Freigabe „video“ zuzugreifen. Wenn die Auflösung des Namens nicht gelingt, probiert man es mit der IP-Adresse. Die Oberfläche fragt dann Benutzernamen und Passwort ab. In einer Umgebung mit zentraler Benutzerverwaltung via Active Directory hilft es mitunter, den Namen der Domäne nicht wie gängig aus dem Benutzernamen mit Backslash oder @-Zeichen zusammenzubauen, sondern ihn in das Workgroup-Feld einzutragen. Die von KDE eingehängten SMB-Freigaben finden sich im Dateisystem nicht. Gnome lässt sie unter dem Verzeichnis /run durchscheinen, sodass man auch im Terminal Zugriff hat.



Linux-Dateimanager bieten meist auch eine spezielle Funktion zum Verbinden mit anderen Servern an.

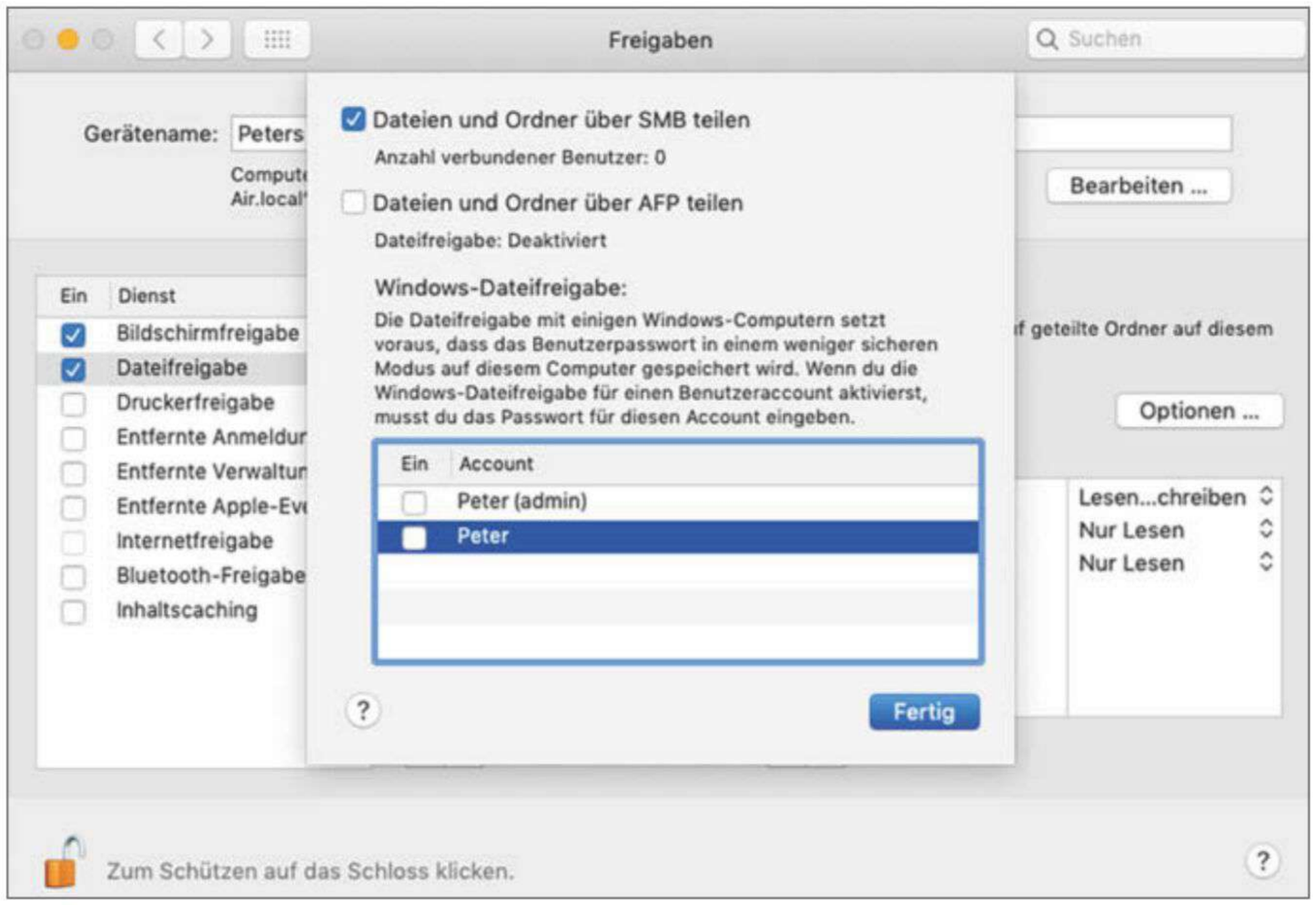
Die so eingebundenen SMB-Freigaben sind allerdings nur sichtbar, solange die Benutzersitzung anhält. Meldet sich der Benutzer ab, sind sie verschwunden. Über den KDE-Assistenten zum Einbinden eines Netzwerkordners kann man sie so einrichten, dass sie sofort nach Anmeldung sichtbar sind. Gnome-Nutzer können sich bei frisch hergestellter Verbindung mittels Rechtsklick auf dieselbe ein Lesezeichen erstellen lassen. Wenn Sie zuvor Gnome gebeten haben, das Passwort für die Freigabe zu speichern, genügt ab sofort ein Doppelklick auf das Lesezeichen, um die Verbindung wiederherzustellen.

Manchmal genügt das nicht, etwa wenn ein Linux-Desktop mit Cronjobs auf Netzwerkfreigaben zugreifen soll, um Backups dorthin zu schieben. Dann bietet es sich an, SMB-Freigaben über einen Eintrag in der Datei /etc/fstab einzubinden. Ein solcher Eintrag ist schnell konstruiert:

```
//192.168.178.12/psbackup /backup cifs uid=9001,↵
↳gid=150,credentials=/etc/samba/backup,rw 0 0
```

Er legt fest, welche Freigabe wo eingehängt wird. Die Art des Dateisystems bestimmt die Option „cifs“. Die lokal verwendete User- und Gruppen-ID steht in `uid` und `gid`.

Die Zugangsdaten für die Freigabe sind am besten in einer separaten Datei aufgehoben (im Beispiel /etc/samba/backup), auf die möglichst wenig Nutzer Zugriff haben sollten – schließlich sind das oft kritische Angaben, die in einem Unternehmen vielleicht auch zum Abrufen von Mails dienen können. Diese Datei schaut wie folgt aus:



Die Dialoge zum Freigeben von Dateien hat Apple seit ewig und drei Tagen nicht überarbeitet. Für alle Benutzer, die per SMB zugreifen sollen, muss man deren Passwort erneut eingeben.

```
username=ps
password=DasFetzt
```

Sie sollte mit `chmod 600` nur für den User root einsehbar gemacht werden. Ohne Root-Rechte geht es an dieser Stelle nicht, weil das Mounten eben im Kontext dieses Nutzers erfolgt. Auf diese Weise eingehängte SMB-Freigaben stehen beim Systemstart losgelöst von einer Nutzeranmeldung bereit. Achtung: Je nachdem, welche Rechte für den Mount-Punkt gelten, könnten dadurch andere Nutzer auf dem Linux-Desktop auf die privaten Daten des Nutzers übers Netz zugreifen!

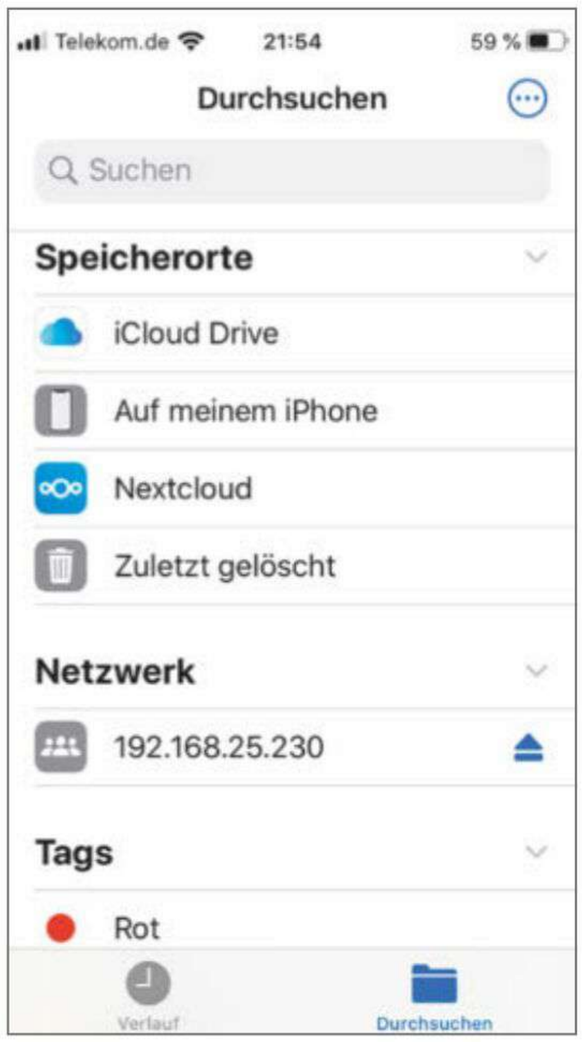
Mac sowohl als auch

Apple hat zwar eine eigene Server-Edition von macOS eingestellt, aber die Fähigkeit, Dateien im Netz bereitzustellen, wohnt auch der regulären Ausgabe inne. Für die Inbetriebnahme fällt wenig Arbeit an: In den Systemeinstellungen unter Freigaben ein Häkchen unter Dateifreigabe setzen und unter Optionen je nach Bedarf AFP (also das Apple-eigene Protokoll) oder SMB aktivieren.

Wenn Sie SMB nutzen, fordert Sie macOS in den Optionen auf, für die Nutzer das Passwort einzugeben. Die Frage kommt, sobald Sie den Zugriff für den jeweiligen Nutzer mit der Checkbox aktivieren. Das Passwort, das Sie eingeben, muss dem für die Person bereits gesetzten entsprechen. Zum Deaktivieren des Zugriffs fragt macOS genau dieses Passwort erneut ab.

Als Client ist macOS üblicherweise unauffällig, von einem Detail abgesehen: Wenn es auf eine SMB-Freigabe zugreift, hinterlässt es dort viele Dateien, die mit einem Punkt beginnen. Darin legt es erweiterte Informationen zu den Dateien und zum Volume ab, für die Apple-Dateisysteme spezielle Strukturen vorhalten. Auf Datenträgern, die so etwas nicht anbieten, benutzt macOS stattdessen einfach normale Dateien mit der eigenwilligen Namensgebung. Mancher, der das zum ersten Mal gesehen hat, erschreckt und hält ein Dateisystem für kaputt.

Für Zugriffe auf eine SMB-Freigabe verwendet man den „Mit Server verbinden“-Dialog des Finders im „Gehe zu“-Menü: Gibt man dort nur den Servernamen mit vorangestelltem „smb://“ an, etwa „smb://nas“, so zeigt macOS die Freigaben auf dem Server an. Beim Verbinden mit einer Freigabe erfragt es Namen und Passwort und erlaubt es, die Zugangsdaten im Schlüsselbund zu speichern.



Seit iOS 13 können sich iPhones und iPads mit einem SMB-Server verbinden.

Fürs automatische Verbinden mit SMB-Freigaben existieren mehrere Wege. Nicht jeder führt in allen macOS-Versionen zum Ziel: Der Klassiker besteht darin, ein verbundenes Laufwerk per Drag & Drop in die Anmeldeobjekte des Benutzers unterhalb von „Benutzer & Gruppen“ in den Systemeinstellungen zu ziehen. Wenn das nicht gelingt, bietet sich ein Automator-Skript als Anmeldeobjekt oder zusätzliche Software an: Die Freeware „ConnectMeNow“ wird dafür immer wieder empfohlen.

Die anderen

Das Vorgehen mit anderen Clients und Servern ergibt sich analog: Auf einem NAS sollte man Benutzer passend zu den Konten einrichten, die auf Windows-Clients zur lokalen Anmeldung verwendet werden. In speziellen Clients, wie sie für Android zum Beispiel in Form von Dateimanagern angeboten werden, gibt man den Pfad zu SMB-Freigaben mit der üblichen Notation ein, etwa „smb://nas/video“ – nur Windows verwendet Backslashes und stellt kein „smb:“ voran. Seit iOS 13 können sogar Apple-Geräte in ihrer Dateien-App direkt mit SMB-Servern in Kontakt treten. Wenn der Austausch per SMB nicht funktionieren will, drehen Sie die Richtung um: Lassen Sie Client und Server die Rollen tauschen. (ps) c't

Literatur

[1] Johannes Merkert, Anke Poimann, **Selbstbau-System**, Heim-Server mit Linux installieren, c't 8/2016, S. 106

Erwähnte Software

ct.de/wj6v

betterCode()

WebAssembly 2021

Die Heise-Konferenz zu Wasm

31. August 2021 ONLINE

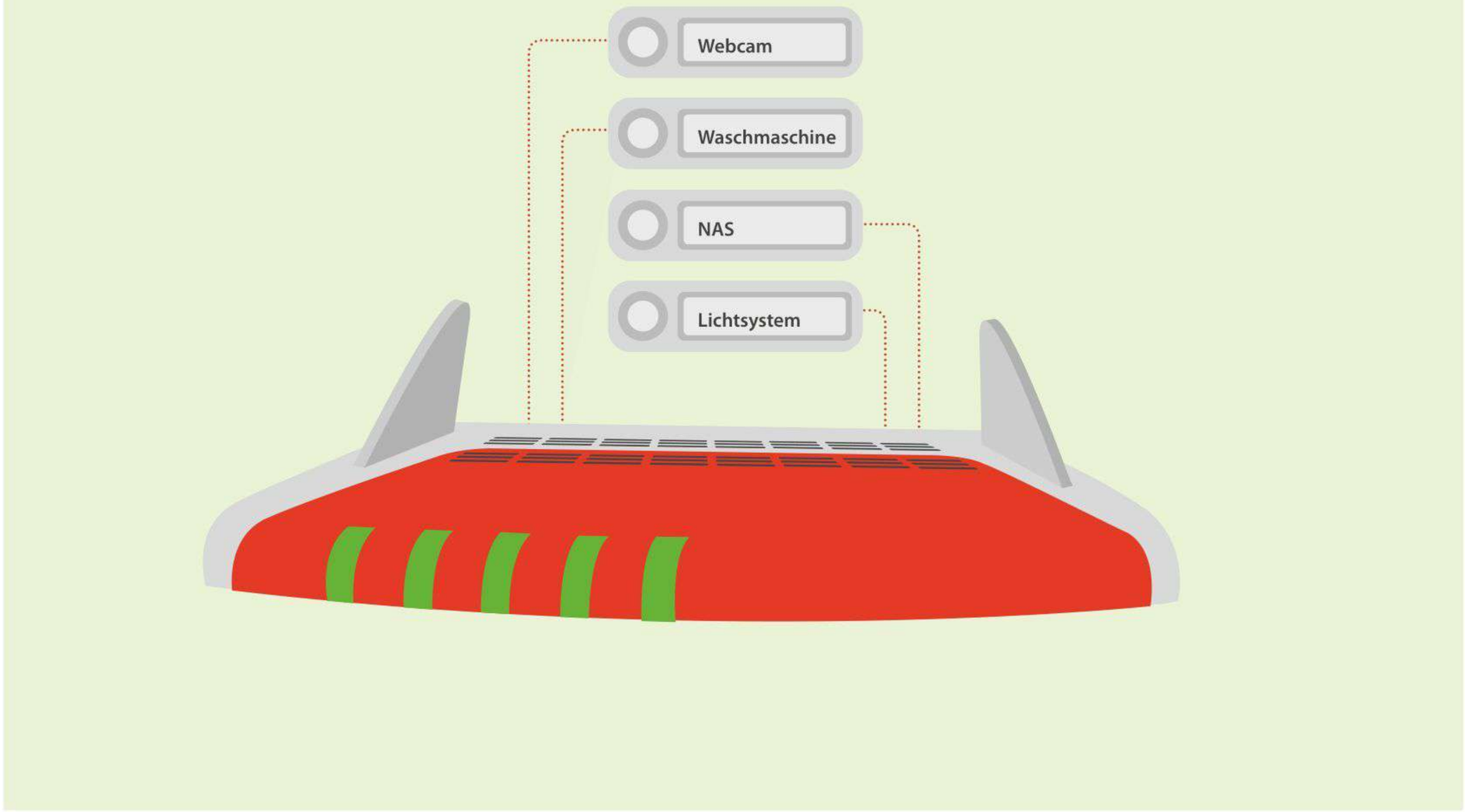
Jetzt Tickets sichern!

Game Changer auch jenseits des Web

- Dein Einstieg in das sprach- und plattformübergreifende Ökosystem
- Lerne den richtungsweisenden W3C-Standard kennen
- Deep Dives in Blazor, Rust, C#, JavaScript, Container und Flutter
- Tausche dich aus mit WebAssembly-Insidern

heise Developer dpunkt.verlag

wasm.bettercode.eu



DynDNS mit IPv6 leicht gemacht

Viele Internetanbieter vergeben aufgrund von Knappheit keine öffentlichen IPv4-Adressen mehr. Für den Zugriff auf Webcams oder NAS-Geräte aus dem Internet bleibt dann nur IPv6. Gängiges DynDNS funktioniert damit jedoch nicht. Doch DynDNS für IPv6 einzurichten ist kein Hexenwerk und lohnt sich selbst mit öffentlichen IPv4-Adressen.

Von **Andrijan Möcker**

Wer Netzwerkgeräte im Heimnetz von unterwegs erreichen möchte, nutzt normalerweise dynamisches DNS. Damit erspart man sich, die aktuelle IP-Adresse des eigenen Anschlusses nachzuschlagen. Stattdessen teilt ein Client im Router oder auf einem Rechner dem DynDNS-Dienstleister die aktuelle IP-Adresse mit und dieser ordnet sie der gewählten DynDNS-Domain zu, sodass man nur diese kennen muss. Mit dem veralteten IPv4-Protokoll ist das leicht überschaubar: Dabei hat nur der Router eine öffentliche Adresse, die er an den DynDNS-Anbieter übermittelt.

Am Router angeschlossene Heimnetzgeräte kommen über die Netzwerkadressübersetzung (NAT) ins Internet. Damit sie eingehende Verbindungen annehmen, lenkt man diese im Router per Portweiterleitung zum richtigen Gerät.

IPv6 funktioniert anders: Der Router erhält statt nur einer Adresse einen Adressblock, sodass alle Geräte hinter dem Router über eine eigene öffentliche IP-Adresse erreichbar sein können. Deshalb entfällt die Netzwerkadressübersetzung genauso wie die Portweiterleitung – stattdessen richtet man im Router eine Portfreigabe ein. Folglich benötigt man für jedes freizugebende Gerät einen eigenen DynDNS-Hostnamen. Das ist von Vorteil: Man kann beispielsweise mehrere Webcams oder Webserver an einem Anschluss betreiben und dennoch alle über Port 443 ansprechen. Mit IPv4 geht das nicht. Weiter kann jedes Gerät eine individuelle Domain erhalten, die ausschließlich auf dessen IPv6-Adresse zeigt.

DynDNS-Präfix-Updates

Viele DynDNS-Anbieter verwerten mittlerweile IPv6-Präfix-Updates. Dabei wird das dynamisch zugeteilte, an Privatanschlüssen regelmäßig ablaufende IPv6-Präfix mit der statischen IPv6-Interface-ID des Geräts zu einem IPv6-DNS-Record (AAA) kombiniert. Meldet der Router ein neues Präfix, aktualisiert der Anbieter automatisch den dynamischen Teil aller DNS-Einträge und alle so angemeldeten Geräte bleiben erreichbar. Der DynDNS-Client der Fritzbox kann das mit wenig Konfigurationsaufwand übernehmen – wie das geht, lesen Sie im Beispiel mit dynv6.com.

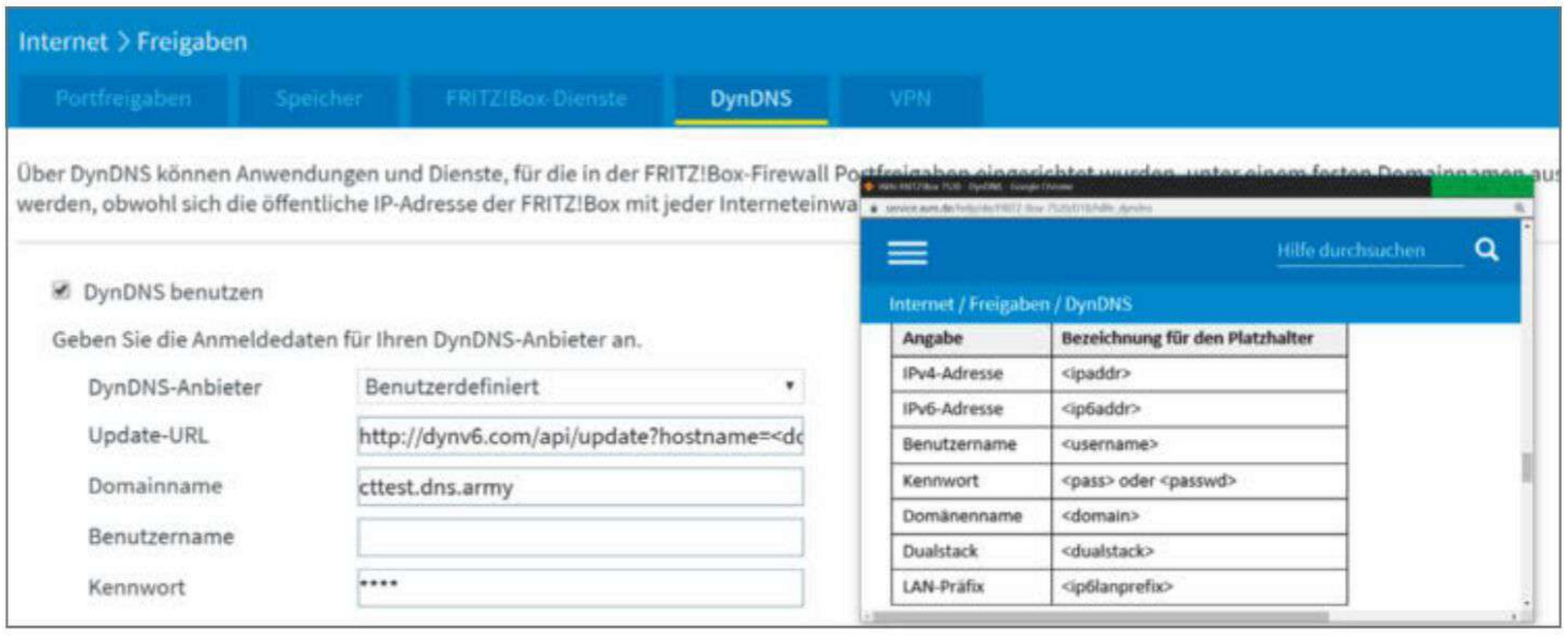
AVM bietet außerdem einen eigenen Dienst für gerätespezifische Hostnames: Über MyFritz erhalten Sie Ihre eigene Subdomain (sechzehnstellige Buchstabenkombination) von myfritz.net. Für diese können Sie Sub-Subdomains mit Hostnamen für alle Geräte in Ihrem Heimnetz erstellen, die Sie aus dem Internet erreichen wollen, beispielsweise `ipcam.abcdefghijklmnop.myfritz.net`. Die Fritzbox kümmert sich selbstständig darum, dass die DNS-Einträge immer auf die aktuelle IPv6-Adresse verweisen.

Die IPv6-Verfügbarkeit an Ihrem Anschluss ist eine Grundvoraussetzung für das beschriebene DynDNS-Verfahren. Im Fritzbox-Webinterface können Sie unter Internet/Online-Monitor prüfen, ob IPv6 genutzt wird. Wechseln Sie gegebenenfalls die Ansicht von Standard auf Erweitert (unten links im Webinterface). In Menü Zugangsdaten / IPv6 können Sie das Protokoll aktivieren, wenn noch nicht geschehen. Bekommt die Fritzbox wider Erwarten keine IPv6-Adresse, schauen Sie in der Dokumentation Ihres Anbieters nach.

MyFritz

AVMs MyFritz-Dienst steckt in jeder aktuellen Fritzbox und lässt sich mit wenigen Klicks aktivieren. Dazu trägt man lediglich eine E-Mail-Adresse ein, an die AVM zur Bestätigung eine E-Mail mit einem Link schickt. Die Registrierung stoßen Sie im Webinterface Ihrer Fritzbox an: Wechseln Sie ins Menü Internet / MyFRITZ!-Konto, tragen Sie Ihre E-Mail-Adresse ein und bestätigen Sie mit Weiter. Öffnen Sie Ihren E-Mail-Posteingang und bestätigen Sie die Aktivierungsmail von AVM. Nach einigen Minuten leuchtet der Punkt bei „Ihre FRITZ!Box ist bei MyFRITZ! angemeldet“ grün und Ihre MyFritz-Adresse steht im Feld darunter.

Erstellen Sie dann eine MyFritz-Freigabe im Menü Freigaben / Portfreigaben. Dafür müssen Sie zunächst ein neues „Gerät für Freigaben hinzufügen“.



Der DynDNS-Updater in FritzOS kann über die Option Benutzerdefiniert jedem DynDNS-Anbieter die aktuelle IP-Adresse melden, der dafür eine HTTP(S)-Schnittstelle vorhält.

Im nachfolgenden Menü wählen Sie das gewünschte Ziel aus der Liste Ihrer Netzwerkgeräte. Sollte bei der Auswahl keine IPv6 Interface-ID im Feld erscheinen, beherrscht das Gerät möglicherweise kein IPv6 oder das Protokoll ist nicht aktiviert.

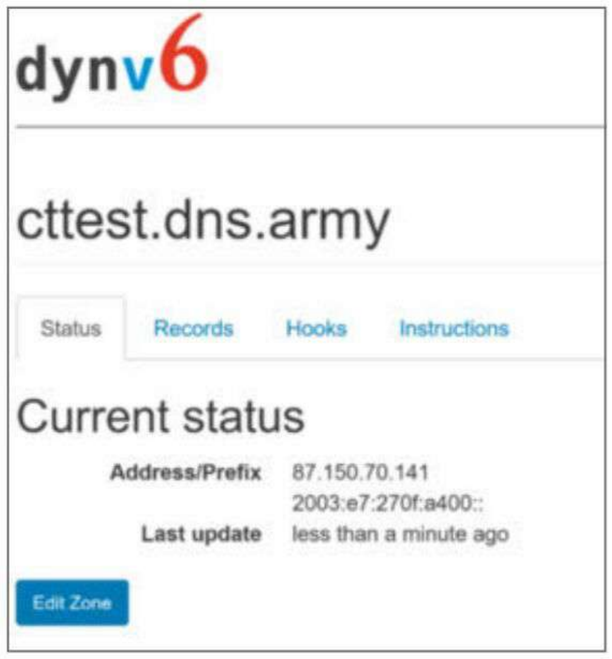
Um eine neue MyFritz-Freigabe anzulegen, klicken Sie unten rechts auf „Neue Freigabe“ und belassen die Voreinstellung auf MyFRITZ!-Freigabe. Falls Sie nur UDP zu einem bestimmten Host durchlassen wollen, müssen Sie eine kleine Hürde überwinden, denn das MyFritz-Menü lässt aus unklaren Gründen nur TCP-Freigaben zu, aber ohne eine MyFritz-Freigabe erstellt die Box keinen MyFritz-Hostnamen für das Gerät. Der Trick: Erstellen Sie zunächst eine gewöhnliche MyFritz-Freigabe für TCP (sie sollte am besten auf einen am Endgerät ungenutzten Port weisen), damit die Fritzbox den MyFritz-Namen erstellt. Anschließend fügen Sie eine Portfreigabe mit dem tatsächlich gewünschten Protokoll und Port hinzu. Die Fritzbox aktualisiert dann trotzdem den DynDNS-Hostnamen mit der IPv6-Adresse des Endgeräts und alle anderen Portfreigaben funktionieren normal. Der MyFritz-Eintrag muss jedoch verbleiben, damit die Fritzbox den Hostnamen weiter aktualisiert.

Über den MyFritz-Hostnamen lassen sich die Geräte zwar ansprechen, aber die langen kryptischen Namen kann man sich kaum merken. Ein Ausweg besteht darin, einen CNAME, also eine DNS-Weiterleitung, auf einer anderen Domain einzurichten, der auf Ihre MyFritz-Domain verweist. Besitzen Sie bereits eine Domain wie `example.com`, die Sie selbst verwalten können, legen Sie dort eine Subdomain wie `ipcam.example.com` an, die auf den MyFritz-Hostnamen verweist.

dynv6.com

Leicht merkbare Subdomains bekommt man bei DynDNS-Anbietern wie dynv6.com. Dort erhalten Sie einen frei wählbaren DynDNS-Namen mit der Endung dynv6.net, dns.army oder v6.rocks. Statt für jedes Gerät die komplette IPv6-Adresse einzeln zu übermitteln, müssen Sie dem Dienst nur einmalig die Interface Identifier Ihrer Hosts melden (IID) und fortan das aktuelle Präfix Ihres Netzwerks. Der Dienst setzt dann die IIDs und das Präfix automatisch zusammen und veröffentlicht die Einträge im weltweiten Domain Name System.

Die Aktivierung ist kaum anspruchsvoller als die von MyFritz: Um sich zu registrieren, öffnen Sie `https://dynv6.com`, klicken oben rechts auf „Sign Up“, tragen Ihre E-Mail-Adresse sowie das gewünschte Passwort ein und bestätigen die Angaben. Anschließend können Sie eine neue Zone, also eine Subdomain anlegen – beispielsweise meinrouter.dynv6.net. Ist der Hostname noch frei, erscheint ein grüner Haken.



Die einfach gehaltene Statusoberfläche des Dynv6-Dienstes lässt erkennen, wann das IPv6-Präfix aktualisiert wurde.

Dynv6 beschreibt die richtigen Einstellungen für den DynDNS-Client von FritzOS in der Dokumentation: In der Statusübersicht Ihrer neuen Subdomain wechseln Sie zum Reiter Instructions und scrollen nach unten zum Absatz „Fritz!OS (German)“. Im Webinterface Ihrer Fritzbox wechseln Sie zu Internet / Freigaben / DynDNS. Setzen Sie den Haken bei „DynDNS benutzen“ und wählen Sie Benutzerdefiniert aus dem Ausklappmenü. Übernehmen Sie die Werte vom Instructions-Reiter auf dynv6.com in das Fritzbox-Interface – das Token ist bereits korrekt gesetzt – und bestätigen Sie mit Übernehmen.



Mit Hilfe von DynDNS-Präfix-Updates muss nur noch die statische IPv6-Interface-ID im Dienst hinterlegt werden. Übermittelt die Fritzbox ein neues Präfix, aktualisiert der Dienst alle zugehörigen Einträge automatisch.

Wechseln Sie im Fritzbox-Webinterface zu Portfreigaben und legen Sie für das Gerät, das Sie aus dem Internet erreichen wollen, die passende Portfreigabe an. Achten Sie darauf, dass die Option „Internetzugriff über IPv6“ aktiviert ist. In der Freigabeübersicht finden Sie danach einen Eintrag für das freigegebene Gerät; er führt die IPv4-Adresse und darunter die IPv6-Interface-ID auf. Kopieren Sie letztere und wechseln Sie bei dynv6 zum Reiter Records. Klicken Sie auf „+Add Record...“ und wählen Sie den IPv6-DNS-Record AAAA. Der Eintrag Name wird später Ihre Sub-Subdomain, bei Data tragen Sie die zuvor kopierte IPv6-Interface-ID ein und bestätigen mit Save. Anschließend zeigt die Seite die automatisch zusammengesetzte IPv6-Adresse des freigegebenen Geräts an.

Probieren Sie den neuen DynDNS-Hostnamen aus, indem Sie ihn anpingen. Das können Sie auf nahezu jedem Betriebssystem in einem Terminal erledigen, auf Linux und macOS: `ping6 ipcam.example.dynv6.net`. Auf Windows: `ping -6 ipcam.example.dynv6.net`. Innerhalb Ihres IPv6-Subnetzes sollte das Gerät auf den Ping antworten. Soll das Gerät auch auf Pings aus dem Internet antworten, müssen Sie in der Portfreigabe die Option „PING6 freigeben“ anhaken.

Andere DynDNS-Anbieter

AVM hat den DynDNS-Updater in FritzOS mittlerweile gut dokumentiert und über die Option Benutzerdefiniert kann die Fritzbox jedem DynDNS-Anbieter mit HTTP(S)-Schnittstelle die benötigten Parameter automatisch übermitteln. Das Fragezeichen oben rechts in den DynDNS-Einstellungen öffnet AVMs Dokumentation für den Dienst.

Viele DynDNS-Anbieter veröffentlichen ihre „DynamicDNS APIs“ auf ihren Webseiten oder in einem separaten Wiki. Mit etwas Recherche können Sie so auch den DynDNS-Anbieter Ihrer Wahl in die Fritzbox eintragen. Der neue DynDNS-Anbieter deSEC liefert beispielsweise DNS-Einträge signiert aus (DNSSEC), sodass diese besser vor Manipulation geschützt sind. (amo) ct

Literatur

[1] Johannes Weber und Carsten Strotmann, **Bekannt verzogen**, Serverbetrieb mit dynamischen IPv6-Adressen, c't 19/2018, S. 156

[2] Jan Mahn, **Unerwartete Dynamik**, Dynamisches DNS kostenlos mit eigener Domain, c't 14/2017, S. 160

Weitere Tipps & Lesestoff

ct.de/w3cj

secIT by Heise SPECIAL

Jetzt Kombi-Rabatt sichern und über 30% sparen!

Die Online-Konferenzen zur secIT by Heise

IT-Security im Fokus

Vertiefen Sie in einer spannenden Keynote sowie in 3 interaktiven Vorträgen Ihr Wissen rund um IT-Security. Jedes secIT Special präsentiert Ihnen ein exklusives Thema.

IR, SOC und SIEM
Als Aufzeichnung erhältlich

16. September 2021
Cybersicherheit für KMU

9. Dezember 2021
Hacking for Security

JETZT ANMELDEN: konferenzen.heise.de/secit-special

Glasfaser-Router

AVMs Fritzbox 5530 stellt den Internetzugang über Glasfaser-Anschlüsse bis 1 GBit/s her und verteilt ihn intern über schnelles Ethernet und modernes WLAN. Bei der Datenrate hat sie sogar noch Luft nach oben.



Von **Ernst Ahlers**

Das Besondere an der Fritzbox 5530 ist ihr Slot für Glasfaser-Module: Der nimmt nicht nur SFP-Module für 1 GBit/s auf, sondern auch schnellere Varianten (SFP+ bis 10 GBit/s), falls die Internetprovider künftig mehr als 1000 MBit/s anbieten. Die kämen dann über den Multi-Gigabit-Ethernet-Port (LAN1, bis 2,5 GBit/s) auch im eigenen Netz an.

Dem Gerät liegen zwei SFP-Module für die heute üblichen Glasfaser-Anschlussvarianten AON und GPON bei (Active Optical Network, Punkt-zu-Punkt sowie Gigabit Passive Optical Network, Punkt-zu-Multipunkt). Voraussetzung für den Einsatz ist, dass der Provider kein „Glasfaser-Modem“ als nicht entfernbaren Leitungsabschluss installiert, sondern man direkt an die Glasfaser-Buchse kommt.

