

Anschlussinhaber vs. WLAN-Router

2011-08-27 13:08:56 Steffen Heintsch

14:35 Uhr

Wie das Onlinemagazin Gulli.com unmissverständlich in seinem Artikel vom 20.08.2011: "[Zahlreiche WLAN-Router unsicher: Standardpasswörter leicht zu erraten](#)" berichtet, sind Standardpasswörter oder vom Werk voreingestellte Passwörter leicht zu erraten und stellen ein Sicherheitsrisiko für den betreffenden Anschlussinhaber dar. Nicht nur für einen Abgemahnten hinsichtlich einer vermeintlichen Urheberrechtsverletzung über ein P2P-Netzwerkwerk ist diese Aussage von Interesse, sondern für jeden Inhaber eines Internetzuganges mittels WLAN-Router.

Abb. Aktuelles Beispiel: WLAN-Experiment

SSID	Authentifizierung	Hersteller
	WPA2-Personal	devolo AG
	WPA-Personal	AVM GmbH
	WPA-Personal	Shanghai DoreGlobal Technologies Co., Ltd.
	WPA2-Personal	AVM GmbH
	WPA-Personal	Arcadyan Technology Corporation
D-link430	WPA2-Personal	D-LINK INTERNATIONAL PTE LIMITED
EasyBox 497738	WPA2-Personal	Arcadyan Technology Corporation
EasyBox 792021	WPA2-Personal	Arcadyan Technology Corporation
EasyBox 894044	WPA2-Personal	Arcadyan Technology Corporation
	WPA2-Personal	AVM GmbH
	Offen	ZyXEL Communications Corporation
	Offen	ZyXEL Communications Corporation
FritzBox Fon WLAN 7112	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7112	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7112	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7113	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7113	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7113	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7141	WPA-Personal	AVM GmbH
FritzBox Fon WLAN 7170	WPA2-Personal	AVM GmbH
FritzBox Fon WLAN 7220	WPA2-Personal	AVM GmbH
	WPA-Personal	Arcadyan Technology Corporation
	WPA-Personal	D-Link Corporation
	WPA2-Personal	D-LINK INTERNATIONAL PTE LIMITED
	WPA2-Personal	AVM GmbH
	WPA2-Personal	devolo AG
	WPA2-Personal	D-Link Corporation
	WPA2-Personal	Arcadyan Technology Corporation
	WPA2-Personal	D-Link Corporation
NTGR_wdkWngTQWZQPQX	WPA2-Personal	NETGEAR
	Offen	ZyXEL Communications Corporation
	Offen	Arcadyan Technology Corporation
	Offen	ZyXEL Communications Corporation
	WPA2-Personal	AVM GmbH
WLAN-0060ED8507	WPA2-Personal	AVM GmbH
WLAN-001CA428596	WPA2-Personal	AVM GmbH
WLAN-203384	WPA2-Personal	Arcadyan Technology Corporation
WLAN-378493	WPA2-Personal	Arcadyan Technology Corporation
WLAN-4C3A30	WPA2-Personal	Arcadyan Technology Corporation
WLAN-R07719	WPA2-Personal	Arcadyan Technology Corporation

zum Vergrößern bitte auf's Bild klicken

Gerade das unwissentliche Betreiben eines offenen WLAN-Internetzugang sowie die Verwendung von Standardpasswörter oder vom Werk voreingestellte Passwörter bergen die Gefahren, dass ein unbekannter Dritter den Internetzugang Fremdbenutzen kann und der betreffende Anschlussinhaber, trotz, dass er selbst kein Filesharing betreibt oder Filesharing-Software installiert hat, abgemahnt werden kann wegen eines Urheberrechtsverstoßes über ein P2P-Netzwerk. Unwissenheit schützt nicht vor Strafe und der Inhaber eines Internetzuganges kann für eine Urheberrechtsverletzung haftbar gemacht werden, eines bekannten bzw. unbekannten Dritten, wenn die Prüfpflichten verletzt werden.

OLG Köln, Beschluss vom 22.07.2011, Az. 6 U 208/10

[...]Als Störer haftet, wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt (BGH, [GRUR 2010, 633 Tz. 19](#) – Sommer unseres Lebens mW.N.). Diese Voraussetzungen hat der Beklagte bereits dadurch erfüllt, dass er einen Internetanschluss eingerichtet hat. Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers allerdings zusätzlich die Verletzung von Pflichten voraus, deren Umfang sich danach bestimmt, ob und inwieweit der als Störer in Anspruch Genommene nach den Umständen eine Prüfung zuzumuten ist (BGH, ebd.).[...]

