E. F. Engelhardt

Know-how ist blau.

3. aktualisierte und erweiterte Auflage

Das große inoffizielle FRITZ!Box Handbuch

> WLAN-Tuning: Mehr Leistung, höhere Geschwindigkeit, verbesserte Sicherheit

> Heimnetzwerk im Griff: Netzwerkfestplatte, Powerline-Verbindung, VPN

> Mobile Geräte einbinden: iPhone, iPad, Android

FRANZIS

E. F. Engelhardt

Das große inoffizielle FRITZ!Box Handbuch

E. F. Engelhardt

3. aktualisierte und erweiterte Auflage

Das große inoffizielle FRITZ!Box Handbuch

Mit 336 Abbildungen

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Lektorat: Anton Schmid
Satz: DTP-Satz A. Kugge, München
art & design: www.ideehoch2.de
Druck: Bercker, 47623 Kevelaer
Printed in Germany

ISBN 978-3-645-60150-4

Vorwort

Wer heute einen DSL-Zugang bestellt, erhält in der Regel ein Kombigerät mit DSL-Modem und WLAN-Router, um sofort loslegen zu können. Meist lässt sich auch innerhalb weniger Minuten das WLAN installieren und in Betrieb nehmen – mit dem entsprechenden Gerät lässt sich dann auf Knopfdruck drahtlos surfen. Der Kalauer »Mobilität hat ihren Preis« aus der Automobilindustrie gilt jedoch auch hier in der IT: So stehen an jeder Straßenecke zig Funknetze zur Verfügung. Allerdings steigt mit zunehmender Funknetzdichte auch die Gefahr bzw. das Risiko entsprechend prozentual an, ein potenzielles Ziel für Angriffe von außen zu werden.

Gerade wenn Sie viele wichtige Daten auf Ihrem privaten Computer oder auf einer Netzwerkfestplatte zu Hause speichern, sollten Sie sich Gedanken um die Sicherheit Ihrer FRITZ!Box und deren Konfiguration machen. Wer sie nicht entsprechend eingerichtet hat, wird leicht Opfer von Spionen oder Angreifern, die Lust am Zerstören haben. Mit den grundlegenden Kenntnissen in Sachen FRITZ!Box-Konfiguration schotten Sie Ihr Heimnetz ab.

Dieses Buch bietet dafür alles, was Sie brauchen, und zeigt Wege, wie Sie Ihre FRITZ!Box mit inoffiziellen Eingriffen erweitern können. Mithilfe ausführlicher Anleitungen stellt das Aufspielen einer inoffiziellen Firmware kein Problem mehr dar. Oder möchten Sie sich über das Internet mit Ihrem Heimnetz verbinden, ohne Ängste in Sachen Mitleser und Datendiebstahl zu haben? Dann finden Sie in diesem Buch etliche Tipps und Tricks für die Konfiguration einer VPN-Verbindung, die zeigen, wie Sie mit Hausmittelchen sicher Daten austauschen können.

Ich wünsche Ihnen ganz viel Spaß mit und vor allem viel Nutzen aus diesem Buch.

E. F. Engelhardt, München im Oktober 2011

Sie haben Anregungen, Fragen, Lob oder Kritik zu diesem Buch? Sie erreichen den Autor per Mail unter *ef.engelhardt@gmx.de*.

Inhaltsverzeichnis

1 FRITZ!Box und WLAN einrichten

Wer in Sachen Netzwerke einigermaßen fit ist und auf ausführliche Erklärungen verzichten möchte, kann die Checkliste für die sichere Konfiguration des WLAN-Routers im Kapitel »FRITZ!Box-Sicherheitseinstellungen« nutzen. Alle anderen kommen mit den jetzt beschriebenen Erläuterungen aber ganz sicher zum Ziel, denn der Grundaufbau ist narrensicher. Knifflig wird's erst später, aber das meistern Sie locker. Auch die wesentlichen Sicherheitsaspekte werden Schritt für Schritt erläutert.

1.1 FRITZ!Box und WLAN startklar machen

Wenn Sie also noch kein drahtloses Netzwerk eingerichtet haben, sollten Sie dieses Kapitel von Anfang bis Ende systematisch nachvollziehen. Danach geht es dann an die Einbindung kabelloser Rechner und die komplette Absicherung.

1.1.1 FRITZ!Box und Computer verbinden

Für die Verbindung zwischen FRITZ!Box und Computer, die Sie benötigen, um den Router einzurichten, gibt es zwei Möglichkeiten:

- die Verbindung per Kreuzkabel (Netzwerkkabel) oder
- die WLAN-Verbindung über einen WLAN-Adapter.

In den meisten Fällen wird ein vorhandener stationärer PC an den Router angeschlossen, für Notebooks wird dann ein WLAN für den Internetzugang und gegebenenfalls die gemeinsame Nutzung von Druckern und Dateien bereitgestellt.

Die meisten aktuellen Desktop-PCs verfügen bereits ab Werk über einen Netzwerkanschluss. Besitzt Ihr PC keinen, müssen Sie eine entsprechende Netzwerkkarte nachrüsten. Sie können aber auch direkt auf WLAN setzen und den PC über einen USB-WLAN-Adapter mit dem Router verbinden.

Bild 1.1: Gruppenfoto der FRITZ!WLAN-USB-Stick-Familie. Der FRITZ!WLAN-USB-Stick N 2.4 (Mitte) unterstützt WLAN N im 2,4-GHz-Frequenzbereich und erreicht Übertragungsraten bis zu 150 MBit/s. Er ergänzt die beiden Modelle FRITZ!WLAN-USB-Stick N (links) und FRITZ!WLAN-USB-Stick (rechts). (Foto: AVM)

In vielen Fällen wird die Steckkarte nicht die erste Wahl sein, denn dafür müssen Sie den PC öffnen und sich sowohl mit den internen Steckplätzen als auch mit der Installation von solchen Karten ein wenig auskennen. Bei den PCs der letzten fünf Jahre ist der Netzwerkanschluss bereits auf der Hauptplatine integriert und von hinten als Buchse zugänglich.

Achten Sie darauf, Router und PC mit dem Kabel zu verbinden, das Sie beim Kauf des Routers mit dazubekommen haben. Oft sind diese Kabel farbcodiert und werden in der Anleitung genau beschrieben. Erst wenn die Verbindung mit dem richtigen Kabel steht, schalten Sie Router und PC ein.

1.1.2 Erste Anmeldung an der FRITZ!Box

Für die erstmalige Anmeldung an der FRITZ!Box bekommt die Netzwerkschnittstelle per DHCP automatisch eine IP-Adresse zugewiesen. Ist das nicht der Fall, stellen Sie sie auf DHCP um. Danach kommen Sie ganz einfach über den Webbrowser in das Konfigurationsmenü des WLAN-Routers. Starten Sie dazu den Browser. Die Konfigurationsadresse, unabhängig von Herstellungsjahr und Modell, ist bei der FRITZ!Box immer:

```
http://fritz.box
```

oder

```
http://192.168.178.1
```

Frisch aus der Verpackung haben die FRITZ!Box-Modelle keinen vernünftigen Passwortschutz. Oftmals hat der Provider hier den WLAN-Schlüssel als Konfigurationspasswort gesetzt. Sind Sie auf der Konfigurationsseite der FRITZ!Box, wird dieser Schutz aus Sicherheitsgründen aktiviert und ein persönliches Passwort verwendet – allerspätestens nach dem Abschluss der Konfiguration sollten Sie es jedoch einstellen.

Bild 1.2: Aber sicher: Ein vernünftiger WLAN-Router sichert die Konfiguration per Zugangskennung ab.

Wenn keine Verbindung zum Router zustande kommt, sollten Sie folgendermaßen vorgehen:

- Zunächst untersuchen Sie die Stromversorgung der FRITZ!Box – Stecker am Netz? Prüfen Sie die Position und den Sitz des Netzwerksteckers. Da bei älteren Modellen die Buchse für das Kabel zum DSL-Splitter und die Buchse für den ersten Netzwerkrechner nebeneinanderliegen, kann man sich da leicht vertun.
- Anschließend prüfen Sie die eingegebene IP-Adresse noch einmal auf Vertipper. Ist kein Schreibfehler zu sehen, heißt es, die Adresse erneut mit der Angabe im Handbuch abzugleichen.
- Ist das Netzwerkkabel an Ihrem Rechner fest eingesteckt, und handelt es sich wirklich um die Netzwerkschnittstelle? Haben Sie das richtige Kabel verwendet? Meist sind die Kabel farbcodiert.

Ist alles in Ordnung, sollte die FRITZ!Box nicht nur laufen, sondern auch auf die Kontaktaufnahme des Computers reagieren. Es gibt ganz seltene Fälle, in denen ein Kabel defekt ist. Bei fabrikneuen Geräten kann man das meist ausschließen, aber es kommt dennoch vor. Es ist also noch Testpotenzial vorhanden. Wir gehen aber davon aus, dass bei Ihnen alles läuft.

1.1.3 Basiseinstellungen per Einrichtungsassistent

Ist der WLAN-Router in Ihrem Netzwerk angeschlossen, muss er konfiguriert werden. Abhängig vom Router-Modell stehen dafür verschiedene Möglichkeiten zur Verfügung. Die FRITZ!Box prüft unmittelbar nach dem erstmaligen Einstecken die Netzwerkumgebung. Hier werden sämtliche angeschlossenen Geräte sowie die Internetverbindung geprüft und, falls möglich, gleich konfiguriert. Zunächst ermittelt die FRITZ!Box, ob sie ordnungsgemäß an einem DSL-Splitter angeschlossen ist. Ist das der Fall, leitet ein Assistent durch die Erstinstallation.

Bild 1.3: Ist die FRITZ!Box noch nicht konfiguriert, bieten Einrichtungsassistenten an, das nach dem Einschalten vorzunehmen.

Für Einsteiger empfiehlt es sich, die Arbeit vom Setup-Assistenten übernehmen zu lassen, gerade wenn man keine Übung darin hat, selbst eine Internetverbindung einzurichten. Sicherer und für Fortgeschrittene empfehlenswert ist jedoch eine manuelle Konfiguration des Geräts.

Wer die Internetverbindung also selbst konfigurieren möchte, wählt bei der FRITZ!Box auf der Startseite der Weboberfläche den Punkt *Einrichtungsassistent* aus, der Schritt für Schritt die für eine Internetverbindung notwendigen Einstellungen abfragt. Hier brauchen Sie selbstverständlich die passenden Installations- und Konfigurationsparameter sowie den Benutzernamen und das Passwort aus den Zugangsunterlagen des Internet Service Provider.

1.1.4 Vorgegebenes Kennwort sofort ändern

Nach dem Auspacken, Aufstellen und Konfigurieren sichern Sie die FRITZ!Box gegen unerwünschte Veränderungen mit einem eigenen Passwort ab. Denn es wäre ärgerlich, wenn all Ihre Mühe umsonst ist, weil ein Spaßvogel im Heimnetz auf die FRITZ!Box zugreifen und die Einstellungen verändern kann. Im Zweifelsfall kämen Sie selbst nicht mehr hinein.

Bild 1.4: Über das Menü *System/FRITZ!Box-Kennwort* ändern Sie das aktuelle Kennwort in ein neues.

Die FRITZ!Box lässt sich nach Abschluss der Konfiguration mit einem Passwort absichern. Über den Webbrowser erreichen Sie per *System/FRITZ!Box-Kennwort* den entsprechenden Dialog. Am besten notieren Sie sich das Kennwort und bewahren es an einem sicheren Ort auf.

Ersteinrichtung per Kabelverbindung
Auch wenn Sie mit einem Notebook und WLAN arbeiten möchten, empfiehlt es sich, die Ersteinrichtung über den Netzwerkanschluss und nicht über das WLAN durchzuführen. Zum Start ist das WLAN auch hier noch nicht optimal gesichert – Sie sollten die Kabelverbindung vorziehen.

1.1.5 Standardeinstellungen manuell anpassen

Beim erstmaligen Einrichten des Routers können Sie möglicherweise die Standardeinstellungen ohne Änderungen übernehmen. Haben Sie bereits ein Heimnetz eingerichtet und der DSL-Router wird nachträglich ins Heimnetz integriert, ist ein Anpassen verschiedener Einstellungen notwendig. Orientieren Sie sich einfach an folgenden Schritten:

1. Die Konfiguration der Internetzugangsdaten nehmen Sie im Menü *Internet/Zugangsdaten* vor. Hier geben Sie den Konto-/Benutzernamen ein. Falls Ihr Internetanbieter Ihnen einen bestimmten Hostnamen mitgeteilt hat (z. B. *X00132454*), geben Sie den hier an. Bei T-Online beispielsweise setzt sich der Log-in-Name aus zwei wesentlichen Komponenten zusammen – der geheimen Anschluss- und der Benutzerkennung, die jeweils aus zwölf Stellen bestehen. Achten Sie deshalb bei der Konfiguration auf die Reihenfolge Anschlusskennung + T-Online-Nummer + (#) Mitbenutzersuffix + @t-online.de. Ein möglicher Benutzername wäre demnach *111111111111222222222220001@t-online.de*.

