

Een draadloos netwerk beveiligen

Introductie

Een draadloos netwerk beveiligen is een stap die mensen vaak achterwege laten bij het aanleggen van een draadloos netwerk. Veel mensen kopen de benodigde apparatuur, sluiten het aan, halen een schakelaar om en er is internet voor de hele buurt. Wireless G, speedboosters, WEP, WPA, encryptie en MAC adressen. Het zijn allemaal termen die weinigen van ons echt begrijpen. Dat is waarom een groot percentage van de draadloze toegangspunten in Nederland niet beveiligd is. Volgens diverse media zou het percentage draadloze netwerken zonder enige beveiliging rond de 50 a 60 procent liggen. Reden voor actie? Misschien.

In dit artikel beschrijf ik een aantal gevaren van draadloos internet en een aantal manieren om een draadloos thuisnetwerk te beveiligen. De voorbeelden in dit artikel komen uit Windows XP Professional met service pack 2. Als router is de Linksys WRT54G gebruikt. Dit artikel is echter ook nuttig voor mensen die een ander besturings-systeem of een andere router gebruiken. De methodes voor het beveiligen van een draadloos netwerk zijn algemeen en niet specifiek voor een bepaalde router of een bepaald besturings-systeem. Lezers met een ander type router zullen misschien wel even moeten zoeken waar in de router ze de instellingen kunnen doen die in dit artikel voor de Linksys WRT54G beschreven staan. Daarover zometeen meer..

Draadloos is kwetsbaar

De toegang tot een draadloos netwerk gaat via een wireless access point (ook wel WAP of AP). Binnen het bereik van het wireless access point kan een computer die voorzien is van een draadloze netwerkkaart toegang krijgen tot het draadloze netwerk. Voor een thuisgebruiker betekent dit dat bijvoorbeeld de burens toegang kunnen krijgen tot het draadloze netwerk. Ook voor bedrijven is het beveiligen van hun draadloos netwerk momenteel een zeer 'hot' onderwerp. In de VS en tegenwoordig ook in Nederland moeten bedrijven zich zelfs actief beschermen tegen 'war drivers'; Mensen die met een laptop met draadloze toegang rondrijden om (eventueel onbeveiligde) draadloze netwerken op te zoeken.

Als thuisgebruiker moet je zelf bepalen of je een draadloos netwerk wil beveiligen en hoe. Laat je het netwerk volledig open, dan zullen omwonenden dit snel merken, omdat hun draadloze netwerkkaarten het signaal van jouw draadloze router of AP kunnen ontvangen. Het is dan een kwestie van 2 (of 1, of zelfs géén!) muisklikken voordat ze op jouw internetverbinding surfen. Naast alleen surfen kan een ongewenste bezoeker ook toegang proberen te krijgen tot andere computers die gebruik maken van de draadloze router of AP. Als deze computers niet voorzien zijn van een firewall (beveiligingsprogramma) dan wordt het de inbreker allemaal wel erg gemakkelijk gemaakt. Is het voorgaande op jou van toepassing? Vrees niet en lees verder.

In de volgende pagina's ga ik in op de meest voorkomende vormen van het beveiligen van een draadloos netwerk. Hiervoor doen we instellingen op de draadloze netwerkrouter (Linksys WRT54G) en op de netwerkcomputers (XP pro SP2).

Encryptie op een draadloos netwerk

Met encryptie kun je een draadloos netwerk beveiligen. Encryptie, ofwel versleuteling, zorgt ervoor dat informatie die over het netwerk vliegt beschermd is door een sleutel. Weet je de sleutel, dan mag je meepraten. Weet je hem niet, dan kom je er niet op. Goed, dat is een wel erg versimpelde weergave van de werkelijkheid, maar het idee mag duidelijk zijn: informatie kun je beschermen met een wachtwoord of sleutel. Op een netwerk worden pakketjes die over het netwerk vliegen voorzien van zo'n sleutel (of eigenlijk: slot). De meeste routers zijn tegenwoordig standaard uitgerust met WEP encryptie en WPA encryptie. Beide varianten kennen subtypes die elk een verschillende mate van beveiliging geven.

