

# 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 Technologieentwicklung 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 Surfgeohnheiten vor fremden Augen und Telefonate vor fremden Ohren.

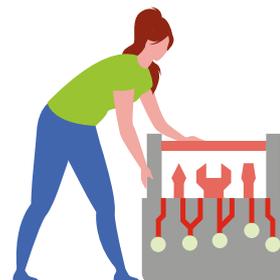
Fällt der Internetzugang aus, kann das zu erheblichen Behinderungen führen. Um Nachteile abzufedern, genügt aber ein einfacher Plan. Damit sind Sie mit Ihrer Fritzbox nervenschonend wieder online, noch bevor der Techniker „DSL-Leitungsanalysator“ buchstabiert hat.

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 Mächtgern-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 Business-Telefone.

- 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





# FRITZBOX

Absichern · Erweitern · Tunen

### Komfortabel telefonieren

- 134 ● Gebrauchte Businesstelefone mit Fritzbox verknüpfen
- 118 ● Abhörer 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

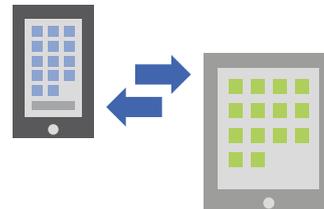
- 40, 6, 10 ● Heimnetz absichern · Tracking verhindern · Privatsphäre schützen
- 36, 28 ● VPN trotz Kabelanschluss einrichten · Malware draußen halten

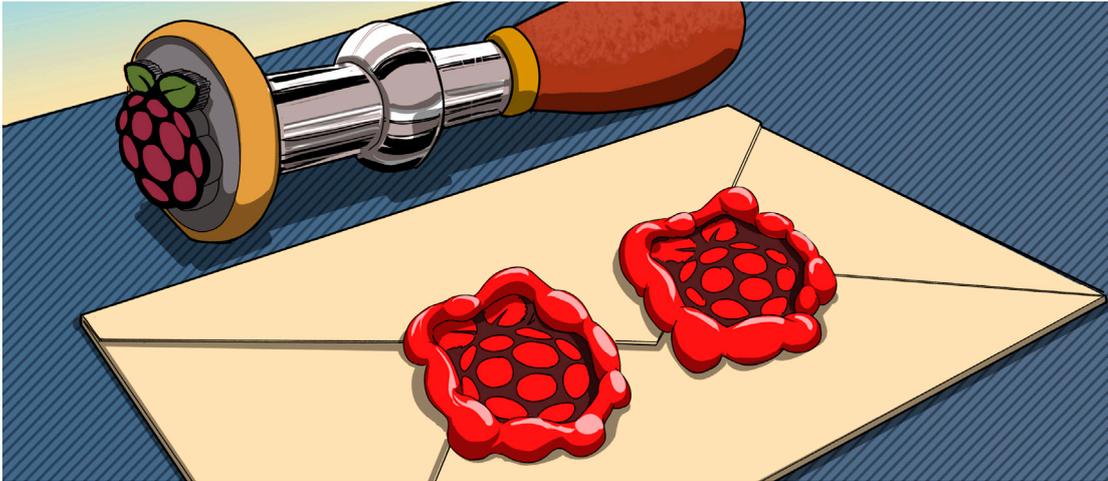
€ 14,90  
inkl. MwSt.  
inkl. Porto



4 190982 314000

 facebook.com/ctspecials





# 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**

**A**n 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](https://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 Paketver-

```
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 Resolvem 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

Lesen Sie mehr in c't Fritzbox 2021



Bild: Andreas Martini

# Extrasichereres 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**

**M**it WPA3 ab FritzOS 7.2x liefert AVM eine Rundenerneuerung 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-Imple-

mentierung 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.

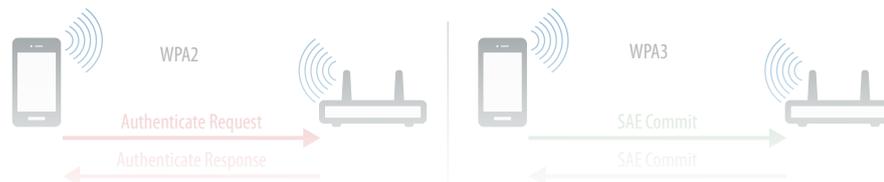
## Bitte würfeln!

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).



Lesen Sie mehr in c't Fritzbox 2021



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**

**S**pätestens, 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



Lesen Sie mehr in c't Fritzbox 2021



# 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**

**S**elbst 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

Unify's 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 UpO-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 Mocker



Lesen Sie mehr in c't Fritzbox 2021



Bild: Thomas Kühlenbeck

# 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**

**D**er 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 abhängen und auch das Gehäuse-design einen Einfluss hat.

Auch in puncto DSL-Modem konnten wir keine Unterschiede feststellen: An unserem Telekom-Super-vectoring-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

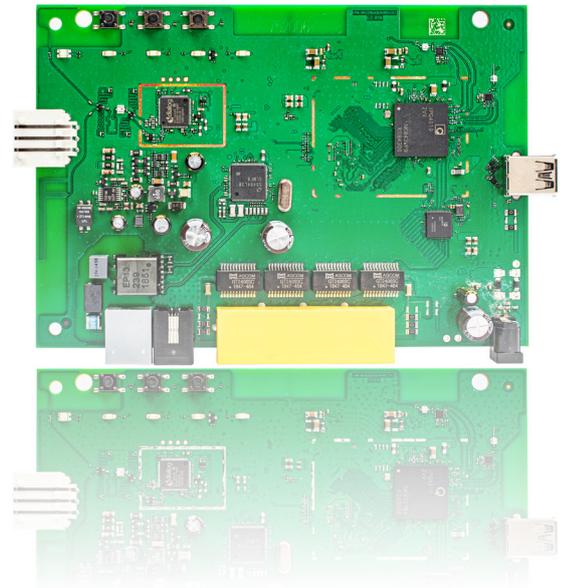
Derart ähnliche Ergebnisse erhält man nur, wenn die Hard- und Software weitgehend gleich sind. Der Blick auf die Platinen bestätigte das: Herzstück beider Geräte ist das Router-System-on-Chip IPQ4019 von Qualcomm mit 128 MByte NAND-Flash und 256 MByte DDR3-RAM. Auf beiden Boards sitzen die glei-

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



Lesen Sie mehr in c't Fritzbox 2021