Inventarisatie gastwifi gemeenten 2020

Hoe veilig zijn de wifi-netwerken van Nederlandse gemeenten?

Paul Francissen

25 juni 2020

publicroam

Inhoud

Samenvatting en conclusie

Dit is een verslag van een inventarisatie naar de manier waarop Nederlandse gemeenten toegang bieden tot wifi aan bezoekers. In juni 2020 is een uitvraag gedaan aan alle gemeenten per mail. 281 gemeenten hebben gereageerd. Aanleiding voor de inventarisatie is het besluit van het Forum Standaardisatie (adviescommissie voor open standaarden benoemd door het ministerie van BZK) d.d. 24 juli 2020 om een onderzoek te starten naar het uitbreiden van de bestaande verplichting voor overheden om de standaard WPA2-Enterprise toe te passen bij het aanbieden van wifi-netwerken. In het intakeadvies werd de veronderstelling gedaan dat veel overheidsorganisaties onveilige openbare wifi-gastnetwerken aanbieden. Dit is in deze inventarisatie getoetst.

Resultaten

- Alle gemeenten (100%) bieden de mogelijkheid aan bezoekers om gebruik te maken van een wifi-netwerk.
- Ten minste 78% van de gemeenten gebruikt een gastwifi-variant die niet veilig is voor gebruikers, tenzij de gebruiker zelf maatregelen treft. Het gaat hier om wifi-toegang zonder wachtwoord of met een gedeeld wachtwoord.
- Ten minste 5% van de gemeenten biedt toegang tot gastwifi via een persoonlijke gebruikersnaam en wachtwoord op basis van WPA2-Enterprise. Dit is de de meest veilige manier.
- Bij 17% van de gemeenten kon op basis van het antwoord niet bepaald worden op welke wijze zij toegang bieden tot het wifi-netwerk.

Conclusie: Uit de inventarisatie blijkt dat het merendeel (78%) van de Nederlandse gemeenten openbare wifi-gastnetwerken aanbiedt die niet veilig zijn voor gebruikers, tenzij gebruikers zelf maatregelen treffen. Dit onderschrijft de veronderstelling in het intakeadvies aan het Forum Standaardisatie. Er is ruimte voor verbetering als het gaat om inzet van veiligere standaarden voor openbare gastwifi bij de overheid.

1. Aanleiding

Verplichting WPA2-Enterprise voor overheden

Op 24 juni 2020 heeft het Forum Standaardisatie (adviescommissie voor open standaarden benoemd door het ministerie van BZK) besloten om een procedure te starten tot wijziging van de verplichting m.b.t. de standaard WPA2-Enterprise. Deze standaard moet worden toegepast bij het aanbieden van interne wifi-netwerken door de overheid. De beoogde aanpassing is erop gericht om de standaard óók te verplichten voor **openbare wifi-gastnetwerken** van de overheid. Een voorstel hiertoe is ingediend door de Stichting Privacy First samen met Publicroam. De beoogde aanpassing is toegelicht in het intakeadvies* d.d. 28 mei 2020 aan het Forum Standaardisatie.

Waarom deze wijziging?

WPA2-Enterprise maakt het mogelijk om veilige wifi-netwerken op te zetten. De huidige verplichting geldt alleen voor wifi-toegang voor overheidsmedewerkers. Er geldt een uitzondering voor openbare wifi-gastnetwerken. Hierdoor wordt het gebruik van de standaard niet bevorderd bij het aanbieden van **wifi-gasttoegang aan burgers en ondernemers**. Dit maakt deze groep gebruikers kwetsbaar voor kwaadwillenden die eenvoudig toegang kunnen krijgen tot persoonlijke gegevens.

Toets

In het intakeadvies (zie p. 3) wordt verondersteld dat de meeste overheidsinstanties openbare wifi-gastnetwerken aanbieden die niet veilig zijn voor gebruikers. Om te toetsen of dit inderdaad zo is, heeft Paul Francissen, mede-initiatiefnemer van Publicroam, deze inventarisatie uitgevoerd.

