Bild: Thorsten Hübner

Keinbruch

Fritzboxen sicher betreiben: Auto-Update, Stealth Mode, WPA3 und vieles mehr

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 die IP-Adresse 185.232.52.55 etliche Male einzuloggen.

Gibt man diese Adresse bei Google ein, landet man schnell bei AbuseIPDB, einer Website, über die 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 auch die Fritzbox explizit als Angriffsziel erwähnt. Recherchiert man weiter, zeigt sich, dass sich die IP-Adresse bereits seit Sommer 2020 auffällig verhält und AVM-Router attackiert.

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-Dienste Shodan: Er verortet die Adresse in Amsterdam und ordnet ihr den

Hostnamen „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 irgendeinem Rechenzentrum. Da die OpenSSH-Version mit 7.4 reichlich alt ist und Sicherheitslücken enthält, wäre es 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 zahllose 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 der Eindringling in spe 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 zur nächsten Haustür weiter und versucht sein Glück erneut. Das ist ohne jede Frage unangenehm, doch noch nicht gefährlich – schließlich bleibt 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.

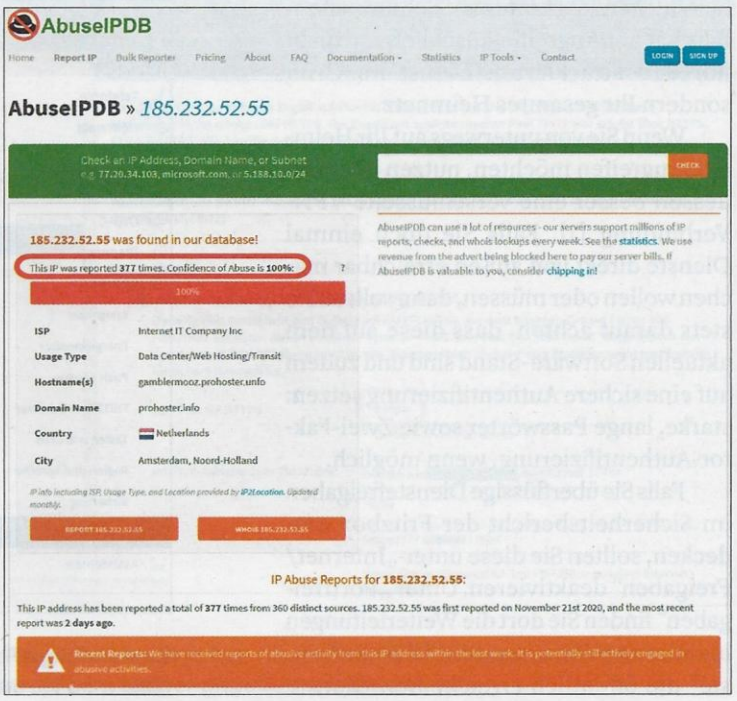
Bevor Sie mit dem Sicherheits-Check loslegen, sollten Sie sicherstellen, dass das Fundament stabil ist: Öffnen Sie die Weboberfläche des Routers, die Sie aus dem internen Netz über http://fritz.box erreichen, und stellen Sie sicher unter „System/Update“ sicher, dass die aktuelle Firmware-Version (FritzOS) 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 AVM-Router automatisch Firmware-Updates einspielt, die der Hersteller für sicherheitsrelevant hält. Darunter können Sie bei „Zeitraum für Updates“ noch eine 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 aktuellen Firmware-Versionen für die verschiedenen Fritzbox-Modelle finden Sie unter ct.de/ynna. Falls Sie den AVM-Router von Ihrem Provider erhalten haben, dann können Sie Firmware-Updates möglicherweise nicht selbst installieren. Dies ist insbesondere bei den Providern von Internet per TV-Kabel der Fall. In diesem Fall können Sie nur abwarten, bis der Provider das Update einspielt.

