Nieuwe router? Doe dit!

Rein de Jong

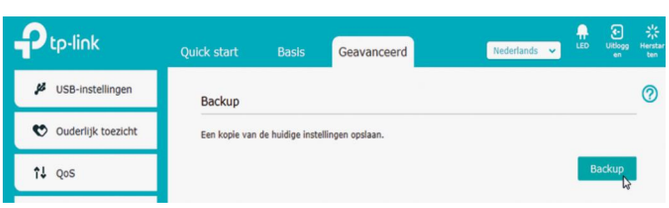
Acht dingen om te doen na het aansluiten van een nieuwe router

Een router wordt vervangen wanneer je overstapt naar een andere provider, of bij een defect, of wanneer je zelf kiest voor meer of betere functionaliteit, zoals een hogere wifi-snelheid, VoIP- of VPN-functies. Vaak wordt de nieuwe router door een monteur geïnstalleerd. De meeste mensen denken dan dat de monteur het allemaal wel goed ingesteld zal hebben. Helaas is dat vaak niet het geval. De monteur wil in zo weinig mogelijk tijd een werkend geheel opleveren en aan veiligheid wordt dan onvoldoende gedacht. Daardoor staat alles standaard ingesteld, en dat is meestal onveilig.
Genoeg redenen om zelf 'in de router te duiken' en je ervan te overtuigen dat de instellingen goed staan.

Bij de grote hoeveelheid instellingen zien veel gebruikers door de bomen het bos niet meer en laten ze het dus maar zo. Bovendien is het 'o, zo makkelijk' om een instelling over het hoofd te zien … en hoe was de oude router ook al weer ingesteld? Dat weet je vaak niet meer.
Een paar minuten, meer is er vaak niet nodig om een aantal belangrijke instellingen aan te passen. Dat behoedt je voor veel ellende nadien. De meeste wifi-routers zijn onvoldoende veilig geconfigureerd. Controleren dus!

1. Wat te doen?

Hoewel ik schermafbeeldingen van verschillende routers toon, kan het (gelet op de grote hoeveelheid verschillende routers) zijn dat je de instellingen niet herkent voor je eigen router. Raadpleeg dan de (online) handleiding om de diverse instellingen, die ik hieronder noem, terug te kunnen vinden. Als je de bedoelde instellingen niet direct vindt, moet je mogelijk eerst de geavanceerde instellingen inschakelen om toegang tot de genoemde opties te krijgen.



Voordat je ook maar iets in de instellingen wijzigt, is het wijs om eerst een back-up van de instellingen te maken. De meeste routers hebben daarvoor een optie die de instellingen wegschrijft naar een bestand. Gaat het dan ergens mis, dan kun je dat bestand, via de herstelmogelijkheid (Restore), weer terugschrijven naar de router. Bovendien is het verstandig om wijzigingen te noteren.

1.1 Wijzig het standaard wachtwoord

De meeste routers zijn ingesteld met een standaard gebruikersnaam en wachtwoord. Die wachtwoorden zijn makkelijk te achterhalen op het net. Er is zelfs een site[1] waar deze combinaties van gebruikersnaam en wachtwoord per fabrikant en type te achterhalen zijn. Vaak zal dat de combinatie *'admin/admin'* zijn.

Gelukkig zijn er routers waarbij je direct na de eerste inlog wordt gevraagd om je eigen wachtwoord in te stellen. Doe dat, voordat iemand anders het voor je doet.

1.2 Update de firmware

De firmware van de router is de software, het programma dat de router stuurt en de mogelijkheid biedt de router in te stellen. Deze software is opgeslagen in een geheugenbank en vormt het besturingssysteem van de router dat alles regelt, van de wifi tot de firewall.

Hoewel er niet zo vaak updates voor de firmware verschijnen, omdat deze in aard en structuur stabiel en veilig is (behoort te zijn), zijn er twee redenen om te kijken of de firmware bijgewerkt moet worden. Ten eerste weet je niet hoelang de router al op de plank heeft gestaan voor de aankoop. In de periode tussen fabricage en verkoop is de kans op een nieuwe firmwareversie groot. Daarnaast kunnen er, met het verstrijken van de tijd, steeds meer gaten en kwetsbaarheden in de firmware zijn ontdekt. Die gaten wil je dichten!

