Veilig online met WPA2-Enterprise?

Maatregelen om het risico op een Man in the Middle-attack te mitigeren

Om in de praktijk de WPA2-Enterprise standaard door middel van een Man in the Middle-attack te misbruiken moet er aan een hele reeks voorwaarden zijn voldaan. Daarmee is de kans op misbruik bijzonder klein. Desondanks blijft het noodzakelijk om de standaard op de juiste manier te implementeren. Het technisch team van govroam heeft de te nemen maatregelen waarmee u het risico kunt mitigeren hieronder op een rijtje gezet.

Correct configureren

Is het device van de eindgebruiker correct geconfigureerd? Dan is er sprake van een veilige verbinding voor het versturen van de inloggegevens tussen apparaat en organisatie. In technisch jargon: eerst wordt een 'end-to-end' TLS tunnel tussen het eindgebruikersapparaat en de RADIUS-server van de organisatie opgezet. Er is dan sprake van een wederzijds vertrouwen ('mutual trust') in de verbinding, waarna de communicatie kan starten. De TLS-versleuteling, ook bekend van het slotje bij het bezoeken van websites, maakt gebruikersnaam en wachtwoord onherkenbaar voor een 'Man in the Middle'. Het beschreven risico bestaat dan eenvoudigweg niet.

Risico foutieve configuratie inperken

Er zijn diverse manieren om het risico op een foutieve configuratie in te perken.

1. Belangrijk is een goede gebruikershandleiding. De gebruiker moet de eerste keer dat hij of zij inlogt op wifi, goed controleren dat er contact wordt gelegd via de eigen organisatie. Dit kan door het RADIUS-servercertificaat te controleren dat bij sommige apparaten in beeld verschijnt. Als er later weer wordt ingelogd en er verschijnt een waarschuwing dat er een *ander* certificaat door de organisatie gebruikt wordt, kan dat duiden op een hackpoging. Uiteraard is het verstandig om niet alleen te vertrouwen op de zelfredzaamheid van de gebruiker.

2. Laat uw gebruikers hun wifi instellen op een vertrouwde locatie. Daarmee wordt het wifi-netwerk eenmalig correct ingesteld. Nog eenvoudiger voor de gebruiker wordt het, als zijn of haar apparaat 'van de zaak' door de organisatie wordt ingesteld. Dat kan met beheertools als Mobile Device Management.

3. Daarnaast kan de organisatie een servercertificaat van een vertrouwde leverancier (een publieke 'Certificate Authority') gebruiken. Dat wordt doorgaans automatisch vertrouwd door het apparaat van de gebruiker.

4. Als uw organisatie dezelfde wifi-login gebruikt als die van kritieke systemen zoals e-mail (de 'Active Directory'-credentials), overweeg dan om andere credentials te gebruiken voor de veel minder kritische wifi-login. Dit lost ook een ander probleem op dat sommige organisaties ondervinden: een 'lock out' of niet meer kunnen inloggen op de kritieke systemen als het wachtwoord daarvan gewijzigd is, maar niet op het apparaat is aangepast voor het gebruik van wifi.

5. Een alternatief voor inloggen met gebruikersnaam en wachtwoord, is het device van de gebruiker te voorzien van een certificaat. Dat certificaat hoort bij het certificaat van de server van de organisatie, een veilige combinatie. Het verstrekken van certificaten aan eindgebruikers is vaak een uitdaging. Op 'managed devices' kan het certificaat geplaatst worden door een Mobile Device Management systeem. In technisch jargon stapt uw organisatie dan over van het gebruik van de beveiligingsstandaard EAP-TTLS of EAP-PEAP naar de standaard EAP-TLS. Deze kunnen alle drie binnen de WPA2-Enterprise standaard gebruikt worden voor het authenticeren van de eindgebruiker.

Voor vragen en opmerkingen kunt u terecht op ons klantportaal *of* info@govroam.nl.