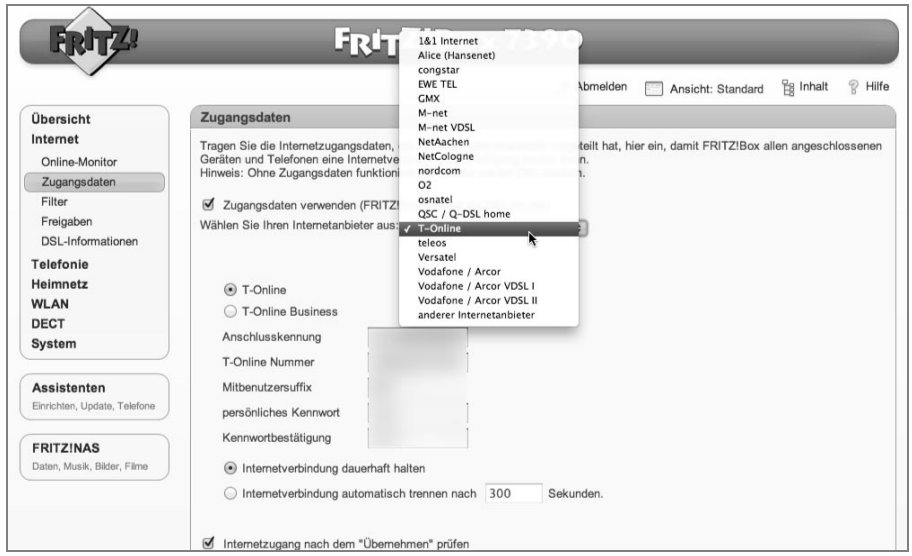

Bild 1.5: Hier wählen Sie zunächst den Anbieter aus dem Drop-down-Menü aus. Ist der gewünschte nicht dabei, wählen Sie die Option *anderer Internetanbieter*.

2. Für eine Verbindung ins Internet benötigt die FRITZ!Box eine IP-Adresse. Stellt die FRITZ!Box eine Verbindung zu Ihrem Internetanbieter her, bezieht sie automatisch eine IP-Adresse, die aus einem Adresspool des Internetanbieters zur Verfügung gestellt wird. Nur wenige Internetanbieter vergeben eine feste (oder statische) IP-Adresse – falls Sie eine solche haben, hat Ihnen der ISP die erforderlichen Informationen in den Unterlagen mitgegeben. In diesem Fall wählen Sie *Statische IP-Adresse verwenden* aus und tragen die IP-Adresse, die Subnetzmaske sowie die Gateway-IP-Adresse in die entsprechenden Felder ein. Bei der Internetkonfiguration der FRITZ!Box wählen Sie dafür im Bereich *Zugangsdaten* nicht die Option *Internetzugang über DSL*, sondern den Punkt *Internetzugang über LAN 1* aus. Anschließend lassen sich die vom ISP angegebenen IP-Adressparameter eintragen.

Bild 1.6: Internetzugang über DSL oder LAN 1.

3. Je nach FRITZ!Box-Modell richten Sie nun den DNS-Server ein. Dieser wird zur Suche von Webadressen basierend auf ihren Namen verwendet und löst den DNS-

Namen in einer IP-Adresse auf. Stehen in den ISP-Unterlagen ein oder zwei DNS-Serveradressen, tragen Sie einfach die primäre und die sekundäre Adresse im Konfigurationsdialog ein. In der Regel reicht der Eintrag *Automatisch vom ISP abrufen*, wenn der ISP den DNS-Server automatisiert zur Verfügung stellt. Näheres dazu finden Sie in Ihren Unterlagen zum DSL-Zugang.

Bei den meisten Modellen der FRITZ!Box ist das Konfigurieren der DNS-Serveradressen des ISP standardmäßig nicht möglich. Möchten oder müssen Sie mit dem PC dennoch einen anderen DNS-Server verwenden, muss bei der IP-Konfiguration des PCs die entsprechende IP-Adresse des gewünschten DNS-Servers eingetragen werden. Hier wählen Sie über die Systemsteuerung bei *Netzwerkverbindungen* die Schnittstelle aus, die für den Internetzugang sorgt, und klicken dort auf *Eigenschaften*. Im Register *Allgemein* ist das TCP/IP-Protokoll zu finden – dort klicken Sie abermals auf *Eigenschaften*. Nun können Sie den Punkt *DNS-Adressen automatisch beziehen* auf *Folgende DNS-Serveradressen verwenden* umstellen und dort die IP-Adresse des gewünschten DNS-Servers eintragen. Nach dem Neustart des PCs sind diese Netzwerkeinstellungen aktiv, und der in der FRITZ!Box eingetragene DNS-Server wird vom PC nicht mehr verwendet.

4. Im nächsten Schritt wird gegebenenfalls die MAC-Adresse der FRITZ!Box konfiguriert. Eine MAC-Adresse (*Media Access Control*) ist eine eindeutige Hardwareadresse in einem Netzwerk und sorgt für zusätzliche Sicherheit beim Verbindungsaufbau, weil jeder Netzwerkkomponente eine eindeutige Adresse zugeordnet ist (in den meisten Fällen ist das die Netzwerkkarte). Selten kommt es vor, dass ein Internetanbieter nur eine bestimmte MAC-Adresse für den Internetzugriff zulässt, mit der (und nur mit der!) eine Verbindung zustande kommen darf. Bei älteren FRITZ!Boxen ist das Ändern der MAC-Adresse nicht ohne Weiteres möglich. Zwar existiert ein Weg über eine Recovery-Konsole via FTP, doch dieser ist ausschließlich Spezialisten vorbehalten. Zu groß ist hier das Risiko, dass die FRITZ!Box nach dem Eingriff nicht mehr startet. Die MAC-Adresse der FRITZ!Box finden Sie über die Kommandozeile heraus.

```
C:\>arp -a

Schnittstelle: 192.168.123.174 --- 0x4
  Internetadresse       Physikal. Adresse     Typ
  192.168.123.21        00-14-6c-57-23-ef     dynamisch
  192.168.123.23        00-30-1b-b8-ec-4f     dynamisch
  192.168.123.38        00-17-f2-ef-f7-ca     dynamisch
  192.168.123.199       00-04-0e-14-1c-51     dynamisch

C:\>nslookup 192.168.123.199
Server:  fritz.fon.box
Address:  192.168.123.199

Name:    fritz.fon.box
Address:  192.168.123.199


C:\>
```

Bild 1.7: Mit dem Befehl *arp –a* im DOS-Fenster liefert *arp* zu jeder IP-Adresse die aktuell zugeordnete MAC-Adresse.

Bei neuen FRITZ!Box-Modellen bzw. FRITZ!Boxen mit einer aktuellen Firmware ist das Konfigurieren der MAC-Adresse etwas umständlicher gelöst. Damit Sie überhaupt an die Einstellung für die Netzwerkparameter herankommen, muss im Hauptmenü zunächst die sogenannte Expertenansicht aktiviert werden.

Bild 1.8: Die Aktivierung der Expertenansicht finden Sie im Menü *System/Ansicht*.

MAC-Adresse ändern nur mit Internetzugang über LAN 1
Das Ändern der IP- bzw. MAC-Adresse der FRITZ!Box ist jedoch nur dann möglich, wenn der Internetzugriff über die Option *Internetzugang über LAN 1* konfiguriert ist. In diesem Fall ist die FRITZ!Box an ein bereits vorhandenes Netzwerk (LAN) oder einen anderen DSL-Router angeschlossen, der die Zugangsdaten für den Provider für das Netzwerk zur Verfügung stellt.

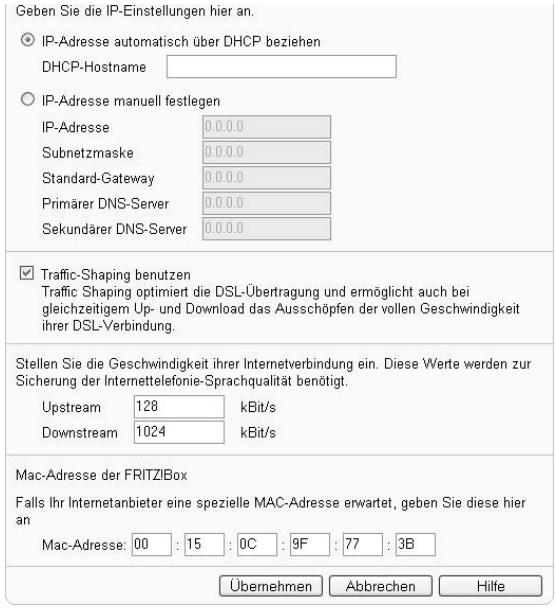

Bild 1.9: Erwartet der Internetanbieter eine spezielle MAC-Adresse für die Internetverbindung, tragen Sie diese hier ein.

1.1.6 Internetverbindung dauerhaft halten?

Internetverbindung ist nicht gleich Internetverbindung. Obwohl die meisten Komplettangebote eine Flatrate bieten, kann es sein, dass sich für manche Zwecke der Stundentarif lohnt, der nach einem bestimmten Zeittakt und Tarif zu bezahlen ist. Abhängig vom Vertrag (Flat/Stundentarif etc.) mit Ihrem Internetanbieter kann die falsche Konfiguration des DSL-Routers dann richtig Geld kosten: Ist er falsch eingestellt, hält der Router die Internetverbindung rund um die Uhr aufrecht, auch wenn kein Rechner angeschaltet ist.

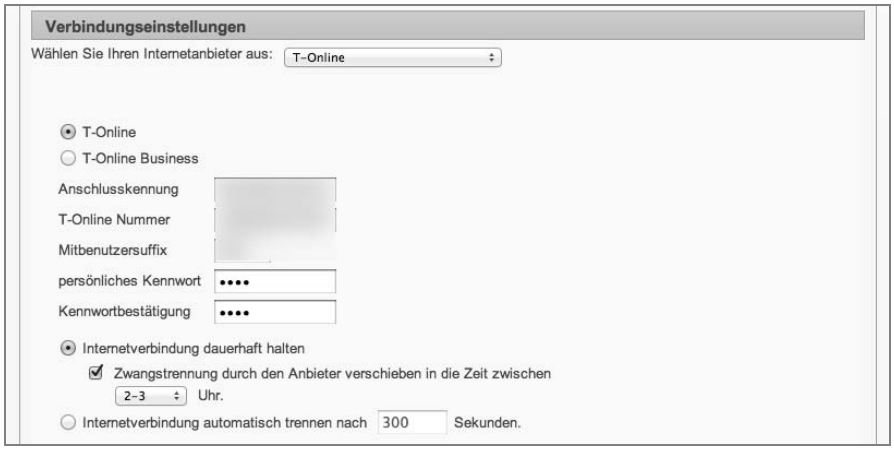

Bild 1.10: Über das Menü *Internet/Zugangsdaten* prüfen Sie in der Expertenansicht die *Verbindungseinstellungen* der FRITZ!Box.

Haben Sie eine Flatrate, kann die Option *Internetverbindung dauerhaft halten* in der Regel aktiviert bleiben. So wird die Internetverbindung nach jedem Time-out automatisch hergestellt, wenn der Router aus dem Heimnetz Verbindungswünsche mit dem Internet feststellt.

1.1.7 Funkkanalwechsel: Wenn andere Router stören

Beim Funkkanal können Sie häufig die Werkeinstellung beibehalten, es sei denn, es sind Störstrahlungen von einem anderen WLAN-Router in der Umgebung vorhanden. Dies macht sich vor allem durch Schwierigkeiten beim Verbindungsaufbau und in der Geschwindigkeit bemerkbar. Hängen in der Nachbarschaft einige andere WLAN-Router an der Steckdose, kann das Umkonfigurieren des Kanals einen Geschwindigkeitsschub bringen.

So läuft das WLAN wieder wie geschmiert
Im Konfigurationsmenü Ihres WLAN-Routers stehen Ihnen 13 Kanäle zur Verfügung. Dabei beträgt der Abstand der Mittenfrequenzen jeweils 5 MHz. Bedingt durch die große Bandbreite jedes einzelnen Funkkanals kommt es zu Überschneidungen der Frequenzbänder. Wird Ihr WLAN immer langsamer oder bricht die Verbindung ganz ab, ist das in den meisten Fällen auf eine Überschneidung mehrerer Funkkanäle zurückzuführen. Für beste Funkqualität sollten daher alle im Umkreis befindlichen WLANs mit einem Abstand von fünf Kanälen betrieben werden. Sendet Ihr Nachbar in seinem WLAN auf *Kanal 6*, wechseln Sie zu *Kanal 1*, *11*, *12* oder *13*, und Ihr WLAN läuft wieder wie geschmiert.

