Quick-scan veilig gastwifi

Er zijn diverse manieren om je bezoekers toegang te geven tot je gastwifi. De ene methode is veiliger voor de bezoeker dan de andere. Deze quick-scan geeft een overzicht van diverse methodes en helpt bij het kiezen van een veilige oplossing. Omdat naast veiligheid ook het aspect gebruiksgemak meeweegt, gaan we daar aan het eind ook kort op in. Tenslotte geven we enkele tips om er verder mee aan de slag te gaan.

Bron: deze quick-scan is gebaseerd op een onderzoek dat is uitgevoerd door Dialogic in opdracht van de Koninklijke Bibliotheek.

Risico's van onveilig gastwifi

Als de verbinding met een openbaar wifi-netwerk niet veilig is, kan iemand eenvoudig het internetverkeer van bezoekers afluisteren. Hierdoor kan de privacy van je bezoekers in het geding komen. Een hacker kan data stelen, zoals wachtwoorden. Ook kan iemand de verbinding manipuleren waardoor een bezoeker bijvoorbeeld naar een nepsite wordt doorgestuurd. Verder kan iemand je wifi-netwerk 'namaken' waardoor een bezoeker denkt dat hij verbonden is met jouw netwerk maar in werkelijkheid op een ander (frauduleus) netwerk zit.

Welke oplossingen zijn er en hoe veilig zijn ze?

De hieronder tabel laat zes inlogmethoden zien voor publieke wifi-netwerken, met daarbij of ze wel/niet geschikt zijn voor het bieden van veilige toegang aan bezoekers[1].

Beveiligingsmethode →	Geen beveiliging		WPA-Personal		WPA-Enterprise	
Inlogmethode →	1 Open (geen inlog)	2 Captive portal	3 Gedeeld wachtwoord	4 Uniek wachtwoord	5 Lokaal account	6 Wifi-roaming
Toepassing:						
- Veilige toegang tot **één** gastwifi	X	X	X/OK	OK	OK	OK
- Veilige toegang tot **meerdere** gastwifi-netwerken (met 1 account)	X	X	X	X	nvt	OK

OK = geschikt X = ongeschikt

Deze tabel is gebaseerd op een onderzoek uitgevoerd door Dialogic in opdracht van de Koninklijke Bibliotheek; Veilige WiFi voor bezoekers van de bibliotheek.

Toelichting per inlogmethode:

1. Open netwerken (geen inlog)

Bij een open wifi-netwerk maakt een bezoeker verbinding zonder wachtwoord. Dit soort wifi-netwerken is onveilig. Ieder apparaat kan meeluisteren met alle verkeer en er bestaat geen verificatie van het netwerk. Aanvullende maatregelen hebben vanuit perspectief van afluisteren en veiligheid geen impact. Het is voor kwaadwillenden eenvoudig om een netwerk met dezelfde

naam op te zetten, waardoor mensen het risico lopen te worden afgeluisterd via een frauduleus netwerk.

2. Captive portal

Bij een captive portal oplossing geeft een bezoeker een 'vinkje voor akkoord' waarna hij of zij online gaat. Wifi-gastnetwerken met een captive portal zijn net zo onveilig en hebben dezelfde risico's als open netwerken.

3. Gedeeld wachtwoord

Voor thuissituaties of toegang voor een afgebakende groep mensen, is de beveiliging van wifi met een gedeeld wachtwoord veelal adequaat. Voor openbare wifi-netwerken is dit niet zo. Het gedeelde wachtwoord is vaak te vinden op het internet. Kwaadwillenden kunnen zo een namaak-netwerk opzetten met dezelfde naam, waarmee bezoekers automatisch kunnen verbinden zonder dit te weten. Dit risico is minder als een organisatie het wachtwoord regelmatig wijzigt maar het risico is niet verdwenen

4. Uniek wachtwoord (PPSK)

Bij private pre-shared key (PPSK)-netwerken krijgt iedere gebruiker een eigen, uniek wachtwoord voor toegang tot een specifiek wifi-netwerk. De verbinding is daarna met een unieke sleutel beveiligd. Hierdoor is de verbinding veilig en privé en niet af te luisteren. PPSK-netwerken kunnen veilig gebruikt worden om toegang te bieden tot één publiek wifi-netwerk. PPSK maakt het niet mogelijk voor bezoekers om met één account veilig te roamen van het ene naar het andere netwerk. Dit komt doordat een apparaat niet automatisch kan vaststellen of het daadwerkelijk verbindt met een bepaald netwerk.

