Bild: Andreas Martini

Speichern ohne Verluste

NAS sicher betreiben

Ein rätselhafter Fall: Statt seiner Daten fand unser Leser Gunther J. nur noch ein Erpresserschreiben auf seinem NAS. Er ahnte noch nicht, dass sich der Netzwerkspeicher sein eigenes Datengrab geschaufelt hatte. So kam es dazu – und so schützen Sie sich.

Von Ronald Eikenberg

Als c't-Leser Gunther J. seine Urlaubsfotos durchstöbern wollte, erlebte er eine unangenehme Überraschung: Alle Dateien auf dem ansonsten zuverlässigen NAS waren gelöscht. Stattdessen entdeckte er eine Datei namens „DATA RECOVERY !!!!.txt“, die wie folgt beginnt: „YOUR REMOTE STORAGE WAS COMPROMISED. YOUR FILES ARE IN OUR POSSESSION.“ J. war offenbar Opfer einer Cyber-Gang geworden, die sich an seinen Urlaubsfotos zu schaffen gemacht hatte.

Die Täter behaupteten, die Dateien seien in Sicherheit, verschlüsselt auf einem Server. Um die Urlaubsfotos aus der digitalen Geiselhaft zu befreien, solle J. 0,03 Bitcoin an die Adresse 18bvWVxx3KD3gaqkBoPSwShimUWkG1eZNL überweisen, das entspricht umgerechnet rund 400 Euro. Doch da gab es zwei Probleme: Zum einen war die Frist der Erpressergruppe, die sich selbst ironischerweise „Data Recovery“ nennt, längst abgelaufen – J. hatte die Misere erst nach zwei Monaten entdeckt. Zum anderen ist es immer eine schlechte Idee, mit Erpressern zu verhandeln.

Gemeinsam mit seiner Frau suchte Gunther J. nach einem Weg, die Urlaubsfotos zu retten. Dann hatte sie eine Idee, die kurz darauf auch in die Tat umgesetzt wurde: Die beiden riefen in der c't-Redaktion an. Bei uns melden sich häufig Opfer von Cyber-Erpressern, doch dieser Fall machte uns besonders neugierig. Denn es war völlig rätselhaft, wie die Täter auf das NAS zugreifen konnten. Es war schnell klar, dass der Anrufer sein Heimnetz mit Bedacht aufgebaut und konfiguriert hatte.

Meist gelingen solche Angriffe, weil ein NAS unzureichend abgesichert und über eine Port-Weiterleitung im Router von außen zugänglich gemacht wurde. Doch

das war anscheinend nicht der Fall, J. griff nur von zu Hause auf seinen Netzwerkspeicher mit den Urlaubsfotos zu und hatte auch keine Port-Weiterleitung eingerichtet. Theoretisch kann die Attacke auch von einem infizierten Rechner im lokalen Netz ausgegangen sein, doch auch diese These schien unwahrscheinlich: J. hatte sämtliche Rechner bereits vor seinem Anruf mit Desinfec't auf Virenbefall untersucht – keine Funde, alles war sauber.

Dennoch war es den Cyber-Erpressern offensichtlich gelungen, auf sein NAS zuzugreifen und die Urlaubsfotos zu löschen. J. erzählte, dass er vor dem Vorfall seine Fritzbox, an der das NAS hing, durch den Standard-Router seines Providers Vodafone ersetzt hatte, ein Gerät des Typs CBN CH6640E. Zwar machte dieses Modell schon in der Vergangenheit durch haarsträubende Sicherheitslücken Schlagzeilen. Vodafone hat die Probleme jedoch längst mit einem automatisch verteilten Firmware-Update gelöst. Wir baten J., uns weitere Informationen zu mailen, und gaben ihm den Tipp, die beiden NAS-Festplatten in einen Rechner einzubauen und sie dort mit dem in Desinfec't enthaltenen Datenrettungs-Tool photorec zu untersuchen – in der Hoffnung, dass sich die Urlaubsfotos doch noch wiederherstellen lassen.

