Mareile Heiting

MEINE DATEN!

Die besten Tipps gegen Datendiebstahl und Hackerangriffe

- E-Mails, Dateien und Benutzerkonten absichern
- Virenschutz, Spam-Abwehr, Surfen ohne Datenspuren
- Onlinebanking und -shopping ohne Risiko
- Daten verschlüsseln, sichern, wiederherstellen

Vierfarben

Darauf sollten Sie bei der Internet-verbindung achten

Online einkaufen, mit Freunden chatten oder schnell mal bei Google prüfen, wo in der Nähe ein gutes Restaurant ist: Für viele ist das Internet mittlerweile zu einer Selbstverständlichkeit geworden. Die Nutzung beschränkt sich schon lange nicht mehr nur auf den heimischen PC oder den Computer im Büro. Auch unterwegs gehen wir mit Smartphone, Tablet und Notebook online. Besteht die Internetverbindung erst einmal, machen sich viele Anwender keinerlei Gedanken mehr darüber, ob diese auch sicher ist. Doch leider gibt es zahlreiche Schlupflöcher, über die Cyberkriminelle Zugriff auf Ihre Geräte erhalten. Das reicht von fehlenden Passwörtern, mit denen Router und WLAN gesichert sein sollten, bis hin zur unverschlüsselten Datenübertragung. Bereits mit wenigen, leicht umsetzbaren Tricks können Sie potenziellen Angreifern den Zugriff auf Ihre Geräte über das Internet schwer machen.

Sicherheitseinstellungen für den Router

Das Drehkreuz zwischen dem Internet und den heimischen Geräten – sei es ein PC, Tablet, Smartphone, Drucker oder Ähnliches – ist der Router. Vereinfacht gesagt ist der Router für die Verteilung von Datenpaketen im Netzwerk zuständig. So sorgt er z. B. dafür, dass die aus dem Internet ankommenden Datenpakete korrekt an die einzelnen Geräte weitergeleitet werden oder auch die innerhalb des Heimnetzwerks verschickten Datenpa-

FRITZ!Box 5491 (Foto: AVM)

kete (etwa vom PC zum Netzwerkdrucker) ihr Ziel erreichen. Zu den bekanntesten Routern zählen die FRITZ!Box-Modelle von AVM sowie der Speedport-Router der Telekom. Bei den meisten Routern handelt es sich heutzutage um WLAN-Router, die neben der kabelgebundenen Datenübertragung auch die kabellose Übertragung via Funksignal ermöglichen.

Tipp 019

Die Internetverbindung steht – warum mehr tun?

Router werden von den Herstellern mittlerweile so ausgeliefert, dass sie sich bequem einrichten lassen und somit bereits nach kurzer Zeit die Verbindung ins Internet genutzt werden kann. Viele Anwender belassen es bei den Werkseinstellungen, die in puncto Sicherheit allerdings doch etwas zu wünschen übrig lassen. Entdecken Cyberkriminelle eine der Sicherheitslücken, gelingt ihnen damit nicht nur der Zugriff auf den Router selbst, sondern auch auf alle angeschlossenen Geräte. Ein Beispiel hierzu: Vor einigen Jahren wurde ein spektakulärer Angriff auf die FRITZ!Box von AVM bekannt, in der ein von außen steuerbares Telefoniegerät in der FRITZ!-Box eingerichtet wurde, über das zahlreiche kurze Anrufe auf teure Auslandsnummern und ausländische Mehrwertnummern getätigt wurden. Die Geschädigten wurden erst durch die extrem hohe Telefonrechnung auf den Angriff aufmerksam. Manche Angriffe bleiben vom Anwender aber auch vollkommen unbemerkt, etwa wenn der eigene PC plötzlich Teil eines sog. *Botnetzes* wird (siehe dazu den folgenden Kasten »Gefahr durch unerkannte Botnetze«).