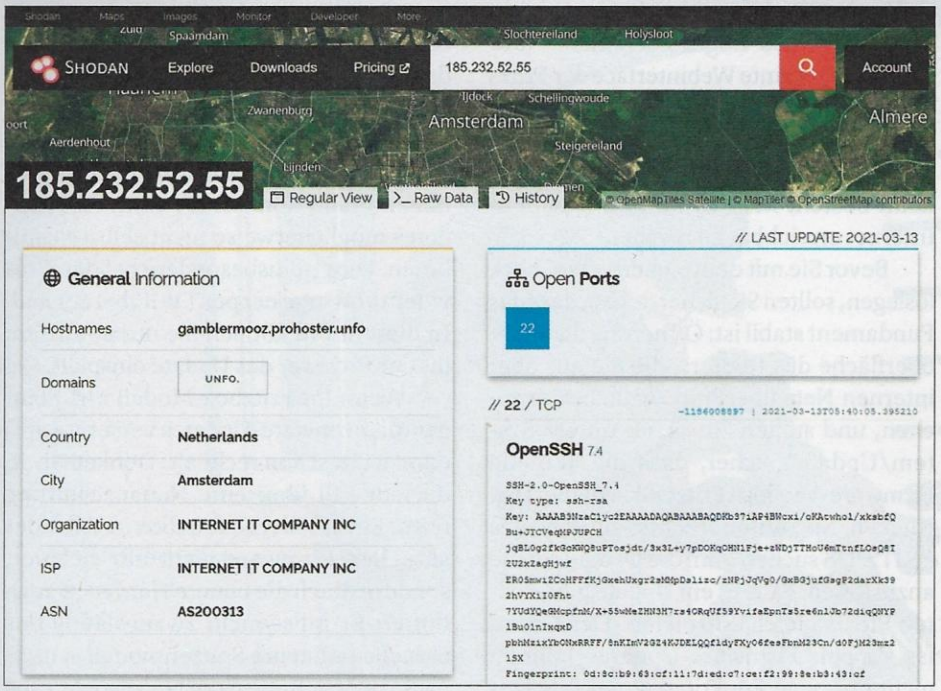
Wenn Ihr Fritzbox-Modell nicht länger mit Firmware-Updates versorgt wird, dann ist es schon recht alt. Denken Sie in diesem Fall über eine Neuanschaffung nach. Eine moderne Fritzbox ist dank der aktuellen Firmware nicht nur sicherer, sondern durch die neuere Hardware auch flotter. Es muss nicht zwangsläufig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

Fenster und Türen verschließen

Steht das Firmware-Fundament, dann können Sie sich einen Überblick über die allgemeine Sicherheitslage verschaffen. Öffnen Sie im Webinterface unter „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“ listet der Router eigene Dienste auf, die für Zugriffe aus dem



Die 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 SSH-Server aus Amsterdam.

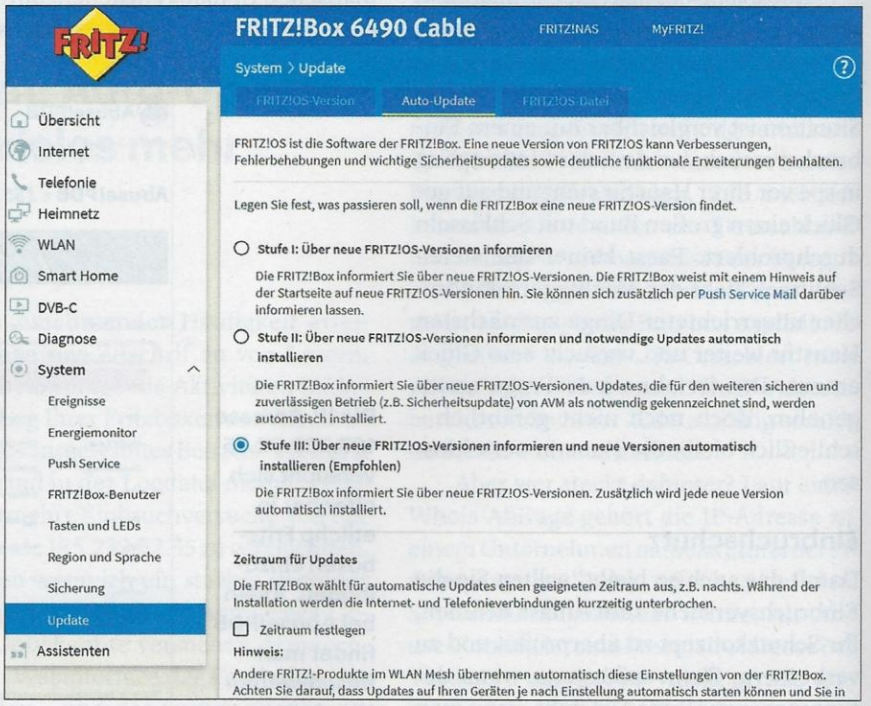
Internet erreichbar sind und unter „Portfreigaben auf Heimnetzgeräte“ erfahren Sie, welche Dienste anderer Geräten im Heimnetz von außen zugänglich sind.

