Beveilig uw draadloos netwerk in vijf stappen

Firewalls en antivirustoepassingen worden intensief gebruikt om de internetbeveiliging te verhogen. De beveiliging van het draadloos (thuis)netwerk daarentegen wordt geregeld uit het oog verloren…

Een netwerk maakt het mogelijk om internettoegang en data te delen. Het is echter niet gewenst om dit met eender wie te doen. Om uw draadloos netwerk optimaal te beveiligen, hoeft u 5 stappen te volgen:

1) Verander de standaard Service Set Identifier (SSID)

De SSID is de naam van het netwerk. Draadloze toestellen krijgen tijdens de productie een standaard SSID toegekend. Hackers kennen dit en kunnen zo toegang krijgen tot het netwerk. Om dit te voorkomen moet je de SSID wijzigen in een unieke naam.

2) Voorkom uitzending van de SSID

De meeste draadloze toestellen zenden de SSID standaard uit. Het is beter dit te blokkeren zodat niet iedereen zomaar het netwerk kan betreden.

3) Verander het standaard paswoord

Draadloze producten als routers en toegangspunten zijn beveiligd met een paswoord om de instellingen te wijzigen.
Om hackers niet de mogelijkheid te geven in te loggen en uw netwerkinstellingen te wijzigen, verandert u best dit standaard paswoord in een persoonlijk paswoord.

4) Maak MAC adres filtering mogelijk

Ieder netwerktoestel heeft een uniek Media Access Control (MAC) adres. Routers maken MAC adres filtering mogelijk. Wanneer MAC adres filtering is ingeschakeld,worden enkel de toestellen met een specifiek MAC adres toegelaten op het netwerk.

5) Maak encryptie mogelijk

Encryptie laat toe om de gegevens die over het draadloos netwerk worden verstuurd te beschermen. Er zijn verschillende manieren om
te encrypteren:

- Met Wired Equivalency Protocol (WEP) worden gegevens gecodeerd door een sleutel voordat ze worden doorgezonden. Hoe langer de sleutel, hoe sterker de encryptie.
- Wi-Fi Protected Access (WPA) maakt gebruik van zogenaamde dynamic key encryption. De sleutel wijzigt constant,waardoor het nagenoeg onmogelijk wordt in het netwerk in te breken.

Er zijn twee versies van WPA met ieder een eigen authenticatieproces:

- **Thuisgebruik**: Temporal Key Integrity Protocol (TKIP) is een mechanisme dat de dynamische key encryption en wederzijdse authenticatie toepast. TKIP levert extra mogelijkheden die de beperkingen van WEP opvangen.
- **Gebruik in het bedrijf**: Extensible authentication Protocol (EAP) wordt toegepast voor berichtenuitwisseling tijdens het authenticatieproces. Het gebruikt 802.1x Server technologie om gebruikers te authenticeren via een RADIUS-server. Dit biedt industriële beveiliging,maar er is wel een RADIUSserver nodig.

WPA2 is de tweede generatie WPA. Het vereist Advanced Encryption Standard (AES) voor de encryptie van data, terwijl WPA Temporal Key Integrity Protocol (TKIP) gebruikt.