WEP encryptie

WEP staat voor *Wired Equivalent Privacy*. WEP encryptie wordt door velen als te zwak gezien voor het beveiligen van een netwerk. Dat is niet onterecht. Een WEP sleutel is namelijk vrij gemakkelijk te kraken. Er zijn zelfs vrij downloadbare tools voor beschikbaar zoals WEPcrack, WEPdecrypt en Airsnort. Een WEP sleutel wordt aangemaakt op basis van een gedeelde sleutel die op elke computer hetzelfde is én een 'initialization vector'. De initialization vector of IV is bij WEP vrij kort, namelijk 24 bits. Dit betekent dat het relatief kort duurt voordat twee datapakketjes versleuteld zijn met dezelfde IV. Hierdoor reizen er om de zoveel tijd (afhankelijk van de drukte op het netwerk) pakketjes over het netwerk die op elkaar lijken. Door deze pakketjes op te vangen wordt het voor een hacker mogelijk om een gemeenschappelijke eigenschap te ontdekken: de netwerksleutel. En zo kan hij/zij toegang krijgen tot het netwerk. Daar komt nog bij dat de headers van pakketjes niet versleuteld worden door WEP. Ze zijn dus zo 'uit de lucht te plukken' door elke computer binnen het bereik van het access point.

WPA encryptie

WPA lost onder andere het 'zwakke headers' probleem van WEP op. WPA maakt gebruik van 'Autonomous Re-keying' of vrij vertaald 'zelfstandige hersleuteling'. Het Temporal Key Integrity Protocol (TKIP) van WPA verzint voor ieder pakketje een nieuwe unieke sleutel. In feite is TKIP de opvolger van WEP. Kort gezegd is de versleuteling van pakketjes bij WPA encryptie sterker en er wordt razendsnel automatisch van sleutel verwisseld. Dit maakt het moeilijk om van buitenaf de netwerksleutel te achterhalen. Een betere encryptievorm die je (nog) niet in elke router vindt (maar wel in de LinksysWRT54G) heet Advanced Encryption Standard (AES) of 'Rijndael'. Deze standaard is in 2001 door de Amerikaanse overheid als standaard aangenomen voor het beveiligen van gevoelige overheidsinformatie. AES is voorlopig de sterkste vorm van beveiliging, maar de thuisgebruiker doet het meestal met WEP of liever WPA met TKIP.

Op de volgende pagina's ga ik in op het instellen van WEP en WPA met TKIP of AES op de Linksys WRT54G draadloze router. De eerste échte stap om je netwerk te beveiligen dus