Erpresserbrief statt Urlaubsfotos

Gunther J. schickte uns unter anderem das Erpresserschreiben, das er auf seinem NAS entdeckt hatte. Zu der darin angegebenen Bitcoin-Adresse lieferte Google interessante Details: Sein NAS ist offenbar einer größeren Angriffswelle zum Opfer gefallen, die auf bestimmte NAS-Modelle des Herstellers LenovoEMC (früher Iomega) abzielt. Tatsächlich hat unser Leser ein solches NAS im Einsatz, nämlich ein Iomega StorCenter ix2-200. Über blockchain.com fanden wir heraus, dass auf der Bitcoin-Adresse der Täter immerhin gut 0.13 BTC eingegangen waren, umgerechnet über 1700 Euro. Weitere Recherchen ergaben, dass die Angreifer vermutlich eine Sicherheitslücke in der Iomega-Firmware ausnutzten. Durch ein ungeschütztes API ist es möglich, ohne Authentifizierung auf das Dateisystem des NAS zuzugreifen (CVE-2019-6160). Im August 2019 hatte Lenovo auf seiner Website vor diesem akuten Sicherheitsproblem gewarnt und ein Firmware-Update zur Verfügung gestellt. Das war unserem Leser offenbar entgangen. Eine Rückfrage ergab, dass die von ihm eingesetzte Firmware älter war.

Doch der Fall war noch längst nicht gelöst, denn auch ein ungeschütztes API ist erstmal nicht für Angreifer aus dem Internet erreichbar – und eine Port-Weiterleitung im Router hatte J. ja nicht eingerichtet. Den letzten Teil des Rätsels löste unser Leser selbst: Er entdeckte, dass in dem Vodafone-Router sehr wohl eine Weiterleitung aufs NAS eingerichtet war. Aber wer hatte die angelegt, wenn nicht J.? Der Übeltäter war das verwundbare Iomega-NAS selbst: Gut versteckt auf Seite 92 des Handbuchs findet sich der folgende Hinweis: „Router-Port-Weiterleitung: Einige Router haben eine UPnP-Option. Bei einem UPnP-Router kann die Software des Iomega Geräts bei Aktivierung automatisch die richtigen Weiterleitungs-Ports konfigurieren."

J. hatte vergessen, nach einem Reset des Routers die UPnP-Funktion abzuschalten. Das NAS hat dies bemerkt, selbstständig ein Port-Forwarding anlegt – und sich damit sein eigenes Datengrab geschaufelt. Die Täter hatten noch am Tag des Router-Resets zugeschlagen. Doch auch diese Geschichte hat ein Happy End: Nachdem der Datenretter photorec durchgelaufen war, konnte unser Leser wieder auf seine Urlaubsfotos zugreifen. Einzig die Sortierung der zahlreichen Dateien war durcheinander geraten, doch das war schnell behoben.

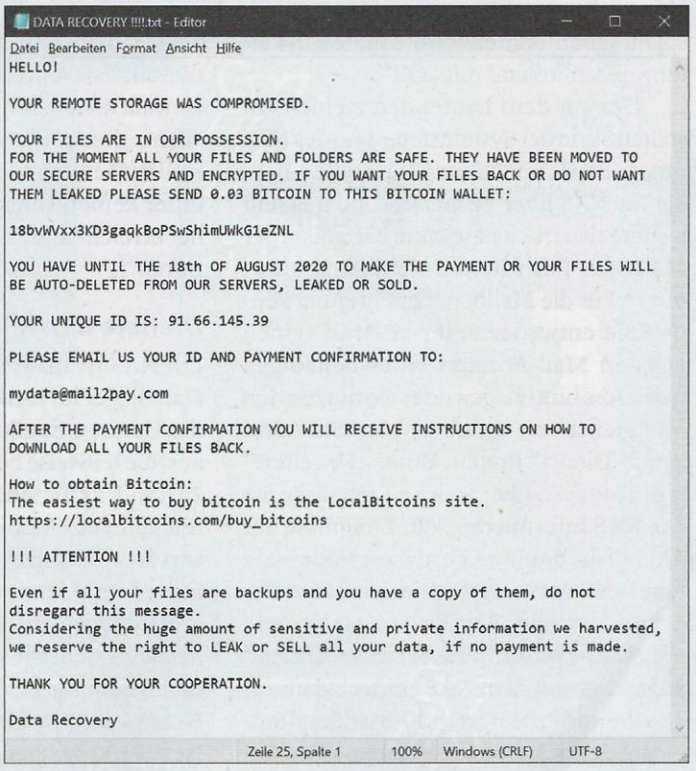
Jetzt sind Sie dran!

