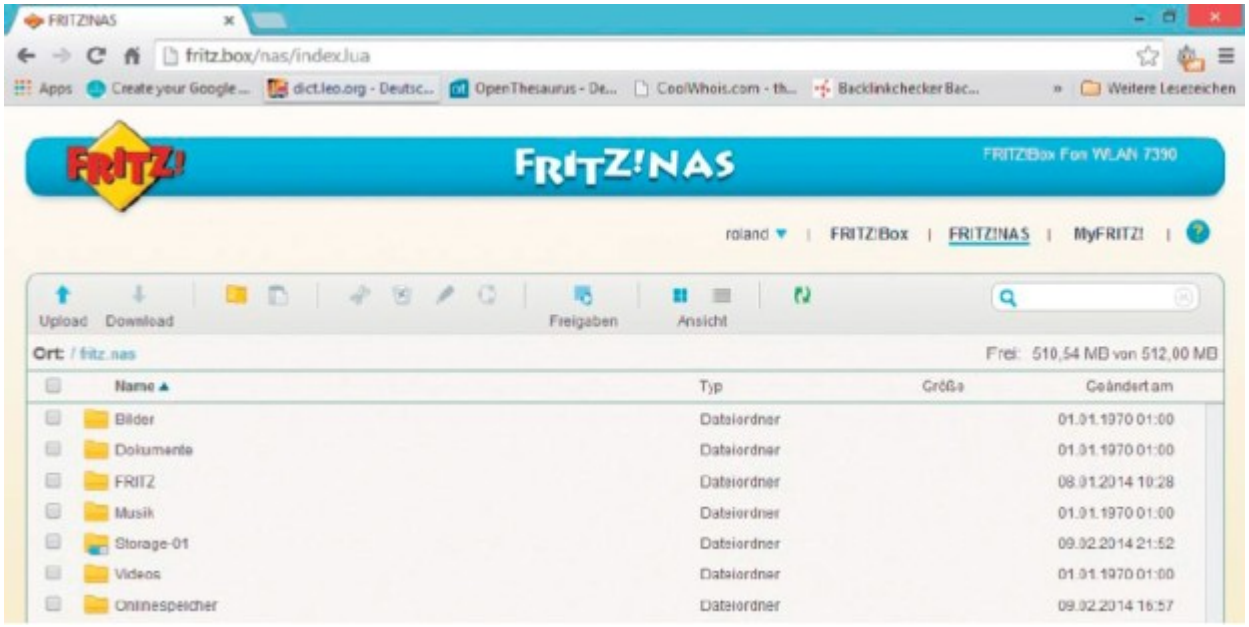
# Die Fritzbox als NAS: So klappt die Einrichtung

**Die Fritzbox bietet ab Werk schon einen eingebauten Netzwerkspeicher von 500 MB. Wer will, kann diesen noch erweitern.**

**Wer nicht in einen eigenen NAS-Server investieren möchte, kann stattdessen mit der Fritzbox USB-Sticks und externe Festplatten schnell und problemlos im Netzwerk einbinden.**

Das Kürzel NAS steht für Network Attached Storage, also einen an das Netzwerk angeschlossenen Speicher. Die Fritzbox ist von Haus aus ein NAS-Server, denn sie bringt einen internen Speicher mit, der ab der Version 7390 mit 512 MB bereits recht ordentlich ausfällt. Zudem bietet sie die Möglichkeit, diesen Speicher mit externen USB-Sticks oder -Festplatten zu erweitern. Und schließlich kann sie auch auf den Online-Speicher von diversen Anbietern zugreifen. Der gesamte Speicherplatz, ganz gleich, ob intern, extern oder online, lässt sich über eine einzige Bedienoberfläche verwalten. Als Erstes sollten Sie sich den internen Speicher der Fritzbox ansehen. Die Box hält dafür eine eigene, Explorer-ähnliche Ansicht bereit. Sie erreichen sie nach Aufruf der Bedienoberfläche mit einem Klick auf „FRITZ!NAS“ am oberen rechten Rand. Andere Möglichkeit: Sie tippen „fritz.nas“ in den Browser ein, um direkt dorthin zu springen. Am elegantesten ist aber sicherlich die Einbindung in Windows: Öffnen Sie den Explorer und klicken Sie auf „Netzlaufwerk verbinden“. Wählen Sie danach einen Laufwerksbuchstaben aus, klicken Sie neben „Ordner“ auf „Durchsuchen“ und wählen Sie in der nun folgenden Übersicht auf dem Gerät „FRITZ-NAS“ den Ordner „fritz.nas“ aus. Nach der Bestätigung mit „OK“ bindet der Explorer den Speicher der Fritzbox in seine Übersicht ein. So prüft Windows bei jedem Start, ob das Laufwerk zur Verfügung steht.

**Tipp:** Damit der direkte Zugriff von einem PC auf den freigegebenen Speicher der Fritzbox reibungslos funktioniert, ist es wie immer bei Windows erforderlich, dass auf beiden Geräten der gleiche Benutzer mit identischem User-Namen und Passwort eingerichtet ist. In der Bedienoberfläche der Box erledigen Sie das unter „System“ und „FRITZ!Box-Benutzer“. Aktivieren Sie jetzt die Option „Anmeldung mit FRITZ!Box-Benutzernamen und Kennwort“ auf der Registerkarte „Anmeldung im Heimnetz“. Wenn Sie den Fritzbox-Speicher mit Inhalten wie MP3-Musik oder Fotos bestücken, sind diese Dateien von jedem Rechner in Ihrem Netzwerk aus erreichbar. Sie können den freien Platz aber auch für den schnellen und einfachen Datenaustausch verwenden.




**Die Fritzbox hält für die Anzeige ihrer internen Speicherinhalte einen eigenen Dateimanager bereit. Er bindet aber auch externe Medien wie USB-Sticks und -Festplatten in seine Ordnerstruktur ein.**