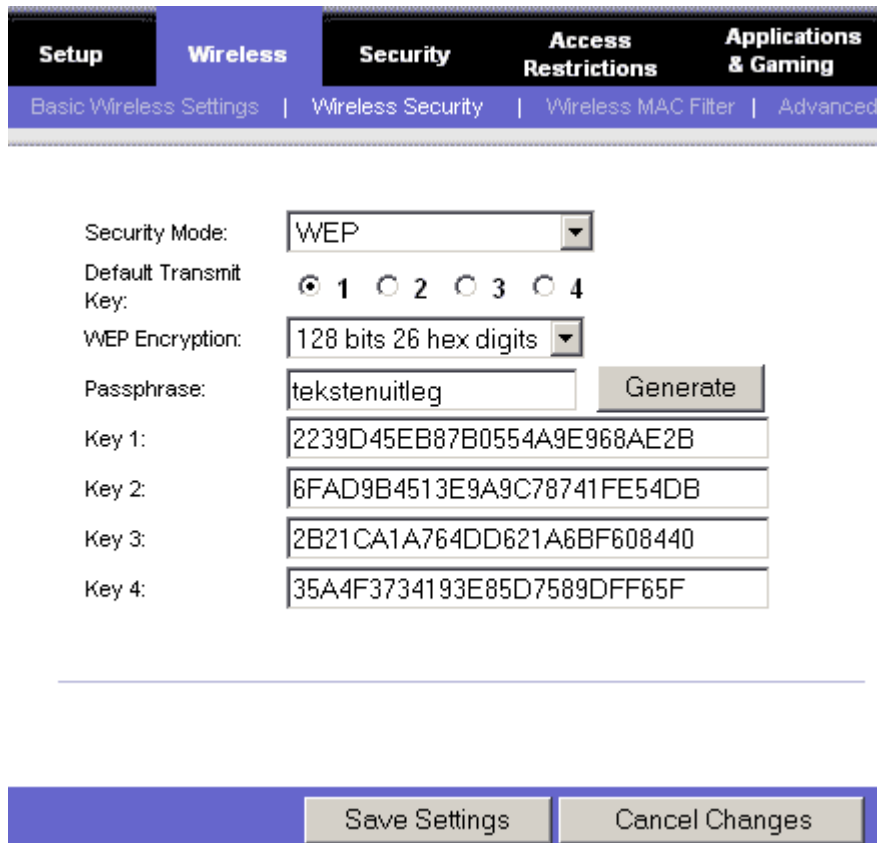
WEP encryptie instellen

Bij WEP encryptie wordt een 64 bits of een 128 bits sleutel gebruikt. Het instellen van WEP kan nogal verwarrend zijn. Daarom eerst een paar weetjes:

- 40 bits en 64 bits betekenen hetzelfde. WEP gebruikt een initialization vector (IV) van 24 bits. Dit is een stuk van de sleutel die niet door de gebruiker verzonden wordt. De ene fabrikant zet 40 bits (64 - 24) in zijn router, de andere 64 bits. Hetzelfde geldt voor 128 bit en 104 bit.
- Netwerkkarten die 128 bits WEP encryptie ondersteunen kunnen samenwerken met netwerkkarten die een 64 bits sleutel gebruiken, mits de 128 bits kaarten ook 64 bits encryptie ondersteunen.
- WEP sleutels kunnen verschillende vormen hebben: ASCII of hexadecimaal.

WEP encryptie instellen op de router

In de WRT54G router van Linksys zie je bij Wireless > Wireless Security de verschillende beveiligingsmogelijkheden. Je kunt hier onder andere WEP encryptie instellen.



Security Mode:

Default Transmit Key: 1 2 3 4

WEP Encryption:

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Je kunt in de Linksys router zelf een WEP sleutel genereren om je netwerk mee te beveiligen. Hieronder staat hoe. Het is echter eerst van belang dat je het SSID van het draadloze netwerk weet, omdat je dat zo nodig hebt om weer te verbinden na het instellen van WEP. Het SSID is de naam van het netwerk. Je vindt het in de Linksys WRT54G bij Wireless > Basic Wireless Settings. Schrijf het even op of onthoud het. In het geval van ons voorbeeld is het SSID "kazam". Je kunt nu met WEP aan de slag.

1. Je voert eerst een zinnetje naar keuze in, de passphrase. Dit zinnetje heeft verder geen betekenis, het wordt alleen gebruikt om een een sleutel mee te genereren. Klik op 'generate' en er verschijnen 4 sleutels. Je kunt kiezen tussen 64 bits en 128 bits WEP. Hoe groter de sleutel hoe veiliger, dus ik heb in het voorbeeld 128 bits gebruikt.
2. Copy-paste de eerste sleutel voor het gemak even naar een tekstbestandje (even Notepad openen) of schrijf hem op, want je hebt hem zo weer nodig.
3. Klik op 'save settings' om de instellingen te bewaren.

Note bene: de verbinding zal nu verbroken worden door de router. Je hebt immers niet de juiste netwerksleutel op je computer ingesteld, dus je krijgt geen verbinding met de router meer. Met andere woorden: het draadloos netwerk beveiligen is in elk geval gelukt. Nu nog zorgen dat je er zelf weer op komt.