Der Fall demonstriert, wie schwierig es ist, Geräte im lokalen Netz vor Hackern zu schützen – selbst wenn man die Gefahren kennt. Damit es Ihnen nicht ähnlich ergeht, fassen wir die wichtigsten Handgriffe zum Absichern eines NAS am Beispiel eines Synology-Geräts in diesem Artikel zusammen. Die Tipps gelten sinngemäß für alle anderen Marken. So können Sie Ihre Daten nicht nur vor Cyber-Angriffen schützen, sondern auch vor anderen Arten des Datenverlustes.

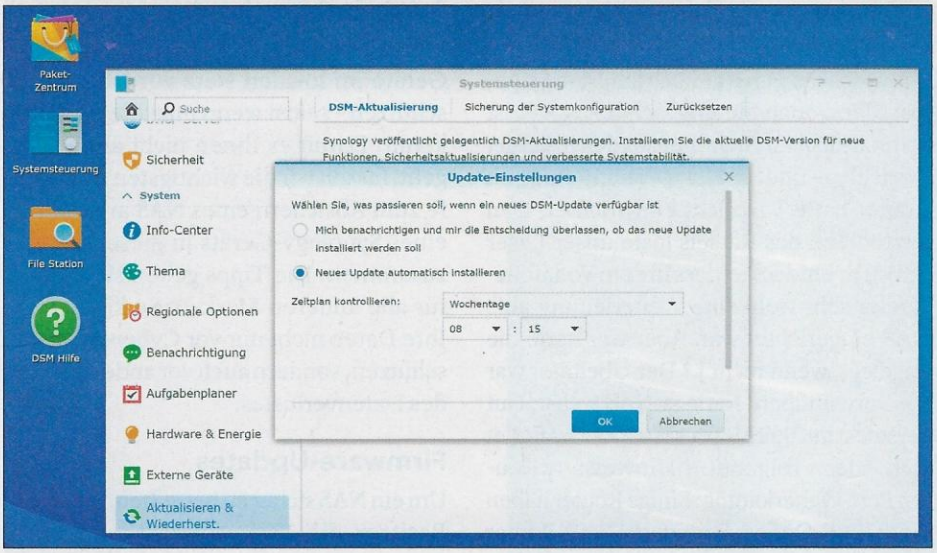
Firmware-Updates

Um ein NAS sicher zu betreiben, muss sein Besitzer die Firmware aktuell halten. Firmware-Updates schließen häufig Sicherheitslücken, durch die Angreifer auf Ihre Daten zugreifen können. Im Idealfall kümmert sich das NAS selbsttätig darum: Es installiert verfügbare Updates automatisch oder informiert den Nutzer zumindest, damit dieser die Installation anstoßen kann. Wenn Ihr NAS einen Auto-Update-Mechanismus hat, schalten Sie ihn ein. Falls das NAS Sie über Updates benachrichtigen kann, etwa per Push-Nachricht oder Mail, aktivieren Sie auch diese Funktion.

Öffnen Sie die Konfigurationsoberfläche im Browser und loggen Sie sich ein. Anschließend klicken Sie auf „Systemsteuerung/Aktualisieren & Wiederherst.",



Das ist alles, was die Cyber-Erpresser auf dem NAS hinterließen: einen Erpresserbrief, in dem sie 0,03 Bitcoin (etwa 400 Euro) Lösegeld fordern.



Firmware-Updates sorgen für Sicherheit. Im Idealfall kümmert sich das NAS automatisch darum.

um zu erfahren, ob die installierte Firmware (Synology spricht von DSM, Disk Station Manager) auf dem aktuellen Stand ist. Falls nicht, können Sie die Aktualisierung direkt anstoßen. Anschließend klicken Sie auf den Button „Update-Einstellungen", um die automatische Update-Installation einzuschalten. Aktivieren Sie hier die Einstellung „Neues Update automatisch installieren". Sie können dort außerdem den Zeitplan für die Installation verändern, um zu verhindern, dass Ihr NAS werktags während der Arbeit im Homeoffice ausfällt, weil es Updates einspielt. Übernehmen Sie die neue Einstellung anschließend mit „OK".

