Meer weten over publicroam en de risico's van open wifi

Hoe werkt publicroam?

Technisch gezien gebruikt publicroam WPA2-Enterprise, de meest veilige vorm van Wifi op dit moment. Om te controleren of een apparaat of wifi-toegangspunt vertrouwd wordt een gedeeld authenticatie knooppunt gebruikt dat gebruik maakt van RADIUS: Remote Authentication Dial-In User Service. Dit protocol wordt door vrijwel alle wifi-netwerken ondersteund. De aangesloten organisaties delen dit knooppunt, in beheer bij publicroam en via dit knooppunt wordt gecontroleerd of een toegangspunt, apparaat of gebruiker vertrouwd is.
Als een bezoeker zich de eerste keer aanmeldt bij een toegangspunt voert publicroam een aantal controles uit en ontvangt de bezoeker een SMS terug met een toegangscode. Na het invoeren van deze code logt het apparaat in het vervolg automatisch in bij alle vertrouwde toegangspunten.
Publicroam is openbaar: dan kunnen ook onbekenden toegang vragen. Bij govroam en eduram krijgen alleen bij de organisaties bekende medewerkers toegang.

Wat doet publicroam

De dienst *publicroam* helpt organisaties veilig en gebruiksvriendelijk gastwifi aan te bieden, onafhankelijk van leveranciers en zonder marketing-bijbedoelingen. Bezoekers hoeven zich maar één keer aan te melden, daarna gaan zij automatisch online bij alle deelnemende organisaties.

De dienst publicroam focust primair op het bieden van veilig en gebruiksvriendelijk gastwifi. De dienst stelt organisaties in staat om hun bezoekers veilig, gemakkelijk en zonder grote beheerskosten toegang te geven tot een wifi-gastnetwerk. Organisaties kunnen aansluiten op publicroam ongeacht hun apparatuur of leverancier. Er worden geen gebruiksgegevens verzameld en er wordt niet verdiend aan gebruikers. De dienst wordt gefinancierd uit bijdragen van deelnemende organisaties.

In de afgelopen jaren zijn er diverse oplossingen op de markt gekomen om veilig gastwifi aan te bieden. De meeste worden aangeboden in combinatie met andere producten of diensten. Zo is veilig gastwifi mogelijk door gebruik te maken van specifieke apparatuur. Andere oplossingen zijn gekoppeld aan netwerkleveranciers. Ook zijn er veilige wifi-diensten die gebruiksgegevens verzamelen voor marketingdoeleinden. En voor weer andere diensten moet de gebruiker betalen. Kortom, bij deze oplossingen is veiligheid niet de kern maar een bijproduct.

Spin-off

Publicroam is een spin-off van de vergelijkbare diensten *govroam* bij de overheid en *eduroam* in het onderwijs. Vrijwel alle studenten en docenten in Nederland en ruim een derde van de overheidsmedewerkers maakt hier inmiddels gebruik van. Zij loggen veilig in op de deelnemende wifi-netwerken. Publicroam verschilt van deze diensten doordat het gericht is op gastnetwerken voor het brede publiek. Bovendien is publicroam beschikbaar voor álle bedrijven en organisaties, dus niet alleen overheden en onderwijsinstellingen.

Risico's van open wifi

De onveiligheid van publiek wifi is al jarenlang een issue. (Semi-)open wifi-netwerken op stations, in hotels, cafés, bibliotheken, musea, theaters, ziekenhuizen, overheidsgebouwen, allemaal zijn ze relatief eenvoudig te hacken. Dit geldt voor netwerken zonder wachtwoordbeveiliging ('vinkje zetten voor akkoord') en ook voor netwerken met een gedeeld wachtwoord. Consumenten die hier gebruik van maken zijn een makkelijk slachtoffer. Cybercriminelen kunnen ongemerkt gegevens achterhalen waarmee zij identiteitsfraude kunnen plegen, inloggen op e-mail of andere accounts en gevoelige informatie kunnen onderscheppen.

