Fabrice Jonvel (Bluesafe) : en route vers le « social hotspot »

Créé il y a 10 ans, **Bluesafe** – dont le nom est la contraction de 'Blue' pour le Bluetooth et 'Safe' pour la sécurité – est aujourd'hui un expert du Wifi dans tous les usages de la mobilité et en particulier en frontal des nouveaux besoins de connectivité. Entretien avec **Fabrice Jonvel**, cofondateur de Bluesafe.

Silicon.fr : Le Wifi semble être devenu une commodité…

Fabrice Jonvel – L'usage domestique du Wifi, avec une liaison dédiée très peu partagée, est trompeur.

Dans l'entreprise, nous devons faire face à des déploiements massifs, de grande taille ou sur une multitude de petits sites. Les déploiements de solutions Wifi sont de plus en plus complexes, avec de grands enjeux technologiques, sur la radio et la sécurité. Nous devons couvrir des surfaces de 10.000 à 60.000 m², pour des entreprises qui veulent de la mobilité.

Dans un usage domestique, la mobilité est locale et ne nécessite pas de 'rooming'. L'enjeu de la radio dans l'entreprise, c'est de permettre à utilisateur de se déplacer avec son terminal sans défaillance du réseau et avec une qualité de service. À nous de concevoir une couverture multicellules et de prendre en compte les terminaux et les équipements.

Les réseaux de l'entreprise ne suffisent pas ?

Sur les petits sites, nous rencontrons moins de difficultés sur la radio, moins de complexité sur les enjeux de répartition des réseaux, sans nécessiter de compétence locale, pour construire des réseaux Wifi fortement centralisés. En revanche, le service WLAN bureautique entraîne une grosse consommation de bande passante, tandis que la TOIP consomme certes peu de bande passante, mais exige un rooming sans faille.

Un hotspot privé, pour l'accueil des visiteurs extérieurs, demande sécurité, authentification et traçabilité des communications. Il change également l'aspect utilisation en s'ouvrant de plus en plus aux collaborateurs, par exemple lorsqu'il n'y a pas de réseau social sur le poste de l'entreprise suite à leur interdiction sur les réseaux locaux.

Cela nous impose de fournir de la connectivité sur le hotspot, afin d'inviter les salariés sur leurs propres équipements. Le phénomène du BYOD entraîne une évolution du WLAN avec une gestion dynamique de l'accès, via par exemple un compte LDAP si le hotspot doit cependant limiter l'accès à l'information.

Les usages du Wifi évoluent également…

En effet, les usages se diversifient : la monétique, les applications de traçabilité, la lecture de codes à barres, l'arrivée du streaming vidéo, la connexion bureautique…

Ils se diversifient principalement dans la grande distribution, dans les agences, etc., qui doivent faire face à une baisse de fréquentation des lieux de vente et du panier moyen. Et faire face aux nouveaux comportements de consommation. Les boutiques sont considérées comme un showroom, où l'on regarde sur le net. La concurrence de l'e-commerce rentre dans les murs.

Le Wifi peut-il être un vecteur de dynamisation de l'activité commerciale ? La question est ancienne, mais nous constatons des changements avec généralisation des smartphones. Le client doit trouver un Wifi qui draine une valeur ajoutée, très faible jusqu'à présent dans la relation client/vendeur, avec pour l'entreprise la contrainte de la traçabilité et des coûts supplémentaires.

La solution n'est-elle pas dans le hotspot public ?

Le hotspot public est resté lettre morte, avec une qualité faible. En d'autres lieux on rend le hotspot payant, mais le taux de conversion est extrêmement faible. Il n'a pas encore trouvé son modèle économique, qui devrait être d'apporter de la valeur ajoutée au client et à l'enseigne.

À suivre en page 2 : de nouvelles solutions pour le hotspot

Quelle solution proposez-vous pour revaloriser le hotspot commercial ?

Pour réinventer le hotspot en lui donnant de la valeur ajoutée, nous sommes partis de la contrainte de traçabilité légale, avec un code de connexion indispensable, afin de rassurer l'entreprise. Et nous avons trouvé une identité numérique ailleurs à utiliser sans la créer.

Dans notre culture de la sécurité, les réseaux sociaux s'inscrivent en fournisseurs d'identités numériques sur internet. Sur un hotspot classique, la facilité la connexion de Facebook Connect laisse la possibilité de créer une identité numérique si elle n'existe pas.

Tel a été notre raisonnement initial. Via un service en mode SaaS, Bluesafe Guest Manager (BGM), avec l'ajout de fonctionnalités d'utilisation d'identités extérieures, comme Connect, Twitter, etc. C'est le concept de 'social hotspot'.

Comment vous est venue cette idée de substituer l'identité sociale à la déclaration de la personne qui veut se connecter ?

Elle nous est venue de la découverte de la stratégie de réseaux sociaux des marques, qui cherchent à développer la relation client, à accéder aux informations liées aux centres d'intérêt des possesseurs de comptes, qui laisse la possibilité d'accepter ou non de laisser voir des caractéristiques du compte.

Cette approche permet de suivre les abonnés en temps réel, et ouvre les portes de la rétribution du client sur ses efforts de promotion. En alimentant les stratégies de réseaux sociaux, nous apportons à l'enseigne la connaissance de la présence du client dans ses locaux. Et nous fournissons la possibilité de déployer une stratégie en temps réel pour que le vendeur aille à la rencontre du client, et lui offre une promotion.

Votre solution est-elle adaptée à la réglementation ?

La loi autour de l'identité reste floue, il n'y a pas de définition du moyen identification. Notre solution consiste à partager un secret qu'il est impossible de remonter. Il n'y a pas de clé de connexion, juste l'adresse MAC de la machine client et l'adresse IP de la ressource vers la connexion. De plus, nous améliorons l'identité stockée dans le journal légal.

Le réseau social se place sous à loi de la traçabilité des accès, et nous améliorons la reconnaissance de l'identité.

Du côté de l'infrastructure, un hotspot, de 1000 à 1500 euros, une connexion au CRM pour fournir un environnement client, et le marketing dans Facebook.

Et concernant les risques de dangerosité du Wifi ?

Notre étique conseille de donner l'information au client, c'est sanitaire, et cela doit être traité avec vigilance. Nous respectons les normes sanitaires, les règles de stockage de l'information, et les règles anti-intrusion.

À nous de faire la promotion de ces technologies en y apportant un minimum de précautions, de mettre en place des solutions qui évitent d'être juge et parti.