Um auf dem Laufenden zu bleiben, sollten Sie in der Systemsteuerung des NAS unter „Benachrichtigung" einstellen, dass Sie Ihr NAS über Firmware-Updates und weitere sicherheitsrelevante Ereignisse per Mail oder Push-Benachrichtigung informiert. Für die Mailbenachrichtigung können Sie entweder unter „E-Mail" einen eigenen Mail-Account eines beliebigen Anbieters hinterlegen oder Sie nutzen den Maildienst von Synology, den Sie unter „Push-Dienst" finden. Unter „Erweitert" legen Sie fest, über welche Ereignisse Sie das NAS informieren soll. Ereignisse zur Aktualisierung der Firmware finden Sie unter „System", weitere interessante Berichte kann Ihnen der „Sicherheitsberater" schicken, etwa wenn das System ein Schadprogramm auf dem NAS entdeckt hat.

Wenn Sie bei Ihrem NAS weder Auto-Updates noch Update-Benachrichtigungen einstellen können, dann setzen Sie sich am besten einen wiederkehrenden Kalendereintrag, der Sie daran erinnert, regelmäßig auf der Hersteller-Website nach Firmware-Updates zu schauen; zum Beispiel alle vier Wochen, mindestens aber alle drei Monate. Überprüfen Sie, ob der NAS-Hersteller Ihr Modell überhaupt noch mit Firmware-Updates versorgt. Falls Sie hierzu keine Informationen auf der Herstellerseite finden, können Sie per Mail beim Hersteller nachfragen. Liegt das letzte Update bereits mehrere Jahre zurück, dann hat der Hersteller den Support höchstwahrscheinlich eingestellt. In diesem Fall sollten Sie darüber nachdenken, auf ein modernes Gerät umzusteigen. Wenn dies nicht infrage kommt, dann stellen Sie zumindest sicher, dass Ihr NAS unter keinen Umständen aus dem Internet erreichbar ist (siehe „Router konfigurieren").

Dienste einstellen

Ein NAS ist inzwischen viel mehr als ein Datenlager im LAN: Die Hersteller statten die Geräte mit allerlei Zusatzfunktionen aus, die teilweise bereits im Auslieferungszustand aktiv sind. Solche Funktionen reichen vom Medien- bis hin zum Mailserver. Allerdings bieten sie Angreifern mit jedem aktiven Dienst eine weitere Angriffsmöglichkeit. Halten Sie die Angriffsfläche so klein wie möglich, indem Sie alle nicht benötigten Dienste deaktivieren. Nutzen Sie Ihr NAS am besten nur als Netzwerkspeicher, alle weiteren Dienste sind auf einem anderen System, etwa einem Raspberry Pi, besser aufgehoben.

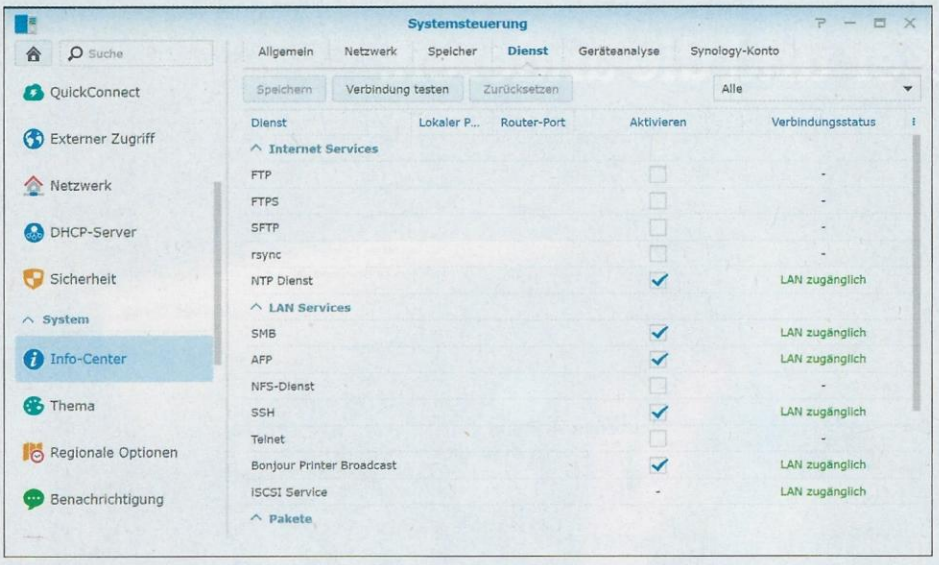
Bei den Synology-NAS finden Sie eine Übersicht über die laufenden Dienste in der Systemsteuerung unter „Info-Center/Dienst". Dort können Sie bei nicht länger benötigten Diensten das Häkchen bei „Aktivieren" entfernen. Klicken Sie anschließend auf „Speichern", um die Änderungen zu übernehmen. Schauen Sie im Paket-Zentrum unter „Installiert" nach nicht verwendeten Apps und deinstallieren Sie diese.