5. WPA-Enterprise met lokaal account

WPA-Enterprise wordt algemeen erkend als de meeste veilige standaard om toegang tot wifi te verschaffen, omdat zowel netwerk als individuele verbindingen zijn beveiligd. Afluisteren is niet mogelijk omdat iedere gebruiker een eigen sleutel krijgt. Het is voor kwaadwillenden vrijwel onmogelijk om een namaaknetwerk op te zetten waarmee mensen automatisch verbinden. Voor de overheid is deze wereldwijde standaard verplicht voor eigen medewerkers en medewerkers van andere overheden. Om WPA2-Enterprise te gebruiken voor gastwifi moet aan elke bezoeker een persoonlijk account (unieke gebruikersnaam en wachtwoord) worden verstrekt. Dit kan lokaal worden opgelost waarbij een organisatie zelf de accounts verstrekt.

6. WPA-Enterprise met wifi-roaming

Wifi-roaming is een oplossing waarbij bezoekers één keer een persoonlijk account aanmaken en daarna automatisch online gaan bij alle aangesloten wifi-netwerken. Organisaties hoeven dan niet zelf accounts te verstrekken. Het biedt de hoge veiligheid van WPA-Enterprise en als bijkomend voordeel dat gasten kunnen roamen van het ene naar het andere netwerk. Een gebruiker hoeft dan niet zelf op de veiligheid te letten; het apparaat authentiseert het netwerk automatisch op iedere roaminglocatie. Bekende wifi-roamingdiensten in Nederland zijn eduroam (studenten en onderwijspersoneel), govroam (ambtenaren) en publicroam (publiek/ bezoekers).

Take away: als je bezoekers veilig toegang wilt geven tot een wifi-gastnetwerk kun je niet volstaan met een open wifi of een gedeeld wachtwoord. Er zijn andere oplossingen waarmee je bezoekers wel veilig toegang kunt bieden.

Gebruiksgemak

Het voordeel van een open wifi-netwerk of een gastwifi-netwerk met een gedeeld wachtwoord is dat gebruikers er bekend mee zijn en direct weten hoe ze kunnen inloggen. En er zijn geen kosten aan verbonden voor het verstrekken van accounts. Deze methoden zijn niet geschikt voor veilige toegang tot wifi. Daarvoor moet je kiezen voor een oplossing met een uniek wachtwoord (PPSK) of met een persoonlijk account (WPA2-Enterprise).

Als je PPSK overweegt, kijk dan of je netwerk er geschikt voor is; de beschikbaarheid is afhankelijk van de fabrikant van de gebruikte wifi-apparatuur. Mogelijk zijn er kosten aan verbonden.

Oplossingen die gebaseerd zijn op WPA-Enterprise (dus met een persoonlijk account) werken over het algemeen op alle type netwerken. Wel moet je rekening houden met kosten voor het verstrekken van accounts en meer uitleg aan je bezoekers hoe ze moeten inloggen. Gebruik van een wifi-roamingdienst maakt dit makkelijker; accounts worden dan centraal vertrekt en de bezoeker hoeft zich maar één keer aan te melden.

Tips om ermee aan de slag te gaan

1) **Bepaal je huidige situatie**
   Gebruik de tabel om te bepalen hoe veilig je huidige gastwifi is.

2) **Ga in gesprek met je wifi-leverancier**
   Vraag naar de mogelijkheden en kosten van een oplossing die in jouw situatie voldoende veiligheid biedt. Vaak volstaat een verbetering van het bestaande netwerk.

3) **Kies een passende oplossing**
   Informeer je management over het belang van veilig gastwifi en de oplossing(en). Maak inzichtelijk wat in jouw situatie de kosten en baten zijn van de verschillende oplossingen. En maak een keuze.

[1] De gegevens zijn gebaseerd op een onderzoek in opdracht van de Koninklijke Bibliotheek: Veilig Wi-Fi voor bezoekers van openbare bibliotheken, Dialogic, 23 november 2020