Das Einrichten des Routers geht wie bei AVM gewohnt leicht per Browser, doch muss man gegebenenfalls das moderne IPv6-Protokoll, die verbesserte WLAN-Verschlüsselung WPA2+3 (Mixed-Mode) und auf Wunsch das Gast-WLAN von Hand aktivieren. USB-Ports und einen ISDN-S0-Bus für die hausinterne Telefonie gibt es nicht, aber alle übrigen, von größeren Fritzboxen und FritzOS 7.2x gewohnten Anschlüsse und Funktionen sind vorhanden.

Performance

Leider akzeptierte die Fritzbox nur die beiliegenden Glasfaser-Module und keines unserer schnelleren Modelle. So konnten wir die Geschwindigkeit des Datenumschlags zwischen Internet und LAN (NAT-Performance, siehe Tabelle) nur mit Gigabit-Ethernet (1000 MBit/s) zwischen den LAN-Ports 1 und 2 messen. Gigabit-Glasfaseranschlüsse wird man mit der Box jedenfalls ausschöpfen können.

Das WLAN der 5530 scheint noch etwas Feintuning zu benötigen: Mit unserem Testnotebook (Asus Vivobook 14 mit Intel-AX200-Modul und Windows-Treiber 22.30) lief der Downstream (Router zu Client) zwar sehr flott (bis zu 917 MBit/s auf 5 GHz), der Upstream aber viel langsamer (max. 113 MBit/s). Im Mittel ergaben sich dennoch je nach Band gute bis sehr gute Werte. AVM optimiert nach eigenen Worten die Firmware weiter.

Fazit

Internet per Glasfaser ist zwar vielerorts noch Zukunftsmusik, doch wo vorhanden, kann man mit der Fritzbox 5530 die Router-Freiheit nutzen und einen vom Provider gestellten Simpel-Router ersetzen. Genügt für die mobilen Clients das 2-Stream-WLAN, dann können AVM-Fans zugreifen. Mit der Option auf XGS-PON ist die 5530 obendrein für künftige Anschlüsse der Multi-Gigabit-Klasse gerüstet. (ea) c't

AVM Fritz!Box 5530

WLAN-Router für Glasfaseranschlüsse	
Hersteller	AVM, www.avm.de
WLAN	2 × Wi-Fi 6 (2) = IEEE 802.11ax-574 + ax-2400, simultan dualband, WPA3, WPS, DFS
Bedienelemente	WLAN, Fon/DECT, Connect/WPS, 5 Statusleuchten
Anschlüsse	SFP/SFP+, 3 × RJ45 (1 bis 2,5 GBit/s, 2 bis 1 GBit/s), RJ11/TAE (Analog-Telefon)
getestete Firmware	7.24-86294 beta
NAT-Perf. PPPoE (DS / US)	921 / 903 MBit/s
IP-zu-IP (DS / US)	949 / 949 MBit/s
WLAN 2,4 GHz nah / 20 m[1]	288 / 61–165 MBit/s
5 GHz nah / 20 m[1]	515 / 84–179 MBit/s
Leistungsaufnahme[2]	8,8 W / 19,4 VA
jährliche Stromkosten[2]	23 €
Preis	169 €

[1] gegen Intel AX200 [2] mit GPON-Modul, idle, bei Dauerbetrieb, 30 Cent/kWh, gerundet

Fritzchens Erleuchtung

Mit der LED-Lampe Fritz!DECT 500 und dem Vierfach-Taster Fritz!DECT 440 nimmt das Smart-Home-System von AVM Konturen an. Doch die Steuerung überzeugt nicht vollständig.



Von **Berti Kolbow-Lehradt**

Fritzboxen mit eingebauter DECT-Basis können neben dem Internet auch Schaltsignale im Smart Home verteilen. Bisher bot AVM nur eine kleine Auswahl an smartem DECT-Zubehör, holt nun aber zum großen Aufschlag aus: smarte Beleuchtung.

Die LED-Lampe Fritz!DECT 500 für den E27-Sockel emittiert weißes und farbiges RGB-Licht mit einer Farbtemperatur von 2700 bis 6500 Kelvin. Mit 806 Lumen bietet die 9-Watt-Birne eine gute Standardhelligkeit, ersetzt allerdings keine klassische 100-Watt-Glühlampe über dem Esstisch. Dimmen lässt sie sich per App, über den ebenfalls neuen Vierfachtaster Fritz!DECT 440 oder eine andere Schalthilfe, die das HAN-FAN-Protokoll des DECT-ULE-Standards (Ultra Low Energy) versteht.

Im Vergleich zum Vorgängermodell mit nur einem Taster bietet der neue Schalter Fritz!DECT 440 nun vier Funktionstasten und eine zusätzliche Menütaste. Damit lassen sich außer der LED-Lampe die beiden Zwischenstecker und der Heizkörperthermostat des Herstellers einzeln oder in Gruppen schalten. Ein E-Paper-Display zeigt die Schaltzustände oder die Raumtemperatur an, die über einen im Taster integrierten Sensor ermittelt wird. Zwei AAA-Batterien liefern Energie, eine Magnethalterung für die Wandhaftung. Die Hardware-Installation geht bei beiden Neuzugängen schnell. Lampe in die Fassung schrauben, Menüknopf auf dem Vierfach-Taster drücken, DECT-Taste auf der Fritzbox halten, schon finden sich die Komponenten automatisch.

Vollständig konfigurieren lässt sich das Zubehör in der Web-Oberfläche der Fritzbox. Für das Tastenquartett legt man dort bis zu drei Funktionen fest, die sich per Menütaste durchschalten lassen. Anzeigeoptionen für den Bildschirm komplettieren das Setup. Für die LED-Lampe lassen sich Schaltroutinen nach Uhrzeit, Tag, Woche, Countdown, Sonnenauf- und -untergang sowie Google-Kalender planen. Manuell kann man sie an- und ausschalten, dimmen, sowie in der geringen Auswahl von zwölf Vollfarben mit drei Sättigungsstufen und neun Weißtönen einstellen.

In der neuen Fritz!App Smart Home ist die Lampe ebenfalls manuell bedienbar, aber die Schaltpläne fehlen. Der Vierfachtaster ist dort zum Testzeitpunkt ein funktionsloser Zombie. Die weiter erhältliche MyFritz!App unterstützt das Duo gar nicht. In einem Fritz!Fon-Mobilteil kann man das Licht an- und ausschalten sowie die vom Taster gemessene Temperatur einsehen.

Wer gern alles per Smartphone konfiguriert, ist bei AVMs Smart-Home-System weiterhin an der falschen Adresse. Der vielseitige Taster ist der interessantere Neuzugang, während die Lampe wegen der kleinen Farbpalette Fans komplexer Lichtstimmungen eher enttäuschen dürfte. Weil außerdem pro Fritzbox nur maximal zehn Leuchtmittel angelernt werden können, lässt sich mit AVMs Leuchtmitteln das Lichtkonzept selbst kleinerer Wohnungen bestenfalls ergänzen. Insgesamt fügt sich das Zubehör gut in das Ökosystem von AVM ein und wertet dessen WLAN-Router als Schaltzentrale für das Smart Home auf. (sha) c't

AVM Fritz!DECT 440 / Fritz!DECT 500

Vierfach-Taster / LED-Lampe	
Hersteller	AVM, www.avm.de
Systemvoraussetzung	Fritzbox ab OS 7.2
Funk	DECT-ULE
Preis	je 40 €

Verschlüsselt per VoIP telefonieren

Zum Schutz der Privatsphäre schaltet man in Fritzboxen die Telefonieverschlüsselung mit nur fünf Mausklicks ein – das klingt komfortabel und tatsächlich schnitt die Box in unseren Praxistests ordentlich ab. Eingehende Laboranalysen deckten aber auch unerwartete Schwächen auf.

Von **Alexander Traud**



Verschlüsselt telefonieren, Grenzen kennen	118
Im Homeoffice komfortabel telefonieren	124
Fritzbox für Homeoffice-Telefonie	130
Unify-VoIP-Telefone an der Fritzbox	134
DECT-VoIP-Telefone bis 100 Euro	140
Telefon klingeln lassen mit Fritzconnection	146
Mobilfunk-Gateway	148

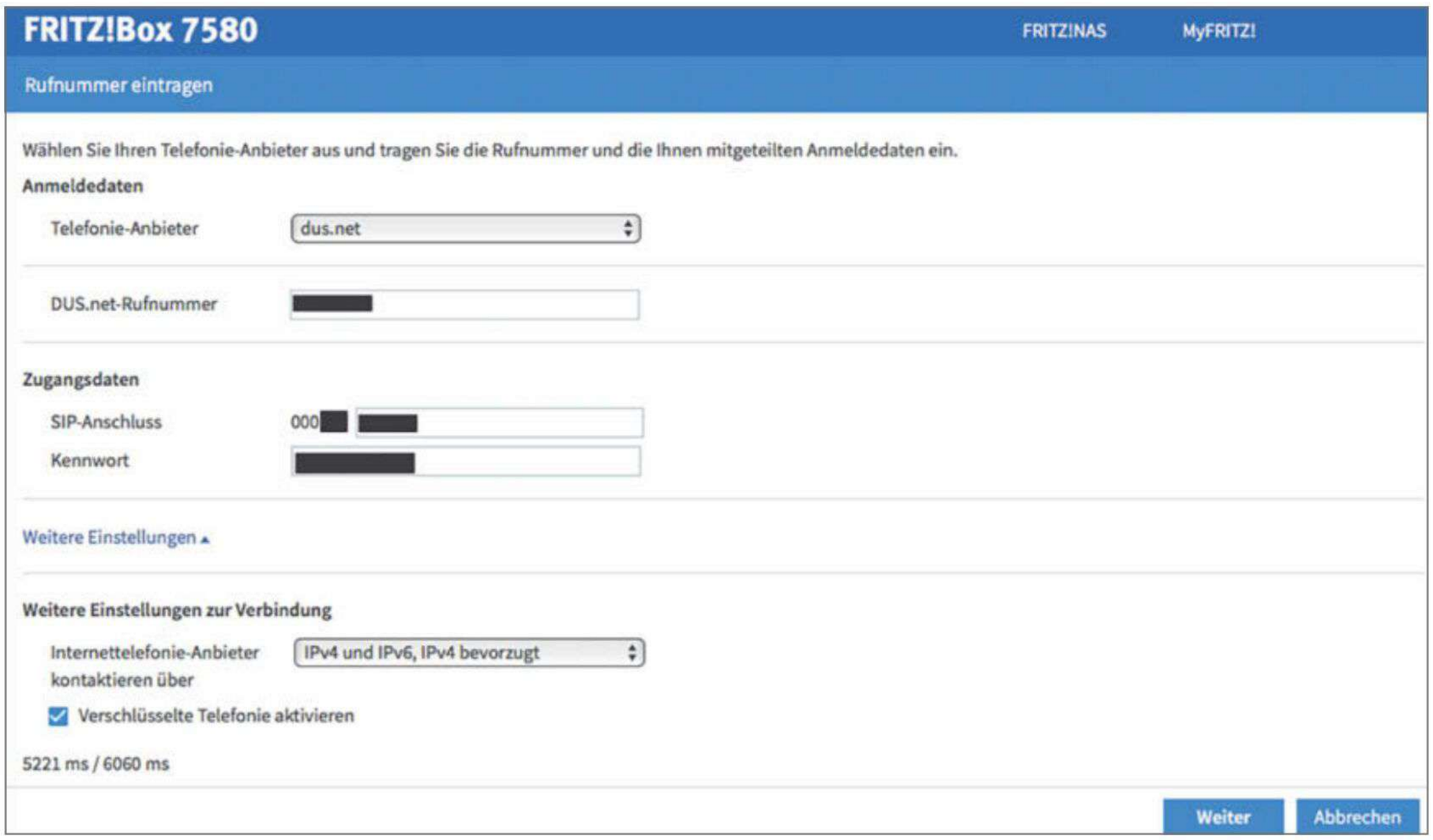
Die Verschlüsselung für die VoIP-Telefonie brachte AVM erstmals mit dem FritzOS 7.20 auf aktuelle Fritzboxen. Seither sind einige Verbesserungen eingeflossen, aber im Wesentlichen funktioniert sie wie eingeführt. Ursprünglich für die Deutsche Telekom und ihren Dienst „Deutschland-LAN SIP-Trunk“ ausgelegt, funktioniert die Methode auch mit VoIP-Konten anderer Anbieter, etwa dus.net und easybell.

Das ist ein wichtiger Schritt, denn Voice-over-IP-Telefonate laufen größtenteils unverschlüsselt ab. Selbst Hacker-Praktikanten kennen Tricks, solche Datenströme unerkannt aufzuzeichnen und dann etwa im Protokollanalysator Wireshark abzuhören. Erste Gegenmaßnahmen in Form von Verschlüsselungen gibt es seit fast 20 Jahren. Dazu gehört die Methode SDES-sRTP (siehe Glossar), die Anfang der 2000er-Jahre in erste Geräte implementiert wurde. Auf Tischtelefone, Soft-Clients, Clouds und Router und so auch auf Fritzboxen zog sie erst in jüngster Zeit ein.

Oft verhindert fehlende Benutzerfreundlichkeit die Nutzung von Verschlüsselungstechniken. Nicht so bei SDES-sRTP: Es bringt gute Voraussetzungen für stillschweigende, also nutzerfreundliche Verschlüsselung mit, weil es alle Parameter automatisch aushandeln kann. Schon 2006 führte Nokia vor, wie das geht: Nokia-Handys forderten nur dann Aufmerksamkeit vom Nutzer, wenn die Verschlüsselung scheiterte und zeigten dann zur Warnung ein offenes Vorhängeschloss.

SDES-sRTP ist eine Transportverschlüsselung für die Strecke vom Teilnehmer bis zum Server des Providers. Das klingt nach weniger, als es ist: Denn Kunden desselben Providers sind damit ebenso abgesichert wie Außendienstler bei hausinternen Telefonaten oder entfernte Niederlassungen von Firmen – zumal „hausinterne“ Gespräche auch Landesgrenzen überspannen können. Nützlich ist die Technik auch, weil in Mehrparteienhäusern die Telefonleitungen blank am gemeinsamem Hausverteiler zusammenlaufen, wo der Verkehr aufgezeichnet werden kann. Und gelegentlich versorgt ein einziger Hausverteiler sogar die Telefonanschlüsse mehrerer Reihenhäuser. Aktiviert man SDES-sRTP, kann also niemand mehr mithören, bloß weil er Know-how und Zugang zum Hausverteiler hat. Schließlich kann man damit seinen SIP-Account prinzipiell auch nomadisch in ungesicherten WLAN-Hotspots nutzen, ohne ein VPN aufzusetzen.

In Fritzboxen muss man die Funktion eigens aktivieren. Dafür ist ein VoIP-Konto bei der Telekom, bei dus.net oder easybell erforderlich: Wenn Sie eines eingerichtet haben, öffnen Sie im Menü „Tele-



Ab FritzOS 7.20 aktiviert man die Telefonieverschlüsselung in Fritzboxen mit nur fünf Klicks.

fonie/Eigene Rufnummern“ eine geeignete Rufnummernkonfiguration und darin den Bereich „Weitere Einstellungen“. Setzen Sie bei der Option „verschlüsselte Telefonie“ das Häkchen – fertig. Jedes Telefon, das zur betreffenden Rufnummer konfiguriert ist, kann nun verschlüsselte Verbindungen nutzen. So haben wir problemlos diverse Telefonate mit unterschiedlichen Geräten netzintern und auch überkreuz zwischen allen drei Anbietern geführt. So weit, so schön.

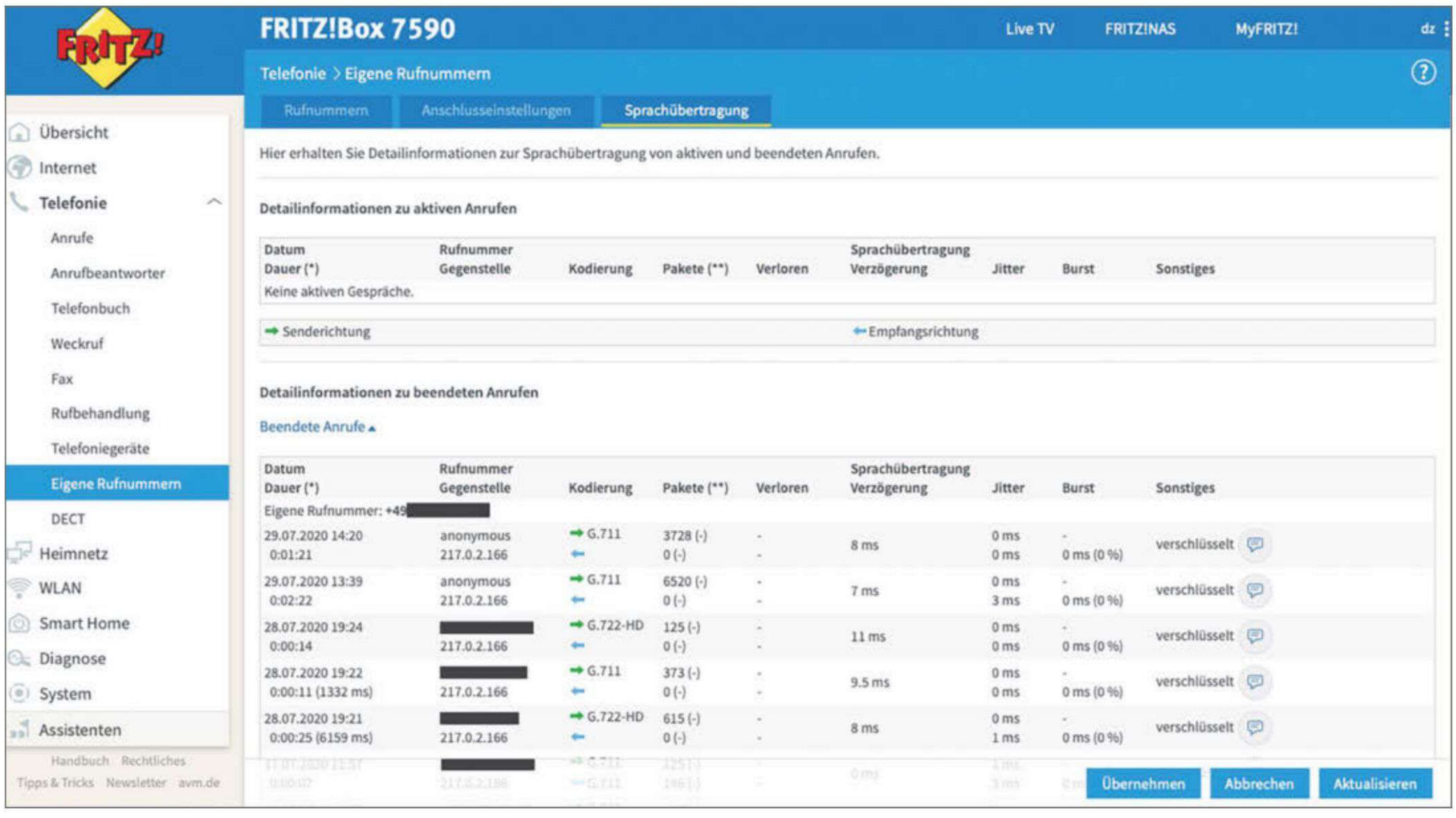
Doch SDES-sRTP ist komplex und die Hersteller implementieren die Technik unterschiedlich. Daher können Verbindungen scheitern oder unverschlüsselt laufen und deshalb möchte man für jeden Anruf wissen, ob er verschlüsselt ist. Doch die Fritzbox zeigt das nicht direkt, auch nicht das hauseigene FritzFon C5 (Firmware 4.57). Ein bisschen verrät die Fritzbox im Menü „Telefonie / Eigene Rufnummern / Sprachübertragung“. Dort blendet sie „verschlüsselt“ ein, wenn sie eine SDES-sRTP-Übertragung ausgehandelt hat.

Jedoch verbirgt sie einen Teil der Optionen. Diese zu verstehen ist nicht weiter schwer, aber die Zusammenhänge sind teils vertrackt, sodass wir einige Grundlagen voranstellen.

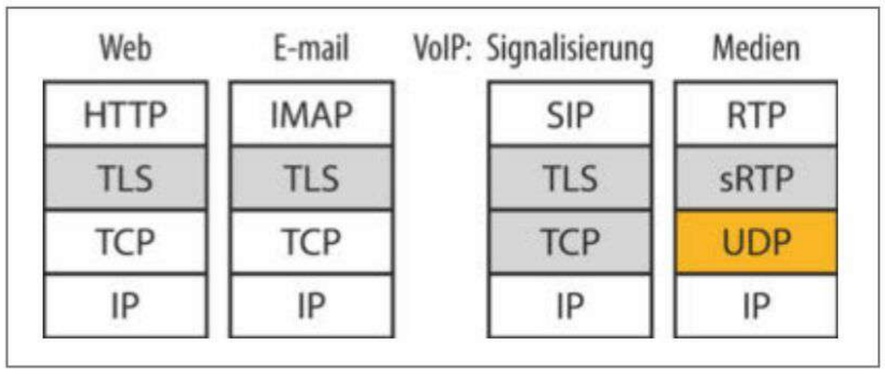
Ohne TLS am Start

Wer im Internet surft oder Mails abruft, nutzt dabei häufig die Verschlüsselung TLS (siehe Glossar). Dabei tauschen der lokale Client und die Gegenstelle Schlüssel aus, bevor Nutzdaten fließen. Die Gegenstelle weist sich mittels eines Zertifikats gegenüber dem Client aus. Diese Merkmale sind auch für die VoIP-Verschlüsselung nützlich. Dennoch wurde VoIP zunächst ohne TLS spezifiziert.

Das liegt daran, dass TLS auf dem Transmission Control Protocol (TCP) aufsetzt und bei TCP der Emp-



Fritzboxen mit aktuellem FritzOS erfassen im Journal, ob sie mit Gegenstellen die Verschlüsselung ausgehandelt haben – auch für laufende Gespräche.



Anders als etwa beim Surfen sind bei der VoIP-Telefonie pro Sitzung zwei Verbindungen aufgebaut: eine für die Signalisierung und eine für die Nutzdatenübertragung.

fänger eingehende TCP-Pakete quittiert, damit der Sender Übertragungsfehler erkennt und per Sendewiederholung ausbügelt. Für VoIP sind Wiederholungen aber nutzlos, denn sie kämen beim Empfänger erst an, wenn ihr Wiedergabezeitpunkt schon verstrichen ist.

So setzt VoIP auf das schlanke User Datagram Protocol auf (UDP), das ohne Wiederholung arbeitet. Da die Sprachpakete nur 20 Millisekunden kurz sind, nimmt der Gesprächspartner einzelne Paketverluste nicht wahr. Unterm Strich blieb: ohne TCP keine TLS-Verschlüsselung. Zu Beginn der VoIP-Ära konnte man nur auf VPN-Vernetzung zurückgreifen, um so zumindest zwischen Niederlassungen geschützt zu telefonieren.

Die übliche, also unverschlüsselte VoIP-Telefonie verzahnt drei Protokolle miteinander: Die Gegenstellen melden sich über das Session Initiation Protocol (SIP) beim Anbieter an, bauen Verbindungen auf und ab et cetera. Über das Session Description Protocol (SDP) handeln sie die genutzten Medien aus (Audio, Video, Text). Und sie einigen sich auf eine UDP-Verbindung für das Real-Time Transport Protocol (RTP) zur Sprachübertragung. Daher existieren während eines Telefonats mindestens zwei Verbindungen: eine für die Signalisierung, eine für Sprachpakete.

Verschlüsselung als Nachschlag

Per SDP lassen sich auch verschlüsselte Übertragungen aushandeln. Damit tauschen die Geräte symmetrische Schlüssel untereinander aus. So wird RTP zum „secure RTP“ (sRTP). Damit die Schlüssel vertraulich bleiben, kommuniziert SDP selbst verschlüsselt. Zumindest dafür und für SIP konnten die Protokolldesigner auf TLS zurückgreifen: Somit war SIP-over-TLS mit SDES-sRTP geboren.

In diesem Zusammenhang ist mit „Gegenstelle“ nicht nur das Telefon des Gesprächspartners gemeint, es kann auch der Server eines Anbieters wie der Telekom sein. So sind netzübergreifende Gespräche möglich, auch ins analoge Festnetz. Damit der Anbieter den Datenstrom zur angerufenen Seite weiterleiten kann, entschlüsselt er ihn. Auch das belegt: SDES-sRTP ist keine Ende-zu-Ende-Verschlüsselung, sondern eine Transportverschlüsselung.

Nun zurück zu FritzOS und dem zweiten Konfigurationsweg für die Verschlüsselung: Öffnen Sie das Webinterface, klicken Sie auf „Telefonie/Eigene Rufnummern“ und dann auf einen der Einträge – dabei muss es sich um Telekom-, dus.net oder easybell-Nummern handeln. Stellen Sie das Menü „Telefonie-Anbieter“ auf „Anderer Anbieter“ um.

Jetzt erscheinen die Einstellungen im Detail und sind änderbar – sichern Sie zuvor die aktuelle Konfiguration, damit Sie sie im Fehlerfall wieder einspielen können. Anderungen bieten sich zum Beispiel an, wenn Sie dus.net etwa an einem Kabelanschluss mit DS-Lite-Konfiguration nicht über IPv4, sondern IPv6 erreichen möchten. Dazu tragen Sie zum Beispiel für eine dus.net-Rufnummer im Feld Registrar securev6.dus.net ein.

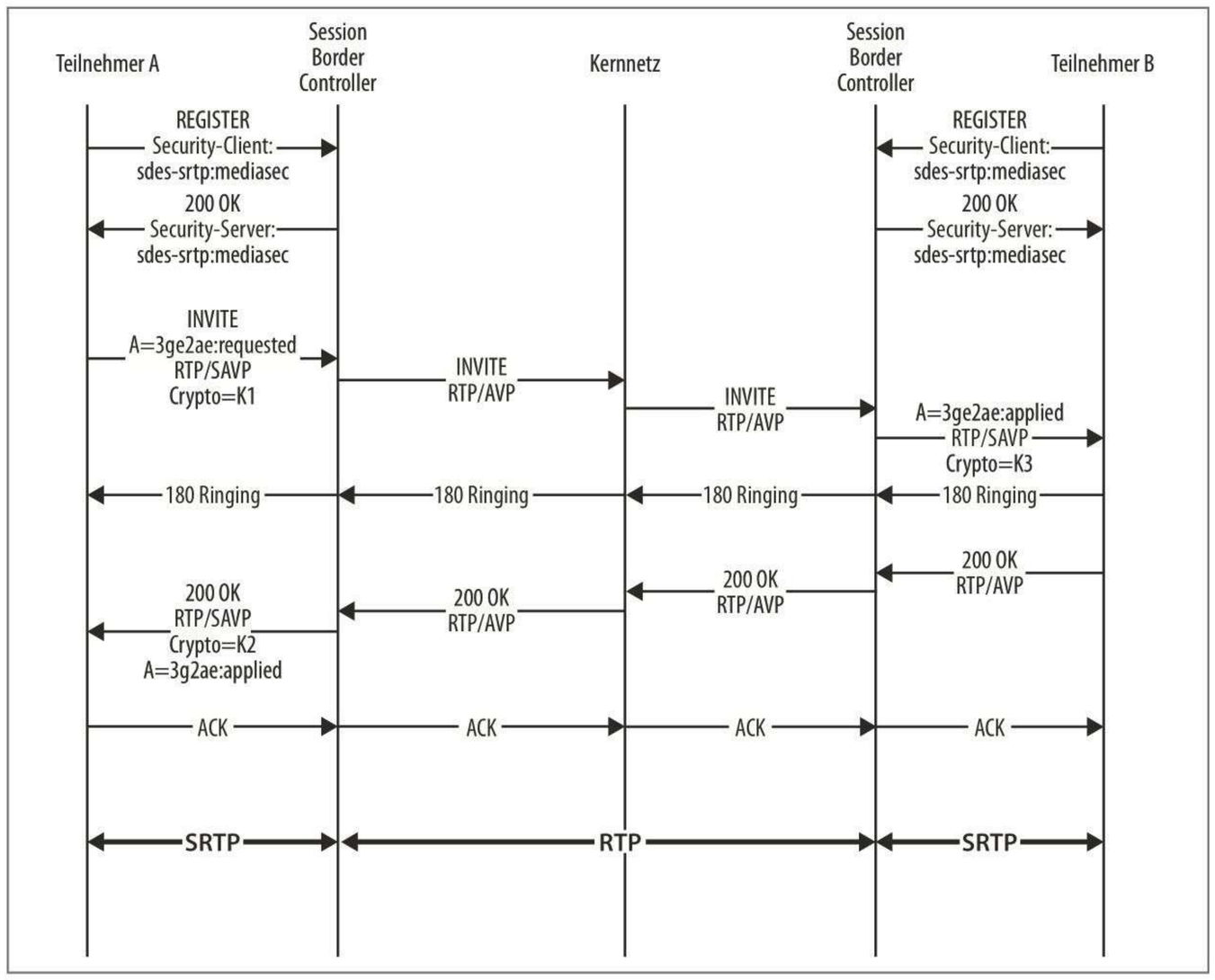
Menü zum Ansehen

Die verschlüsselte Telefonie wird mittels drei Optionen eingeschaltet. Im Menü Transportprotokoll muss TLS aktiviert sein und die Option „Anbieter unterstützt verschlüsselte Telefonie“ muss angehakt sein. Die dritte Option folgt im Menü „Media Protocol“.

Hier sind drei Einträge zu finden: RTP/AVP, „RTP/SAVP und RTP/AVP“ sowie RTP/SAVP (siehe RFC 8643). Was genau gewählt ist, hängt vom Anbieter ab und sollte nur nach Absprache mit ihm geändert werden. Wir beschreiben dieses Menü dennoch, weil manches Fritzbox-Verhalten besser verständlich wird.

Mit der Einstellung RTP/AVP wird ein Gespräch wie üblich aufgebaut, nur wird via SDP zusätzlich ein Schlüssel übertragen. Wenn die Gegenstelle SDES-sRTP beherrscht, greift sie sich diesen, sendet ihren eigenen zurück und fortan wird chiffriert telefoniert. Wenn sie sich nicht für SDES-sRTP eignet, soll sie den Schlüssel ignorieren. So wird SDES-sRTP also optional verwendet.

Aber dabei lauern Stolperfallen: Nimmt die Gegenstelle den Schlüssel an, kann sie statt mit RTP/AVP alternativ mit RTP/sAVP antworten. Die Spezifikation toleriert diesen Fall stillschweigend. Der Entwickler muss also selbst darauf kommen, diesen Ablauf korrekt zu behandeln. Fritzboxen tun das nicht, sondern legen einfach auf. Das passiert reproduzierbar mit Gegenstellen wie Digium Asterisk und Sangoma FreePBX mit dem Channel-Driver chan_sip.



Mit der Methode SDES-sRTP lässt sich die Transportschicht vom Teilnehmergerät zum Server des VoIP-Anbieters verschlüsseln.

Die Einstellung „RTP/SAVP und RTP/AVP“ soll dieses Problem lösen. Dabei wird ein Gespräch mit einem verschlüsselten und einem unverschlüsselten Medienstrom angeboten, damit die Gegenstelle den bevorzugten selbst wählt. Auch damit wird SDES-sRTP also nur optional ausgehandelt. Diese Variante setzt AVM beim dus.net-Profil ein.

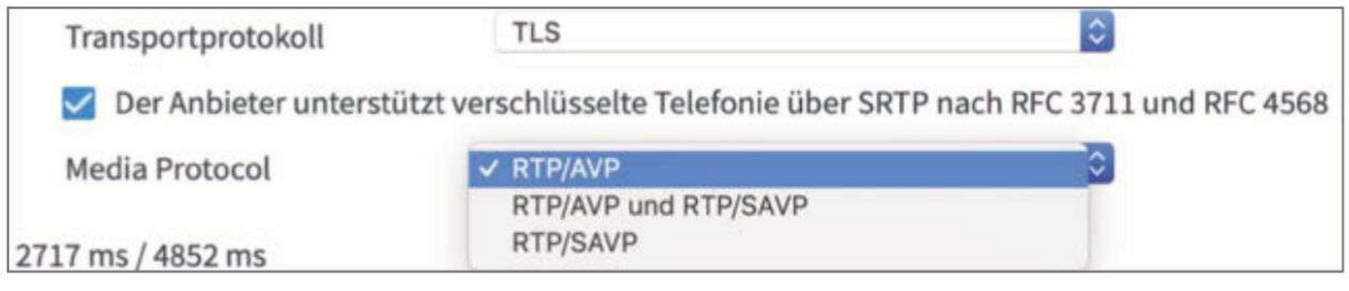
Erst mit der Einstellung RTP/sAVP erzwingt man SDES-sRTP. Das nutzt die Fritzbox für easybell- und Telekom-Profile. Wenn die Gegenstelle die Option ablehnt und den SIP-Fehler 488 sendet, scheitert der Verbindungsaufbau. Ein FritzFon meldet dann „Ziel nicht kompatibel“ und die Fritzbox notiert im Journal „Internettelefonie war nicht erfolgreich. Ursache: 488“.

Zwischenfazit: Positiv fällt auf, dass das FritzOS ab Version 7.2x drei Optionen offeriert. Die Digitalisierungsboxen von Bintec-elmeg (Standard, Smart, Premium) sowie Zyxel (Basic) bieten nur RTP/sAVP.

Der RFC 8643 diskutiert als Gedankenspiel noch eine weitere Option, verwirft sie aber, weil diese Variante zur Folge haben kann, dass der Status 488 nicht bei der anrufenden Seite ankommt (Option „RTP/SAVP, SIP-Status 488, RTP/AVP“). Bei Fritzboxen und anderen Routern ist sie konsequenterweise nicht eingebaut, nur Lancom hat sie dennoch implementiert.

Die Telekom fordert für chiffrierte Telefonie zusätzlich das Erfüllen der MediaSec-Spezifikation. Die Telekom weiß so, dass das Endgerät mit Verschlüsselung umgehen kann, auch bei ankommenden Telefonaten. AVM hat das eingebaut, ebenso die Routerhersteller Bintec-Elmeg, Lancom und Zyxel sowie die Tischtelefon-Hersteller Cisco Sipura (ab Multiplatform-Firmware 11.3) und Snom (ab Firmware 10.1).

Weitere Stolpersteine lauern bei der Aushandlung der Chiffre, denn AES-128 ist verpflichtend und AES-256 optional. Doch an der korrekten Behandlung nicht berücksichtigter Chiffren hapert es bei manchen Gegenstellen. Falls eine Gegenstelle damit



Fritzboxen können zur Aushandlung der Verschlüsselung eines von drei Verfahren verwenden. Manche andere Router nutzen nur eines.

nicht klarkommt, ist es also wünschenswert, AES-256 abschalten zu können. Bei Cisco Sipura ist diese Chiffre standardmäßig ausgeschaltet, bei Lancom abschaltbar, bei AVM jedoch nicht.