Sehen Sie davon ab, NAS-Dienste direkt aus dem Internet erreichbar zu machen. Wenn Sie Ihr NAS aus der Ferne erreichen können, dann können das auch Hacker. Falls Sie von unterwegs auf Ihre Dateien zugreifen möchten, dann nutzen Sie besser einen VPN-Tunnel ins Heimnetz. Als VPN-Server können Sie zum Beispiel viele Router (Fritzbox, Speedport & Co.) oder einen Raspberry Pi einsetzen. Wenn möglich, sollten Sie das flinke und stabile WireGuard-Protokoll (siehe ct.de/ygt7) nutzen.

UPnP abdrehen

Deaktivieren Sie im NAS die UPnP-Funktion zur Konfiguration des Routers, sofern vorhanden. Mit der Funktion könnte der Netzwerkspeicher selbstständig Port-Weiterleitungen im Router einrichten, was schwerwiegende Folgen haben kann (siehe Fall oben). Bei Synologys DSM steckt UPnP in der Systemsteuerung unter „Externen Zugriff/Routerkonfiguration". Falls aktiv, schalten Sie diese Komfortfunktion aus.

Deaktivieren Sie UPnP auch im Router, damit auch keine anderen Geräte im lokalen Netz ohne Ihr Zutun Port-Weiterleitungen anlegen (siehe „Router konfigurieren"). Um sicherzustellen, dass Ihr NAS tatsächlich nicht aus dem Internet ansprechbar ist, können Sie den Netzwerkcheck von heise Security nutzen (siehe ct.de/ygt7). Dieser kostenlose Dienst überprüft, welche Ports bei Ihrem Anschluss über das Internet erreichbar sind. Im Idealfall sind es keine. Wenn es welche gibt, sollten Sie im Netz recherchieren, was es damit auf sich hat, damit Sie geeignete Maßnahmen treffen können (etwa, indem Sie die Weiterleitung der Ports im Router abschalten). Häufig ist der Port 5060 von außen erreichbar, dafür gibt es jedoch oft einen guten Grund: Router wie die Fritzbox öffnen ihn für eingehende VoIP-Telefonate. Lassen Sie ihn also in Ruhe. Der SMB-Port 445 für Windows-Dateifreigaben hingegen hat im Internet nichts verloren.



Weniger ist mehr: Schalten Sie alle nicht benötigten NAS-Dienste ab, um die Angriffsfläche zu reduzieren.

Sichere Passwörter

Sie haben es sicher schon oft gehört, dennoch muss es erwähnt werden: Nutzen Sie sichere Passwörter. Sicher bedeutet: individuell und möglichst lang. Ein sicheres Passwort funktioniert nur bei einem Dienst, wählen Sie also für jeden Zweck ein anderes. Geht es um lokale Verschlüsselung, zum Beispiel um die Festplatten Ihres NAS zu verschlüsseln, dann können Sie durch den Einsatz möglichst langer Kennwörter dafür sorgen, dass sich Angreifer möglichst lange die Zähne daran ausbeißen. Durch den Hersteller voreingestellte Kennwörter sollten Sie stets ändern.

Für weiteren Schutz sorgt die sogenannte Zwei-Faktor-Authentifizierung (2FA), die Sie bei einigen Diensten aktivieren können. Dann ist zum Einloggen nicht nur das Passwort nötig, sondern auch ein zweiter Faktor, etwa in Form eines USB-Sicherheitsschlüssels oder eines einmalig gültigen Codes, den eine Authenticator-App generiert. 2FA schützt effektiv vor Angriffen, weil ein Hacker, der das Passwort erbeutet hat, in aller Regel keinen Zugriff auf den zweiten Faktor hat. Bei Synology-NAS schalten Sie 2FA über die Systemsteuerung und „Benutzer/Erweitert/2-Stufen Verifizierung“ für Admins oder alle Nutzer scharf.

