

WAT kunt U doen om uw draadloze netwerk TE BEVEILIGEN?

Om onbevoegden buiten de deur te houden kunt u uw netwerk op een aantal manieren beveiligen. Natuurlijk werkt slechts een van deze maatregelen alleen niet om je netwerk te beschermen: elke stap biedt weer net iets meer veiligheid.

DOEN!

- Schakel de uitzending van het 'naamkaartje' (SSID) van het accesspoint uit. Computers kunnen deze naam opvangen en zo verbinding maken met het accesspoint. Vaak is het handig om bij het instellen van het netwerk het uitzenden van de SSID aan te laten. Nadat alles goed werkt, is het echter aan te bevelen de uitzendingen uit te schakelen: uw eigen computer(s) kan de router wel vinden, maar voor anderen is uw netwerk niet direct zichtbaar.
- Wijzig het wachtwoord van uw accesspoint/ draadloze modem/ router. Zorg er in ieder geval voor dat dit niet meer het standaardwachtwoord is zoals ingesteld door de fabrikant. Op deze manier voorkomt u dat derden de configuratie van uw netwerk kunnen zien en kunnen aanpassen.
- Geef alle computers op uw netwerk een vast IP-adres en geef alleen deze adressen toegang tot uw router. Geef alleen de MAC-adressen van de netwerkkaart(en) van uw computer(s) toegang tot uw router.
- Beveilig uw draadloze netwerk met encryptie. Gebruik hiervoor Wi-Fi Protected Access (WPA of WPA2). Hiermee zorgt u ervoor dat anderen geen toegang krijgen tot uw draadloze netwerk

- en niet uw netwerkverkeer kunnen af luisteren. Als niet al uw apparaten WPA ondersteunen gebruik dan de sterkst beschikbare versie van WEP.
- Wijzig het wachtwoord van uw Access Point/ draadloze modem/router. Zorg er in ieder geval voor dat dit niet meer het standaardwachtwoord is zoals ingesteld door de fabrikant.
- Beveilig de computers op je netwerk met een blankvirusscanner, regelmatige blankupdates en een software firewall.
- Let bij het aanschaffen van apparatuur op dat minimaal WPA wordt ondersteund.

NIET DOEN!

- Er zijn verschillende manieren om een draadloos netwerk te beveiligen. Eenvoudige methoden zijn het "verbergen" van de naam (SSID) van het netwerk of alleen bekende computers toegang geven met behulp van het (mac-)adres van hun netwerkkaart. Dit haalt echter niet meer uit dan het weren van diegenen die uw netwerk, onder kwade bijbedoelingen, zouden willen gebruiken voor internettoegang. Vertrouw niet alleen op het verbergen van de SSID en toegang op basis van mac-adres!

Meer INFORMATIE

DIGIBEWUST

Digibewust informeert over de mogelijkheden maar ook over de gevaren van digitale middelen zoals internet. Op de website vindt u informatie over veilig internetten voor uzelf, uw kinderen en uw bedrijf. Kijk op www.digibewust.nl.

WAARSCHUWINGSDIENST.NL

Via de website kunt u zich aanmelden voor het ontvangen van waarschuwingen over de nieuwste computervirussen en lekken in software.

COLOFON

Dit is een uitgave van Digibewust, een samenwerkingsverband tussen overheid en bedrijfsleven om het veilig gebruik van internet en andere digitale middelen te vergroten.



Contactgegevens:
Postbus 262, 2260 AG Leidschendam
tel 070-4190309 – fax 070-4190650
www.digibewust.nl – info@digibewust.nl

©2007, Digibewust



WiFi=
Draadloos
Hoe beveiligt u uw draadloze netwerk?



Steeds meer mensen kiezen tegenwoordig voor een **DRAADLOOS NETWERK** (WiFi). Hiermee is het

mogelijk om vanuit iedere kamer, vanuit de luie stoel of vanuit de tuin te internetten. Makkelijk dus, zo **ZONDER KABELS**. Maar wees wel bewust van de mogelijke gevaren en risico's van een draadloos netwerk en ook van de **MAATREGELN** die u daar zelf tegen kunt nemen.

WAT is een **DRAADLOOS NETWERK**?

Simpel: een netwerk zonder kabels. Het enige wat u nodig heeft is een access point (meestal ingebouwd in uw (draadloze)modem of router) en een netwerkkaart of (USB) adapter voor uw computer. In een laptop is dit laatste vaak standaard ingebouwd. Dit draadloze netwerk kan door computers en andere apparaten, zoals spelcomputers en geluidsapparatuur, gebruikt worden om met elkaar en met internet te communiceren.

Een **access point** zorgt ervoor dat u draadloos verbinding kunt maken met uw router.

Een **modem** zorgt ervoor dat u verbinding kunt maken met het internet.

Een **router** is een apparaat dat voor een koppeling tussen uw internetverbinding en uw (thuis)netwerk (een of meerdere computers) zorgt.

Een **netwerkkaart** is een hardware-onderdeel in een computer, nodig om die computer deel te laten uitmaken van een computernetwerk.

Wat zijn de **MOGELIJKE GEVAREN?**

Een draadloos netwerk stopt niet bij uw voordeur of tuinhekje. Dat betekent dat, zonder extra beveiliging, iedere wildvreemde die zich in de buurt van uw woning bevindt toegang heeft tot uw netwerk. De indringer kan dan van uw internetverbinding gebruikmaken om bijvoorbeeld bestanden te downloaden, te e-mailen enzovoort. Heeft u een beperkt internetabonnement, dan zijn de kosten voor het dataverkeer van anderen voor u. Maar indringers kunnen mogelijk ook illegale activiteiten uitoefenen waar u, als

eigenaar van het draadloze netwerk, vervolgens voor verantwoordelijk kunt worden gehouden. Denk bijvoorbeeld aan het versturen van spam. En wanneer een onbekende eenmaal toegang heeft tot uw netwerk, kan hij misschien ook toegang krijgen tot de computers die aangesloten zijn op het netwerk en zo allerlei persoonlijke gegevens inzien, kopiëren en veranderen. Een goede beveiliging van uw draadloze netwerk is daarom noodzakelijk.

GEHEIMTAAL

Het gegevensverkeer op uw draadloze netwerk kunt u ook beveiligen door het te versleutelen (ook wel encryptie genoemd). Dat betekent simpelweg dat de zendende computer de gegevens die hij verstuurt omzet in een soort geheimtaal. Alleen de computer die de gegevens moet ontvangen heeft de code (ofwel sleutel) om deze geheimtaal leesbaar te maken. De gegevens die over uw draadloze netwerk verstuurd worden zijn zo onleesbaar voor onbevoegden.