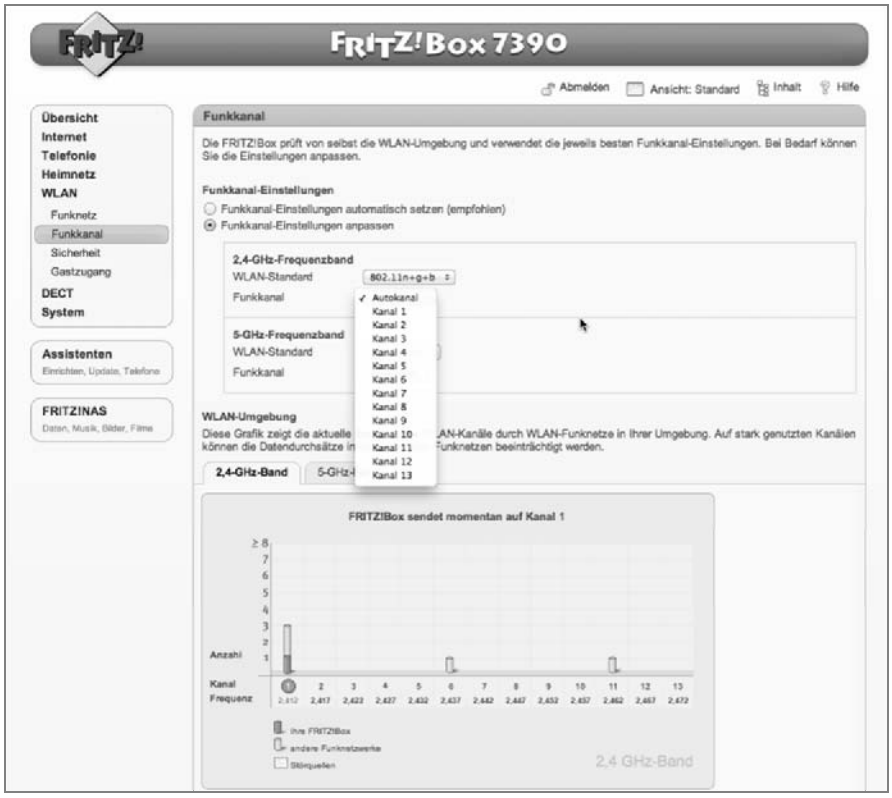

Bild 1.11: FRITZ!Box-Spezialität: Kommt es auf einem Funkkanal zu Übertragungsspitzen, wechseln Sie in diesem Dialog einfach den Kanal. Hier lassen sich die Kanäle des 2,4-GHz- und des 5-GHz-Frequenzbands getrennt konfigurieren.

Feintuning der WLAN-Geschwindigkeit: Wer keine Uraltgeräte (mit dem alten 802.11b-Standard) mehr im Einsatz hat oder haben möchte, wählt im Drop-down-Menü bei *WLAN-Standard* anstelle des Standardeintrags *802.11n+g+b* die Einstellung *802.11n+g* aus. Damit verhindern Sie, dass ältere Geräte nach dem b-Standard das WLAN-Netz auf 11 MBit/s drosseln.

1.1.8 Strom sparen mit der FRITZ!Box

Trotz Flatrate wird der Internetzugang in den wenigsten Fällen rund um die Uhr benötigt. Gerade wer die WLAN-Schnittstelle der FRITZ!Box für den Internetzugang nutzt, kann mit etwas Feinkonfiguration ein paar Kilowatt Strom sparen. Drücken Sie vor dem Zubettgehen manuell den WLAN-Schalter am FRITZ!Box-Gehäuse, haben Sie die WLAN-Funktion einfach per Knopfdruck ausgeschaltet.

Wem das zu umständlich ist, der kann dafür auch die Nachtschaltungsfunktion der FRITZ!Box nutzen, mit der sich die WLAN-Funktionen für einen definierten Zeitraum komplett ausschalten lassen. Sie aktivieren die Nachtschaltung unter *Übersicht/Erweiterte Einstellungen/System/Nachtschaltung*.

Bild 1.12: Wer nachts ruhig schlafen möchte, kann neben der *Nachtschaltung* auch per Mausklick eine nächtliche *Klingelsperre* aktivieren, die für Ruhe vor Telefonanrufen über die Anschlüsse der FRITZ!Box sorgt.

Nutzen Sie die WLAN-Funktion zudem nur in den eigenen vier Wänden – beispielsweise nur in einem Raum –, können Sie zusätzlich Strom sparen, indem Sie die Funkleistung der FRITZ!Box reduzieren. Das sorgt nicht nur für weniger Strahlung im Haus, sondern auch für weniger Störsignale in der Nachbarschaft sowie etwas mehr Schutz vor ungebetenen Eindringlingen, da die reduzierte WLAN-Funkleistung im Idealfall an der Hauswand scheitert.

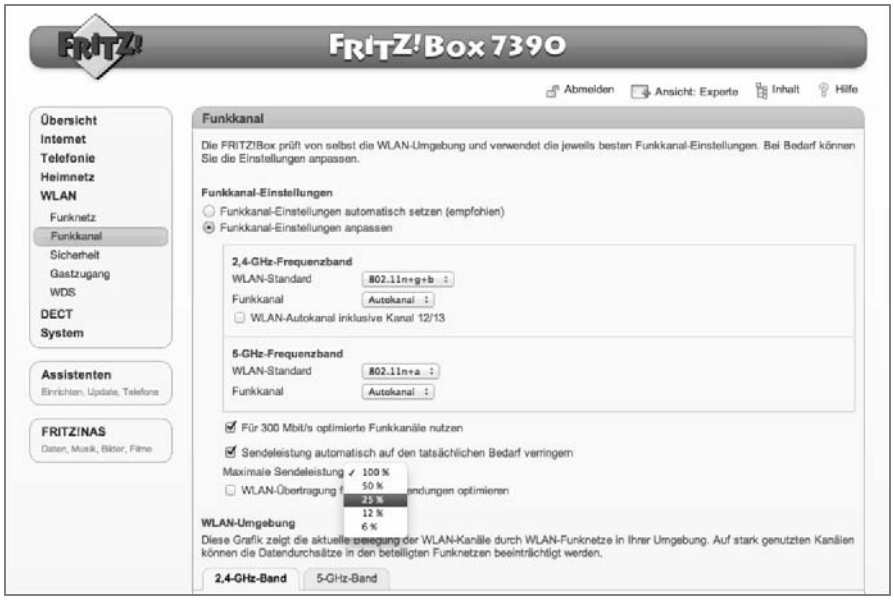

Bild 1.13: Die Hauswand als natürliche Firewall: Kommen die eingesetzten WLAN-Geräte ausschließlich in einem einzigen Raum zum Einsatz, kann die Sendeleistung automatisch auf den tatsächlichen Bedarf verringert werden.

Wird nur wenig Energie benötigt, um die Verbindung zum Internet herzustellen, wird bei aktiviertem TCP (*Transmission Power Control*) auch die Funkleistung auf die tatsächlich benötigte Energiemenge reduziert. Über die Benutzeroberfläche der FRITZ!Box stellen Sie die Funkleistung auf Ihre persönliche Umgebung zu Hause ein.

1.2 WLAN gegen Eindringlinge dicht machen

Das Aufsetzen eines drahtlosen Netzwerks ist leichter, als Sie denken. Normalerweise genügen ein Browser und die Eingabe der wichtigsten Standardeinstellungen, und dann kann es losgehen mit dem kabellosen Surfvergnügen. Doch wollen Sie auf Nummer sicher gehen, sollten Sie vorher das WLAN-Netzwerk dicht machen, damit niemand anderer als Sie selbst über das Funknetz arbeiten kann. Denn: Viele Schmarotzer können auf Ihre Kosten mitsurfen.

Haben Sie eine Flatrate, gibt es zwar bezüglich der Kosten keinen Unterschied, steht jedoch eines Tages bei Ihnen der Staatsanwalt vor der Haustür, hat ein Eindringling möglicherweise über Ihren Internetanschluss Unfug getrieben. Deshalb sollten Sie die vorhandenen Sicherheitsmechanismen des Routers nicht nur kennen, sondern auch nutzen.

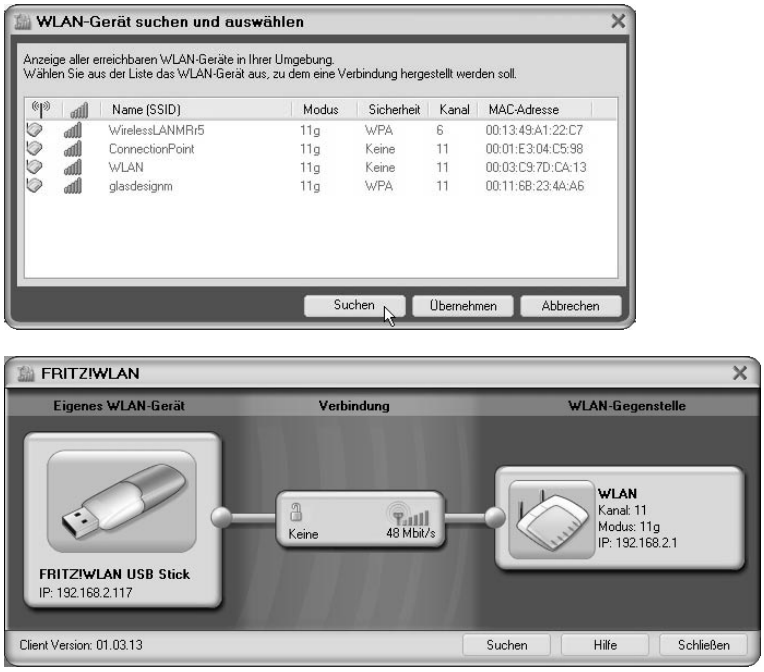

Bild 1.14: Ausprobiert: Das ungesicherte Funknetz *WLAN* kann problemlos angesprochen werden – ganz einfach mit einem USB-WLAN-Adapter.

1.2.1 Grundlage für jede Absicherung: die SSID

Das Wichtigste für eine sichere WLAN-Konfiguration ist eine sichere und unsichtbare SSID (*Service Set Identifier*). Mit der SSID ist nach Abschluss der Konfiguration das WLAN für die Umgebung sichtbar. Jeder, der sich an das Netz anmelden möchte, benötigt diesen Netzwerknamen (SSID), und sämtliche WLAN-Geräte müssen ihn kennen. Funknetze werden in der Standardeinstellung mit dieser Kennung angezeigt, die Kennung wird sozusagen mitgesendet.

Ändern Sie sofort die Standardeinstellung des Herstellers. Bei der FRITZ!Box ist im Auslieferungszustand als SSID meist der Name des Geräts eingetragen, z. B. *FRITZ!Box Fon WLAN 7390*. Der ist für potenzielle Angreifer nicht nur zu sehen, sondern bei verborgener SSID dennoch leicht zu erraten, er wird auch in den Supportforen der Hersteller für jedes Router-Modell genannt.

Ein sicherer SSID-Name besteht aus einer zufälligen Reihenfolge von Zahlen und Buchstaben, gemischt mit Groß- und Kleinbuchstaben. Möglich ist auch eine nur Ihnen bekannte Kombination aus persönlichen Daten, Namen sowie Groß- und Kleinschreibung (z. B. *MeineOmaIngridhatte3Hundeund2Katzen!*).

Konfigurieren Sie eine neue SSID und notieren Sie sich diese Kennung auf einem Zettel, der sich beim WLAN-Handbuch befindet. Die FRITZ!Box bietet Ihnen aber auch das Ausdrucken der Einstellungen an. Wer ganz auf Nummer sicher gehen möchte, ändert

in regelmäßigen Abständen diesen SSID-Namen, um es etwaigen Eindringlingen auf Dauer schwer zu machen.

Das ist natürlich nur dann richtig sinnvoll, wenn die Rundumsendung der SSID (SSID-Ratio) versteckt wird. Der SSID-Name der FRITZ!Box lässt sich im Menü *Übersicht/Einstellungen/WLAN/Funkeinstellungen* bzw. bei den aktuellen Firmwareversionen über *Übersicht/Erweiterte Einstellungen/WLAN/Funknetz* ändern.

Bild 1.15: Spezialität der topaktuellen FRITZ!Box 7390: Erst wenn das Häkchen bei *2,4-GHz-Frequenzband* und/oder *5-GHz-Frequenzband* gesetzt ist, lässt sich der Name der SSID auf einen beliebigen Namen setzen.

Profis richten das WLAN-Netzwerk mit einem individuellen SSID-Namen ein und deaktivieren anschließend das SSID-Ratio – also das Versenden des SSID-Namens an die Umgebung. Bei der FRITZ!Box nehmen Sie hierfür das Häkchen bei *Name des Funknetzes (SSID) bekannt geben* heraus. Nur passend konfigurierte WLAN-Karten und WLAN-VoIP-Telefone können anschließend den WLAN-Router noch sehen und mit ihm Verbindung aufnehmen. Damit haben Sie schon viel für die Absicherung getan, denn eine komplizierte SSID, die man nicht einfach erraten kann, muss von einem potenziellen Hacker erst einmal herausgefunden werden.

Manchmal praktisch: Neuere FRITZ!Boxen wie die FRITZ!Box Fon WLAN 7390 bzw. neuere Firmwareversionen lassen hier auch eine getrennte Handhabung des 2,4-GHz- und des 5-GHz-Frequenzbands zu. So lassen sich ältere WLAN-Geräte mit einer anderen SSID betreiben – sprich, die FRITZ!Box drosselt die Geschwindigkeit der schnellen WLAN-Geräte nicht auf den kleinsten gemeinsamen Standard herunter.

1.2.2 Nur mit aktiver WLAN-Verschlüsselung

Ebenso wichtig wie die SSID ist die Verschlüsselung des WLAN. Damit sich beispielsweise Nachbarn nicht per Funk über die FRITZ!Box in das Internet einwählen können,

sollten, neben dem Verzicht auf die SSID-Rundumsendung, unbedingt die WEP- oder WPA-/WPA2-Sicherheitsoptionen aktiviert werden.

Die Standards sind unterschiedlich sicher (WEP ist vergleichsweise unsicher, WPA2 bisher nicht knackbar), ihre Verwendung hängt aber von den genutzten Geräten ab. Ältere Geräte können über USB-Adapter auch zur Unterstützung moderner Standards gebracht werden, entscheidend ist letztlich der Router.