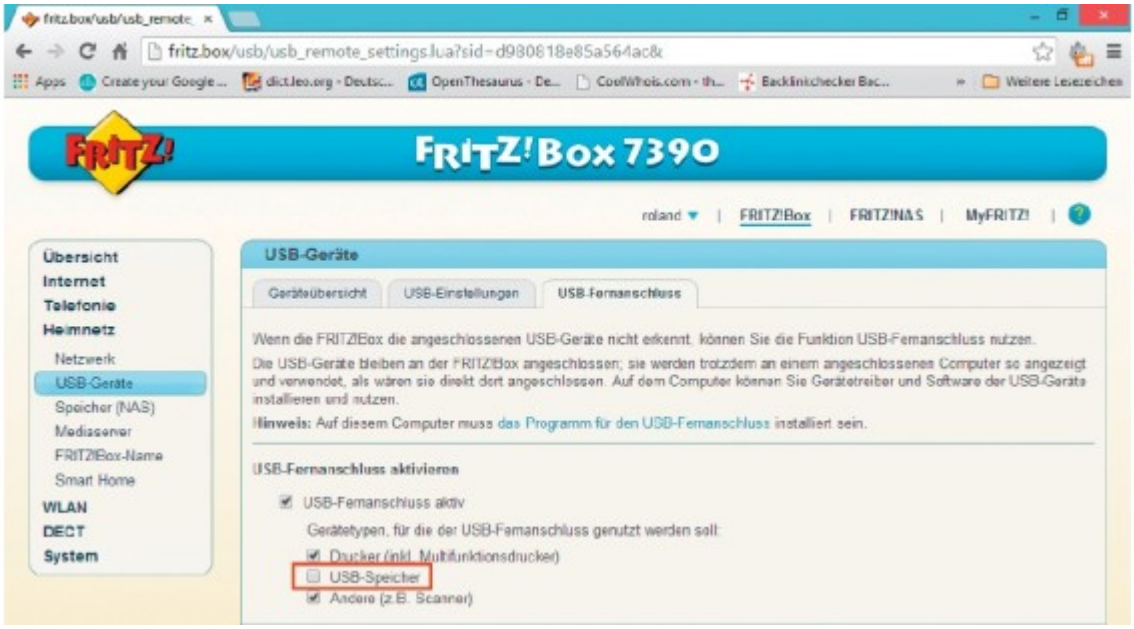
## USB-Speicher anschließen

512 MB sind zwar ausreichend für Hunderte von Office-Dokumenten, oft benötigt man jedoch mehr Platz. Kein Problem: Die Fritzbox 7390 bietet zwei USB-Ports, über die Sie den Speicher erweitern können. Sie akzeptieren USB-Speicher mit Kapazitäten bis zu zwei Terabyte, die mit den Dateisystemen NTFS, FAT/ FAT32 oder EXT2 formatiert sind. Bevor Sie allerdings den USB-Stick oder die Festplatte anschließen, müssen Sie zunächst den USB-Fernanschluss konfigurieren. Diese Funktion der Fritzbox dient zum Anschluss von USB-Druckern oder Multifunktionsgeräten, die damit dem gesamten Netzwerk zur Verfügung gestellt werden. Wenn Sie den Fernanschluss bislang noch nicht benutzt haben, brauchen Sie nichts weiter zu unternehmen. Falls doch, vergewissern Sie sich zunächst, dass für die Fritzbox-Bedienoberfläche die erweiterte Ansicht eingeschaltet ist. Gehen Sie daraufhin auf „Heimnetz“ und „USB-Geräte“ und wechseln Sie zum Register „USB-Fernanschluss“. Sehen Sie nach, ob der Fernanschluss aktiviert ist, und entfernen Sie gegebenenfalls das Häkchen vor „USB-Speicher“. Bestätigen Sie mit „Übernehmen“.

Dann können Sie den USB-Stick oder die Festplatte an die Fritzbox anschließen. Es empfiehlt sich, die Dateien, die Sie ihm oder ihr anvertrauen wollen, zuvor an der USB-Buchse Ihres PCs auf den Speicher zu überspielen. Das ist deutlich schneller, als wenn Sie die Files später über das Netzwerk an den USB-Anschluss der Fritzbox schicken. Nachdem Sie den Stick oder die Platte angeschlossen haben, werden die Daten von der Fritzbox automatisch indexiert, das kann bei großen Medien einige Zeit dauern. Anschließend taucht der Speicher in der Übersicht von „FRITZ.NAS“ und auch im Windows- Explorer auf.

**Tipp:** Falls Sie den USB-Speicher über den Explorer mit Dateien bestücken, werden sie eventuell nicht indexiert. Sie müssen die Aktualisierung des Index manuell anstoßen. Gehen Sie dazu in der Fritzbox-Oberfläche auf „Heimnetz > Speicher (NAS)“ und klicken Sie neben dem Eintrag des USB-Geräts auf „ist erstellt“.

**Hinweis:** Ein wichtiger Nachteil der Fritzbox gegenüber einem echten NAS sei hier nicht verschwiegen. Aufgrund der schwachbrüstigen CPU der Fritzbox kommt sie lediglich auf Übertragungsraten von etwa 5 MB/s. Selbst NAS-Geräte für Einsteiger erreichen bei Lesezugriffen Datenraten von 100 MB/s und mehr.




**Bevor Sie das USB-Medium anschließen, ist es wichtig, dass Sie den USB-Fernanschluss für den Speicher deaktivieren. Ansonsten werden die Speichersticks und Festplatten nicht erkannt.**

## Online-Speicher einbinden

Manche Provider bieten ihren Kunden einige Gigabyte kostenlosen Online-Speicher an. Am besten binden Sie diesen zusätzlichen Speicherplatz über die Fritzbox in Ihr Netzwerk ein. So haben Sie von allen Computern aus Zugriff darauf. Es gibt dabei allerdings eine Einschränkung: Sie können nämlich nur dann einen Online-Speicherdienst einrichten, wenn Sie bereits ein USB-Medium konfiguriert haben, am besten eine Festplatte. Die

Fritzbox benötigt sie als Zwischenspeicher beim Upload und Download von Dateien.

Rufen Sie dazu „Heimnetz“ und „Speicher (NAS)“ auf. Im Abschnitt „Online-Speicher Einstellungen“ finden Sie eine Auswahlliste mit mehreren Anbietern. Im Rahmen der automatischen Konfiguration der Fritzbox tragen einige Provider die Zugangsdaten gleich für Sie ein. Ansonsten wählen Sie bei „WebDAV-Anbieter“ einen Hosting-Anbieter und geben darunter die E-Mail-Adresse oder Ihren Benutzernamen und das Kennwort ein. Leider ist es aber nicht möglich, hier Dienste wie Dropbox oder Skydrive einzubinden. Schuld daran ist das Web- DAV-Protokoll, das die Fritzbox nutzt. Web-DAV steht für Web-based Distributed Authoring and Versioning und ist eine Erweiterung des HTTP-Standards für Online-Festplatten. Es wird allerdings von Dropbox und anderen Diensten dieser Art nicht unterstützt. Nur über kostenpflichtige Dienste wie Otixo lässt sich der Speicher doch einbinden. Otixo fasst mehrere Cloud-Speicher zusammen und erlaubt den Web-DAV-Zugriff darauf.

