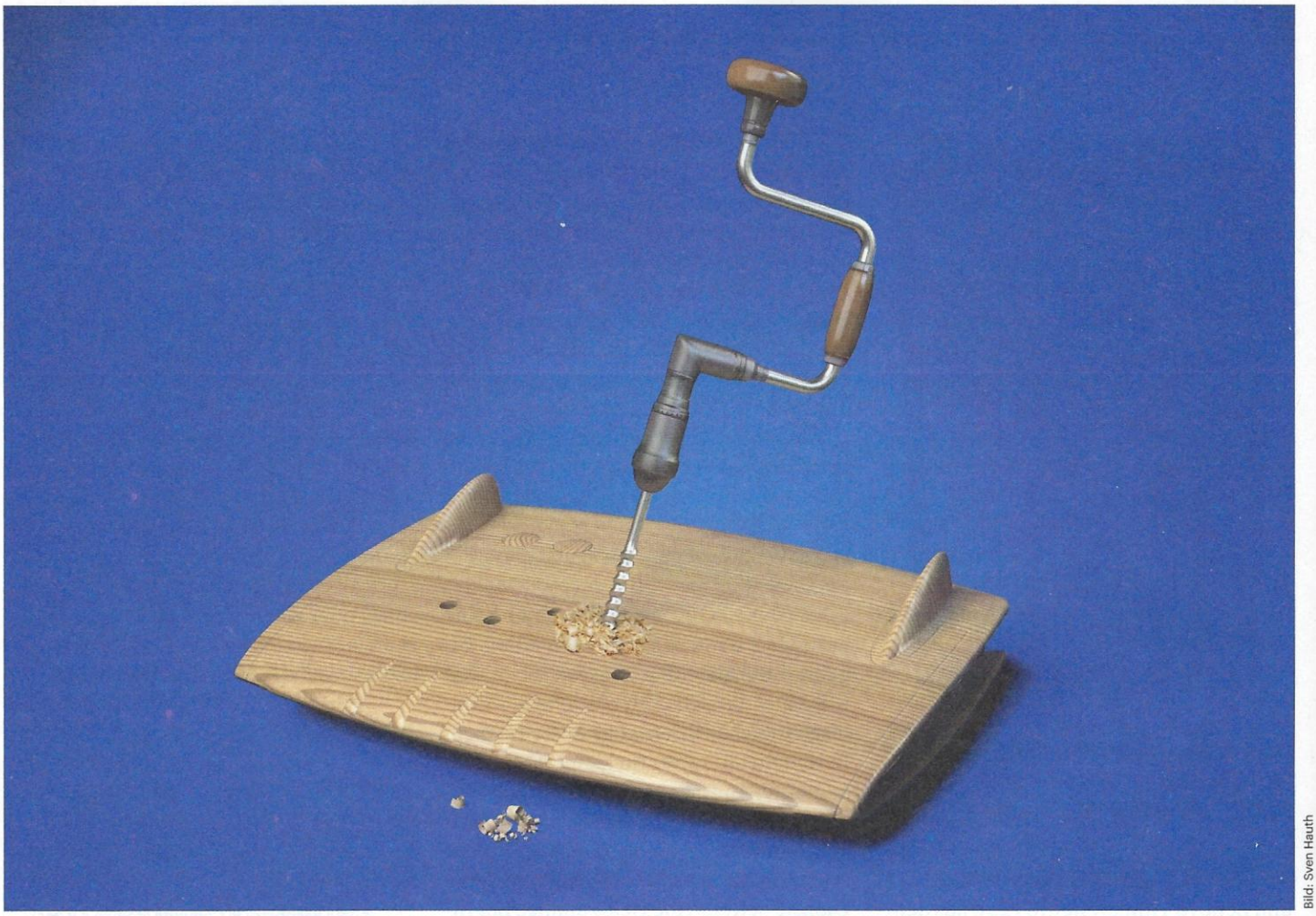


Bild: Sven Hauth

Löchlein bohren

Dienste aus dem eigenen Netz ins Internet bringen

Oft sollen Dienste des eigenen Servers hinter dem heimischen Router aus dem Internet erreichbar sein, etwa der Kalender von Nextcloud oder die Weboberfläche der Smart-Home-Zentrale. Mit einer Fritzbox geht das ganz leicht – ähnlich einfach gelingt das aber auch mit Routern anderer Hersteller.