Das am häufigsten eingesetzte Verfahren zur Verschlüsselung ist bei älteren WLAN-Routern WEP, das für *Wired Equivalent Privacy* steht – übersetzt etwa Kabelnetz-äquivalenter Schutz. Beim Einsatz von WEP ist ein sogenannter Netzwerkschlüssel für die Verschlüsselung notwendig. Diesen können Sie bei der Konfiguration des Routers selbst eingeben. WEP ist allerdings problemlos innerhalb einiger Minuten knackbar. Das sollten Sie wissen. Wenn Sie also nur auf WEP setzen können, weil Ihre Netzwerkgeräte keine andere Verschlüsselungstechnologie unterstützen, sollten Sie regelmäßig den Schlüssel und idealerweise auch die SSID wechseln.

Bild 1.16: Neuere FRITZ!Box-Modelle sind ab Werk schon mit einem sicheren WPA2-Schlüssel vorkonfiguriert. Dieser befindet sich auf der Bodenplatte des Geräts.

Abhängig von der Geräteinfrastruktur im Heimnetz sind unterschiedliche Schlüssellängen möglich. Im Zweifelsfall nutzen Sie den längsten Schlüssel. Denn je länger der Schlüssel ist, desto sicherer ist auch die Datenübertragung. So sind meist eine 64-Bit-Verschlüsselung (auch manchmal 40 Bit genannt) und eine 128-Bit-Verschlüsselung möglich. Abhängig vom »kleinsten gemeinsamen Nenner«, stehen hier folgende Optionen zur Verfügung:

Schlüsseltypen	*Beschreibung*
Deaktivieren	Keine Datenverschlüsselung (nicht zu empfehlen).
WEP (Wired Equivalent Privacy)	64-Bit- oder 128-Bit-WEP-Datenverschlüsselung verwenden (nutzen, wenn die übrigen WLAN-Geräte kein WPA-PSK oder WPA2 unterstützen). Wenn WEP aktiviert ist, können Sie die vier Datenschlüssel manuell eingeben oder automatisch erstellen lassen. Diese Werte müssen auf allen PCs und Access Points in Ihrem Netzwerk identisch sein und verwendet werden.
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA-PSK-Standardverschlüsselung verwenden (empfohlen). Manche WLAN-Karten unterstützen diese Verschlüsselung nicht. In diesem Fall nutzen Sie 128-Bit-WEP. Auch hier ist ein Verschlüsselungswert erforderlich.

Schlüsseltypen	Beschreibung
WPA2-AES (Advanced Encryption Standard)	Bieten der Router und die angeschlossenen Geräte WPA2 oder WPA-AES an, sollte aus Sicherheitsgründen diese Verschlüsselung genutzt werden. Dieser Sicherheitsstandard ist derzeit das Maß aller Dinge und in Verbindung mit einem nicht erratbaren Schlüsselwert eine sichere Sache.

Ende des Jahres 2004 wurde WPA2, also die 802.11i-Spezifikation für WLANs, festgelegt. Dafür ist in der Regel neue Hardware notwendig, beispielsweise ein WLAN-Router sowie passende WLAN-Karten. WPA2 verwendet statt des Verschlüsselungsprotokolls RC4 den sichereren *Advanced Encryption Standard* (AES). Nutzen Sie immer die aktuellste Verschlüsselung.

Auf WPA2-Kompatibilität achten
Achten Sie beim Kauf von WLAN-Komponenten auf die WPA2-Kompatibilität, es ist ärgerlich, nur aufgrund eines Geräts die Sicherheit des gesamten WLAN-Netzes zu schwächen. Wenn für eine ältere FRITZ!Box eine aktuelle Firmware angeboten wird, können Sie auch auf moderne Verschlüsselungsstandards umstellen.

Näheres zum Firmware-Update finden Sie im Kapitel »FRITZ!Box per Firmware-Update frisch halten«.

WEP-Schlüssel erstellen

Beim Erstellen eines Sicherheitsschlüssels im WEP-Verfahren stehen meist zwei unterschiedliche Methoden zur Verfügung: Sie können entweder den Schlüssel automatisch erstellen lassen oder selbst manuell einen eingeben.

Bei der automatischen Schlüsselerstellung geben Sie ein Wort oder eine Zeichenfolge in das Feld *Kennwort* ein und klicken auf die Schaltfläche *Erstellen.* Anschließend baut der Router selbstständig einen WEP-Schlüssel im Hexadezimalformat zusammen. In diesem Format werden nur die Zahlen von 0 bis 9 sowie die Buchstaben von A bis F genutzt.

Bei der Verschlüsselungsstärke 64 Bit füllt der Router automatisch alle vier Schlüsselfelder mit einem Schlüsselwert auf, bei der Verschlüsselungsstärke von 128 Bit ist das lediglich ein Wert. Egal ob Sie 64 Bit oder 128 Bit nutzen, dieser Schlüsselwert oder einer der Werte wird anschließend beim Einrichten der WLAN-Netzwerkkarte gebraucht.

Im manuellen Eingabemodus wählen Sie aus, welcher der vier Schlüssel (im Fall von 64 Bit) verwendet werden soll, und geben die Informationen zum WEP-Schlüssel für das Netzwerk im Hexadezimalformat in das ausgewählte Schlüsselfeld ein. Bei der WEP-Verschlüsselungsstärke von 64 Bit geben Sie 10 Hexadezimalzahlen ein, bei der WEP-Verschlüsselungsstärke von 128 Bit tragen Sie 26 Hexadezimalzahlen ein. Damit lässt sich die WLAN-Karte sicher mit dem WLAN-Router verbinden.

WPA-Schlüssel erstellen

Als sehr sicher schätzen Experten die Sicherheitsverschlüsselung WPA-PSK ein, das neuere WPA2-AES wird als noch sicherer eingestuft. Aus diesem Grund sollten Sie auch

dieses Verfahren für Ihr WLAN-Netzwerk nutzen. Ältere Centrino-Notebooks (beispielsweise Baujahr 2004) beherrschen allerdings meist nur WPA-PSK. Bei der Schlüsselerstellung geben Sie ein Wort bzw. eine Zeichenfolge in das Feld *Kennwort* ein, das mindestens 8 und höchstens 63 Zeichen lang sein darf. So können Sie beispielsweise ein ähnlich langes Kennwort wie dieses nutzen:

```
AdamundEvagehenindenWaldundholen6Äpfelheraus!GibtesApfelkuchen.
```

Es kann aber auch etwas Persönliches sein, solange Sie Ziffern etc. mit einbauen. Sie sollten es sich auf Papier notieren, da es beim Einrichten des WLAN-Client-PCs für die Verbindung gebraucht wird. Ist die Verschlüsselung aktiviert, ist der Grundstein gelegt, damit keine Fremden über Ihren WLAN-Router Unfug anstellen können. Anschließend aktivieren Sie die Protokollierung, damit Sie über sämtliche Aktivitäten des WLAN-Routers informiert sind.

Bild 1.17: Die FRITZ!Box unterstützt mit *WPA + WPA2* die derzeit aktuellste Verschlüsselung für WLANs. Lässt sich WPA2 bei einer betagten FRITZ!Box nicht auswählen, hilft in der Regel ein Firmware-Update, um die Box auf den aktuellen Stand zu bringen.

1.2.3 Wireless-Modus-Einstellungen richtig festlegen

Fast alle aktuellen WLAN-Router sind abwärtskompatibel, doch veraltete WLAN-Netzwerkkarten können manchmal nicht im Auto-Modus (automatische Erkennung des verwendeten Modus) betrieben werden und fordern den passenden Wireless-Modus explizit an, damit eine Übertragung überhaupt zustande kommen kann. So sind folgende Wireless-Modus-Einstellungen möglich:

Wireless-Modus	*Beschreibung*
n + a	Hier können sowohl 802.11a- als auch 802.11n-konforme Wireless-Geräte verwendet werden. Die Geschwindigkeit wird jeweils an das langsamste Gerät angepasst. 802.11a-Geräte erreichen eine maximale Bruttodatenrate von 54 MBit/s – achten Sie also auf den Einsatz von schnellen 802.11n-Geräten.
n + g	Hier können sowohl 802.11g- als auch 802.11n-konforme Wireless-Geräte verwendet werden. Die Geschwindigkeit wird jeweils an das langsamste Gerät angepasst.
b + g	Hier können sowohl 802.11g- als auch 802.11b-konforme Wireless-Geräte verwendet werden. Die Geschwindigkeit wird jeweils an das langsamste Gerät angepasst.
g	Im g-Modus können nur 802.11g-konforme WLAN-Geräte genutzt werden. Die Geschwindigkeit liegt standardmäßig bei 54 MBit/s und wird nur bei Verbindungsproblemen angepasst.
g++	Diese Bezeichnung ist vor allem bei neueren AVM-Geräten verbreitet. Dieser erweiterte g-Modus lässt sich nur mit hauseigenen AVM-Geräten nutzen.
b	Vergangenheit: Hier können alle 802.11b-konformen WLAN-Geräte verwendet werden. Zudem können 802.11g-konforme WLAN-Geräte im 802.11b-Modus betrieben werden. Die Geschwindigkeit orientiert sich am b-Standard, liegt also bei 11 MBit/s.
Nur 108 MBit/s	Bei aktuellen Geräten nicht mehr vorhanden: Wie bei g++ auch, ist dieser Modus herstellerabhängig. Der 108-MBit/s-Modus kann nur von kompatiblen 802.11g-Wireless-Geräten genutzt werden.
n + g + b	Es können alle 802.11n-, 802.11g- und 802.11b-Geräte verwendet werden.
Für 300 MBit/s optimierte Funkkanäle nutzen	Je schneller, desto besser: Ist die FRITZ!Box auf dem neuesten Stand, sollen die neuen WLAN-Geräte auch den schnellsten Standard nutzen dürfen.

Im b-Modus können alle 802.11b-konformen WLAN-Geräte verwendet werden. Zudem können 802.11g-konforme WLAN-Geräte auch im 802.11b-Modus betrieben werden. Ist die Option *108 Mbit/s-Einstellungen/Erweiterte 108 Mbit/s-Einstellungen deaktivieren* vorhanden und markiert, deaktiviert der Wireless-Router die Datenkomprimierung, das Packet-Bursting und die Unterstützung großer Frames. Wer beispielsweise eine PSP (*PlayStation Portable*) mit einem Netgear-Router nutzen möchte, muss dieses Feature ausschalten.

Diese Funktion ist bei manchen FRITZ!Box-Modellen bei den WLAN-Einstellungen unter 802.11g++ versteckt. Soll beispielsweise eine mobile PSP-Spielkonsole via WLAN mit dem Heimnetzwerk oder dem Internet verbunden werden, muss also eingegriffen werden: Der in der PSP eingebaute WLAN-Standard der ersten Generation ist 802.11b, der eine Übertragungsgeschwindigkeit von etwa 11 MBit/s ermöglicht. Im PSP-Betrieb muss der FRITZ!Box-g++-Schalter daher zwingend deaktiviert werden. Schnellere Datenübertragungsraten sind derzeit mit der PSP nicht möglich.

1.2.4 Wichtige Systemereignisse dokumentieren

Ein Protokoll ist prinzipiell eine detaillierte Aufzeichnung der Webseiten, auf die die angeschlossenen Rechner in Ihrem Netzwerk zugegriffen haben bzw. zuzugreifen versucht haben. Aus Sicherheitsgründen sollten Sie, falls vorhanden, diese Option aktivieren. Damit können Sie, sollte es zu Zwischenfällen oder Problemen kommen, nachschauen, was welcher Computer angestellt hat oder auch nicht. Die FRITZ!Box bietet derzeit keine Protokollierung der Webseiten, sondern nur eine Dokumentation wichtiger Systemereignisse, wie Internetverbindungsauf-/-abbau, Onlinezeit sowie das verbrauchte Onlinedatenvolumen.

Fungiert die FRITZ!Box auch als VoIP-Telefonzentrale, wird zusätzlich eine Anrufliste mitdokumentiert. In der Anrufliste werden alle ein- und ausgehenden Telefonate erfasst, die mit der FRITZ!Box geführt wurden. Ob allerdings eine Rufnummer protokolliert wird, hängt davon ab, ob Ihr Telefonanschluss das unterstützt. Kommen bei einem Analoganschluss keine Rufnummernübermittlungen an, kann auch die Box nichts anzeigen. Dann sehen Sie nur die von Ihnen getätigten Telefonate.

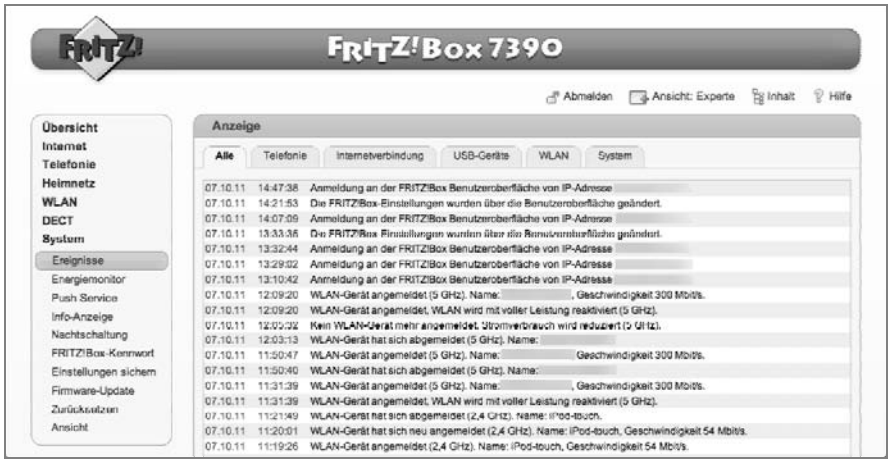

Bild 1.18: Spartanisch: In Sachen Protokollierung beschränkt sich die FRITZ!Box auf die wesentlichen Ereignisse. Diese sind über *System/Ereignisse* abrufbar.