### Mediaserver aktivieren

Die Fritzbox und die an ihr angeschlossenen Speichermedien lassen sich auch als Mediaserver verwenden. Das bedeutet, dass Sie dort Ihre Audio- und Video-Files ablegen, die dann im Netzwerk von geeigneten Mediaplayern als Stream abgespielt werden können. Auf diese Weise organisieren Sie eine Art private Radio und Fernsehstation, die an jedem Computer in Ihrem Netz empfangen werden kann.

Zunächst schalten Sie den Mediaserver ein. Klicken Sie dazu unter „Heimnetz“ auf „Mediaserver“ und machen Sie ein Häkchen bei „Mediaserver aktiv“. Markieren Sie darunter die Medienquellen, die der Server verwenden soll, und drücken Sie auf „Übernehmen“. Auch das Streaming von Internetradios und Podcasts lässt sich hier einrichten. Um auf die Medien zuzugreifen, eignen sich der VLC Media Player und der Windows Media Player. Letzterer erkennt den Mediaserver der Fritzbox automatisch und zeigt ihn in seiner Übersicht an.

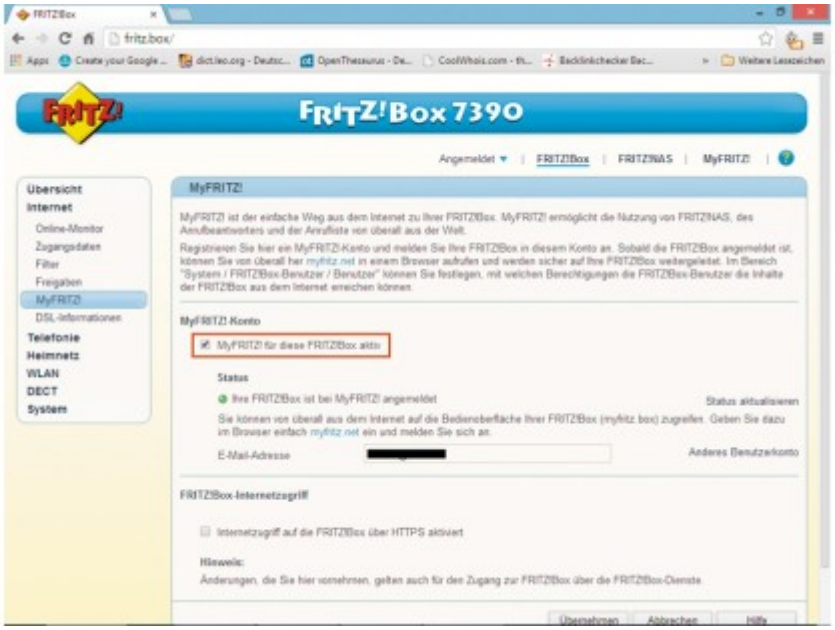
# Via Fernzugriff auf die Fritzbox zugreifen

**Ein Fernzugriff auf das Heimnetzwerk ermöglicht die Überwachung und den Zugriff auf alle angeschlossenen Geräte.**

**Die Fritzbox ist nicht nur aus dem eigenen Netzwerk, sondern auch aus dem Internet erreichbar. Damit können Sie etwa eingegangene Anrufe überprüfen oder die Box gar als Vermittlungsstelle nutzen.**

Fritzbox bringt eine umfangreiche Ausstattung für den Fernzugriff mit. Bereits mit wenigen Klicks lässt sie sich so einstellen, dass Sie die Menüs und den internen Speicher von unterwegs über das Internet erreichen können. Aber das ist noch nicht alles: Die Box ist zudem in der Lage, die Gespräche Ihres Smartphones weiterzuvermitteln. Es ist also möglich, dass Sie sich mit Ihrer Daten-Flatrate gratis bei Ihrer heimischen Fritzbox anmelden und über Ihre Telefonanlage zum oft günstigeren Festnetztarif telefonieren.

Sind Sie mit einem Notebook unterwegs und haben den Verdacht, dass ein öffentliches WLAN Ihre persönlichen Daten nicht genug schützt, können Sie eine sichere, verschlüsselte Verbindung aufbauen und über die Fritzbox und Ihren eigenen Provider im Internet surfen oder Mails abholen. Das funktioniert, da AVM den Geräten einen vollwertigen VPN-Server spendiert hat.

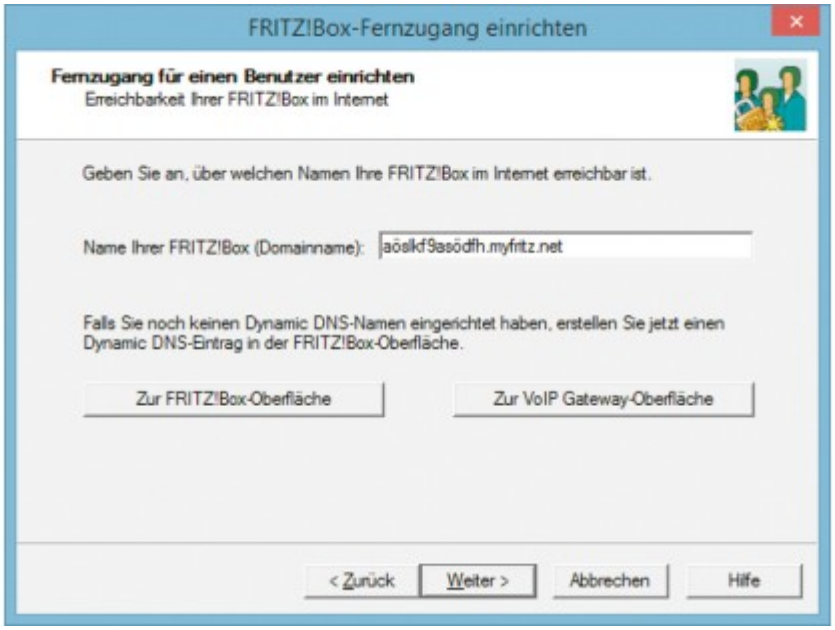



**Mit einem Klick auf das Kontrollkästchen bei „Myfritz! für diese FRITZ!Box aktiv“ starten Sie den Assistenten für die Einrichtung und können dann Schritt für Schritt Ihre Daten eingeben.**

**Erste Vorbereitungen**

Für den Fernzugriff auf die Fritzbox sind einige Vorbereitungen erforderlich. Zunächst müssen Sie dafür sorgen, dass die Box unter einer festen Adresse erreichbar ist. Internetprovider weisen ihren Kunden bei der Einwahl – etwa nach einer Zwangstrennung – immer wieder neue IP-Adressen zu. Umgehen lässt sich das mit dynamischen DNS-Diensten, wie beispielsweise Free DNS , die in einer Datenbank die aktuellen IP-Adressen vermerken und an die DNS-Server weitergeben. Unter dem Namen „Myfritz“ bietet auch AVM einen solchen Service an. Er ist kostenlos und nur für Fritzbox-Besitzer nutzbar.