Gefahr durch unerkannte Botnetze

Vielleicht haben Sie auch schon einmal den Begriff *Botnetz* (engl. *Botnet*) gehört. Hierbei werden Tausende von Computern, die mit einem speziellen Schadprogramm infiziert wurden, zu einem Netzwerk zusammengeschlossen. Ein Computer innerhalb eines solchen Botnetzes wird als *Bot* bezeichnet. Da der Computer vom Botnetz-Betreiber ferngesteuert wird, ist häufig auch von einem *Zombie-PC* die Rede. Das Botnetz nutzt die Rechenleistung und Daten des infizierten Computers, ohne dass dessen Besitzer davon weiß, geschweige denn je seine Einwilligung erteilt hat. Ist ein Computer erst mal Teil eines Botnetzes, wird er häufig für illegale Zwecke, wie etwa das Versenden von Spam-Mails, eingesetzt. Es gibt mittlerweile aber auch legale Einsatzbereiche, etwa zu Forschungszwecken. Dass Ihr Computer Teil eines Botnetzes ist, lässt sich höchstens durch eine langsamere Internetverbindung und deutlich schwächere Rechenleistung feststellen. Meist bleibt die Infektion aber unentdeckt. Schutz vor einem Botnetz bieten eine Vielzahl der im Buch aufgeführten Tipps, wie etwa der Einsatz einer Sicherheitssoftware oder auch die Aktualisierung jeglicher Software inklusive der *Firmware* des Routers, wie z. B. in Tipp 021 auf Seite 53 gezeigt.

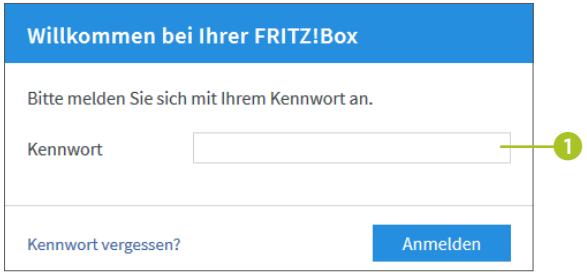
Tipp 020

Passwort des Routers ändern

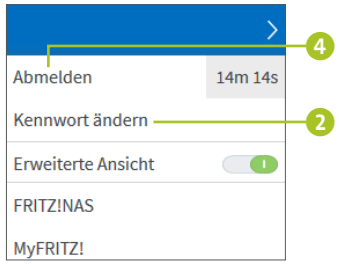
Wenn Sie die Einstellungen der FRITZ!Box ändern möchten, starten Sie den Browser (z. B. Firefox, Safari oder Google Chrome) und rufen die Adresse *http://fritz.box* auf. Beim Speedport-Router lautet die Adresse *http://speedport.ip*. Bevor Sie die Benutzeroberfläche des Routers zu Gesicht bekommen, wird ein Passwort abgefragt. Bei vielen Geräten wird dieses Router-Passwort bereits ab Werk voreingestellt. Das Passwort können Sie je nach Gerät entweder auf der Unterseite des Routers ablesen oder auch über die Support-Webseiten des Herstellers ausfindig machen. Wer herausfindet, welches Modell von welchem Anbieter Sie im Einsatz haben, hat leichten Zugang zu Ihrem Router (lesen Sie hierzu auch

Tipp 025 auf Seite 59). Eine der wichtigsten Sicherheitsmaßnahmen besteht also darin, das Passwort zu ändern. Wie dies funktioniert, zeige ich anhand der FRITZ!Box. Während der Konfiguration des Routers sollten Sie nicht parallel das Internet nutzen. Verwenden Sie außerdem ein Gerät (PC oder Notebook), das Sie per Kabel an den Router anschließen.