Manche WLAN-Router bieten zusätzlich zur Protokollierung eine Content-Filterung. Ist diese Option aktiviert, ist in den Protokollen zu sehen, wann ein Rechner in Ihrem Netzwerk auf eine gesperrte Site zuzugreifen versucht hat. Bei einer aktivierten E-Mail-Benachrichtigung wird Ihnen das Protokoll automatisch in einer E-Mail zugestellt, Sie brauchen dann nicht immer über den Webseitendialog des Routers zu gehen.

1.2.5 Inaktive Dienste in der FRITZ!Box-Firewall sperren

Ein wesentlicher Sicherheitsaspekt bei der Konfiguration der FRITZ!Box sind die konfigurierten Dienste sowie die geöffneten Ports der integrierten Firewall. Eine Firewall muss prinzipiell zwei Funktionen erfüllen: Sie muss den PC und andere an ihn angeschlossenen Geräte nach außen in Richtung Internet absichern, damit Eindringlinge

keine Chance haben. Dazu soll die Firewall den auf dem PC laufenden Programmen und Spielen eine sichere Verbindung nach außen gewähren.

Die Firewall überwacht den Datenstrom an sogenannten Ports, das sind virtuelle Ein- und Ausgänge, die der PC verwaltet. Bei der Übertragung von Daten wird ein Port festgelegt und verwendet, Standardfunktionen wie FTP (*File Transfer Protocol*) oder HTTP haben vorgegebene Ports. Da ein Programm aber auch an einem beliebigen Port warten kann, macht die Firewall außerhalb der bekannten Ports meist zunächst mal dicht. Die wichtigsten »Alltagports« sind bei der FRITZ!Box geöffnet:

Portnummer	*Beschreibung*
20/21	FTP
80/8080	HTTP
53	DNS
110	POP3
1723	PPTP
25	SMTP
995	POP/SSL
143	IMAP
993	IMAP/SSL

Angriffsfläche der FRITZ!Box verringern
Je weniger Ports geöffnet sind, desto weniger Angriffsfläche bietet die FRITZ!Box. Wird der Router zu konservativ konfiguriert, ist das Heimnetz oder der PC zwar optimal abgesichert, aber unter Umständen leidet die Funktionalität. Wer mit seinem Spiele-PC hinter einer FRITZ!Box oder einer Personal Firewall online zocken möchte, muss den Router entsprechend einstellen, damit die Rückmeldungen von Spielserver und Mitspielern aus dem Internet auch zum PC zurückkommen. Erst dann kann dieser richtig mitfraggen. Welche Ports Sie für den PC im Endeffekt öffnen, hängt von Ihren persönlichen Ansprüchen und Sicherheitsbedürfnissen ab.

Insgesamt gibt es 65.535 verschiedene Ports. Damit bestimmten Anwendungen feste Portnummern zugewiesen werden können, sind die Ports im Wesentlichen in drei Gruppen unterteilt:

Bereich/Portnummer	*Beschreibung*
0 bis 1023	well known ports
1024 bis 49151	registered ports
49152 bis 65535	dynamic und/oder private ports

Beim Netzwerk-Gaming hängt es vor allem vom Spiel ab, welche Ports zur Verfügung stehen müssen.

Damit das Spielen grundsätzlich funktioniert, sind meist folgende Ports nach ICMP (*Internet Control Message Protocol*) notwendig:

```
53
80
443
```

ICMP dient dem Austausch von Fehler- und Informationsmeldungen bei TCP/IP- und UDP-Protokollen. Es sorgt dafür, dass eine Verbindung stabil bleibt – sprich aufrechterhalten wird – und es zu keinen ungewollten Verbindungsabbrüchen kommt. Ob weitere Ports gebraucht werden, steht im Handbuch zum Spiel. Dort sollte beschrieben sein, welche Ports offen sein müssen, damit das Spiel online gespielt werden kann. Welche Ports es gibt und wofür welcher TCP- bzw. UDP-Port zuständig ist, ist auf folgender Webseite zusammengefasst:

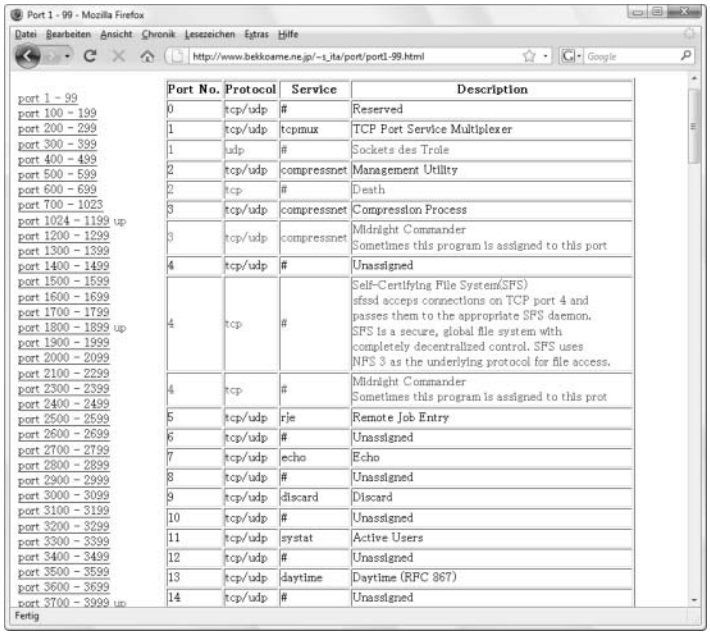

Bild 1.19: Für jeden Einsatzzweck sind die Ports 1 bis 65535 hier übersichtlich beschrieben: *www.bekkoame.ne.jp/~s_ita/port/port1-99.html*.

Die TCP- und UDP-Ports (*User Datagram Protocol*) sorgen für die Kommunikation auf Netzwerk- bzw. Anwendungsebene. Grundsätzlich gilt: Weniger ist mehr. Je weniger Ports geöffnet und Dienste verfügbar sind, desto weniger Angriffsfläche bietet der DSL-Router nach außen. So können Sie die Nutzung bestimmter Internetdienste wie das Surfen im WWW (HTTP), das *File Transfer Protocol* (FTP) und viele andere für alle oder einige Benutzer in Ihrem Netzwerk blockieren. Doch Vorsicht: Wird der Router zu sicher eingestellt, leidet die Funktionalität, weil bestimmte Programme nicht mehr richtig arbeiten.

Wer beispielsweise einen Webserver (HTTP-Protokoll mit Port 80) hinter einem Router oder einer Personal Firewall betreiben möchte, muss den DSL-Router so einstellen, dass die Anfragen aus dem Internet auch bis zum Server kommen können. Erst dann kann dieser reagieren und die Anfragen beantworten. Welchen Port Sie öffnen, hängt von

dem eingesetzten Serverprogramm und vor allem von Ihren persönlichen (Sicherheits-) Bedürfnissen ab.

Der Router kann auch so eingestellt werden, dass bestimmte Ports an ihm offen sind, die Daten, die dort ankommen, aber nur an einen bestimmten Rechner bzw. eine bestimmte IP-Adresse weitergeleitet werden. Diese Technik läuft unter dem Namen Portweiterleitung bzw. Port-Triggering.

Die Porteinstellungen der FRITZ!Box richten Sie über das Menü *Internet/Freigaben/Portfreigaben* ein.

Bild 1.20: Per Klick auf die Schaltfläche *Neue Portfreigabe* richten Sie eine neue Verbindung von außen auf einem PC im Netzwerk ein.

Ports einzeln angeben
Leider ist es bei der FRITZ!Box mit älteren Firmwareversionen nicht möglich, einen ganzen Portbereich (beispielsweise 16384 bis 16389) zur Weiterleitung freizugeben. Wer in diesem Fall einen Block von TCP- oder UDP-Ports in der Firewall freigeben möchte, muss jeden Port einzeln angeben. Sie ersparen sich unter Umständen Konfigurationsarbeit, wenn Sie zunächst die aktuelle Firmware in die FRITZ!Box einspielen. Das erledigen Sie im Webbrowser per *System/Firmware-Update*.

Portfreigabe und Zieladresse
Achten Sie darauf, dass bei der Konfiguration einer Portfreigabe die Zieladresse immer gleich bleibt. Hier ist es möglicherweise besser, für den Zielrechner im heimischen Netz wie oben beschrieben eine feste IP-Adresse einzurichten. Verwenden Sie im Zweifelsfall statt einer DHCP-Adresse für den PC eine statische IP-Adresse. Mithilfe der FRITZ!Box-Portfreigabe lassen sich so Dienste und verwendete Ports explizit bestimmten Rechnern im Heimnetz zuordnen.

Bild 1.21: Nach einem Firmware-Update lassen sich Portbereiche bei einer Portfreigabe einrichten.

1.2.6 Push Service: Systemmeldungen von der FRITZ!Box

Bei der FRITZ!Box ist in der Benutzeroberfläche ein sogenannter Push Service integriert, der den Anwender auf Wunsch per Mail über den Systemzustand und über Änderungen informiert. Grundvoraussetzungen dafür sind selbstverständlich ein E-Mail-Konto und die passenden Zugangsdaten, damit die FRITZ!Box entsprechend konfiguriert werden kann.

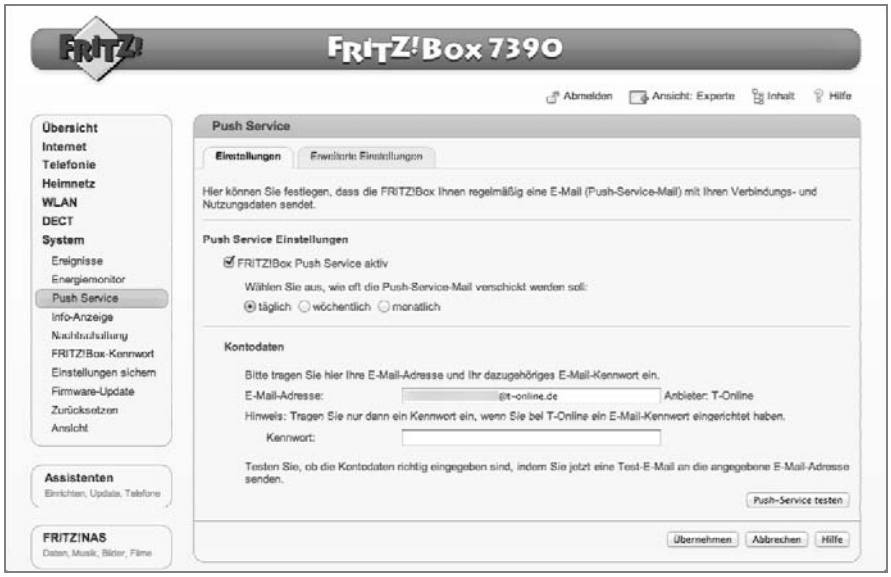

Bild 1.22: Im Menü *System/Push Service* richten Sie das gewünschte E-Mail-Konto ein, das die Systemmeldungen der FRITZ!Box in Empfang nehmen soll.

Sind sämtliche Einstellungen eingetragen, können Sie per Klick auf die Schaltfläche *Push-Service testen* die ordnungsgemäße Funktion überprüfen. Haben Sie nach wenigen

Minuten eine E-Mail im Posteingang, können Sie mit einem Klick auf die Schaltfläche *Übernehmen* die Einstellungen speichern.

1.3 Erweiterte WLAN-Sicherheitseinstellungen

Viele WLAN-Router bieten neben den Standard-Wireless-Einstellungen auch eine Option an, mit der Sie erweiterte Einstellungen für das Funknetz konfigurieren können. Durch einen geschickten Eingriff machen Sie das WLAN-Netz für andere fast unsichtbar und beschränken den Zugriff auf das Netzwerk auf Clients, die sich anhand ihrer MAC-Adresse authentifizieren. Hier kann auch WLAN grundsätzlich deaktiviert werden.

Das ist zu empfehlen, wenn keine WLAN-Geräte zum Einsatz kommen und der WLAN-Router ausschließlich für kabelgebundene Clients zuständig sein soll. Standardmäßig erhält jede WLAN-Karte, die mit einer passenden SSID und dem korrekten Schlüssel sowie dem passenden Verschlüsselungsstandard konfiguriert ist, Zugriff auf das drahtlose Netzwerk.

Bei der FRITZ!Box hängt es von der eingesetzten Firmwareversion sowie vom FRITZ!Box-Modell ab, welche Optionen im Bereich *Übersicht/Erweiterte Einstellungen/WLAN* zur Verfügung stehen. Mit Auswahl der Option *WLAN aktivieren* können Sie auf andere Optionen zugreifen. Benutzen Sie kein WLAN, schalten Sie es über diese Option am Router aus.