Sie finden „Myfritz“ im Menü der Box unter „Internet“. Setzen Sie ein Häkchen neben „Myfritz! für diese FRITZ!Box aktiv“ und klicken Sie auf „Übernehmen“. Im folgenden Fenster geben Sie Ihre E-Mail-Adresse an, definieren ein Passwort und klicken auf „Weiter“. Sie werden nun auf die Website von Myfritz geführt, wo Sie per E-Mail-Adresse und Kennwort einen Account einrichten. Kurz darauf bekommen Sie eine Mail mit einem Link zur Bestätigung. Mit einem Klick schließen Sie die Einrichtung ab und werden nun übers Internet zum Menü Ihrer Fritzbox geführt. Später lassen sich durch Eingabe von „Myfritz.net“ in Ihren Browser die Menüs Ihrer Box von überall her erreichen.

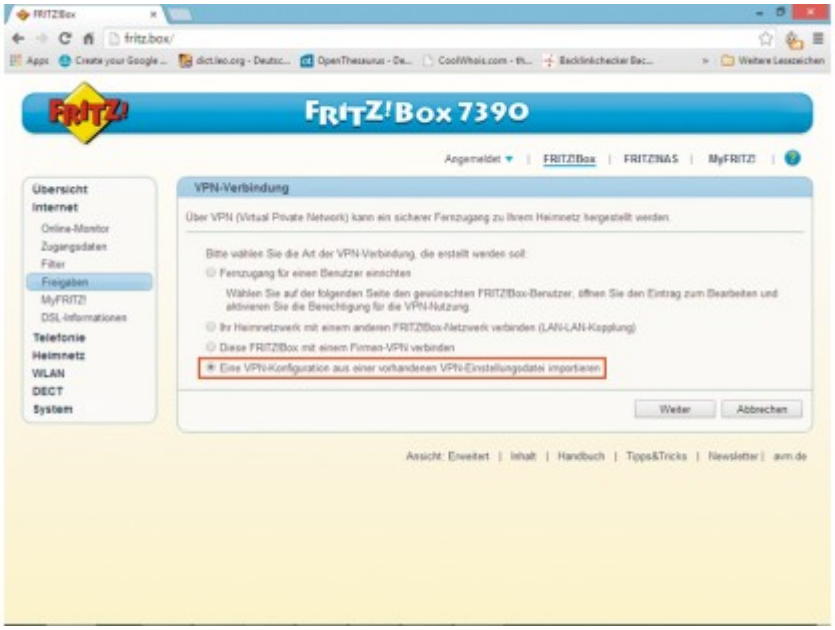



**Mit dem kostenlosen Tool zum Einrichten des Fernzugangs treffen Sie auf dem Notebook die nötigen Einstellungen für den VPN-Zugriff.**

**Einen PC-Client konfigurieren**

Sie können jetzt bereits auf Ihre Fritzbox zugreifen, aber noch nicht über sie ins Internet gehen. Dazu installieren Sie auf dem PC, den Sie unterwegs nutzen, in einem ersten Schritt das Programm Fritzbox-Fernzugang einrichten. Laden Sie die EXE-Datei herunter, klicken Sie zwei Mal auf „Weiter“ und schließlich auf „Fertig stellen“. Danach starten Sie das Tool und klicken auf „Neu“ und „Fernzugang für einen Benutzer einrichten“. Nach einem „Weiter“ markieren Sie nun „PC mit FRITZ!Fernzugang“, klicken erneut „Weiter“ und geben Ihre E-Mail-Adresse ein. „Weiter“ klicken. Jetzt will das Programm den Domainnamen Ihrer Fritzbox wissen. Sie finden diesen im Menü der Fritzbox unter „Internet“ und „Freigaben“. Öffnen Sie dort das Register „FRITZ!Box-Dienste“, notieren Sie sich den Inhalt des Feldes „Adresse Ihrer Fritzbox“ oder kopieren Sie ihn einfach über die Zwischenablage. Damit der Name hier erscheint, muss „Internetzugriff auf die FRITZ!Box über HTTPS aktiviert“ eingeschaltet sein, was nach Aktivieren von Myfritz automatisch erfolgt.

Alles, was hinter „https://“ steht, ist der Domainname, normalerweise eine wirre Zeichenkombination, gefolgt von „.Myfritz.net“. Geben Sie ihn in das Fernzugangs-Tool ein und klicken Sie anschließend auf „Weiter“. Belassen Sie es im folgenden Fenster bei den voreingestellten Werkseinstellungen, markieren Sie jedoch „Alle Daten über den VPN-Tunnel senden“. Klicken Sie danach auf „Weiter“, markieren Sie „Das Verzeichnis anzeigen, das die Konfigurationsdateien enthält“ und bestätigen Sie mit „Fertig stellen“.




**Die mit dem Fernzugangs-Tool von AVM erzeugten Konfigurationsdaten für den Fernzugriff per VPN über das Internet importieren Sie schließlich über die Bedienoberfläche in die Fritzbox.**

Die Software öffnet nun den Windows-Explorer und führt Sie in einen Unterordner des Verzeichnisses, in dem das Fernzugangs-Tool liegt. Dort finden Sie eine Konfigurationsdatei mit einem Namen in der Form vpnuser_[E-Mail-Adresse].cfg. Gehen Sie eine Ordnerebene höher, dort ist eine zweite Konfigurationsdatei mit der Bezeichnung fritzbox_[Zeichenkombination]_Myfritz_net.cfg gespeichert. Kopieren Sie beide Dateien am besten in einen einfach erreichbaren Standardordner, denn Sie brauchen die Dateien noch. Wechseln Sie jetzt wieder zum Menü der Fritzbox und rufen Sie dort unter „Internet“ und „Freigaben“ das Register „VPN“ auf.