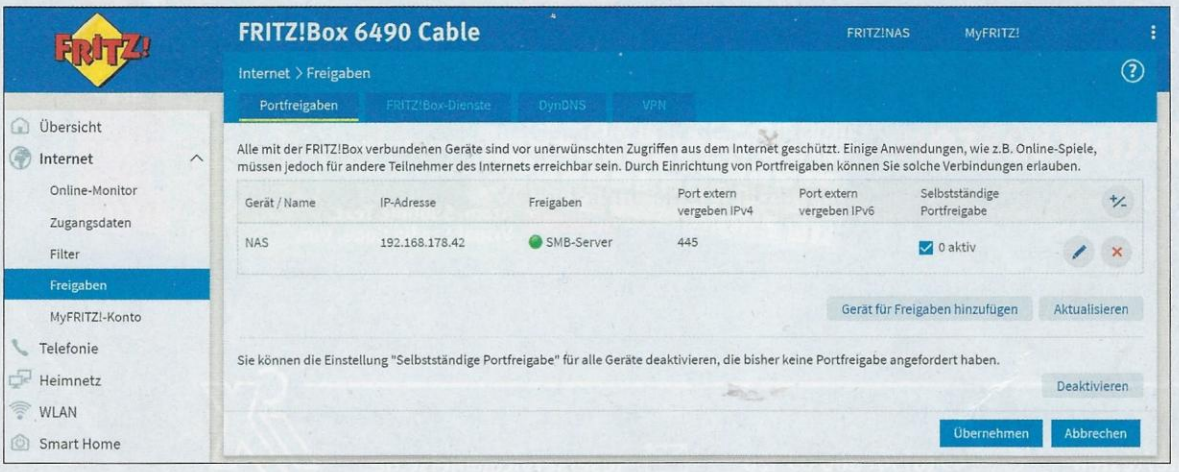
Wenn es eine Nutzerverwaltung mit unterschiedlichen Zugriffsrechten gibt, machen Sie davon Gebrauch. Jeder Nutzer sollte so wenig Rechte wie möglich haben: Sinnvoll sind etwa ein Admin-Account zur Konfiguration des Geräts und weitere Konten ohne Admin-Rechte, die jeweils nur auf genau die Daten und Funktionen zugreifen dürfen, die sie etwas angehen.

Seien Sie Ihr eigener Gast und versetzen Sie sich in die Lage eines Besuchers, der zum Beispiel über das WLAN auf das Internet zugreifen darf. Probieren Sie, als Gast auf das NAS zuzugreifen, um herauszufinden, welche Bereiche für jeden einsehbar sind. Unter Umständen möchten Sie zwar gewisse Bereiche für Gäste öffnen, aber etwa Ihre Urlaubsfotos und Dokumente privat halten.

Router konfigurieren

Sie müssen sich nicht nur um Ihr NAS kümmern, sondern auch um Ihren Router. Er ist die einzige Barriere zwischen Angreifern aus dem Internet und Ihrem Netzwerkspeicher. Die meisten der Empfehlungen aus diesem Artikel lassen sich auch auf den Router übertragen: Nutzen Sie sichere, individuelle Passwörter. Das WLAN-Passwort (WPA-Passphrase) darf nicht zugleich die Konfigurationsoberfläche (Webinterface) entsperren und so weiter. Voreingestellte Standardpasswörter sollten Sie auch beim Router ändern. Als WLAN-Verschlüsselung sollte mindestens WPA2 eingestellt sein, besser ist das aktuelle WPA3-Verfahren [1], das jedoch noch nicht von allen Geräten unterstützt wird. Bei der Fritzbox sorgt die Einstellung „WPA2 + WPA3“ dafür, dass beide Verschlüsselungsverfahren parallel aktiv sind.