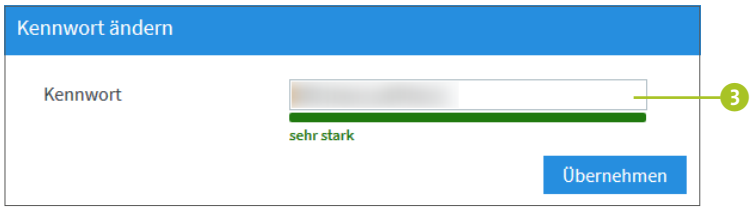
1. Starten Sie den Browser, und rufen Sie die Adresse *http://fritz.box* auf. Melden Sie sich mit dem vom Hersteller vorgegebenen Kennwort an (1). Sollten Sie das Passwort bereits zu einem früheren Zeitpunkt selbst geändert haben, sollten Sie es aus Sicherheitsgründen trotzdem regelmäßig austauschen.



2. Befinden Sie sich in der Benutzeroberfläche der FRITZ!Box, klicken Sie oben rechts auf das kleine Symbol mit den drei Punkten ⋮. Im aufklappenden Menü wählen Sie den Befehl **Kennwort ändern** (2).



3. Geben Sie im Feld **Kennwort** ein neues Passwort ein (3). Der Balken unterhalb des Feldes zeigt, wie »stark«, d. h. wie gut das Passwort ist. Berücksichtigen Sie bei der Passwortwahl die im vorherigen Kapitel vorgestellten Tipps. Wenn Sie einen Passwort-Manager wie LastPass einsetzen, können Sie auch den Passwort-Generator für die Erzeugung des Passwortes nutzen (siehe den Kasten »Sichere Passwörter mithilfe des Passwort-Generators erzeugen« auf Seite 29). Bestätigen Sie das Passwort mit **Übernehmen**.

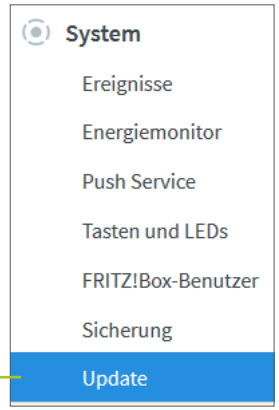


Wenn Sie gleich im Anschluss auch die folgenden Tipps ausprobieren möchten, bleiben Sie bei der FRITZ!Box-Oberfläche angemeldet. Wenn Sie die Konfiguration des Routers unterbrechen müssen, sollten Sie sich unbedingt abmelden. Hierzu reicht ein Klick auf das Symbol mit den drei Punkten und dann auf **Abmelden** (4). Für die folgenden Tipps müssen Sie sich dann natürlich wieder anmelden, wie in Schritt 1 gezeigt – nun allerdings mit Ihrem selbst erstellten Passwort.

Firmware-Update installieren

Tipp 021

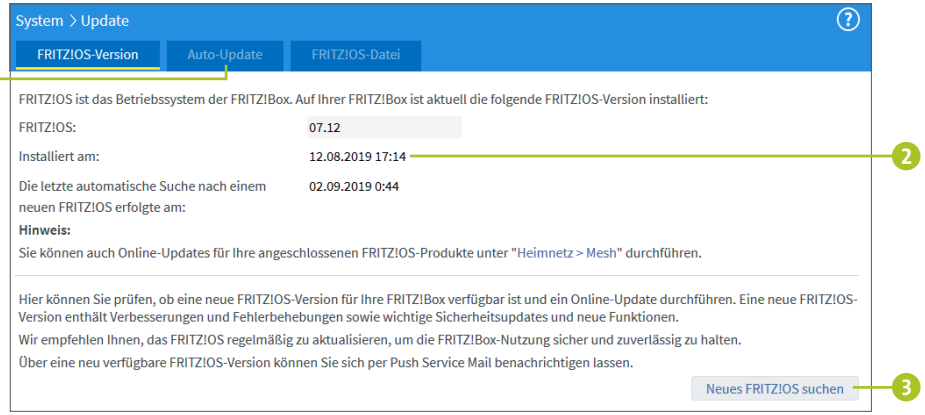
Die Hersteller von Routern veröffentlichen regelmäßig aktualisierte Versionen der Firmware (sprich des Betriebssystems des Routers). Diese enthalten nicht nur neue Funktionen, sondern auch Fehlerbehebungen. Aus Sicherheitsgründen sollten Sie immer die neueste Firmware installieren. Für das Betriebssystem der FRITZ!Box, *FRITZ!OS* genannt, geschieht dies im Normalfall automatisch. Um die Einstellungen sicherheitshalber zu überprüfen, gehen Sie folgendermaßen vor:



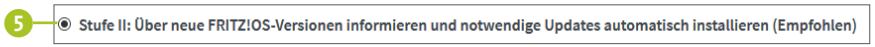
1. Stellen Sie nach der Anmeldung in der Benutzeroberfläche zunächst sicher, dass die erweiterte Ansicht aktiviert ist. Hierzu klicken Sie auf das Symbol ⋮. Der Regler rechts von **Erweiterte Ansicht** sollte grün gefärbt sein.

2. Klicken Sie in der Benutzeroberfläche der FRITZ!Box links auf **System ► Update** (1).

3. Rechts erfahren Sie im Register **FRITZ!-OS-Version**, wann die letzte Version des Betriebssystems installiert wurde (2). Liegt die Installation bereits geraume Zeit zurück, sollten Sie über die Schaltfläche **Neues FRITZ!OS suchen** (3) die Suche nach einer neuen Version starten und diese anschließend installieren.



4. Die Einstellungen zur automatischen Installation wichtiger Updates überprüfen Sie im Register **Auto-Update** (4). Hier sollte mindestens **Stufe II** ausgewählt sein (5). In diesem Fall werden Sie über neue FRITZ!OS-Versionen informiert. Die notwendigen Updates werden außerdem automatisch durchgeführt. Sollten Sie hier Änderungen an den Einstellungen vorgenommen haben, müssen Sie diese mit **Übernehmen** bestätigen.



Weitere FRITZ!Box-Geräte aktualisieren

Haben Sie von AVM noch weitere Geräte im Einsatz, wie etwa einen Repeater, um die Reichweite des WLANs zu erhöhen, oder einen Powerline-Adapter, um Ihre Computer über das interne Stromnetz der Wohnung zu vernetzen? Auch diese Geräte sollten immer auf dem neuesten Stand sein. Um dies zu überprüfen, rufen Sie in der Benutzeroberfläche der FRITZ!Box links **Heimnetz ► Mesh** auf. Blättern Sie rechts in der **Mesh-Übersicht** nach unten bis zur Auflistung der Heimnetzgeräte. Überprüfen Sie in der Spalte **Update**, ob für eines der Geräte eine Aktualisierung vorliegt. Mit einem Klick auf **Update ausführen** stoßen Sie dieses an.

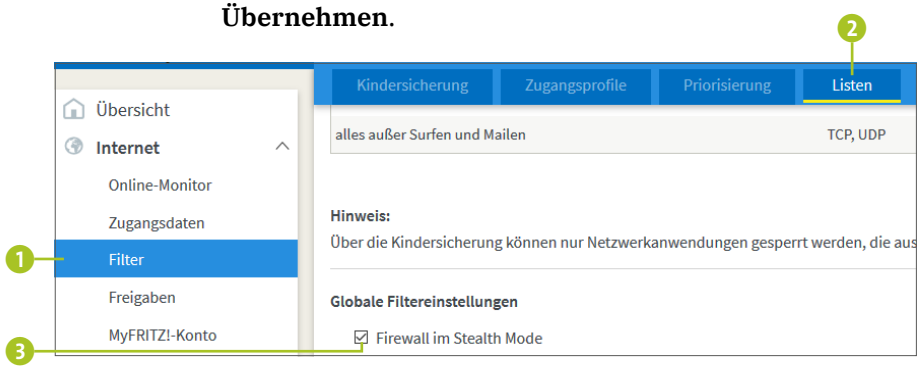
Router-Firewall im Stealth-Modus betreiben