Was Fritz schon kann

Für die obigen Ergebnisse haben wir die Fritzbox in einem Testaufbau genauer unter die Lupe genommen: Um die Signalisierung mitlesen zu können, haben wir als VoIP-Server Asterisk 13 LTS mit dem Channel-Driver chan_sip aufgesetzt und diesen in der Fritzbox über das Menü „Anderer Anbieter“ konfiguriert. Asterisk war dabei auf TLS 1.2 mit der Chiffre AES-GCM fixiert und der Verschlüsselungsschutz Perfect Forward Secrecy deaktiviert. So lassen sich sowohl an der Fritzbox als auch am Asterisk-Server Daten mitschneiden und in Wireshark analysieren.

Dabei kam unter anderem heraus: AVM nutzt mit dem getesteten FritzOS 7.20 intern die Bibliothek OpenSSL 1.1.1 und damit auch das moderne TLS 1.3. Auch NIST-freie Kryptografie mittels Curve25519 und sogar Curve448 sind eingebaut. Das ist vorbildlich. Zwar nutzt Lancom ebenfalls OpenSSL 1.1.1. Aber das aktuelle LCOS 10.42.116 bietet weder TLS 1.3 noch Curve448.

Zusätzlich haben wir die Fritzbox mit VoIP-Clients wie Linphone getestet. Damit kann man Peer-to-Peer-Telefonate mit Internet-Gegenstellen führen (z. B. von Linphone zu iptel.org). Verbindungen zu traditionellen Telefonnetzen bekommt man allenfalls mit kostenpflichtigen Tarifen. Mit FritzOS 7.20 klappte im Test die unverschlüsselte Kommunikation mit linphone.org/freesip, iptel.org, voip.opensips.org und sip2sip.info reibungslos. Gespräche mit SIP-over-TLS kamen nur mit antisip.com/service zustande.

Was Fritz noch lernen sollte

Telefonie-Router bieten nicht nur Adapter für analoge und ISDN-basierte Telefone. An manchen lassen sich auch SIP-Telefone anmelden. AVM bietet seinen Registrar nur über UDP und TCP an, bisher aber nicht über TLS (Bintec-Elmeg und Lancom tun das). Wer sich aus der Ferne mit einem SIP-Soft-Client in seine Fritzbox einbucht, braucht also weiterhin VPN als Transportmedium, um unerwünschte Mithörer fernzuhalten.

Noch aus den VoIP-Anfangszeiten bringt eine Fritzbox die Funktion zum direkten Anruf einer SIP-Gegenstelle mit, also am üblichen Anbieter vorbei. Für diese „Anwahl von Internetrufnummern“ (SIP-URI-Dialing) legt man im Fritz-Telefonbuch Einträge im E-Mail-Adressformat an (z. B. 500@hd-telefonie.avm.de). Doch weil die automatische Transporterkennung für TLS fehlt (DNS-NAPTR), kann die Fritzbox beim SIP-URI-Dialing nicht verschlüsseln.

Ab OpenSSL 1.1 könnten User je nach Sicherheitseigenschaften ihres Geräts prinzipiell eine durchgehende Mindestverschlüsselung in Stufen von 1 bis 5 festlegen. Das fehlt bei den meisten Produkten, auch in FritzOS 7.20. Dabei eignet sich FritzOS 7.20 sogar für die Stufe 4. Stattdessen schließt AVM lediglich TLS 1.0 aus und fordert mindestens TLS 1.1. Für die Authentifizierung setzt TLS Zertifikate voraus. Aber in FritzOS 7.20 fehlt eine Zertifikatsverwaltung, um kompromittierte Zertifikate stillzulegen oder eigene Zertifikate hinzuzufügen. AVM erwägt, den einen oder anderen Verbesserungsvorschlag in jüngere FritzOS-Versionen aufzunehmen.

Fazit

AVM macht es den Nutzern leicht, die Verschlüsselung zu verwenden. An den Komfort führender Implementierungen kommen Fritzboxen aber noch nicht heran, schon weil die Verschlüsselung aktiv eingeschaltet werden muss. Und den Status kann man nur umständlich überwachen. Aber ein Anfang ist gemacht – besser eine Verschlüsselung, die etwas Mitarbeit erfordert als gar keine. Und nicht zuletzt ist die Verschlüsselung in Fritzboxen in manchen Punkten umfangreicher als bei anderen Routern. (dz) c't

Glossar

AVP: Audio Video Profile

RTP: Real-time Transport Protocol

sRTP: Secure RTP

SAVP: Secure Audio Video Profile

SDP: Session Description Protocol

SDES: Session Description Protocol Security Descriptions

SIP: Session Initiation Protocol

TCP: Transmission Control Protocol

TLS: Transport Layer Security

Infos zu SDES-sRTP

ct.de/w7ca



Bild: Thorsten Hübner

Im Homeoffice komfortabel telefonieren

Gerade im Homeoffice ist die telefonische Erreichbarkeit wichtig. Mit ein paar Tricks sorgen Sie dafür, dass Sie zu Hause und unterwegs unter der Firmennummer stets gut erreichbar sind und dass Ihre private Rufnummer dabei wirklich privat bleibt.

Von **Urs Mansmann**

Mit der Corona-Krise fanden sich Millionen Arbeitnehmer von heute auf morgen im Homeoffice. In aller Eile wurden Bürostühle nach Hause gewuchtet, Rufumleitungen geschaltet, der heimische PC aufgerüstet und Webcams für Videokonferenzen installiert. Inzwischen wird klar: Das Homeoffice wird für viele sogar zum Dauerarbeitsplatz – und damit das Telefon zu Hause zum unverzichtbaren Werkzeug. Eine einfache Rufumleitung auf den privaten Festnetzanschluss oder das Diensthandy reicht da auf Dauer nicht.

Die perfekte Telefonielösung ist die Anbindung des Homeoffice ans Firmennetz und die dortige Haustelefonanlage. Mit einem vom Admin eingerichteten und verwalteten VoIP-Telefon oder einer Telefonie-App für den PC oder das Smartphone kann man zu Hause telefonieren, als wäre man im Büro, die Abrechnung läuft über die Firma. Nach Feier-

abend kann man das Telefon stumm schalten. Anrufe kann man intern weiterverbinden, auch Besetztfeldanzeigen und interne Voice-Mail-Systeme funktionieren ohne Einschränkung. Wenn Ihr Homeoffice so komfortabel angebunden ist, können Sie hier aufhören zu lesen.

Leider stellen nur wenige Unternehmen diese Lösung zur Verfügung. Werkelt im Betrieb noch eine ISDN-Anlage, ist eine Fernanschaltung per Internet nicht möglich. Und selbst wenn bereits VoIP-Anlagen im Einsatz sind, scheuen viele Admins den Aufwand, die Mitarbeiter im Homeoffice zu betreuen oder fürchten Angriffe auf das Firmennetz über schlecht gesicherte Homeoffice-PCs und -Netze und verweigern deshalb den Zugriff auf die VoIP-Anlage vom Homeoffice aus. Zusätzliche VoIP-Telefone an den Heimarbeitsplätzen verursachen zusätzliche Kosten oder sprengen womöglich die Kapazität der Anlage und erfordern eine Erweiterung. Aber gerade in der Krise möchten viele Geschäftsführer zusätzliche Investitionen vermeiden. Manche lassen außer acht: Über geteilte Büroplätze könnten diese Kosten kompensiert werden.

So ist die naheliegende Lösung in vielen Fällen die Weiterleitung der Büronummer auf einen vorhandenen Festnetz- oder Mobilfunkanschluss des Arbeitnehmers. Eingehende Anrufe werden vom Büro weitergeleitet, ausgehende führen Heimarbeitende über ihre privaten Mobilfunk- oder Festnetzanschlüsse. Das hat aber erhebliche Nachteile.

Mobilfunk oder Festnetz?

Wer die Wahl hat, sollte für die Telefonie im Homeoffice möglichst aufs Festnetz zurückgreifen. Mobilfunkverbindungen sind mitunter wacklig und weisen je nach Funktechnik teils erhebliche Qualitätsmängel auf. Eine besonders schlechte Idee ist es, für die Homeoffice-Telefonate ein altes, abgelegtes Handy einzusetzen, das noch keine HD-Telefonie beherrscht. Bei gutem Empfang und mit einem modernen Handy schlägt Mobilfunk das Festnetz zwar hinsichtlich der Sprachqualität, das ist aber die Ausnahme und nicht die Regel. Das Festnetz hingegen steht für stabile Verbindungen und zumindest ordentliche Sprachqualität. Als Backup für einen Ausfall der Internetverbindung oder des VoIP-Dienstes taugt das Mobiltelefon aber allemal.

Telefone an Festnetzanschlüssen sind stets per VoIP ans Telefonnetz angebunden. Dabei spielt es keine Rolle, ob die lokale Verbindung zum Telefonapparat analog, per ISDN, DECT oder IP erfolgt – dahinter liegt im Router oder spätestens im Anschlusskasten an der Straßenecke eine VoIP-Verbindung.

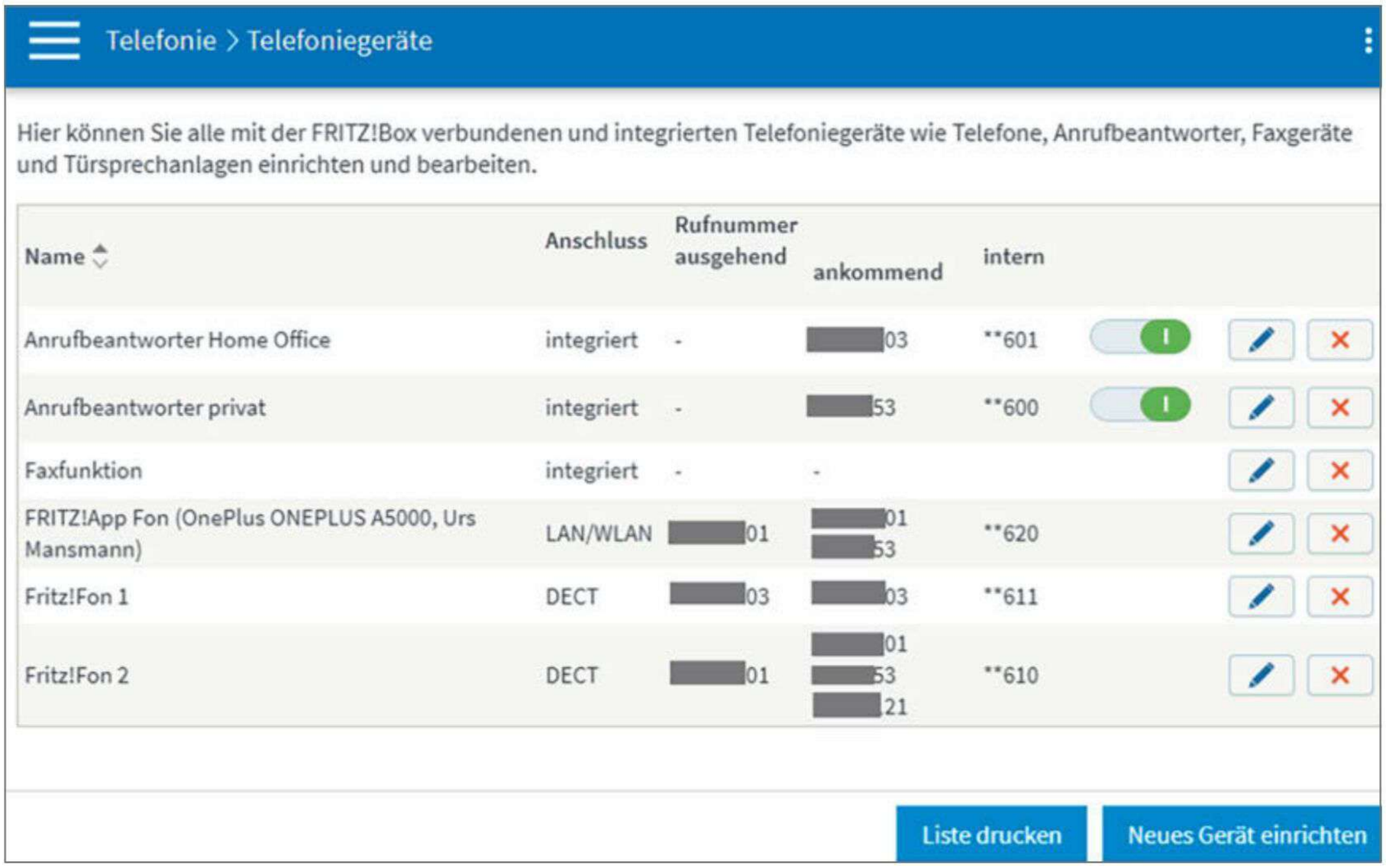
Die jahrelang gescholtene VoIP-Technik erweist sich dabei als robust und flexibel zugleich und ermöglicht Telefonate mit verlässlicher Sprachqualität. Die beste darf man bei HD-Voice-fähigen DECT- und IP-Telefonen erwarten. Sie übertragen an HD-fähigen Anlagen mit ebensolchen Gegenstellen rund 7 statt 3,1 kHz Audiobandbreite. ISDN- und Analogtelefone hingegen sind technisch auf die traditionellen 3,1 kHz festgelegt.

Mit einem separaten Gerät für die geschäftliche Nutzung kann man Berufliches und Privates besser trennen und beispielsweise das dienstliche Telefon manuell beim Verlassen des Homeoffice oder nach einem Zeitplan stumm- oder abschalten. Auch lassen sich abgehende geschäftliche Anrufe auf diese Weise viel leichter getrennt von den privaten erfassen, beispielsweise zur Abrechnung oder als Tätigkeitsnachweis. Dafür braucht man dann aber auch wenigstens eine zweite Rufnummer und eine Telefonanlage.

Wer gerne per Mobilfunk erreichbar sein, aber auf den Komfort der Festnetzanlage nicht verzichten will, kann an einer Fritzbox einen Mobilfunk-Stick nachrüsten und dort die gewünschte Mobilfunk-SIM einlegen. Der Stick wird von der Anlage als Telefonverbindung verwaltet: Eingehende Anrufe lassen sich bestimmten Telefongeräten zuordnen, ausgehende Anrufe können je nach verwendetem Apparat oder nach Zielrufnummer über bestimmte VoIP-Accounts oder die Mobilfunk-SIM geführt werden. So lässt sich beispielsweise eine netzinterne Mobilfunk-Flat für kostenlose Anrufe von den Festnetztelefonen aus nutzen. Will man die Mobilfunknummer auch in einem Smartphone nutzen, benötigt man einen Mobilfunkvertrag mit MultiSIM. Mobilfunk-Sticks mit Sprachfunktion sind inzwischen freilich selten. Wir haben daher eine andere Variante dieses Konzepts im Projekt ab Seite 148 mit einem Raspberry Pi, der Tk-Anlage Asterisk und einem Smartphone umgesetzt.

Die Internetanbindung für das Homeoffice sollte nicht zu sparsam bemessen sein. Anschlüsse mit 16 MBit/s oder weniger im Downstream sind im Upstream – meist 1 bis 2,5 MBit/s – so langsam, dass die Bildqualität bei Videokonferenzen oft sichtbar leidet. Sind parallel größere Dateien zu verschicken oder zu empfangen, kann das bei der VoIP-Telefonie zu Aussetzern führen.

Solange man den Anschluss tagsüber alleine nutzt, ist man ab 5, besser 10 MBit/s in Senderich-



Auf einer Fritzbox können Sie mehrere Anrufbeantworter einrichten und den Telefonen unterschiedliche Nummern zuweisen.

tung und 50 in Empfangsrichtung auf der sicheren Seite. Gibt es weitere Homeoffice- oder Homeschooling-Nutzer, ist es durchaus sinnvoll, noch eine Schippe draufzupacken, wo das möglich ist.

Eingehende Anrufe verwalten

Moderne VoIP-Router wie die beliebte Fritzbox bieten für eingehende Anrufe zahlreiche Optionen. Einfache Analog- oder ISDN-Adapter oder Analoganschlüsse der Telekom und anderer Telefonanbieter bieten solche Funktionen nicht oder nur sehr rudimentär. Falls Sie noch solche Einfach-Gerätschaften oder gar einen Analoganschluss nutzen, sollten Sie auf eine VoIP-Anlage umsteigen, die auch für Einzelnutzer im Homeoffice sinnvolle Funktionen bereithält.

Geschäftliche Anrufe sollten Sie möglichst auf eine separate, ansonsten ungenutzte Rufnummer Ihres Anschlusses umleiten. So lassen sie sich leicht von privaten unterscheiden. Sind alle Rufnummern bereits belegt, fragen Sie Ihren Anbieter, ob Sie zusätzliche Nummern erhalten können.

Eine zusätzliche Rufnummer können Sie aber auch von anderen VoIP-Anbieter erhalten und in Ihrer Anlage zusätzlich einrichten. Nachteil dieser Lösung ist, dass man gebuchte Flatrates für gehende Anrufe über die separate Nummer nicht nutzen kann. Die getrennte Rechnungslegung vereinfacht aber die Abrechnung von betrieblichen Ausgaben; zudem lässt sich die Nummer einfacher ins Café-Office oder das Wochenendhaus mitnehmen. Die Ausfallsicherheit ist höher. Fällt der VoIP-Server des einen Anbieters aus, kann man noch über den des anderen telefonieren.

Bei der Einrichtung eines Telefons an Ihrer lokalen VoIP-Anlage legen Sie fest, auf welche Anrufe das Telefon reagiert. Gehen private und geschäftliche Anrufe unter verschiedenen Zielrufnummern ein, kann man danach filtern und hört schon am Klingeln oder sieht daran, welches Telefon reagiert, ob es sich um einen privaten oder geschäftlichen Anruf handelt.

An einer Fritzbox lassen sich für jedes Telefon tageszeitabhängige Klingelsperren festlegen. Bei



Fritzboxen binden mit der „Fritz!App Fon“ das Smartphone als zusätzliches Festnetzgerät ein.

Anrufen zur Unzeit bleibt das geschäftliche Telefon dann stumm. Wichtige Anrufe, die Sie auch außerhalb der Dienstzeiten erreichen müssen, können Sie dennoch durchlassen, indem Sie die betreffenden Rufnummern ins Adressbuch der Fritzbox eintragen und mit dem Flag „wichtige Person“ versehen.

Wenn Sie nicht noch ein Festnetztelefon beschaffen wollen, können Sie auch Ihr Smartphone als Festnetzapparat nutzen. Mit einer App wie Zoiper lässt es sich mit beliebigen VoIP-Anbietern als IP-Telefon einsetzen; Sie müssen lediglich die Zugangsdaten des VoIP-Accounts eintragen. VoIP-Accounts der Telekom lassen sich allerdings nur aus dem Telekom-Festnetz ansprechen, also nicht mit einer mobilen Verbindung.

Noch einfacher einzurichten ist für Fritzbox-Nutzer die App „Fritz!App Fon“, die das Smartphone als lokales Festnetztelefon für die VoIP-Anlage konfiguriert. Die App funktioniert auch unterwegs, solange eine VPN-Verbindung ins Heimnetz besteht, die sich mit einer Fritzbox mit wenigen Handgriffen einrichten lässt.

Auch Faxanschlüsse lassen sich umleiten. Eine freie Rufnummer auf der Fritzbox kann zum Empfang von Faxen konfiguriert werden. Auf Wunsch legt sie eingegangene Faxe nicht nur zum Abruf auf der Box ab, sondern leitet sie auch per E-Mail als PDF-Anhang an eine festzulegende Adresse weiter.

Umleitung umleiten

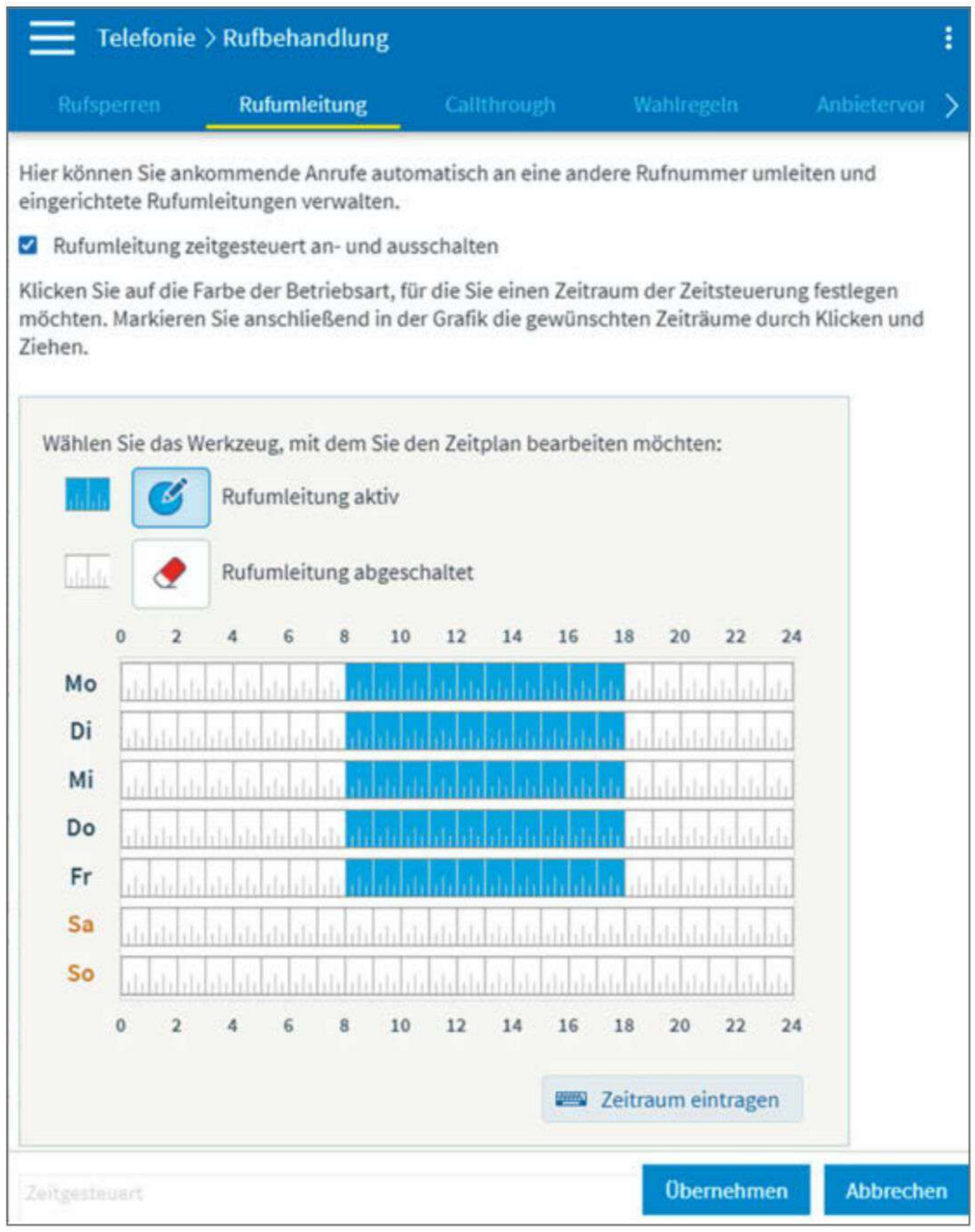
Mit der Fritzbox können Sie eingehende Anrufe nicht nur umleiten, sondern auch an angeschlossenen Telefonen signalisieren und gleichzeitig an zusätzlichen Anschlüssen klingeln lassen, beispielsweise an Ihrem Handy oder in der Ferienwohnung. Ist das annehmende Gerät ein externes, leitet die Fritzbox den Anruf allerdings nicht dorthin um, sondern baut eine zusätzliche Verbindung auf. Hierbei geht die Rufnummerninformation des Anrufers verloren, auf dem externen Gerät ist die eigene Rufnummer sichtbar. Wenn Ihr Festnetzanschluss eine Flatrate hat, die die angerufene Nummer umfasst, ist ein solcher Anruf kostenlos. Anderenfalls müssen Sie dafür wie bei gewöhnlichen Umleitungen die vereinbarten Entgelte je nach Ziel entrichten, denn Sie haben diesen zusätzlichen Anruf ja selbst initialisiert.

Über zeitgesteuerte Umleitungen können Sie außerhalb der Bürozeiten einen Anrufbeantworter in der Fritzbox aktivieren, der Nachrichten ohne Klingeln entgegennimmt. Tagsüber können Sie ihn so einrichten, dass er nach 20 oder 30 Sekunden annimmt oder sofort, wenn Sie gerade telefonieren. Alternativ können Sie eine Ansage abspielen lassen, beispielsweise zeitgesteuert abends und am Wochenende: „Leider rufen Sie außerhalb unserer Geschäftszeiten an.“

Wenn Sie möchten, dass ein Besetztzeichen ertönt, wenn Sie gerade telefonieren, müssen Sie die Option „busy on busy“ in Ihrem VoIP-Router aktivieren. Die Alternative wäre ein Anklopfen, bei dem im Gespräch ein Signalton ertönt, wenn ein weiterer Anruf eingeht. Über einen Tastendruck am Telefon können Sie dann den anderen Anruf annehmen, zwischen den beiden Gesprächen wechseln oder eine Dreierkonferenz mit beiden Gesprächspartnern schalten. In der Praxis möchten die meisten Anwender lieber ungestört telefonieren.

Die richtige Nummer anzeigen

Wenn Sie aus dem Homeoffice anrufen, sollten Geschäftspartner oder Kunden Ihre Privatnummer nicht sehen. Schon deshalb ist es sinnvoll, für das Home-



Per Zeitsteuerung lassen sich Anrufe außerhalb der Geschäftszeiten stumm schalten, Rufumleitungen an- und abschalten oder Anrufe auf die interne Mailbox umleiten.

office eine Nummer zu verwenden, die ansonsten nicht eingesetzt wird und lediglich auf dem geschäftlich genutzten Apparat landet.

Viele VoIP-Anbieter, beispielsweise Sipgate, Easybell oder dus.net, lassen das Setzen einer beliebigen Rufnummer zur Anzeige beim Angerufenen zu. Einige Anbieter verifizieren diese durch einen Kontrollanruf. Allerdings wird bei ausgehenden Telefonaten stets auch die eigentliche Rufnummer mitgeschickt und an manchen Anschlüssen angezeigt, insbesondere wenn Sie ins Ausland telefonieren.

Alternativ kann man die Rufnummer unterdrücken. Allerdings wird die Rufnummer bei jeder Verbindung mitgeschickt und erst in der letzten Vermittlungsstelle unterdrückt. Die Unterdrückung funktioniert erheblich zuverlässiger als die Anzeige einer selbst festgelegten Rufnummer, allerdings kann man sich nicht darauf verlassen, dass alle Vermittlungsstellen und -anlagen korrekt konfiguriert sind und die unterdrückte Rufnummer nicht doch beim Angerufenen erscheint.

Fazit

Mit den richtigen Einstellungen am VoIP-Router und einem zusätzlichen Telefon sind Sie im Homeoffice stets gut erreichbar und enthüllen Gesprächspartnern nicht ungewollt Ihre private Rufnummer. Geschäftliche und private Anrufe lassen sich sauber trennen, nach Dienstschluss bleibt das Telefon still. Handy und Festnetzanschluss arbeiten mit einem Parallelruf Hand in Hand, sodass Sie auch unterwegs keinen Anruf auf Ihre Festnetznummer verpassen. Mit einer Fritzbox lassen sich sogar Faxe im Homeoffice empfangen und per E-Mail weiterleiten. (uma) c't

c't iX Mac&i heise Developer heise Security



ALLES AUF ANFANG

Neustart der IT-Weiterbildung

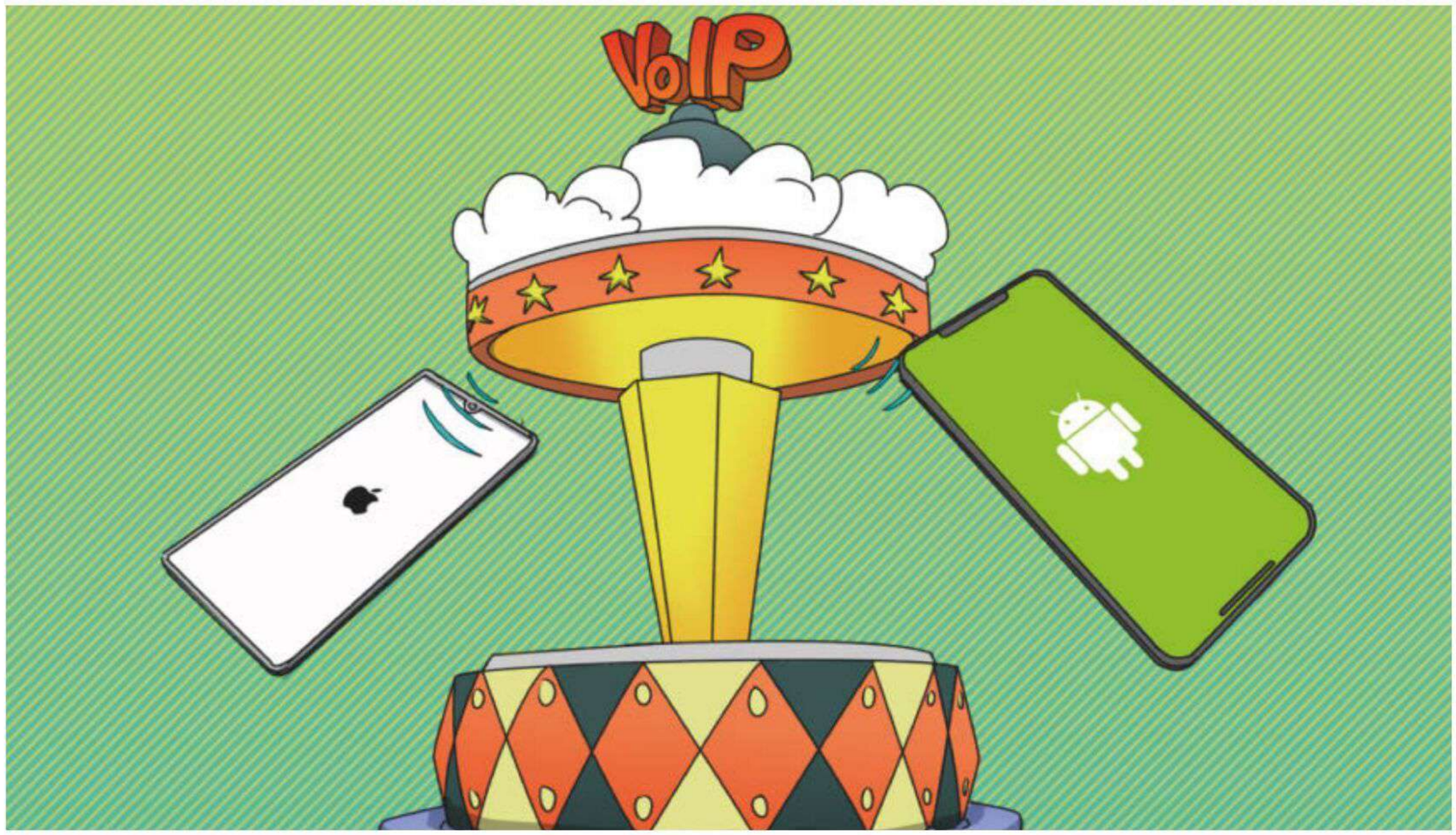
Kennst du schon die neue interaktive Lernplattform für IT-Professionals?

Bei uns findest du das Wissen zu den angesagten IT-Themen - von Experten für Professionals.

Jetzt testen! Hier gehts zu den ersten Gratis-Videos:

heise Academy

heise-Academy.de | @heise_Academy | #heiseAcademy



Homeoffice-Telefonie mit der Fritzbox

Separate Rufnummern, zeitgesteuerte Anrufbeantworter, Rufumleitungen, Smartphone-Apps und mehr – AVMs FritzOS bietet allerhand Funktionen, mit denen Sie sich die Telefonie im Homeoffice erleichtern können. Die wichtigsten im Überblick.

Von **Andrijan Möcker**

Die Corona-Pandemie hat dem Thema Homeoffice einen gehörigen Schub verpasst. Die klassische geschäftliche Telefonnummer hat diesen Wandel in vielen Unternehmen jedoch nicht mitgemacht – statt VoIP-Zugänge zur Unternehmenstelefonanlage zu legen, wurden die Anschlüsse oft einfach auf die heimische Rufnummer oder das Handy umgeleitet. Das bedeutet jedoch gleichzeitig, dass das private Gerät klingelt, wenn die dienstliche Rufnummer angerufen wird – zu jeder Tages- und Nachtzeit.

Wenn Sie eine Fritzbox Ihr Eigen nennen, können Sie das Problem meist schnell lösen: AVMs FritzOS kann bis zu 20 Internettelefonie-Rufnummern gleichzeitig bedienen und ist unter den Routerbetriebssystemen für Privatkunden eines der umfangreichsten in puncto Telefoniefunktionen.

Getrennte Rufnummern

Um private von geschäftlichen Anrufen zu unterscheiden, ist es sinnvoll, für beide unterschiedliche Num-

mern zu haben. Das Telefon beim Arbeitgeber leitet man dann auf die geschäftliche Heimnummer um.

Prüfen Sie zunächst, ob Sie schon mehrere Rufnummern haben: Selbst, wenn Sie schon lange Kunde bei einem Anbieter sind und gewohnheitsmäßig nur eine Rufnummer nutzen, kann es sein, dass Sie zur Umstellung auf die Internettelefonie (Voice over IP, VoIP) ein bis zwei weitere Rufnummern bekommen haben. Je nach Anbieter stehen die Rufnummern auf den Vertragsinformationen oder im Kundenportal.

Lässt die Fritzbox automatische Konfigurationsänderungen durch den Anbieter zu, sind die Rufnummern möglicherweise bereits eingerichtet und warten nur darauf, einem Telefon zugewiesen zu werden. Schauen Sie dazu in der Fritzbox-Weboberfläche (http://fritz.box) unter „Telefonie/Eigene Rufnummern“ nach. Wenn dort keine weiteren Nummern stehen, benötigen Sie die Zugangsdaten für die VoIP-Konten; sie bestehen in der Regel aus der Rufnummer, einer SIP-Serveradresse (Session Initiation Protocol, De-facto-Standard für VoIP-Telefonie), Benutzername, Kennwort und in manchen Fällen auch aus einer Proxy-Server-Adresse.

Diese Anmeldedaten muss Ihnen der Anbieter in Deutschland frei herausgeben, das „Gesetz zur Auswahl und zum Anschluss von Telekommunikationsendgeräten“ alias die „Routerfreiheit“ verpflichtet ihn dazu. Viele Provider haben daher Automatismen eingeführt, die die Zugangsdaten für alle vertraglich vereinbarten Dienste entweder im Kundenportal oder über einer PDF-Datei zur Verfügung stellen. Vergleichbare Gesetze gibt es in Österreich und der Schweiz nicht.

Haben Sie keine weiteren Rufnummern, schauen Sie zunächst im Kundenportal Ihres Anbieters in den Zusatzoptionen für Ihren Tarif; meist können Sie weitere Telefonnummern hinzubuchen, in vielen Fällen wird dafür aber eine einmalige oder monatliche Gebühr fällig. Recherchieren Sie vorher, wie viele Gesprächskanäle Ihr Anbieter Ihnen zur Verfügung stellt; diese sind unabhängig von der Anzahl der Rufnummern und bestimmen, wie viele gleichzeitige Gespräche Sie an Ihrem Anschluss führen können. Je nachdem, wie hoch Ihr Bedarf ist, müssen Sie zusätzliche Gesprächskanäle hinzubuchen.

