

DRAADLOOS NETWERK BEVEILIGEN

Inleiding:

Veel mensen die thuis draadloos internet via hun modem en/of router gebruiken hebben dit niet beveiligd met een wachtwoord.

Deze 'netwerken' zijn dus voor iedereen toegankelijk! Dat betekent niet alleen dat onbekenden via uw verbinding internetten, maar ook dat zij, met een beetje handigheid, uw computer kunnen doorsnuffelen, uw e-mails kunnen lezen, uw wachtwoorden kunnen zien, meekijken tijdens het internetbankieren of u zelfs van uw eigen netwerk af kunnen gooien! Het verstandigst is het natuurlijk om niet draadloos, maar met kabels te internetten. Maar genoeg mensen hebben goede redenen om wél draadloos te willen internetten (denk bijv. aan het niet kunnen of willen aanleggen van allerlei kabels door het hele huis of mensen die hun laptop overal in huis willen kunnen gebruiken.)

Daarom is het zeer verstandig om uw draadloos netwerk te beveiligen.

Dit lijkt moeilijker dan het is, het probleem alleen is dat elk merk modem of router een ander menu heeft waarin de instellingen moeten worden veranderd.

Het bij de hand hebben van de meegeleverde handleiding is daarom aan te raden.

Mocht u uw handleiding kwijt zijn dan kunt u proberen op internet via de website van de fabrikant een nieuwe te downloaden. Wanneer u de instellingen gaat veranderen is het verstandig de verbinding tussen het modem en computer te laten verlopen via een netwerkkabel en niet via de draadloze verbinding. Het veranderen van instellingen kan tot gevolg hebben dat u de draadloze verbinding tussen het modem en de computer verliest waardoor instellingen niet worden opgeslagen. Hernieuwde verbinding met het modem is als gevolg daarvan vaak niet meer mogelijk.

Uitleg over de verschillende manieren van beveiligen:

Er zijn verschillende manieren (technieken) om uw netwerk te beveiligen.

WEP, WPA (TKIP) en WPA2 (AES). Laat u niet afschrikken door deze termen;

De oudste methode om het netwerk te beveiligen is door middel van WEP.

In de praktijk blijkt de WEP versleuteling zeer eenvoudig te kraken.

Een draadloos netwerk beveiligen met WEP is niet echt aan te raden.

Maar wanneer uw draadloos netwerk apparatuur geen andere mogelijkheden biedt, is het beter WEP te gebruiken dan helemaal geen beveiliging.

Een meer recente standaard voor het beveiligen van een draadloos netwerk is WPA.

WPA heeft een aantal grote beveiligingsvoordelen t.o.v. WEP.

WPA gebruikt TKIP als encryptie (versleuteling).

Het wachtwoord is hierdoor lastig te kraken door hackers.

Nog moderner en veiliger is WPA2, op dit moment één van de veiligste manieren om uw netwerk te beveiligen. WPA2 gebruikt AES als encryptie (versleuteling).

Ook WPA2 is te kraken, zoals onlangs op een conventie in Amerika werd gedemonstreerd, maar het is wel zeer moeilijk.

WPA2-Mixed wil zeggen dat uw modem met zowel WPA als WPA2 om kan gaan (er kunnen dus ook pc's of laptops 'inloggen' die alleen met WPA werken)

Dus , afhankelijk van de mogelijkheden die uw modem biedt gecombineerd met de mogelijkheden die uw pc's en/of laptops aankunnen, kiest u voor de veiligste methode.

Instellingen aanpassen in modem:

Om de instellingen te kunnen aanpassen is het mogelijk om via Internet Explorer verbinding te maken met uw modem. Dit gaat als volgt;

Open Internet Explorer,

Zoek in de handleiding naar het IP-adres (nummer/adres) van uw modem.
Bijv. 192.168.1.245 of iets dergelijks.

Typ dit nummer in de adresbalk van Internet Explorer (daar waar www.blablabla.nl staat)
En druk op enter.

Er zal nu om een gebruikersnaam en een wachtwoord worden gevraagd.
De meeste modems hebben een standaard gebruikersnaam en wachtwoord (bijv: **admin**).
Dit is wederom terug te vinden in de handleiding.

Zodra deze gegevens juist zijn ingevoerd komt u in het hoofdmenu van uw modem.

Hier ergens kunt u de beveiliging instellen, dit kunt u vinden onder bijvoorbeeld:
Draadloze instelling → Beveiliging
Kijk voor de exacte locatie van deze instellingen in uw handleiding.

