KIJK UIT voor de nep-hotspot

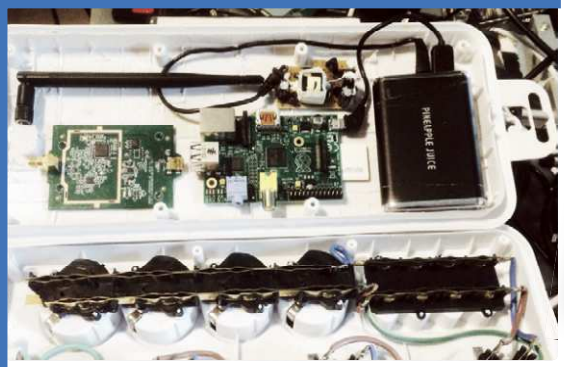
De tassen zijn gepakt en de tablet, smartphone of laptop gaat mee op vakantie. Elke fatsoenlijke camping of hotel heeft tegenwoordig gratis wifi, maar is het wel verstandig om daarvan gebruik te maken? Hoe kunt u zeker weten dat u niet wordt afgeluisterd? En welke voorzorgsmaatregelen kunt u treffen om uzelf te beschermen?

Kwaadwillen kunnen een nep-hotspot in de lucht brengen, zoals deze Wifi Pineapple.

Dat het gebruik van wifi via een open hotspot niet zonder risico is, weten de meeste mensen wel. Maar waarom eigenlijk? We vragen het security-expert Dennis Baaten. "Kwaadwillenden kunnen een nep-hotspot in de lucht brengen. Vervolgens kunnen ze mobiele apparaten zodanig misleiden dat die de nep-hotspot blindelings vertrouwen en er een verbinding mee maken. Internetgebruikers zijn vervolgens niet verbonden met het officiële accesspoint, maar met hack-apparatuur, zonder dat ze daar weet van hebben." Zo'n aanval uitvoeren kan bijvoorbeeld met kant-en-klare hack-apparatuur als de Wifi Pineapple, die voor nog geen honderd dollar vanuit Amerika via internet te bestellen is.

Veel beveiligingsexperts maken gebruik van de Pineapple om de beveiliging van netwerken te testen, maar het valt zeker niet uit te sluiten dat ook internetcriminelen deze nep-hotspot inzetten. "Er zijn tot nu toe 161 van dit soort apparaten besteld door inwoners van Nederland," zegt ethisch hacker oxDUDE. "Maar het bouwen van een 'rogue accesspoint' gaat ook prima vanaf bijvoorbeeld een Linux-laptop of een Raspberry Pi, dus de dreiging komt zeker niet alleen van de Wifi Pineapple."

Apparaten als de Wifi Pineapple kunnen op twee manieren misbruik maken van mobiele apparaten. Baaten: "De eerste methode speelt in op het vertrouwen dat mobiele apparaten hebben in het lijstje met vertrouwde netwerken." Dat zijn netwerken waarmee ze eerder succesvol een verbinding hebben gemaakt. Kwaadwillenden kunnen met speciale software dit lijstje scannen en zich vervolgens uitgeven voor een vertrouwd netwerk. Baaten: "Als wifi aan staat op een mobiel apparaat, dan gaat dat protocol het lijstje van vertrouwde netwerken continu af, van boven naar beneden: Hallo, 'thuisnetwerk', ben je toevallig in de buurt? Hallo, 'internet in de trein', ben jij er misschien? De Pineapple is zo geprogrammeerd dat deze op elk van deze vragen kan



Aanvallers kunnen ook zelf een 'rogue acces point' in elkaar knutselen.
Foto's: oxDUDE.

Hotspot of notspot?

Ethisch hacker oxDUDE.

zeggen: *Ja, dat ben ik*." Wanneer het om een open netwerk gaat, kan de verbinding vervolgens probleemloos tot stand komen. Een wachtwoord is dan immers niet noodzakelijk. De gebruiker krijgt alleen een melding dat hij of zij verbonden is met het netwerk, maar dat zal meestal geen argwaan wekken. Hoogstens wanneer het gaat om een accesspoint dat overduidelijk niet in de buurt kan zijn, zoals een thuisnetwerk op Schiphol.

Is het echt niet mogelijk een nep- van een echt hotspot te onderscheiden? oxDUDE: "Nee, dat kan alleen een beveiligingsexpert zien met behulp van speciale software." Volgens de ethisch hacker bestaat er daarom, wanneer u buitenshuis gebruikmaakt van een open wifi-accesspoint, vrijwel altijd een risico dat uw internetverkeer wordt afgeluisterd of zelfs gemanipuleerd.