Auch die Sicherheit Ihres Routers steht und fällt mit der Aktualität der Firmware. Prüfen Sie wie beim NAS also regelmäßig, ob die aktuelle Firmware installiert ist, und aktivieren Sie Mechanismen, die neue Updates automatisch einstellen oder zumindest eine Benachrichtigung auslösen, wenn es etwas Neues gibt. Bei den verbreiteten Fritzboxen aktivieren Sie die automatischen Updates wie folgt: Öffnen Sie das Webinterface des Routers im Browser (http://fritz.box) und klicken Sie nach dem Einloggen auf „System/Update/Auto-Update“. Wählen Sie die Option „Stufe III: Über neue FRITZ!OS-Versionen informieren und neue Versionen automatisch ins-



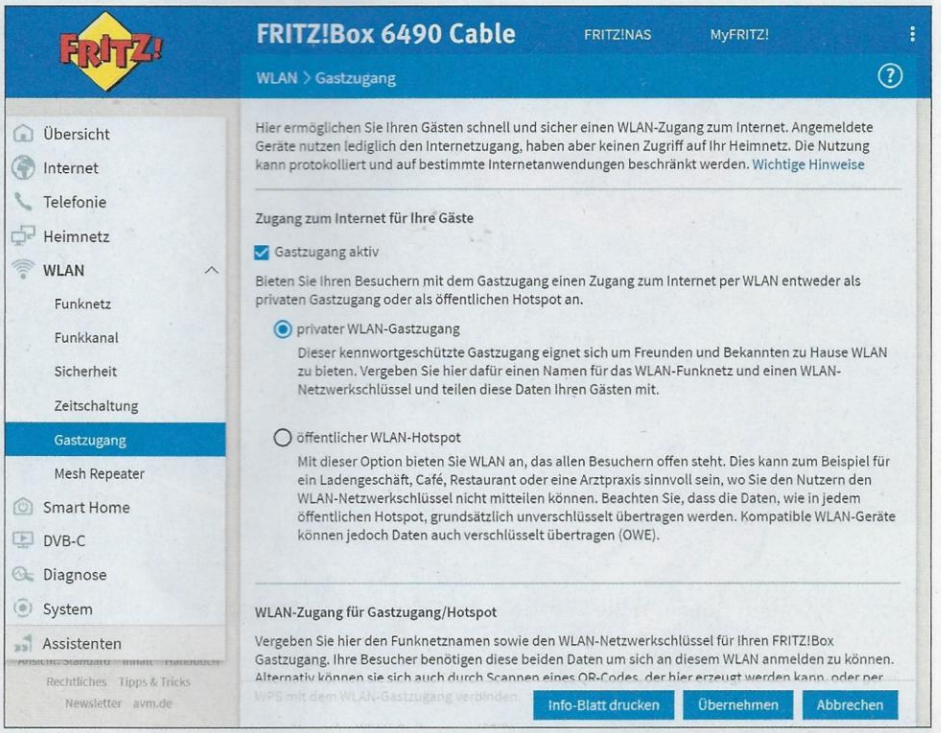
Räumen Sie bei den Portfreigaben gründlich auf. Insbesondere der hier gezeigte SMB-Port 445 sollte unter keinen Umständen in der Liste auftauchen.

tallieren (Empfohlen)“. Unter „Zeitraum für Updates“ können Sie eine Tageszeit für die automatische Update-Installation vorgeben. Vergessen Sie nicht, die Änderungen mit einem Klick auf „Übernehmen“ zu speichern.

Öffnen Sie abschließend die Unterseite „FRITZ!OS-Version“ und klicken Sie dort auf „Neues FRITZ!OS suchen“, um verfügbare Updates sofort zu finden und zu installieren. Falls Sie Ihre Fritzbox vom Provider gemietet haben, dann kann es sein, dass sich dieser um die Aktualität der Firmware kümmert und Sie die Installation nicht beeinflussen können. Dies ist auch bei Mietroutern anderer Hersteller häufig der Fall.

Kontrollieren Sie im Webinterface des Routers, welche Port-Weiterleitungen eingerichtet sind, und entfernen Sie alle nicht verwendeten. Bei der Fritzbox finden Sie die Weiterleitungen unter „Internet/Freigaben“. Deaktivieren Sie zudem die Konfigurierbarkeit des Routers über UPnP. Bei der Fritzbox klicken Sie hierzu auf den Button „Deaktivieren“, der sich unter dem Text „Sie können die Einstellung *Selbstständige Portfreigabe* für alle Geräte deaktivieren, die bisher keine Portfreigabe angefordert haben“ befindet. Suchen Sie unter „Heimnetz/Netzwerk“ zudem nach Geräten, bei denen unter Eigenschaften „selbst. Portfreigabe erlaubt“ angezeigt wird. Klicken Sie dort auf den Stift, um den Eintrag zu ändern, und deaktivieren Sie „Selbstständige Portfreigaben für dieses Gerät erlauben“.