WEP encryptie instellen op de computer

Nu is het zaak om de computer zo in te stellen dat-ie gebruik maakt van WEP encryptie en de juiste netwerksleutel. We doen dat hier in Windows XP met service pack 2. Dit is echter niet verplicht. Draadloze netwerkkaarten worden voor zover ik weet altijd met software geleverd om de netwerkverbindingen te beheren. Als je liever de software van de fabrikant gebruikt om je draadloze verbindingen te regelen doe je dat. De informatie die je in moet vullen om WEP in te stellen blijft hetzelfde.

1. Ga naar Start > Settings > Network Connections
2. Dubbelklik op de draadloze verbinding (wireless network connection). Als het goed is zie je nu het menu met de beschikbare draadloze netwerken. In de afbeelding hieronder is 'kazam' het netwerk in kwestie.



4. Klik op 'change advanced settings' linksonder in het raampje. Je krijgt nu een raampje met de



eigenschappen van de draadloze verbinding. Ga naar het tabblad 'Wireless Networks'. De netwerkver-

binding waarbij je nu WEP wil instellen kan voorzien zijn van een rood kruisje. Selecteer de juiste netwerkverbinding en kies 'properties' (eigenschappen).



5. Je ziet nu het scherm waar je encryptie voor het netwerk kan instellen. Bij Windows XP met Service Pack 2 ziet het er zo uit. Het juiste SSID staat als het goed is al ingevuld. Kies bij network authentication 'Open'. Kies bij Data encryption 'WEP'. In de twee lange velden kun je de netwerksleutel kwijt. Key index mag op 1 blijven staan. 'The key is provided to me automatically' moet uit staan en de onderste optie voor het opzetten van een ad-hoc verbinding moet ook uit staan.
6. Als dit ingesteld is klik je op OK. Als het goed is kun je nu verbinden met de router en heb je een met WEP beveiligde verbinding.

Tip: soms wil het niet in een keer lukken om te verbinden. Ik kwam erachter dat het soms helpt om de verbinding even helemaal te verwijderen en daarna opnieuw aan te maken. Je kunt dit doen in het bovenstaand raampje bij stap 3.

Opmerking: je hoeft deze instellingen niet per sé via de ingebouwde software van Windows te doen. Elke draadloze netwerkkaart die ik ken wordt geleverd met eigen software voor het beheren van verbindingen. Of je dit via Windows doet of via andere software, zoals die van de fabrikant, is aan jou. De principes en instellingen zijn in beide gevallen gelijk.

WPA encryptie instellen

De procedure om je draadloos netwerk te beveiligen met WPA encryptie (Wi-Fi Protected Access) lijkt op die van WEP encryptie. Voordat we de instellingen doen eerst nog wat weetjes

- WPA-PSK staat voor WPA Pre-Shared Key. Dit is een mechanisme voor het verzenden van sleutels tussen computers voor thuisgebruikers. In een professionele omgeving wordt vaak met een speciale server gewerkt die dit proces afhandelt (RADIUS server).
- Even herhalen: TKIP staat voor Temporal Key Integrity Protocol. TKIP is in feite het werkpaard achter WPA. TKIP zorgt voor de daadwerkelijke encryptie van de pakketjes die over het netwerk reizen.
- In het voorbeeld hieronder staat dus WPA-PSK / TKIP beveiliging ingesteld. Dit is momenteel voor thuisgebruikers de beste manier om een draadloos netwerk te beveiligen, omdat het veilig is en omdat het goed ondersteund wordt door verschillende fabrikanten. AES, een nieuwere en sterkere encryptievorm wordt minder vaak ondersteund, maar wel in de Linksys WRT54G router
- Windows XP met Service Pack 2 ondersteunt WPA, maar XP met SP1 niet. Gebruik je Windows XP met SP1 lees dan [dit artikel](#) over de WPA update voor Windows XP

WPA encryptie instellen op de router

In de WRT54G router van Linksys je bij Wireless > Wireless Security de verschillende beveiligingsmogelijkheden. Je kunt hier onder andere WPA encryptie instellen.