In dem heutigen Artikel wollen wir uns mit dem Thema: WLAN-Router und Passworteinstellung beschäftigen. Die regelmäßige Rechtsprechung in Klageverfahren ist mittlerweile eindeutig. So haben die Bundesrichter in Ihrer Entscheidung "[Sommer unseres Lebens](#)" sinngemäß festgelegt:

"Die Prüfpflicht des Anschlussinhabers bezieht sich aber auf die Einhaltung der im Kaufzeitpunkt des Routers für den privaten Bereich marktüblichen Sicherungen. Er hat nach dem Anschluss des WLAN-Routers die werkseitigen Standardsicherheitseinstellungen an seinen Gegebenheiten anzupassen und für den Zugang zum WLAN-Router ein persönliches, ausreichend langes und sicheres Passwort zu vergeben. Der Schutz von Computern, Kundenkonten im Internet und Netzwerken durch individuelle Passwörter gehörte auch Mitte 2006 bereits zum Mindeststandard privater Computernutzung und lag schon im vitalen Eigeninteresse aller berechtigten Nutzer. Sie war auch mit keinen Mehrkosten verbunden."

Die Initiative AW3P hat sich mit einem befreundeten Systemadministrator zusammengesetzt und anhand von gängigen WLAN-Router der Modellreihe "FritzBox" i.V.m. "dLAN Wireless extender" und "Speedport" eine Art Checkliste zusammengestellt, in der aufgezeigt wird, was ein Anschlussinhaber, nach Inbetriebnahme des WLAN-Routers, beachten sollte. Natürlich kann auch jeder andere Anschlussinhaber hier überprüfen, ob er die notwendigen Einstellungen vorgenommen hat. Es soll nicht als Bevormundung oder Schikane verstanden werden, sondern als Hilfsmittel, was muss ein Anschlussinhaber eines Internetzuganges über einen WLAN-Router beachten!

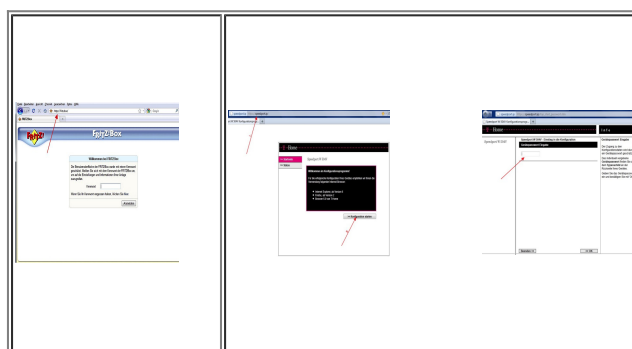
Hinweis

- ⇒ Bitte zum Lesen bzw. Vergrößern der Bilder, diese mit der linken Maustaste anklicken.
 - ⇒ Studieren Sie hierzu ausführlich das Handbuch bzw. Bedienungsanleitung Ihres persönlichen WLAN-Routers, falls es zu Abweichungen hinsichtlich Ihres Modells kommt.
-

Checkliste Konfiguration Router und WLAN

1. Wie kann ich auf die Konfiguration des Routers zugreifen?

Öffnen Sie den Browser Ihres Vertrauens und tippen Sie im Adressbereich ein: ***http://fritzbox/*** oder ***http://speedport.ip/*** (bzw. über die Router-IP: ***http://192.168.2.1.***). Dieses funktioniert On- wie Offline.

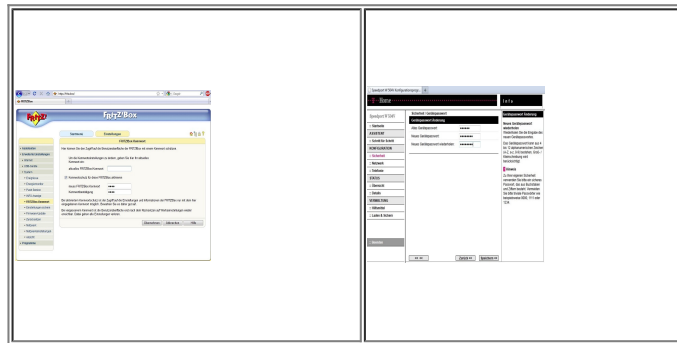


zum Vergrößern bitte auf's Bild klicken

2. Passwort/Kennwort WLAN-Router aktivieren bzw. ändern

⇒ Nicht das Standardpasswort bzw. die Werkseinstellung verwenden!