De krachtigste hotspot wint

Kwaadwillenden kunnen er niet alleen voor zorgen dat uw mobiele apparaat een verbinding legt met een nep-hotspot, ze kunnen uw apparaat zelfs zo gek krijgen dat deze dat doet ten koste van een bestaande, betrouwbare wifi-verbinding. oxDUDE: "Ook als een mobiel apparaat al wel verbinding heeft met een ander wifi-netwerk, kan met hack-apparatuur zoals de Pineapple een aanval worden uitgevoerd. Dat komt omdat het wifi-protocol zo is ontworpen dat het continu naar bekende netwerken vraagt, ook als het apparaat al verbinding

TIEN TIPS voor veilig hotspotgebruik

Deze adviezen geven security-expert Dennis Baaten en ethisch hacker oxDUDE voor het gebruik van openbare hotspots:

- Maak liever geen verbinding met een open wifi-netwerk.
- Als u kunt kiezen tussen open wifi en een wachtwoord-beveiligd wifi-netwerk, kies dan voor de laatste mogelijkheid. Uw informatie wordt dan versleuteld verzonden, op basis van dit wachtwoord. Zelfs als een hacker dit wachtwoord kent, kan hij de bestaande verbinding die uw mobiele apparaat heeft met het vertrouwde accesspoint niet afluisteren.
- Mocht u toch verbinding leggen met een open hotspot, voer dan geen persoonlijke gegevens in zoals wachtwoorden en inlognamen. U kunt namelijk nooit zeker weten of uw internetverbinding niet wordt afgeluisterd.
- Ook wanneer u een https-verbinding opbouwt, kan uw internetverkeer via een open hotspot worden afgeluisterd.
- Maak geen gebruik van Internet Explorer wanneer u internet via een open hotspot. Dit is een advies van de Betaalvereniging Nederland.
- Als u gebruik hebt gemaakt van een open hotspot, verwijder dit netwerk dan na gebruik meteen uit het lijstje van vertrouwde netwerken. Anders is het voor een kwaadwillende mogelijk om zich voor te doen als dit zelfde vertrouwde netwerk, als u uw wifi aan hebt staan.
- Als u uw wifi niet gebruikt, zet dan wifi op uw telefoon of tablet uit. Installeer eventueel een app die ervoor zorgt dat uw wifi automatisch uitgaat wanneer u zich niet op een vertrouwde locatie bevindt, zoals thuis of op kantoor. Een voorbeeld van zo'n app is Wifi Matic, dat uw locatie bepaalt op basis van gsm-masten.
- Maak uitsluitend gebruik van wpa2 voor uw thuisnetwerk. Zowel wep als wpa bieden onvoldoende beveiliging voor veilig internetgebruik.
- Stel uw mobiele apparaat zodanig in dat het niet automatisch verbinding legt met bekende wifi-netwerken.
- Wanneer u onderweg vertrouwelijke handelingen wilt verrichten, maak dan gebruik van uw 3g- of 4g-verbinding.

heeft. De reden daarvoor is dat het wifi-protocol van nature altijd op zoek gaat naar het sterkste signaal. Hackers kunnen van die eigenschap misbruik maken door een extra krachtige zender zoals de Pineapple in de lucht te brengen." Baaten: "Maar ze kunnen bijvoorbeeld ook, met hun hack-apparatuur verstopt in een rugzak, op een plek in het restaurant gaan zitten waar de ontvangst slechter is omdat de afstand tot het accesspoint daar groter is. Als het hack-apparaat zich vervolgens voordoet als een krachtig en vertrouwd accesspoint zal de smartphone, tablet of laptop de bestaande verbinding verbreken en automatisch contact leggen met het wifi accesspoint van de hacker."

Gerichte aanvallen

Stel nu dat iemand met een richtantenne voor uw huis gaat staan, en uw thuisnetwerk heeft geen wachtwoordbeveiliging, bent u dan zelfs daar onveilig? oxDUDE: "Thuis is het gevaar een stuk lager omdat de thuisrouter doorgaans de sterkste verbinding heeft. Maar toch is het wel mogelijk om zelfs deze connectie te verbreken. De gemiddelde thuisrouter kan niet harder zenden dan met 0,1 watt. Er zijn echter ook specifieke apparaten die maar liefst 60 watt halen. Daardoor kunnen ze zelfs op afstand een andere partij 'overschreeuwen' en zo andere zenders wegdrukken." oxDUDE weet dit uit eigen ervaring. Als beveiligingsexpert heeft hij dit soort apparaten namelijk uitgebreid getest. En gebruikt om de beveiliging van netwerken te testen, waaronder die van de Nuclaire Top in Den Haag. oxDUDE: "De langste afstand die ik bij experimenten ooit heb gehaald is zeshonderd meter, met vrij zicht."