Da SIP der De-facto-Standard für Internettelefonie ist, können Sie unabhängig vom Telefoniedienst Ihres Internetanbieters weitere Rufnummern bei anderen VoIP-Anbietern buchen, die obendrein viele nützliche Zusatzdienste bieten. Gleiches gilt, wenn Ihnen Ihr Arbeitgeber einen SIP-Zugang zur Firmen-Telefonanlage anbietet. FritzOS bedient bis zu 20 SIP-Konten gleichzeitig und in den Telefonie-Einstellungen können Sie, sofern die Fritzbox nicht mit einer Anbieter-Firmware abgeriegelt wurde, einfach auf „Neue Rufnummer“ klicken und die Zugangsdaten eintragen.

Separate Telefone

Bis auf die Modelle 4020 und 4040 erhält man heute keine Fritzboxen ohne Telefonfunktion mehr. Zur Standardausstattung gehören meist ein oder zwei



Weitere Rufnummern für den heimischen Anschluss zu besorgen ist dank Internettelefonie (VoIP) sehr leicht. Moderne Fritzboxen können bis zu 20 VoIP-Konten gleichzeitig bedienen und die Rufnummern müssen nicht unbedingt vom eigenen Internetanbieter stammen.

analoge Telefonports, eine DECT-Basis und ein SIP-Server für bis zu 10 IP-Telefone; größere Modelle haben zudem einen S0-Port für ISDN-Telefone und Telefonanlagen. Kurzum: Wer ein separates Telefon für seine dienstliche Heimrufnummer haben möchte, hat große Auswahl.

Den geringsten Hardware-Aufwand haben Sie, wenn Sie Ihr Smartphone mittels App zum VoIP-Telefon machen. AVM bietet dafür das „Fritz!App Fon“ in den App-Stores von Android und iOS. Die Software nutzt die VoIP-Schnittstelle der Fritzbox, um Ihr Smartphone als Nebenstelle zu registrieren. Zusätzlich hat AVM das Fritzbox Telefonbuch, die Anrufliste sowie die Rufnummerneinstellungen der virtuellen Nebenstelle integriert. Beachten Sie, dass die App je nach Energiesparrichtlinie Ihres Smartphones, nicht im Hintergrund aktiv bleibt, um Anrufe zu empfangen. Je nach System finden Sie eventuell Optionen, um das Energiesparverhalten für Apps zu ändern, in der App-Liste in den Systemeinstellungen oder im Akku-Menü.

Ähnlich einfach hat man es mit einem weiteren DECT-Telefon: Die DECT-Basen aller Fritzboxen unterstützen das Generic Access Profile (GAP), das eine grundlegende Interoperabilität zwischen den Handsets und den Basisstationen verschiedener Hersteller gewährleistet. Wenn Sie beispielsweise drei DECT-Telefone im Haus über eine Basis nutzen, die analog an die Fritzbox angeschlossen ist, können Sie via GAP eines davon für den Homeoffice-Betrieb abzweigen und direkt in die Fritzbox einbuchen. AVM bietet eigene DECT-Telefone, die optimal auf die Funktionen und Dienste der Fritzbox abgestimmt sind.

Um ein neues DECT-Gerät einzubuchen, öffnen Sie im Fritzbox-Webinterface in „Telefonie / Telefoniegeräte“ den Einrichtungsassistenten („Neues Gerät einrichten“). Im Menü des DECT-Telefons heißt die Einstellung zum Einbuchen in eine neue Basis etwa „Anmelden“ oder „Basis registrieren“. Da GAP nur das Nötigste regelt, fehlen dann in der Regel Merkmale wie Anrufbeantworterabfrage oder Telefonbücher. Die grundlegende Telefonie sollte jedoch funktionieren. Wenn der Hersteller die DECT-Erweiterung CAT-iq implementiert hat, funktioniert wahrscheinlich auch HD-Telefonie.

Wenn das Homeoffice-Telefon etwas professioneller sein soll, beispielsweise weil sie bessere Freisprechqualität brauchen als ein DECT-Handset bietet, können Sie ein kabelgebundenes VoIP-Telefon verwenden. Es kann über die Nebenstellenfunktion des SIP-Dienstes von FritzOS wie ein normales Telefon verwendet und intern angewählt werden (**6XX). Da solche Telefone seit mehr als einem Jahrzehnt verbreitet sind, gibt es einen großen Gebrauchtmarkt, auf dem Sie sich zu kleinen Preisen ab etwa 10 Euro bedienen können. Ab Seite 134 beschreiben wir, wie sich preisgünstige Geräte der Markte Unify für Fritzboxen anpassen lassen.

Von solchen Telefonen dürfen Sie gute Sprachqualität, leichte Bedienbarkeit und robuste Gehäuse erwarten. Beispiele sind etwa HFA- oder SIP-Telefone von Unify (siehe Seite 134) oder die CP-/SP-Reihen von Cisco [1, 2]. Manche Details des SIP-Protokolls können den Betrieb jedoch auch verhindern; recherchieren Sie daher zunächst nach Erfahrungen mit dem jeweiligen Modell beim Betrieb an Fritzboxen, bevor Sie Geräte anderer Hersteller kaufen. Die Konfiguration einer neuen VoIP-Nebenstelle läuft über den Einrichtungsassistenten für Telefoniegeräte; die Anschlussart heißt „LAN/WLAN (IP-Telefon)“; zur Anmeldung des Telefons trägt man einen beliebigen Benutzernamen und ein Kennwort ein.

Auf dem gleichen Weg können Sie auch Ihren Computer zum VoIP-Telefon (Softphone) machen. Anwendungen wie Linphone oder PhonerLite buchen sich über das SIP-Protokoll wie ein Hardware-Telefon in die Fritzbox ein und arbeitet dann genauso. Jedoch funktioniert die Echounterdrückung dieser Programme nicht immer zuverlässig; daher empfiehlt sich zum Telefonieren ein Kopfhörer oder besser noch ein Headset.

Anrufbeantworter und Rufumleitungen

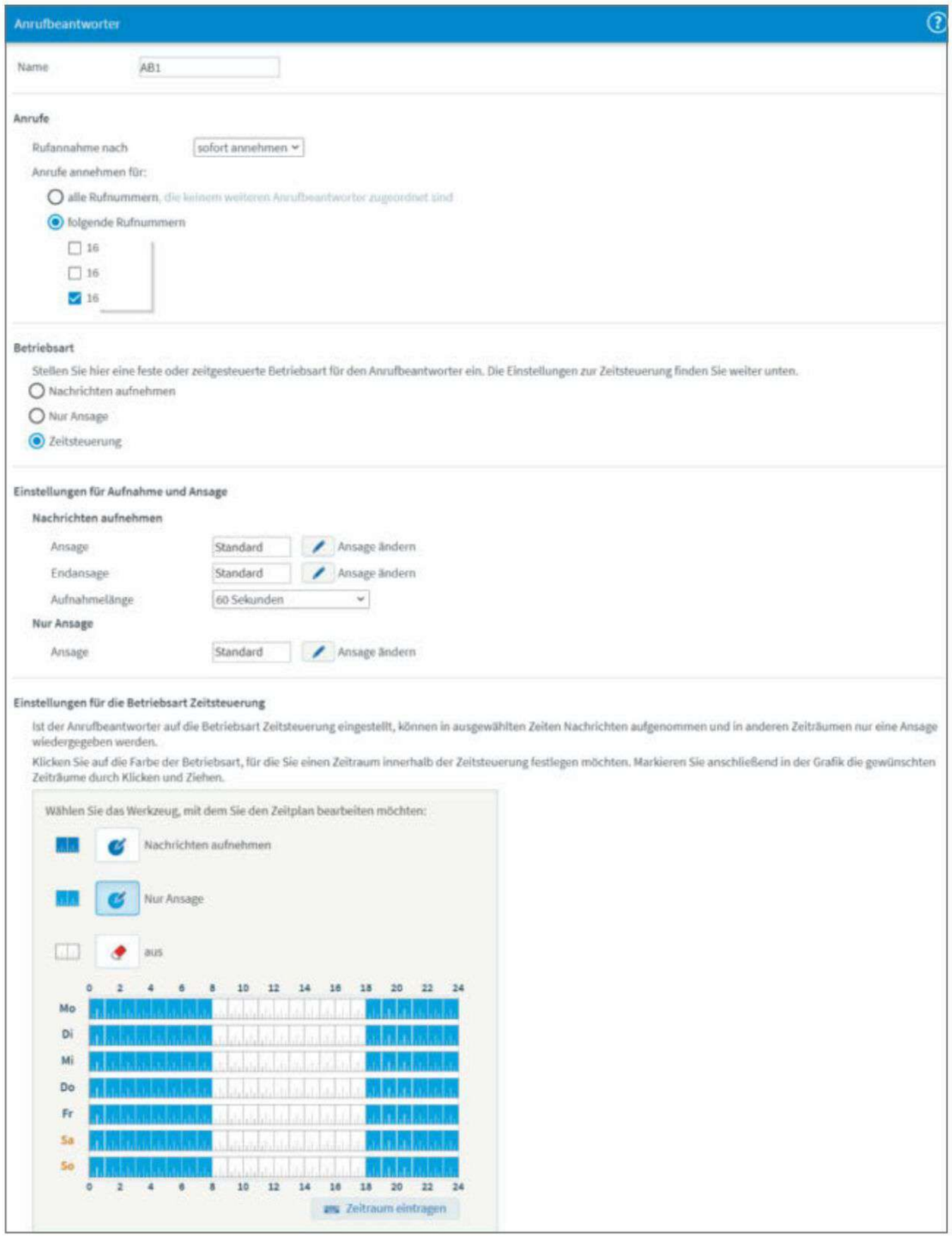
FritzOS unterstützt bislang keine Klingelsperre für einzelne Rufnummern sowie VoIP- oder ISDN-Nebenstellen. Doch es gibt einen Trick, um trotzdem nach Feierabend dienstliche Anrufe automatisch abzublocken statt die für den Dienstanschluss benutzten Telefone stummzuschalten: zeitgesteuerte Anrufbeantworter. Diese können Sie in FritzOS als Anrufabfänger für bestimmten Zeiten konfigurieren – entweder mit Aufzeichnung oder nur einer Ansage. Wenn Sie den Anrufbeantworter in den Modus „sofort annehmen“ versetzen, klingeln die zugehörigen Telefone nur noch außerhalb der Anrufbeantworterzeiten.

Mehrere Anrufbeantworter für die gleiche Rufnummer sind möglich, beispielsweise wenn Sie während Ihrer Arbeitszeit Nachrichten aufzeichnen wollen, danach aber nicht mehr. Besonders praktisch: Wenn Sie ein Mailkonto für Ihre Fritzbox eingerichtet haben, können Sie aufgezeichnete Nachrichten per Mail an Ihre dienstliche Adresse weiterleiten.

Literatur

[1] Florian Klan, **Verbrüderung**, Cisco-IP-Telefone an der Fritzbox betreiben, c’t 14/2017, S. 136

[2] Jan Mahn, Andrijan Möcker, **Günstige Netzwerker**, Sparen mit gebrauchter Netzwerkhardware, c’t 6/2020, S. 100



Zeitgesteuerte Anrufsperren gibt es in FritzOS nur für Analog- und DECT-Telefone, nicht aber für VoIP- oder ISDN-Geräte. Mit einem zeitgesteuerten Anrufbeantworter im Modus „Sofort annehmen“ kann man das Problem umgehen. Er fängt Anrufe nach Feierabend ab, sodass das zugehörige Telefon stumm bleibt.

Wenn Ihr VoIP-Tarif mindestens zwei Sprachkanäle umfasst, können Sie Ihre Erreichbarkeit mit einigen Rufumleitungen etwas flexibler gestalten. Legen Sie in „Telefonie / Rufbehandlung / Rufumleitung“ beispielsweise einen Parallelruf an, klingelt Ihr Handy mit und Sie können entweder am Festnetzgerät oder mobil abnehmen, ohne dass der Anrufer eine andere Rufnummer wählen muss. Haben Sie einen „Feierabend-Anrufbeantworter“ konfiguriert, bleibt das Handy nach Feierabend still. Beachten Sie aber, dass sämtliche Rufumleitungen durch die Fritzbox ausgelöst werden, nicht durch das Netz – Sie tragen also immer die Kosten einer Weiterleitung und wenn die Internetverbindung unterbrochen ist, funktionieren derartige Umleitungen nicht.

Günstige Telefonate

Wenn Sie aus dem Homeoffice oft per Mobilfunk oder international telefonieren müssen, können die Kosten schnell in die Höhe gehen. Selbst wenn Ihr Arbeitgeber die Kosten übernimmt, können Sie mithilfe von Vor-Vorwahlen („Call-by-Call“) oder zusätzlichen VoIP-Angeboten die Rechnung drücken. FritzOS speichert bis zu neun Sparvorwahlen und verwendet diese entsprechend den Wahlregeln. Call-by-Call steht nur an Anschlüssen der Deutschen Telekom zur Verfügung. Zusätzliche VoIP-Angebote lassen sich hingegen an allen Anschlüssen nutzen.

Im Fritzbox-Webinterface können Sie unter „Telefonie / Rufbehandlung / Anbietervorwahlen“ die zuvor im Netz recherchierten Vor-Vorwahlen für verschiedene Ziele eintragen. Anschließend muss in der Registerkarte „Wahlregeln“ eine neue Wahlregel für das Ziel erstellt und die zuvor eingetragene Vorwahl bei „verbinden über“ ausgewählt werden. Dafür können Sie auch VoIP-Accounts einsetzen, die gerade bei Mobilfunk- und Auslandstelefonaten sehr günstige Tarife bieten. Dass die Wahlregel greift, erkennen Sie an der Ansage des Preises sowie der um die Vorwahl ergänzten angerufenen Nummer in der Fritzbox-Anrufliste. Sollten sich Preise ändern oder neue Alternativen hinzukommen, können Sie einzelne Einträge ändern, ohne die Wahlregeln dazu insgesamt neu einzurichten.

Fazit

Die Homeoffice-Telefonie lässt sich mit FritzOS leicht optimieren. Wer sich mit den Funktionen auseinandersetzt, kann schnell Privates und Geschäftliches trennen, spart Geld bei Telefonaten zu Rufnummern in Mobilfunk- oder Auslandsnetzen und hat Ruhe nach Feierabend. Lobenswert ist, dass AVM kein Mehrklassen-Betriebssystem baut und durchweg allen Fritzboxen die gleichen Funktionen spendiert – unabhängig vom Preis des Geräts. (amo) c't



Unify-VoIP-Telefone an der Fritzbox

Gebrauchte IP-Telefone von Unify gibts günstig gebraucht: Oft erhält man gut erhaltene Geräte für nicht einmal 20 Euro. Wir zeigen, wie man das richtige Telefon auswählt und ihm klassisches SIP beibringt, sodass es an Fritzboxen oder mit freien VoIP-Anbietern funktioniert.

Von **Andrijan Möcker**

Selbst die teuerste und schickste Hardware sortieren Firmen irgendwann aus und oder ersetzen sie mit etwas, das mehr Funktionsumfang hat oder dem Chef besser gefällt. Doch was große Firmen ausmustern, genügt den Ansprüchen im heimischen Umfeld oder in kleinen Büros oft noch. Wer genau hinschaut, kann aussortierte Hardware als Schnäppchen ergattern. IP-Telefone lohnen sich hier besonders für Festnetztelefonierer: Sie integrieren sich ins sowieso benötigte Büro- oder Heimnetzwerk und kommen ohne separate Verkabelung und Hardware (Telefonanlage) aus.

Zuletzt berichteten wir 2017 über Ciscos abgekündigte VoIP-Telefone, die zuhauf für kleines Geld bei eBay den Besitzer wechselten [1]. Sie sind zwar vielfältig konfigurierbar, doch ohne komplizierte Konfigurationsdateien und einen dauerhaft verfügbaren TFTP-Server läuft nichts.

Die OpenScape- und OpenStage IP-Telefon-Serien der ehemaligen Siemens-Tochter Unify sind da einfacher zu handhaben: Sie haben ein Webinterface zur Konfiguration. Parameter sind meist klar beschriftet und auch für lesewillige VoIP-Telefon-Einsteiger leicht zu verstehen. Die Modelle werden langsam, aber sicher aussortiert und auf den Internetmarktplätzen gibt es mittlerweile ein großes Angebot an Gebrauchtgeräten zu Preisen ab circa 10 Euro – wenn man denn darauf achtet, wie und wo man einkauft.

Weise Auswahl

Unifys' OpenScape-Serie enthält nur IP-Geräte. Bei OpenStage-Telefonen aus der Siemens-Zeit der Firma muss man jedoch genau auf das Suffix in der Modellbezeichnung achten: Außer den IP-basierten HFA- und SIP-Varianten der Telefone gibt es T-Varianten. Das sind Systemtelefone, welche nur die aus der ISDN-Welt stammende zweidrahtige Up0-Schnittstelle nutzen. Ohne passende Siemens-HiPath-Telefonanlage und separate Kabelinfrastruktur funktionieren sie nicht. Dennoch bezeichnen manche Verkäufer die T-Systemgeräte fälschlich als IP-Telefone.

HFA- und SIP-Geräte können Sie jedoch gefahrlos kaufen. Sie unterscheiden sich hauptsächlich in der leicht zu ändernden Firmware und der Anschlussgeschwindigkeit der beiden Ethernet-Ports. Meist handelt es sich um 100-MBit/s-Ports, was für VoIP mehr als genug ist. Wer über den zweiten Port seines Telefons ein zusätzliches Gerät anbinden möchte, muss prüfen, ob Fast-Ethernet ausreicht und ansonsten ein Gigabit-Modell kaufen – erkennbar am Zusatz „G“. Eine weitere Ausnahme sind seltene Modelle mit dem E-Zusatz, die keine Lautsprecher-Telefonie zulassen.

Alle Modelle versorgt man per Power-over-Ethernet (IEEE 802.3af) mit Strom. Zum Preis des Telefons kommen also noch rund 10 bis 20 Euro für einen Injektor. Ab zwei Telefonen am selben Ort ist ein PoE-Switch günstiger – TP-Link liefert beispielsweise vier PoE-Ports plus Uplink-Port für 30 (100 MBit/s) beziehungsweise 37 Euro (Gigabit-Ethernet).

Spezifische technische Daten zu den interessantesten Modellen finden Sie in den Kurzbeschreibungen ab Seite 138.

Clever eingekauft

Sucht man auf den üblichen Internetmarktplätzen wie eBay oder Amazon nach „Unify“, „OpenStage“



Bild: Karl-Heinz Möcker

Das Unify OpenStage 15 HFA hat acht Funktionstasten, die frei belegt werden können – in diesem Fall nur mit Direktwahlen für den Betrieb als Notfalltelefon mit den wichtigsten Rufnummern.

oder „OpenScape“ sind die Telefone auf den ersten Blick deutlich teurer als 10 oder 20 Euro. Dabei handelt es sich meist um generalüberholte Geräte, die vom Händler gereinigt, getestet und gegebenenfalls repariert wurden. Dafür bekommt man ein Telefon, das definitiv funktioniert und kaum zusätzliche Arbeit macht.

Als „Gebraucht“ markierte Angebote sind günstiger. Oft sind die Telefone in einem ähnlichen Zustand wie generalüberholte oder erfordern nur geringfügige Aufarbeitung. Um unnötigen Ärger zu vermeiden, sollten Sie die Beschreibungen genau lesen und gegebenenfalls beim Anbieter nachfragen, in welchem Zustand ein angebotenes Gerät ist.

Ein Blick in eBay-Kleinanzeigen lohnt sich ebenso, denn hier landen oft ganze Büroauflösungen. Viele Verkäufer sind außerdem bereit zu Verhandlungen.

Firmware

Ein Großteil der verkauften Telefone bringt die HFA-Firmware mit, die ausschließlich mit HiPath-Telefonanlagen funktioniert. Die Umstellung auf SIP dauert aber nur wenige Minuten.

Die erforderlichen Firmware-Dateien gibt es aufgrund der enthaltenen Verschlüsselungstechniken nicht frei zum Download. In unserem Fall reagierte Unify innerhalb weniger Stunden mit einem temporären Downloadlink auf eine Anfrage über das Kontaktformular (siehe ct.de/w2du). Inoffizielle Downloadlinks fanden wir in einem Beitrag zum IP35G im tek-tips-Forum – dabei sollte man aber die Gefahr von manipulierten Dateien im Hinterkopf behalten.

Abgesehen von der modellspezifischen Datei läuft die Firmwareänderung bei allen Telefonen gleich: Das System lädt die Datei einmalig per HTTPS oder FTP herunter. Neuere Modelle wie das IP35 nehmen das Binary auch über das Webinterface entgegen.

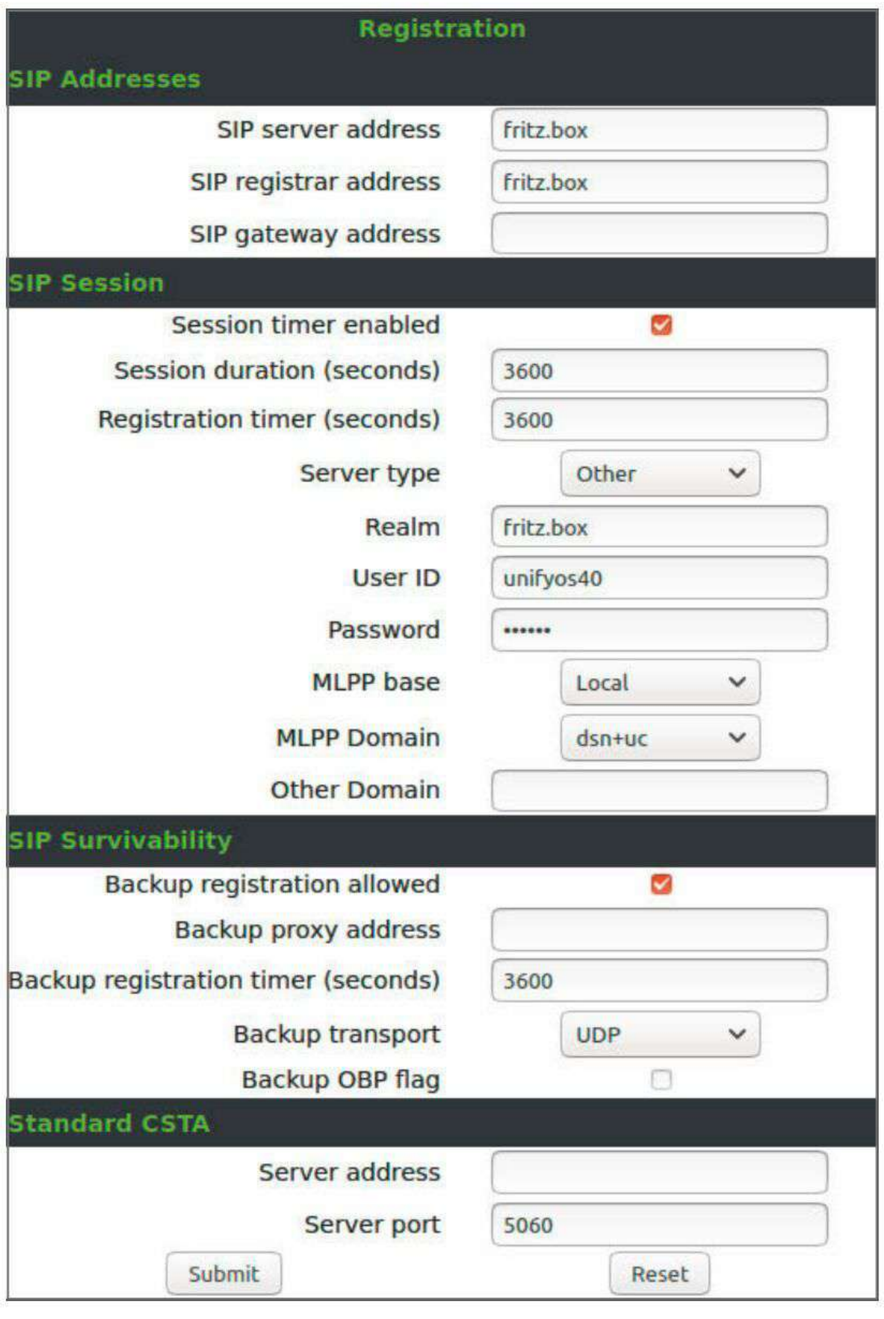
Aus HFA mach SIP

Vor der Installation sollten Sie Ihr Telefon zurücksetzen. Stecken Sie es dazu an den PoE-Adapter, ohne es mit Ihrem Heimnetz zu verbinden, und lassen Sie das Telefon booten. Dann drücken Sie die Tasten 2, 8 und 9 gleichzeitig, tippen die Pin 124816 ein und bestätigen mit der Ok-Taste.

Während sich das Telefon zurücksetzt, richten Sie einen beliebigen FTP-Server auf Ihrem Rechner ein – sofern Ihr Router nicht sowieso einen bietet. Sie können den Dateinamen auch kürzen, um die Eingabe später im Webinterface zu erleichtern.

Nach dem Reset verbinden Sie das Telefon mit Ihrem Netzwerk – im Werkszustand versucht es eine Adresse per DHCP zu beziehen. Ermitteln Sie die IP-Adresse des Geräts über die Oberfläche Ihres Routers oder mithilfe einer Netzwerkscanner-App wie Fing. Mittels IP-Adresse rufen Sie die Weboberfläche des Telefons über einen beliebigen Browser auf. Da die Telefone HTTP-Anfragen abweisen, muss man „https://“ manuell vor die IP-Adresse stellen.

In der Registerkarte „Administratorseiten“ (Werkspasswort: 123456) wechseln Sie zu „File transfer“, „Defaults“, setzen die „Download method“ auf FTP, tragen die nötigen Parameter ein und bestätigen mit Submit. Wenn Sie die Firmware-Datei im Root-Verzeichnis des FTP-Servers abgelegt haben, tragen Sie nur / in „FTP path“ ein. Über das Menü „Phone application“ geschieht der Rest: Haken Sie „Use defaults“ an, geben Sie den Dateinamen an



Klar beschriftet und in wenigen Minuten erledigt: Die Unify-Einstellungen sind auch für Anfänger keine große Hürde.

Extratasten

Mit Funktionstasten können die Unify- und Siemens-VoIP-Telefone weitgehend individualisiert werden. Doch wenn viele Funktionen und wichtige Rufnummern direkt erreichbar sein sollen, reicht möglicherweise der Platz nicht mehr. Tastenerweiterungen gibt es in diesem Fall als einfache Erweiterungsoption: Das OpenStage Key Module 15 ist, je nach Zustand, schon für rund 20 Euro zu haben. Es erweitert OpenStage-Geräte wie das OS15 oder das OS40 um 18 Funktionstasten inklusive LED.

Stolze 90 Funktionstasten erhält man mit dem Unify Busy Lamp Field 40. Das Erweiterungsmodul schlägt jedoch mit satten 250 bis 430 Euro zu Buche, je nach Händler und Zustand.

Doch aufgepasst – nicht alle Key Module von Unify passen an alle Telefone. Eine Kompatibilitätsliste gibt es im jeweiligen Unify-Wiki-Eintrag des Telefons.



Das OpenStage Key Module 15 erweitert Telefone um 18 weitere frei zu belegende Tasten.

(Filename) und setzen Sie „After submit“ auf „start download“.

Stellen Sie sicher, dass das Telefon zuverlässig mit dem Netzwerk und der Stromversorgung verbunden ist, dann klicken Sie auf „Submit“. Warten Sie, bis das Telefon die Firmware geladen hat und sich erneut über nicht funktionierende Telefonie beschwert. Öffnen Sie dann das Webinterface wieder. Reagiert die Oberfläche mit der neuen Firmware nicht auf Befehle, leeren Sie den Cache Ihres Browsers.

Einrichtung

Um das Telefon vor unbefugtem Zugriff zu schützen, ändern Sie zunächst das Administratorpasswort unter „Security and Policies“, „Password“, „Change Admin password“. Anschließend können Sie im Untermenü „Network“ optional eine feste IP-Adresse und weitere IP-Parameter einstellen.

Die Sprachen- und Zeitkonfiguration nehmen Sie in den „User pages“ im Menüpunkt „Locality“ vor. Die Zeitumstellung muss in den „Administratorseiten“ unter „Date and time“ konfiguriert werden.

Die „Canonical dial settings“ in „Local functions“, „Locality“ ermöglichen dem Telefon, die vom SIP-Dienst vollständig signalisierten Rufnummern sinnvoll zu kürzen. Geben Sie keine zusammengesetzten Blöcke ein, sondern jeden Parameter für sich. So lautet der „Local country code“ „49“, der „International access code“ „00“ und das „National prefix digit“ „0“. Der „Local national code“ Ihre Ortsvorwahl muss ohne führende „0“ eingetragen werden.

HD-Telefonie ist in den Werkseinstellungen nicht aktiviert. Unter „Speech“ können Sie den für breitbandige Telefonie verwendeten Codec G.722 einfach anhaken und über die Pfeile an oberste Stelle setzen, sodass er bevorzugt verwendet wird.

Gefritzt

Die Einrichtung der Unify-Telefone an der Fritzbox ist unkompliziert. Für den Einsatz mit VoIP-Anbietern sollten Sie jedoch in dessen Dokumentation nach einer dedizierten Anleitung für Ihr Telefon beziehungsweise Ihr Unify- oder Siemens-Gerät schauen. Der Anbieter hat unter Umständen besondere Konfigurationsanforderungen, beispielsweise hinsichtlich Verschlüsselung und Ports.

In Ihrer Fritzbox-Konfiguration legen Sie zuerst eine neue VoIP-Nebenstelle für das Telefon an: Im Webinterface rufen Sie dazu „Telefonie“, „Telefonie-



Unify OpenScape IP35(G) (eco)

Das OpenScape IP35 ist eines der neueren Geräte in unserer Auswahl. Wie das OS15 besitzt das IP35 ein zweizeiliges Display mit 205 × 41 Pixeln. Leider hat Unify auf eine Hintergrundbeleuchtung verzichtet, sodass immer eine externe Lichtquelle nötig ist, um das Display abzulesen. Auch Funktionstastenmodule funktionieren mangels Anschluss nicht.

Davon abgesehen punktet das IP35G mit seiner großen roten Signalisierungs-LED, einem kräftigen Lautsprecher und dem im Standfuß enthaltenen Hörerclip. Diesen kann man einfach herausbrechen und in die Höreraufnahme einsetzen, wenn das Telefon an die Wand montiert werden soll.

Das Gerät kostet gebraucht zwischen 15 und 40 Euro.



Siemens / Unify OpenStage 15 HFA/SIP (G)

Das OpenStage 15 ist gebraucht für 5 bis 20 Euro das günstigste Telefon von Unify beziehungsweise Siemens. Mit seinem nach vorne geneigten Display ohne Hintergrundbeleuchtung eignet es sich primär als Tischtelefon. Zur Wandmontage wird weiteres Zubehör für rund 20 Euro benötigt.

Das OS15 besticht besonders durch seine acht frei belegbaren Funktionstasten, die entweder mit Stift oder mit der Druckvorlage (siehe Absatz „Funktionstasten“) beschriftet werden können. Je nach Konfiguration können die LEDs der Tasten auch als Belegtindikatoren arbeiten. Reichen die Tasten nicht, erweitert man es per Key Modul.

Das OS15 eignet sich so gut als Notfall- oder Seniorentelefon mit schneller Direktwahl und leichter Bedienung.

geräte“ auf und klicken auf „Neues Gerät einrichten“. Wählen Sie „Telefon“ und im nächsten Menü „LAN / WLAN (IP-Telefon)“. Folgen Sie dem Assistenten weiter und passen Sie die Einstellungen wenn nötig an. Achten Sie besonders darauf, ein sicheres individuelles Passwort zu vergeben.

Dann tragen Sie die Accountdaten im Unify-Webinterface ein: Wechseln Sie auf der Administrationsseite auf „System“ und dann „System Identity“. In „Terminal number“ geben Sie den Benutzernamen Ihrer VoIP-Nebenstelle ein. Mit „Display identity“ bestimmen Sie die auf dem Bildschirm angezeigten Daten des Telefons, beispielsweise: „0511 12345/**620“. Im Webnamen können Sie eine individuelle Gerätebezeichnung eingeben, beispielsweise „dachboden“ und anschließend die „DNS name construction“ darauf einstellen – so bleibt das Telefon im Netzwerk klar erkennbar. Zuletzt setzen Sie den Haken bei „Enable ID“ und bestätigen die Parameter.

Dem Telefon fehlen jetzt nur noch die Serverdaten, bevor es einsatzbereit ist: In „Registration“ tragen Sie für die Server- und die Registrar-Adresse entweder die IP-Adresse Ihrer Fritzbox oder alternativ „fritz.box“ ein. In „User ID“ und „Password“ geben Sie die zuvor in der Fritzbox angelegten Accountdaten ein. Dann setzen Sie „Server type“ auf „other“ und bestätigen die Einstellungen mit „Submit“.



Siemens / Unify Openstage 40 HFA/SIP (G)

Das OS40 gehört zur Komfortklasse „Executive“: Es hat ein gut lesbares, beleuchtetes 5-Zoll-Display mit 240 × 128 Pixeln Auflösung. Ebenso an Bord sind dedizierte Tasten zur Einrichtung einer Rufumleitung, Weiterleitung von Gesprächen und um aufzulegen, ohne den Hörer anzuheben. Zudem sind rechts vom Bildschirm sechs Touch-Funktionstasten angebracht und es lässt sich per Key Modul erweitern.

Die Bedienung des Telefons macht auf dem großen, neigbaren Bildschirm deutlich mehr Spaß, als auf den zweizeiligen Displays der kleinen Geräte.

Trotz der besseren Ausstattung ist das OpenStage 40 mit einem Preis von 10 bis 30 Euro eines der günstigen Modelle.

Literatur

[1] Florian Klan, **Verbrüderung**, Cisco-IP-Telefone an der Fritzbox betreiben, c’t 14/2017, S. 136

Unify-Wiki und mehr

ct.de/w2du

Warten Sie, bis Ihr Telefon keine Fehlermeldung mehr anzeigt und die eingestellten Parameter erscheinen. Dann starten Sie einen Testanruf und passen gegebenenfalls die Parameter an.

Die Telefone wie auch die Fritzbox sprechen das ursprünglich von ISDN stammende Merkmal „Message Waiting Indicator“ auf IP-Basis. Darüber teilt die Fritzbox der Nebenstelle mit, wenn auf ihrem Anrufbeantworter eine Nachricht wartet. Um das Merkmal einzurichten, tragen Sie in „System“, „Features“, „Addressing“ den Host „fritz.box“ als „MW server URI“ ein. In „Voice mail number“ fehlt dann nur noch die Nummer Ihres Anrufbeantworters, beispielsweise **601.