Tipp 022

Die meisten Router haben mittlerweile eine Firewall an Bord, deren Aufgabe es ist, den ein- und ausgehenden Datenverkehr zu überprüfen und unerwünschte Datenpakete abzublocken. Dies gilt auch für die FRITZ!Box. Sogenannte *Ping*-Anfragen, mit denen Angreifer zunächst nur das Vorhandensein der IP-Adresse prüfen, werden in den Standardeinstellungen allerdings nicht verhindert. Fällt eine solche Ping-Anfrage positiv aus, erhält der Angreifer die Bestätigung, dass die IP-Adresse vergeben ist. Damit rentiert sich für ihn ein richtiger Angriff. Eine wichtige Sicherheitseinstellung besteht also darin, derartige Anfragen zu verhindern. Hierzu muss die

Firewall im sog. *Stealth-Modus* betrieben werden. Um ihn zu aktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der linken Spalte der Benutzeroberfläche der FRITZ!Box auf **Internet ► Filter** (1).
2. Wechseln Sie in der rechten Fensterhälfte in das Register **Listen** (2). Blättern Sie nun ganz nach unten bis zum Bereich **Globale Filtereinstellungen**.
3. Versehen Sie das Kästchen vor **Firewall im Stealth Mode** mit einem Häkchen (3). Bestätigen Sie die Einstellung mit **Übernehmen**.

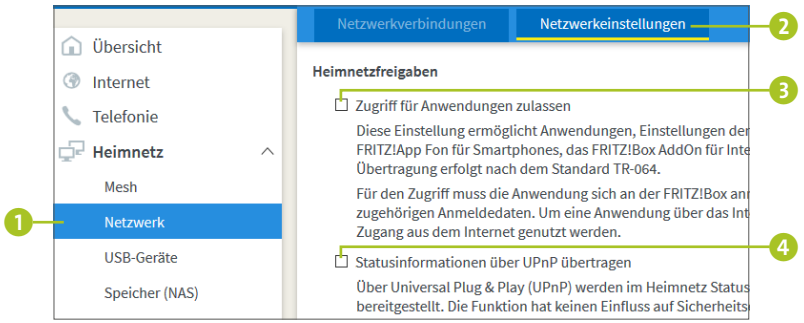


Tipp 023

Berechtigungen für Portfreigabe unterbinden

Ob Fitnessuhr oder das Smart-TV-Gerät: Beide zählen zum *Internet der Dinge* (kurz: IoT für *Internet of Things*). Diese IoT-Geräte werden meist per WLAN an das Heimnetzwerk angeschlossen. Hierfür nutzen die Geräte *UPnP* (Abkürzung für *Universal Plug and Play*), das eine Kommunikation zwischen Geräten unterschiedlicher Hersteller ermöglicht. Ist in Ihrem Router UPnP aktiviert, kann allerdings jedes beliebige Gerät und auch jede Software inklusive Schadprogramme im Heimnetzwerk den Router konfigurieren und so z. B. bestimmte Ports in der Firewall öffnen (lesen Sie hierzu auch den Kasten »Vorsicht mit der Freigabe von Ports« auf Seite 95). Aus Sicherheitsgründen sollten Sie UPnP deshalb in Ihrem Router deaktivieren. In der FRITZ!Box gehen Sie hierzu folgendermaßen vor:

1. Rufen Sie in der Benutzeroberfläche der FRITZ!Box links nacheinander **Heimnetz ► Netzwerk** (1) auf. Wechseln Sie dann rechts in das Register **Netzwerkeinstellungen** (2).
2. Blättern Sie auf der Seite nach unten bis zu den **Heimnetzfreigaben**. Hier entfernen Sie das Häkchen vor **Zugriff für Anwendungen zulassen** (3). Die **Statusinformationen über UPnP übertragen** (4) können Sie wiederum aktiviert lassen. Bestätigen Sie mit **Übernehmen**.