Daarom is het wijs om de nieuwste en veiligste firmware geïnstalleerd te hebben. Tevens beschik je dan over nieuwste mogelijkheden die de router biedt.

De firmware in de router wordt, op een enkele uitzondering na, niet automatisch geüpdated. Daarom is het verstandig om ééns in de zoveel tijd te controleren op updates. Er zijn routers die je via de mail kunnen waarschuwen dat er nieuwere firmware is en waarom die is uitgebracht.
Dat is o.a. bij de FRITZ!Boxen het geval. Doe dat dus!

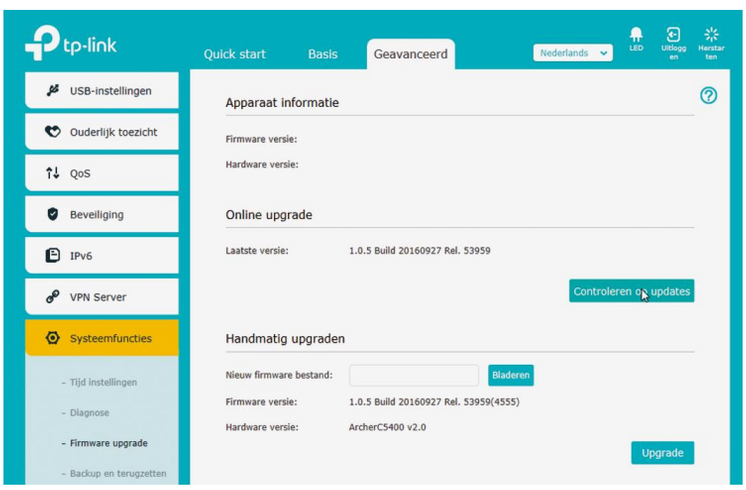
1.3 Wifi-netwerknaam aanpassen

De naam van je wifi-netwerk, meestal aangeduid als SSID (Service Set Identifier), kan veel bijzonderheden van de router onthullen. Heel vaak zijn, op basis van de string, merk en type van de router te herleiden zodat een aanvaller al weet welke router het betreft. Dat maakt het eenvoudiger om de standaard inlog en kwetsbaarheden te achterhalen.
Zo hebben meeste KPN Experiaboxen een SSID die begint met VGV.
Mijn advies is om de SSID te wijzigen in je initialen en huis-

nummer of je mailadres in pietjeATpukPUNTnl formaat, zodat buurtgenoten met je in overleg kunnen treden wanneer routers elkaar storen.

1.4 Wifi-wachtwoord wijzigen

Al jaren worden er routers uitgeleverd met maar matige wifi-instellingen en soms zelfs met een standaard wifi-wachtwoord. Gelukkig worden de meeste nieuwe routers wel uitgeleverd met het hoogste niveau van wifi-encryptie en een random wifi-wachtwoord. Vaak worden wifi-instellingen met een programma gegenereerd met behulp van een algoritme op basis van de SSID. Wanneer zo'n programma 'ontsnapt' dan zijn 'de rapen gaar'. Klanten van KPN hebben daar met de Experiaboxen last van gehad. Blokkeer daarom de mogelijkheid van de internetprovider om de router op afstand te configureren. Zo voorkom je dat providers onveilige instellingen terugplaatsen. Ondanks dat KPN de veiligheidsproblemen kende, deden ze dat doodleuk toch, waardoor de wijzigingen van klanten ongedaan werden gemaakt!



