



# Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

## 3 Ist Ihr Router-Betriebssystem veraltet?

Aktualisieren Sie in 7 Schritten das Router-Betriebssystem. Die Sicherheit Ihrer Internetverbindung hängt davon ab!

## 4 Werden Sie auf Betrugsseiten entführt?

Überprüfen Sie Windows und Ihren Router auf Namensmanipulationen. So werden Sie nicht auf gefälschte Seiten gelenkt.

## 5 Lässt Ihr Funknetzwerk Hacker herein?

Eine Gefahr für Ihre Internetverbindung ist die WPS-PIN. Schließen Sie mit meinen Tipps alle Schlupflöcher.

## 7 Schaut Ihnen jemand aus dem Ausland zu?

Erlauben Sie keinen Fernzugriff auf Ihren Router. Mit meiner Hilfe stellen Sie alle Fernsteuerungsfunktionen sicher ein.

**+++ Schließen Sie alle Sicherheitslücken Ihres Routers! Damit wird Ihr Router nicht gehackt oder manipuliert +++**

## Der teure Router-Hack: Telefonrechnungen über 50.000 €!

Stellen Sie sich vor, Ihr Konto ist plötzlich weit im Minus. Ihre Ersparnisse sind von heute auf morgen weg.

Denn von Ihrem Konto wurde eine Telefonrechnung in Höhe von mehreren Zehntausend Euro abgebucht.

Sie sollen angeblich 12.000 Telefonate ins Ausland geführt haben, und zwar in nur drei Tagen.

Die Ursache kann sein, dass Hacker in Ihren Router eingebrochen sind und Telefonanrufe über ein Wählprogramm gestartet haben.

Das ist zwei PC-Anwendern aus Baden-Württemberg im ersten Halbjahr 2018 passiert, wie die Bundesnetzagentur meldete.

Zum Glück für die Betroffenen wurde deren Internetanbieter durch die vielen Anrufe auf den Router-Hack aufmerksam.

**Meine Empfehlung:** Kontrollieren Sie regelmäßig Ihren Router. Alles was Sie dazu wissen müssen, erfahren Sie in diesem Spezialreport.



Viele Grüße, Ihr

Michael-Alexander Beisecker,  
Deutschlands  
PC-Sicherheitsexperte Nr. 1

Schließen Sie die Sicherheitslücken Ihres Routers durch ein Betriebssystem-Update

## Mit diesen 7 Sicherheits-Checks vermeiden Sie teure Router-Hacks

**Jeder vierte Router hat mindestens eine offene Sicherheitslücke (26,2 Prozent, Quelle Avira). Der Tipp des FBI zu Ihrem Schutz: Sie sollen den Router kurz aus- und wieder einschalten, dann soll die Gefahr vorbei sein. Das hilft aber nur kurzfristig. Wirklichen Schutz bietet Ihnen nur eine vollständige Kontrolle mit meinen nachfolgenden Sicherheits-Checks, die ich für Sie ausgearbeitet habe.**

Ziehen Sie bei Ihrem Router einmal die Woche das Netzkabel aus der Steckdose und stecken Sie es nach rund einer Minute wieder ein. Dieser vom FBI empfohlene Router-Neustart bewirkt ein vollständiges Löschen des Arbeitsspeichers Ihres Routers und damit auch etwaiger Schadprogramme im Speicher. Das ist aus Sicherheitsgründen sinnvoll und wichtig für einen störungsfreien Betrieb. Sicher wird Ihr Router aber durch diese einzelne Maßnahme keineswegs.

Ein unsicheres Zugangskennwort, eine veränderte DNS-Einstellung (Domain Name System, ist für den Aufruf von Internetseiten essenziell), unsichere WLAN-Einstellungen, Sicherheitslücken im Betriebssystem oder gar ein Hacker-Betriebssystem sind auch nach dem erneuten Einschalten Ihres Routers weiter vorhanden.

Gehen Sie daher kein Risiko ein und kontrollieren Sie mit den nachfolgenden Sicherheits-Checks gründlich, ob nach dem Neustart noch Gefahren bestehen.

### Die 7 Sicherheitschecks für die Kontrolle Ihrer Internet-Verbindung auf einen Blick:

- |                             |  |
|-----------------------------|--|
| <b>Sicherheits-Check 1:</b> | Ist Ihr Router durch ein sicheres Kennwort geschützt?    |
| <b>Sicherheits-Check 2:</b> | Ist das Router-Betriebssystem auf dem neuesten Stand?    |
| <b>Sicherheits-Check 3:</b> | Werden Sie heimlich auf Betrugsseiten umgelenkt?         |
| <b>Sicherheits-Check 4:</b> | Haben ungebetene Besucher Zugriff auf Ihr WLAN?          |
| <b>Sicherheits-Check 5:</b> | Können Hacker per WPS auf Ihr Netzwerk zugreifen?        |
| <b>Sicherheits-Check 6:</b> | Lassen Sie zu, dass Kriminelle Ihren Router fernsteuern? |
| <b>Sicherheits-Check 7:</b> | Haben Besucher vollen Zugriff auf Router und Internet?   |



**Mein Tipp:** Keine Angst, die sicheren Einstellungen nehmen Sie unter meiner Anleitung Schritt für Schritt vor. Sie werden sehen, in weniger als 60 Minuten ist Ihr Router vor Hacker-Angriffen besser geschützt und Ihre Internetverbindung sicher!