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

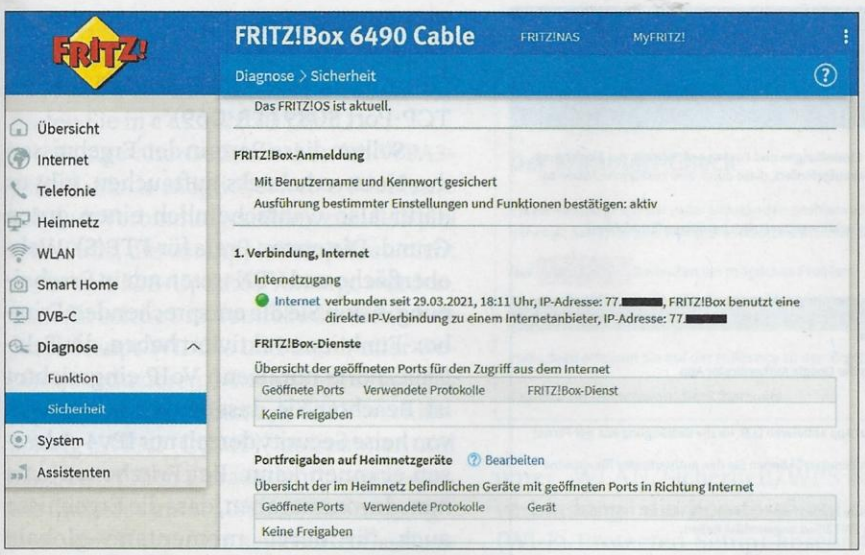
Wenn Sie von unterwegs auf Ihr Heimnetz zugreifen möchten, nutzen Sie stattdessen besser eine verschlüsselte VPN-Verbindung [1]. Falls Sie doch einmal Dienste direkt von außen erreichbar machen wollen oder müssen, dann sollten Sie stets darauf achten, dass diese auf dem aktuellen Software-Stand sind 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 unter „Internet/Freigaben“ deaktivieren. Unter „Portfreigaben“ finden Sie dort die Weiterleitungen ins interne Netz, unter „FRITZ!Box-Dienste“ die öffentlich erreichbaren Dienste der Fritzbox selbst. 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 unter „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. Der erlaubte Bereich für TCP-Ports 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 im Einsatz ist. Um Angreifern das Auffinden offener Ports nicht leichter als nötig zu machen, sollten Sie unter „Internet/Filter/Globale Filtereinstellungen“ die Option „Firewall im Stealth Mode“ einschalten. Das erschwert den Angreifern Portscans enorm, weil die Fritzbox



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



Alles auf einen Blick: Unter „Diagnose/Sicherheit" listet die Fritzbox viele sicherheitsrelevante Einstellungen auf. Dort finden Sie auch Dienste, die aus dem Internet erreichbar sind.

nun nicht mehr mit einem Lebenszeichen reagiert (Zugriff verweigert), sondern gar nicht.

