Cyber
Weerbaarheidscentrum
Greenport

Wifi-hotspots

Je ziet ze tegenwoordig op steeds meer plekken: wifi-hotspots. Een wifi-hotspot is een openbare plek waar draadloze internettoegang wordt aangeboden. Hier kun je als ondernemer gebruik van maken.

Openbare wifi-hotspots worden aangeboden door bijvoorbeeld hotels, vliegvelden en bibliotheken. Maar je vindt ze ook vaak in koffiebars, flexwerkplekken en bedrijfsverzamelgebouwen. Om toegang te krijgen moet je je bij sommige aanbieders eerst - al dan niet tegen betaling - aanmelden via een webpagina (een zogeheten *captive portal*). Voor andere hotspots is er geen inlog of aanmelding noodzakelijk.

Als ondernemer kan het erg handig zijn om gebruik te maken van een wifi-hotspot, bijvoorbeeld om even je mail te checken in de lobby van het hotel of als je buiten de deur werkt in een koffietent. Het voordeel is dat je zo geen data uit je bundel verbruikt. Echter, veel wifi-hotspots kennen weinig tot geen beperkingen. Wees je bewust van de beveiligingsrisico's.

Kwaadaardige wifi-hotspots

Het is voor hackers relatief eenvoudig om een kwaadaardige wifi-hotspot te maken. Vaak doen ze dit op plekken waar veel mensen samenkomen, zoals een koffietent of eetgelegenheid. Deze hotspots hebben meestal dezelfde naam als de reguliere variant. Als gebruiker merk je hier dus niks van. Na het verbinden met het kwaadaardige wifi-punt lijkt er niets aan de hand en werkt het internet zoals je gewend bent. Deze hotspot is echter volledig onder controle van de aanvaller die met diverse hulpmiddelen het internetverkeer van verbonden apparaten onderschept.

Het internetverkeer zal door de aanvaller worden opgeslagen en geanalyseerd om te zien of er bruikbare informatie tussen zit. Hierbij moet je denken aan gebruikersnamen, wachtwoorden, bankgegevens, interessante mailtjes en klantinformatie. Met deze informatie kan de aanvaller zich vervolgens toegang verschaffen tot allerlei vertrouwelijke informatie en (bedrijfs)systemen.

Ook kunnen aanvallers kwaadaardige wifi-hotspots en slechte of onbeveiligde wifi-netwerken gebruiken om malware te verspreiden op apparaten die op het netwerk zijn aangesloten. Zodra jouw laptop of mobiele apparaat het delen van bestanden toestaat is het voor een aanvaller zeer eenvoudig om malware via het netwerk op verbonden apparaten planten.

Hoe bescherm je jezelf tegen kwaadaardige wifi-hotspots?

Het gebruik van een wifi-hotspot is niet zonder risico's. Wel zijn er enkele handelingen die je kunt uitvoeren om deze risico's te beperken.

- ### Gebruik je databundel (3G/4G/5G)
  Wanneer je voor de keuze staat om connectie te maken met een openbare wifi-hotspot of gebruik te maken van een mobiele verbinding (3G/4G/5G), is het veiliger om voor mobiel internet te kiezen. Mobiel internet wordt beheerd door de telecomaanbieder en, hoewel 100% veiligheid niet bestaat, is het gebleken dat mobiel internet veel moeilijker te hacken is dan een openbare wifi-hotspot. Ondanks dat een mobiele internet verbinding data (en dus geld) kost ben je wel een stuk beter beschermd en gelden bovenstaande risico's niet.

- ### Gebruik een VPN
  Maak gebruik van een VPN (Virtual Private Network). Dit is een beveiligde verbinding tussen jouw apparaat en de dienst waar je gebruik van wilt maken op het internet (bijvoorbeeld een webshop). Een VPN-verbinding is versleuteld. Hierdoor kunnen anderen het internetverkeer niet inzien of

afluisteren. Goede VPN-dienstverlening kost echter wel geld maar daar tegenover kun je versleuteld en op een veilige manier gebruik maken van elk openbaar wifi-netwerk. Lees hier over de verschillende VPN-diensten die er zijn.

- ### Controleer een wifi-hotspot
  Voordat je verbinding maakt met een openbare wifi-hotspot is het verstandig om te bekijken welke aanbieder het draadloos internet verzorgt. Vraag bijvoorbeeld bij de desbetreffende koffiebar naar de naam van het wifi-punt en de (mogelijke) inloggegevens. Maak in zijn algemeenheid met zo min mogelijk verschillende wifi-punten verbinding en gebruik het liefst vertrouwde of eerder gebruikte wifi-hotspots.

- ### Doe alles over HTTPS
  Internetverkeer dat wordt verzonden en ontvangen over een onbeveiligde HTTP-verbinding (zonder s) is voor een aanvaller die netwerkverkeer afluistert zeer gemakkelijk in te zien. Door gebruik te maken van een beveiligde HTTPS-verbinding maak je het voor aanvallers in veel gevallen onmogelijk het netwerkverkeer te ontcijferen. Dit kun je doen door bijvoorbeeld alleen websites te bezoeken die gebruik maken van HTTPS.
  Let op: Als je gebruik maakt van Google Chrome versie 76 (en hoger) dan wordt in de adresbalk 'www.' en 'https://' niet meer getoond. In het geval dat je toch een 'http://' pagina bezoekt zal in de adresbalk aangegeven worden dat de verbinding met de website niet is beveiligd.

- ### Download en installeer liever niets
  Wanneer je verbonden bent met een openbare wifi-hotspot is het aan te raden om niets te downloaden en te installeren. Je weet immers nooit precies wat je binnenhaalt via openbaar draadloos internet. Tevens kun je er zo zeker van zijn dat je niet per ongeluk malware op je apparaat installeert. Dit geldt overigens ook voor het doorvoeren van updates. Zorg ervoor dat je deze uitvoert wanneer je verbonden bent met een vertrouwd bedrijfsnetwerk of mobiele verbinding.

- ### Zet netwerk en bestandsdeling uit
  Over het algemeen staan zowel Apple als Windows het niet toe dat systemen bestanden kunnen delen via openbare wifi-netwerken. Maar het kan zijn dat de instellingen op jouw apparaat dit toch toelaten. In Windows is in het netwerkcentrum in te zien hoe deze ingesteld staan. Op Apple-apparaten is ook uitgebreide netwerk en bestandsdeling mogelijk, daarnaast kan Airdrop gebruikt worden om bestanden te delen binnen een netwerk. Voordat je verbinding maakt met een openbare wifi-hotspot is het dus goed om deze te controleren en ervoor te zorgen dat er geen malware op je apparaat geplaatst kan worden via het netwerk.

Overige tips voor veilige instellingen van je apparatuur

- Log je accounts direct uit als je klaar bent.
- Verbreek verbinding of nog beter: zet je wifi uit als je klaar bent.
- Maak niet automatisch verbinding met wifi-netwerken.
- Maak bij voorkeur nooit gebruik van wifi-hotspots voor bankzaken, privacy gevoelige zaken en vertrouwelijk zakelijke informatie.
- Ga niet naar websites waar gevoelige informatie, zoals bijvoorbeeld financiële gegevens, over jou of je bedrijf is opgeslagen.
- Doe betalingen via officiële betaalapps en niet via de browser.
- Gebruik tweefactorauthenticatie voor diensten die dit ondersteunen.

Dit document is gebaseerd op het document 'Wifit-hotspots' van het Digital Trust Center. Het originele document is te vinden via https://www.digitaltrustcenter.nl/wifi-hotspots