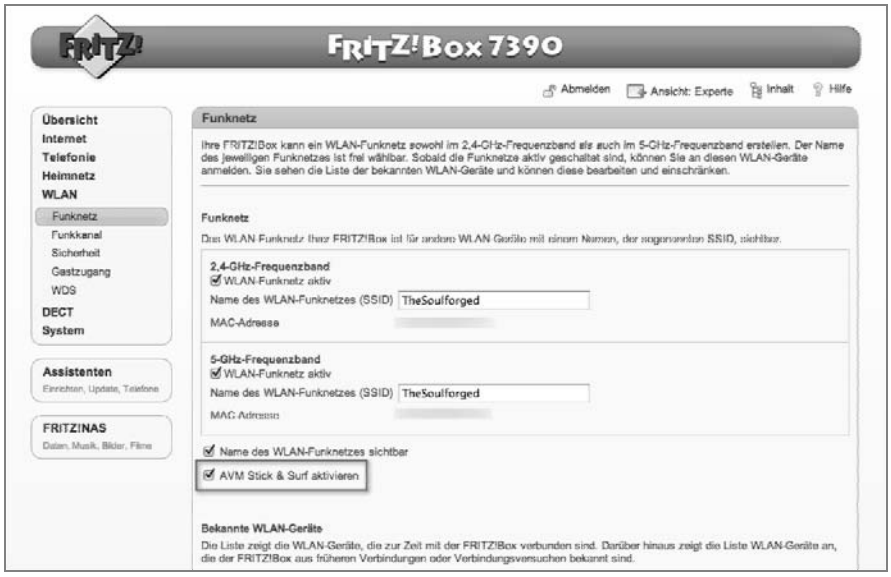

Bild 1.23: Nur wer einen AVM-USB-Stick im Einsatz hat, muss das Häkchen bei *AVM Stick & Surf aktivieren* setzen.

Wireless-Router-Einstellungen	*Beschreibung*
Name des Funknetzes (SSID)	Hier lässt sich der Name des WLAN-Netzes konfigurieren. Ist das Häkchen bei *WLAN aktivieren* gesetzt, sendet die FRITZ!Box ihren Netzwerknamen (SSID, *Service Set Identifier*) an alle Wireless-Stationen.
Funkkanal auswählen	Dieser Schalter legt fest, welche Betriebsfrequenz der Router nutzen soll. Hier können Sie die Werkeinstellung beibehalten, es sei denn, es sind Störstrahlungen von einem anderen WLAN-Router in der Umgebung bemerkbar. Dies macht sich vor allem durch Schwierigkeiten beim Verbindungsaufbau und in der Geschwindigkeit bemerkbar. Hängen in der Nachbarschaft einige andere WLAN-Router an der Steckdose, kann das Umkonfigurieren des Kanals einen Geschwindigkeitsschub bringen.
Name des WLAN-Funknetzes sichtbar	Ist diese Option aktiviert, sendet der Wireless-Router seinen Netzwerknamen (SSID, *Service Set Identifier*) an alle Wireless-Stationen. Stationen, die keine SSID (oder den Wert null) haben, können dann die korrekte SSID für Verbindungen zu diesem Access Point annehmen.
AVM Stick & Surf aktivieren	Diese Option ist für USB-Adapter aus dem Hause AVM gedacht. Setzen Sie einen AVM-USB-Adapter ein, sollte hier das Häkchen gesetzt werden.

Zusätzlich können bei manchen FRITZ!Box-Modellen noch verschiedene Einstellungen zum Übertragungsmodus, sprich der Sendeleistung, vorgenommen werden.

Bild 1.24: Sie konfigurieren den Übertragungsmodus in Abhängigkeit von den verwendeten WLAN-Komponenten.

Für mehr Sicherheit ist die Option *Sicherheit* bei der FRITZ!Box ideal: Hier können Sie den Zugriff auf das WLAN auf Grundlage der MAC-Adresse des PCs beschränken.

1.3.1 Zugriffsliste für neue WLAN-Geräte einrichten

Standardmäßig wird jedem drahtlosen PC, der mit einer korrekten SSID, dem richtigen Verschlüsselungsstandard sowie dem passenden Schlüssel ausgestattet ist, Zugang zum drahtlosen Netzwerk gewährt. Jeder Router beinhaltet jedoch eine MAC-Adressfilterung, bei der PCs basierend auf ihren MAC-Adressen eine Verbindung zum Router aufbauen dürfen oder auch nicht.

Bei einer FRITZ!Box sorgen Sie für mehr Sicherheit, wenn Sie per *Übersicht/WLAN/Funknetz* die Option *WLAN-Zugang auf die bekannten WLAN-Geräte beschränken* aktivieren, nachdem der Computer über WLAN erstmalig Verbindung mit dem WLAN-Router aufgenommen hat. Diese Option aktivieren Sie erst dann, wenn die FRITZ!Box fertig konfiguriert und erstmals eine Verbindung erfolgreich zwischen Computer und DSL-Router hergestellt worden ist. In diesem Fall merkt sich die FRITZ!Box die MAC-Adresse des PCs und verweigert anderen Geräten die Zusammenarbeit.

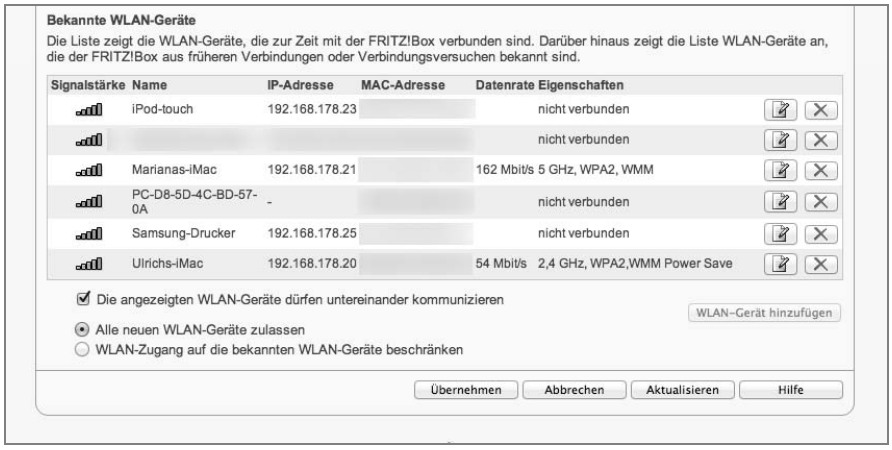

Bild 1.25: Nur bei der erstmaligen Konfiguration des WLAN-Netzwerks braucht der Schalter *Alle neuen WLAN-Geräte zulassen* aktiviert zu sein. Sind die gewünschten Geräte einmal mit der FRITZ!Box verbunden worden, merkt sich die FRITZ!Box deren MAC-Adresse.

Wird beim Eintragen des Geräts der Gerätename nicht angezeigt, können Sie selbst einen beschreibenden Namen für den PC eingeben, den Sie der MAC-Adresse hinzufügen. Wie alle anderen wichtigen Ereignisse dokumentiert die FRITZ!Box auch die An- und Abmeldevorgänge der WLAN-Stationen. Über die Weboberfläche unter *Übersicht/System/Ereignisse* im Register *WLAN* können Sie das Protokoll einsehen. Hier finden Sie auch die abgelehnten Zugriffe. Das kann ein Hinweis darauf sein, dass von außen jemand versucht, auf Ihr WLAN zuzugreifen.

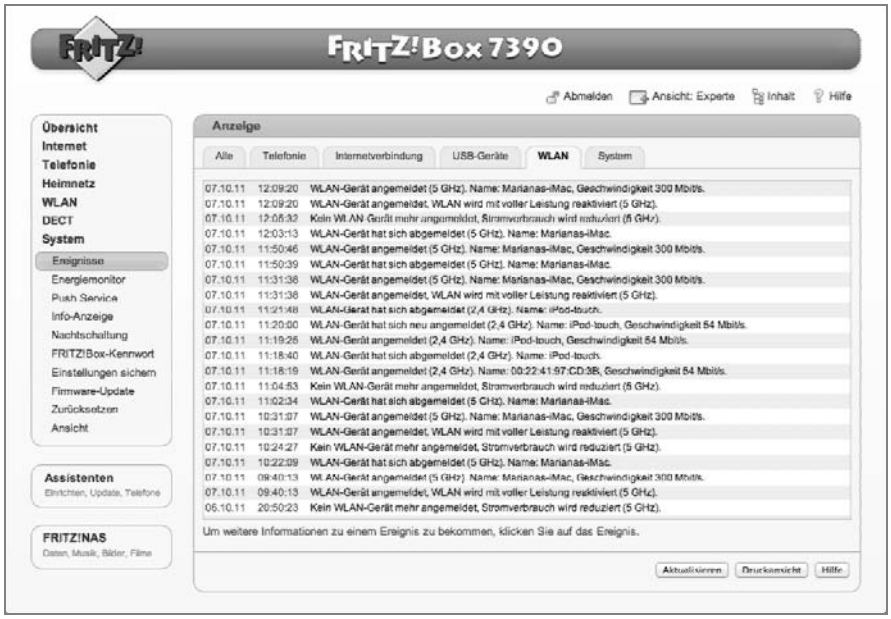

Bild 1.26: Sämtliche An- und Abmeldevorgänge an der FRITZ!Box sowie die zugewiesenen IP-Adressen und dazugehörige Verbindungsgeschwindigkeiten werden im Menü *System/Ereignisse/WLAN* erfasst.

1.3.2 Zugang erlaubt? – Angeschlossene Geräte checken

Jeder vernünftige Router bietet einen Dialog, der eine Übersicht über angeschlossene Geräte liefert. In der Regel sind die IP-Adresse, der Gerätename, den Sie unter Windows vergeben haben, und die MAC-Adresse jedes eingeschalteten Computers zu sehen, der mit dem Router verbunden ist.

Das ist besonders praktisch, wenn Sie vermuten, dass sich ein Fremdling in Ihrem Netz befindet. In diesem Fall sollten Sie die Sicherheitseinstellungen der FRITZ!Box nochmals überprüfen. Dazu schalten Sie am besten alle Ihre PCs, die über das Funknetz zugreifen, aus, und es sollte nur noch ein Rechner mit seiner MAC-Adresse (unbedingt notieren) zu sehen sein. Gibt es weitere, müssen Sie sich Gedanken machen.

Mithilfe der FRITZ!Box können Sie die Verbindungen direkt unterbrechen. Sie sollten aber sofort die SSID wechseln, sie unsichtbar machen und die Verschlüsselung mit einem neuen Schlüssel aktualisieren. Danach gilt es, die Protokolle daraufhin zu überprüfen, was alles aufgerufen wurde. Rechtlich sieht es so aus, dass die Nutzung unzureichend gesicherter Funknetze eine Grauzone ist, denn für Sicherheit hat jeder selbst zu sorgen.

Bei einer FRITZ!Box sorgen Sie für mehr Sicherheit, wenn Sie die Option *WLAN-Zugang auf die bekannten WLAN-Geräte beschränken* (bei älteren FRITZ!Boxen: *Keine neuen WLAN-Netzwerkgeräte zulassen)* aktivieren, nachdem der Computer mit WLAN-Karte erstmalig Verbindung mit dem WLAN-Router aufgenommen hat. In diesem Fall

merkt sich die FRITZ!Box die MAC-Adresse des Computers und verweigert die Zusammenarbeit mit anderen Geräten.

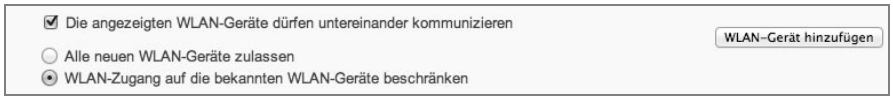

Bild 1.27: Standardmäßig erhält jede WLAN-Karte, die mit einer passenden SSID konfiguriert ist, Zugriff auf das drahtlose Netzwerk. Für mehr Sicherheit bei der FRITZ!Box sorgt dieser Dialog: Im Menü *WLAN/Funknetz* können Sie den Zugang auf das WLAN auf Grundlage einer MAC-Adresse beschränken, falls Sie das Optionsfeld *WLAN-Zugang auf die bekannten WLAN-Geräte beschränken* umlegen.

Standardmäßig wird jedem drahtlosen Gerät, das mit einer korrekten SSID und dem passenden Schlüssel ausgestattet ist, Zugang zu dem drahtlosen Netzwerk gewährt. Jeder Router bietet jedoch eine MAC-Adressfilterung, bei der Geräte basierend auf ihren MAC-Adressen eine Verbindung zum Router aufbauen dürfen – oder auch nicht.

1.3.3 Kindersicherung für den Familien-PC

Nutzen Sie im Haushalt einen Computer und melden sich Ihre Kinder mit ihren eigenen Benutzernamen darauf an, können Sie die Kindersicherung der FRITZ!Box nutzen. Bevor Sie die Kindersicherung auf der FRITZ!Box aktivieren, muss auf dem Windows-PC eine spezielle AVM-Software installiert werden.

Den Link auf die Internetseite von AVM zu dem entsprechenden Windows-Programm *FRITZ!Box Kindersicherung* finden Sie im Hauptmenü Ihrer FRITZ!Box über *Einstellungen/Programme*. Im Zusammenspiel mit diesem Programm können Sie die FRITZ!Box nun so konfigurieren, dass der Computer im Kinderzimmer nur zu bestimmten Zeiten und in begrenztem Umfang in das Internet kann.

Zunächst installieren Sie das Windows-Programm *FRITZ!Box Kindersicherung* – in der Regel klicken Sie die Installation problemlos durch. Anschließend melden Sie sich am PC im Kinderzimmer mit dem Kinder-Account an und stellen eine Internetverbindung her, etwa für das Windows-Update oder das Update des Virenscanners. In diesem Fall kennt die FRITZ!Box anschließend den Windows-Benutzer *SYSTEM*, der für Windows-Updates und Updates von Virenschutzprogrammen zuständig ist. Nun bekommen Sie den Benutzernamen *SYSTEM* sowie den Benutzernamen des Kindes im Kindersicherungsdialog angezeigt.