Sicherheitsschloss installieren

Falls ein Angreifer das Webinterface auf dem exotischen Port entdeckt, wird er mit einem Login-Formular konfrontiert, in das er einen Benutzernamen und ein Passwort eingeben muss. Nur wenn beide Angaben stimmen, kann er die Fritzbox steuern. 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 auf „System/FRITZ!Box-Benutzer". Anschließend können Sie einen vorhandenen 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 sich beim späteren Fernzugriff auf die Fritzbox noch daran erinnern können. 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 anderen 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.

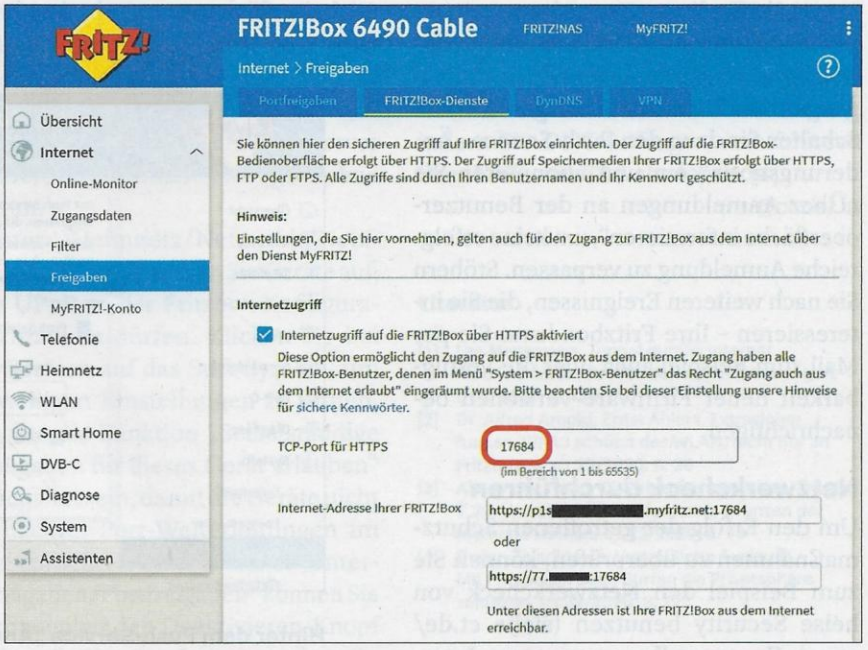
Stellen Sie auf der Unterseite „Zusätzliche Bestätigung" sicher, dass die Option „Ausführung bestimmter Einstellungen und Funktionen zusätzlich bestätigen (Empfohlen)" eingeschaltet ist. Dann müssen Sie beim Ändern folgenreicher Einstellungen gesondert bestätigen, dass Sie vor Ort und somit wahrscheinlich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

Recht neu ist die Möglichkeit, die zusätzliche Bestätigung auch aus der Ferne durchzuführen, etwa 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 kurzzeitig gültige Einmalcodes generieren, mit denen Sie sicherheitskritische Einstellungen auch aus der Ferne ändern dürfen. Der Einmalcode ersetzt den Knopfdruck am Router. Leider ist es derzeit noch nicht möglich, schon das Einloggen am Webinterface der Fritzbox durch diesen zweiten Faktor zu schützen.