>>> Lesen Sie bitte weiter auf Seite 2

&gt;&gt;&gt; Fortsetzung von Seite 1

## Sicherheits-Check 1: Ist Ihr Router durch ein sicheres Kennwort geschützt?

Vertrauen Sie beim Router-Kennwort weder auf den Router-Hersteller noch auf Ihren Internetanbieter. Haben Sie den Router selbst gekauft, ist das voreingestellte, sehr einfache Kennwort in Sekundenschnelle gehackt. Es lautet zum Beispiel „admin“, „0000“ oder „1234“ und steht öffentlich zugänglich im Router-Handbuch oder ist auf einem Aufkleber am Router zu finden. Hat Ihr Internetanbieter den Router geliefert, lassen sich der voreingestellte Benutzername und das Kennwort womöglich über ein Tool berechnen. Vergeben Sie daher ein eigenes, sicheres Kennwort mit einer Länge von mindestens 16 Zeichen.

Die nachfolgende Anleitung und alle weiteren in diesem Spezialreport wurden für den weitverbreiteten FRITZ!Box-Router geschrieben. Haben Sie einen anderen Router, achten Sie auf meine Hinweise zu möglichen Unterschieden und schauen Sie im Handbuch zu Ihrem Router nach.



**Mein Tipp:** Laden Sie das Handbuch zu Ihrem Router als PDF-Datei von der Internetseite des Router-Herstellers oder Ihres Internetanbieters herunter. Eine Übersicht der Support-Seiten wichtiger Router-Hersteller finden Sie auf unserer sicheren Service-Webseite: [www.pc-sicherheitsberater.de](http://www.pc-sicherheitsberater.de).

### In 10 Minuten richten Sie Ihr sicheres Router-Kennwort ein

Rufen Sie mit Ihrem Browser, also zum Beispiel mit Firefox, die Router-Oberfläche auf. Dazu geben Sie ins Adressfeld die IP-Adresse Ihres Routers ein, wie zum Beispiel **192.168.178.1**, ein oder die spezielle Anmeldeadresse wie **fritz.box** bei einem FRITZ!Box-Router, **http://speedport.ip** bei einem Speedport-Router der Telekom und **routerlogin.com** bei Routern anderer Hersteller.



**Mein Tipp:** Kennen Sie die IP-Adresse Ihres Routers nicht, drücken Sie **Windows + (R)**, geben **cmd** ein und klicken auf **OK**. An der Eingabeaufforderung geben Sie **ipconfig** ein, drücken die Eingabetaste **(↵)** und lesen die IP-Adresse in der Zeile **Standardgateway** ab.

1. Geben Sie **Benutzer** und **Kennwort** oder – wenn keine Benutzer eingerichtet sind – auch nur das Kennwort ein. Klicken Sie nach der Eingabe auf **Anmelden** oder auf die betreffende Schaltfläche. Kennen Sie Benutzer und Kennwort nicht, finden Sie diese entweder im Router-Handbuch, auf einem Aufkleber am Router oder auf einem Notizzettel, der dem Router beiliegt.
2. Haben Sie bereits ein Router-Kennwort vergeben, überprüfen Sie es auf Sicherheit: Es sollte mindestens 16

Melden Sie sich mit Ihrem Kennwort an.

Kennwort




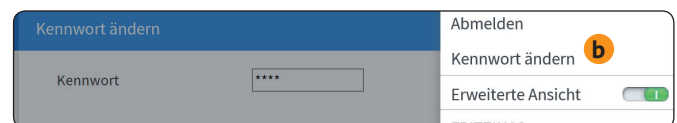
*Haben Sie keine Benutzer eingerichtet, geben Sie zur Anmeldung bei Ihrer FRITZ!Box nur das Kennwort **a** ein.*

Zeichen lang sein, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Ist Ihr Kennwort sicher, machen Sie mit Sicherheits-Check 2 weiter.



**Mein Tipp:** Lässt Ihr Router kein 16 Zeichen langes Kennwort zu, ist er wahrscheinlich veraltet. Tauschen Sie Ihren Router gegen ein aktuelles Modell aus, wenn der Hersteller-Support abgelaufen ist. Ist der Router noch aktuell, sollte das Passwort so lang wie möglich sein.

3. Vergeben Sie ein neues, sicheres Passwort. Klicken Sie dazu bei der FRITZ!Box auf das **Menü-Symbol**  in der oberen rechten Ecke und auf **Kennwort ändern** **b**. Geben Sie das neue Kennwort ein und klicken auf **Übernehmen**.



*Ein aktueller Router hat eine deutsche Oberfläche und ist so einfach mit der Maus zu bedienen wie Windows.*

### So lösen Sie das häufige Problem eines unbekannten oder vergessenen Router-Kennworts

Hat Ihr Internetanbieter das Router-Kennwort vergeben und Sie kennen es nicht, fordern Sie das Kennwort über den Support des Internetanbieters an. Der Internetanbieter muss Ihnen das Kennwort aushändigen.

Haben Sie das selbst vergebene Router-Kennwort vergessen, klicken Sie am Anmeldebildschirm der FRITZ!Box auf **Kennwort vergessen?**, ziehen für 5 Sekunden den Netzstecker der FRITZ!Box und folgen dann den Anweisungen auf dem Anmeldebildschirm.

Bei einem anderen Router suchen Sie nach einer kleinen Öffnung im Gehäuse mit einem Reset-Taster. Drücken Sie diesen Taster mit einer Kugelschreiberspitze oder einer aufgebogenen Büroklammer für mehrere Sekunden herunter.