Von Peter Siering

Ein Server, der hinter einem DSL- oder Kabel-Router steht, wird durch dessen Firewall geschützt. Wer unterwegs etwa mit dem Smartphone auf die Dienste zugreifen will, muss hinter die Firewall gelangen. Dafür bieten die meisten Router Portfreigaben oder -weiterleitungen an (gebräuchlich sind beide Begriffe, sie meinen dasselbe). Die Geräte registrieren dann Netzwerkanfragen von außen und leiten sie an vom Nutzer festgelegte Ports interner Geräte weiter – ähnlich wie sie Anfragen aus dem lokalen Netzwerk ins Internet durchreichen, eben nur in umgekehrter Richtung.

Die ominösen Ports, von denen die Rede ist, sind letztlich Teil einer Netzwerkadresse und tauchen manchmal auch am Ende von URLs auf. So weist „https://ct.de:443“ in der Adresszeile einen Browser an, eine Verbindung zum Webserver auf ct.de aufzubauen und dazu den Port 443 anzusprechen (der für HTTPS verwendet wird). Für eine Fülle der Ports ist definiert, welcher Dienst dahinter steht. Somit muss man den Port üblicherweise nicht angeben.

Die Idee, einen privaten Webserver auf einem ungebräuchlichen Port laufen zu lassen, um ihn notdürftig zu verstecken, ist übrigens doof: Rechner im Internet werden regelmäßig von Portscans heimgesucht, sodass so ein Versteck schnell auffliegt. Die Häscher erkennen nicht nur, dass ein Port offensteht, sondern finden ebenso schnell heraus, mit welchem Dienst sie es dort zu tun haben [1]. Auf einem SSH-Server, den man auf einem ungewöhnlichen Port sicher wähnte, häufen sich schnell die Anmeldeversuche Unbefugter.

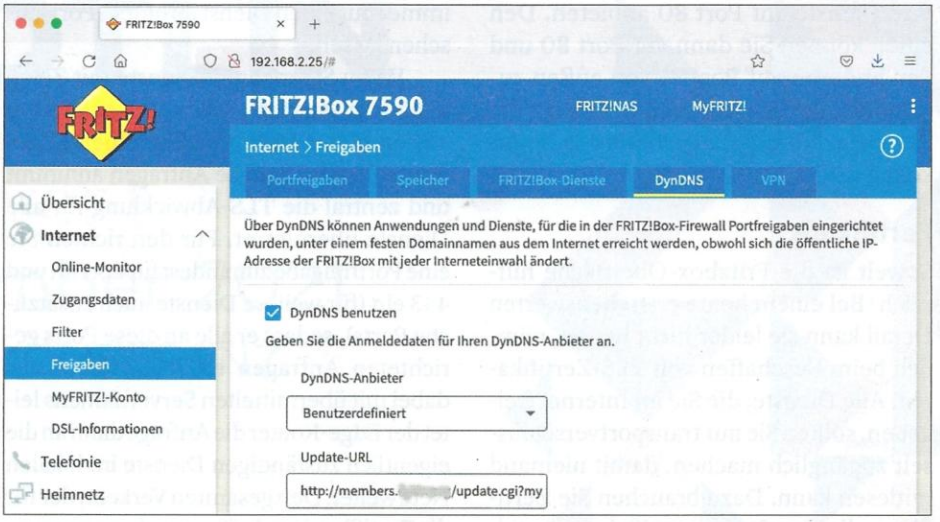
Namenssachen

Damit das Weiterleiten von Ports allein genügt nicht: Die meisten Internetzugänge nutzten dynamische IP-Adressen. Das heißt, dass sich die Adresse gelegentlich oder sogar regelmäßig ändert, unter der der Router und somit auch dahinter angebotene Dienste erreichbar sind. Indem man den Router dazu anweist, nach erfolgreicher Verbindung seine Adresse bei einem Dienst für dynamisches DNS zu hinterlegen, erhält der einen weltweit eindeutigen Namen wie „heise.de“. Dann kann man unter dem registrierten Namen stets die eigene externe IP-Adresse beziehungsweise dahinter angebotene Dienste erreichen.