The screenshot shows the 'Wireless Security' configuration page in a Linksys WRT54G router. The navigation tabs at the top are 'Setup', 'Wireless', 'Security', 'Access Restrictions', and 'Applications & Gaming'. Under the 'Wireless' tab, there are sub-tabs for 'Basic Wireless Settings', 'Wireless Security', 'Wireless MAC Filter', and 'Advanced'. The 'Wireless Security' sub-tab is active. The configuration fields are as follows:

- Security Mode: WPA Pre-Shared Key (dropdown menu)
- WPA Algorithms: TKIP (dropdown menu)
- WPA Shared Key: WekjRLkskOSLKPeklaOPkleOSlp (text input field)
- Group Key Renewal: 3600 seconds (text input field)

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'.

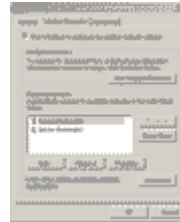
Selecteer zoals in het voorbeeld WPA-Pre-Shared Key en TKIP als algoritme. De WPA netwerksleutel mag (met de standaard firmware) tussen de 8 en 32 tekens lang zijn. Een langere sleutel is beter. Een sleutel die bestaat uit totaal onzin is veiliger dan een 'normale' en/of kortere zin. Zinnen in gewone mensentaal als sleutel zijn makkelijker te raden met behulp van een 'woordenboekaanval'. In het voorbeeld zie je een goede sleutel: 32 tekens lang en bestaande uit totaal willekeurige onzin. Vergeet niet om even op 'save settings' te klikken als je de instellingen hebt gedaan.

Note bene: de verbinding zal nu verbroken worden door de router. Je hebt immers niet de juiste netwerksleutel op je computer ingesteld, dus je krijgt geen verbinding met de router meer. Met andere woorden: het draadloos netwerk beveiligen is in elk geval gelukt. Nu nog zorgen dat je er zelf weer op komt.

WPA encryptie instellen op de computer

Nu is het zaak om de computer zo in te stellen dat-ie gebruik maakt van WPA encryptie en de juiste netwerksleutel.

1. Ga naar Start > Settings > Network Connections
2. Dubbelklik op de draadloze verbinding (wireless network connection). Als het goed is zie je nu het menu



met de beschikbare draadloze netwerken. In de afbeelding hieronder is 'kazam' het netwerk in kwestie.



3. Klik op 'change advanced settings' linksonder in het raampje. Je krijgt nu een raampje met de eigenschappen van de draadloze verbinding. Ga naar het tabblad 'Wireless Networks'. De netwerkverbinding



waarbij je nu WPA wil instellen kan voorzien zijn van een rood kruisje. Selecteer de juiste netwerkverbinding en kies 'properties' (eigenschappen).

4. Je ziet nu het scherm waar je encryptie voor het netwerk kan instellen. Bij Windows XP met Service

Pack 2 ziet het er zo uit: Het juiste SSID staat als het goed is al ingevuld. Kies bij network authentication 'WPA-PSK'. Kies bij Data encryption 'TKIP'. In de twee lange velden kun je de netwerksleutel kwijt.

5. Als dit ingesteld is klik je op OK. Als het goed is kun je nu verbinden met de router en heb je een met WPA beveiligde verbinding

MAC adressen filteren

MAC adressen filteren is een beveiligingsmethode die vaak in combinatie met encryptie gebruikt wordt. Een MAC adres (ook wel 'hardware adres' of 'fysiek adres' genoemd) is een ingebakken adres dat uniek is voor elk netwerkapparaat. Het MAC adres is een hexadecimale code van twaalf tekens, bijvoorbeeld 00-C0-26-A9-42-F7. Deze code kan gebruikt worden om toegang tot het netwerk toe te zeggen of juist te blokkeren. In feite is het erg gemakkelijk

1. Ga via je browser naar je router (type 192.168.1.1 in de adresbalk in geval van de WRT54G).
2. Ga naar de pagina Wireless > Wireless MAC filter en zet Wireless MAC Filter op 'enable'.