Telefonbuch

Die Telefonbuch-Funktion hat Unify auf Unternehmenskunden ausgerichtet: Mithilfe der LDAP-Integration können die Telefone eigenständig Verzeichnisse durchsuchen und Telefonnummern anwählen. Wer einen LDAP-Server betreibt, muss ein passendes LDAP-Template nach den Vorgaben von Unify erstellen, es per FTP hochladen (ct.de/w2du) und in „Local functions“ die Einstellungen anpassen.

Ein lokales Telefonverzeichnis existiert zwar, macht jedoch wenig Spaß. In den Benutzerseiten können Sie im Bereich „Telefonbuch“ Kontakte eintragen und die Liste anzeigen lassen – jedoch nur manuell und mit nur einer Rufnummer pro Kontakt.

Die meisten Unify- und Siemens-Telefone bringen eine dedizierte Taste für den Verzeichniszugriff mit. Im Fall des OS15, des OS40 und des IP35G erkennen Sie diese an den drei horizontalen Strichen mit einem Pfeil auf der linken Seite. „Persönlich“ führt zum lokalen Telefonbuch, „Unternehmen“ ruft die LDAP-Suche auf.

Funktionstasten

Je nach Modell besitzen die VoIP-Telefone unterschiedlich viele Tasten, die man nach Wunsch mit diversen Funktionen belegen kann. Das erledigt man im Administratormenü unter „System“, „Features“, „Program keys“. Um beispielsweise eine Direktwahl anzulegen, wählt man zuerst „Selected dialling“ im Klappmenü und klickt dann auf „edit“, um die Parameter einzutragen. Benennen Sie das Label passend, um den Überblick zu behalten.

Für alle Telefone und Erweiterungsmodule mit Beschriftungseinsatz bietet Unify das „Key Labelling Tool“, das aus einer Doc-Datei mit Tabellen besteht, die auf A4-Papier die richtige Größe für den Einsatz haben (ct.de/w2du).

Da geht noch mehr

Die Unify-Telefone lassen sich dank gut umgesetztem SIP-Standard mit überschaubarem Aufwand mit Fritzboxen verknüpfen. Die Telefone, die wir beispielhaft konfiguriert haben, bieten einen deutlich größeren Funktionsumfang als hier beschrieben. Dazu gehören Belegtasten, automatische Weiterleitungen, weitere Telefonbücher und vieles andere mehr. Weitere Einzelheiten stehen in der Dokumentation von Unify, die Sie über ct.de/w2du finden. (amo) c't



DECT-VoIP-Telefone bis 100 Euro

In Firmen telefoniert man meist mit stationären VoIP-Telefonen, die per Ethernet-Kabel am LAN hängen und den Nutzer an den Schreibtisch binden. Die Schnurlos-Variante mit DECT-Funk bringt dagegen den von zuhause gewohnten Komfort ins Büro. Wir haben vier Sets bis 100 Euro getestet.

Von **Andrijan Möcker**

Festnetztelefonie spielt sowohl im privaten als auch im Unternehmensumfeld noch eine Rolle, denn Sprachqualität und Klang sind oft besser als beim Smartphone und viele Teilnehmer aus dem beruflichen Umfeld sind hauptsächlich über Festnetznummern erreichbar. Laut einer Analyse des VATM summierte sich die tägliche Festnetztelefonie 2018 in Deutschland auf im Schnitt 293 Millionen Minuten pro Tag; über Mobilfunk kommen täglich 330 Millionen Minuten zusammen.

In Router integrierte DECT-Basisstationen sind heute weit verbreitet und bieten HD-Telefonie, Telefonbuchdienste und Weiteres, das analoge Telefonie nicht leistet. Doch was, wenn der Router keine DECT-Basis hat oder im Keller stehen muss und dicke Wände die DECT-Reichweite stark verringern? Keine

Sorge, weder müssen Sie sich mit nervigem Knacken noch mit dürftigen DECT-Repeatern oder der Rückkehr zur analogen Doppelader abfinden: Viele Hersteller bieten mittlerweile DECT-VoIP-Sets, die aus einer Basis und einem Mobilteil mit Ladeschale bestehen. Für den Einsatz in kleinen Büros und daheim haben wir vier besonders günstige DECT-VoIP-Sets von Yealink, Gigaset, Panasonic und Snom unter die Lupe genommen. Alle kosteten zum Zeitpunkt des Tests zwischen 70 und 100 Euro.

VoIP-Grundlagen

Um zu verstehen, wie DECT-VoIP-Telefone arbeiten, hilft es, einige Grundlagen heutiger Festnetztelefonie zu kennen. Bis auf einige letzte Bastionen der ISDN- oder Analog-Technik, läuft heute der gesamte Telefonieverkehr im Festnetz über das Internet, daher auch VoIP genannt. Letzteres steht für „Voice over Internet Protocol“. Die VoIP-Telefonie ist einer von vielen Internet-Diensten – sie muss nicht mehr getrennt auf das Übertragungsmedium aufgebracht und umständlich gewandelt werden. Wer glaubt, noch analog zu telefonieren, weil das heimische Telefon über den bei analogen Anschlüssen üblichen Rippenstecker (TAE) im Router steckt, liegt höchstwahrscheinlich falsch: Der Router digitalisiert das analoge Signal, enkodiert es, um Bandbreite zu sparen, und schickt es über die Internetverbindung an den Telefonieserver des Anbieters.

Ein weiterer Vorteil der VoIP-Telefonie ist, dass sie über nahezu jede Internetverbindung funktioniert: Ob DSL, Mobilfunk, Koaxialkabel (DOCSIS) oder eine andere Zugangstechnik, das spielt keine Rolle mehr. Sofern die Verbindung mindestens 140 KBit/s pro Richtung befördern kann, lässt sich darüber telefonieren. Welches Gerät die Telefonieverbindung aufbaut, spielt ebenfalls keine Rolle mehr. Wenn beispielsweise dem Router die gewünschten Funktionen oder Anschlüsse fehlen, kann eine VoIP-Telefonanlage, ein Client auf einem PC, ein Smartphone oder ein anderes Gerät, beispielsweise eine DECT-VoIP-Basis, die Aufgabe übernehmen.

„VoIP“ hat sich als Kürzel für Internettelefonie etabliert, doch beide Begriffe bezeichnen lediglich die Übertragung von Sprache über Netzwerkverbindungen, nicht etwa Protokolle oder Standards. Dienste wie Skype oder Telefonie-Integrationen von Messengern wie WhatsApp, Signal oder Telegram sind ebenfalls VoIP-Dienste, die große Ähnlichkeit mit denen der klassischen Telefonie haben, aber damit nicht kompatibel sind. Das Session-Initiation-Protocol (SIP) ist heute weltweiter Standard für rufnummernbasierte Internettelefonie. SIP-Telefone, zu denen auch die getesteten DECT-VoIP-Telefone gehören, weisen deshalb eine hohe Kompatibilität mit Anbietern weltweit auf und können oft sogar mehrere SIP-Konten gleichzeitig nutzen. Das ermöglicht beispielsweise, sich aus dem Homeoffice mit der Cloud-Telefonanlage des Arbeitgebers zu verbinden oder zusätzliche Festnetznummern bei anderen Anbietern zu buchen – so kann man sich im Ausland aufhalten und von dort mit Anschlüssen in Deutschland zum hiesigen Inlandstarif telefonieren.

Codecs bestimmen bei digitalen Tonübertragungen die Sprachqualität und Signalbandbreite. Heute sind vor allem G.711, G.726 und G.722 verbreitet. Die ersten beiden bieten die Bandbreite und Sprachqualität einer typischen analogen Leitung beziehungsweise eines GSM-Gesprächs, also 3,1 KHz (300 Hz bis 3,4 KHz). G.722 dürfte vielen als „HD Voice“ oder HD-Telefonie bekannt sein. Dieser Codec bietet fast 7 KHz Bandbreite, sodass das Gespräch deutlich natürlicher klingt als mit G.711 und G.726. HD-Telefonie funktioniert heute in und zwischen vielen Festnetzen sowie in vielen Mobilfunknetzen. Alle Geräte im Test bringen den benötigten Codecs mit.

Einrichtung

Bis auf eine Ausnahme sind alle DECT-VoIP-Sets betriebsbereit und enthalten das erforderliche Zubehör. Lediglich beim Snom M215 SC fehlt das Netzteil für die Basisstation. Wie die Basen von Yealink und Panasonic lässt sie sich per Power-over-Ethernet (IEEE 802.af) speisen, also über die Netzwerkleitung. Alternativ verkauft Snom ein passendes Netzteil.

Damit die Telefonie funktioniert, muss die Basis mit Serveradressen und Zugangsdaten für den VoIP-Dienst versorgt werden. Unter den Testgeräten enthielt nur das Gigaset CL690A SCB einen Einrichtungsassistenten im Mobilteil. Der lohnt sich, wenn es für den verwendeten Anbieter ein vordefiniertes Profil gibt und die Serveradressen nicht mehr eingetragen werden müssen. Alle anderen Systeme kann man nur über ein Webinterface konfigurieren, das auf der Basisstation läuft. Die IP-Adresse der Basis findet man in der Regel über die Weboberfläche des Routers oder mit einem IP-Scanner. Bei der Einrichtung kommt man nicht drumherum, sich mit den Begrifflichkeiten der SIP-Telefonie zu befassen. Für die meisten Modelle gibt es jedoch Hinweise im Netz, um schnell zum Ziel zu kommen.



Snom M215 SC

Snom macht am Anfang den gleichen Fehler wie Panasonic: Im Karton gibts eine Schnellstartanleitung, die Mobilteil und Basis grob erklärt. Ein Hinweis auf eine Dokumentation fehlt – nicht nur auf dem Papier, sondern auch auf der Produktwebsite bei Snom. Unverständlich, denn bemüht man eine Suchmaschine, findet man die PDFs im Snom-Wiki und die Anleitungen sind gut, wenngleich nur englisch.

Einmal darin angekommen, überzeugt das Webinterface mit leichter Konfiguration und übersichtlicher Sortierung. Vorbildlich: Verlässt man das Webinterface nach der Konfiguration, ohne das Administratorkennwort zu ändern, nerven die eingebuchten Mobilteile zu Recht regelmäßig mit einem Hinweis.

Das Snom M215 SC ist aufs Erforderliche beschränkt: Das Mobilteil ist robust, das Display gut lesbar und die Menüführung klar verständlich. Alle Tasten sind klar separiert, haben einen angenehmen Rastpunkt und sind so auch mit größeren Händen gut zu bedienen.

- **leicht zu konfigurieren**
- **zweckorientiert**
- **robust**
- **Dokumentation versteckt**

Preis: 90 Euro



Yealink W52P

Die Schnellstartanleitung des Yealink W52P irritiert zunächst, denn die deutschen Beschreibungen enthalten die englische Menüführung des Mobilteils, obwohl es seine Menüs auch in Deutsch anzeigen kann. Der Eindruck, dass die Anleitung eher Englisch als Menüsprache empfiehlt, ist leider nicht ganz unberechtigt: Sowohl im Webinterface als auch auf dem Mobilteil ist die Übersetzung der Menüpunkte dürftig. Besonders bei der Konfiguration auf der Basis ist das irritierend, denn einige Menüpunkte entsprechen nicht den üblichen Bezeichnungen oder sind gar nicht übersetzt.

Die Bedienung des Mobilteils ist etwas umständlich: Die Wähltasten sind mit 4 × 10 mm vergleichsweise klein und insbesondere das Steuerkreuz, das nur drei Millimeter Druckfläche bietet, in Menüs aber unerlässlich ist, bremst die Navigation. Menschen mit größeren Fingern werden das W52P nicht ohne Schwierigkeiten bedienen können und sollten dann eher zum Snom greifen.

Die Klangqualität des Yealink kann indes überzeugen: Besonders die Hörkapsel tönt vergleichsweise kräftig, der Lautsprecher ausreichend, um gelegentlich freizusprechen.

- **gute Anleitung**
- **günstigstes Modell**
- **Übersetzung verbesserungswürdig**
- **Tasten zu klein**

Preis: 80 Euro



Panasonic KX-TGP600CE

Dem KX-TGP600CE merkt man seine Ausrichtung auf Geschäftskunden mit eigenem Administrator sofort an: Im Karton steckt nur eine einfache Anleitung zum Koppeln des Mobilteils mit der Basis. Das Webinterface muss am Handset über ein Untermenü aktiviert werden: Diese Lösung liefert aber ein 178-seitiges englisches Dokument, gut versteckt in den Supportdownloads. HD-Voice und viele weitere Funktionen kann man nur über eine auf einem Webserver abgelegte Konfigurationsdatei aktivieren – diese ist allerdings gleich auf 400 Seiten beschrieben. Eine erweiterte Schnellstartanleitung und ein neues Webinterface mit allen Parametern würde dem KX-TGP600CE gut zu Gesicht stehen.

Davon abgesehen liefert Panasonic ein solides Gesamtpaket, das sich preisgünstig mit weiteren Geräten ergänzen lässt. Alleine die mitgelieferte Basis bietet acht schmalbandige beziehungsweise vier HD-Sprachkanäle gleichzeitig. Eventuell erforderliche Repeater bietet Panasonic für rund 90 Euro an. Das mitgelieferte Mobilteil liegt gut in der Hand, lässt sich leicht bedienen, liefert gut verständliche Sprachsignale und trägt sich dank Gürtelclip komfortabel.

- **gute Erweiterbarkeit**
- **viele gleichzeitige Gespräche**
- **umständliche Einrichtung**
- **knappe Anleitung**

Preis: 85 Euro



Gigaset CL690A SCB

Das CL690A SCB imponiert durch leichte Einrichtung: Die Schnellstartanleitung beschreibt die Installation in einsteigerfreundlicher Form. Außer Mobilteil, Ladestation, Basis und den Netzteilen liegt ein Netzwerk- sowie ein klassisches Telefonkabel bei. Jedoch fehlt ein Hinweis, dass das Telefonkabel nur selten erforderlich ist und die Tonqualität negativ beeinflusst.

Die VoIP-Einrichtung hat Gigaset komplett auf dem Mobilteil untergebracht. Ein Assistent offeriert eine lange Liste mit VoIP-Anbietern, sodass nur noch die persönlichen Zugangsdaten einzugeben sind. Alternativ gibt es ein Webinterface zur Einrichtung. Hier hat Gigaset aber etwas Updatebedarf: Kein IPv6, kein HTTPS, nur eine vierstellige Pin zur Sicherung und diese auch noch voreingestellt auf 0000. Auch SIP-Verschlüsselung und SRTP fehlen.

In puncto Tonqualität hinterlässt das CL690A einen sehr guten Eindruck – sowohl die Hörmuschel als auch der Lautsprecher klingen angenehm und sind für normal Hörende weder zu laut, noch zu leise.

- **sehr einsteigerfreundlich**
- **großes, gut lesbares Display**
- **umfangreiche Zusatzdienste**
- **keine Telefonieverschlüsselung**

Preis: 90 Euro

Unabhängige VoIP-Anbieter stellen ihre Zugangsdaten in der Regel im Internet zur Verfügung oder in gedruckten Dokumentationen. In Deutschland sind Telekommunikationsanbieter seit der Einführung der Routerfreiheit im Jahr 2016 verpflichtet, alle für den Zugang erforderlichen Daten herauszurücken – das schließt die VoIP-Zugangsdaten ein.

Wenn möglich, sollten Sie die Telefonie gleich verschlüsselt einrichten. Klappt HD-Telefonie nicht auf Anhieb, hilft meist ein Blick in die Codec-Einstellungen im Webinterface. Hier sollte G.722 aktiviert und an oberste Stelle der Prioritätenliste gerückt werden.

Schlaue Telefone

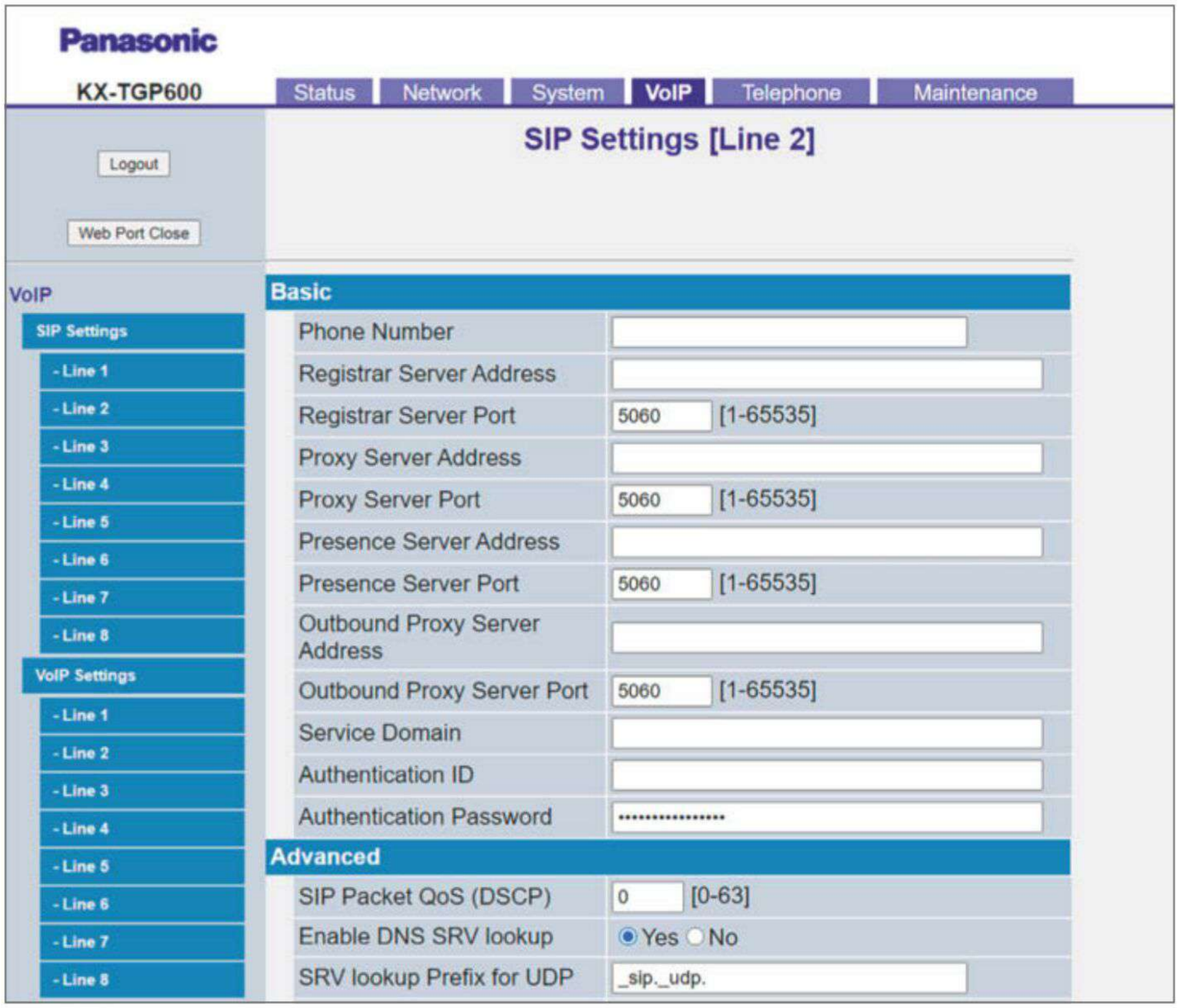
Alle vier Testkandidaten haben neben klassischer Telefonie auch Zusatzfunktionen an Bord: Bei Yealink, Panasonic und Snom ist LDAP als verbreiteter Verzeichnisdienst dabei, über den das Telefonbuch Daten komfortabel von einem Server beziehen kann. Optional fragen die Telefone bei Eingehenden Anrufen, ob ein Kontakt vorhanden ist, und zeigen die Daten auf dem Display. Alle drei lesen außerdem XML-formatierte Telefonbücher, wenn auch im jeweils hauseigenen Format. Kontakte lassen sich aber bei allen auch klassisch ohne Server im lokalen

DECT-VoIP-Telefone

Modell	W52P	CL690A SCB	M215 SC	KX-TGP600CE
Hersteller	Yealink	Gigaset	Snom	Panasonic
Testfirmware (Basis / Handset)	25.81.0.60 / 26.81.0.50	42.256 / 119.13	2.10.32.4da7 / 1.38.65	13.002 / 03.08.004
Hardware				
Maße (Mobilteil inkl. Clip / Basis)	4,9 × 14,4 × 2,5 cm / 15,5 × 11,5 × 5 cm	5,3 × 15,9 × 2,2 cm / 13,2 × 10,7 × 4,6 cm	4,8 × 17,4 × 2,7 cm / 4,4 × 15,5 × 11,7 cm	5,4 × 15,7 × 3 cm / 12 × 8,9 × 4,5 cm
Gürtelclip	–	–	✓	✓
Display	1,8 Zoll, Farbe, 120 × 160 Pixel	2,4 Zoll, Farbe, 240 × 320 Pixel	1,9 Zoll, monochrom, 96 × 65 Pixel	1,8 Zoll, Farbe, 120 × 160 Pixel
Akku	2 × AAA NiMH, 800 mAh	2 × AAA NiMH, 750 mAh	AAA-Akkupack (2,4 V, 550 mAh, Molex 5264-2P)	2 × AAA NiMH, 630 mAh
Power over Ethernet (Basis)	✓ / IEEE 802.3af	–	✓ / IEEE 802.3af	✓ / IEEE 802.3af
Leistungsaufnahme (Basis)	1,8 W	1,3 W	1,7 W	2,3 W
Telefonie				
Mobilteile pro Basis	5	6	6	8
SIP-Konten	5	6	6	8
gleichzeitige Gespräche	4	2	4	8 (4 mit HD-Telefonie)
SIP-TLS / SRTP	✓ / ✓	– / –	✓ / ✓	✓ / ✓
Codecs	iLBC, G.722, 711, 723, 729	G.722, 711, 726, 729	iLBC, G.722, 711, 726, 729	G.722, 711, 729
integr. Anrufbeantworter	–	✓	–	–
Gesprächsstunden (laut Hersteller)	5–10	14	7	8
Software				
IPv4 / IPv6	✓ / ✓	✓ / –	✓ / ✓	✓ / ✓
Webinterface	✓	✓	✓	✓
Telefonbücher	intern, LDAP, XML-HTTP(S)	intern, „Das Telefonbuch“	intern, LDAP, XML-HTTP(S)	intern, LDAP
TB-Import	XML, CSV	VCF	XML, CSV	CSV
Monitoring	Syslog	–	Syslog	Syslog, SNMP
Bewertung				
Einrichtung	⊕	⊕⊕	⊕	○
Funktionsumfang	⊕	⊕	⊕⊕	⊕⊕
Klangqualität	⊕⊕	⊕⊕	⊕⊕	⊕⊕
Klangqualität (Lautsprecher)	⊕	⊕	⊕⊕	⊕
Preis	80 €	90 €	90 €	90 €

✓ vorhanden – nicht vorhanden ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht

Die Konfiguration von DECT-VoIP-Telefonen erfolgt größtenteils per Webinterface, wie hier bei Panasonic. Nur das Gigaset CL690A brachte einen Assistenten zur VoIP-Einrichtung auf dem Mobilteil mit.



Telefonbuch eintragen oder über die Weboberfläche wahlweise als CSV, VCF oder XML importieren.

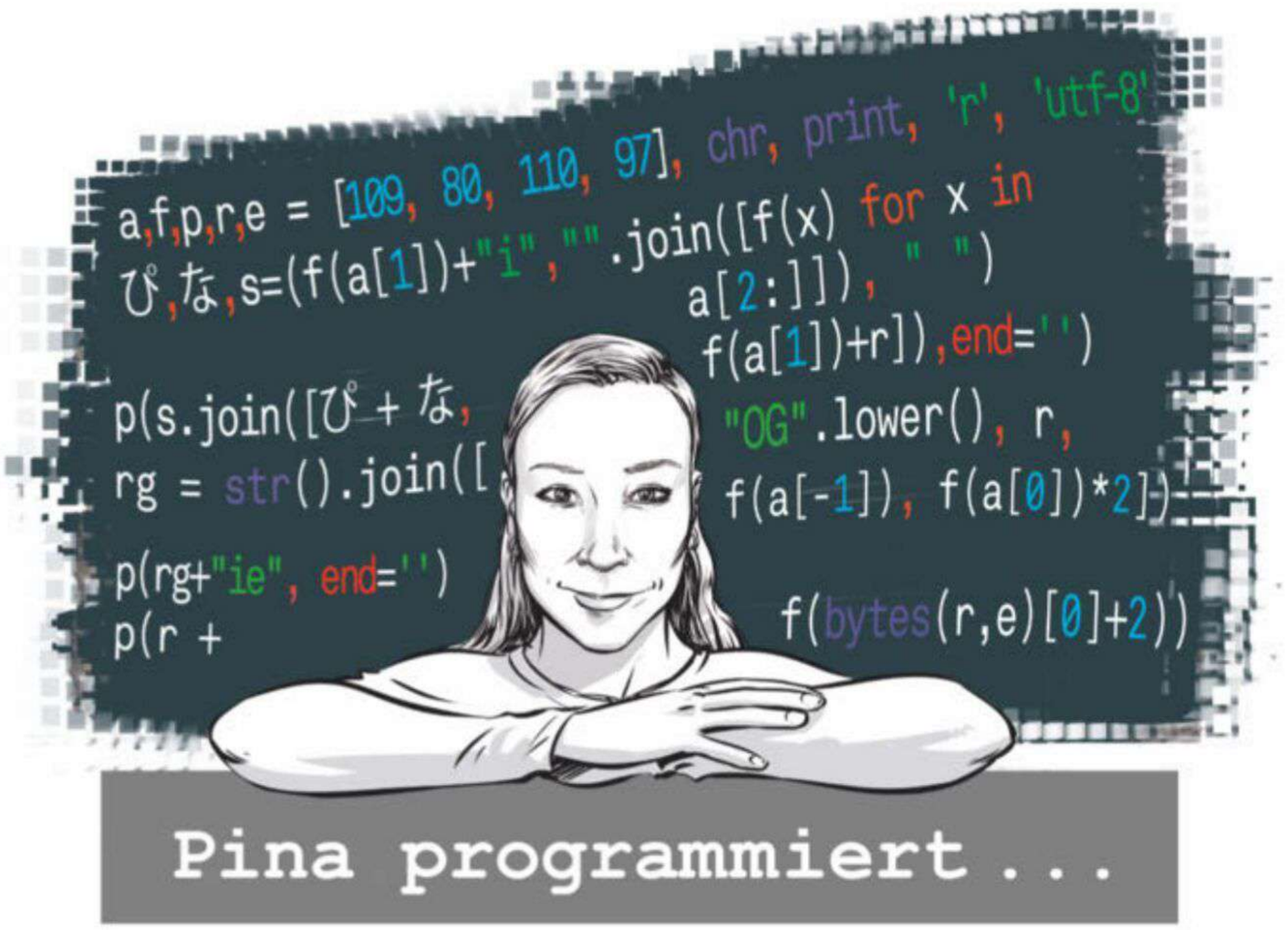
Gegenüber den eher schlichten Business-Modellen bietet das Gigaset einen fast schon übergroßen Funktionsumfang: Das Online-Verzeichnis „Das Telefonbuch“ ist integriert und wird bei Anrufen automatisch durchsucht. Besonders praktisch sind die umfangreichen Listen zum Sperren diverser Rufnummerngassen, darunter für Servicenummern die mit 0180 beginnen, für Mobilfunknetze, Ortsvorwahlen etc. Das kann sogar automatisch erfolgen: Gigaset kooperiert mit dem Bewertungsdienst tellows, sodass man von anderen Nutzern als störend bewertete Nummern automatisch blockieren lassen kann. Zusätzlich gibts allerhand Infodienste, die stark an die Featurephones von vor 10 bis 15 Jahren erinnern: Das CL690A SCB kann die Wettervorhersage abrufen, eBay-Auktionen beobachten, Text übersetzen, E-Mails versenden und Horoskope anzeigen. Vieles wirkt jedoch eher verspielert als wirklich notwendig – besonders aus der Sicht geschäftlicher Nutzer.

Weitere Infos

ct.de/wcr5

Fazit

Insgesamt taugen alle getesteten Geräte für den Heim- und Unternehmensbetrieb. Das Snom M215 SC bietet dabei, abgesehen von der schwer zu findenden Dokumentation, das beste Gesamtpaket, wenn ein leicht zu konfigurierendes VoIP-Telefon ohne Schnickschnack gesucht ist. Das Yealink W52P ist ungefähr gleichauf, könnte aber eine neue Übersetzung des Webinterfaces und der Telefonmenüs vertragen. Panasonics Set kann sich ebenfalls sehen lassen, doch bei der Dokumentation, deren Zugänglichkeit und der Konfiguration könnte der Hersteller nachbessern, um die Einrichtung zu erleichtern. Gigaset liefert mit Abstand die einfachste Einrichtung, was gerade Privatkunden ansprechen dürfte. Die fehlende Verschlüsselung und die lasche Absicherung des Webinterfaces sind jedoch nicht mehr zeitgemäß. Doch wenn die Hardware der Box das hergibt, braucht es vielleicht nur ein Update, um entsprechend nachzurüsten. (amo) c't



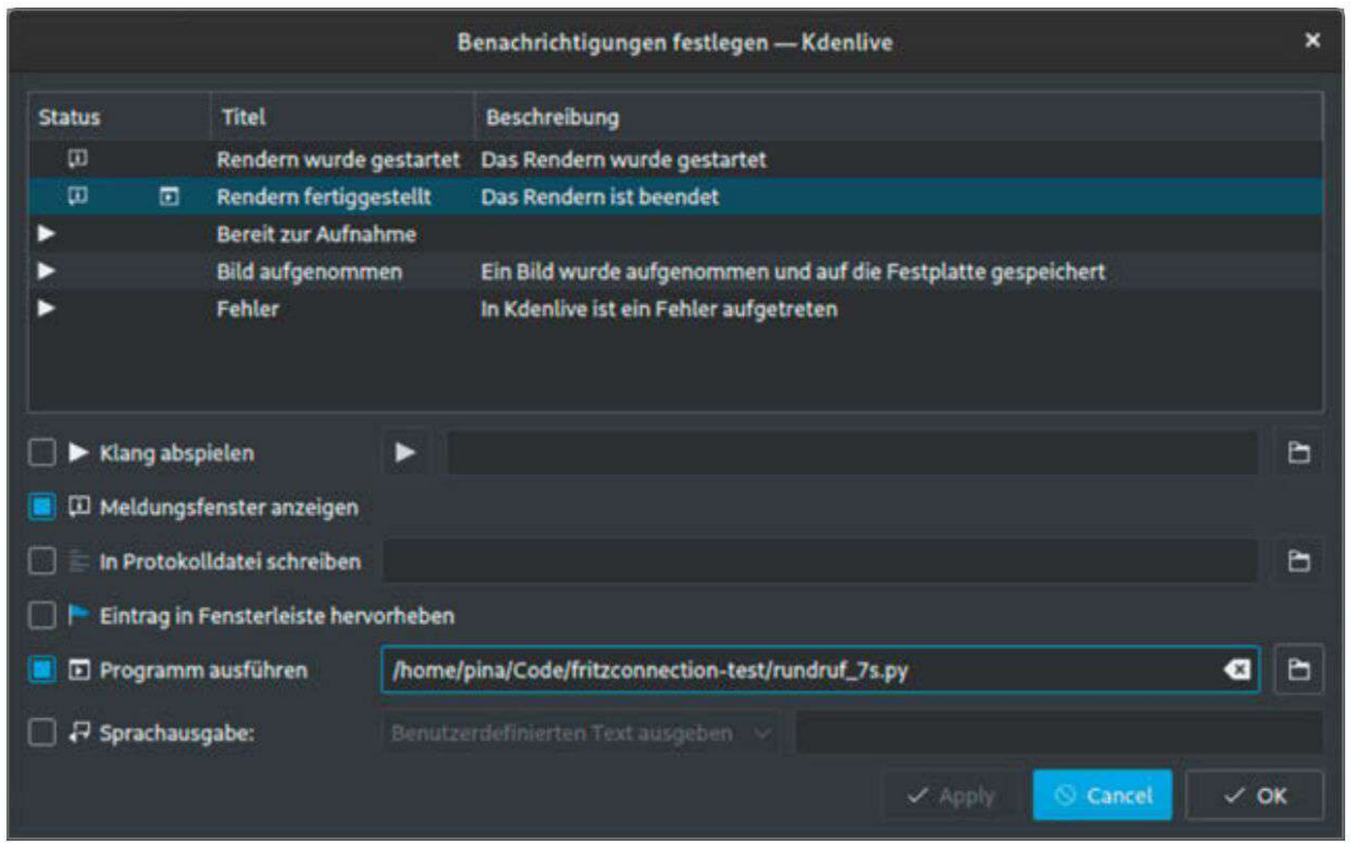
Telefon klingeln lassen mit Fritzconnection

Über das TR-064-Protokoll kann man der Fritzbox übers Netzwerk Befehle geben. Dank der Python-Bibliothek fritzconnection wird die Fritzbox-Fernsteuerung per Skript zum Spaziergang. Zum Beispiel kann die Fritzbox einen Rundruf absetzen, wenn der Videoschnitt beendet ist.

Von **Pina Merkert**

Nach dem Videoschnitt beginnt das Warten. Das ist beim Rendern im Videoschnittprogramm Kdenlive nicht anders als bei anderen. Während der Rechner Bilder durch den Videoencoder schiebt, bietet sich eine Pause abseits vom Bildschirm an, da der Computer beim Rendern nicht mehr sonderlich flüssig reagiert. Die Zwangspause muss aber nicht länger werden als nötig. Deswegen wäre es schön, der angestrengte Rechner würde hörbar Bescheid geben, sobald er mit dem Rendern und Speichern fertig ist.

Klingeln im ganzen Haus die Telefone, ist das ein gut hörbares Signal. Andrijan Möcker hatte für ein c't-Bastelprojekt mit einem WLAN-fähigen ESP8266-Mikrocontroller an der Türklingel mal gezeigt, wie dieser über das TR-064-Protokoll der Fritzbox Bescheid gibt, damit die per Rundruf alle Telefone klingeln lässt [1]. Das Schöne daran: Die Telefone



Unter „Einstellungen/Benachrichtigungen festlegen“ kann man Kdenlive anweisen, ein Skript auszuführen, sobald der Render-Job abgeschlossen ist. Trägt man dort das beschriebene Python-Skript ein, klingeln die Telefone, sobald die Videodatei fertig ist.

klingeln beim Rundruf mit einem anderen Ton als bei menschlichen Anrufern, sodass man das Signal als Benachrichtigung erkennt und nicht verwirrt „Hallo, wer ist da?“ ins nächste Telefon fragt.