⇒ **Password-Check**



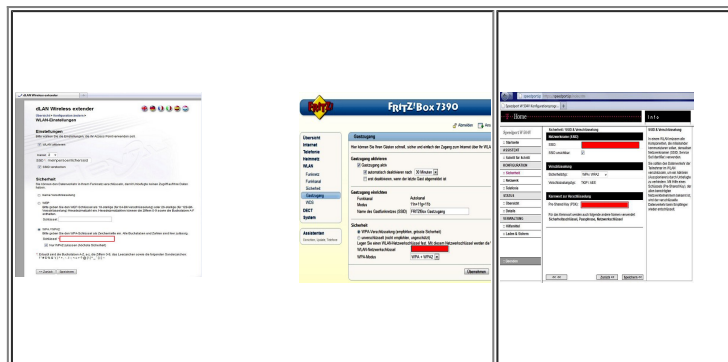
zum Vergrößern bitte auf's Bild klicken

3. Passwort WLAN ändern

⇒ Keine unsicheren Passwörter bzw. die Werkseinstellung verwenden!

⇒ Kanzlei Wilde, Beuger & Solmecke: **Ein unsicheres WLAN Passwort kann schon nach sechs Minuten geknackt werden**

⇒ Freeware: **WLAN-Keygen**

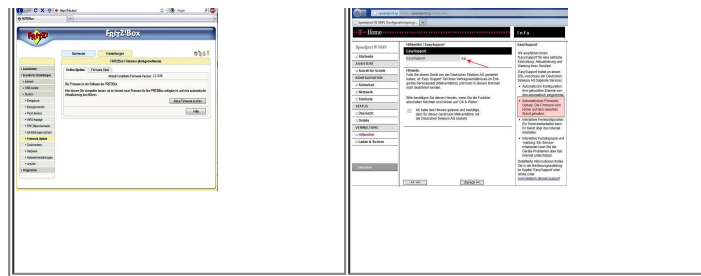


zum Vergrößern bitte auf's Bild klicken

Zusätzliche Empfehlungen und mögliche sinnvolle Einstellungen

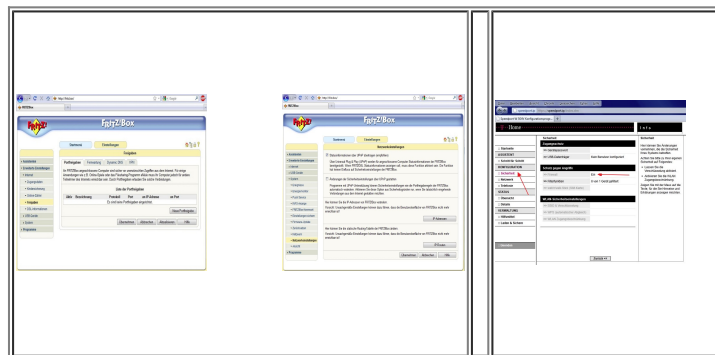
4. Firmware aktuell? Auf WWW-Seite des Herstellers informieren!





