Panoptinet

Gardez un oeil sur votre réseau

25% des réseaux Wi-Fi sont vulnérables

admin · Thursday, October 20th, 2011

Par définition, le Wi-Fi est facilement piratable. Il l'est encore plus lorsque qu'il n'est pas du tout crypté, ou crypté avec un chiffrement obsolète tel que le WEP. C'est malheureusement le cas d'un quart des réseaux Wi-Fi étudiés...

L'omniprésence des connexions sans fil est telle que la vie sans elles est à peine imaginable. Presque tous les particuliers ou professionnels possèdent au moins un routeur (box). La technologie Wi-Fi permet de **se connecter facilement** au Web et de naviguer rapidement, sans câble. Le **revers de la médaille** est que cela permet aux **pirates** d'en faire autant.

La **sécurité des réseaux Wi-Fi** est un aspect critique qui reste souvent **négligé**. Compte tenu du fait que la plupart des routeurs sans fil (box) sont immédiatement utilisables pour en faciliter l'installation par des clients non professionnels, certains routeurs et points d'accès sans fil déployés dans les bureaux ou chez les particuliers sont mal protégés, voire complètement **dépourvus de mesures de sécurité**. C'est en tout cas ce que révèle une enquête, basée sur l'étude de 2133 réseaux sans fil (entreprises et particuliers) entre novembre 2010 et octobre 2011.

Etat des lieux de la sécurité des réseaux sans fil

61% des réseaux étudiés semblent correctement sécurisés puisqu'ils sont cryptés avec un protocole de type **WPA ou WPA2**. Encore faut-il que les **mots de passe** censés protéger ces cryptages soient pertinents, ou autrement dit difficilement crackables (10 conseils pour un mot de passe solide).

Parallèlement, **19% des réseaux Wi-Fi** recensés dans l'étude sont chiffrés avec un **cryptage WEP**, particulièrement obsolètes : de nombreux tutoriels écrits ou vidéo pour cracker un cryptage WEP en moins de 5 minutes pullulent sur le web...

6% des détenteurs de réseaux Wi-Fi ont eux carrément fait l'**impasse sur le**

cryptage, laissant ainsi leur réseau ouvert : cela signifie que n'importe qui peut se connecter incognito à leur signal Wi-Fi, et qu'il est très facile d'**espionner toutes les informations** échangées sur le réseau (identifiants, mots de passe, courriels, etc.) ou stockées sur les ordinateurs qui le composent (documents, programmes, etc.).

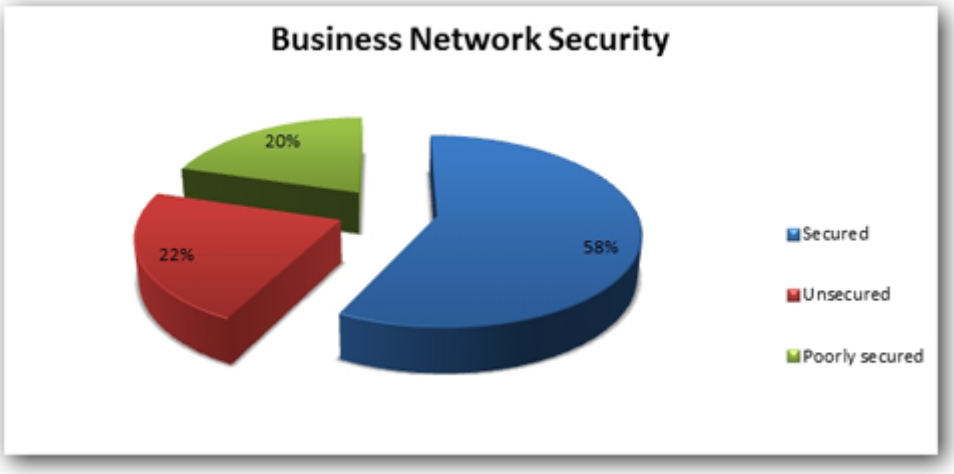
Par ailleurs, **11% des routeurs** (box) étudiés restent accessibles avec leur **mot de passe d'origine** (souvent *admin / admin* ou *admin / password*). Il est impératif de le changer pour préserver un accès privé au cœur du réseau !

Enfin, **3% des abonnés** internet ont choisi de **masquer leur SSID** (nom du réseau) dans la liste des réseaux sans fil disponibles. Si cette précaution permet de rester discret par rapport aux pirates en herbe, les hackers plus expérimentés verront ces réseaux cachés sans aucune difficulté.

Les réseaux Wi-Fi en entreprise

Les pirates affectionnent les réseaux Wi-Fi pour de multiples raisons. Certains hackers spécialisés visent notamment les réseaux sans fil des entreprises, notamment pour y dérober des **informations à haute valeur ajoutée** : codes sources, listes de clients, propriété industrielle, etc.