Fritzconnection

Einen Mikrocontroller braucht man für eine Kdenlive-Benachrichtigung nicht. Mit der Python-Bibliothek `fritzconnection` spricht der Rechner ohne viel Mühe das TR-064-Protokoll (siehe ct.de/weyc). Die Bibliothek ist mit `pip` ruckzuck installiert, mit `sudo` davor auf allen Linuxen systemweit:

```
sudo pip install fritzconnection
```

Das Skript für einen Rundruf von sieben Sekunden ist so kurz, dass es vollständig in diesen Artikel passt:

```
#!/usr/bin/python
from time import sleep
from fritzconnection import (
                        FritzConnection)
fc = FritzConnection(
             address='192.168.178.1',
             user="klingel",
             password="ctis2cool4all")
fc.call_action("X_VoIP1",
               "X_AVM-DE_DialNumber",
               arguments={
    "NewX_AVM-DE_PhoneNumber": "**9"})
sleep(7)
fc.call_action("X_VoIP1",
               "X_AVM-DE_DialHangup")
```

Markiert man die Datei `rundruf_7s.py` mit `chmod +rwxrwxrx rundruf_7s.py` als ausführbar, sucht die Shell in der ersten Zeile nach dem Programm, das den Rest interpretiert (ein Shebang – kurz für „Hash and Bang“, wegen der Zeichenfolge `#!`, hinter der der Pfad zum Interpreter steht). Die Imports in den folgenden Zeilen laden lediglich die `sleep()`-Funktion aus der Python-Klasse `time` und die Klasse `FritzConnection`. Sie kümmert sich um die Kommunikation mit der Fritzbox über TR-064. Zeile 5 initialisiert die Klasse mit der IP-Adresse der Fritzbox, einem Benutzernamen und einem Passwort. Die Instanz von `FritzConnection` landet in der Variablen `fc`. Wie Sie den Benutzer und die Rundruf-Funktion in der Fritzbox einstellen, können Sie in [1] nachlesen – das führt hier zu weit.

Rundruf

Mit `fc.call_action()` gibt das Skript der Fritzbox den Befehl zum Rundruf. Der erste Parameter enthält den Service, der zweite den Befehl. Parameter für den Befehl steckt man in ein Dictionary (ein Datentyp aus Key-Value-Paaren) und übergibt das als optionalen Keyword-Parameter `arguments`. Dank seiner allgemeinen Struktur können Sie mit der Funktion `fc.call_action()` ziemlich beliebige TR-064-Befehle absetzen. Dabei funktionieren nicht nur die im TR-064-Standard definierten Befehle, sondern auch die Fritzbox-spezifischen Erweiterungen von AVM (siehe ct.de/weyc). Mit fritzconnection können Sie Ihre Fritzbox daher weitgehend per Python-Skript konfigurieren.

Das Skript dreht nach dem Rundruf an die Nummer `**9` mit `sleep(7)` für sieben Sekunden Däumchen. Diese Zeitspanne reicht, damit die Telefone zweimal klingeln. Je nachdem, welche Telefone Sie genau in Ihrem Haushalt einsetzen und wie oft diese klingeln sollen, passen Sie die Zeitspanne in Ihrem Skript an Ihre Bedürfnisse an. Danach legt das Skript mit `fc.call_action()` und dem Befehl `"X_AVM-DE_DialHangup"` wieder auf. Fertig! (pmk) c't

Literatur

[1] Andrijan Möcker, **ESP-Überallklingel**, IoT-Klingel mit Fritzbox-Anbindung, c’t 17/2018, S. 142

Dokumentation

ct.de/weyc



Bild: Andreas Martini

Mobilfunk-Gateway

Größere Fritzboxen lassen sich zu GSM-Gateways und weiter zu VoIP-Least-Cost-Routern aufrüsten. So sparen sie Geld und bringen Mobilfunksignale auch an unversorgte Stellen eines Hauses. Als universeller Vermittler macht sich dabei ein Raspberry Pi nützlich.

Von **Sebastian Piecha, Dušan Živadinović**

Wer viel telefoniert, hat mehrere gute Gründe, Fritzboxen zu Mobilfunk-Gateways aufzurüsten: Man kann das Gateway mit der integrierten Festnetztelefonie zu einem Least-Cost-Router kombinieren, der Gespräche immer auf den günstigsten Weg leitet. Denn viele Telefonie-Flatrates sind lückenhaft, sodass man unversehens draufzahlt, wenn man etwa per Festnetztelefon eine Mobilfunknummer anruft. Wie man Least-Cost-Funktionen aufsetzt, hängt von den jeweiligen Verträgen ab. Die Funktion lässt sich in Fritzboxen mit eingebauter Telefonanlage im Menü Telefonie / Wahlregeln / Neue Regel leicht einrichten.

Ein weiterer Grund für ein Mobilfunk-Gateway kann eine in Häusern unzureichende Mobilfunkabdeckung sein. Eigentlich hat die Mobilfunkbranche das Problem gelöst: Es gibt winzige Mobilfunkzellen (Femto-Zellen), die ein Haus oder eine Wohnung abdecken und sich über die Internetleitung ins Mobilfunknetz einbuchen. Femto-Zellen haben sich aber nicht durchgesetzt. Alternativ kann man in modernen Smartphones das Wi-Fi-Calling für Voice over

LTE (VoLTE) aktivieren, wobei Mobilgespräche per WLAN zum Router und dann wiederum über die Internetleitung laufen. Das funktioniert prima, aber die WLAN-Reichweite setzt der Funktion in Gebäuden enge Grenzen (je nach Bausubstanz 10 bis 15 Meter) – wenn man nicht mit einem Mesh-WLAN-System und Repeatern nachhilft.

Läuft die Fritzbox als Mobilfunk-Gateway, kann man für Gespräche über die Mobilnummer(n) DECT-Schnurlos-Telefone einbinden und deren höhere Reichweite nutzen (in Gebäuden 40 Meter, mit Glück 50 Meter).

Fritzboxen bringen die wesentlichen Voraussetzungen für den Bau eines Gateways mit. Im Prinzip braucht man als Ergänzung nur einen GSM/UMTS-Stick mit passender SIM-Karte. Jedoch ist die Methode in die Jahre gekommen und nicht mehr praktikabel: Geeignete Sticks mit aktiviertem Circuit Switched Voice (CSV) waren schon zur GSM- und UMTS-Blütezeit selten. Wegen SIM- oder Net-Locks bauen manche obendrein keine Sprachverbindungen auf. Auch saugen sie relativ viel Strom, was in Kombination mit USB-Verlängerungen zu instabilem Betrieb der Fritzbox führen kann. Die Statusabfrage von Mobilfunkverträgen ist auch nur per Mobiltelefon möglich. Eine Warn-SMS über fehlendes Guthaben versandet auf der SIM-Karte des Sticks.

Wer keine Kommandozeilen-Allergie hat, kann an einem freien Nachmittag ein deutlich flexibleres Gateway aus einem ausrangierten Smartphone, einem Raspberry Pi und einem einfachen Bluetooth-USB-Adapter zusammensetzen. Raspi und Smartphone können abgesetzt von der Fritzbox für bestmöglichen Empfang in Fensternähe stehen. Das Smartphone wickelt alle Mobiltelefonate ab, egal ob GSM, UMTS oder VoLTE. SMS-Nachrichten kann man wie üblich auf dem Smartphone lesen und schreiben.

Das Konzept lässt sich zu einem Multi-SIM-Szenario erweitern, bei dem drei (oder mehr) SIM-Karten unter derselben Rufnummer in verschiedenen Geräten laufen: im Smartphone, das man mit sich führt, in der Freisprechanlage des Autos, im Mobilfunk-Gateway … Eingehende Anrufe klingeln auf allen Geräten. Nimmt man den Ruf mit einem davon an, stellen die übrigen das Klingeln ein. Eingehende Rufnummern landen in den Anruferlisten aller Geräte. So kann man auch Rückrufe per DECT-Telefon unter der Mobilnummer führen und natürlich übliche Mobiltelefonate, also ohne dass vorher jemand angerufen hat. Wer möchte, kann im Gateway mehrere Mobilfunknummern mit mehreren Handys und BT-Dongles einrichten.

Gateway-Voraussetzungen

Für das Gateway benötigen Sie eine Fritzbox mit integrierter Tk-Anlage, also eine mit TAE-Anschlüssen. Wir haben die Modelle 7390 und 7580 verwendet. Außerdem sind erforderlich: ein DECT- oder Tischtelefon, ein Raspberry Pi mit aktuellem Raspbian, dazu ein USB-Bluetooth-Adapter und ein Smartphone mit Bluetooth. Gut geeignet, weil gebraucht schon für rund 50 Euro zu bekommen, sind beispielsweise das Samsung Galaxy S5 oder Google Nexus 5.

Außerdem haben wir am Gateway die iPhone-Modelle 6, 8, 8plus und 10 sowie die Android-Smartphones Essential PH1, Google Pixel 3a und Xiaomi Mi Mix 2S mit LineageOS erfolgreich betrieben. Anstatt eines Smartphones könnte man auch alte GSM-

Hat man in der Fritzbox ein Mobilfunk-Gateway eingerichtet, lässt sich über Wählregeln leicht festlegen, dass Anrufe ins Mobilfunknetz grundsätzlich darüber zu laufen haben.



oder UMTS-Handys einsetzen. Doch das Protokoll zur Bluetooth-Kopplung wurde vor Jahren umfassend geändert, sodass es ungewiss ist, ob das Pairing klappt. Bei uns scheiterte die Kopplung mit dem vor vielen Jahren verbreiteten Nokia 6310i. Älteren Kompatibilitätslisten kann man entnehmen, dass sich etliche GSM- und UMTS-Handys nur eingeschränkt eignen (siehect.de/w6wv).

Ein wichtiges Element ist der USB-Bluetooth-Adapter: Leider eignet sich der im Raspi 3B, 3B+ und 4 integrierte Bluetooth-Chip nicht, möglicherweise wegen ungünstiger Hardware-Anbindung (ct.de/w6wv). Er überträgt Sprachdaten derart verzerrt, dass man den Gesprächspartner kaum versteht. Verschwenden Sie also keine Zeit darauf.

Wir haben die Adapter Asus USB-BT400, Renkforce 1491408 (10 m Reichweite), Renkforce 1483951 (50 m Reichweite), Trendnet TBW-106UB, Vivanco 30447 und IOgear GBU521W6 erfolgreich eingesetzt. Manche dieser Sticks sind schon für unter 10 Euro erhältlich. Bluetooth-Adapter mit Chips von Cambridge Silicon Radio funktionierten ohne Weiteres (z. B. die beiden Renkforce-Sticks). Der IOgear braucht wie der Asus und andere Sticks, die mit Broadcom-Chips ausgerüstet sind, etwas Nacharbeit. Ob das bei Ihrem Adapter der Fall ist, bringt folgender Befehl ans Licht:

```
dmesg | grep -i bluetooth | grep -i firmware
```

Wenn in der Ausgabe etwas wie „failed with error -2“ steht, fehlt in der Regel die Firmware für den Broadcom-Chip. Eine typische Folge ist, dass sich zwar das Smartphone koppeln lässt, aber keine Sprachdaten durchgehen – die Leitung bleibt stumm.

Zum Glück sind etliche Firmware-Dateien für ältere Broadcom-Adapter auf GitHub erhältlich (ct.de/w6wv). Lesen Sie die genaue Bezeichnung des Broadcom-Adapters aus der `dmesg`-Ausgabe aus (z. B. BCM207 02A1-0a5c-21e8.hcd für den IOGear GBU521W6). Laden Sie die Datei mit genau dieser Bezeichnung von GitHub und bringen Sie sie in den Ordner `/lib/firmware/brcm/`. Starten Sie den Raspi neu oder trennen Sie den Stick für einige Sekunden vom Raspi und stecken Sie ihn dann wieder an. Danach sollte `dmesg` keinen Fehler mehr melden und der Broadcom-Adapter sollte Sprachsignale übertragen.

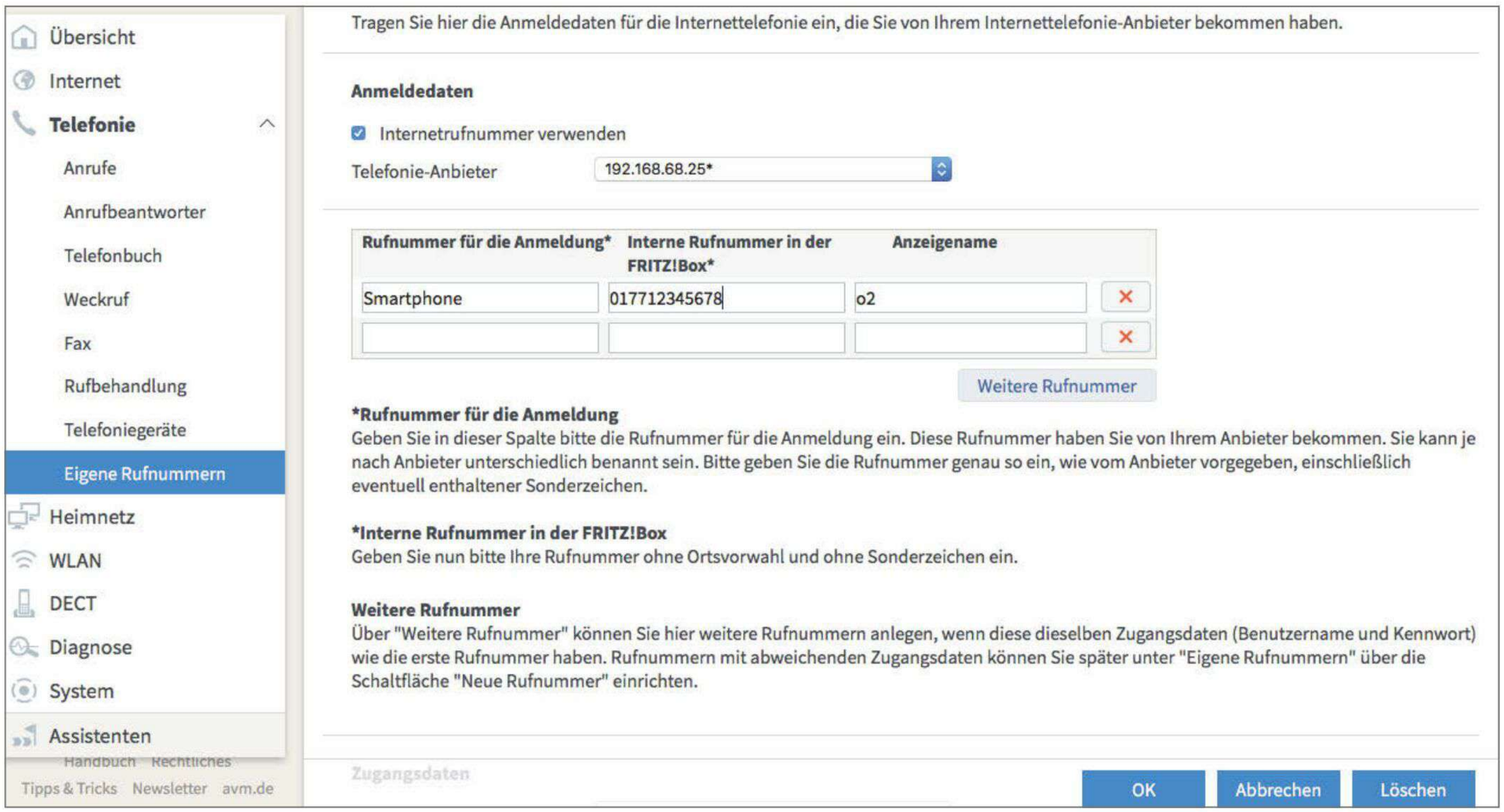
Wenn die Hardware komplett ist, koppeln Sie den Raspi per Ethernet-Kabel an die Fritzbox und stecken Sie eine SIM-Karte in das Smartphone. Für SIMs im Nano-Format sind bei älteren Smartphones Adapter auf das Micro- oder Mini-Format erforderlich. Stellen Sie sicher, dass die Mobiltelefonie funktioniert.

Asterisk installieren

Im Mobilfunk-Gateway hat die Tk-Anlage Asterisk zwei Rollen: Gegenüber der Fritzbox verhält sie sich

```
~ — pi@nero: ~ — 80×23 — ⌥⌘1
[[NEW] Device 10:CD:B6:04:A8:5D Essential Phone                    ]
 Request confirmation
[[agent] Confirm passkey 645207 (yes/no): yes                      ]
 [CHG] Device 10:CD:B6:04:A8:5D Modalias: bluetooth:v00E0p1200d1436
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001105-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 0000110a-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 0000110c-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 0000110e-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001112-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001115-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001116-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 0000111f-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 0000112d-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 0000112f-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001132-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001200-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001800-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D UUIDs: 00001801-0000-1000-8000-00805f9b34fb
 [CHG] Device 10:CD:B6:04:A8:5D ServicesResolved: yes
 [CHG] Device 10:CD:B6:04:A8:5D Paired: yes
 [CHG] Device 10:CD:B6:04:A8:5D ServicesResolved: no
 [CHG] Device 10:CD:B6:04:A8:5D Connected: no
 [bluetooth]#
```

Eine Handvoll Befehle genügen, um ein Smartphone per Bluetooth an den Raspi anzukoppeln. Jedoch sollte man für das Mobilfunk-Gateway nicht den internen Blutooth-Chip verwenden.



Sind Raspi und Asterisk konfiguriert, richtet man das Gespann in der Fritzbox als SIP-Anbieter ein.

wie ein SIP-Anbieter. Gegenüber dem Handy, an das sie per Bluetooth ankoppelt, verhält sie sich wie ein Headset. Damit die Fritzbox den SIP-Dienst der Asterisk-Tk-Anlage zuverlässig findet, weisen Sie dem Raspi in der Fritzbox eine feste IP-Adresse zu (Menü „Heimnetz / Netzwerk / Raspi / Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“). Installieren Sie die für Asterisk benötigten Pakete:

```
sudo apt update && sudo apt install↵
↳ asterisk asterisk-mobile bluez
```

Das Paket asterisk-mobile enthält die Module zur Bluetooth-Kopplung an das Smartphone. Falls Sie einen Raspi mit eingebautem Bluetooth verwenden (Modell Pi 3B, 3B+ und 4), lassen Sie den Bluetooth-Stick zunächst weg und identifizieren Sie erst mal den internen Adapter, um ihn fortan sicher meiden zu können:

```
sudo hciconfig
```

In der Ausgabe sollte nur ein Host-Controller-Interface aufgeführt sein, nämlich hci0. Merken Sie sich dessen MAC-Adresse. `hciconfig` gibt auch an, über welche Schnittstelle ein Blauzahn im System hängt. Beim integrierten Blauzahn ist das der UART-Port (Universal Asynchronous Receiver Transmitter), bei den übrigen USB.

Stecken Sie nun den ersten Bluetooth-USB-Stick an und geben Sie `hciconfig` erneut ein. Raspbian weist nun dem neuen Adapter das Host-Controller-Interface hci0 zu und dem internen hci1. Notieren Sie sich den Schnittstellennamen und die MAC-Adresse des externen Adapters. (z. B. hci0, 00:1B:DC:00:11:22). Aktivieren Sie den Kopplungsmodus Secure Simple Pairing und die Bluetooth-Sichtbarkeit:

```
sudo hciconfig hci0 sspmode 1
sudo hciconfig hci0 piscan
```

Im nächsten Schritt wird in der `bluetoothctl`-Konsole der Haupt-Bluetooth-Adapter (default) eingestellt, auf

den sich spätere Befehle beziehen. Lassen Sie sich dafür zunächst alle verfügbaren Adapter anzeigen und stellen Sie dann den externen Adapter ein (im Beispiel ist das 00:1B:DC:00:11:22):

```
sudo bluetoothctl
list
select 00:1B:DC:00:11:22
```

Schalten Sie im Smartphone das Pairing ein (iPhone: Einstellungen / Bluetooth, Android: Einstellungen / verbundene Geräte / Neues Gerät koppeln). Aktivieren Sie das Pairing und das Scannen in `bluetoothctl`:

```
pairable on
scan on
```

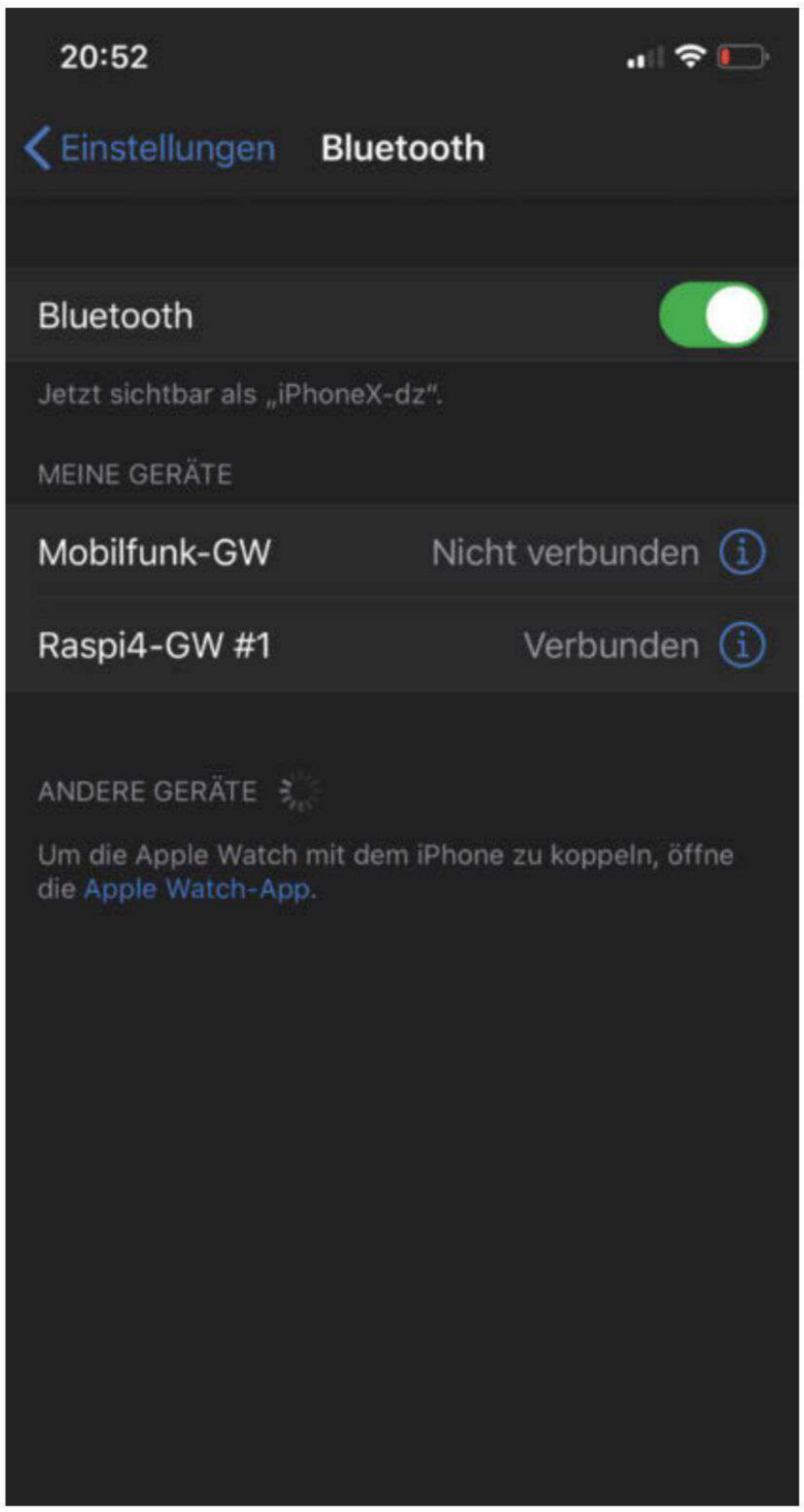
Identifizieren Sie Ihr Smartphone und dessen MAC-Adresse. Manchmal dauert es einige Sekunden, bis `bluetoothctl` in der Ausgabe neben den gefundenen MAC-Adressen auch den Namen des gesuchten Smartphones einblendet. Im iPhone können Sie dessen MAC-Adresse aus Einstellungen / Allgemein / Info auslesen. Manche Androids blenden die Adresse ein, wenn man sie in den Kopplungsmodus schaltet. Alternativ findet man sie in Einstellungen / System oder Einstellungen / Über das Telefon. Wenn Sie die MAC-Adresse haben, koppeln Sie das Smartphone an den Raspi:

```
pair E5:11:1D:4B:4A:43
```

Im obigen Beispiel ist E5:11:1D:4B:4A:43 die MAC-Adresse des Smartphones. Stellen Sie sicher, dass das Smartphone und der Raspi dieselbe Prüfziffer anzeigen. Ist das der Fall, akzeptieren Sie die Kopplung: OK auf dem Smartphone und `yes` in bluetoothctl. Markieren Sie das Smartphone als vertrauenswürdig und beenden Sie `bluetoothctl`:

```
trust E5:11:1D:4B:4A:43
scan off
pairable off
quit
```

Für Asterisk sind nun vier Dateien geringfügig anzupassen. Alle befinden sich im Ordner `/etc/asterisk`. In die Datei chan_mobile.conf trägt man die Bluetooth-Einstellungen ein, über die Asterisk das Smartphone anspricht. In `modules.conf` fügen Sie ein Modul hinzu, das Asterisk beim Start automatisch laden soll. In `sip.conf` richten Sie VoIP-Konten



Obwohl aktuelle iPhones einen kopplungsbereiten Raspi nicht zur Auswahl anbieten, lassen sie sich dennoch mit ihm verbinden.

ein und in `extensions.conf` stehen die Regeln zur Rufbehandlung bei aus- und eingehenden Anrufen; die Namen darin verweisen auf den SIP-Account in sip.conf.

Öffnen Sie chan_mobile.conf in einem Editor wie `pico`, um die MAC-Adressen Ihres externen Bluetooth-Adapters und des Smartphones einzufügen:

```
sudo pico /etc/asterisk/chan_mobile.conf
```

Ersetzen Sie in der Zeile beginnend mit `address=` die Beispiel-MAC-Adresse mit der Adresse Ihres externen Blauzahn-Adapters:

```
[adapter]
id=bluetooth
address=00:1B:DC:00:11:22
```

Fügen Sie darunter den folgenden Textblock ein:

```
[Smartphone]
address=E5:11:1D:4B:4A:43
;port=1
context=incoming-mobile
adapter=bluetooth
group=1
;sms=no
```

Ersetzen Sie im obigen Textblock `E5:11:1D:4B:4A:43` mit der Adresse des Smartphones. Speichern Sie die Änderungen mit der Tastenkombination Strg+X,Y und starten Sie den Asterisk-Dienst neu:

```
sudo systemctl restart asterisk
```

Öffnen Sie mittels `sudo rasterisk -vvvv` eine Konsole auf der Asterisk-Telefonanlage. Geben Sie dort ein:

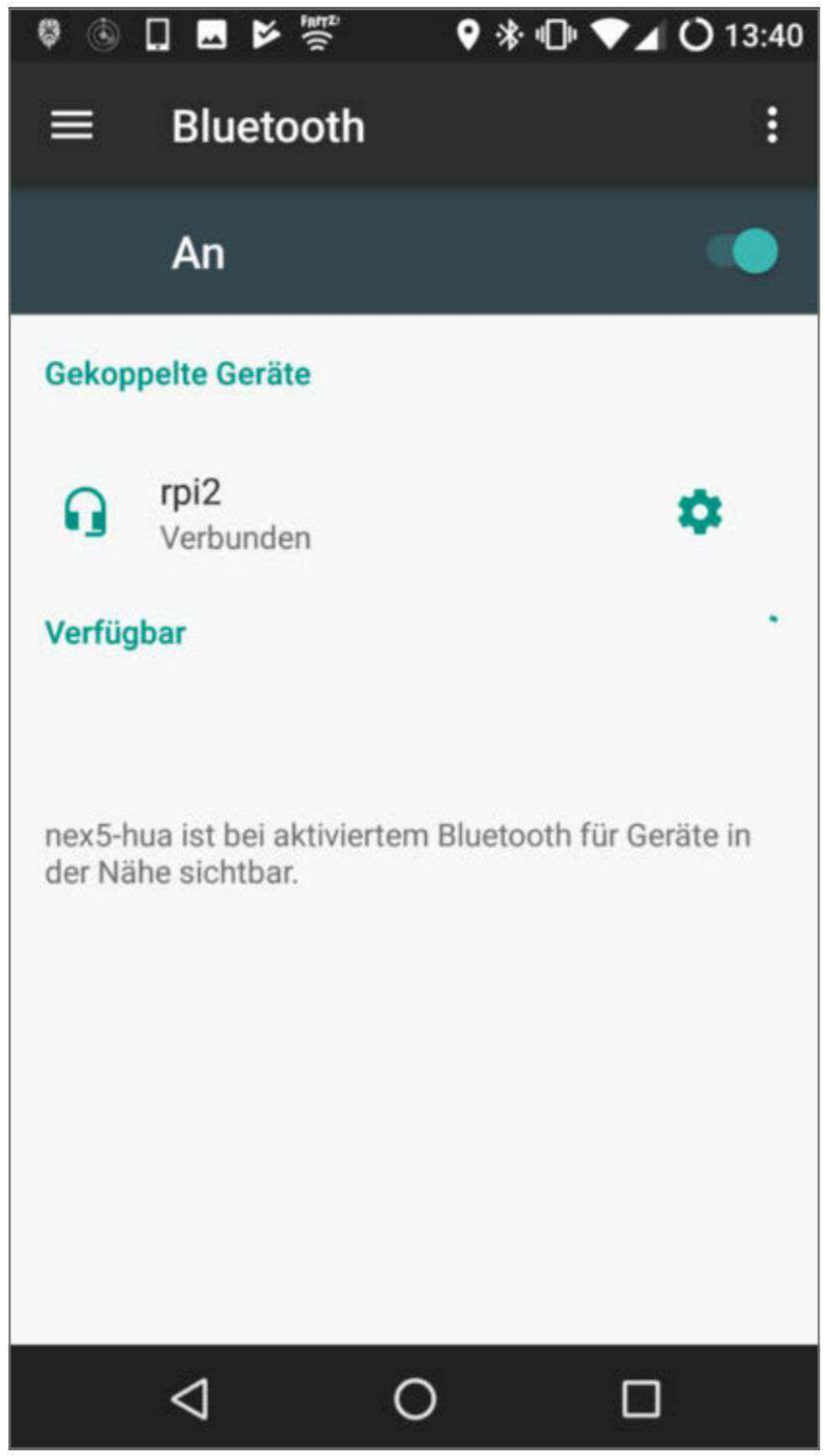
```
module load chan_mobile.so
```

Asterisk meldet nun „Skipping device Smartphone. Missing required port or address setting“. Das ist okay, denn die Portnummer wird erst im nächsten Schritt ermittelt. Schalten Sie das Smartphone in den Kopplungsmodus und geben Sie `mobile search` ein. Bis der Befehl das vollständige Ergebnis liefert, kann es einige Sekunden dauern. Eine Beispielausgabe sieht so aus:

```
mobile search
Address Name Usable Type Port
E5:11:1D:4B:4A:43 Smartphone Yes Phone 3
```

Die Portnummer lautet im obigen Beispiel 3. Tragen Sie die Portnummer, die auf Ihrem Raspi angezeigt wird, in `/etc/asterisk/chan_mobile.conf` ein und entfernen Sie das Semikolon vor dieser Variablen. Im Beispiel wird also `;port=1` zu `port=3`. Entladen Sie das Modul chan_mobile und laden Sie es mit der neuen Port-Einstellung wieder:

```
module unload chan_mobile.so
```



Für den Betrieb in einem Mobilfunk-Gateway sind preisgünstige Android-Handys prädestiniert. Nach der Kopplung lassen sie sich so wie iPhones über das Headset-Profil in das Mobilfunk-Gateway einbinden.

```
module load chan_mobile.so
```

Nun sollte Asterisk unter anderem melden: „Loaded chan_mobile.so => (Bluetooth Mobile Device Channel Driver)“. Es kann mehr als eine Minute dauern, bis Asterisk das erste Mal eine vollständige Verbindung inklusive korrektem Port aufgebaut hat. Dann meldet die Software schlussendlich „Bluetooth Device Smartphone initialized and ready“. Beenden Sie rasterisk mit `quit`.

Legen Sie nun fest, dass das Modul chan_mobile.so automatisch geladen wird. Fügen Sie dazu in der Datei `/etc/asterisk/modules.conf` als letzte Zeile am Ende des Bereichs Global diese Zeile ein:

```
load = chan_mobile.so
```

Starten Sie Asterisk neu und öffnen Sie die Asterisk-Konsole aufs Neue:

```
sudo systemctl restart asterisk
sudo rasterisk -vvv
```

Geben Sie `mobile show devices` ein. In der Ausgabe sollte das Smartphone aufgeführt sein.

```
ID Address Group Adapter Connected
State SMS
Smartphone E5:11:1D:4B:4A:43 1
bluetooth Yes Free No
```

Nun folgt die Konfiguration der Aktionen für ein- und ausgehende Anrufe. Tragen Sie dazu zunächst das VoIP-Konto in der Datei `/etc/asterisk/sip.conf` ein. Ändern Sie dazu die Zeile `;language=en`, dass sie so aussieht:

```
language=de
```

Bringen Sie den Cursor zum Abschnitt `[my-codecs](!)`. Um später passende Codecs leichter zu identifizieren, deaktivieren Sie zunächst alle Codecs durch Voranstellen eines Semikolons bis auf `g722`, `gsm` und `alaw`:

```
[my-codecs](!)
disallow=all

;allow=ilbc
allow=g722
allow=gsm
;allow=g729
;allow=g723
;allow=ulaw
allow=alaw
```

Fügen Sie am Ende der Datei folgenden Abschnitt ein; einige dieser Parameter gibt man später in der Fritzbox zur Anmeldung ein:

```
[Smartphone](my-codecs)
type=friend
host=dynamic
secret=passwort
dtmfmode=rfc2833
canreinvite=no
nat=no
qualify=no
context=Smartphone
```

Speichern Sie die Änderungen und tragen Sie das Call-Routing für ein- und ausgehende Anrufe in die Datei `/etc/asterisk/extensions.conf` ein. Fügen Sie dazu folgenden Abschnitt ans Ende an:

```
[Smartphone]
exten => _X.,1,Dial(Mobile/Smartphone/${EXTEN},45)
_X.,n,Hangup

[incoming-mobile]
exten => s,1,Noop(Accepting mobile call from
↳${DID})
exten => s,n,Dial(SIP/Smartphone)
```

Speichern Sie die Änderungen und starten Sie Asterisk neu:

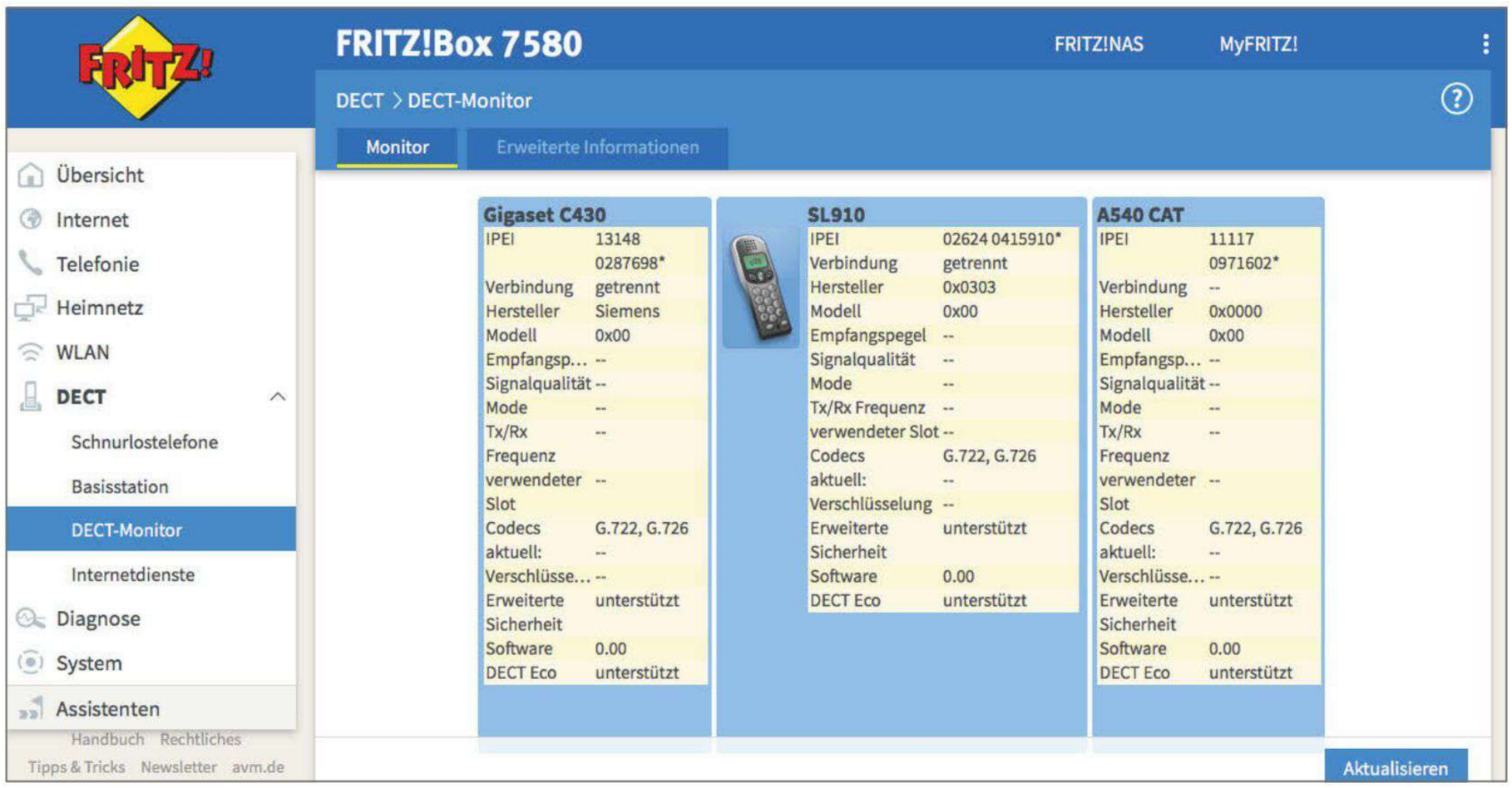
```
sudo systemctl restart asterisk
```

Fritzbox und die Codecs

Damit ist Asterisk eingerichtet und Sie können die Fritzbox konfigurieren. Melden Sie sich dazu an der Fritzbox an und öffnen Sie das Menü Telefonie / Eigene Rufnummern. Klicken Sie auf „Neue Rufnummer“, übernehmen Sie im Menü Telefonie-Anbieter den Punkt „Anderer Anbieter“ (ggf. zuvor „IP-basierter Anschluss“ einstellen). Geben Sie im Feld „Rufnummer für die Anmeldung“ die Zeichenkette „Smartphone“ ein und tragen Sie daneben in „Interne Rufnummer in der Fritzbox“ die Mobilfunknummer ein, die zum Smartphone gehört (z. B. 01771234567).