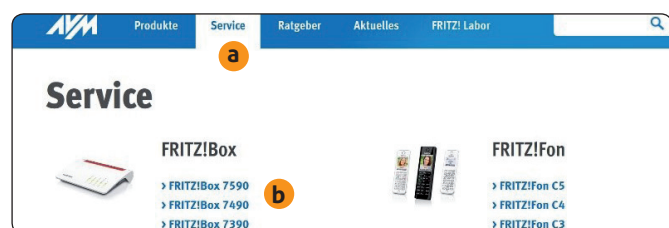
**Achtung:** Mit dem Zurücksetzen des Kennworts oder dem Reset-Taster wird Ihr Router auf die voreingestellten Werkseinstellungen zurückgesetzt. Sie müssen anschließend alle Einstellungen inklusive des Kennworts und Ihrer Internet-Verbindungsdaten neu eingeben.

# Sicherheits-Check 2: Ist das Router-Betriebssystem auf dem neuesten Stand?

Ihr Router hat wie Ihr PC ein internes Betriebssystem. Sicherheitslücken werden wie bei Windows durch Updates geschlossen. Das erfolgt jedoch beim Router nicht automatisch. Sehen Sie daher regelmäßig auf der technischen Hilfeseite des Router-Herstellers nach, ob dort eine neuere Betriebssystem-Version für Ihren Router angeboten wird. Zur technischen Hilfeseite für Ihren Router gelangen Sie über die Liste der Support-Seiten auf unserer sicheren Service-Webseite [www.pc-sicherheitsberater.de](http://www.pc-sicherheitsberater.de).

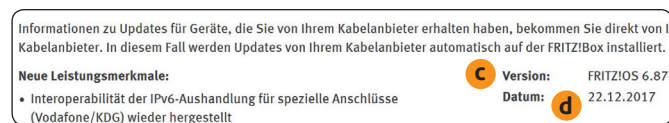
Befolgen Sie die speziellen Hinweise des Router-Herstellers für Ihr Modell, sofern diese nicht mit der folgenden Anleitung übereinstimmen:

1. Rufen Sie die technische Hilfeseite zu Ihrem Router auf. Haben Sie eine FRITZ!Box, gelangen Sie auf das Register **Service** **a** der Internetseite des FRITZ!Box-Herstellers AVM.
2. Wählen Sie die Bezeichnung Ihres Routers **b** aus, die Sie auf einem Etikett an der Rück- oder Unterseite Ihres Routers finden. Sie gelangen dann auf die spezielle Service-Seite für Ihren Router.



Finden Sie Ihr Router-Modell nicht in dieser Übersicht, klicken Sie auf **Weitere Produkte**.

3. Links unter **Übersicht** klicken Sie auf **Downloads**, um zu den herunterladbaren Dateien zu gelangen. Hier finden Sie die neueste Betriebssystem-Version Ihres Routers. Vergleichen Sie die Angaben hinter **Version** **c** und **Datum** **d** mit den Angaben Ihres Routers.



Das Betriebssystem des FRITZ!Box-Routers heißt FRITZ!OS; dies ist die Abkürzung für FRITZ! Operating System.

4. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
5. Suchen Sie nach dem Menüpunkt für das Firmware-Update. Im Fall der FRITZ!Box nehmen Sie die Aktualisierung über **System** und **Update** oder **Firmware-Update** vor.

6. Klicken Sie auf die Schaltfläche **Neues FRITZ!OS suchen** oder **Neue Firmware suchen** oder die entsprechende Schaltfläche bei Ihrem Router.

7. Findet Ihr Router eine neue Version, klicken Sie die Schaltfläche **Update jetzt starten** oder **Firmware-Update jetzt starten** an und das Betriebssystem wird aktualisiert. Während dieser Zeit blinken unter Umständen LEDs am Gerät. Warten Sie, bis das Update abgeschlossen ist.



**Mein Tipp:** Aktivieren Sie die **Auto-Update**-Option, wenn Ihr Router automatische Updates unterstützt. Das neueste Betriebssystem wird dann wie bei Windows zukünftig automatisch installiert. Weitere Hinweise zur Auto-Update-Option finden Sie im Handbuch zu Ihrem Router.

## Was machen Sie, wenn es keine Update-Funktion gibt?

Finden Sie keine Update-Funktion, hat Ihr Internetanbieter diese Funktion gesperrt. Ist das Router-Betriebssystem veraltet, fordern Sie von Ihrem Internetanbieter eine Aktualisierung oder den Austausch des Routers gegen ein aktuelles Modell. Sie haben das Recht darauf, einen eigenen, sicheren Router zu verwenden.

## Pannenhilfe, wenn das Kennwort nicht mehr erkannt wird

Nach dem Betriebssystem-Update kennt Ihr Router womöglich Ihr sicheres Kennwort nicht mehr und verweigert Ihnen die Anmeldung. Der Router wurde dann wie beim Reset (siehe Seite 2) auf die Werkseinstellungen zurückgesetzt.

Verwenden Sie zur Anmeldung in diesem Fall das Standard-Passwort, das Sie in der Dokumentation zu dem Gerät finden, oder das Passwort auf dem Router-Aufkleber. Geben Sie wie im Sicherheits-Check 1 beschrieben erneut ein sicheres Kennwort ein. Dann richten Sie den Router entsprechend den Vorgaben Ihres Internetanbieters neu für einen Internetzugang ein.

## LESERSERVICE

**Redaktionshilfe:** Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

Melden Sie sich dazu einfach kostenlos unter <https://club.computerwissen.de> an und stellen Sie ihm dort Ihre Fragen.

**Michael-Alexander Beisecker** und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.



# Sicherheits-Check 3: Werden Sie heimlich auf Betrugsseiten umgelenkt?

Haben Internetkriminelle die Einstellung für den Domain-Namen-Server bei Ihrem Router geändert, werden Sie unbemerkt auf Betrugsseiten umgelenkt. Sie geben zum Beispiel die Internetadresse pc-sicherheitsberater.de ein und landen auf einer ganz anderen Seite der Betrüger. Damit Sie die Täuschung nicht bemerken, sieht die gefälschte Seite fast wie die echte Seite aus. Führen Sie meine zwei folgenden Checks aus, damit Sie nicht in diese Falle laufen.