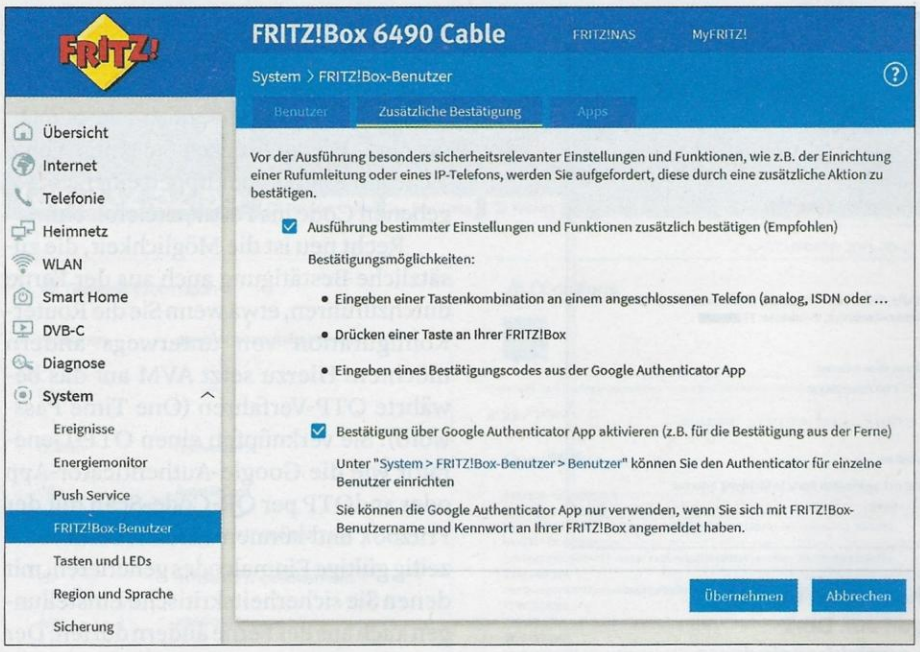
Wenn Sie schon mal den Bereich „FRITZ!Box-Benutzer" offen haben, sollten Sie dort auch gleich unter „Apps" nicht länger genutzten Apps die Zugriffsrechte auf den Router entziehen. Klicken Sie hierzu neben einem Eintrag auf das rote X.

Alarmanlage scharfschalten

Um über verdächtige Aktivitäten auf dem Laufenden zu bleiben, sollten Sie von Zeit



Ändert man die Ports der Fritzbox-Dienste auf einen hohen, zufälligen Port, klopft deutlich seltener ungebetener Besuch an.



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

zu Zeit das Ereignis-Log unter „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.

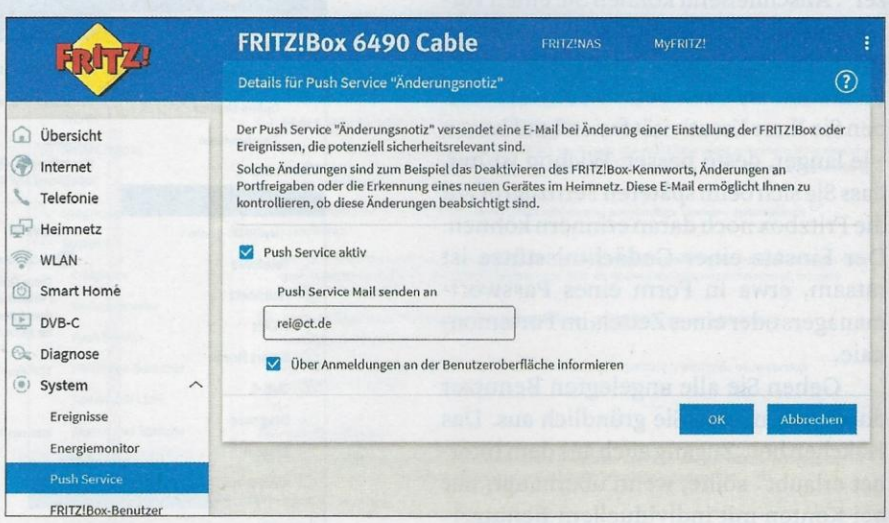
Über „System/Push Service“ kann die Fritzbox per Mail über diverse Ereignisse informieren. Sie müssen zunächst unter „Absender“ ein Mailkonto konfigurieren, das die Fritzbox zum Versand nutzen soll. Legen Sie für diesen Zweck besser ein separates Konto an, damit Sie nicht das Kennwort Ihres primär genutzten 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-Versionen benachrichtigen.