* https://www.forumstandaardisatie.nl/vergaderingen-en-stukken (selecteer: ’24 juni 2020’)

2. Aanpak

Kader veiligheid wifi-toegang

Allereerst is bepaald wanneer een wifi-netwerk wel/niet veilig is voor gebruikers. Hiervoor is gekeken naar de veiligheidsaspecten van de meestgebruikte gastwifi-varianten:

1. **Gedeeld wachtwoord (Pre Shared Key) -** Hierbij wordt het wachtwoord gedeeld met meerdere personen. Deze variant is om meerdere redenen niet veilig als het gaat om openbare wifi-netwerken: (1) Het wachtwoord wordt breed gedeeld en kan dus in handen komen van een hacker. Die kan daarmee het netwerk nabootsen. Gebruikers die geen maatregelen treffen kunnen dan automatisch verbinden met het netwerk van de hacker. (2) Het verkeer wordt onversleuteld verstuurd van het apparaat (smartphone, laptop, tablet) naar het wifi access point. Hierdoor kan het verkeer afgeluisterd worden, tenzij de gebruiker maatregelen treft. (3) Wanneer een eenvoudig wachtwoord wordt gebruikt kan dit worden achterhaald door middel van een brute force attack.

2. **Captive portal (vinkje voor akkoord) -** Hierbij maakt een apparaat verbinding met een wifi access point zonder wachtwoord. Nadat gekozen is om te verbinden met het wifi-netwerk, verschijnt er een webpagina. Vaak kan hier een vinkje-voor-akkoord worden geplaatst waarna men online gaat. Deze variant is om meerdere redenen niet veilig: (1) Er is geen wachtwoord. Een hacker kan het netwerk daardoor eenvoudig nabootsen. Gebruikers die geen maatregelen treffen kunnen dan automatisch verbinden met het netwerk van de hacker. De captive portal biedt hiertegen weinig bescherming. (2) Het verkeer wordt onversleuteld verstuurd van het device naar het wifi access point. Hierdoor kan het verkeer afgeluisterd worden, tenzij de gebruiker maatregelen treft.

3. **Open netwerk (zonder captive portal) -** Hierbij maakt een apparaat verbinding met een wifi access point zonder wachtwoord en zonder captive portal. Nadat gekozen is om te verbinden met het wifi-netwerk, komt de verbinding direct tot stand. Deze variant is om dezelfde redenen onveilig als de variant met een captive portal (zie hiervoor)

4. **Persoonlijke gebruikersnaam en wachtwoord (WPA2-Enterprise) -** Hierbij maakt een apparaat verbinding met een wifi access point op basis van een persoonlijke gebruikersnaam en wachtwoord. Deze variant is het meest veilig: (1) Het wachtwoord wordt niet gedeeld met meerdere personen. Een hacker kan het netwerk daardoor niet eenvoudig nabootsen. (2) Het verkeer wordt versleuteld verstuurd van het device naar het wifi access point. Hierdoor kan het verkeer niet afgeluisterd worden. (3) Bij het authentiseren wordt gebruik gemaakt van een certificaat. Hiermee kan de integriteit van het netwerk automatisch worden vastgesteld (je weet zeker dat je verbindt met het netwerk van de organisatie waarmee je wilt verbinden).

Vraagstelling

Op basis van de hiervoor genoemde veiligheidsaspecten zijn de volgende vragen richting gemeenten geformuleerd:

- *Kan ik als bezoeker gebruikmaken van gastwifi bij de gemeente?*
- *Moet ik hier van te voren een account voor aanvragen? Of kan ik ter plekke inloggen met een gedeeld wifi-wachtwoord / of via toegangspagina met vinkje-voor-akkoord?*

De vragen zijn zo geformuleerd dat beantwoording geen technische kennis vereist.

Uitvraag

De vragen zijn per mail aan alle Nederlandse gemeenten voorgelegd (n=355). Dit is gedaan door op persoonlijke titel (‘als burger’) een mail te sturen aan de griffies van alle gemeenten. De mails zijn verstuurd tussen 17 en 19 juni 2020.

Wanneer uit een antwoord niet kon worden opgemaakt op welke wijze toegang verkregen kan worden tot het wifi-netwerk, werd hier in een tweede mail nogmaals naar gevraagd.

Verwerking van antwoorden

De antwoorden zijn verwerkt ‘as is’. Wanneer uit een antwoord niet expliciet kan worden opgemaakt hoe de toegang tot wifi is geregeld, is dit verwerkt in de categorie ‘Niet duidelijk of niet bekend’.

3. Response

Populatie

De uitvraag is gedaan onder alle 355 Nederlandse gemeenten.