Premier écueil des réseaux sans fil professionnels : fréquemment, le SSID indique explicitement le nom de l'entreprise (ex : *dupont&associes_wifi*). Les pirates n'en demandent pas tant !

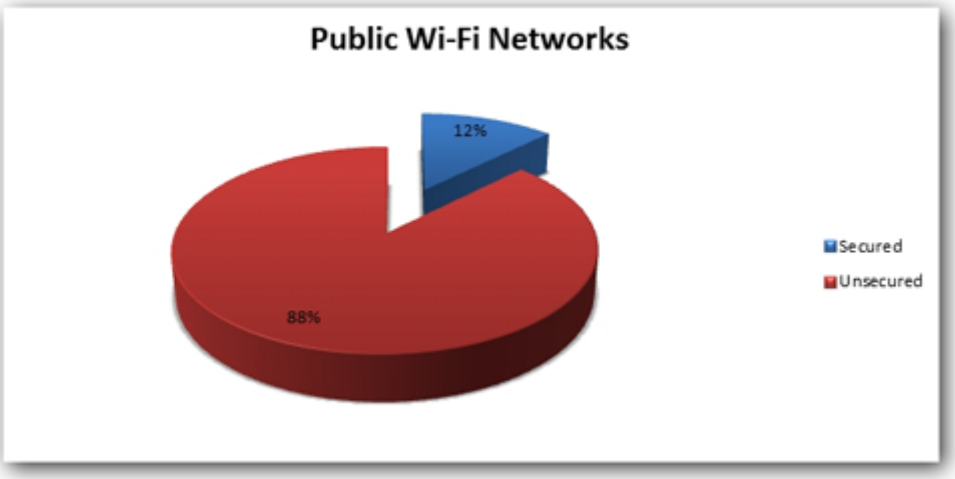


62% des entreprises étudiées protègent leur réseau sans fil avec un cryptage solide de type WPA ou WPA2. **20% ont choisi un chiffrement obsolète** (15% de WEP), et **22% aucun protocole de cryptage** !

De manière générale, les réseaux Wi-Fi en entreprise sont largement déconseillés. Souvenez-vous d'ailleurs du piratage d'informations au sein du studio de musique de David Guetta. Si toutefois l'entreprise décide tout de même de mettre en place un réseau Wi-Fi, que les dirigeants s'assurent qu'ils soit suffisamment **protégé** (cryptage WPA2, mot de passe solide, filtrage MAC), et complètement **indépendant** du réseau informatique principal.

Et la sécurité des hotspots ?

Les hotspots, c'est à dire les réseaux Wi-Fi ouverts que l'on trouve dans les restaurants, les hôtels, les gares, etc., sont par définition **accessibles à tous**. Il devient alors très facile pour un pirate connecté d'**espionner tous les échanges d'informations** des autres internautes sur le réseau. C'est même à la portée de tous avec des applications telles que Firesheep, Droidsheep ou FaceNiff…



Sur l'ensemble des réseaux Wi-Fi publics étudiés, seuls **12% sont protégés par une clé de cryptage**, souvent remise au client sur son ticket de caisse. Les hotspots restants (88%) ne sont sécurisés par **aucun chiffrement**. Autant dévoiler vos identifiants et autres accès (sites, mails, banque, etc.) avec un mégaphone sur la place du marché un samedi à midi, vous gagnerez du temps…

Une sécurité de façade

Certaines mesures censées sécuriser les réseaux Wi-Fi donnent un **sentiment de protection** mais représentent en réalité de **vraies passoires** : c'est notamment le cas du cryptage WEP, du mot de passe par défaut pour accéder au routeur (box), et même du filtrage par adresse MAC. Ces "sécurités" sont crackables ou contournables facilement de nos jours : il suffit pour cela de suivre la marche à suivre dictée par de nombreux tutos disponibles sur internet. Bref, le Wi-Fi inspire fréquemment **un faux sentiment de sécurité**.

Pour autant, **configurer une sécurité raisonnable** sur son réseau Wi-Fi est assez rapide, et même assez **simple à réaliser** soit-même. Notamment si vous suivez les **fiches pratiques** et les **didacticiels** Panoptinet, adaptés à chaque box !

Enfin, n'oubliez pas que sécuriser son Wi-Fi, c'est bien sûr le **protéger** (cryptage WPA2), mais aussi le **surveiller** avec un logiciel adapté (ex : Achiwa).

25% des réseaux Wi-Fi sont vulnérables. Et le vôtre ?

Source : malwarecity.fr

This entry was posted on Thursday, October 20th, 2011 at 2:38 pm and is filed under Autres actualités
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.