Netzwerkcheck durchführen

Um den Erfolg der getroffenen Schutzmaßnahmen zu überprüfen, können Sie zum Beispiel den Netzwerkcheck von heise Security benutzen (siehe ct.de/ynna): Er scannt Ihre momentane Internet-IPv4-Adresse nach offenen Standard-Ports und zeigt eine Warnung an, 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 Funktionen wie die VoIP-Telefonie einsatzfähig sind. 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 auftauchen, gibt es dafür also wahrscheinlich einen guten Grund. Die ersten Ports für FTP(S), Weboberfläche und VPN treten nur in Erscheinung, wenn Sie die entsprechenden Fritzbox-Funktionen aktiviert haben, die Telefonie-Ports nur, wenn VoIP eingerichtet ist. Beachten Sie, dass der Netzwerkcheck von heise Security derzeit nur IPv4-Adressen scannen kann. Bei Fritzboxen darf man davon ausgehen, dass die Ergebnisse auch für deren momentane 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 werden, damit sich Ihre Nachbarn nicht in Ihrem Heimnetz umschauen oder ungefragt über Ihren Anschluss surfen. 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 unterstützen, 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-



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.

Geräten (PMF) aktivieren" aktiv sein. Einen ausführlichen Hintergrundartikel über die Vor- und Nachteile von WPA3 finden Sie in c't 22/2020 [2].

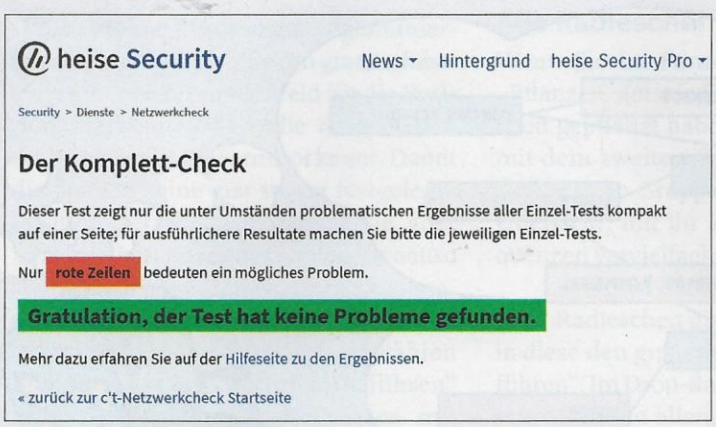
Einige alte Geräte haben im WPA3-Mixed-Mode möglicherweise Probleme mit dem Verbindungsaufbau, zum Beispiel alte iPads, die von Apple seit Jahren nicht mehr mit iOS-Updates versorgt wurden. Statt für solche Problemfälle die Sicherheit Ihres Haupt-WLANs und damit aller Geräte zu reduzieren, können Sie einfach das Gastnetz der Fritzbox mit der Verschlüsselung „WPA2 (CCMP)" aufspannen und die betroffenen Geräte damit verbinden. 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 unter „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.



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.

Hintertüren absichern

Damit Ihr mühsam errichteter 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.

Unter „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 dürfen. 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. In c't 22/2020 haben wir ausführlich beschrieben, wie Sie mit der Fritzbox verschlüsselt über VoIP telefonieren [3] und Ihre Privatsphäre beim Surfen verbessern, indem Sie DNS-Anfragen verschlüsselt über DNS over TLS abwickeln [4].

(rei@ct.de) **ct**

Literatur

[1] Urs Mansmann, Tunnel durchs Internet, Mobile Geräte mit VPN sicher ins Netz bringen, c't 3/2016, S. 126
[2] Dr. Alfred Arnold, Ernst Ahlers, Extrasicher funken, WPA3 schützt das WLAN, nicht nur an Fritzboxen, c't 22/2020, S. 26
[3] Alexander Traud, Chiffriert fernsprechen, FritzOS 7.20: Verschlüsselt telefonieren, Grenzen der Methode kennen, c't 22/2020, S. 18
[4] Dušan Živadinović, Vertrauliche Auskunft, Mit Fritzboxen beim Surfen die Privatsphäre schützen, c't 22/2020, S. 22

Firmware-Versionen & Netzwerkcheck: ***ct.de/ynna***