Kontrollieren Sie den DNS-Server auf zwei Ebenen: auf der Windows-Ebene und bei den Einstellungen für den DNS-Server in Ihrem Router.

## Check 1: Manipuliert ein Schadprogramm die Domain-Namen auf Ihrem Windows-PC?

1. Drücken Sie die Tastenkombination **Windows + R**, um das **Ausführen**-Fenster aufzurufen.
2. Geben Sie **cmd** ein und klicken Sie auf **OK**. Die Eingabeaufforderung öffnet sich.
3. Rufen Sie mit **ipconfig /all** die eingerichteten Internetverbindungen ab und überprüfen Sie bei den Angaben zum **Ethernet-Adapter** **a** die Adresse hinter **DNS-Server** **b**.

```
Windows-IP-Konfiguration

Hostname . . . . . : DESKTOP-SQK92Q0
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert . . . . . : Nein
WiNS-Proxy aktiviert . . . . . : Nein
DNS-Suffixsuchliste . . . . . : fritz.box

Ethernet-Adapter Ethernet: a

Verbindungsspezifisches DNS-Suffix: fritz.box
Beschreibung. . . . . : Intel(R) Ethernet Connection (2) I218-V
Physische Adresse . . . . . : 70-8B-CD-55-3F-F8
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . . . : Ja
Verbindungslokale IPv6-Adresse . . . . . : fe80::4106:34b2:b56a:3cef%14(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.178.43(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Freitag, 16. September 2016 09:13:15
Lease läuft ab. . . . . : Freitag, 30. September 2016 12:39:51
Standardgateway c . . . . . : 192.168.178.1
DHCP-Server . . . . . : 192.168.178.1
DHCPv6-IAID . . . . . : 91261901
DHCPv6-Client-DUID . . . . . : 00-01-00-01-1F-5B-AE-96-70-8B-CD-55-3F-F8
DNS-Server b . . . . . : 192.168.178.1
NetBIOS über TCP/IP . . . . . : Aktiviert
```

Die Adresse hinter **DNS-Server** muss mit der für **Standardgateway** **c** übereinstimmen, also mit der IP-Adresse Ihres Routers.

4. Stimmt die IP-Adresse hinter **DNS-Server** nicht mit der Ihres Routers überein, wird auf einen anderen DNS-Server umgelenkt. Überprüfen Sie Ihren PC mit Ihrem Antiviren-Programm auf Schadprogramme.
5. Öffnen Sie mit dem Windows-Explorer das Systemlaufwerk (meist Festplatte C:) und dort den Ordner **\Windows\System32\drivers\etc**.
6. Klicken Sie mit der rechten Maustaste auf **hosts** und wählen Sie **Öffnen mit** und **Editor**. In der Hosts-Datei sollten unterhalb des voreingestellten Eintrags für **localhost** **d** keine zusätzlichen Einträge stehen, sofern Sie diese nicht selbst dort eingetragen haben.

```
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97      rhino.acme.com      # source server
# 38.25.63.10      x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#
# 127.0.0.1        localhost
# ::1              localhost
127.0.0.1          gdpwmgrlocalhost d
```

Manipulieren Schadprogramme diese Hosts-Textdatei, werden Sie unbemerkt auf betrügerische Internetseiten geführt.

## Check 2: Wurde der Domain-Server-Eintrag Ihres Routers geändert?

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Überprüfen Sie die eingetragene DNS-Server-Adresse. Verwenden Sie eine FRITZ!Box, wählen Sie dazu **Internet, Zugangsart** und öffnen das Register **DNS-Server**.
3. Hier sollte die Option **Vom Internetanbieter zugewiesener DNSv4-Server verwenden (empfohlen)** aktiviert sein. Sind stattdessen unter **Andere DNSv4-Server verwenden** eine oder zwei IP-Adressen eingetragen, überprüfen Sie diese mit dem IP-Lookup-Tool, das Sie an der Adresse <https://www.whois.net/> finden.. Geben Sie die IP-Adresse des DNS-Servers ein **e** und das Tool zeigt Ihnen an, wer den Dienst betreibt und in welchem Land und Ort er sich befindet **f**.

### WHOIS IP Lookup Tool

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

80.69.96.12 **e** **Go »**

Related Tools: [DNS Traversal](#) [Traceroute](#) [Vector Trace](#) [Ping](#) [WHOIS Lookup](#)

```
Source: whois.ripe.net
IP Address: 80.69.96.12 (Germany)

% This is the RIPE Database query service.
% The objects are in RPSL format.
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '80.69.96.0 - 80.69.97.255'

% Abuse contact for '80.69.96.0 - 80.69.97.255' is 'abuse@umkbw.de'

inetnum:      80.69.96.0 - 80.69.97.255
netname:      DE-FNDW-IP1
descr:        Unitymedia
descr:        Kerpen
country:      DE f
```

Diese IP-Adresse wird vom Internetanbieter Unitymedia aus Kerpen, Deutschland, verwendet und der DNS-Server ist daher sicher.