Bild 1.28: Wenn Sie die *Kindersicherung* nicht benötigen, achten Sie darauf, dass sie ausgeschaltet ist. Andernfalls sorgt die Kindersicherung auf Port 14013 für überflüssige Kommunikation im Heimnetzwerk.

Im nächsten Schritt aktivieren Sie über das Menü *Internet/Filter/Kindersicherung* die Zugangsregeln für die Computer im Heimnetz. In der Liste der Geräte wählen Sie den zu beschränkenden Benutzer aus und legen in der darauf erscheinenden Übersicht die zeitliche Beschränkung der Internetnutzung fest.

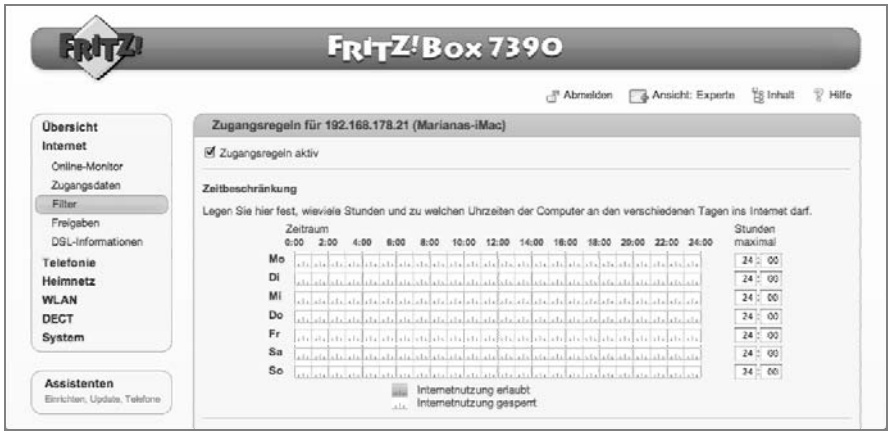

Bild 1.29: Hier lassen sich in den entsprechenden Feldern die Zeitintervalle festlegen, in denen das Internet genutzt werden darf. Es sind unterschiedliche Einstellungen für Montag bis Donnerstag, für den Freitag und für das Wochenende möglich.

1.3.4 Firewall immer einschalten

Grundsätzlich gilt: Beim Surfen im Internet sollte die Firewall zwingend eingeschaltet sein. Die SPI-Firewall (*Stateful Port Inspection*) schützt das Netzwerk vor DoS-Attacken (*Denial of Service*, Überlastung des Systems durch eine Unzahl von Anfragen) und anderen Übeltätern. Die Firewall ist in der Regel standardmäßig bei den meisten Herstellern ab Werk aktiviert.

1.3.5 Ping ignorieren

Das Suchen von potenziellen Opfern für DoS-Angriffe etc. wird über den *ping*-Befehl realisiert. Auf diese Weise kann ein anderer Rechner feststellen, ob die angepingte Maschine noch läuft und für Anfragen aus dem Netz erreichbar ist. Manche Modelle lassen sich so konfigurieren, dass sie nicht auf einen Ping aus dem Internet reagieren. Finden Sie eine Option mit einem Namen wie *Auf Ping am Internet-Port reagieren*, sollten Sie sie deaktivieren, es sei denn, Sie haben einen guten Grund, sie aktiviert zu lassen. Das hat übrigens nichts mit der Möglichkeit des »Anpingens« im heimischen Netzwerk, die Sie weiter unten kennenlernen werden, zu tun. Der netzinterne Ping wird anders interpretiert als einer über den Internetport.

1.3.6 MTU richtig einstellen

Das Konfigurieren der MTU-Größe (*Maximum Transmission Unit*, maximale Übertragungseinheit) hat weniger mit Sicherheit zu tun, es dient eher dem Feintuning und der Totaloptimierung des DSL-Routers.

Bei der FRITZ!Box kann kein MTU-Wert eingestellt werden. Lässt der DSL-Router hier einen Eingriff zu, lohnt es sich, die Einstellungen zu überprüfen. Der passende MTU-Wert für die meisten Ethernet-Netzwerke beträgt 1.500 Byte oder 1.492 Byte für PPPoE-Verbindungen bzw. 1.436 Byte für PPTP-Verbindungen. Bei einigen Internetanbietern ist möglicherweise das Reduzieren der maximalen Übertragungseinheit notwendig.

Wenn der MTU-Wert nicht passt, kann es passieren, dass manche Seiten nicht aufgerufen werden können. Um zu prüfen, ob der konfigurierte MTU-Wert passt oder nicht, verwenden Sie einfach den *ping*-Befehl:

```
C:\WINDOWS\system32>ping -f -l 1464 www.franzis.de

Ping www.franzis.de [217.64.171.171] mit 1464 Bytes Daten:

Antwort von 192.168.123.254: Paket müsste fragmentiert werden, DF-Flag ist jedoc
h gesetzt.
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.

Ping-Statistik für 217.64.171.171:
    Pakete: Gesendet = 4, Empfangen = 1, Verloren = 3 (75% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

C:\WINDOWS\system32>
```

Bild 1.30: Mit dem *ping*-Befehl überprüfen Sie die eingestellte MTU-Größe. Kommt die Meldung *Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt*, ist die MTU-Konfiguration in Ordnung.

Mit dem Befehl:

```
ping -f -l 1464 www.franzis.de
```

auf der Kommandozeile prüfen Sie die MTU-Einstellungen für die TCP/IP-Verbindung. Geben Sie beispielsweise einen anderen MTU-Wert mit dem Befehl

```
ping -f -l 1460 www.franzis.de
```

ein, erscheint folgende Rückmeldung:

```
Antwort von 80.237.218.241: Bytes=1460 Zeit=64ms TTL=47
Antwort von 80.237.218.241: Bytes=1460 Zeit=61ms TTL=47
Antwort von 80.237.218.241: Bytes=1460 Zeit=61ms TTL=47
Antwort von 80.237.218.241: Bytes=1460 Zeit=61ms TTL=47
```

Der Ping geht also durch den DSL-Router zum Zielserver mit der IP-Adresse *80.237.218.241*, der anschließend fehlerfreie Pakete zurücksendet. Addieren Sie nun 28 Byte für den notwendigen IP/ICMP-Header zu den 1460 Byte, beträgt der ideale Wert 1488. Abhängig von der Verbindung stellen Sie die passende MTU ein.

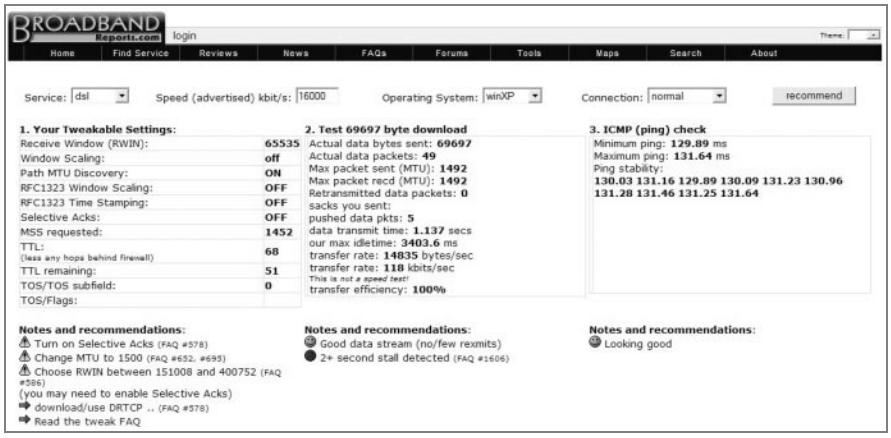

Bild 1.31: Hier finden Sie einen Geschwindigkeitstest, um die MTU-Einstellungen zu überprüfen – siehe *www.dslreports.com/tweaks*.

Bei manchen Anbietern ist dieser Wert mit 1492 angegeben. Sind einige Webseiten nicht zu erreichen oder treten Probleme beim Upload von Dateien oder E-Mails auf, prüfen Sie den MTU-Wert des Routers. Testen Sie Werte wie 1488, 1492 und 1500 – der ideale Wert hängt vom Provider ab. Im Zweifelsfall erkundigen Sie sich im Supportbereich auf der Webseite Ihres Internetproviders nach dem idealen MTU-Wert. Diese Maßnahme sorgt auch für eine bessere Qualität beim Telefonieren über das Internet. Also unbedingt testen!

1.4 Für alle Fälle: FRITZ!Box-Einstellungen sichern

Ist die FRITZ!Box ordnungsgemäß und sicher konfiguriert, sollten Sie die gemachten Einstellungen sichern. Bessere Geräte geben dafür die Möglichkeit, die Einstellungen in einer Konfigurationsdatei zu speichern. Bietet Ihr Modell diese Option nicht an, sollten Sie die gemachten Einstellungen per Screenshot speichern und ausdrucken. Dafür drücken Sie einfach die Druck-Taste, um diesen Bildschirm in die Zwischenablage zu kopieren. Anschließend öffnen Sie beispielsweise Word und fügen mit der Tastenkombination Strg+V den Inhalt der Zwischenablage ein. Schließlich speichern Sie das Dokument oder drucken es wie gewohnt aus.

1.4.1 Router-Einstellungen als Datei herunterladen

Gehen Sie folgendermaßen vor: In der Benutzeroberfläche wählen Sie in der Expertenansicht im Menü *System* die Funktion *Einstellungen sichern*. Geben Sie Ihr Kennwort ein und bestätigen Sie mit *Sichern*.

Bild 1.32: Übersichtlich gelöst: Das *Sichern* und *Wiederherstellen* der FRITZ!Box-Konfiguration geschieht in ein und demselben Dialog.

Arbeiten mehrere Anwender mit dem heimischen Rechner, ist es unter Umständen sinnvoll, die FRITZ!Box-Konfiguration passwortgeschützt auf der Festplatte abzulegen, damit kein Unbefugter die Konfigurationsparameter einsehen oder gar ändern kann. In diesem Fall geben Sie bei *Kennwort* sowie *Kennwortbestätigung* ein Passwort ein. Um die Einstellungen auf die Festplatte herunterzuladen, genügt der Klick auf die Schaltfläche *Sichern*.

Bild 1.33: Die FRITZ!Box exportiert die Einstellungen in eine Datei mit der Bezeichnung *FRITZ.Box Fon WLAN 7390 84.05.05_07.10.11_1558.export*. Der Name unterscheidet sich je nach Modelltyp und Exportdatum.

Sie können die Router-Einstellungen aus dieser Datei wiederherstellen. In der Regel sollten Sie darauf achten, dass Sie beim Wiederherstellen oder Löschen der Router-Einstellungen nicht online sind. Ziehen Sie vorsichtshalber das Internetkabel heraus.

1.5 FRITZ!Box per Firmware-Update frisch halten

Kein Hersteller ist perfekt: Täglich gibt es neue Veröffentlichungen über Sicherheitslücken und Angriffsmöglichkeiten bei den verschiedensten Router-Modellen. Meist wird mit unterschiedlichen Hackertools versucht, den Router zu kompromittieren oder ihn per Buffer-Overflow-Mechanismen in einen nicht betriebsfähigen Zustand zu versetzen.

Deshalb sollten Sie regelmäßig auf den Supportseiten des Herstellers nach neuer Firmware Ausschau halten. Oft gehen Verbesserungen der Sicherheit auch mit Erweiterungen der Funktionalität oder sogar der Implementierung neuer Standards (WPA2-Verschlüsselung) einher.

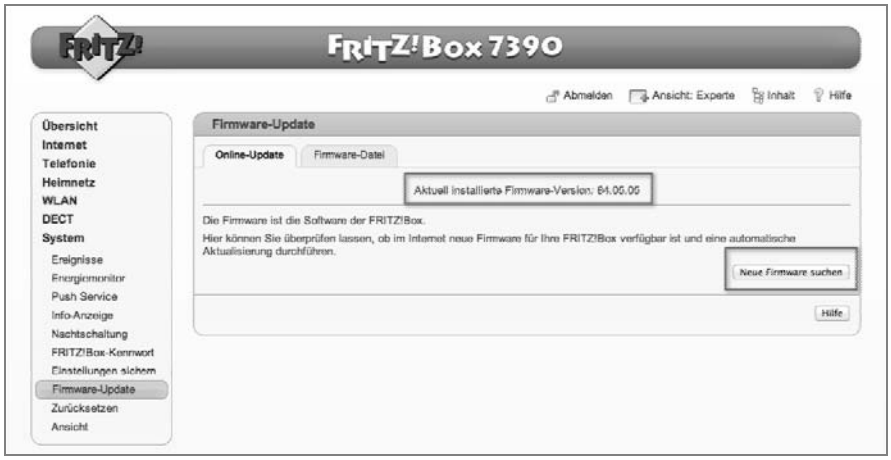

Bild 1.34: Freie Auswahl: Bei der FRITZ!Box können Sie die Firmware entweder über den AVM-Server (hier Schaltfläche *Neue Firmware suchen*) oder über eine Firmwaredatei (Register *Firmware-Datei*), die sich auf der Festplatte befindet, aktualisieren.