Daarom is het belangrijk om naast de SSID ook het standaard wifi-wachtwoord van de router aan te passen. Bij het wijzigen van het wifi-wachtwoord kom je instellingen tegen zoals WEP, WPA en WPA2. Kies dan voor WPA2 met AES versleuteling. AES is veiliger dan TKIP en belast de processor van de router minder. Mocht je nog oudere apparaten hebben die WPA2 nog steeds niet ondersteunen, overweeg dan of je die apparaten nog echt nodig hebt of zet een extra toegangspunt met een apart netwerk in voor die oude apparaten. Alles lager dan WPA2 is relatief eenvoudig te kraken. WEP is zo kinderlijk eenvoudig te kraken dat het eigenlijk niet meer thuis hoort op moderne routers.
Bij het kiezen van een wifi-wachtwoord moet je je realiseren dat lengte belangrijker is dan tekenset. Liever een wachtwoord als *'mijn OMA is ouder dan 90 en vitaal'* dan *'Pip0&kl#kkl#k'*. Zo'n lange zin is trouwens makkelijker te onthouden dan een gekunsteld wachtwoord. Leef je uit! Kun je geen lang wachtwoord bedenken of onthouden? Je mag het natuurlijk kopiëren en dan vier of vijf keer plakken in het wachtwoord.
Kijk ook of je het wachtwoord simpel en eenvoudig vanaf een smartphone in kunt tikken. Gebruik dus alleen tekens die op het standaard getoonde toetsenbord staan. Maar dan wel _echt_ lang. Alleen cijfers is ook afdoende, mits je er ten minste 36 gebruikt!
Het wifi-wachtwoord mag maximaal 63 tekens bevatten. Er komt een tijd dat zelfs dát niet genoeg is… Voor nu geldt: hoe langer, des te veiliger!

1.5 Wifi-kanaalnummer optimaliseren

Moderne routers kunnen tegelijkertijd een verbinding opzetten op zowel de 2,4 GHz- als de 5 GHz-band. Slecht bereik wordt vaak veroorzaakt door interferentie tussen naburige wifi-routers en andere apparatuur die op dezelfde of overlappende kanalen uitzenden. Het onderling storen kun je op de 2,4 GHz band beperken door alleen de niet overlappende kanalen 1, 6 en 11 te gebruiken. Gebruik jij 1, laat dan je naaste buren 6 respectievelijk 11 gebruiken. Is er geen vrij kanaal 1, 6 of 11, kies dan uit deze drie het kanaal dat het minst sterk is. Moderne routers onderhandelen dan samen over de optimale mix. Vergeet de kanalen boven de 11. Deze zijn exotisch, waardoor niet elk apparaat daarmee kan omgaan. De kanalen 2, 3, 4, 13 en 14 veroorzaken interferentie met het Bluetooth-signaal.

De 5 GHz band beschikt over 24 niet-overlappende kanalen, waardoor er meer ruimte is om een ongestoorde wifi-verbinding te kunnen kiezen. Alleen al daarom verdient de 5 GHz-band de voorkeur.

1.6 Gastnetwerk instellen

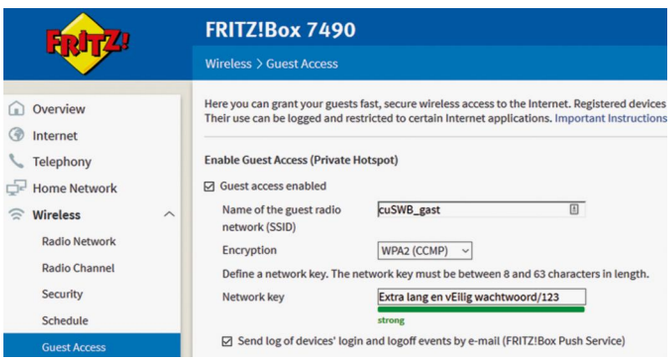
Het veiligst is het om helemaal geen wifi te gebruiken of te werken met wifi op een apart toegangspunt dat niet op het hoofdnetwerk kan. Je biedt dan je gasten en je eigen mobiele apparaten toegang, maar ze kunnen niet op het hoofdthuisnetwerk komen. Zo zijn je gedeelde netwerkmappen en andere gevoelige data ontoegankelijk voor gebruikers van het gastnetwerk. Vaak kun je ook de bandbreedte of de toepassingen (op basis van poortnummer) die het gastnetwerk mogen gebruiken, beperken. Dan word je niet gestoord in je bezigheden op het hoofdnetwerk. Let wel! Je gastnetwerk moet net zo goed beveiligd zijn als je hoofdnetwerk. Dus WPA2 en een eigen, lange wifi-sleutel. Anders heb je kans dat er allerlei gegevens die veilig horen te zijn onversleuteld door de lucht gaan.