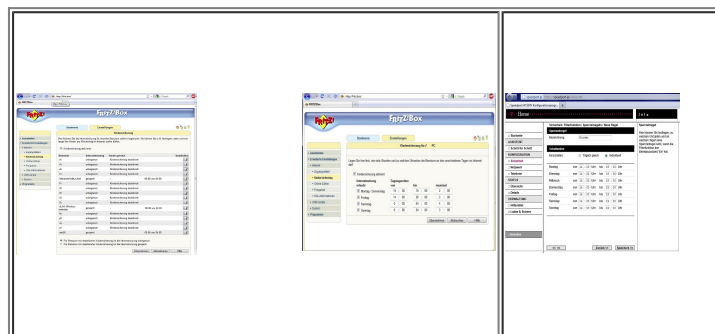
zum Vergrößern bitte auf's Bild klicken

5. Ist mein Firewall zu?



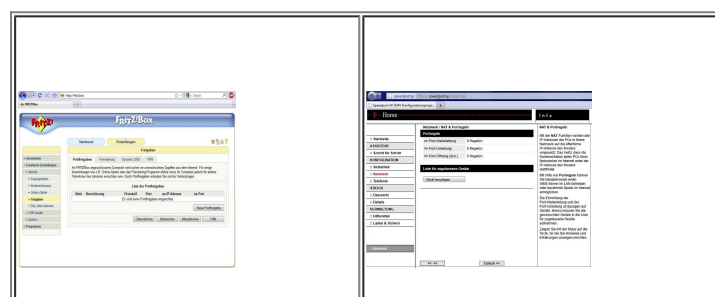
zum Vergrößern bitte auf's Bild klicken

6. Kindersicherung aktivieren und einrichten (beim Speedport über Filterregeln)



zum Vergrößern bitte auf's Bild klicken

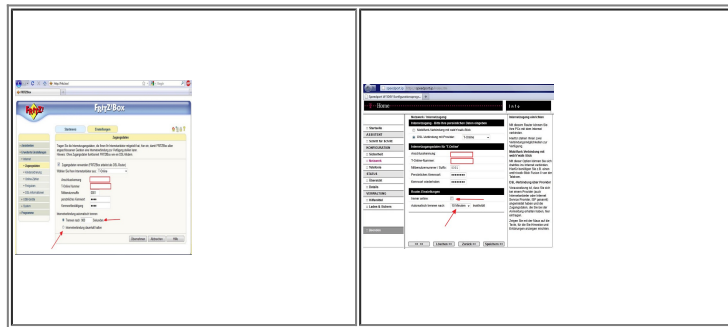
7. Portfreigabe



zum Vergrößern bitte auf's Bild klicken

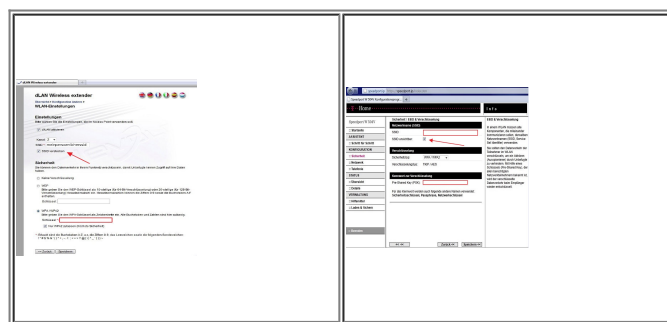
8. Schalter <Immer Online> deaktivieren (wo möglich)

⇒ Der Schalter "Internetverbindung automatisch trennen" bewirkt, dass z.B. nach 900 Sekunden/10 min die Internetverbindung getrennt wird, wenn keine Daten mehr mit dem Internet ausgetauscht werden. Wenn wieder Daten fließen, wird die Internetverbindung erneut aufgebaut und man erhält immer eine neue IP. Jedenfalls bei der Telekom.



zum Vergrößern bitte auf's Bild klicken

9. WLAN: SSID definieren, wenn möglich verstecken, maximale Verschlüsselung angeben

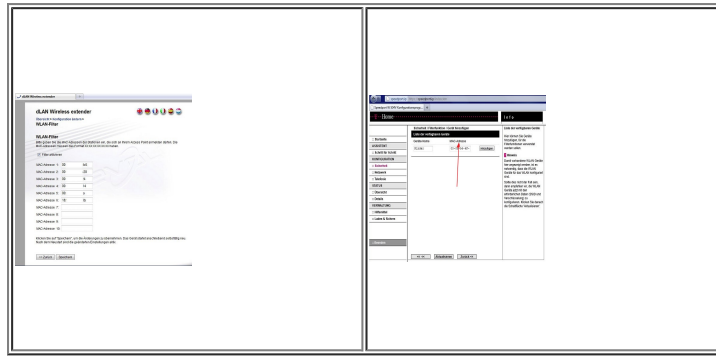


zum Vergrößern bitte auf's Bild klicken

10. WLAN: MAC-Filter aktivieren

⇒ Das bedeutet, nur Geräte mit den eingetragenen Adressen der WLAN-Karte können das Netzwerk nutzen!

Hinweis: Zum Anschließen neuer WLAN-Geräte ist es zweckmäßig, den SSID kurzfristig sichtbar zu machen, das WLAN-Gerät ins Netz einzubinden, dessen MAC-Adresse in den Filter einzutragen und abschließend den SSID wieder zu verstecken!!!!



zum Vergrößern bitte auf's Bild klicken

Sicherlich sollte man sich nach den Hinweisen und Anleitungen in den Beschreibungen des eigenen Routers halten und diese kurze Checkliste – als das Nötigste – ansehen. Die Anforderungen an den Anschlussinhaber hinsichtlich zumutbarer Prüfpflichten werden stetig zunehmen, sodass es von Vorteil ist, die empfohlenen Einstellungen schon heute zu übernehmen.

SH für die Initiative AW3P

.....

 Like  One like. [Sign Up](#) to see what your friend