WiFi et sÃ©curitÃ© : 6 conseils pour protÃ©ger votre rÃ©seau sans fil
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 14/6/2011 13:00:00

Que se soit pour se protÃ©ger contre les attaques malveillantes, pour**assurer la protection de ses donnÃ©es** ou mÃªme pour Ãªtre en accord avec la lÃ©gislation HADOPI, sÃ©curiser son rÃ©seau WiFi est aujourd'hui indispensable. **Peter Vogt,** directeur commercial pour la France chez Astaro, expert en sÃ©curitÃ© informatique, nous **donne ses conseils.**

Pour preuve, il y a quelques semaines, le DJ franÃ§ais **David Guetta** annonÃ§ait que le rÃ©seau WiFi de son studio d'enregistrement avait Ã©tÃ© piratÃ© depuis l'extÃ©rieur dans le but d'obtenir la version inachevÃ©e d'une chanson inÃ©dite sur laquelle il Ã©tait en train de travailler.

Autre exemple rÃ©cent : le scandale en 2010 de la collecte de donnÃ©es non protÃ©gÃ©es par Google, qui avait soulevÃ© pour la premiÃ¨re fois le problÃ¨me du manque de sÃ©curitÃ© au niveau des points d'accÃ¨s WiFi. Les vÃ©hicules Street View de Google avaient, non pas piratÃ© ou volÃ©, mais simplement collectÃ© des donnÃ©es qui, d'un point de vue mÃ©taphorique 'flottaient dans l'air' et qui, en thÃ©orie, Ã©taient Ã©galement accessibles Ã tous.

Si de telles affaires restent encore marginales, force est de constater qu'elles se sont multipliÃ©es ces derniers mois et soulignent l'importance pour les particuliers comme les professionnels de mettre en place des solutions de sÃ©curitÃ© adaptÃ©es.

Car de nos jours, n'importe qui ayant des compÃ©tences technologiques raisonnables peut collecter des donnÃ©es Wifi, aussi est-il important de renforcer la protection des rÃ©seaux sans fil.

Voici quelques conseils faciles Ã suivre pour sÃ©curiser son rÃ©seau WLAN :

â¢ Utiliser le chiffrement WPA2 - Les anciennes options de sÃ©curitÃ© telles que la clÃ© WEP peuvent Ãªtre dÃ©jouÃ©es en quelques instants sans Ã©quipements ou techniques spÃ©cifiques en utilisant quelque chose d'aussi simple qu'un module complÃ©mentaire de navigateur ou une application de tÃ©lÃ©phone mobile. WPA2 est le dernier algorithme de sÃ©curitÃ© inclus avec pratiquement tous les systÃ¨mes sans fil, accessible le plus souvent via l'Ã©cran de configuration.

â¢ Utiliser un mot de passe de plus de 10 caractÃ¨res - MÃªme les derniers mÃ©canismes de chiffrement tels que le WPA2 peuvent Ãªtre compromis en utilisant des attaques qui emploient un processus automatisÃ© pour essayer des milliards de mots de passe possibles. Les longs mots de passe n'ont pas besoin d'Ãªtre difficiles Ã retenir. L'utilisation d'une phrase telle que Â« securiser parfaitement mon reseau sans fil Â» plutÃ´t qu'un mot de passe court et complexe comme Â« w1f1p4ss! Â» offre bien plus de sÃ©curitÃ©, Ã©tant donnÃ© que la puissance de calcul nÃ©cessaire pour tester et craquer une clÃ© aussi longue est impossible Ã atteindre.

â¢ Dans votre mot de passe, ajouter des nombres, des caractÃ¨res spÃ©ciaux et des majuscules et minuscules - Les mots de passe complexes multiplient la quantitÃ© de caractÃ¨res qui doivent Ãªtre pris en compte pour les craquer. Par exemple, si votre mot de passe comprend 4 chiffres et que vous n'utilisez que des nombres, il y a 10 puissance 4 (10 000) possibilitÃ©s. Si vous utilisez en plus l'alphabet en minuscules seulement, vous obtenez alors 36 puissance 4 (1,6 million) possibilitÃ©s. Forcer un programme de piratage Ã choisir parmi 104 caractÃ¨res puissance 11 (11 chiffres) gÃ©nÃ¨re quelque 15 394 540 563 150 776 827 904 possibilitÃ©s. Le temps nÃ©cessaire pour dÃ©jouer un tel mot de passe est alors multipliÃ©, passant de quelques secondes Ã plusieurs millions d'annÃ©es !

â¢ Ne pas utiliser de SSID standard - Beaucoup de routeurs WiFi sont livrÃ©s avec un nom de rÃ©seau sans fil par dÃ©faut (ou SSID) tel que Â« netgear Â» ou Â« linksys Â» que la plupart des utilisateurs ne prennent pas la peine de changer. Cet identifiant SSID est utilisÃ© comme Ã©lÃ©ment du mot de passe par le chiffrement WPA2. Ne pas le modifier permet aux pirates de composer des listes de consultation de mot de passe pour les SSID courants, qui accÃ©lÃ¨rent considÃ©rablement les processus de piratage, ce qui leur permet de tester des millions de mots de passe Ã la seconde. Un SSID personnalisÃ© augmente significativement le temps et le travail nÃ©cessaires pour tenter de compromettre un rÃ©seau sans fil.

â¢ Ne pas inclure vos informations personnelles dans votre SSID - Il ne faut pas donner aux hackers la possibilitÃ© de savoir que votre rÃ©seau vaut la peine d'Ãªtre compromis. Indiquer Â« Cabinet comptable Durand Â» comme SSID fournit des indications qui peuvent Ãªtre utiles Ã un voisin indÃ©licat et techniquement habile ou pour quelqu'un qui veut nuire Ã votre sociÃ©tÃ©. N'offrez pas aux pirates le moyen de savoir si un rÃ©seau sans fil vous appartient, ou s'il dÃ©pend de la sociÃ©tÃ© qui se trouve au coin de la rue. Utilisez un identifiant vague qui ne vous dÃ©signe pas personnellement, ni ne permet de vous localiser.

â¢ RÃ©gler au plus juste la portÃ©e du signal radio - Les points d'accÃ¨s modernes disposent de plusieurs antennes et puissances de transmission, et diffusent des signaux bien au-delÃ des murs de votre sociÃ©tÃ© ou votre maison. Certains produits vous permettent de rÃ©gler la puissance de transmission des ondes radio via des options de menu. Il est ainsi possible de limiter gÃ©ographiquement la couverture d'un rÃ©seau WiFi, empÃªchant des utilisateurs extÃ©rieurs de se connecter et maximisant la protection.