Portfreigaben für ein bestimmtes Gerät erteilen

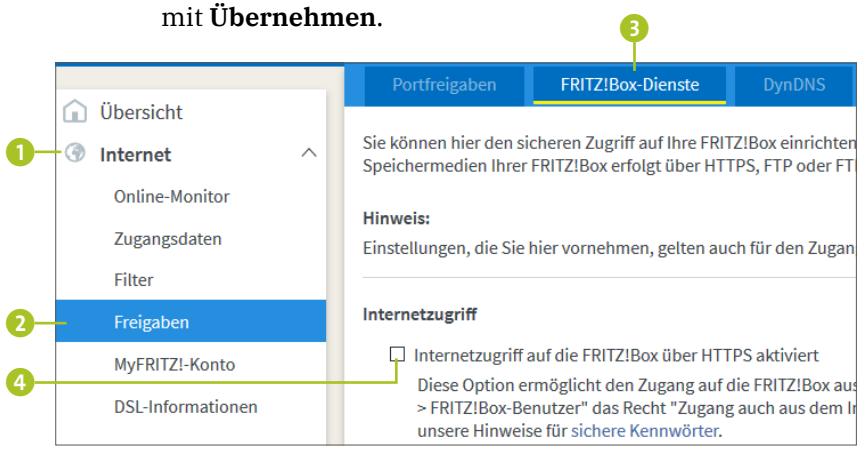
Eine Spielekonsole, die Sie gerne nutzen, benötigt unbedingt UPnP, um die Portfreigaben des Routers steuern zu können? In der FRITZ!Box ist es möglich, nur ganz bestimmten Geräten die Portfreigabe zu erlauben. Rufen Sie hierzu **Heimnetz ► Netzwerk** auf, und markieren Sie rechts das Register **Netzwerkverbindungen**. Suchen Sie in der folgenden Liste das gewünschte Gerät, und klicken Sie auf das Stiftsymbol rechts, um die Einstellungen für dieses Gerät zu öffnen. Auf der folgenden Seite aktivieren Sie **Selbstständige Portfreigaben für dieses Gerät erlauben** und bestätigen mit **OK**.

Tipp 024

Fernzugriff nur dann, wenn nötig

Auf die Benutzeroberfläche der FRITZ!Box lässt sich auch von unterwegs aus zugreifen. Der entsprechende Dienst nennt sich *MyFRITZ!*. Um ihn nutzen zu können, müssen Sie sich einmal in der Benutzeroberfläche der FRITZ!Box über **Internet ► MyFRITZ!-Konto** mit einer E-Mail-Adresse registrieren. Anschließend können Sie z. B. über die MyFRITZ!-App von Ihrem Smartphone aus auf eine an die FRITZ!Box angeschlossene USB-Festplatte zugreifen. Was Ihnen möglich ist, kann aber auch Angreifern gelingen. Wer diesen Dienst also nicht wirklich dringend benötigt, sollte aus Sicherheitsgründen lieber darauf verzichten. Um sicherzustellen, dass der Fernzugriff deaktiviert ist, gehen Sie folgendermaßen vor:

1. Klicken Sie in der linken Spalte der Benutzeroberfläche der FRITZ!Box auf **Internet** (1) und dann auf **Freigaben** (2).
2. Rufen Sie rechts das Register **FRITZ!Box-Dienste** (3) auf.
3. Stellen Sie sicher, dass das Kästchen vor **Internetzugriff auf die FRITZ!Box über HTTPS aktiviert** nicht mit einem Häkchen versehen ist (4). Sollte der Dienst aktiviert sein, entfernen Sie das Häkchen per Mausklick und bestätigen mit **Übernehmen**.



Das private WLAN schützen

Ein *WLAN* (Abkürzung für *Wireless Local Area Network*) in den eigenen vier Wänden ist ausgesprochen praktisch. Nur wenige Schritte sind nötig, und schon sind Computer, Tablet, Smartphone und mehr mit dem Internet und dem Heimnetzwerk verbunden – und das ganz ohne Kabelsalat. Wie für den Router gilt auch für das Funknetzwerk: Übernehmen Sie nicht blind die Werkseinstellungen des Herstellers, sondern überprüfen Sie die Sicherheitseinstellungen, um Ihr privates WLAN vor Angriffen von außen zu schützen. Sie stellen damit zugleich sicher, dass keine Person außerhalb Ihrer eigenen vier Wände über Ihr WLAN eine Verbindung ins Internet herstellt. Denn denken Sie daran: Sie haften für alles (legal oder illegal), was über Ihre Internetverbindung geschieht.