## Sicherheits-Check 4: Haben ungebetene Besucher Zugriff auf Ihr WLAN-Funknetzwerk?

Sie haben Ihr Funknetz schon mit einem sicheren Kennwort und aktueller Router-Software geschützt. Die Zeiten ungesicherter WLAN-Funknetzwerke und des unsicheren, veralteten WEP-Verschlüsselungsverfahrens sind zum Glück auch vorbei. Jeder aktuelle Router hat voreingestellt die bessere WPA-/WPA2-Verschlüsselung aktiviert. Doch nach wie vor hacken sich Angreifer aus der Nachbarschaft und vor der Haustür in Ihr WLAN-Funknetzwerk, wenn Sie nicht aufpassen. Das eingestellte WLAN-Kennwort ist meist nicht sicher genug. Lassen Sie nur Ihnen bekannte Geräte auf Ihr WLAN zugreifen.

### Check 1: Überprüfen Sie Funknetz-Aktivierung und -Name

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Wählen Sie bei einer FRITZ!Box erst **WLAN** und dann **Funknetz**.
3. Haben Sie alle Ihre Rechner per Kabel an den Router angeschlossen und brauchen daher kein WLAN, entfernen Sie den Haken vor der Option **Funknetz aktiv** und klicken auf **Übernehmen**.
4. Lassen Sie **Funknetz aktiv** aktiviert, sollte der Name Ihres WLAN-Funknetzes (SSID) keinen Hinweis auf Router-Hersteller oder -Modell enthalten. Hacker könnten diese Informationen nutzen, um gezielt Sicherheitslücken Ihres Router-Typs auszunutzen. Ändern Sie also zum Beispiel eine Standard-SSID wie **FRITZ!Box 6490 Cable** in **Mein WLAN** oder entfernen Sie den Haken von der Option **Name des WLAN-Funknetzes sichtbar**.

### Check 2: Überprüfen Sie Verschlüsselung und Kennwort

1. Wechseln Sie nun in **WLAN** und **Sicherheit**. Hier sollte **WPA-Verschlüsselung** aktiviert sein, denn sie bietet Ihnen die größte Sicherheit.
2. Im Listenfeld **WPA-Modus** stellen Sie **WPA+WPA2** ein, damit auch ältere PCs, Tablets und Smartphones ohne WPA2-Unterstützung das Funknetz nutzen können.
3. Überprüfen Sie den **WLAN-Netzwerkschlüssel** auf Sicherheit. Er sollte mindestens 20 Zeichen lang sein und aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

**Achtung:** Der voreingestellte WLAN-Netzwerkschlüssel Ihres Internetanbieters ist nicht sicher. Er ist zu kurz und besteht meist nur aus Ziffern. Der WLAN-Netzwerkschlüssel steht zudem auf einem Aufkleber am Router und kann dort auch von Unbefugten abgelesen werden.

4. Ist der **WLAN-Netzwerkschlüssel** nicht sicher genug, ändern Sie ihn.
5. Haben Sie bei **Sicherheit** Änderungen vorgenommen, klicken Sie auf **Übernehmen**.
6. Haben Sie Änderungen an der Verschlüsselung oder dem WLAN-Kennwort vorgenommen, sind Ihre Geräte nun

nicht mehr mit dem Funknetzwerk verbunden. Führen Sie folgende Änderungen an Ihren Rechnern durch:

- **Desktop-PCs und Notebooks:** Klicken Sie auf das WLAN-Symbol, wählen Sie Ihr WLAN aus und geben Sie das neue WLAN-Kennwort ein.
  - **Repeater zur Signalverstärkung:** Stellen Sie die Verbindung laut Herstellerbeschreibung oder über die WPS-Taste wieder her.
  - **Smartphone mit Android/iPhone:** Rufen Sie die WLAN-Einstellungen auf, wählen Sie das WLAN aus und geben Sie den Netzwerkschlüssel ein.
7. Lässt sich ein älterer PC, ein älteres Tablet oder Smartphone nach den Änderungen nicht mehr mit dem WLAN verbinden, unterstützt es vermutlich nur die veraltete, unsichere WEP-Verschlüsselung. Sie sollten das Gerät gegen ein aktuelles Modell austauschen. Das wird wahrscheinlich auch zu einer deutlich schnelleren Verbindung im Funknetzwerk führen.

### Check 3: Überprüfen Sie MAC- und andere Filter


Lassen Sie nur die Geräte in Ihr WLAN-Funknetzwerk, die Sie kennen und denen Sie vertrauen. So schließen Sie Hacker und spionierende Geräte aus.

Die Zugangskontrolle nehmen Sie über die Gerätenamen und im Zweifel über die MAC-Adresse der Geräte vor. Diese Media-Access-Control-Adresse wird wie die Nummer Ihres Personalausweises weltweit für jedes Gerät nur einmal vergeben. Jedes Gerät lässt sich also über seine MAC-Adresse eindeutig erkennen und nötigenfalls aussperren.



**Hinweis:** Professionelle Hacker können die MAC-Adresse ihrer PCs über spezielle Tools ändern (MAC-Spoofing) und ihnen die MAC-Adresse eines anderen Geräts in Ihrem WLAN-Funknetzwerk zuweisen. Bricht häufiger die Internetverbindung eines Ihrer Geräte ab, ist das daher ein Alarmsignal. Doch keine Sorge: Zum Schutz vor den Nachbarskindern und deren Eltern reicht ein MAC-Filter vollkommen aus. Angriffe über eine vorgetäuschte MAC-Adresse kommen bei Privatpersonen nur sehr selten vor.

### Schritt 1: Richten Sie eine WLAN-Zugangsbeschränkung ein

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).

2. Wählen Sie **WLAN** und dann **Funknetz**. Sie erhalten die Liste der mit Ihrem WLAN-Funknetz verbundenen Geräte angezeigt.
3. Trennen Sie die Verbindung zu unbekannten Geräten, die Sie nicht vom Namen oder der MAC-Adresse her identifizieren können. Dazu klicken Sie bei der FRITZ!Box ganz einfach auf das **Löschen**-Symbol  am Ende des Geräteeintrags.
4. Damit sich neue Geräte nicht noch einmal unbefugt anmelden, wechseln Sie unterhalb von **WLAN** in **Sicherheit** und aktivieren die Option **WLAN-Zugang auf die bekannten WLAN-Geräte beschränken**.