Behalve dat aanvallers via nephotspots op grote schaal vertrouwelijke gegevens kunnen afluisteren, zoals inlognamen en wachtwoorden, kunnen kwaadwillenden wifi ook gebruiken voor gerichte aanvallen. oxDUDE: "Stel dat een crimineel graag het thuisadres wil achterhalen van een bepaald persoon. Dan is daarvoor geen speciale apparatuur nodig, alleen een willekeurig wifi-apparaat waarop speciale hack-software is geïnstalleerd. Wanneer de aanvaller er in slaagt binnen wifi-afstand van zijn of haar slachtoffer te komen, kan de crimineel vervolgens met de speciale software het lijstje inzien van vertrouwde netwerken op alle andere wifi-apparaten in de buurt. Vaak is in dit lijstje de naam van het thuisnetwerk wel te herkennen. Aan de hand van het unieke mac-adres van dit thuisnetwerk kan de aanvaller vervolgens online de gps-locatie opzoeken van het thuisadres van de persoon die hij of zij aan het afluisteren is." De besturingssystemen van smartphones en tablets verzamelen namelijk wereldwijd voortdurend anoniem gegevens over de gps-locaties van wifi-netwerken. Databases met deze gegevens zijn online voor iedereen in te zien, bijvoorbeeld op www.wigle.net. Dat is handig, bijvoorbeeld voor app-ontwikkelaars die hun app kunnen vragen om de database te doorzoeken om zo ook binnen gebouwen te achterhalen op welke gps-locatie een smartphone of tablet zich bevindt. "Maar deze informatie kan ook misbruikt worden in het geval een kwaadwillende graag wil weten waar iemand woont."

Security expert Dennis Baaten.

Met een app als Fing kan iedereen zien wie er nog meer op het zelfde netwerk zit.

Schermfoto: oxDUDE.

Als het goed is kan de aanvaller met Fing geen open poorten ontdekken. Als dat wel zo is, dan is het apparaat onvoldoende beveiligd tegen 'portscans'.

Schermfoto: oxDUDE.

Zelfs https niet veilig

Wat kan een hacker doen zodra deze uw tablet, smartphone of laptop zo gek heeft gekregen een verbinding te leggen met zijn of haar open nep-hotspot? Baaten: "De aanvaller fungeert nu als doorgeefluik tussen uw mobiele apparaat en het internet en kan dus al het verkeer afluisteren." Over een wachtwoordloos wifi-netwerk wordt dat internetverkeer immers onversleuteld doorgegeven. Zelfs wanneer u op bepaalde websites gebruikmaakt van extra beveiliging zoals ssl over http (https). Kwaadwillenden blijken namelijk zelfs die extra beschermlaag te kunnen omzeilen. Dat gaat via een heel eenvoudige truc. We nemen een internetbankier-sessie als voorbeeld. Baaten: "Een internetaanvaller kan de browser ertoe aanzetten om af te zien van het opbouwen van een https-sessie en in plaats daarvan gewoon gebruik te maken van het normale http-protocol. De bank heeft niets in de gaten, omdat de aanvaller zelf wel een https-verbinding opzet met de bank." Wie goed oplet kan deze aanval wel bemerken omdat het slotje in de adresbalk ontbreekt. Tenminste, als de aanvaller niet zo slim is geweest een nepslotje te plaatsen op de nepwebpagina. Baaten: "Vervolgens kan de internetaanvaller tijdens het bankieren het rekeningnummer van de begunstigde aanpassen zonder dat de gebruiker dat merkt."

Websites kunnen een beveiliging inbouwen tegen dit soort aanvallen door een zogeheten 'hsts'-header mee te sturen. Baaten: "Daarmee zeggen ze tegen de browser dat deze voor deze webapplicatie geen http-verbinding mag accepteren. Die browser moet dan wel ondersteuning bieden voor hsts. Mozilla Firefox, Google Chrome en Apple Safari hebben die ingebouwde ondersteuning; Internet Explorer helaas niet. Daarom heeft Betaalvereniging Nederland eind mei opgeroepen om voorlopig geen gebruik meer te maken van deze browser."

Tekst: Jolein de Rooij