Daarvan heeft 78% gereageerd (n=281).

De inventarisatie geeft daarmee een representatief beeld van de situatie bij alle gemeenten in Nederland.

Analysedata

De onderliggende analysedata zijn op aanvraag beschikbaar. Stuur hiervoor een mail naar info@publicroam.nl

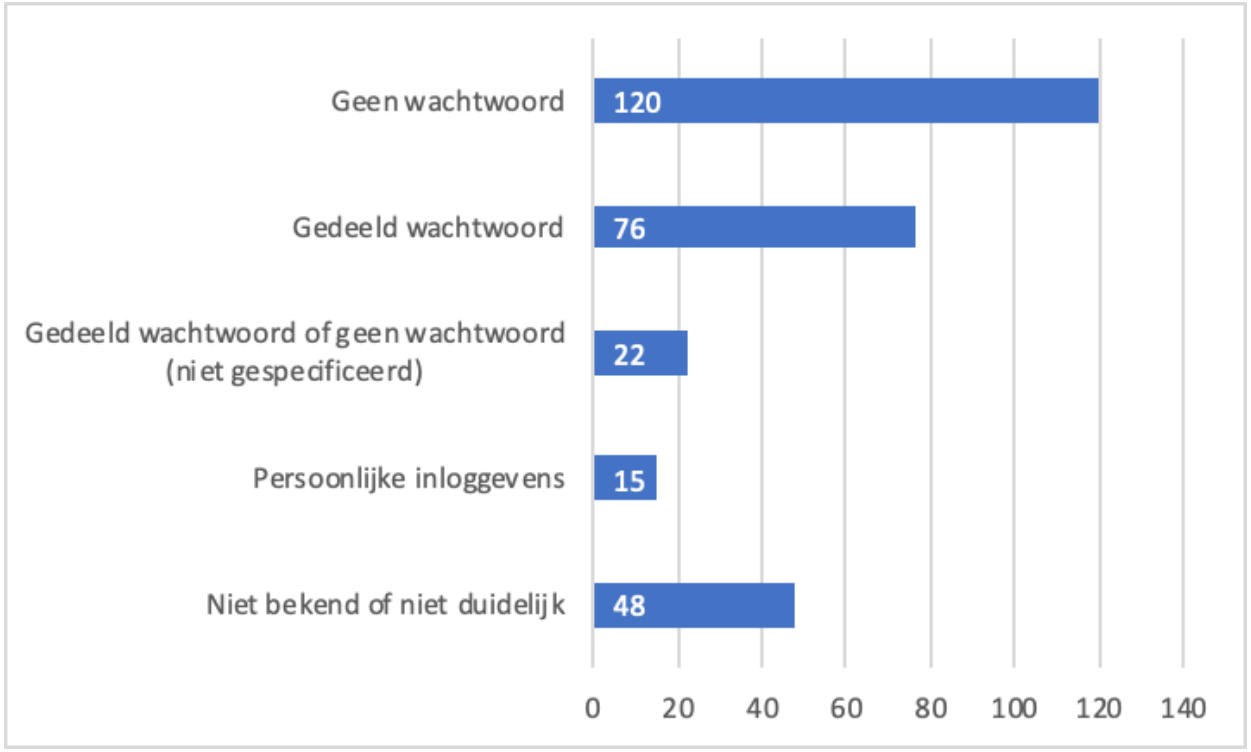
4. Resultaten

Beschikbaarheid gastwifi

Alle gemeenten die gereageerd hebben (n=281) bieden bezoekers de mogelijkheid om gebruik te maken van een wifi-netwerk. Een aantal gemeenten geeft aan dat wifi alleen beschikbaar is voor bezoekers met een afspraak.

Toegangsbeveiliging

Onderstaande grafiek geeft weer hoe gemeenten de toegang tot gastwifi hebben beveiligd.
Op de vervolgpagina's wordt dit toegelicht.



Geen wachtwoord

43% van de gemeenten (n=120) geeft aan dat zij toegang bieden tot wifi zonder wachtwoordbeveiliging. Hiervan laten 65 gemeenten weten dat zij werken met een captive portal (een webpagina die verschijnt na aanmelding). 4 gemeenten bieden een geheel open wifi, zonder captive portal. De overige gemeenten verstrekken hierover geen informatie.

