KPN Experia Box (TG789)
Standaard WPA/WPA2-beveiliging ingesteld

1 Beveiliging

1.1 Beveiliging instellen of wijzigen met de KPN Experia Box Thomson TG789v

1. Open Internet Explorer (of een andere browser) en vul op de adresbalk het adres **http://192.168.2.254** in en druk op **Enter**. **Typ geen www!** Als er een inlogscherm verschijnt, vult u de standaard gebruikersnaam **kpn** en het standaard wachtwoord **admin** in, of de door u aangemaakte gebruikersnaam en wachtwoord.
2. Klik in de linkerkolom op **Thuisnetwerk**. In het kader verschijnt een overzicht van uw netwerk.
3. Klik op de tekst die begint met **WLAN: Thomson**.....
4. Klik nu rechtsboven op de tekst **Configureren**. U komt in het configuratiescherm van het draadloze toegangspunt.

1.2 Voor WPA en WPA2-beveiliging

1. Selecteer achter **Encryption**: het rondje voor **WPA-PSK-codering gebruiken**.
2. Selecteer achter **WPA-PSK-versie:** de gewenste versie. Let op! Er zijn draadloze apparaten die de dubbelfunctie WPA+WPA2 niet ondersteunen. Selecteer hiervoor in de plaats **WPA** of **WPA2** (WPA2 is beter) afhankelijk van wat uw draadloos apparaat ondersteunt.
3. Vul achter **WPA-PSK-coderingssleutel** een door u verzonnen sleutel in.
4. Klik op **Toepassen**.

1.3 Voor WEP-beveiliging

1. Selecteer achter **Encryption:** het rondje voor **WEP-codering gebruiken**.
2. Selecteer achter **Lengte WEP-sleutel:** de gewenste sleutellengte **64 bit** of **128 bit** (veiliger)
3. Vul achter **WEP-coderingssleutel** de juiste sleutel in (10 karakters bij 64 bit en 26 karakters bij 128 bit).
4. Klik op **Toepassen**.

2 Het verschil tussen WEP, WPA en WPA2

WEP, WPA en WPA2 zijn versleutelingsmethodes om draadloos netwerkverkeer te beveiligen. Wanneer u een WEP-sleutel gebruikt, wordt de data met één en dezelfde sleutel versleuteld. Wat ontvangen wordt moet dan eerst worden ontcijferd met deze sleutel. Een WEP-sleutel is door computers met veel rekenkracht op lange termijn te kraken.

Bij WPA-encryptie wordt er met sleutels gewerkt die om de 4 seconden wisselen. Hierdoor hebt u een hoge mate van veiligheid aangezien er geen tijd is om de gebruikte sleutel te kraken. Dit gebeurt volledig automatisch.

Om verbinding te maken met het netwerk, maakt u gebruik van een vast wachtwoord. Voor de sleutel kunnen alle cijfers en letters worden gebruikt, inclusief de meeste speciale karakters en spaties. Deze sleutel bevat meestal tussen de 8 en 63 karakters en moet exact hetzelfde aan beide zijden van de verbinding worden ingevuld. Deze sleutel is moeilijker te achterhalen vanwege de vele mogelijkheden. Tijdens de gehele duur van de verbinding zullen het draadloze modem en het draadloos aangesloten apparaat constant nieuwe sleutels met elkaar afspreken. Voor elk aangemeld draadloos apparaat zijn dit andere sleutels. Dit heeft wel als nadeel,dat het bij het verlies van de draadloze verbinding soms vrij lang kan duren voor de draadloze verbinding wordt hersteld, beide kanten moeten hiervoor weer terug naar de vooraf ingestelde sleutel.

WPA2 is de opvolger van WPA en maakt gebruik van hetzelfde principe als WPA dat de sleutel regelmatig verandert. WPA2 maakt gebruik van een andere berekening en gebruik van een wisselend aantal bits voor deze sleutel.