Hotspots met gratis WiFi

Stavaza 28 maart 2013

# Uitgangspunten

Niet alleen lokale besturen bieden gratis WiFi hotspots aan (of wensen die aan te bieden) maar ook veel private bedrijven bieden dit aan. (hamburgerrestaurants, cafés, wachtruimtes van garages,…).

Wie zien voornamelijk drie methoden van het gratis aanbieden:

1. Na complexe registratieprocedure, bv. kopie van identiteitskaart gevolgd door een unieke login (verschillend per gebruiker)
2. Na een eenvoudige loginprocedure met een universele login voor iedere gebruiker:
   1. Op aanvraag bij een balie e.d.m.
   2. Login wordt opgehangen in het betrokken lokaal
   3. Login wordt meegegeven met de loginpagina
3. Een anonieme login. Iedereen die in de buurt van de hotspot zit kan inloggen en surft dus anoniem. In het beste geval wordt het MAC-adres gelogd[[1]](#footnote-1)

Hierbij zien we varianten in beperking van toegestane tijdsduur, bandbreedte voor upload en download, volumebeperkingen, filteren van toegang[[2]](#footnote-2),…

Vaak wordt nog meegegeven wat mag en niet mag (illegaal downloaden, e.d.m.)

Strikt juridisch is enkel de eerste methode volledig sluitend. De tweede methode heeft weinig of geen juridische waarde en dient enkel om ‘overconsumptie’ te kunnen tegen gaan, bouwt een psychologische rem in en geeft je wat oneigenlijke gemoedsrust.[[3]](#footnote-3)

De derde methode –volledig anonieme login – lijkt mij nog steeds de meest evidente keuze. Juridisch zitten we nog wel in een schemerzone (wordt verder onderzocht). Maar in het slechtste geval kan politioneel het WiFi netwerk worden afgesloten en dient het duidelijk te zijn dat de gebruiker niet gekend is en dat de verantwoordelijkheid niet bij de aanbieder ligt.

# Naar een praktijk

Indien men hotspots wil aanbieden dient men een aantal –voor de hand liggende- zaken te organiseren:

1. Zorg dat het Hotspot-netwerk fysiek zo sterk mogelijk afgescheiden is van het eigenlijke –zakelijk- netwerk. U voorkomt problemen met crossover (hacking e.d.) én bij strafrechtelijke overtredingen wordt enkel Hotspot-netwerk afgesloten en/of geblokkeerd. U riskeert evenmin dat de eigen netwerkverbinding op zgn. blacklists komt.
2. Als u kiest voor een eenvoudige login, bedenk dan dat u zich niet beter indekt dan bij een anonieme login. Het enige is dat u iets meer ‘controle’ heeft over wie toegang krijgt. Maar als u de login op een openbare plek uithangt heeft u evenmin controle (bv. de login in het café van het Brugse Concertgebouw is gewoon het telefoonnummer dat op een bord aan de meer staat). Als u individuele logins gaat aanmaken, bedenk dat dit de administratieve (personeels)kosten enorm verhoogt.
3. Een aantal manier om misbruiken te voorkomen kunnen zijn:
   1. Beperk de upload-bandbreedte voldoende. Dit ontmoedigt gebruikers van peer-to-peer netwerken. Een foto uploaden naar facebook moet haalbaar zijn, maar DVD’s uploaden moet niet de bedoeling zijn.
   2. Beperk de gebruiksduur, op basis van MAC-adres, maar wees niet te zuinig en laat dit ook afhangen van de locatie. Studenten die hun laptop meebrengen naar de bibliotheek om te studeren en op te zoeken gebruiken dit soms de hele dag.
   3. Log het MAC-adres, volume en tijden. Let op: ga niet “sniffen” naar de inhoud omdat je dan zelf de privacyregels overtreed. Maar indien nodig kan je MAC-adressen blokkeren. Merk op: er bestaat genoeg software om MAC-adressen te spoofen !
   4. Kijk de log-bestanden regelmatig na op onregelmatigheden en neem maatregelen.
   5. Beperk wanneer nodig de toegangstijden, maar bedenk dat bv. avondvergaderingen in een cultuurcentrum kunnen uitlopen !

# Naar een advies

Wij adviseren **momenteel** om, waar mogelijk, te opteren voor anoniem surfen via WiFi-hotspots. Zorg voor een heel goede scheiding tussen hotspot en het eigen netwerk. Gebruik de aanbevelingen over upload-bandbreedte, volume en tijdsduur. Log de basisbewegingen en kijk deze logs regelmatig na (niet alleen in het begin !). Gebruik, indien je dit toch wenst, een systeem van logincode. Als je dit doet, verander deze dan regelmatig. Je kan, indien gewenst, steeds een openingsscherm tonen waarin de ‘spelregels’ staan uitgelegd. Bondig, to the point (niet zoals de gebruiksvoorwaarden van I-tunes – 80 bladzijden juridische informatie). De juridische waarde ervan is evenwel betwistbaar.

# Hoe verder

Er is een vraag gesteld aan onderzoekers om hierrond verder te werken. De vraag of ze het spontaan opnemen is nog niet geheel duidelijk. Het kan zijn dat we voor het advies –op onze beurt- zullen moeten betalen…

Herman Callens

1. MAC-adres is een wereldwijde unieke cijfercombinatie voor elk “apparaat” binnen een (internet)werk. Het is hardcoded in het toestel zelf (netwerkkaart op laptop, smarthphone, tablet, router, repeater, enz…). Het idee dat je het MAC-adres niet kan veranderen is echter ook reeds lang achterhaald. [↑](#footnote-ref-1)
2. Volgens de Europese normen betekent evenwel netneutraliteit dat je eigenlijk niets filtert. Er schuilt enige logica in. Maar als het er op aan komt zal opnieuw een rechtbank uitmaken wat kan en niet kan. [↑](#footnote-ref-2)
3. Het is zoals het bordje bij een bewaakte vestiaire dat claimt dat de organisatie niet verantwoordelijk is voor gebeurlijke diefstallen… Een rechtbank aanvaardt dat niet. [↑](#footnote-ref-3)