### Schritt 2: Finden Sie die MAC-Adressen Ihrer Geräte

**Windows-PCs:** Öffnen Sie mit  + **R** das **Ausführen**-Fenster, geben Sie **cmd** ein und klicken Sie auf **OK**. An der Eingabeaufforderung geben Sie **ipconfig /all** ein, drücken die Eingabetaste  und lesen hinter **Physikalische Adresse** die MAC-Adresse des PCs ab.

**Android-Smartphone oder -Tablet:** Ziehen Sie die Benachrichtigungsleiste (Schnellstartleiste) herunter und tippen Sie auf das **Zahnrad**-Symbol (Einstellungen). Oder sagen Sie einfach **OK Google – Öffne Einstellungen**. Dann kommt **Geräteinformationen** bzw. **Telefoninfo** und Sie wählen **Status**. Im nächsten Bildschirm finden Sie die **MAC-Adresse**.


Alternativ tippen Sie je nach Hersteller und Android-Version bei aktivem Homescreen (der Desktop von Android-Mobilgeräten) auf die **Menü**-Taste und wählen **Systemeinstellungen**. Dann tippen Sie auf **Telefoninfo**, **Hardware-Information**, **Über das Telefon** oder **Über das Tablet** und auf **Status**. Lesen Sie die MAC-Adresse unter **WLAN/WiFi.MAC-Adresse** ab.

**iPhone, iPad von Apple:** Wählen Sie **Einstellungen**, **Allgemein** und **Info**. Blättern Sie nach unten und lesen Sie die MAC-Adresse hinter **WLAN-Adresse** ab.

**Andere Geräte:** Weil die MAC-Adresse fest einem Gerät zugeordnet ist, steht sie meist auf einem Aufkleber an der Geräterückseite. Sie finden sie so zum Beispiel bei Ihrem Router, Repeater oder internetfähigem Smart-TV. Schauen Sie ansonsten in die Bedienungsanleitung oder fragen Sie beim Hersteller-Support nach. Für die MAC-Adresse eines Samsung-Fernsehers drücken Sie zum Beispiel auf die **Menü**-Taste der **Fernbedienung**, wählen **Netzwerk** und **Netzwerkstatus**.

### Schritt 3: Melden Sie neue Geräte über deren MAC-Adresse an

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Wählen Sie **WLAN** und **Sicherheit**.
3. Klicken Sie auf **WLAN-Gerät hinzufügen**, geben Sie die **MAC-Adresse** des Geräts ein und klicken Sie auf **OK**.
4. Damit Sie das Gerät in der Funknetzliste leicht erkennen, geben Sie ihm einen sprechenden Namen. Dazu

wählen Sie **WLAN** sowie **Funknetz** und suchen das neue Gerät über seine MAC-Adresse in der Liste. Dann klicken Sie auf die **Bearbeiten**-Schaltfläche  und ändern den voreingestellten Namen wie **android-9b9063e9e3ac1332** zum Beispiel um in **Mein Android-Telefon**.

### Schritt 4: Stellen Sie weitere neue Sicherheitsfilter ein

Aktuelle Router bieten Ihnen neue Sicherheitsfunktionen. Sie können zum Beispiel über eine **Kindersicherung** den **Gastzugang** (siehe Seite 7) einschränken, durch **Listen** erlaubte und auch gesperrte Internetseiten (Whitelist und Blacklist) festlegen und globale Filter aktivieren. Stellen Sie die folgenden 3 Sicherheitsfilter wie folgt perfekt ein:

- **Firewall im Stealth-Mode:** Erhöht den Schutz vor Port-Scans. Das sind Anfragen nach offenen Ports (Schnittstellen), über die Kriminelle auf Ihren PC zugreifen. Sie sollten den Filter testweise aktivieren, um die Sicherheit zu erhöhen. Kommt es bei vertrauenswürdigen Anwendungen zu Fehlern, deaktivieren Sie diesen Filter wieder, denn er kann zu Kompatibilitätsproblemen führen.
- **E-Mail-Filter über Port 25 aktiv:** Verhindert den Missbrauch Ihres **Internetzugangs** durch Würmer. Das sind Schadprogramme, die über den ungesicherten Port 25 massenhaft E-Mails verschicken. Aktivieren Sie diesen Filter. Kommt es anschließend bei Ihrem E-Mail-Programm zu Fehlern, deaktivieren Sie diesen Filter wieder. Er ist dann zu Ihrem E-Mail-Programm nicht kompatibel.
- **Torodo-Filter:** Dieser Filter ist bei der FRITZ!Box voreingestellt aktiv und sollte auch aktiv bleiben, solange Ihr Internetanbieter die Internetverbindung mit IPv4 verwendet. Ist Ihr Internetanbieter bereits auf IPv6 umgestiegen, kann der Torodo-Filter deaktiviert werden.

