Panoptinet

Gardez un oeil sur votre réseau

Pourquoi les pirates adorent le Wi-Fi

admin · Monday, May 9th, 2011

Si pour les abonnés Internet, les risques d'un réseau Wi-Fi mal sécurisé sont aujourd'hui mieux connus, quelles sont les raisons qui incitent les pirates à utiliser les technologies sans fil pour voler des données personnelles ou stratégiques, ou bien encore « squatter » des accès web en toute discrétion ? Pourquoi le Wi-Fi est-il aussi apprécié ?

Sur le plan mondial, les « cyber-larcins » commis via des connexions Wi-Fi sont en augmentation, qu'ils concernent les particuliers ou les entreprises. Coïncidence ou pas ? Hélas non, en voici d'ailleurs les raisons :

Le Wi-Fi est un moyen de contourner les sécurités physiques

Les réseaux sans-fil permettent de faire **circuler des informations dans les airs**. Celles-ci se « baladent » donc souvent en dehors des murs. Le pirate n'a par conséquent aucun besoin de s'infiltrer physiquement dans un bâtiment pour "hacker" un réseau informatique : inutile de cambrioler un particulier ou de forcer la sécurité d'une entreprise.

Le Wi-Fi offre l'avantage de la mobilité

Tout comme les simples utilisateurs de la technologie sans fil, les hackers utilisent de **petits appareils, accessibles, mobiles et puissants** : ordinateurs portables, tablettes, smartphones, etc. En déjouant la sécurité du réseau – si tant est qu'il y en ait une – il devient alors possible de se connecter aux échanges de données, et même directement à certains postes informatiques ciblés, tout en se déplaçant à proximité.

Le Wi-Fi rend possible l'anonymat et la non-traçabilité

La discrétion est un des soucis majeurs des pirates. Or il est difficile aujourd'hui d'utiliser une interface de communication qui permet de rester anonyme et invisible :

les téléphonies fixes et mobiles, ainsi que les abonnements Internet, sont des marchés organisés par des opérateurs qui peuvent identifier des communications spécifiques et leurs auteurs. Même en cybercafé, les propriétaires enregistrent les identités de leurs clients.
Avec le Wi-Fi, il devient possible de **se connecter via l'identité de quelqu'un d'autre**, assurant ainsi au pirate l'anonymat et la non-traçabilité.

Les réseaux Wi-Fi sont des proies faciles

En France ou à l'étranger, de nombreuses personnes ne sécurisent pas du tout – ou pas suffisamment (WEP) – leur réseau Wi-Fi. Y compris certaines entreprises ! Par ailleurs, beaucoup de pirates réussissent à **contourner certaines protections**, jugées fiables à tort (WPA, WPA2, Filtrage MAC, etc.).
Enfin, les hotspots – ou points d'accès publics sans fil – se multiplient sur le territoire : restaurants, hôtels, aéroports, parcs, etc. Leurs utilisateurs de passage sont peu méfiants, et pourtant, éparpillent des informations personnelles, confidentielles voire bancaires dans les airs, sans réaliser qu'il est très facile de les « capturer ».

La portée et le débit du Wi-Fi sont excellents

Pour des communications locales sans fil, le Wi-Fi est un merveilleux outil. En tout cas bien **meilleur que le Bluetooth ou l'infrarouge**, en termes de portée et de débit. Les pirates peuvent ainsi opérer à bonne distance (à parfois plus de 100 mètres, et encore, sans équipement spécial). Ils peuvent aussi envoyer ou recevoir des données en masse, grâce à un débit généreux, presque comparable à l'Ethernet depuis l'apparition de la norme 802.11n.

Les failles du Wi-Fi sont connues et assez faciles à exploiter

Les **trous de sécurité** des réseaux sans fil sont nombreux et largement détaillés sur Internet : points d'accès rogues (bornes voleuses), honeypots ou mobiles (smartphones), dénis de service, etc. Ces techniques peuvent être mises en œuvre par de nombreux logiciels disponibles gratuitement sur le web.
D'autres vulnérabilités comme la faiblesse des clés WEP, du protocole TKIP, du « Hole 196 » fragilisant les clés WPA2, etc. peuvent être utilisées pour infiltrer ou attaquer un réseau Wi-Fi.

Les réseaux Wi-Fi sont très rarement surveillés

Contrairement aux réseaux filaires, la plupart des réseaux Wi-Fi ne sont **pas contrôlés**, du fait d'un manque de sensibilisation aux risques de l'Internet sans fil. Cette insouciance représente un avantage pour ceux qui piratent les accès Wi-Fi, souvent ignorés car **non-détectés**.

Pour toutes ces raisons, le Wi-Fi est une porte d'entrée idéale pour tous les pirates qui souhaitent s'introduire dans un réseau informatique. Par ailleurs, les appareils

mobiles qui intègrent la technologie sans fil sont de plus en plus nombreux, notamment les smartphones. Il est donc à craindre que des **applications spécialisées dans le hacking** de réseaux Wi-Fi se multiplient, et se simplifient. Or les chances de bloquer ce type d'intrusion sont proches de zéro si certaines **mesures de sécurité** ne sont pas appliquées :

- Les particuliers et les entreprises doivent « **monitorer » leur réseau**, c'est à dire surveiller en permanence qui s'y connecte. Pour les entreprises, des logiciels existent, mais ils peuvent être chers et complexes (administration réseau). Pour les particuliers, Panoptinet conseille **Achiwa** : simple, fiable, abordable et pédagogique, c'est l'outil idéal pour le « monitoring » des réseaux personnels (box). C'est aussi une **solution respectueuse de la vie privée**, contrairement à certains logiciels « mouchards ».
- En fonction des risques et de la valeur des informations (personnelles, confidentielles, bancaires) échangées ou disponibles sur le réseau, l'abonné Internet doit mettre en place des **mesures de sécurité minimum**. C'est pourquoi Panoptinet vous propose un test (Quel niveau de sécurité choisir ?) qui vous suggère un niveau de sécurité à adopter : 1, 2 ou 3. Selon le résultat, des tutoriels propres à chaque box sont disponibles gratuitement. Si vous les suivez pas à pas, vous comprendrez que sécuriser votre réseau ne demande que très peu de temps !
- Des précautions particulières sont à prendre pour toutes les connexions aux **hotspots**, que ce soit à partir d'un ordinateur personnel ou professionnel. Là encore, vous trouverez une fiche pratique dédiée à cette problématique : sécuriser sa connexion sur un hotspot.

Les pirates adorent le Wi-Fi, c'est indéniable. Mais les internautes également ! A eux de faire en sorte que cette technologie sans fil soit un outil pratique, et non une invitation à se faire « squatter » sa connexion (avec tous les risques que cela suppose, notamment depuis le vote des lois **Hadopi**) ou voler ses données personnelles !

Source : infosecurity-us (en)

This entry was posted on Monday, May 9th, 2011 at 10:44 am and is filed under Actualités décryptées par Panoptinet
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.