Les réseaux sans-fil sont plus sûrs mais…

Pour la seconde année, **Motorola** réalise une étude sur les **tendances de la sécurité des réseaux sans-fil**. Baptisé AirDefense, l'étude cible les efforts réalisés par les 4.000 boutiques situées à Atlanta, Boston, Chicago, Londres, Los Angeles, New York, San Francisco, Paris, Séoul et Sydney en vue de sécuriser au mieux les terminaux.

Si **44% des appareils sans fil** utilisés par les détaillants, à savoir des ordinateurs portables, des smartphones ou encore des lecteurs de codes barres pourraient être **vulnérables**, ce chiffre est en très nette diminution par rapport à l'année précédente. En **2007**, le rapport sur la vente au détail relevait alors que **85%** des appareils sans fil étaient susceptibles de contenir des failles de sécurité.

Concernant la sécurité des mobiles, l'étude cible les failles principales et récurrentes : « ***faiblesse du cryptage****, fuite des données,* ***mauvaise configuration*** *des points d'accès et installation d'un microprogramme obsolète sur les points d'accès. En utilisant la* ***même technologie****, la même configuration, la même sécurité et/ou les mêmes conventions de nommage dans tous leurs points de vente,* ***les mêmes vulnérabilités se reproduisent sur l'ensemble de la chaîne de magasins*****«** .

De même Motorola AirDefense a étudié 7.940 points d'accès de connexions de type WLAN avec un résultat probant : « ***32 % n'étaient pas cryptés****. Les conclusions sont les mêmes que l'année dernière : 25 % des points d'accès continuent d'utiliser le protocole* ***WEP*** *(Wired Equivalent Privacy), peu puissant et qui peut être décodé en quelques minutes*« .

A la loupe, l'étude révèle d'autres détails intéressants comme le fait que les détaillants de **Los Angeles et de New York** sont en tête en matière de déploiement de solutions de cryptage (**77 %** de leurs points d'accès sans fil). Les distributeurs parisiens se classent en deuxième position avec 76 % .

Reste qu'à travers le monde, 22 % des points d'accès, soit **1.740, sont mal configurés,** un chiffre presque effarant qui représente une augmentation de 13% par rapport à l'enquête 2007.

Par ailleurs, certains réseaux sont déployés à l'aide de configurations par défaut et de SSID (Service Set Identification), tels « Sans fil détail », « Caisse enregistreuse », « WiFi PDV » ou « Magasin n°1234 » et « Par défaut ». C'est un signal pour les pirates qui leur indique que rien n'a changé sur ces appareils et sur l'ensemble du réseau.

« Dans tout le pays, les enseignes nationales améliorent leur sécurité sans fil, ce qui explique la diminution importante des appareils sans fil vulnérables que nous avons découverts lors de nos initiatives de surveillance cette année , beaucoup, l'objet d'une réflexion a posteriori ». explique Richard Rushing, Senior directeur de la sécurité de l'information, Mobile Devices, Motorola. Toutefois, la plupart des détaillants restent encore exposés à une intrusion de réseau, signe que la sécurité sans fil fait, pour

L'étude cible donc les efforts qu'il reste à réaliser en matière de sécurisation des communications sans fil. Véritable manne pour les constructeurs, elles constituent aussi un point d'entrée de plus en plus important pour les hackers