Spannen Sie, wenn möglich, ein Gastnetz für Ihre Besucher auf, das keine Zugriffe auf das Heimnetz erlaubt (bei der Fritzbox unter „WLAN/Gastzugang“). So verhindern Sie, dass sich Ihre Gäste auf dem NAS umsehen. In dieses Netz können Sie auch Geräte sperren, denen Sie nicht vertrauen – zum Beispiel neue Smart-Home-Geräte, die Sie erstmal ausprobieren und beobachten möchten. Falls Sie Gästen das WLAN-Passwort fürs interne Netz ausgehändigt haben, ändern Sie es nach einer Weile, um unerwünschte Zugriffe aufs Heimnetz zu unterbinden.



Gäste gehören ins Gastnetz. Dort können sie aufs Internet zugreifen, nicht aber auf Ihre Urlaubsfotosammlung, die auf dem NAS lagert.

NAS ≠ Backup

Ein NAS ist ohne Frage als Backup-Speicher prädestiniert, allerdings sollten Sie sich nicht allein darauf verlassen. Wie der Fall unseres Lesers zeigt, ist auch das NAS nicht vor Datenverlust gefeit. Für den Daten-GAU müssen nicht mal Hacker im Spiel sein, auch NAS-Festplatten und -SSDs werden unweigerlich irgendwann durch einen Hardwaredefekt ausfallen. Sie sollten daher auch den NAS-Inhalt per Backup sichern und dieses regelmäßig aktualisieren – zumindest dann, wenn die Daten unersetzlich sind. Worauf Sie dieses Backup speichern, ist fast egal. Der Datenträger sollte allerdings möglichst langlebig [2] und nicht dauerhaft mit Computer oder NAS verbunden sein.

Viele Krypto-Trojaner nehmen nämlich nicht nur die Dateien des infizierten Systems in Geiselhaft, sondern befallen auch externe Datenträger und Netzwerkfreigaben. Geeignet ist zum Beispiel eine externe USB-Platte, die nur während des Backups mit dem System verbunden ist. Auch ein verschlüsseltes Backup in die Cloud [3] kann sinnvoll sein: Bei vielen Cloud-Speichern können Sie frühere Versionen Ihrer Dateien wiederherstellen, etwa nachdem ein Krypto-Trojaner zugeschlagen hat. Bewährt hat sich die 3-2-1-Regel: Bewahren Sie drei Kopien Ihrer Daten (das Original zählt mit) auf zwei unterschiedlichen Datenträgertypen auf, eine davon außer Haus. Dann sind Sie selbst dann noch auf der sicheren Seite, wenn das Haus abbrennt – zumindest, was Ihre Daten betrifft.

Security-Checkup

Machen Sie regelmäßig ein Security-Check-up, um sicherzustellen, dass Ihr NAS weiterhin geschützt ist. Manchmal sorgen Konfigurationsänderungen dafür, dass ein Sicherheitsleck entsteht. Oder man probiert eine neue Funktion aus, ohne sich über die Konsequenzen bewusst zu sein. Auch Firmware-Updates können unerwartete Änderungen an der Konfiguration oder neue Funktionen mitbringen, welche die Sicherheit gefährden. Daher ist es nicht damit getan, NAS und Router genau ein Mal sicher einzurichten.

Hilfreich beim Absichern von NAS, Router, Smartphone & Co. sind auch unsere Security-Checklisten, die wir in c’t 20/2020 veröffentlicht haben. Damit können Sie schnell die wichtigsten Punkte durchgehen, um Ihren digitalen Fuhrpark vor den häufigsten Cyber-Angriffen zu schützen. Unter **ct.de/check2021** können Sie kostenlos eine Kurzfassung als PDF-Booklet herunterladen.

(rei@ct.de) c't

Literatur

[1] Dr. Alfred Arnold und Ernst Ahlers, Extrasicher funken, WPA3 schützt das WLAN, nicht nur an Fritzboxen, c’t 22/2020, S. 26
[2] Lutz Labs, Stabile Magnetpartikelchen, Langzeitarchivierung mit Festplatten, c’t 22/2020, S. 64
[3] Holger Bleich, Auf Eis gelegt, Daten langfristig in der Cloud sichern, c’t 22/2020, S. 72

Netzwerkcheck & weitere Infos:
ct.de/ygt7