Die Namen, die Dienste für dynamisches DNS (DynDNS) anbieten, kann man sich indes nicht einfach ausdenken. Sie sind in der Regel begrenzt auf eine Auswahl vorgegebener Internet-Domains wie „dyndns.org“. Lediglich den Host-Anteil der Adresse wie „icke23“, der „dyndns.org“ vorangestellt wird, kann man sich dabei aussuchen, solange das nicht bereits ein anderer Kunde getan hat. Große Provider lassen obendrein in die Firmware ihrer Router nur wenige Dienste für dynamisches DNS zu – oft solche, die ihr kostenloses Modell auf bezahlte Dienste umgestellt haben.

AVM ist da gnädiger: Fritzboxen kennen viele Anbieter und über die Konfiguration von benutzerdefinierten URLs für das Namensupdate bekommt man so ziemlich jeden DynDNS-Dienst eingerichtet. Auch bietet der Routerhersteller selbst im Rahmen seiner MyFritz-Dienste einen DynDNS-Dienst an. Die Fritzbox eines dort registrierten Nutzers erhält einen eindeutigen Namen wie „rtvw4nftt8qxpudp.myfritz.net“. Die Konfiguration läuft unter „Internet“ in „MyFRITZ!-Konto“. Die Eingabe einer E-Mail-Adresse genügt für die Registrierung. Die Konfigurationsoberfläche Ihrer Fritzbox öffnen Sie dadurch nicht ins Internet.

Wenn Ihnen der Sinn nach schöneren Namen als „icke23.dyndns.org“ oder „rtvw4nftt8qxpudp.myfritz.net“ steht, dann bietet sich das Registrieren einer eigenen Domain an. Eine „.de“-Domain gibt es bei den einschlägigen Domain-Hostern für rund 10 Euro pro Jahr. In der Domain-Verwaltung können Sie üblicherweise solche DynDNS-Namen als CNAME eintragen, also eine Weiterleitung von „www.ihrefirma.de“ auf den DynDNS-Namen „icke23.dyndns.org“ einrichten. So brauchen Sie keinen Domain-Hoster zu suchen, der seinen Kunden DynDNS für die eigene Domain erlaubt.



Bei wechselnden IP-Adressen unverzichtbar: ein DynDNS-Dienst, der den Serverdiensten einen Namen gibt. Fritzboxen kennen dafür nicht nur einige vorgefertigte Dienste, sondern lassen sich im Detail konfigurieren.

Nach dem Eintragen eines CNAME für die eigene Domain, also Änderungen an der Konfiguration des Nameservers des Domain-Hosters, brauchen Sie etwas Geduld. Oft dauert es mehrere Stunden, bis sich solche Änderungen im dezentralen DNS-System herumgesprochen haben, also auch der Nameserver des Providers den neuen Namen zur Kenntnis genommen hat.

Weiterleitungen

Die Portfreigaben finden sich bei Fritzboxen unter „Internet“ und dort in „Freigaben“. Das Gerät beziehungsweise die VM, der Container, was auch immer Sie aus dem Internet erreichbar machen wollen, sollte zu diesem Zeitpunkt der Fritzbox bekannt sein; das ist dann der Fall, wenn das Gerät aktiv war und von der Fritzbox eine Adresse erhalten hat. Dann können Sie es bequem auswählen. Andernfalls müssen Sie die IP-Adresse von Hand eingeben, was gerade bei IPv6-Geräten mühsam sein kann.

Bei IPv4 können Sie ein Gerät vollständig dem Internet aussetzen (Exposed Host). Die Fritzbox reicht dann alle eingehenden IPv4-Netzwerkanfragen auf allen Ports an dieses Gerät durch. In der Regel will man das nicht: Wenn Sie gezielt nur die Ports für aktive Dienste öffnen, können Sie entspannt die Gesamtkonfiguration des Geräts vornehmen, etwa einen SSH-Dienst laufen lassen, auch wenn der übers Internet nicht erreichbar sein soll – als Exposed Host wäre jeder Dienst im Internet sichtbar.