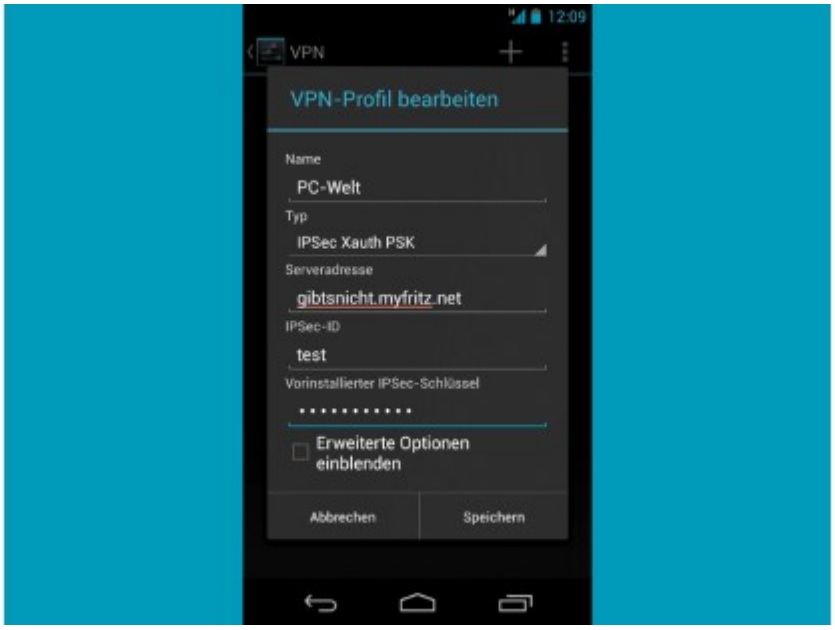
**Achtung:** Das Menü ist nur in der erweiterten Ansicht verfügbar. Klicken Sie auf „VPN-Verbindung hinzufügen“ und im nächsten Fenster auf „Eine VPN-Konfiguration aus einer vorhandenen VPN-Einstellungsdatei importieren“. Nach einem Klick auf „Weiter“ drücken Sie den Button „Datei auswählen“, steuern die eben generierte Datei fritzbox_[Zeichenkombination]_Myfritz_net.cfg an und klicken „OK“. Nachdem Sie die Sicherheitsabfrage mit „OK“ beantwortet haben, importiert die Fritzbox die Einstellungen des Myfritz-Zugangs.

**Es empfiehlt sich, im Client für den Fernzugang ein Kennwort zu definieren, um den Zugang zu schützen.**

**VPN-Client einrichten**

Nun benötigen Sie noch einen Client, also eine Software, mit der Sie die VPN-Verbindung zu Ihrem Netzwerk daheim von Ihrem Notebook aus aufbauen. AVM bietet sie unter dem Namen Fritzfernzugang gratis zum Download an. Zum Installieren rufen Sie die EXE-Datei des Tools auf, klicken zwei Mal auf „Weiter“ und nach Abschluss der Installation auf „Fertig stellen“. Daraufhin müssen Sie Ihren PC neu booten. Danach starten Sie das Programm. Beim ersten Mal verlangt das Tool nach der eben erzeugten Datei vpnuser_[E-Mail-Adresse].cfg. Zeigen Sie dem Tool über das gewohnte Dateifenster den Pfad zur Datei und klicken Sie auf „Öffnen“. Fritzfernzugang importiert die Einstellungen und zeigt die Verbindung in seinem Fenster als Icon an. Markieren Sie diese und klicken Sie auf „Aufbau“, um den VPN-Tunnel zu starten.

Von nun an läuft der gesamte Internet-Traffic Ihres Notebooks über die verschlüsselte Verbindung zu Ihrer Fritzbox. Die Geschwindigkeit ist dabei allerdings deutlich niedriger, als wenn Sie von daheim aus ins Internet gehen. Zwar kann die Fritzbox Websites in der gewohnten Geschwindigkeit laden, doch das Senden der Site an Ihr Notebook geht nur mit der Upload-Datenrate Ihres Internetzugangs. Diese liegt meist bei nur 1 bis 2 MBit pro Sekunde.




**Android bietet eine VPN-Funktion mit vorgefertigter Maske für die Eingabe der Zugangsdaten an.**

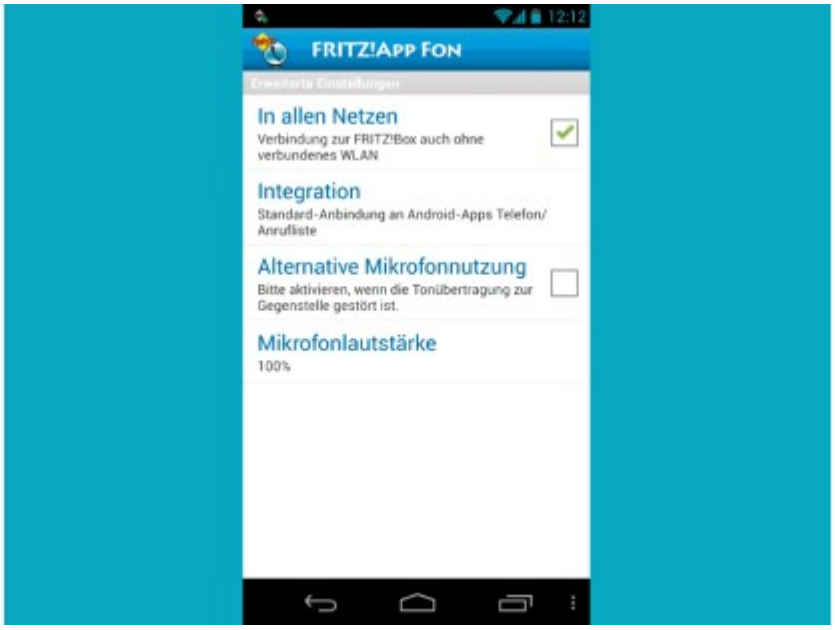
**Android-Clients konfigurieren**

Sie können auch mithilfe eines Android-Smartphones oder -Tablets auf den VPN-Server der Fritzbox zugreifen und über ihn eine sichere Internetverbindung aufbauen. Dazu müssen Sie noch nicht einmal eine weitere App installieren, das Mobilbetriebssystem bringt schon alles Notwendige mit. Sie sollten aber bereits alle benötigten Daten zur Hand haben. Diese bekommen Sie über das Menü der Box: Gehen Sie dort auf „System“ und „FRITZ!Box-Benutzer“ und klicken Sie beim Eintrag zu Ihrem Benutzernamen auf den Button „Bearbeiten“. Im folgenden Fenster finden Sie unten die Option „VPN“ und dort den Link „VPN-Einstellungen anzeigen“. Durch Anklicken öffnen Sie ein Fenster mit den benötigten Daten für VPN-Verbindungen mit Android-Geräten und iPhones. Wählen Sie noch „Diese Seite drucken“.