Gedeeld wachtwoord

27% van de gemeenten (n=76) geeft aan dat zij toegang bieden tot wifi via een gedeeld wachtwoord. Dit is een wachtwoord dat aan meerdere personen wordt verstrekt. Gemeenten gaan verschillend om met het beheer en het verstrekken van dit wachtwoord. Eenderde van deze gemeenten (n=25) verstrekt het wachtwoord in de antwoordmail. Een aantal gemeenten geeft aan dat het wachtwoord wordt getoond op bordjes in de receptieruimten. Enkele gemeenten geven aan dat het wachtwoord wordt verstrekt aan de balie of door degene met wie men een afspraak heeft. Tenslotte geeft een deel van de gemeenten aan dat zij het wachtwoord periodiek wijzigen, veelal maandelijks.

Gedeeld wachtwoord of geen wachtwoord

8% van de gemeenten (n=22) geeft aan dat zij een open wifi hebben voor gasten zonder te specificeren op welke wijze de toegang is geregeld.

Persoonlijke inloggegevens

5% van de gemeenten (n=15) geeft aan dat zij gasten toegang bieden tot het openbare gastwifi via een persoonlijke gebruikersnaam en wachtwoord. Zij gebruiken hiervoor de wifi-roamingdienst publicroam op basis van WPA2-Enterprise.

Alle gemeenten die op deze wijze toegang bieden tot het openbare gastwifi zijn daarnaast ook aangesloten op govroam, de wifi-roaming dienst voor overheidsmedewerkers.

Niet bekend of niet duidelijk

Uit de antwoorden van 17% van de gemeenten (n=48) kon niet worden opgemaakt op welke manier toegang geboden wordt tot het wifi.

publicroam

#OveralVeiligWifi

Publicroam geeft bezoekers veilig en makkelijk toegang tot gastwifi. Zonder steeds opnieuw in te loggen. Gratis.

Eén account, overal online

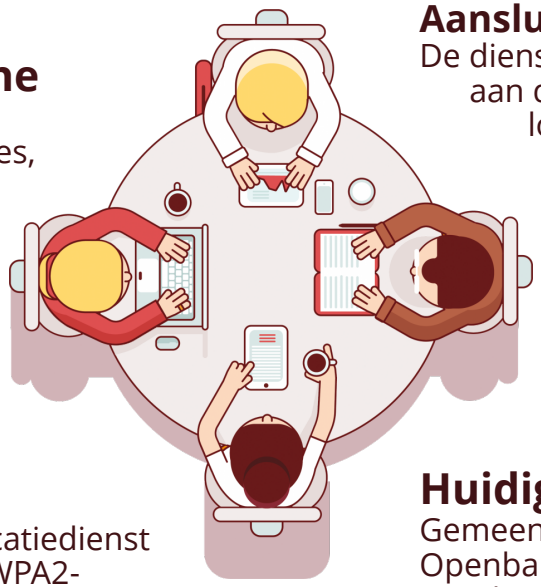
Gebruikers gaan met één account direct online op steeds meer locaties, bij gemeenten, bibliotheken, zorginstellingen, theaters, etc.

Bewezen technologie

Publicroam is gebaseerd op bestaande oplossingen voor overheid (govroam) en voor onderwijs (eduroam).

Onafhankelijk

Het is een onafhankelijke authenticatiedienst gebaseerd op open standaarden (WPA2-Enterprise en RADIUS). Het werkt in combinatie met alle gangbare wifi-apparatuur.



Privacy proof

Publicroam respecteert de privacy. Gegevens worden niet gedeeld met derden.

WINNAAR 2020
Nederlandse PRIVACY AWARDS

Aansluiten

De dienst kan eenvoudig toegevoegd worden aan de bestaande infrastructuur. Er hoeft lokaal geen identity management ingericht te worden.

Kosten

Organisaties betalen een aansluit-vergoeding (eenmalig) en een deelnamevergoeding (jaarlijks). De hoogte is afhankelijk van het aantal locaties en access points

Huidige deelnemers

Gemeenten Amsterdam, Den Haag, Alkmaar, Openbare Bibliotheek Amsterdam, Parkstad IT Heerlen, Werkorganisatie Duivenvoorde, A2-Samenwerking, Stichting ICTU, en meer.

https://publicroam.nl
info@publicroam.nl