Weiter unten im Bereich Zugangsdaten sind nun Benutzername, Kennwort und Registrar für den Zugang zu Asterisk auszufüllen. Die beiden ersten Parameter stehen auf dem Raspi in /etc/asterisk/sip.conf und lauten: `Smartphone` und `passwort`. Im Feld Registrar tragen Sie die IP-Adresse des Raspi ein (z. B. 192.168.178.125). Diese können Sie in der Fritzbox aus dem Menü Heimnetz / Netzwerk auslesen.

Klicken Sie auf OK, um die Änderungen zu übernehmen. Am Ende sollte die Fritzbox den neuen SIP-Anbieter mit der soeben eingetragenen Mobil-



Nützlich für die Feinheiten: Um die von DECT-Schnurlosgeräten verwendeten Codecs zu erfahren, öffnet man den DECT-Monitor der Fritzbox.

funknummer und grünem Punkt in der Statuszeile anzeigen. Wenn das nicht der Fall ist, stellen Sie sicher, dass Sie den Benutzernamen und das Passwort eingetragen haben, die Sie in Asterisk konfiguriert haben.

Wenn der grüne Punkt leuchtet, ist die Fritzbox bereit für den ersten Testanruf. Rufen Sie am besten eine Festnetznummer an. Im Smartphone-Display sollte der Vorgang zu sehen sein. Wenn die Sprache verzerrt ist oder die Laufzeit zu hoch, verwenden die beiden Gegenstellen vermutlich nicht denselben Codec.

Asterisk kann das zwar bis zu einem gewissen Grad per eigener Codec-Umwaldung ausbügeln, aber das dauert ein wenig und erhöht so die Signallaufzeit unerwünschtermaßen. Daher möchte man, dass Anrufer und Empfänger denselben Codec verwenden. Mit `rasterisk -vvv` und dem Befehl `core show translation` können Sie auslesen, welche Codecs Asterisk parat hat und wie lange das Umkodieren im jeweiligen Fall dauert.

Den optimalen Codec findet man leicht durch Ausprobieren. Um einen Codec zu aktivieren, entfernen Sie in `/etc/asterisk/sip.conf` das Kommentarzeichen `;` vor einem Codec. Meiden Sie `ilbc`, denn damit baut Asterisk keine Verbindung auf. Speichern Sie die Änderungen, starten Sie Asterisk neu und testen Sie den neuen Codec, bis Sie einen gefunden haben, der mobilfunkübliche Sprachqualität liefert.

Falls Sie ein DECT-Telefon verwenden, kann die Fritzbox bei der Einstellung des richtigen Codecs helfen. Öffnen Sie das Menü Fritzbox/DECT/Monitor. Dort führt der Router für alle DECT-Telefone auf, welche Codecs diese gemeldet haben. Stellen Sie die dort aufgeführten in `/etc/asterisk/sip.conf` ein.

Ist das erledigt, stellen Sie das Smartphone an seinen endgültigen Platz. Die maximale Distanz hängt von den Sendeleistungen der Bluetooth-Module im Smartphone und Bluetooth-Stick ab. Die meisten Smartphones und Sticks arbeiten mit Sendeleistungsklasse 3 und überbrücken etwa 10 Meter. Um auch bei Störungen durch WLAN und andere 2,4-GHz-Sender eine ausreichende Signalgüte zu gewährleisten, sollte man das Smartphone im Abstand von ein bis zwei Metern zum Raspi aufstellen. Dann kann man es ebenso gut per USB-Kabel vom Raspi mit Strom speisen lassen. Sticks der Sendeleistungsklassen 2 und 1 überbrücken größere Entfernungen mit ausreichender Signalqualität; da gehen dann auch schon mal 10 Meter und mehr, zumal, wenn auch das Smartphone einen Blauzahn der Klasse 2 hat. (dz) c't

Bluetooth-Firmware, chan_mobile-Infos

ct.de/w6wv

Ersatzrouter zum Sparpreis

AVMs für 1&1 gebaute Fritzbox 7412 landet derzeit für 5 bis 20 Euro auf den Internetmarktplätzen der Republik – ein Schnäppchen, das auch an aktuellen VDSL2-Anschlüssen funktioniert und sich mit wenig Aufwand als reines DSL-Modem oder VoIP-DECT-Basis einsetzen lässt.

Von **Andrijan Möcker**



Fritzbox 7412 als Zweitrouter nutzen	156
Fritzbox 7520 ohne Einschränkungen	160
Fritzbox 7412 als OpenWrt-Kompagnon	164
Telefon als Türklingel nutzen	167
Fritzbox 7362 SL mit OpenWrt	168

Der deutsche Internetanbieter 1&1 verzichtet als einer der wenigen Provider auf eine eigene Routermarke und setzt stattdessen auf Fritzboxen von AVM. Alle paar Jahre entsteht dabei ein mehr oder minder abgespecktes Derivat einer aktuellen Fritzbox, wie beispielsweise die Modelle 7112, 7240, 7412 oder zuletzt die Fritzbox 7520. Die Preise der älteren 1&1-Modelle fallen zur Einführung des Nachfolgers schnell. Aktuell erhält man das Modell 7412 für 5 bis 20 Euro.

Wer angesichts des Preises an eine lahme Möhre denkt, hat weit gefehlt: Die 7412 hat einen 500-MHz-Dual-Core-Prozessor, 128 MByte RAM und ein Vectoring-fähiges VDSL-2-Modem – gute Merkmale für einen einfachen DSL-Router. Damit taugt das Modell mindestens als günstiger Schrankhüter, der nach dem nächsten Blitzschlag das zerstörte Gerät würdig vertritt, bis Ersatz eintrifft. Selbst wer schon Supervectoring gebucht hat, kann die 7412 einsetzen: Telekom-DSLAMs und somit auch deren Reseller-Anschlüsse sperren sich nicht gegen die Nutzung der vorherigen VDSL2-Version mit weniger Datenrate. Im Zweifelsfall erteilt der Anbieter Auskunft.

PPPoE-Trickserei

Die Fritzbox 7412 kann auch als reines DSL-Modem zum Einsatz kommen, beispielsweise in Kombination mit einer Firewall Appliance oder einem nachgeschalteten OpenWrt-Router. Voraussetzung ist das PPPoE-Passthrough: Es leitet das bei DSL verwendete Einwahlprotokoll PPP durch, sodass die 7412 nur noch als Medienkonverter (VDSL2/Fast-Ethernet) für den nachgeschalteten Router arbeitet. Dieser baut die PPP-Sitzung dann selbst auf, erhält die öffentlichen IP-Adressen und kann diese direkt verwalten. Lästige doppelte Netzwerkadressübersetzungen (NAT) und Portfreigaben entfallen.

Da viele Anbieter nur eine PPP-Sitzung pro Anschluss zulassen, muss man bei der Konfiguration tricksen (siehe Screenshot nächste Seite): Statt der Fritzbox korrekte Zugangsdaten mitzugeben, wählt man in der Konfiguration (Internet/Zugangsdaten) die Auswahl „Weiterer Internetanbieter“ und „Anderer Internetanbieter“. „Werden Zugangsdaten benötigt“ ändert man auf „Nein“, anschließend bearbeitet man die Verbindungseinstellungen. Hier ändert man die VLAN-ID auf die Anbietervorgabe, beispielsweise „7“ an Telekom- und deren Reseller-Anschlüssen. Auch Virtual-Path-Identifier (VPI) und Virtual-Channel-Identifier (VCI) variieren von Anbieter zu Anbieter. Die korrekten Werte finden sich aber meist nach kurzer Websuche. Zuletzt erlaubt man anderen Netzwerkgeräten, eine eigene Internetverbindung aufzubauen und deaktiviert die Zugangsprüfung nach Übernahme der Einstellungen (Haken ganz unten).

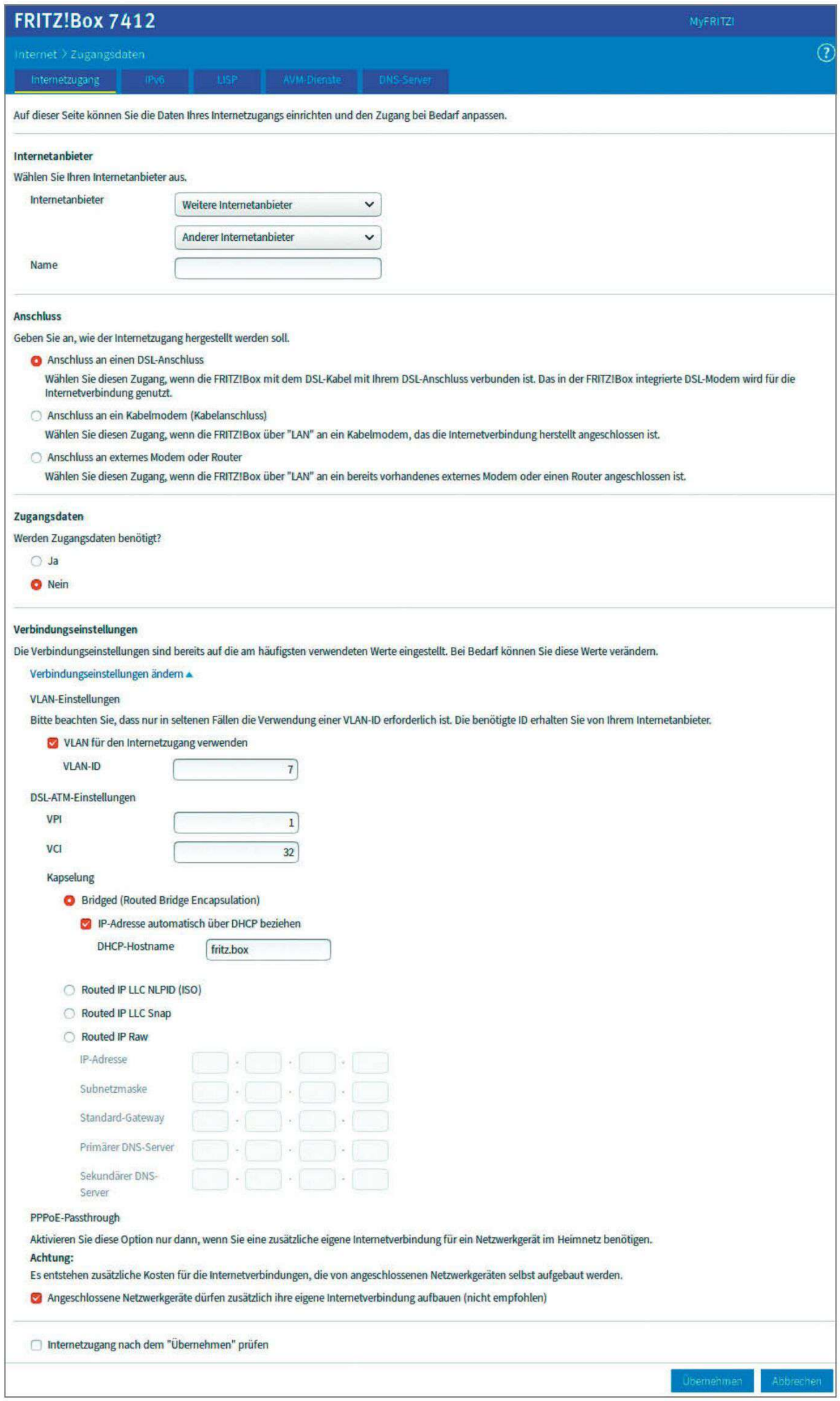
Danach können Sie die 7412 mit dem DSL-Anschluss und über die WAN-Buchse mit dem nachgeschalteten Router verbinden. Letzterer stellt die Internetverbindung selbst via PPPoE her. Die erforderlichen Zugangsdaten schicken Provider meist separat per Post. Bei neueren BNG-Anschlüssen der Telekom klappt es auch ohne. Verlangt der nachgeschaltete Router trotzdem Zugangsdaten, tippen Sie eine beliebige Buchstabenfolge ein – die Terminierungsstelle der Telekom akzeptiert alle Authentifizierungsversuche.

DECT-Basis

Festnetztelefonierer werden Empfangslücken im heimischen DECT-Netz genauso ärgern wie solche im WLAN. Zwar arbeitet die 7412 nicht als DECT-Repeater, durchaus aber als per VoIP-verbundene DECT-Basis zum Sparpreis. Das lohnt, wenn man ein DECT-Telefon beispielsweise ein oder zwei Stockwerke entfernt vom Hauptrouter stationiert hat und es auch nur dort nutzt.

Damit das funktioniert, muss man die 7412 zunächst über die WLAN-Einstellungen in den Repeater- oder alternativ in den Access-Point-Modus versetzen, indem sie sich über ihren LAN-Anschluss eine Adresse aus dem Heimnetz besorgt: Im Menü „Zugangsdaten“ setzen Sie dazu „Internetanbieter“ auf „Weitere Internetanbieter“ und „Anderer Internetanbieter“. Anschluss und Betriebsart stellen Sie auf „Anschluss an externes Modem oder Router“ und „Vorhandene Internetverbindung mitbenutzen (IP-Client-Modus)“. Tragen Sie Ihre Anschlussbandbreite sowie einen individuellen Namen ein (Verbindungseinstellungen) und übernehmen Sie die Einstellungen. Anschließend verbinden Sie die 7412 per Kabel mit Ihrem Heimnetz. Die neue IP-Adresse der Box finden Sie entweder über die Weboberfläche Ihres Routers oder mit einem Netzwerkscanner wie Fing.

Wenn Ihr Hauptrouter eine Fritzbox ist, legen Sie dort für die 7412 ein neues LAN/WLAN-Telefoniegerät mit Benutzername und Kennwort an. In der 7412 fügen Sie das Konto unter „Eigene Rufnummern“ mit der Voreinstellung „anderer Anbieter“ hinzu, wobei Sie die Felder für die interne und die Anmelderufnummer frei belegen können, beispielsweise mit der Festnetznummer. Tragen Sie anschließend Ihre zuvor vergebenen Zugangsdaten ein



Gibt man der Fritzbox wie im Screenshot vor, DHCP über DSL zu benutzen, belegt sie den bei Privatanschlüssen meist einzigen PPPoE-Slot beim Anbieter nicht. Nachgeschaltete Router können dann problemlos eine Verbindung aufbauen.

sowie „fritz.box“ als Registrar. Nach erfolgreicher Prüfung verbinden Sie Ihr DECT-Telefon über das Telefoniegeräte-Menü mit der Fritzbox.

Viele andere Router enthalten keinen SIP-Server in ihrer Telefonanlage. Die Lösung ist meist, die 7412 mit den VoIP-Zugangsdaten Ihres Anbieters zu versorgen und zu hoffen, dass dessen Server mehrere gleichzeitige SIP-Sitzungen zulässt. Um das zu prüfen, tragen Sie die VoIP-Zugangsdaten ein und verbinden ein DECT-Telefon mit der Fritzbox. Anschließend rufen Sie mit Ihrem Handy die Festnetz-Rufnummer an – klingeln die Telefone an beiden Routern, funktioniert die Konfiguration. Im Zweifelsfall erteilt der Provider Auskunft.

WLAN-Lückenfüller

Die 7412 ist in Bezug auf WLAN überholt: Sie funkt nur gemäß Wi-Fi 4 auf 2,4 GHz und mit nur zwei MIMO-Streams. Als Repeater möchte man sie daher nicht einsetzen, insbesondere bei enger 2,4-GHz-Nachbarschaft. Aber mit einer Kabelanbindung kann die 7412 als Access-Point ein sinnvoller Lückenfüller sein, der für einfaches Surfen und Videostreaming am Smartphone genug Durchsatz liefert – das klappt auch gleichzeitig mit dem DECT-Betrieb. Hierzu setzt man WLAN-Namen und -Netzwerkschlüssel auf die gleichen Werte wie im Hauptrouter. Bekannte WLAN-Geräte verbinden sich anschließend automatisch.

OpenWrt

Wer Funktionen benötigt, die FritzOS nicht hat, installiert OpenWrt auf der 7412 und erhält damit deutlich größere Auswahl. DECT und Analogtelefonie unterstützt OpenWrt zwar nicht, doch die Installation klappt dennoch und mit einigen Befehlen auf der Kommandozeile kann man das Webinterface LuCI installieren. Die Box eignet sich dann beispielsweise als Wireguard-Peer oder OpenVPN-Server und stellt als TFTP-Server Konfigurationsdateien für VoIP-Telefone und andere Geräte bereit. Mit satten 128 MByte NAND-Flash bietet die 7412 viel Platz für Extra-Software. Wie Sie OpenWrt auf der Fritzbox 7412 installieren, lesen Sie auf Seite 164. (amo) c't

IMMER AUF AUGENHÖHE

2× Mac & i mit 35 % Rabatt testen und Geschenk sichern!



Mac & i – Das Magazin rund um Apple

- Tipps & Workshops
- Hard- & Softwaretipps
- Apps und Zubehör
- inkl. Club-Mitgliedschaft

Für nur 14,40 € statt 21,80 €

NEU: Mit Mac & i Club-Mitgliedschaft exklusive Vorteile genießen



Jetzt bestellen: **www.mac-and-i.de/miniabo**

leserservice@heise.de 0541 80 009 120

Mac & i. Das Apple-Magazin von c't.

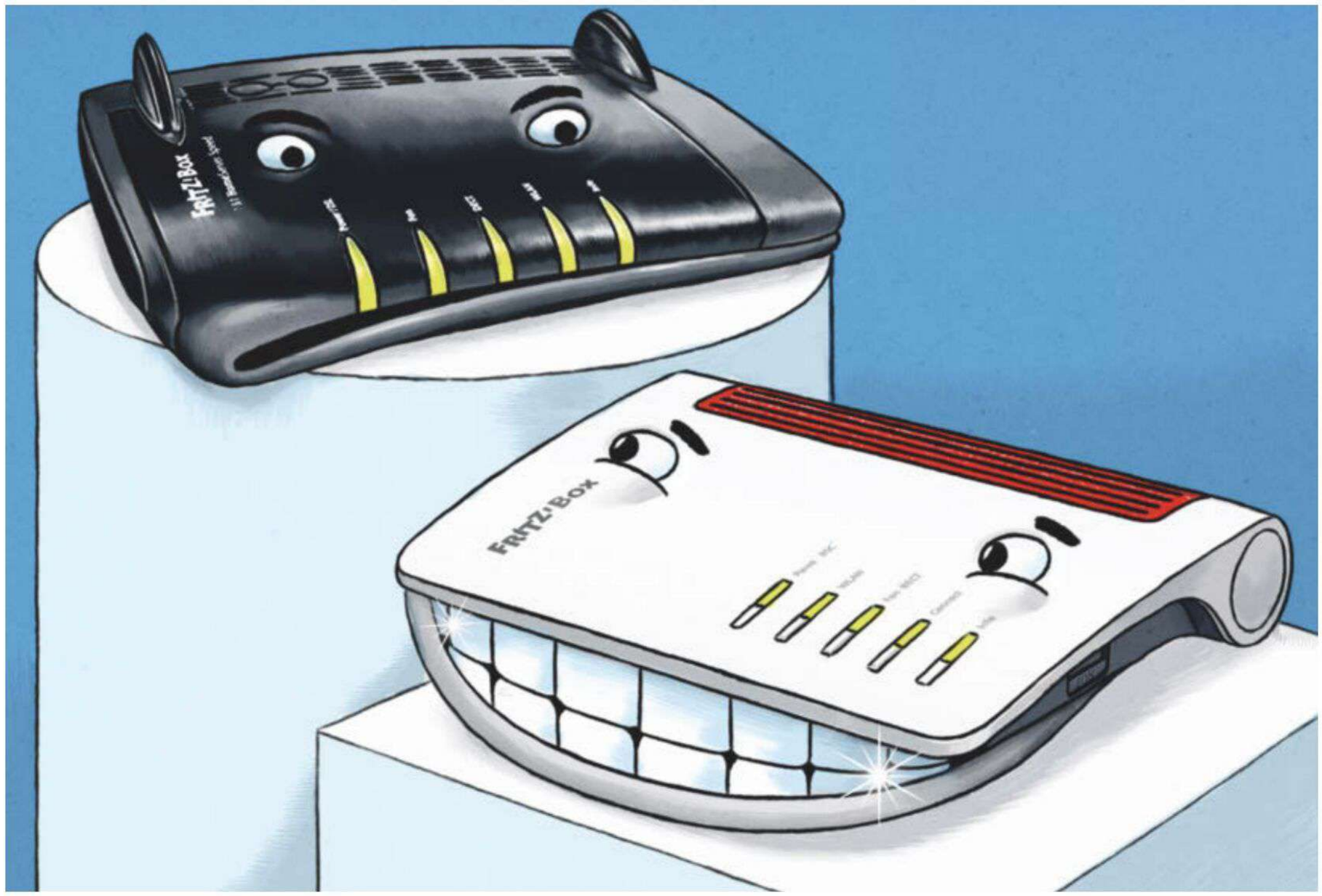


Bild: Thomas Kuhlenbeck

Flunkerbox: Fritzbox 7520

Die Fritzbox 7520 ist AVMs aktuelles OEM-Modell für den Internetanbieter 1&1 und die kleine Schwester der 7530. Laut Datenblatt erhält man nur zwei Gigabit-Ports und nur USB 2.0. Doch die Limitationen sind geflunkert und mit ein paar Anpassungen verpasst man der 7520 das 7530-Upgrade.

Von **Andrijan Möcker**

Der Internetanbieter 1&1 verzichtet anders als die meisten DSL-Provider auf eine eigene Routermarke und lässt stattdessen Fritzboxen leicht abspecken und mit Logo versehen. Das aktuelle Einsteigermodell des Anbieters ist die Super-Vectoring-fähige Fritzbox 7520. Sie wird seit Anfang 2019 als Standardrouter zu den 250-MBit/s-Tarifen herausgegeben und ist nur bei 1&1 zu haben, wo sie 2,99 Euro pro Monat kostet. Nach Vertragsende darf man sie behalten, weshalb man die Box auch gebraucht für 40 bis 70 Euro erhält. Das nächstgrößere Modell 7530 kostet 4,99 pro Monat (120 Euro

im freien Handel) und wird von 1&1 mit zahlreichen Vorteilen beworben – dazu später mehr.

Vergleich

Gegenüber der 7530 zeigt das Datenblatt der 7520 einige Nachteile: Sie hat nur zwei Gigabit-Ethernet-Ports gegenüber vier Ports bei der 7530. Die zwei übrigen Ports der 7520 liefern nur Fast Ethernet, also 100 MBit/s. Der USB-Port erreicht nur USB-2.0-Geschwindigkeit (480 MBit/s statt 5 GBit/s). Der Rest ist jedoch gleich: WLAN gemäß Wi-Fi 5 (IEEE 802.11ac) mit bis zu 866 MBit/s im 5-GHz-Band und 400 MBit/s bei 2,4 GHz. Ins Internet gehts mit VDSL inklusive (Super-)Vectoring bis zu 300 MBit/s schnell. Analoge Telefone schließt man per RJ11- oder TAE-Kabel an, eine DECT-Basis ist auch an Bord.

Der WLAN-Durchsatz beider Router deckt sich in unserer störungsfreien Testumgebung nahezu aufs letzte Megabit pro Sekunde. Lediglich auf größere Entfernung schnitt mal die eine, mal die andere Fritzbox im 5-GHz-Band um 10 bis 20 MBit/s schlechter ab, wobei diese Unterschiede stark von der Geräteorientierung abhingen und auch das Gehäusedesign einen Einfluss hat.

Auch in puncto DSL-Modem konnten wir keine Unterschiede feststellen: An unserem Telekom-Supervectoring-Testanschluss in der Redaktion erreichten beide Modelle über circa 160 Meter Leitungslänge die gleichen Übertragungsraten, die sich auch mit denen der sonst angeschlossenen Fritzbox 7590 deckten.

Innere Auffälligkeiten

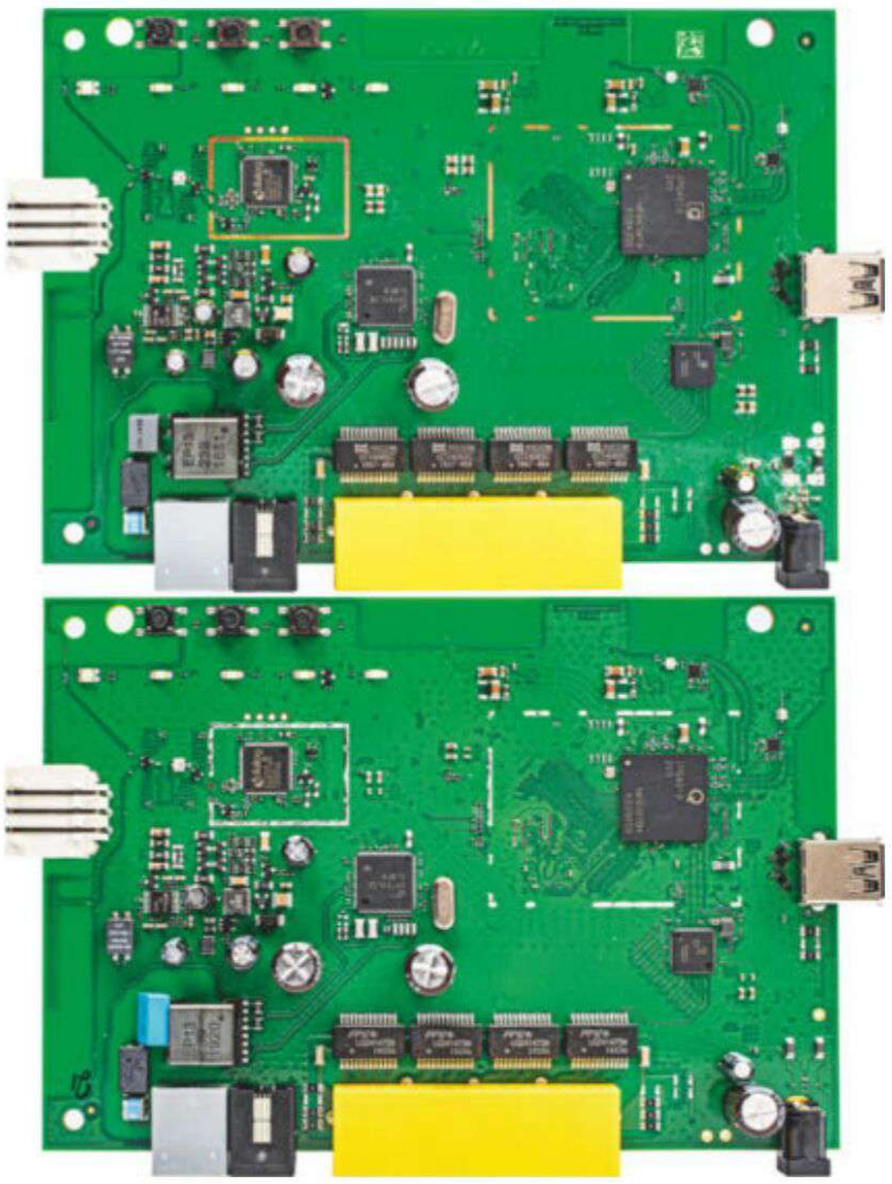
Derart ähnliche Ergebnisse erhält man nur, wenn die Hard- und Software weitgehend gleich sind. Der Blick auf die Platinen bestätigte das: Herzstück beider Geräte ist das Router-System-on-Chip IPQ4019 von Qualcomm mit 128 MByte NAND-Flash und 256 MByte DDR3-RAM. Auf beiden Boards sitzen die gleichen RAM- und Flash-Module sowie Intels xDSL-Modem VRX518. Auch bei den restlichen Komponenten muss man genau hinsehen, um Unterschiede zu erkennen: Manche SMD-Bauteile unterscheiden sich, sind anders gesetzt oder stecken nur auf einer der beiden Platinen.

Auf beiden Boards sitzt der Qualcomm QCA8075, ein 5-Port-Gigabit-Ethernet-Transceiver. Doch weshalb hat die Fritzbox 7520 dann nur zwei Gigabit-Ethernet-Ports? In ihrer Bandbreite limitierte Ethernet-Signalübertrager wären eine mögliche Antwort. AVM setzt jedoch sowohl für die Gigabit- als auch für die 100-MBit/s-Ports die gleichen Transformatoren ein.

Das Platinenlayout ist auch im sichtbaren Bereich vor der USB-Buchse bei beiden Modellen gleich. Doch ein langsamerer Anschluss wäre durchaus plausibel, denn der verwendete IPQ4019 besitzt Pins für einen USB-2.0- und einen USB-3.0-Anschluss. Wo der Port am SoC angeschlossen ist, lässt sich aufgrund der mehrlagigen Platine schwer von außen sagen. Aber auch hier fiel uns etwas auf: Die USB-Buchse besitzt die zusätzlichen Pins für USB 3.0.

Firmware-Hack

Die Witterung aufgenommen, versuchten wir die Firmware der 7530 auf der 7520 zu installieren: Wie erwartet wehrte sich die Box mit Händen und Füßen und beschwerte sich sowohl im Webinterface als



Kaum zu unterscheiden: Die Platine der 7520 (oben) sieht fast genauso aus wie die der 7530 (unten). Nur die Beschriftung „7520X...“ und die Seriennummern verraten, dass es sich um eine Platine mit kleinen Änderungen handelt.

auch in AVMs Recovery-Tool, dass die eingespielte Firmware gar nicht für sie gedacht sei. Mitgeschnittene Kommunikation und die Recherche des c't-Autors Vincent Wiemann offenbarten jedoch eine Lücke in AVMs Bootloader: Das Recovery-Tool erhält per FTP mehrere Parameter, anhand derer es die Fritzbox identifiziert. Alle sind Teil der Bootloader-Variablen – die auch per FTP geändert werden können.

Der Weg zur Firmware-Änderung ist so nur zehn leichte Schritte lang: Zunächst lädt man das Recovery-Tool für die 7530 auf einem Windows-Rechner mit LAN-Interface herunter (ct.de/wh8u), ändert die IP-Adresse des LAN-Interface statisch auf 192.168.178.2 (255.255.255.0) und verbindet sich per Kabel mit der vom Strom getrennten Fritzbox 7520. Anschließend öffnet man zwei Kommandozeilenfenster: Im ersten läuft ein Ping auf die Adresse der Box (`ping 192.168.178.1 -t`), um das FTP-Zeitfenster beim Start abzupassen. Im zweiten wartet der vorbereitete FTP-Befehl zur Ausführung im richtigen Moment (`ftp 192.168.178.1`). Gibt man der Box Strom, kommt nach wenigen Sekunden die erste Ping-Antwort und die FTP-Verbindung kann hergestellt werden. Klappt das mehrmals nicht, benötigt der Netzwerkadapter des genutzten PCs zu lange für die Verbindungserkennung und ein dazwischengeschalteter Switch muss helfen.

Benutzername und Passwort für den FTP-Zugang sind gleich: `adam2`. Steht die Verbindung, ändert man mit vier Befehlen die ausschlaggebenden Variablen.

```
quote SETENV ProductID Fritz_Box_HW236
quote SETENV HWRevision 236
quote SETENV HWSubRevision 1
quote SETENV firmware_version avm
```

Danach beendet man die FTP-Verbindung mit `quit` und startet das Recovery-Tool der Fritzbox 7530, das dann anstandslos die Firmware in den Speicher schreibt - vorausgesetzt man ignoriert die Aufforderung, den Stromversorgung der Box zu ziehen; die Bootloader-Änderungen gehen dabei verloren. Nach ein bis zwei Minuten bootet die 7520 als Mod-7520, also mit Fritzbox-7530-Firmware. Linux- und macOS-Nutzer benötigen etwas länger, da das Recovery-Tool nur unter Windows läuft, dann beispielsweise in einer virtuellen Maschine.



1&1-Website

Wer bei 1&1 einen DSL-Anschluss buchen möchte, bekommt die Fritzboxen 7520, 7530 und 7590 zur Auswahl. Obwohl die 7520 und die 7530 nahezu baugleich sind, schmälert der Anbieter bei der 7520 gezielt Produkteigenschaften.