**Konfiguration des Android-Handys:** Rufen Sie die Einstellungen-App an Ihrem Smartphone auf, tippen Sie im Abschnitt „Drahtlos & Netzwerke“ auf „Mehr“ und anschließend auf „VPN“. Durch Antippen des Pluszeichens öffnen Sie das Formular zum Anlegen eines neuen VPN-Profils. Ganz oben tragen Sie unter „Name“ eine beliebige Bezeichnung ein. Zur Auswahl des Typs tippen Sie rechts unten in diesem Feld auf das kleine Dreieck, um das Auswahlmenü zu öffnen. Wählen Sie in der Liste „IPSec Xauth PSK“.
Die weiteren Einstellungen lesen Sie von dem Ausdruck ab. Übernehmen Sie die Server-Adresse, tragen Sie unter „IPSec-ID“ den „IPSec Identifier“ ein und bei „Vorinstallierter IPSec-Schlüssel“ den „IPSec Pre-Shared Key“. Tippen Sie zum Abschluss auf „Speichern“. Zum Aufbauen der Verbindung tippen Sie sie an und geben unter „Nutzername“ und „Passwort“ die Daten ein, die Sie für den Benutzer Ihrer Fritzbox definiert haben. Nach einem Klick auf „Verbinden“ wird das VPN gestartet, und Ihre Internetverbindung läuft über die Fritzbox.

**Tipp:** Es kommt vor, dass der Browser des Android-Geräts bei eingeschalteter VPN-Verbindung die eingegebenen Webadressen nicht findet und meldet, die Adresse sei nicht verfügbar. Wenn das regelmäßig passiert, bessern Sie bei der VPN-Verbindung noch einmal nach. Nachdem Sie den Eintrag der Verbindung ein paar Sekunden lang per Finger berührt haben, erscheint ein kleines Menü mit dem Befehl „Profil bearbeiten“. Kreuzen Sie „Erweiterte Optionen einblenden“ an und geben Sie einen DNS-Server an, zum Beispiel den Server von Google mit der Adresse 8.8.8.8. Speichern Sie die Einstellungen und bauen Sie die Verbindung daraufhin neu auf.

Risiko Router: So schützen Sie Ihr Netzwerk




**Aktivieren Sie in Fritz App Fon die Option „In allen Netzen“, um per VPN über die Fritzbox zu telefonieren.**

**Mobil telefonieren per VPN**

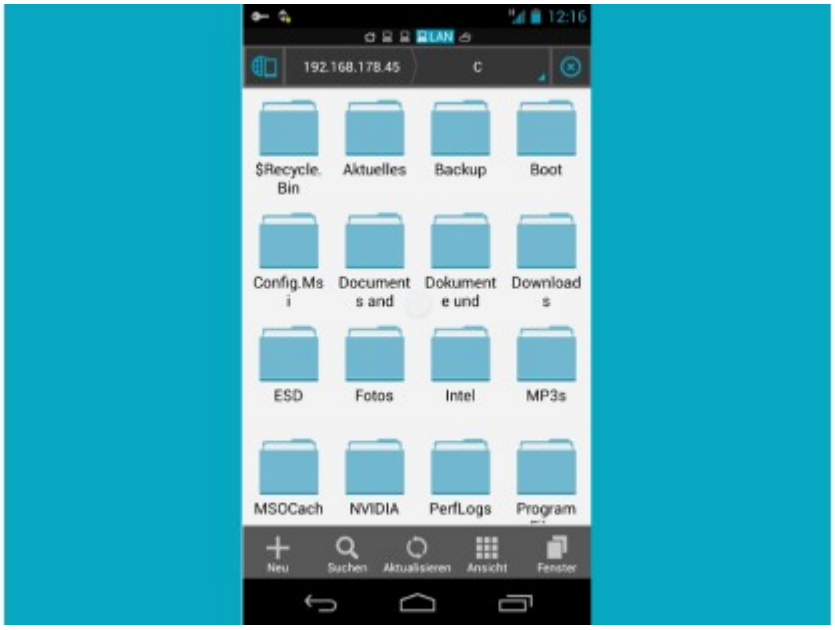
Sie können die VPN-Verbindung vom Smartphone zur Fritzbox nicht nur für einen sicheren Internetzugang nutzen, sondern darüber auch telefonieren. Hierzu benötigen Sie ein Android-Tool von AVM namens Fritz App Fon, das normalerweise dazu dient, Handygespräche über ein WLAN zu führen. Das Programm klinkt sich über

das Funknetzwerk in die Fritzbox ein und bietet eine Wähltastatur, sodass Sie die Möglichkeit haben, zu Hause mit dem Smartphone über das Festnetz zu telefonieren. Und wenn Anrufe eingehen, klingelt neben dem Festnetz- auch das Mobiltelefon.

Installieren Sie Fritz App Fon auf Ihrem Handy und rufen Sie es auf. Beim ersten Start will es von Ihnen das Kennwort für die Bedienoberfläche der Box wissen. Dann legt es ein neues Telefoniegerät an und weist ihm eine interne Kurzwahl zu. Die App wird automatisch gestartet, sobald das Smartphone mit dem WLAN der Fritzbox verbunden ist. Tippen Sie in dem Programm auf „Mehr“ und auf „Einstellungen“. Öffnen Sie rechts unten das Android-Menü, gehen Sie auf „Erweitert“ und markieren Sie die Option „In allen Netzen“. Bauen Sie jetzt über Ihr Smartphone eine VPN-Verbindung auf. Wenn Sie nun über die Software-Tastatur von Fritz App Fon Nummern wählen, werden die Gespräche automatisch per VPN zur Fritzbox und von dort ins Festnetz geleitet.

**Auf Windows-Freigaben zugreifen**

Sobald die VPN-Verbindung steht, ist das Notebook oder Android-Gerät quasi ein Client in Ihrem lokalen Netzwerk. Der DHCP-Server der Fritzbox weist ihm dazu eine passende IP-Adresse zu, in der Voreinstellung die 192.168.
178.201. Sie können nun in Ihrem LAN agieren, als wären Sie daheim. So ist es beispielsweise kein Problem, auf die Freigaben der eingeschalteten Rechner zuzugreifen. Öffnen Sie den Windows-Explorer und tippen Sie in seine Eingabezeile zwei Backslashs ein, gefolgt von der IP-Adresse des Rechners, den Sie ansteuern möchten. Das sieht dann zum Beispiel so aus: \\192.168.178.21.