Für IPv6 erlaubt es die Fritzbox, mehrere Exposed Hosts einzurichten. Das liegt daran, dass sie bei vielen Internet-Providern auch alle Geräte im lokalen Netz mit einer globalen, also weltweit eindeutigen und erreichbaren IPv6-Adresse versorgt. Das klappt, wenn der Provider der Fritzbox zusätzlich zu ihrer eigenen IPv6-Adresse auch ein IPv6-Präfix aushändigt; ein solches Präfix enthält mehrere IPv6-Netze, aus dem die Fritzbox den Clients Adressen zuteilt. Kein Grund zur Panik: Die Firewall der Fritzbox lässt Pakete an die IPv6-Adressen nicht passieren. Es sei denn, Sie konfigurieren den Client IPv6-seitig als Exposed Host.

Sowohl im Fall von IPv4 als auch von IPv6 ist es zumeist besser, ausgewählte Ports an die Geräte weiterzuleiten, weil man so kaum versehentlich Dienste ins Internet bringen kann; bei einem Exposed Host ist nur eine Frage der Zeit, dass Sie versehentlich nur für den lokalen Einsatz gedachte Dienste öffentlich zugänglich machen. Für eine gezielte Portfreigabe müssen Sie nach der Auswahl des Geräts eben auch auswählen, welchen Netzwerkport Sie erreichbar machen wollen. Beim Aufrufen des Assistenten bietet die Oberfläche die Wahl zwischen MyFritz-Freigabe oder Portfreigabe.

Portfreigabe ist die bessere Option: Damit können Sie auswählen, welcher externe auf welchen internen Port weitergeleitet werden soll. Das kann praktisch sein, wenn Sie mehrere Webserver nach außen freigeben wollen und beide, etwa in einer VM oder einem Container, intern

ihre Dienste auf Port 80 anbieten. Den einen können Sie dann auf Port 80 und den anderen auf Port 81 von außen zugänglich machen. Außerdem erlaubt die Portfreigabe auch die Auswahl von Protokollen wie UDP und TCP.

Zertifikate

Soweit ist die Fritzbox-Oberfläche hilfreich. Bei einem heute erstrebenswerten Detail kann sie leider nicht helfen, nämlich beim Beschaffen von TLS-Zertifikaten. Alle Dienste, die Sie im Internet freigeben, sollten Sie nur transportverschlüsselt zugänglich machen, damit niemand mitlesen kann. Dazu brauchen Sie Zertifikate, die eine Stammzertifizierungsstelle ausgestellt hat, deren Zertifikat Browser und andere Geräte akzeptieren. Bei selbst signierten Zertifikaten würden Sie Nutzer womöglich dazu animieren, Zertifikatswarnungen zu ignorieren – was die besser nicht lernen sollten.

Geeignete Zertifikate liefert die Zertifizierungsstelle Let's Encrypt kostenlos. Um ein solches Zertifikat zu erhalten, kann man auf oftmals in einzelnen Serverdiensten vorhandene Funktionen dafür zurückgreifen. Das hat allerdings den Nachteil, dass der Prozess, den eine Automatik ja für die nur 90 Tage gültigen Zertifikate wiederholen muss, nur für genau diesen einen Dienst funktioniert. Der für die Aktualisierung gebräuchliche Mechanismus von Let's Encrypt (ACME) setzt voraus, dass auf Port 80 ein speziell präparierter Webserver für die Zertifikatsausstellung und -aktualisierung antwortet. Sie können aber immer nur einen Dienst an einem Port lauschen lassen.