Tipp 025

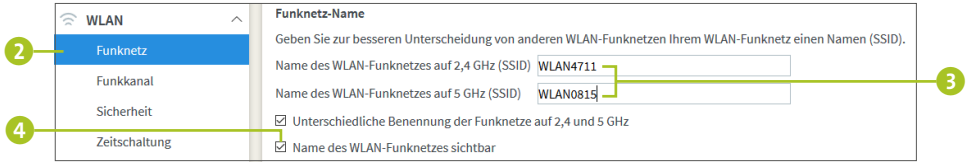
Eigenen Namen für WLAN vergeben

Jedes Funknetzwerk verfügt über einen Namen, die sog. *SSID* (Abkürzung für *Service Set Identifier*). Dies gilt natürlich auch für Ihr eigenes, privates WLAN daheim. Per Werkseinstellung vergeben Hersteller wie AVM hier meist den Namen des Routers, also z. B. *FRITZ!Box 4790*. Diese Angabe lässt nicht selten aber auch Rückschlüsse auf das per Werk vergebene Passwort zu (siehe hierzu auch den nächsten Tipp). Doch die SSID des WLANs ist schnell geändert:

1. Melden Sie sich in der Benutzeroberfläche der FRITZ!Box an, so wie in Tipp 020 auf Seite 51 gezeigt. Stellen Sie nach einem Klick auf das Symbol sicher, dass **Erweiterte Ansicht** aktiviert ist (1).

2. Klicken Sie in der linken Spalte auf **WLAN** und dann auf **Funknetz** (2). Blättern Sie in der rechten Fensterhälfte nach unten bis zum Bereich **Funknetz-Name**.

3. Die meisten Modelle der FRITZ!Box arbeiten sowohl mit dem 2,4-GHz-Frequenzband als auch mit dem 5-GHz-Frequenzband. Vergeben Sie für jedes einen eigenen Namen (3). Dieser sollte weder einen Rückschluss auf den verwendeten Router zulassen, noch auf Sie oder Ihr Haus hinweisen. Name, Straße und Hausnummer sind also keine gute Wahl. Damit es keine Probleme mit Funknetzen in der Nachbarschaft gibt, sollten Sie einen noch nicht vergebenen Namen wählen.



4. Bestätigen Sie die Eingaben mit **Übernehmen**.

Funknetz-Namen unsichtbar machen

Immer wieder hört man den Rat, den Namen des WLANs zu verbergen, frei nach dem Motto: »Was man nicht sieht, kann man auch nicht finden«. Umgesetzt ist dieser Ratschlag schnell: Einfach unter **WLAN ► Funknetz** im Bereich **Funknetz-Name** das Häkchen vor **Name des WLAN-Funknetzes sichtbar** (4) entfernen, mit **Übernehmen** bestätigen, und schon erscheint das WLAN nicht mehr in der Liste der verfügbaren Funknetzwerke. Die bereits angemeldeten Geräte bleiben dabei weiterhin mit dem WLAN verbunden. Um vor den Nachbarn das WLAN zu verbergen, mag der Tipp geeignet sein. Einen Profi, der über ein Spähprogramm verfügt, hält eine versteckte SSID allerdings nicht ab!

Inhalt

Am Passwort führt kein Weg vorbei

Darauf sollten Sie bei der Internetverbindung achten

So schützen Sie Ihren PC

Mit dem Smartphone sicher unterwegs

Für alle Fälle: Daten sichern

Die Kommunikation per E-Mail absichern

Wichtige Schutzmaßnahmen für den Browser

Gut geschützt: Bankgeschäfte im Internet erledigen

Entspannt Reisen buchen und online shoppen

Schwachstellen in sozialen Netzwerken

Das richtige Troubleshooting