Ist eine Internetverbindung eingerichtet, bieten manche Geräte auch eine Aktualisierung der Firmware ohne Umwege an. Dafür steht eine Option auf den Router-Konfigurationsseiten zur Verfügung. Hier sucht der Router selbstständig die aktuellste Version auf den Supportseiten.

Bild 1.35: Auch auf der AVM-Website *www.avm.de* können Sie die aktuelle Firmwareversion im *Download*-Bereich abfragen.

Je nach Herangehensweise müssen Sie bei einem Direktdownload nach dem Herunterladen diese Datei entpacken, bevor Sie das Gerät mit der neuen Firmware aufrüsten können. In einigen Fällen kann es sein, dass der Router nach dem Einspielen der Firmware neu konfiguriert werden muss. Deshalb ist es sinnvoll, vor dem Einspielen der neuen Firmware die Router-Einstellungen zu sichern.

Bei den neueren Modellen verlangt die FRITZ!Box das Anfertigen eines Backups mit den Einstellungen, bevor eine neue Firmware aufgespielt werden kann. Hierzu sichern Sie zunächst die FRITZ!Box-Einstellungen, wie im vorigen Kapitel beschrieben. Sind die Einstellungen gespeichert, kann die neue Firmware in die Box geladen werden. Dafür wählen Sie zunächst über die *Datei auswählen*-Schaltfläche den Pfad zur Firmwaredatei aus.

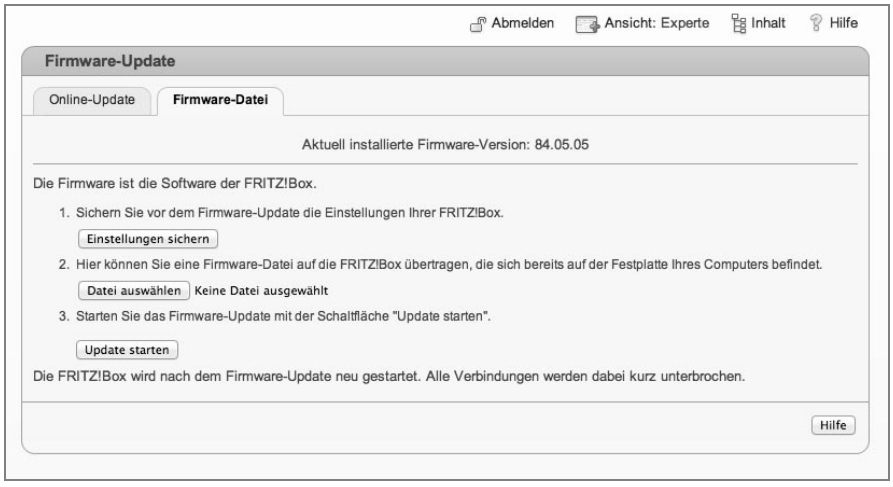

Bild 1.36: Entweder via Internet oder über eine Firmwaredatei: Eine frische Firmware sorgt für Sicherheit.

Mit einem Klick auf eine der Schaltflächen *Update starten* spielt der Router die neue Firmware selbstständig ein.

Während dieses Vorgangs darf der Router weder ausgeschaltet werden noch online (also im Internet) sein. Ist der Vorgang abgeschlossen, rufen Sie den Router-Status auf und prüfen die Firmwareversion, um sicherzustellen, dass auf dem Router nach dem Update die neueste Software installiert ist.

Bild 1.37: Bitte warten: Während der Übertragung der Firmware auf den Router darf die Stromversorgung nicht unterbrochen werden.

1.5.1 Windows-Blockade lässt FRITZ!Box-Firmware-Update nicht zu

Ein Firmware-Update der FRITZ!Box ist bekanntlich von Zeit zu Zeit nicht nur sinnvoll, sondern aus Sicherheitsgründen auch ratsam. Neue Funktionen und das Stopfen von Sicherheitslücken sorgen dafür, dass der Computer bzw. das Heimnetz vor etwaigen Angriffen aus dem Internet geschützt bleibt. Setzen Sie Windows Vista oder Windows 7 mit einem älteren Internet Explorer als Version 8 ein, ist ein Firmware-Update nicht auf Anhieb möglich.

Der Grund: Die Sicherheitseinstellungen des standardmäßig installierten Internet Explorer oder auch der Firewall lassen das Ausführen des Firmware-Updates nicht zu. Haben Sie sich aus dem Internet eine aktuelle Firmwaredatei besorgt, erscheint beim eigentlichen Firmware-Update die Meldung *Bitte den vollständigen Pfadnamen angeben*, und die Installation ist nicht möglich.

Bild 1.38: Spielen Sie wie gewohnt eine frische Firmware ein.

Bild 1.39: Erhalten Sie bei einem Firmware-Update die Fehlermeldung *Bitte den vollständigen Pfadnamen angeben*, ist das Firmware-Update mit diesem Browser nicht möglich.

Abhilfe schafft das Ändern der Sicherheitseinstellungen im Internet Explorer oder das temporäre Deaktivieren der aktiven Schutzprogramme, z. B. der Windows-Firewall. Nach dem Update können Sie die Schutzprogramme wieder einschalten.

Empfehlenswerter ist auf jeden Fall das Aktualisieren des Internet Explorer auf die aktuellste Version via Windows Update oder gar der komplette Umstieg auf den Mozilla Firefox-Browser. Firefox kennt die beschriebenen Update-Probleme nicht.

1.6 FRITZ!Box für Internettelefonie konfigurieren

Für das Telefonieren über das Internet gibt es verschiedene Standards. Neben SIP (*Session Initiation Protocol*) ist auch RTP (*Realtime Transport Protocol*) eine tragende Säule. Während SIP dafür sorgt, dass der Anruf auch beim Gegenüber ankommt, ist RTP im Fall eines aktiven Gesprächs für die Audiodatenübertragung zuständig. Skype nutzt eine andere Übertragungstechnik als die klassischen VoIP-Programme und ist bei der Auswahl der Ports deutlich flexibler. Bei Skype spielen SIP und RTP keine Rolle.

1.6.1 Internettelefonie mit dem Computer

Wer mit seinem Computer über das Internet telefonieren möchte, sollte beachten, dass die Konfiguration der Firewall bzw. des DSL-WLAN-Routers vornehmlich von der eingesetzten SIP-Software auf dem Rechner abhängig ist. Da eine NAT-Firewall (*Network Address Translation*) nach außen eine IP-Adresse und nach innen im Heimnetz mehrere IP-Adressen zu versorgen hat, kann es beim Telefonieren hier anfänglich zu Problemen kommen, sollte NAT, also die Portweiterleitung, falsch konfiguriert sein. NAT macht nichts anderes, als eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. Bei einem Router bzw. einer Firewall sorgt NAT dafür, private IP-Adressen auf öffentliche IP-Adressen abzubilden.

Bei NAT kennt der Telefonieclient die aktuelle Internet-IP-Adresse nicht, er besitzt ja eine lokale nach dem Muster 192.168.X.X. Deshalb nutzen die SIP-Gateways die Absender-IP-Adresse, also die Internetadresse des DSL-WLAN-Routers. Dafür ist der STUN-Server (*Simple Traversal of UDP through NAT*) des VoIP-Anbieters zuständig. Dieser versorgt den Telefonieclient mit den nötigen Informationen, damit es mit dem Telefonieren auch funktioniert.

Eine Firewall bzw. ein DSL-WLAN-Router kann nur Daten von außen zu einem bestimmten Client transportieren, wenn bekannt ist, wohin diese weitergeleitet werden müssen. Dafür sorgt der interne Initialisierungsvorgang der SIP-Software bzw. des IP-Telefons. Damit das Telefonieren mit einer NAT-Firewall auch erfolgreich verläuft, müssen in der Regel folgende Ports konfiguriert sein:

*Benötigte Ports**	*Programm/Protokoll*
80 (TCP)	Freigabe, Registrierung
3478–3479 (UDP)	NAT/STUN (STUN ist nur notwendig, wenn NAT benutzt wird)
5004 (UDP)	RTP
5060 (UDP)	SIP Signal Telefon
5062 (UDP)	SIP Signal Anrufbeantworter
5069 (UDP)	iPhone Freenet
5070, 5072 (UDP)	1&1 SoftPhone, Nero SIPPS
8000–8006 (UDP)	X-Lite
8000–8012 (UDP)	X-Pro
10000–10012 (UDP)	Datenverkehr IP-Telefon Hersteller X

*Benötigte Ports**	*Programm/Protokoll*
16384–16390 (UDP)	Datenverkehr Freenet iPhone
30000–30012 (UDP)	Datenverkehr Nikotel-Anrufbeantworter
* Alle ein- und ausgehenden UDP- und TCP-Ports.	

Für SIP wird in der Regel immer der UDP-Port 5060 benötigt. Meist überwacht eine Firewall nur den eingehenden Datenverkehr, teure und restriktive Produkte sorgen jedoch auch beim ausgehenden Datenverkehr für Sicherheit.

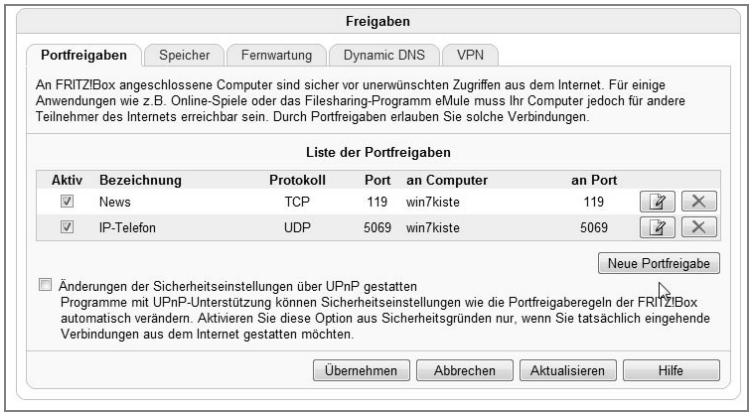

Bild 1.40: Bei der FRITZ!Box wird der für die Internettelefonie notwendige Port unter *Portfreigaben* eingetragen.

Für VoIP sind in der Firewall bzw. Portfreigabe meist zusätzlich die Ports 5062, 5070, 5072, 3478 und 30000 bis 30005 freizugeben, damit das Telefonieren auch möglich ist. Hier aktivieren Sie *port forwarding* für die oben angegebenen Ports und leiten diese auf den Rechner um, von dem aus ins Internet telefoniert wird.

Durch die Umleitung der Daten, die auf Port 5060 auf dem Router bzw. der Firewall eintreffen, sorgt dieser Mechanismus dafür, dass sie an den vorgesehenen Rechner im Netzwerk weitergeleitet werden. Der ist nach außen von der Firewall geschützt und außerhalb des Routers bzw. der Firewall nicht direkt erreichbar. Abhängig davon, welches SIP-Programm verwendet wird, können noch zusätzliche oder andere Ports maßgeblich sein. Kommt es hier zu Problemen, hilft die Suche in den Foren bzw. auf der Website des jeweiligen Herstellers weiter.

1.6.2 FRITZ!Box Fon WLAN: eine für alles

Internettelefonie ist nicht gleich Internettelefonie. Der wesentliche Unterschied liegt in der Auswahl der Endgeräte. Neuere Internettelefone sehen aus wie konventionelle Telefone. Eingesteckt werden sie am Festnetzanschluss. Auch ein bereits vorhandenes analoges Telefon kann für Voice over IP genutzt werden. Dafür ist manchmal ein SIP-Adapter nötig, der direkt am Router angesteckt wird. Anschließend wird das analoge

Stichwortverzeichnis

E. F. Engelhardt

Das große inoffizielle FRITZ!Box Handbuch

Ihre FRITZ!Box kann weit mehr, als der Hersteller verrät. Dieses Buch zeigt, wie Sie die Reichweite Ihrer FRITZ!Box mit einer leistungsstarken Antenne erhöhen, wie Sie Ihre eigene FRITZ!Box-Firmware programmieren und mit den richtigen Einstellungen maximale Datenpower herausholen, egal ob Sie einen DSL-Anschluss, UMTS oder Kabel benutzen. Auch die WLAN-Sicherheit und die Einbindung von iPhone, iPad und Android-Geräten in das Netzwerk kommen nicht zu kurz. Mit diesem Buch machen Sie Ihre FRITZ!Box noch besser und sicherer.

Sie besitzen einen T-Home Speedport und möchten ihn als FRITZ!Box nutzen? Hier finden Sie alles über die optimale Konfiguration und Einbindung der Box in Ihr Heimnetz.

Lernen Sie, wie Sie für Ihre FRITZ!Box eine eigene Firmware entwickeln und mit inoffiziellen Eingriffen um neue Funktionen erweitern.

Verbinden Sie sich sicher von jedem Ort der Welt mit Ihrem Heimnetz: Hier finden Sie das Wissen, wie Sie einen Fernzugang via VPN einrichten. Und mit ein paar Tricks machen Sie aus Ihrer FRITZ!Box einen von überall erreichbaren FRITZ!-Server.

Nutzen Sie die USB-Schnittstelle der FRITZ!Box für den Anschluss einer externen USB-Festplatte, und die Datensicherung wird für alle Computer in Ihrem WLAN zum Kinderspiel. Wenn Sie immer schon wissen wollten, was wirklich in Ihrer FRITZ!Box steckt, liegen Sie mit diesem Buch genau richtig!

Aus dem Inhalt:

9 783645 601504

25,– EUR [D]

ISBN 978-3-645-60150-4