**Mit dem ES Datei Explorer greifen Sie per VPN auf die Ordner Ihres Windows-Rechners daheim zu.**

**Tipp:** Falls Sie die Adresse nicht kennen, öffnen Sie auf dem Notebook einen Browser und geben Sie www.Myfritz.net ein. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Kennwort an und gehen Sie rechts oben im Menü auf „FRITZ!Box“. So erreichen Sie die Bedienoberfläche, wo Sie unter „Heimnetz“ die aktuell angemeldeten Geräte und deren IP-Adressen einsehen können. Das funktioniert auch mit Android-Geräten. Um auf Windows-Freigaben zuzugreifen, benötigen Sie allerdings einen Dateimanager, der das SMB-Protokoll von Microsoft beherrscht (SMB = Server Message Block), über das Datei- und Druckerfreigaben verwaltet werden. Ein Beispiel ist der „ES Datei Explorer“. Installieren und öffnen Sie das Programm und tippen Sie bei laufender VPN-Verbindung links oben auf das Feld mit der halben Weltkugel. Gehen Sie unter „Netzwerk“ auf „LAN“ und tippen Sie unten auf das Pluszeichen. Tragen Sie bei „Server“ die IP-Adresse des Computers ein, diesmal ohne die vorangestellten Backslashs. Geben Sie bei „Benutzername“ und „Kennwort“ Ihre Anmeldedaten bei Windows ein und tippen Sie auf „OK“. Die App legt nun für den Rechner ein Icon an. Tippen Sie es an, um Zugriff auf die Freigaben zu bekommen.

# Risiko Router: So schützen Sie Ihr Netzwerk

**Ein Router soll eigentlich Ihr Netzwerk absichern. Dumm nur, wenn diese Mauer Löcher hat. Wir zeigen, wie Sie sich mit einfachen Mitteln schützen können.**

Kaum ein Tag vergeht, an dem kein Router-Hersteller im Kreuzfeuer steht: AVM, Asus, D-Link – selbst die Branchengrößen mussten einräumen, dass ihre Router nicht sicher sind. Findige Hacker nutzten Sicherheitslücken aus, um auf die Router zuzugreifen und dort Passwörter auszulesen oder sie zu manipulieren. Das wichtigste Einfalltor ist dabei nicht mehr ein nur mangelhaft geschütztes WLAN: Die meisten Router-Hersteller haben diesem Weg verbaut, indem sie ihre Geräte ab Werk verschlüsselt oder mit Einrichtungs-Assistenten ausliefern, die eine Verschlüsselung  fordern. Stattdessen nutzen die Hacker aus, dass viele Anwender und Hersteller sehr bequem sind: Sie versäumen es, regelmäßig neue Firmware einzuspielen – wenn sie es denn überhaupt gibt. Oder sie schätzen den angenehmen Fernzugriff auf den Router übers Internet, um ihn zu konfigurieren oder auf das dahinterliegende Heimnetzwerk zuzugreifen. Ist dieser unzureichend geschützt oder fehlerhaft programmiert, haben Sie damit ein riesiges Loch in Ihr Sicherheitsnetz gerissen.

Die gute Nachricht: Die meisten Router-Gefahren können Sie mit wenigen Einstellungen schnell beheben. Wir sagen Ihnen, wo die größten Risiken lauern und worauf Sie achten müssen, damit Ihr Router nicht mehr einladend für Hacker wirkt.

**So schalten Sie den Fernzugriff bei der Fritzbox ab**

## Gefahr: Ungesicherter Fernzugriff

Übers Internet auf den eigenen Router zuzugreifen, hat sich in den letzten Jahren zum Trend entwickelt. Früher waren nur IT-Administratoren daran interessiert, den Firmen-Router aus der Ferne zu warten, um sich Wege zu sparen. Doch auch für Privatnutzer hat der Fernzugriff zahlreiche Vorteile: Sie können den Router aus der Ferne einstellen und analysieren – So haben Sie zum Beispiel jederzeit im Blick, ob die DSL-Verbindung stabil läuft oder wie lange die Kinder schon online sind. Außerdem können Sie über den Router auf Ihr Heimnetzwerk zugreifen: So besorgen Sie sich Dokumente vom heimischen PC oder laden Filme, Musik und Fotos von der NAS oder der am Router angeschlossenen Festplatte aufs Notebook oder Smartphone.

## Das Ziel

Auf die Web-Oberfläche des Routers gelangen Sie normalerweise, wenn Sie die lokale IP-Adresse des Routers in den Browser eingeben. Wie ein Web-Server liefert der Router eine Webseite zurück, auf der Sie sich einloggen, um zu den Router-Einstellungen zu gelangen.

Aktivieren Sie dort die Option „Fernzugriff“ (auch „Remote Management“ genannt), können Sie die Web-Oberfläche auch übers Internet aufrufen – statt der lokalen IP geben Sie die öffentliche IP-Adresse ein, die der Router vom Internet-Anbieter erhalten hat. Wer diese IP-Adresse des Routers kennt und die Kombination aus Benutzername und Passwort, dem steht die Weboberfläche des Routers frei.

**Zugriff begrenzen: Viele Router lassen sich so einstellen, dass sie einen Fernzugriff nur von bestimmte IP-Adressen aus erlauben**

## Die Angriffe

In vielen Fällen können Angreifer eine Schwachstelle der Router-Software bequem ausnutzen, weil der Fernzugriff aktiv ist. So lassen sich zum Beispiel auf anfälligen Routern eine manipulierte Firmware sowie ein Schnüffelprogramm installieren. Damit können Angreifer den Netzwerkverkehr belauschen und Passwörter abgreifen. Als Einfalltor nutzen sie dabei zum Beispiel eine Lücke in der alternativen Router-Firmware DD-WRT.

## So schützen Sie sich

Der Schutz ist einfach: Schalten Sie den Fernzugriff aus – beziehungsweise gar nicht erst ein. Denn bei fast allen Routern ist der Remote-Zugriff ab Werk nicht aktiviert. Wollen Sie sich mit dieser sicheren, aber unbequemen Lösung nicht abfinden, sollten Sie unbedingt das Benutzerkennwort und das Passwort für die Web-Oberfläche des Routers ändern. Die Standard-Passwörter stehen nämlich im Router-Handbuch und sind somit öffentlich verfügbar. Nutzen Sie für das Router-Menü eine Kombination, die Sie für keinen anderen Zugang verwenden, zum Beispiel für Web-Mail oder den Online-Einkauf.

Viele Router bieten außerdem die Möglichkeit, den Fernzugriff auf bestimmte IP-Adressen zu beschränken: Diese können sie nutzen, wenn Sie immer von derselben Gegenstelle – etwa dem Arbeitsplatz – auf den Heim-Router zugreifen wollen. Bei der Fritzbox finden Sie die Einstellungen zum Fernzugriff unter „Internet, Freigaben, Fritzbox-Dienste“.