Instellen van de beveiliging:

U stelt het modem in op WEP, WPA, WPA2 of evt. WPA-Mixed.

U typt bij 'Passphrase' of 'Sleutel' een wachtwoord naar keuze in.
Kies een sterk wachtwoord; gebruik het liefst zowel letters als cijfers, neem minimaal 8 tekens (tip: verander letters in cijfers, 'Wachtwoord' wordt dan 'W8chtw00rd' en 'Gezellig' wordt 'G3z3ll1g'). Onthoud dit wachtwoord want u moet het later op iedere pc of laptop die verbinding gaat maken (eenmalig) invoeren.

Klik op 'OK' of 'Toepassen' om de instellingen op te slaan.

Als u nu met uw computer verbinding probeert te maken met het draadloze netwerk zal de computer om het wachtwoord vragen, voer dit wachtwoord in het laat de computer de verbinding tot stand brengen.

U kunt nu eventuele kabels die u heeft gebruikt om het modem te configureren weer verwijderen.

Meer beveiligingsinstellingen:

Sommige van onderstaande handelingen zijn niet voor beginners, d.m.v. het aantal sterretjes (1-5) kunt u het moeilijkheidsniveau bekijken (= simpel / ***** = moeilijk).*

*

De meeste modems hebben een standaard gebruikersnaam en wachtwoord (bijv: **admin**). Dit is terug te vinden in de handleiding.

Zodra deze gegevens juist zijn ingevoerd komt u in het hoofdmenu van uw modem.

Het is belangrijk om in ieder geval het wachtwoord direct te wijzigen!

Soms kan ook de gebruikersnaam gewijzigd worden.

Deze standaard gebruikersnaam en wachtwoord zijn per merk op internet te vinden,

Dus dient u dit zo snel mogelijk te wijzigen.

Gebruik een sterk wachtwoord;

- min. 8 tekens
- zowel cijfers als letters
- liefst ook tekens als % * @ { ? + !

*

Ergens in het beveiligingsmenu van uw modem staat iets als 'SSID' of 'ESSID'.

Hierachter staat een naam (vaak de naam van de fabrikant bijv. 'SITECOM', 'LINKSYS' of 'SPEEDTOUCH'), dit is de naam van uw netwerk, aan de hand van deze naam kunnen hackers zien welk merk modem u gebruikt met de nodige risico's.

U kunt ervoor kiezen om deze naam te veranderen. Kies bijvoorbeeld een andere fabrikant (U hebt een SITECOM maar verandert de naam in SPEEDTOUCH).

**

Ook kunt u ervoor kiezen om de SSID (netwerknnaam) helemaal niet uit te zenden.

Daarmee voorkomt u dat het draadloos netwerk zich bekend maakt aan de buitenwereld.

Dit betekent wel dat u de SSID eenmalig op de computer moet aangeven met welk draadloos netwerk u verbinding wilt maken.

Met het programma 'Netstumbler' kunt u kijken op welke kanalen de draadloze netwerken in de omgeving uitzenden. Ga bij voorkeur niet op hetzelfde kanaal zitten als bijvoorbeeld uw buurman, maar kies een ander kanaal.

Als u de MAC-adressen van de pc's / laptops op het draadloze netwerk achterhaalt, kunt u d.m.v. 'MAC Adres Filter optie' precies welke pc's of laptops wel of niet verbinding mogen maken.

Uitleg:

Het *MAC-adres* kunt u op de volgende wijze achterhalen:

Als eerste start u een DOS venster op:

U gaat naar **Start / Uitvoeren** en typt in **command** (of **cmd**). En klik hierna op **OK**.

Er verschijnt een zwart venster. Hier typt u **ipconfig /all**.

Als uitkomst krijgt u bij uw draadloze netwerkverbinding een fysiek adres te zien.

Dit is het MAC adres wat u kunt noteren (xx-xx-xx-xx-xx-xx).

Wanneer nieuwe firmware beschikbaar is voor uw modem/router kunt u die downloaden naar uw computer. Raadpleeg de handleiding van uw modem/router om erachter te komen hoe u de firmware van uw modem/router kunt updaten. Hou er rekening mee dat bij het updaten van firmware doorgaans alle instellingen verloren gaan. Het is dan ook aan te raden notities te maken van instellingen voordat u de firmware gaat updaten.

Copyright 2009 www.pcbeveiligen.nl

Niets uit deze uitgave mag worden verspreid of gekopieerd zonder behoud van de oorspronkelijke bronvermelding (www.pcbeveiligen.nl)