

Courbois Software

Veilig Draadloos

Een draadloos netwerk is een computernetwerk waarbij de aangesloten apparaten niet via fysieke koperen kabels of glasvezelkabels communiceren, maar via elektromagnetische straling (radiosignalen). Op deze manier kun je overal in huis (en zelfs in de tuin) op internet surfen of bestanden van andere pc's opvragen. De belangrijkste draadloze technologie is Wi-Fi (lokaal netwerk).

Zo'n draadloos netwerk stopt niet precies bij je voordeur of je tuinhekje; ook de buren of toevallige voorbijgangers kunnen gebruik maken van zo'n draadloze verbinding. Daarom is het belangrijk, de verbinding te beveiligen. Dat betekent dat alleen mensen die het wachtwoord kennen, van de verbinding gebruik kunnen maken.

Veel mensen vergeten een draadloos netwerk te beveiligen, of ze hebben er gewoon geen zin in. Dan kan het gebeuren dat anderen gebruikmaken van de verbinding. Dat kan tot gevolg hebben dat je opeens je datalimiet bereikt hebt, terwijl je zelf niet veel downloadt. De verbinding kan ook veel trager worden, omdat die door meer mensen gebruikt wordt.

Gevaren

Als onbekenden stiekem gebruik maken van je verbinding, kan dat allerlei nare gevolgen hebben:

- Onbeveiligde netwerken worden soms gebruikt voor illegale activiteiten. Als dat via jouw verbinding gebeurt, ben jij daarvoor verantwoordelijk.
- Wanneer een onbekende eenmaal toegang heeft tot het netwerk, kan hij misschien ook toegang krijgen tot de andere computers in het netwerk en zo allerlei persoonlijke gegevens inzien, kopiëren en veranderen.
- Onbeveiligde wifi-netwerken worden vaak misbruikt om spam mee te versturen. Professionele spam-verstuurders rijden in auto's door buurten op zoek naar open netwerken. Wanneer ze die vinden, sturen ze in korte tijd miljoenen spammails via die verbinding.

Gevaar voorkomen

Het ongewild meesurfen van onbekenden kan eenvoudig vermeden worden, door het draadloos internet met WEP of WPA te beveiligen (in mindere mate het filteren van de MAC-adressen). Deze beveiligingen kunnen echter met geavanceerde software eenvoudig gekraakt worden. Er bestaat geen beveiligingsmethode die het netwerk even veilig als een conventioneel bedraad netwerk maakt. Hieronder worden verschillende beveiligingen opgesomd:

SSID

De naam van een netwerk wordt 'uitgezonden' door een draadloze router/modem. U kunt deze naam, ook wel SSID, verbergen. Om verbinding te maken met een netwerk dient de juiste SSID te worden opgegeven. Dus, wanneer deze SSID verborgen is, is de kans dat iemand verbinding maakt met uw netwerk aanzienlijk kleiner. Let wel: het uitschakelen van het uitzenden van de SSID is absoluut geen totale beveiligingsmethode, maar dient gezien te worden als een aanvulling op de beveiliging.

filteren MAC-adres

Iedere netwerkkaart, draadloos of niet, heeft een uniek MAC-'adres' (Media Access Control). Dit adres identificeert de betreffende kaart en is uniek; er bestaat maar 1 van. De meeste routers kunnen zo ingesteld worden dat uitsluitend netwerkkaarten met bepaalde MAC-adressen toegelaten worden op het netwerk.

Met bepaalde programma's kan het MAC-adres van een netwerkkaart echter aangepast worden, zodat het filteren van het MAC-adres niet een goede bescherming biedt. Het biedt wel een extra beveiliging bovenop een WEP- of WPA-versleuteling.

WEP-versleuteling

WEP-encryptie (Wired Equivalent Privacy) is een manier om de gegevens die over het draadloos netwerk verstuurd worden, te versleutelen. Hoewel deze versleuteling compatibel is met bijna elke router, wordt het gebruik ervan enigzins afgeraden: de beveiliging (met DES) is te zwak; de WEP-sleutel is eenvoudig te kraken. Hiervoor kunnen programma's als WEPcrack, WEPdecrypt en Aircrack-ng gebruikt worden.