**Update per Knopfdruck: Wenn sich die Router-Firmware so einfach aktualisieren lässt wie bei der Fritzbox, gibt es keine Argumente, darauf zu verzichten**

## Gefahr: Fehlende Firmware-Updates

Jeder Router hat sein eigenes Betriebssystem: Es setzt meist auf Linux auf und ist in der Firmware des Routers gespeichert. Und wie bei anderen Betriebssystemen, kann auch Router-Firmware fehlerhaft sein: Qualitätsbewusste Hersteller bemühen sich daher um schnelle und häufige Firmware-Updates. Und sicherheitsbewusste Anwender aktualisieren die Firmware häufig.

### Das Ziel

Viele Router-Lücken können Sie selbst schließen, indem Sie Funktionen abschalten – wie beispielsweise beim Fernzugriff. Doch sinnvoller ist es, wenn der Hersteller diese Lücken mit einem Firmware-Update behebt. Außerdem lassen sich einige Software-Fehler nur durch ein Update beheben. Doch viele Anwender verzichten darauf, eine aktuelle Firmware einzuspielen – sei es, weil der Update-Vorgang zu kompliziert ist oder weil sie überhaupt nicht wissen, dass es Update für den Router vorliegt. Diese Update-Müdigkeit können Angreifer ausnutzen. Viele Lücken sind nämlich seit Jahren dokumentiert – die Schwachstelle bei DD-WRT beispielsweise wurde schon vor vier Jahren aufgedeckt. Oft melden sich Hacker auch zuerst beim Hersteller, wenn sie eine Sicherheitslücke entdeckt haben – in der Hoffnung, dass diese sie sofort mit einem Update reagiert. Aber selbst dann ist die Lücke erst geschlossen, wenn das Update auf dem Router installiert wird.

**Update frei Haus: Bei Zwangs-Routern sorgt der Internet-Provider automatisch für eine neue Firmware. Das wäre sehr bequem, wenn Updates auch immer schnell und regelmäßig erscheinen würden**

### Die Angriffe

Das spektakulärste Angriffsziel der letzten Zeit waren die Fritzbox-Router von AVM. Aufgrund einer Schwachstelle in der Router-Firmware konnten Angreifer die komplette Kontrolle über den Router gewinnen, wenn auf einer Webseite, die der Router aufruft Schadcode eingebaut ist. Bei den konkreten Angriffen auf die Fritzbox wurden Rufumleitungen eingerichtet, um damit über die Fritzbox Anrufe an kostenpflichtige Service-Telefonnummern im Ausland durchzuführen – in einem Fall hatte das eine vierstellige Telefonrechnung bei einem Fritzbox-Besitzer zur Folge.

Bei bestimmten Routern von D-Link – zum Beispiel DIR-100 und DI-524 – kann ein Angreifer auf die Web-Oberfläche zugreifen, ohne ein Passwort eingeben zu müssen. Dazu muss er die Browser-Einstellungen für den User Agent verändern – und zwar, indem er eine bestimmte Buchstaben- und Ziffernkombination eingibt. Über diese Hintertür soll die Router-Firmware problemlos Zugang zu bestimmten Einstellungen erhalten, auch wenn der Anwender die Zugangskennung geändert hatte. Diesen Firmware-Fehler konnte jeder Angreifer mit Zugang

zum Router ausnutzen. Ein ähnliches Problem liegt beim Sitecom-WLM-3500 vor: Dieser Router hat zwei Benutzernamen und Kennwörter dauerhaft gespeichert, die Zugriff auf die Weboberfläche geben.

**So schützen Sie sich**

Die Faustregel lautet: Aktualisieren Sie immer, wenn es eine neue Firmware gibt. Da viele Hersteller nicht klarstellen, welche Lücken sie mit einem Update schließen, ist ein Update in jedem Fall sinnvoller als darauf zu verzichten. Viele aktuelle Router suchen automatisch nach neuer Firmware, wenn sie online sind und geben bei Updates einen Hinweis in der Web-Oberfläche. Oft finden Sie diesen auf der Startseite des Konfigurationsmenüs, manchmal müssen sie dafür aber auch ins Menü „Administration“ oder „System“. Bei der Fritzbox gehen Sie dazu in „System, Update, Online-Update“. Sie können auch auf den Support-Webseiten der Router-Hersteller nach Firmware-Updates recherchieren.

| Hersteller | Webseite |
|---|---|
| AVM | http://www.avm.de/de/Service/Service-Portale/index.php |
| Asus | http://www.asus.com/de/support/ |
| D-Link | http://more.dlink.de/sicherheit/router.php |
| Belkin | http://www.belkin.com/de/support-article?articleNum=38510 |
| Buffalo | http://www.buffalo-technology.de/de/support/ |
| Draytek | http://www.draytek.de/hilfe-u-support.html |
| Lancom | http://www.lancom-systems.de/service-support/ |
| Linksys | http://support.linksys.com/de-eu/support/linksys |
| Netgear | http://support.netgear.de/for_home/ |
| Sitecom | http://sitecom.com/de/sie-suchen-eine-lsungkein-problem/71 |
| Telekom | http://hilfe.telekom.de/hsp/cms/content/HSP/de/3388/0/Downloads-und-Handbuecher |
| Trendnet | http://www.trendnet.com/langge/support/ |
| TP-Link | http://www.tp-link.com.de/support/download/ |
| Zyxel | http://www.zyxel.com/de/de/support/download_library.shtml |

Machen Sie die Update-Frequenz auch zum Kaufkriterium: Hersteller die häufig Updates liefern, kümmern sich intensiver um ihre Produkte. Das gilt besonders, wenn sie auch Updates für ältere Router anbieten. Wenn möglich, sollten Sie auch aus Sicherheitsgründen auf Zwangs-Router vom Internet-Provider verzichten. Denn meist müssen Firmware-Updates auf diese speziellen Modelle erst angepasst und vom Provider freigegeben werden. Deshalb dauert es länger, bis eine neue Firmware bereit steht – wenn sie überhaupt verfügbar ist. Beim Fritzbox-Hack im Februar lieferte AVM drei Tage nach dem Angriff für die meisten Modelle eine sichere Firmware aus. Bei den Fritzbox-Modellen der Kabel- und Internetprovider stand das Update dagegen erst nach rund einer Woche bereit.

Bei den Provider-Routern müssen Sie sich dafür normalerweise nicht darum kümmern, das Update einzuspielen. Über das Protokoll TR-069 erledigt der Provider das per Fernzugriff: Die Funktion ist normalerweise ab Werk aktiviert. Bei Telekom-Routern finden Sie sie unter „Verwaltung, Hilfsmittel, EasySupport“. Fritzbox-Modelle für den Internetzugang per TV-Kabel bieten eine ähnliche Funktion unter „Internet, Zugangsdaten, Anbieter-Dienste“.