7520 + 10 = 7530

Die neue Firmware bestätigt alle Vermutungen: In den Netzwerkeinstellungen können wir alle vier Ports auf Gigabit-Ethernet hochschalten und in den USB-Einstellungen steht der „Power Mode USB 3.0“ zur Auswahl. Erneut durchgeführte Leistungsmessungen an allen Ethernet-Ports und Versuche mit einer USB-3.0-SSD beweisen: Die 7520 ist eine künstlich verschlechterte 7530.

Die Modifikation klappt mit aktuellen Recovery-Tools von AVM in der Regel problemlos. Lediglich der Webupdater der Box funktioniert in der Modifikation nicht mehr - die Box erkennt das heruntergeladene 7530-Image als ungültig und bricht ab, sodass die alte Firmware wieder bootet. Händische

AVM / 1&1 Fritz!Box 7520

WLAN-Router für SVDSL	
Hersteller	AVM, www.avm.de
WLAN	2 × Wi-Fi 5 (2) = IEEE 802.11ac-400/866, simultan dualband, WPA, WPS, DFS
Bedienelemente	WLAN, Fon/DECT, Connect/WPS, 5 Statusleuchten
Anschlüsse	4 × RJ45 (2 × Gigabit-, 2 × Fast-Ethernet), 1 × xDSL (RJ45, ADSL + VDSL incl. Super-Vectoring bis 300 MBit/s), 1 × USB 2.0, DECT (max. 6 Handsets), 1 × TAE/RJ11 (Analogtelefon), 1 × 5,5-mm-DC-Hohlstecker (12 Volt)
getestete Firmware	FritzOS 7.14 und FritzOS 7.14 (7530-Version)
NAT-Perf. IP-zu-IP (DS / US)	956 / 949 MBit/s
WLAN 2,4 GHz nah / 20 m	212 / 134–207 MBit/s
5 GHz (HT80) nah / 20m	680 / 42–230 MBit/s
Leistungsaufnahme	6,5 Watt
jährliche Stromkosten	18 Euro
Preis	2,99 € / Monat, 40–70 € gebraucht

[1] mit iperf3, zwei LAN-Hosts, LAN1 als WAN, je 10 TCP-Streams
[2] 1 × GE belegt, SVDSL-Sync, kein Traffic [3] Dauerbetrieb, 30 ct/kWh, gerundet

Fritz!Box-7530-Recovery-Tool

ct.de/wh8u

Updates per 7530-FritzOS-Datei kann man aber noch machen. AVM stellt die Images auch auf https://ftp.avm.de bereit, sodass man sie mit wenigen Klicks herunterladen und installieren kann.

Fehler oder Funktionsausfälle, wie sie bei einer Firmwaremodifikation immer ein Risiko sind, konnten wir bis Redaktionsschluss nicht feststellen. Die Mod-7520 lief im Test mehrere Wochen ohne einen merklichen Unterschied zur 7530 am Supervectoring-Anschluss des Autors.

Gezielte Verwirrung

Doch damit nicht genug: 1&1 unterschlägt in der Router-Auswahl auf seiner Webseite gezielt Funktionen der 7520: Die 7530 wird mit „Premium-WLAN mit 1.266 MBit/s und als „Zukunftssicher – gerüstet für schnelles Supervectoring mit bis zu 300 MBit/s beworben. Bei der 7520 gibt es keinen Hinweis auf Super-Vectoring, beim WLAN lässt 1&1 die 400 MBit/s im 2,4-GHz-Band außen vor und spricht von „866 MBit/s im WLAN-AC Band (5 GHz)“. Wer als Kunde nicht das technische Wissen mitbringt oder genauer in die Datenblätter schaut, wird sich eher für das mutmaßlich bessere Modell entscheiden.

c’t fragte sowohl 1&1 als auch AVM, ob die Limitationen der 7520 bewusst abgesprochen waren und ob in der Vergangenheit „künstlich“ limitierte Geräte ausgegeben wurden. 1&1 sagte dazu, dass AVM die Fritzbox 7520 in Abstimmung mit 1&1 entwickelt hat. Das Modell hätte man eingeführt, um den Kunden einen günstigen Top-Router anbieten zu können. AVM blieb dabei, dass es sich bei den beiden Routern um zwei unterschiedliche Produkte mit verschiedenen Eigenschaften handle und wies darauf hin, dass das Aufspielen einer produktfremden Firmware zum Verlust der Garantie führe. Weitere Angaben zur Partnerschaft mit 1&1 konnte AVM nicht machen. (amo) c't

heise Academy

JETZT GRATIS-LEKTIONEN ONLINE ANSCHAUEN

Von Experten. Für Experten.
heise-academy.de



Continuous Delivery von A bis Z

CI/CD-Pipelines mit Gitlab und Jenkins entwickeln, konfigurieren und testen

▸ 74 Videos, 7 Std. Spielzeit



Azure Active Directory im hybriden Kontext

Grundlagen, Strategien und fortgeschrittene Techniken für Planung und Betrieb

▸ 60 Videos, 6 Std. Spielzeit



Fritzbox 7412 als OpenWrt-Kompagnon

Die Fritzbox 7412 war bis Ende 2018 der Standardrouter des Internetanbieters 1&1. Mittlerweile gibt es das Gerät für 5 bis 20 Euro gebraucht. Wir zeigen, wie Sie die Box auf OpenWrt umrüsten und so zu modernen Ergänzungen wie Wireguard-VPN oder DNS-Verschlüsselung befähigen.

Von **Andrijan Möcker**

Die 1&1-Fritzbox 7412 ist ein unterschätzter Mini-Router für wenig Geld, den man mit dem quelloffenen Router-Betriebssystem OpenWrt zum Beispiel als reines DSL-Modem einsetzen kann (siehe S. 156). Zudem unterstützt OpenWrt die Fritzbox 7412 seit Januar 2020 offiziell. Lediglich der Telefonie-Analogport und die DECT-Basis liegen brach. Dennoch kann die Box aber damit zur preisgünstigen Ergänzung im Heimnetz werden, die sich dann lohnt, wenn ein größeres System wie eine Fritzbox 4040 oder ein Raspberry Pi überdimensioniert ist.

Die Systemeigenschaften der Fritzbox 7412 entsprechen den aktuellen Empfehlungen der OpenWrt-Entwickler: 128 MByte NAND-Flash und 128 MByte DDR2-RAM. CPU und Flash-Speicher reichen aus, um eine Vielzahl von Zusatzpaketen installieren und auch noch in einigen Jahren die aktuelle OpenWrt-Version einsetzen zu können.

Zwar steuert OpenWrt auch das xDSL-Modem der 7412 an, die Implementierung erwies sich in den Versuchen an unseren drei Testanschlüssen jedoch als instabil und für den täglichen Gebrauch ungeeignet. Wer sich das AVM-Recovery abspeichert

kann die Box im Notfall schnell zum DSL-Router machen.

Vorbereitung

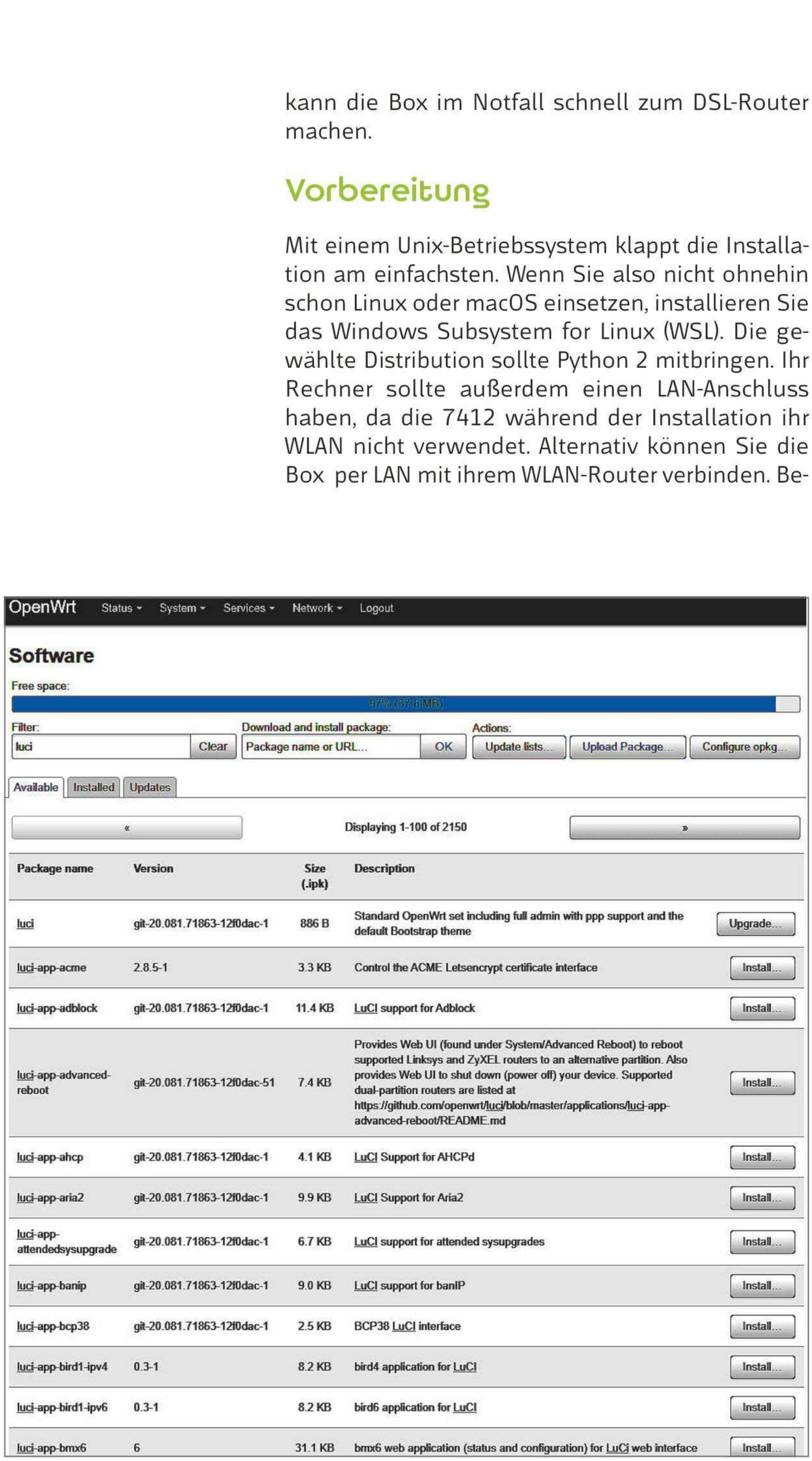
Mit einem Unix-Betriebssystem klappt die Installation am einfachsten. Wenn Sie also nicht ohnehin schon Linux oder macOS einsetzen, installieren Sie das Windows Subsystem for Linux (WSL). Die gewählte Distribution sollte Python 2 mitbringen. Ihr Rechner sollte außerdem einen LAN-Anschluss haben, da die 7412 während der Installation ihr WLAN nicht verwendet. Alternativ können Sie die Box per LAN mit ihrem WLAN-Router verbinden. Beachten Sie jedoch, dass OpenWrt in der Grundkonfiguration Adressen vergibt, was die Geräte in Ihrem Netzwerk kurzzeitig beeinträchtigen kann.

Die OpenWrt-Installation erledigt ein Python-Skript, das das neue Betriebssystem zunächst über den Bootloader in den Arbeitsspeicher der Box lädt und von dort aus bootet. Anschließend kopiert man OpenWrt händisch final auf den Speicher: Öffnen Sie eine neue Kommandozeile beziehungsweise das WSL und laden Sie zunächst das Ramboot-Skript mit

```
wget ↵
 ↳https://raw.githubusercontent.com↵
 ↳/openwrt/openwrt/openwrt-19.07↵
 ↳/scripts/flashing/eva_ramboot.py
```

herunter. Um die aktuelle OpenWrt-Version für die 7412 herunterzuladen, öffnen Sie die Hardware-Seite der Box im OpenWrt-Wiki (siehe ct.de/wh7q) und laden die Release-Abbilder avm_fritz7412-initramfs-kernel.bin und avm_fritz7412-squashfs-sysupgrade.bin mit `wget` herunter. Achten Sie darauf, nicht in der Zeile zu verrutschen, da Sie sonst ein potenziell fehlerhaftes Snapshot-Abbild herunterladen.

Zur Installation sind zwei statische Adressen nötig: 192.168.178.2 und 192.168.1.2, beide mit der Subnetzmaske 255.255.255.0. Vergeben Sie die Adressen an Ihr LAN-Interface beziehungsweise an Ihr WLAN-Interface, wenn die 7412 über Ihren WLAN-Router läuft. Anschließend stecken Sie die noch vom Strom getrennte 7412 an die Netzwerkschnittstelle und bereiten zwei Kommandozeilenfenster auf Ihrem Rechner vor, in das Sie jeweils eins der folgenden Kommandos eintragen: `python eva_ramboot.py 192.168.178.1 <Initramfs-Datei>` und `ping 192.168.178.1`.



Softwarerweiterungen, Protokolle, Sprachdateien: Über 2000 Pakete erweitern bei Bedarf das Webinterface LuCI, sodass man nahezu alle Grundfunktionen und viele Add-ons bequem über den Browser installieren kann.

Installation

Lösen Sie den Ping aus und wechseln Sie in das Fenster mit dem vorbereiteten Ramboot-Skript. Versorgen Sie die 7412 mit Strom und führen das Skript bei der ersten Ping-Antwort aus. Achtung, der Bootloader ist nur kurz beim Start der Box aktiv. Wenn Sie das Skript nicht rechtzeitig ausführen konnten, trennen Sie die 7412 kurz vom Strom und beginnen von vorne. Haben Sie mehrfach keinen Erfolg, reagiert möglicherweise ihr Netzwerkinterface nicht schnell genug – dann kann ein dazwischengeschalteter Switch helfen.

Lief das Skript erfolgreich durch, brechen Sie den Ping ab und pingen stattdessen 192.168.1.1 an.

Wenn Sie von dort Antworten erhalten, übertragen Sie die Sysupgrade-Datei auf den Arbeitsspeicher:

```
scp <Sysupgrade-Datei> root@192.168.1.1:/tmp
```

Anschließend verbinden Sie sich per SSH mit der Box, wechseln in das Verzeichnis `/tmp` und starten die finale Installation:

```
ssh root@192.168.1.1
cd /tmp
sysupgrade -n <Sysupgrade-Datei>
```

Wenn die Box auch nach zwei bis drei Minuten nicht wieder ansprechbar ist, versucht der Bootloader möglicherweise die falsche Partition zu booten: Trennen Sie die Box vom Strom, pingen Sie 192.168.178.1 an und bereiten Sie in einem zweiten Terminal den Befehl `ftp 192.168.178.1` vor. Stecken Sie die Box wieder an und führen Sie den ftp-Befehl umgehend nach der ersten Pingantwort aus. Benutzername und Kennwort für den FTP-Zugang lauten beide `adam2`. Lesen Sie den Boot-Parameter mit

```
quote getenv linux_fs_start
```

aus (1 oder 0), invertieren Sie ihn mit

```
quote setenv linux_fs_start <0 oder 1>
```

und starten Sie die Box mit `quote reboot` neu. Dass OpenWrt bootet, erkennen Sie an der nach einigen Sekunden schnell blinkenden Power-LED; die Installation ist dann abgeschlossen.

Netzwerkkonfiguration

Wenn die Power-LED aufhört zu blinken, rufen Sie das OpenWrt-Webinterface unter http://192.168.1.1 auf, klicken auf „Login“ und dann auf die Passwort-Aufforderung, um ein Systempasswort zu setzen. Anschließend wechseln Sie in „Network“ „Interface“, löschen die beiden nicht benötigten WAN-Schnittstellen und bestätigen mit „Save & Apply“.

Damit sich der DHCP-Server der 7412 nicht in die IP-Adressvergabe Ihres Hauptrouters eimischt, klicken Sie zunächst beim LAN-Interface auf Edit, setzen im Reiter „DHCP Server“ den Haken bei „Ignore Interface“ und deaktivieren in den untergeordneten „IPv6 Settings“ den „Router Advertisement-Service“ und den „DHCPv6-Service“. Danach ändern Sie in den „General Settings“ das Protocol auf „DHCP client“, bestätigen mit „Switch Protocol“ und Save. Bevor Sie auf „Save & Apply“ klicken, ändern Sie über den Pfeil rechts der Schaltfläche das Verfahren auf „Apply unchecked“ – OpenWrt erwartet sonst eine Rückmeldung vom Browser. Bleibt diese aus, macht das System die Änderungen rückgängig. Bestätigen Sie die Einstellungen anschließend über die rote Schaltfläche. Die neue IP-Adresse der Box finden Sie entweder über das Webinterface Ihres Routers oder über eine Netzwerkscanner-App wie Fing.

Zurück auf der Weboberfläche legen Sie im selben Menü ein neues IPv6-Interface an, damit die 7412 auch über das aktuelle IP-Protokoll erreichbar ist: „Add new interface“, Name: „LANv6“, Protokoll: „DHCPv6 client“, Interface: „Alias Interface:,@la“, „Create interface“. Im folgenden Fenster deaktivieren Sie die IPv6-Präfix-Anfrage und setzen in den „Firewall Settings“ lan als Firewall-Zone. Speichern Sie die Einstellungen mit Save und „Save & Apply“. Nun ist die Box vollständig aus Ihrem Heimnetz erreichbar und hat Zugriff auf das Internet.

Einsatzmöglichkeiten

Bei Redaktionsschluss bot das Paket-Repository von OpenWrt satte 8350 Pakete. Nach der OpenWrt-Installation bleiben auf der 7412 noch 38 MByte für

Modifizierte AVM/1&1 Fritz!Box 7412

WLAN-Router für VDSL	
Hersteller	AVM, www.avm.de
Bedienelemente	WPS, DECT, 5 Statusleuchten
Anschlüsse	1 × RJ45 (FastEthernet), 1 × xDSL1 (RJ45, ADSL + VDSL incl. Vectoring bis 100 MBit/s), DECT[2], 1 × TAE/RJ11[2], Wi-Fi 4 (2, 2,4 GHz) (IEEE 802.11n),
Hardware	128 MByte NAND-Flash, 128 MByte DDR2-RAM, Lantiq XWAY VRX220 CPU (MIPS 34Kc, 2 × 550 MHz)
Getestete Firmware	OpenWrt 19.07.2 r10947-65030d81f3
Wireguard-Durchsatz[3]	33 MBit/s
OpenVPN-Durchsatz (AES-CBC, 128/256 Bit)[3]	11 / 7 MBit/s
Leistungsaufnahme[4]	5,5 Watt
jährliche Stromkosten	15 €

[1] siehe Text für xDSL-Modem, DECT, TAE/RJ11 [2] Nicht von OpenWrt unterstützt
[3] mit iperf3 [4] FastEthernet belegt, WLAN aktiviert, kein Traffic
[5] Dauerbetrieb, 30 ct/kWh, gerundet

Literatur

[1] Andrijan Möcker, **Schwesterkiste**, Fritzbox 4040 mit OpenWrt betreiben, c't 10/2019, S. 28

[2] Andreas Itzchak Rehberg, **Selbstauskunft**, Namensauflösung inklusive Datenschutz fürs Heimnetz, c't 12/2017, S. 130

[3] Carsten Strotmann, **Privatsphäre per Tunnel**, Domain Name Service: Datenschutz selbstgebaut, c't 20/2017, S. 154

[4] Carsten Strotmann, **Privatvermittlung**, Privater Nameserver und Adblocker im LAN, c't 21/2017, S. 158

[5] Carsten Stromann und Duan ivadinovi, **Erweiterte Privatvermittlung**, Update zu Unbound als privater Nameserver und Adblocker, c't 4/2018, S. 162

Pakete – wie Sie sie verwenden, entscheiden Sie nach Ihrem persönlichen Bedarf.

Wir haben in der Vergangenheit bereits über einige OpenWrt-Anwendungen berichtet: zum Beispiel, wie Sie mit Stubby DNS-Anfragen verschlüsseln und diese so vor Manipulation und Tracking schützen, sowie wie Sie das neue VPN-Protokoll Wireguard einsetzen, um deutlich höheren Durchsatz zu erzielen als mit den etablierten VPN-Methoden [1]. Unsere Reihe zu DNS-Verschlüsselung und Validierung mit dem Resolver Unbound bezieht sich zwar auf ein großes Linux, ist aber auch auf OpenWrt übertragbar [2, 3, 4, 5]. Wenn Sie einen Anwendungsfall haben, der sich auf der Fritzbox 7412 besonders lohnt, freuen wir uns über eine E-Mail von Ihnen. (amo) c't

OpenWrt-Links

ct.de/wh7q

Telefon als Türklingel nutzen

Wenn der Besuch klingelt, sollen auch die Festnetztelefone schellen – das geht mit dem KlingelPaul und einer Fritzbox.

Von **Sven Hansen**



Der KlingelPaul von UK-Intech ist ein Kästchen, das sich per Telefonkabel (TAE) an Fritzboxen mit Anlagenfunktion anstöpseln lässt. Das dafür erforderliche Anschlusskabel Western/TAE ist nicht im Lieferumfang enthalten. Die Box verbindet man über den zweipoligen Pfostenstecker mit einem zusätzlichen Taster oder man betreibt sie parallel zu einem bereits angeschlossenen Türgong (max. 18 Volt).

Über die Fritzbox-Oberfläche bindet man den KlingelPaul als Türsprechanlage ein, indem man im Menü Telefonie ein neues Gerät anmeldet, Türsprechanlage auswählt und den analogen Anschluss einstellt, an dem das Kästchen hängt. Über den Menüpunkt Weiterleiten bestimmt man anschließend, welches an der Fritzbox angeschlossene Telefon beim Aktivieren des KlingelPauls anschlagen soll. Klingelt es an der Tür, wird der Besucher fortan über die gewünschten DECT- oder Analogtelefone angekündigt. Nutzt man ein FritzFon, lässt sich dessen Klingelton frei wählen.

Die Fritzbox kann noch mehr: Im Menü für die Türsprechanlagen lässt sich auch eine Videokamera einbinden, deren Live-Bild die DECT-Telefone als Motion-JPG anzeigen. So verrät das Telefon gleich, wer da vor der Tür steht. Wer KlingelPauls Standardkonfiguration ändern will, muss zum Schraubendreher greifen. Unter anderem lässt sich die voreingestellte Klingeldauer von 15 Sekunden im Morseverfahren über einen kleinen Taster auf der Platine anpassen. (sha) c't

KlingelPaul	
Türklingelmodul für Fritzbox	
Hersteller	UK-Intech, www.uk-intech.de
Anschlüsse	RJ-Buchse (Western), Pfostenstecker
Preis	60 €

Fritzbox 7362 SL mit OpenWrt



Der Einstieg in die Welt der OpenWrt-Router muss nicht teuer sein: Die Fritzbox 7362 SL bekommt man gebraucht für 10 bis 20 Euro. Sie eignet sich trotz ihres Alters prima als Hardware für Netzwerkprojekte mit der offenen Router-Firmware. Mit einem Python-Skript ist sie in wenigen Schritten in einen Open-Source-Router verwandelt.

Von **Andrijan Möcker**

Das quelloffene Router-Betriebssystem OpenWrt lädt mit seinen über 15.000 Erweiterungspaketen für diverse Router-Architekturen zum Basteln ein und ermöglicht viele individuelle Netzwerkideen. Wer günstig einsteigen oder erst einmal experimentieren möchte, muss nicht viel Geld ausgeben: Die etwas in die Jahre gekommene Fritzbox 7362 SL reicht für viele Zwecke aus und ist preislich kaum schlagbar; wir erstanden ein Testexemplar für 15 Euro über eBay Kleinanzeigen. Die Box bringt 128 MByte RAM und 128 MByte Flash-Speicher mit; für OpenWrt ist das viel und dürfte noch locker für die nächsten Jahre ausreichen. Das eingebaute Lantiq-SoC (Dual-Core, 500 MHz) bietet zwei Gigabit- und zwei FastEthernet-Ports sowie zwei USB-2.0-Ports – allesamt mit OpenWrt nutzbar.

Einsatzmöglichkeiten

Dank der OpenWrt-Community stehen hunderte Pakete für allerhand Anwendungsfälle zur Verfügung, über die man schrittweise mit dem System warm werden kann – und den Router beispielsweise als Werbefilter, DNS-Verschlüsselungsdienst, VPN-Server/-Client oder auch als ergänzender WLAN-Access-Point nutzen kann (wenn auch nur auf 2,4 GHz). In den Literaturverweisen finden Sie weiteren Lesestoff zum Thema.

Vorbereitung

Mit Linux- oder macOS-Systemen klappt die Installation am einfachsten. Unter Windows empfehlen wir dafür das Windows Subsystem for Linux (WSL). Ein Python-Skript erledigt die OpenWrt-Installation: Es lädt das neue Betriebssystem zunächst über den Bootloader in den Arbeitsspeicher der Box und startet es von dort aus. Anschließend installiert man OpenWrt final in den Speicher des Routers. Außerdem benötigt Ihr Rechner einen LAN-Anschluss, da die Box während der Installation kein WLAN verwendet.

Die Installation erfordert drei Dateien: das Python-Skript, die RAM-Boot-Datei `Initramfs` und die finale Installationsdatei `sysupgrade`. Das Skript finden Sie über ct.de/wm5y. Die aktuellen Installationsdateien laden Sie von der ebenfalls dort verlinkten Hardware-Seite der Fritzbox 7362 SL herunter: Kopieren Sie die Links unter „Firmware OpenWrt Install URL“ und „Firmware OpenWrt Upgrade URL“ und laden Sie die Dateien mit `wget <Link>` herunter. Achten Sie dabei darauf, nicht in der Zeile zu verrutschen und versehentlich ein Snapshot-Image herunterzuladen.

Da die Fritzbox während der Installation keine IP-Adressen vergibt, geben Sie der LAN-Schnittstelle Ihres Rechners die statischen IP-Adressen `192.168.178.2` und `192.168.1.2`, jeweils mit der Subnetzmaske `255.255.255.0`. Dann verbinden Sie die

Literatur

[1] Merlin Schumacher, **Darfs ein bisschen mehr sein?**, Alternative Router-Firmware: Was OpenWrt besser macht, c’t 6/2019, S. 154

[2] Ernst Ahlers, **Mehrzonal**, OpenWrt als Router für mehrere Netzwerkzonen einrichten, c’t 9/2019, S. 158

[3] Andrijan Möcker, **Schwesterkiste**, Fritzbox 4040 mit OpenWrt betreiben, c’t 10/2019, S. 28

[4] Andrijan Möcker, **Eintrittsduo**, VPN mit WireGuard und OpenWrt einrichten für Einsteiger, c’t 10/2020, S. 160

Box noch stromlos über eine beliebige LAN-Buchse mit der Schnittstelle Ihres Rechners. Bereiten Sie zunächst das Kommandozeilenfenster mit dem Ramboot-Skript vor: `python eva_ramboot.py <Iitramfs-Datei> 192.168.178.1`. Der Bootloader ist nur wenige Sekunden nach dem Start aktiv, weshalb Sie in einer weiteren Konsole einen Ping starten müssen, um den richtigen Moment zu erkennen: `ping 192.168.178.1`.

Installation

Wechseln Sie in die Konsole mit dem Ramboot-Skript. Versorgen Sie die Fritzbox mit Strom und starten Sie das Skript direkt nach der ersten Ping-Antwort. Der Bootloader ist nur kurz beim Start aktiv; meldet das Skript einen Fehler, trennen Sie die Box kurz vom Strom und wiederholen Sie den Vorgang. Klappt es mehrfach nicht, ist Ihr Netzwerkadapter möglicherweise zu träge. Dann kann ein Switch zwischen Fritzbox und Rechner helfen.

Lief das Skript erfolgreich, pingen Sie die OpenWrt-Default-IP-Adresse `192.168.1.1` an. Nach der ersten Antwort können Sie die finale Installationsdatei mit `scp <Sysupgrade-Datei> root@192.168.1.1:/tmp` auf die Box übertragen. Anschließend verbinden Sie sich per SSH, wechseln in das Verzeichnis `/tmp` und starten die finale Installation:

```
ssh root@192.168.1.1
cd /tmp
sysupgrade -n <Sysupgrade-Datei>
```

Sobald die Power-LED schnell blinkt, bootet OpenWrt. Wenn sich auch nach mehreren Minuten nichts tut, versucht der Bootloader möglicherweise die falsche Partition zu booten. Dann müssen Sie den zugehörigen Bootloader-Parameter ändern: Nehmen Sie die Box vom Strom, pingen Sie erneut `192.168.178.1` an und bereiten Sie in einer weiteren Konsole den Befehl `ftp 192.168.178.1` vor. Stecken Sie das Netzteil wieder an und führen Sie den FTP-Befehl bei der ersten Antwort aus. Benutzername und Kennwort für den FTP-Zugang lauten beide `adam2`. Mit `quote getenv linux_fs_start` lesen Sie den Boot-Parameter aus; schreiben Sie ihn invertiert zurück: `quote setenv linux_fs_start <0 oder 1>`, dann starten Sie die Box neu: `quote reboot`. Anschließend bootet die Box mit OpenWrt.

Netzwerk

Damit der DHCP-Server der Box dem DHCP-Server Ihres Hauptrouters nicht ins Handwerk pfuscht, deaktivieren Sie ihn, sodass auf der Box nur der DHCP-Client läuft. Melden Sie sich dazu auf dem Webinterface unter 192.168.1.1 an, vergeben Sie ein Passwort und wechseln Sie in „Network „Interface“. Beim LAN-Interface klicken Sie auf Edit, setzen im Reiter „DHCP Server“ den Haken bei „Ignore Interface“ und deaktivieren in den untergeordneten „IPv6 Settings“ den „Router Advertisement-Service“ und den „DHCPv6-Service“. Danach ändern Sie in den „General Settings“ das Protocol auf „DHCP client“, bestätigen Sie mit „Switch Protocol“ und Save. Bevor Sie auf „Save & Apply“ klicken, ändern Sie über den Pfeil rechts der Schaltfläche das Verfahren auf „Apply unchecked“ – andernfalls erwartet OpenWrt eine Rückmeldung vom Browser. Anschließend ist die Box bereit für Ihre Experimente und im Heimnetz erreichbar. Die neue IP-Adresse finden Sie beispielsweise mit einem Netzwerkscanner wie Fing oder im Webinterface Ihres Routers. (amo) c't

[5] Andreas Itzchak Rehberg, **Selbstauskunft**, Namensauflösung inklusive Datenschutz fürs Heimnetz, c't 12/2017, S. 130

[6] Carsten Strotmann, **Privatsphäre per Tunnel**, Domain Name Service: Datenschutz selbstgebaut, c't 20/2017, S. 154

[7] Carsten Strotmann, **Privatvermittlung**, Privater Nameserver und Adblocker im LAN, c't 21/2017, S. 158

[8] Carsten Stromann und Dušan Živadinovi, **Erweiterte Privatvermittlung**, Update zu Unbound als privater Nameserver und Adblocker, c't 4/2018, S. 162

OpenWrt-Wiki-Links

ct.de/wm5y



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.ct-special.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)

Koordination: Ann-Sophie Eikermann (ase), Angela Meyer (anm)

Redaktion: Ernst Ahlers (ea), Mirko Dölle (mid), Ronald Eikenberg (rei), Sven Hansen (sha), Urs Mansmann (uma), Pina Merkert (pmk), Andrijan Möcker (amo), Angela Meyer (anm), Peter Siering (ps), Dušan Živadinović (dz)

Mitarbeiter: Alfred Arnold, Jasper Bongertz, Guido R. Hiertz, Berti Kolbow-Lehradt, Sebastian Max, Sebastian Piecha, Alexander Traud

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

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Sarah Hiller, Natalie Hollstein, Kirsten Last, Martina Lübke, Steffi Martens, Marei Stade, Matthias Timm, Ricardo Ulbricht, Ninett Wagner

Fotografie: Andreas Wodrich, Melissa Ramson

Produktion: Christine Kreye (Ltg.), Melanie Becker, Anna Hager, Kevin Harte, Martin Kreft, Pascal Wissner

Illustration: Rudolf A. Blaha, Frankfurt am Main; Thorsten Hübner, Berlin; Thomas Kuhlenbeck, Münster; Andreas Martini, Wettin

Titel: Ninett Wagner, www.flaticon.com, www.freepik.com, www.stock.adobe.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, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung: Beate Gerold, Jörg Mühle

Verlagsleiter: Dr. Alfons Schräder

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: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

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

Vertrieb Einzelverkauf:
VU Verlagsunion KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1800
E-Mail: info@verlagsunion.de

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

Erstverkaufstag: 27.07.2021

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

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen in c't erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2021 by
Heise Medien GmbH & Co. KG

Aufrüsten im Homeoffice

NEU



Heft + PDF mit 29 % Rabatt

c't Hardware fürs Homeoffice 2021

Die Arbeit im Homeoffice gelingt am besten, wenn nicht nur die richtige Software zur Verfügung steht, sondern auch die passende Hardware dazu. Mit einer schlechten Tastatur vertippt man sich ständig, auf pixeligen Monitoren will man keine langen Texte lesen und wenn das WLAN zickt, friert ständig das Bild in der Videokonferenz ein. Die Tests und Kaufberatungen in diesem Heft helfen Ihnen bei der Technik-Auswahl.

Auch als einzelnes Heft erhältlich.

shop.heise.de/ct-hardware-ho21

Heft + PDF für nur 19,90 € ›

› 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

shop.heise.de/ct-hardware-ho21 ›

Vodia

Die perfekte Telefon-anlage für Ihren Router!

Mit der Vodia IOP können Sie nun die Vodia PBX direkt neben Ihrem Router installieren. Und zwar buchstäblich: Die Vodia IOP ist nur so groß wie eine Scheckkarte! Nutzen Sie dafür einfach die VoIP-Anbindung des Routers. Sollten Sie einen separaten VoIP-Telefonanschluss haben, können Sie die IOP auch direkt mit diesem verbinden. Die riesige Auswahl an kompatiblen Geräten – wie IP-Telefonen, Analog-Telefon-Adaptern und Durchsagelautsprechern – und Apps deckt alle Anforderungen ab. Haben Sie die IOP beispielsweise in Ihrer Autowerkstatt installiert, kann Ihre Buchhaltung ihre vom Büro her gewohnte Festnetznummer auch im Homeoffice verwenden. Und das Ganze zu einem Preis, den Sie vielleicht nicht erwarten würden.

Ihre Vorteile auf einen Blick:

- Ausgereifte Telefonanlage auf Basis der Vodia PBX
- Kompatibel mit den gängigen VoIP-Telefonen und SIP-Trunks
- Kostenlose Nutzung von Windows-, Android- und iOS-Apps
- Installation und Wartung über das Webinterface
- Geringer Stromverbrauch, keine beweglichen Teile
- 64 GB Speicher auch für anspruchsvolle Installationen

... und vieles Weitere.

Wenn Sie den persönlichen Kontakt bevorzugen, wenden Sie sich bitte an:
Anastasios Papadopoulos, Vertriebsleiter DACH, Vodia Networks GmbH
Skalitzer Str. 104 • 10997 Berlin • Telefon: +49 30 55578992 • E-Mail: ap@vodia.com

Mehr erfahren auf
https://vodia.com.