Campagnes hebben weinig effect
Gebruikers worden alom gewaarschuwd. Zo heeft Europol een internationale preventiecampagne tegen 'Risks of using public Wi-Fi'[1]. In Nederland kennen we de campagnes via veiliginternetten.nl[2]. Helaas is het effect betrekkelijk gering. Uit diverse onderzoeken[3] blijkt dat veel consumenten regelmatig publiek wifi gebruiken maar dat slechts een klein deel maatregelen treft, zoals het gebruik van een VPN. Ze weten dat open wifi onveilig is, maar handelen er blijkbaar niet naar.

Onveilig gastwifi is normaal geworden
De ICT-afdelingen van de meeste bedrijven en organisaties zijn bekend met de risico's die kleven aan open wifi-gastnetwerken. De reden om niet te kiezen voor veiligere alternatieven is dat ze een te grote (administratieve) belasting vormen voor de organisatie. En omdat ze omslachtig zijn voor de gebruiker. Het gevolg is dat we blijven we zitten met onveilig gastwifi. Sterker nog, we zijn het inmiddels normaal gaan vinden. Maar dat is het natuurlijk niet!

Illegaal gebruik
Een bijkomend probleem van open wifi is het voorkomen van illegaal gebruik. Door gebrek aan registratie van gebruikers is het niet eenvoudig om te achterhalen wie gebruik maakt van een open netwerk. Daardoor zijn wifi-gastnetwerken bij uitstek geschikt voor het verspreiden van illegale content. Juridisch gezien is een aanbieder hiervoor niet aansprakelijk. Maar in een recent arrest[4] heeft het Europees Hof geoordeeld dat de netwerkaanbieder wel degelijk een *verantwoordelijkheid* heeft om illegaal gebruik tegen te gaan.

Meer informatie
Wil u meer weten over publicroam kijk dan op https://publicroam.nl

Kenmerken van publicroam
- *Publicroam zorgt voor een veilige verbinding tussen het apparaat en het wifi-accespoint*
- *De dienst wordt toegevoegd aan de bestaande wifi-infrastructuur, als een extra authenticatievoorziening*
- *Het werkt op basis van de standaard WPA2-Enterprise*
- *Gebruikers worden centraal geauthentiseerd, via een RADIUS-koppeling met een beveiligde server*
- *Bezoekers melden zich één keer aan via een aanmeldprocedure waarbij zij een username en password ontvangen*
- *Na een eerste keer inloggen gaan bezoekers automatisch online bij alle wifi-gastnetwerken die aangesloten zijn op publicroam*
- *Publicroam verzorgt alleen de authenticatie, het internetverkeer loopt via het bestaande wifi-netwerk*
- *De dienst voldoet aan eisen van privacywetgeving. Gegevens worden niet gedeeld met derden zonder toestemming van de gebruiker*
- Publicroam is beschikbaar voor zowel publieke als private organisaties. Om ruimte te bieden aan investeringen in verdere groei en innovatie is gekozen voor een private ondernemingsvorm met een maatschappelijke doelstelling.

[1] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/risks-of-using-public-wi-fi
[2] https://veiliginternetten.nl/themes/situatie/hoe-herken-ik-een-onveilig-wifi-netwerk/
[3] Bijvoorbeeld: https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf
[4] EU-arrest in de zaak McFadden.

4G of toch wifi?

Vaak wordt 4G genoemd als alternatief voor gastwifi. Maar de praktijk is weerbarstig. Organisaties bieden hun gasten wifi omdat ze gastvrij willen zijn. Bezoekers vragen erom, ook al hebben ze 4G. Waarom? Om uiteenlopende redenen: De dekking van 4G is niet overal even goed, zoals in gebouwen. Wifi is vaak sneller en gaat niet af van de databundel. Je hoeft geen hotspot op te zetten met je smartphone (omslachtig en kost veel batterij). Verder is het gewoon fijn als je je laptop openklapt en je bent direct online, net als thuis. We willen dus de beste dataverbinding óveral waar we zijn. Onderweg is dat 4G en als we ergens rustig zitten is dat wifi, liefst veilig en zonder gedoe met wachtwoorden.