### Nutzen Sie keine FRITZ!Box? Wie Sie neue Geräte bei anderen Routern über die MAC-Liste hinzufügen

Haben Sie keine FRITZ!Box, suchen Sie bei Ihrem Router nach einer der folgenden Menüoptionen: **Access-Control List (ACL)**, **MAC-Adress-Filterung**, **MAC-Filterliste**, **Wireless-Zugriffsliste**, **Zugriffsliste** oder **Zugriffssteuerung**. Das folgende Beispiel zeigt Ihnen das Einrichten der Zugangsbeschränkung bei einem der weitverbreiteten Netgear-Router:

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Wählen Sie **WLAN-Konfiguration** und **Zugriffsliste anpassen**.
3. Setzen Sie einen Haken bei **Zugriffssteuerung aktivieren**.
4. Klicken Sie auf **Hinzufügen** und tragen Sie einen Namen für das Gerät und dessen MAC-Adresse ein.
5. Eingabefehler korrigieren Sie mit **Bearbeiten**.
6. Nachdem Sie alle Geräte eingetragen haben, speichern Sie die MAC-Zugangsliste mit **Übernehmen** ab.



## Sicherheits-Check 5: Können Hacker per WPS auf Ihr Netzwerk zugreifen?

Schauen Sie nach, ob Sie bei Ihrem Router eine Taste mit der Beschriftung **WPS (WiFi Protected Setup)** finden oder **WPS** im Router-Handbuch erwähnt wird. Mit WPS lassen sich ganz einfach neue Geräte in Ihr WLAN-Funknetz aufnehmen. Sie müssen dazu nur innerhalb von ein paar Minuten an beiden Geräten die WPS-Taste drücken oder einen achtstelligen Zugangscode (WPS-PIN) eingeben. Der WPS-Code lässt sich allerdings mit speziellen Hacker-Tools knacken. Diese Programme probieren zunächst die häufigsten Zugangscodes aus und dann nacheinander alle möglichen Zugangscodes (**Brute-Force-Angriff**). Dafür brauchen sie nur Minuten. Schließen Sie daher diese Sicherheitslücke.

Deaktivieren Sie WPS bei Ihrem Router und schalten Sie es nur bei Bedarf vorübergehend ein, wenn Sie ein neues Gerät in Ihrem WLAN-Funknetz anmelden möchten:

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Bei einer FRITZ!Box gelangen Sie über **WLAN** und **Sicherheit** zur WPS-Einstellung. Verwenden Sie einen anderen Router, schauen Sie im Handbuch nach.
3. Öffnen Sie das Register **WPS-Schnellverbindung**. Haben Sie den Namen Ihres WLAN-Funknetzes versteckt (siehe Seite 5), wird WPS bei einer aktuellen FRITZ!Box bereits deaktiviert sein. Sie brauchen nichts weiter unternehmen und können direkt zu Sicherheits-Check 6 gehen.

4. Sofern vorhanden entfernen Sie den Haken vor der Option **WPS aktiv** und klicken auf **Übernehmen**.



**Mein Tipp:** Möchten Sie die WPS-Taste aktiv lassen, aktivieren Sie **Push-Button-Methode (WPS-PBC, Push Button Configuration)**.

Hacker können jetzt die WPS-Zugangscode nicht mehr zum Einbruch in Ihr Funknetz verwenden. Ihnen steht die WPS-Taste aber weiter für das einfache Hinzufügen von Geräten zur Verfügung. Bedenken Sie jedoch, dass sich ein Besucher oder Einbrecher über die WPS-Taste unrechtmäßig mit einem Gerät bei Ihrem WLAN-Funknetz anmelden könnte.

## Sicherheits-Check 6: Lassen Sie zu, dass Kriminelle Ihren Router fernsteuern?

Die Router-Hersteller preisen in ihrer Werbung den Zugriff über das Internet mit einem Smartphone (Mobiltelefon mit der Leistung eines Desktop-PCs) als tolle Zusatzfunktion an. Doch in solchen Fernsteuerungsfunktionen wurden wiederholt gefährliche Sicherheitslücken gefunden. Kontrollieren Sie daher die Sicherheit des Internetkennworts oder schalten Sie den Internetzugriff komplett aus. In nur 4 Schritten sind Sie am Ziel.

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Wählen Sie **Internet** und **MyFRITZ!-Konto** bei einer FRITZ!Box. Der Hersteller AVM bietet über einen MyFRITZ!-Server im Internet den Zugriff auf den Anrufbeantworter, die Anrufliste sowie das FRITZ!NAS an. Das ist ein optionales Netzwerklaufwerk, das Sie über das Internet auch als Online-Speicher nutzen können. Dazu stecken Sie einfach einen USB-Stick oder ein USB-Laufwerk an und haben Zugriff auf die dort abgespeicherten Daten.
3. Überprüfen Sie, ob ein Internetzugang bei Ihrem Router aktiviert ist. Im Fall der FRITZ!Box sehen Sie

dann einen Haken bei der Option **MyFRITZ! für diese FRITZ!Box aktiv** oder der Option **Internetzugriff auf die FRITZ!Box über HTTPS aktiviert**. Entfernen Sie die Haken bei diesen Optionen, sofern Sie die Funktion nicht unbedingt benötigen.

4. Benötigen Sie den Internetzugang, sollte Ihr MyFRITZ!-Konto durch ein sicheres Kennwort geschützt sein. Das Kennwort sollte also mindestens 16 Zeichen lang sein, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erfüllt Ihr Kennwort diese Anforderungen nicht, melden Sie sich bei Ihrem MyFRITZ!-Konto an und ändern das Kennwort.

### Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299  
Dieses monothematische Supplement  
„Ihr Leitfadens für eine sichere Internet-Verbindung  
und Router-Schutz“ gehört zu dem Titel  
„Ihr PC-Sicherheits-Berater“.  
Computerwissen, ein Verlagsbereich der  
VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop  
Chefredakteur: Michael-Alexander Beisecker  
(V.i.S.d.P.), Oberhausen  
Herausgeberin: Patricia Sparacio  
Adresse: Verlag für die Deutsche Wirtschaft AG,  
Theodor-Heuss-Str. 2-4, 53177 Bonn  
Telefon: 0228/9550190, Fax: 0228/3696350

Eingetragen: Amtsgericht Bonn HRB 8165  
Die Beiträge in „Ihr PC-Sicherheits-Berater“ wurden mit  
Sorgfalt recherchiert und überprüft. Sie basieren jedoch  
auf der Richtigkeit uns erteilter Auskünfte und unterliegen  
Veränderungen. Daher ist eine Haftung, auch für telefonische  
Auskünfte, ausgeschlossen. Vervielfältigungen jeder Art sind  
nur mit Genehmigung des Verlags gestattet.  
© Copyright 2019 by Verlag für die Deutsche Wirtschaft AG;  
Bonn, Bukarest, Manchester, Warschau



## Sicherheits-Check 7: Haben Besucher vollen Zugriff auf Router und Internet?

Besucher erwarten heute schon fast selbstverständlich, dass Sie ihnen einen Zugang zu Ihrem WLAN-Funknetz gewähren. Das ist jedoch ein erhebliches Sicherheitsrisiko. Ihre Gäste könnten gefährliche Internetseiten aufrufen, Ihre Rechner mit Schadprogrammen verseuchen oder gar illegale Downloads durchführen.

**Der beste Schutz vor diesen Gefahren:**

**Richten Sie einen Gastzugang in Ihrem Router ein**

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Wählen Sie **WLAN** und **Gastzugang**. Sind diese Optionen bei Ihrem Router nicht vorhanden, schauen Sie im Handbuch nach, ob Ihr Router einen Gastzugang unterstützt und wie die entsprechenden Optionen lauten.
3. Setzen Sie einen Haken bei **Gastzugang aktiv** und tragen Sie bei **Name des Gastfunknetzes (SSID)** einen Namen ein.
4. Wählen Sie die **Verschlüsselung**. Ich empfehle hier **WPA + WPA2**.
5. Tragen Sie einen sicheren Netzwerkschlüssel mit einer Länge von mindestens 20 Zeichen ein, der aus

Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen besteht.

6. Wählen Sie die gewünschten Optionen aus. Sie können zum Beispiel die Internetnutzung auf Surfen und Mailen beschränken. Sie haben also auch als Privatanwender eine umfassende Kontrolle, so wie in einem Internetcafé.
7. Nachdem Sie alle Einstellungen vorgenommen haben, klicken Sie auf **Übernehmen**.



**Mein Tipp:** Klicken Sie auf **Info-Blatt drucken** und Sie erhalten eine Information für Ihre Gäste mit dem Namen Ihres WLAN-Funknetzes und dem WLAN-Netzwerkschlüssel, Ihre Gäste werden das sicher als tollen Service empfinden.

## Für Ihre schnelle, tägliche Kontrolle: Alle Anmeldungen und Sicherheitseinstellungen auf einen Blick

Sicherheit ist wichtig, aber die sieben Sicherheits-Checks sind Ihnen womöglich nach einiger Zeit zu aufwendig und Sie suchen nach einer schnellen Lösung. Es gibt beim aktuellen FRITZ!Box-Betriebssystem zwei sehr wichtige Funktionen, die Sie unbedingt kennen und nutzen sollten. Sie kontrollieren damit nicht nur schnell und einfach Ihre Einstellungen, sondern auch deren Wirksamkeit. Nutzt jemand heimlich Ihre Internetverbindung, fällt das sofort auf, denn Ihr Router protokolliert alles mit.

Ich überprüfe einmal pro Woche, welche Anmeldungen und sonstigen Ereignisse bei meiner FRITZ!Box stattgefunden haben. Das empfehle ich auch Ihnen, um Missbrauch auf die Spur zu kommen.

**Hat jemand illegal Ihre Internetverbindung genutzt?**

In wenigen Sekunden haben Sie die Antwort:

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).
2. Wählen Sie **System** und **Ereignisse**.
3. Prüfen Sie zuerst, ob die Liste seit Ihrem letzten Besuch lückenlos weitergeführt wurde. Ein Hacker könnte nämlich auf **Liste löschen** klicken und damit würden seine Aktivitäten fehlen.
4. Gehen Sie die Liste der Geräteanmeldungen und die Uhrzeiten durch. Haben sich unbekannte Geräte angemeldet? Sind Anmeldungen zu ungewöhnlichen Zeiten erfolgt, wie zum Beispiel mitten in der Nacht?

**Stimmen noch alle Sicherheitseinstellungen?**

1. Melden Sie sich bei Ihrem Router an (siehe Seite 2).

2. Wählen Sie **Diagnose** und **Sicherheit**.

3. Blättern Sie durch die Übersicht und prüfen Sie, ob das Betriebssystem noch aktuell ist und alle Einstellungen Ihren Wünschen entsprechen.

**Schutz vor einer hohen Telefonrechnung**

Zum Schutz vor einer hohen Telefonrechnung durch einen Router-Hack (siehe Seite 1) sperren Sie zum Beispiel Telefonate ins Ausland:

1. Wählen Sie **Diagnose** und **Sicherheit**.
2. Blättern Sie nach unten bis zu **Rufbehandlung** und klicken Sie hinter **Telefonate ins Ausland** auf **Bearbeiten** und dann auf **Neue Rufsperr**.
3. Bei **Rufart wählen** aktivieren Sie die Option **Ausgehende Rufe** und stellen **Ausland** bei **Bereich** ein. Speichern Sie die neue Einstellung mit **OK** ab.

Ihr Router wählt nun keine Auslandsgespräche mehr an. Sie können auch weitere Rufsperrn für **Auskunft** und **Sonderrufnummern** einstellen, damit diese teuren Rufnummern nicht angewählt werden können.