Een aantal routers voorziet standaard in een gastnetwerk. Gebruik dat dan ook voor je gasten en voor je eigen mobiele spullen die niet op het hoofdnetwerk hoeven. Een bedrade netwerkverbinding heeft nog steeds de voorkeur. Zowel wat snelheid betreft, alsook uit veiligheidsoverwegingen. Je netwerkkabels steken immers niet, zoals wifi, buiten je huis uit.

Let op met de routers van Linksys en Belkin. Er zijn problemen met de isolatie en encryptie van hun gastnetwerk. Heb je een router van een van die merken, google dan of jouw router die problemen heeft en hoe je die zou kunnen oplossen.

1.7 Toegang op afstand uitzetten

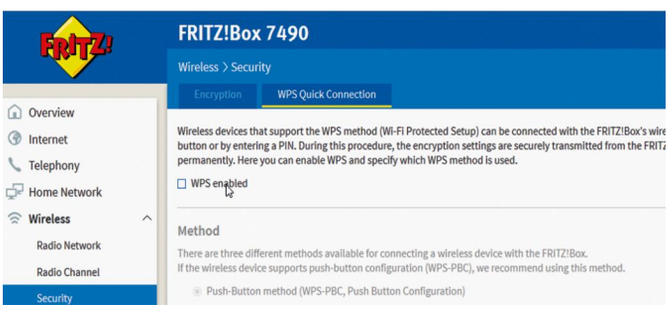
Het kan heel handig zijn om van buitenaf je router te kunnen configureren. Voor de meerderheid van de thuisgebruikers is dit een volstrekt overbodige functie. Het uitschakelen van die mogelijkheid, meestal 'Remote access' genoemd, maakt je netwerk minder kwetsbaar. De router is immers niet alleen je 'netwerkregelneef', maar ook je firewall naar buiten. Wanneer een aanvaller van buiten op je router kan komen, kan deze ook de firewall uitschakelen en zo volledige toegang krijgen tot je thuisnetwerk.



Gelukkig nemen routerfabrikanten hun standaard instellingen steeds meer serieus en je zou dus ook wel eens aangenaam verrast kunnen zijn dat toegang op afstand al is uitgeschakeld. Maar blijf deze instellingen controleren. Ook na een firmware-update.
AVM heeft op de nieuwere FRITZ!Boxen een optie die je, bij bepaalde wijzigingen, verplicht een fysieke actie uit te voeren via een aangesloten telefoon of het indrukken van een bepaalde knop op de router. Dat heeft als voordeel dat hackers op afstand niets kunnen: je moet fysiek aanwezig zijn.

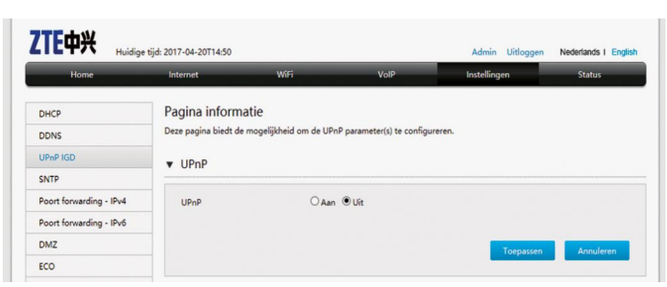
1.8 Schakel WPS en UPnP uit
Voorgaande instellingen zijn redelijk helder. De meeste mensen zullen de betekenis herkennen. Echter, Wifi Protected Setup (WPS) en met name Universal Plug and Play (UPnP) zijn wat minder bekende begrippen. Beide zijn bedoeld om ons het leven makkelijker te maken. Alleen hebben deze twee technieken helaas verschillende beveiligingsfouten.

WPS is de methode om met een knop op de router, of met behulp van een pincode, nieuwe draadloze apparaten op een simpele wijze toegang te geven tot de router. De gebrekkige WPS-implementatie met de pincode weegt niet op tegen het gebruiksgemak. Er is ook een WPS-methode met behulp van een knop. Die methode is wel 'veilig'. Wanneer je die separaat kunt instellen, is WPS 'veilig' te gebruiken.
Zo niet, zet het dan uit en koppel je draadloze apparaten op basis van SSID en invoer van het wifi-wachtwoord.