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming

Basic Wireless Settings | Wireless Security | **Wireless MAC Filter** | Advanced

Wireless MAC Filter: **Enable** **Disable**

Prevent: **Prevent** PCs listed from accessing the wireless network

Permit only: **Permit only** PCs listed to access the wireless network

Edit MAC Filter List

Save Settings | Cancel Changes

3. Je kunt nu kiezen tussen Prevent en Permit only. Als je prevent kiest dan kun je in de Mac filter lijst MAC adressen invullen die géén toegang tot het netwerk mogen hebben. Je gaat er dan vanuit dat iedereen mag verbinden, behalve de MAC adressen die jij opgeeft. Kies je voor Permit only, dan worden alléén de MAC adressen die jij invult toegelaten op het netwerk. Zo kun je dus per computer toegang verlenen.
4. Vul in de MAC filter lijst de MAC adressen in die je wilt blokkeren of juist toegang verlenen.

Hoe vind ik het MAC adres van mijn netwerkkaart(en)?

Ga in Windows XP of 2000 naar Start > Run (uitvoeren) > type 'cmd' > type 'ipconfig /all' in de prompt. Het MAC adres staat in het lijstje achter 'physical address' of 'fysiek adres'.

MAC adressen filteren is een beveiliging die vaak bovenop encryptie gebruikt wordt. Een combinatie van WPA TKIP met MAC adres filters is voor de thuisgebruiker een zéér degelijke beveiliging

SSID broadcast

Als SSID broadcast aan staat dan zendt het access point om de paar seconden de netwerknaam (SSID) uit. Zo worden computers in de buurt snel op de hoogte gesteld van het netwerk. SSID broadcast is handig in een omgeving waar computers snel van netwerk moeten kunnen wisselen. In een thuisnetwerk is dit meestal overbodig

Het is vanuit beveiligingsopzicht af te raden om SSID aan te zetten, want het SSID wordt onversleuteld uitgezonden. Het kan makkelijk opgepikt worden uit de lucht door een inbreker en die is daarmee weer een (klein) stapje dichterbij toegang tot het netwerk. In de Linksys WRT54G zet je SSID broadcast eenvoudig uit.

- Log in op de router (type 192.168.1.1 in de adresbalk van de browser en type het wachtwoord in. Standaard wachtwoord: admin)



- Ga naar Wireless > Basic Wireless Settings
- Zet SSID broadcast op 'disable'

Router wachtwoord

De router zelf kun je ook beveiligen met een wachtwoord. Draadloze routers hebben vaak een standaard wachtwoord als ze van de fabriek komen. Meestal admin of iets anders voor de hand liggends. Een goed router wachtwoord instellen is een must als je je draadloos netwerkje wil beveiligen. Het is in de Linksys WRT54G zo simpel dat ik er niet eens een plaatje aan ga wijden.

- Ga naar je router (open je browser, type 192.168.1.1 in de adresbalk) en log in met het standaard wachtwoord: admin. Je hoeft geen gebruikersnaam in te vullen.
- Ga naar de pagina Administration en vul daar een goed wachtwoord in. Het mag maximaal 32 tekens zijn en geen spaties bevatten. Hoe meer tekens je gebruikt, hoe moeilijker het wachtwoord te kraken is

• Conclusie

- Als je de instellingen uit dit artikel hebt gebruikt om je eigen draadloos netwerk te beveiligen dan kun je er van opaan dat het gros van de inbrekers 100 meter verder rijdt naar het volgende access point dat waarschijnlijk minder goed beveiligd is. De combinatie van
 - WPA encryptie
 - MAC filtering
 - SSID broadcast uit zetten
 - en een sterk router wachtwoord

is zeker voor de thuisgebruiker een gedegen arsenaal aan beveiligingsmaatregelen. De professional pleegt te zeggen dat een netwerk nooit veilig is, of dat je daar op zijn minst nooit vanuit mag gaan, maar als thuisgebruiker ben je met deze maatregelen goed beschermd