Wenn Sie mehrere Dienste mit Zertifikaten ausstatten wollen, lassen Sie am besten hinter Ihrer Fritzbox einen Edge-Router laufen, der alle Anfragen annimmt und zentral die TLS-Abwicklung für alle Dienste übernimmt. Für den richten Sie eine Portfreigabe zumindest für Port 80 und 443 ein (für weitere Dienste auch zusätzliche Ports), sodass er alle an diese Ports gerichteten Anfragen erhält. Anhand des dabei mit übermittelten Servernamens leitet der Edge-Router die Anfrage dann an die eigentlich zuständigen Dienste im lokalen Netz weiter. Den gesamten Verkehr, der für die Zertifikatsbeschaffung und -erneuerung notwendig ist, wickelt er selbst ab.

Als Edge-Router empfiehlt sich die Open-Source-Anwendung Traefik [2]. Wenn Sie bereits mit Containern hantieren, wird Ihnen Traefik möglicherweise vertraut sein. Alle anderen sollten sich etwas Zeit nehmen: Bis man Traefik so weit durchschaut hat, dass man es im Blindflug einsetzen kann, vergeht schon einige Zeit. Besonders gilt das, wenn Sie es manuell betreiben und nicht den Komfort einer Container-Umgebung nutzen, in der Traefik idealerweise neue Container namentlich kennt und sogar im DNS registrieren kann.

Aber es geht auch zu Fuß: Das in Go geschriebene Traefik gibt es auf der Release-Page in GitHub für diverse Plattformen als ausführbare Datei (siehe ct.de/yfaa). Diese Programmdatei sowie eine Datei mit einer Grundkonfiguration genügen, um Traefik auf einem beliebigen Host hinter Ihrem Router in Betrieb zu nehmen. Für jeden Dienst, für den es Vermittlung und Zertifikatsbeschaffung erledigen soll, müssen Sie dann eine weitere Beschreibung in einer Konfigurationsdatei ablegen. Ein Beispiel für einen einfachen Webserver stellen wir zum Download bereit.

Sicheres Ende

Dienste hinter einem Router zu betreiben, ist kein Hexenwerk. Wichtig ist, dass Sie stets sicherstellen, nicht die falschen Dienste ins Netz zu bringen, und diese akribisch zu konfigurieren. Diese sollten nur nach einer Anmeldung zugänglich sein. Sie sollten nur starke Kennwörter nutzen und eventuelle Mitbenutzer anhalten, es ebenso zu halten. Dass Sie regelmäßig, am besten automatisiert, Sicherheitsupdates einspielen sollten, sei nur der Vollständigkeit halber erwähnt. Falls Sie sehr hohe Ansprüche an die Sicherheit haben, wäre auch ein VPN-Zugang in Ihr Netz eine Option, um darüber interne Dienste erreichbar zu machen – das allerdings erfordert zumindest eine Portfreigabe für den VPN-Verkehr, wenn der Router nicht selbst den VPN-Server gibt. *(ps@ct.de)* c't

Literatur

[1] Jan Mahn, Merlin Schumacher, c't deckt auf, Dateien, IoT und Industrieanlagen ungeschützt im Netz, c't 23/2020, S. 14

[2] Jan Mahn, HTTP-Einweiser, Eingehenden HTTP-Verkehr mit Traefik routen, c't 17/2019, S. 158

Traefik-Beispiel für Stand-alone-Betrieb: ct.de/yfaa

Portfreigaben: IPv4 versus IPv6

Mit einer Portfreigabe erlauben Sie einem Router wie der Fritzbox, eingehende Netzwerkverbindungen weiterzuleiten. Die sind an einen Port gerichtet, zum Beispiel an den für unverschlüsselte Webzugriffe verwendeten Port 80. Den öffnen Sie in der Firewall wahlweise für IPv4 und für IPv6.
Die Wege, die die Pakete dann nehmen, unterscheiden sich: Bei IPv4 kann die Fritzbox die Anfrage an genau ein Gerät mit privater IP-Adresse im Intranet weiterleiten, denn die Fritzbox hat selbst nur eine globale IPv4-Adresse.
Bei vollumfänglicher IPv6-Unterstützung erhält jedes Gerät hinter der Fritzbox eine eigene globale IPv6-Adresse. Dann reicht die Fritzbox die Pakete direkt an die globale IPv6-Adresse des Geräts im Intranet durch. Die IPv6-Adresse der Fritzbox ist nicht beteiligt.