WEP versleutelt door middel van een sleutel die wordt aangemaakt door een relatief korte (24 bits) initialization vector (startvector). Doordat deze vector niet lang genoeg is, duurt het niet lang voordat twee pakketjes met éénzelfde sleutel beveiligd werden. Op een druk netwerk zullen geregeld pakketjes rondgestuurd worden die met dezelfde sleutel zijn beveiligd. Met deze sleutel is het voor de hacker eenvoudig de netwerksleutel te ontdekken door het dataverkeer te onderscheppen.

In de meeste gevallen is een beveiliging met WEP voldoende (kies dan wel voor de 128 bits variant). Voor een grotere zekerheid kan overgegaan worden naar WPA.

Het nadeel van WEP is dat alleen de toegang tot de router wordt versleuteld. Het dataverkeer wordt niet versleuteld. Door het onderscheppen van de onversleutelde data, is het mogelijk de WEP sleutel te achterhalen en zo toegang tot het netwerk te verkrijgen. Dit werkt als volgt. Alle data wordt onversleuteld verzonden. Slechts een bepaald gedeelte van de data blijft hetzelfde, de wep-sleutel. Door genoeg data te ontvangen is de wep-sleutel te extraheren uit de onversleutelde data, immers, de wep-key blijft dezelfde. Dus is er in ieder dataverkeer steeds eenzelfde pakketje met dezelfde gegevens: de wep key.

WPA-versleuteling

WPA-encryptie maakt gebruik van 'Autonomous Rekeying', vrij vertaald 'zelfstandige versleuteling'. De versleuteling bij WPA is niet alleen sterker dan WEP, maar er wordt ook geregeld van sleutel gewisseld.

Deze beveiliging is veiliger dan de WEP-beveiliging, maar blijkt ook kraakbaar te zijn. De versleuteling wordt echter niet door alle routers en toebehoren aanvaard, kies eventueel een WPA-versleuteling. Een WPA-versleuteling is aan te bevelen boven een WEP versleuteling.

Gebruik een moeilijk te kraken wachtwoord

Elke beveiliging en versleuteling ten spijt is uw beveiligde netwerk weinig waard indien het wachtwoord eenvoudig te raden is. Besef dat het onheil meestal wordt aangericht door mensen uit uw omgeving (letterlijk te nemen), en dat die bijgevolg uw naam (en eventuele bijnamen of de naam van uw huisdier) weten. Verder is het mogelijk dat uw wachtwoord gekraakt wordt door alle mogelijkheden af te lopen. Om een veilig wachtwoord te kiezen, kiest u een wachtwoord van voldoende lengte (langer dan 6 tekens), dat niet voorkomt in een woordenboek (dus bijvoorbeeld niet 'zeehond'), en zorgt u dat er zowel letters, cijfers, als vreemde tekens (@,#,!,+) in voor komen. Verder vervangt u het wachtwoord geregeld.

Installeer een netwerkcontroleprogramma.

Indien u vermoedt dat vreemden op uw netwerk meesurfen, kunt u gespecialiseerde software installeren die de activiteit op het netwerk toont.

Conclusie

Gebruik minimaal een WPA versleuteling plus een mac-filter instelling indien u veilig wilt surfen. Op deze manier loopt u het minste risico op meesurfers. Let wel, hoe hoger de beveiliging, hoe beter het signaal van uw netwerk dient te zijn. Wanneer u een matige verbinding heeft en WPA gebruikt kan het zijn dat de verbinding wegvalt omdat, door de beveiliging, de sleutel niet goed overkomt.

Net als bij fietsslots geldt dat een perfect slot niet bestaat: alles is te kraken. Maar als je zorgt voor een goed slot / goede beveiliging is de kans groot dat kwaadwillenden aan je fiets of huis voorbij gaan en het ergens anders gaan proberen.: