Les hot-spot Wi-Fi de SFR vulnérables aux pirates?

On le sait, le protocole Wi-Fi ne présente pas une sécurité maximum. Les opérateurs assurent que les liaisons à partir des hot-spot (bornes d'accès) sont protégées. Ce n'est pas l'avis d'Integralis, société anglaise de services dans le domaine de la sécurité informatique dont l'étude va donner des sueurs froides aux opérateurs et aux utilisateurs.

Integralis a testé la vulnérabilité des hot-spot de SFR en France mais aussi de Vodafone et de T-Mobile en Europe. Sa conclusion est sans appel: un utilisateur lambda qui utilise un certain type de mobile bluetooth, notamment certains Nokia et Sony-Ericsson, pour se connecter peut très facilement se faire pirater à distance sa liaison. Le pirate utilisera ainsi gratuitement la connexion de sa victime, sans que cette dernière s'en rende compte. En cause, le système d'authentification qui selon Integralis est trop simple: envoi du numéro d'abonné en guise d'authentification, réception du login via SMS. Schématiquement, en piratant la liaison bluetooth de la victime (très simple à quelques mètres de distance), le pirate accède simplement au login et au password de la victime. Chez SFR, cette information tombe plutôt mal. L'opérateur va inaugurer le 23 juin son hot-spot à la Défense, en plein quartier d'affaires. Si l'entreprise refuse pour l'instant de commenter cette étude, il assure qu'il fera un point sur la sécurité lors cette inauguration. Par ailleurs, si SFR est épinglé par ce test, rien ne dit que les hot-spot d'Orange par exemple sont mieux sécurisés. L'étude d'Integralis ne s'est penché que sur un seul opérateur français… Mais pour empêcher que sa connexion soit piratée, il n'y a pas 36 solutions. Ne pas utiliser de mobile bluetooth ou apprendre à sécuriser cette liaison. De son côté SFR devra sûrement rajouter une couche de sécurité à ses équipements. L'étude d'Integralis: http://www.integralis.co.uk/about_us/press_releases/2004/150604SA.html