Mocht je een draadloze printer willen aansluiten of een apparaat waarvan het wachtwoord lastig is in te voeren, zet WPS dan alleen voor de installatie even aan en direct daarna weer uit.

UPnP is relatief onbekend. In tegenstelling tot WPS is dit in theorie veel nuttiger. Het zorgt voor het automatisch openen van poorten in de router wanneer een applicatie als Skype of een online spelletje dat vraagt. Helaas kan het ook hackers toegang tot de router geven en dát wil je niet. Controleer via de instellingen van de router of UPnP aan staat. Zo ja? Uitzetten! Heb je desondanks open poorten nodig? Open die dan handmatig.



Interessant was een uitzending van Opgelicht?!, over het onbewust delen van bestanden doordat UPnP aanstaat[2].
UPnP is in het hele netwerk onnodig. Het is zelfs hinderlijk dat allerlei ongewenste apparaten in de netwerkmap worden getoond. Het programma van Steve Gibson (UNpnp.exe)[3] schakelt het ook onder Windows 10 uit. UNpnp.exe schakelt de Windowsondersteuning voor UPnP uit door de service UPnP Device Host uit te schakelen.
Het kan zijn dat je antivirusprogramma het programma UNpnp.exe onterecht blokkeert. Is dat zo? Schakel dan de realtime-beveiliging van je antivirusprogramma even uit, download UNpnp.exe en voer het uit. Schakel daarna de beveiliging van je antivirus weer in.
Zij die weten hoe je handmatig een service via *Configuratiescherm* > *Services uitschakelt*, (niet op Handmatig zetten) hebben het programma UNpnp.exe niet nodig.

2. Tot slot

Kun je de juiste instellingen voor jouw specifieke router en provider niet vinden, zoek die dan met een zoekmachine. Voorbeeld: de zoektermen *'router uitschakelen UPnP'* gevolgd door het merk en type van je router, geeft vast een stappenplan. Bekijk dat bij voorkeur op de site van de routerleverancier of die van je provider.

In het algemeen is het een goed idee om op de router alles uit te schakelen wat je niet nodig hebt. Twijfel je na zoeken op internet nog steeds bij een instelling? Schakel die dan uit (en noteer het). Kijk na een week of alles nog steeds goed werkt en laat het dan uit. Vervolgens kun je een tweede twijfelgeval uitzetten. En zo verder. Ook hier kan Google je helpen informatie te vinden.
Denk hierbij aan VoIP, Ongebruikte USB-poorten, Media-server, NAS-functionaliteit en Poort-sharing.
Veel informatie kun je ook vinden op de site van security.nl[4].
En test eens, als het gaat om ongenode toegang, of je router veilig staat ingesteld. Test dat met behulp van ShieldsUp op deze site[5].

Ben je tevreden met de instellingen? Maak dan screenprints van de diverse router instellingen en maak van de instellingen een back-upbestand. Die laatste is niet voor mensen inzichtelijk en dient om de instellingen terug te kunnen plaatsen.

Denk je na het lezen van dit artikel dat dit allemaal onnodig is, lees dan het boek *'Er komt een vrouw bij de h@cker'*[6], geschreven door Maria Genova, een 'eenvoudige' internetgebruiker. Het is een leuk en leerzaam boek dat gemakkelijk wegleest.

Links:

Verkorte links kunnen je zomaar naar een onveilige site verwijzen. Wees dus voorzichtig! Testen kun je met www.urlunshortener.com of www.unshorten.it

1. Routerwachtwoorden	http://bit.ly/rtr-ww
2. Opgelicht?!	http://bit.ly/rtr_opg
3. UPnP uitzetten	http://bit.ly/rtr-unpnp
4. Security.nl	http://bit.ly/r-secnl
5. Router veilig?	http://bit.ly/r-shup
6. Komt een vrouw bij de h@cker	http://bit.ly/r-hcker
Dit artikel	http://reindejong.nl/routertips
Veiligheid op internet	http://reindejong.nl/veiligheid
Mijn eigen site	http://reindejong.nl