



Article de Patrick Naoum
Vice-président, Technologies et Services professionnels
ESI Technologies

La communication sans fil... sans sécurité ?

Au bureau, à la maison ou en déplacement, les utilisateurs reliés à un réseau local sans fil Wi-Fi négligent trop souvent la sécurité de leurs opérations informatiques.

Dans ce type de communication, tout est mis en oeuvre pour procurer un accès facile à l'utilisateur. La sécurité y est beaucoup moins étendue que dans un réseau d'entreprise. Entre autres négligences, le pare-feu n'existe généralement pas. Le risque est grand, mais ignoré en grande partie. Résultat : le sans fil prolifère, mais les incidents se multiplient.

Ainsi, il est facile pour quelqu'un s'y connaissant le moins de se relier au réseau sans fil d'une personne se trouvant dans un rayon rapproché – c'est-à-dire à l'échelle d'un quartier. Non seulement un pirate peut-il alors naviguer gratuitement sur Internet, mais il lui est possible d'accéder aux transactions bancaires et aux autres opérations informatiques confidentielles effectuées par ce voisin.

Ainsi, les points d'accès indésirables - rogue access points en anglais – constituent une menace importante. En accédant à un réseau local sans fil, des personnes mal intentionnées sont en mesure d'y rattacher un réseau clandestin, comprenant des pages Web vers lesquelles elles attirent les utilisateurs, qui croiront qu'il s'agit là d'un site légitime. Cette pratique est en pleine croissance, et il est très difficile de détecter de tels réseaux. On n'y parviendra qu'à l'aide d'outils spécialisés.

La multiplication des points d'accès sans fil – ou hot spots – favorise les actes malveillants. Aujourd'hui, ces accès publics se retrouvent un peu partout : dans les aéroports, les chambres d'hôtel, les bibliothèques, les cafés Internet et de nombreux autres endroits. D'ailleurs, des solutions sont offertes au grand public afin de mettre sur pied et de gérer des services de points d'accès sans fil, de façon étonnamment aisée.

Les utilisateurs sont très peu conscientisés par rapport aux dangers auxquels les expose la communication sans fil. Pourtant, des mesures élémentaires peuvent être prises pour se protéger. Dans un premier temps, il est impératif d'installer sur son PC un coupe-feu configuré en fonction de la norme Wi-Fi, de même qu'un antivirus.

On peut aussi protéger ses systèmes ou ses fichiers critiques à l'aide de mots de passe, en prenant soin de choisir des termes complexes, que l'on ne pourra pas deviner. Facteur important à cet égard, les mots de passe fournis dans la configuration initiale de produits tels les routeurs et les antivirus doivent être changés, car ils sont connus de tous.

Les contenus d'entreprise devraient toujours être chiffrés. Beaucoup d'organisations ont adopté des mesures strictes à cet effet, et les employés doivent les appliquer quand ils font appel à la norme Wi-Fi pour travailler à l'extérieur du bureau. Également, on doit éviter de transmettre des courriels à partir des points d'accès publics, parce qu'il est alors facile de les intercepter. Enfin, une autre précaution de base consiste à ne pas laisser son ordinateur connecté au réseau sans fil durant les périodes où on ne l'utilise pas.

Il existe d'autres solutions permettant de renforcer la sécurité de la communication sans fil, mais comme elles font appel à des technologies récentes, leur mise en oeuvre est complexe et onéreuse. L'une de ces solutions permet d'équiper le réseau d'un mécanisme d'autodéfense, grâce auquel les ordinateurs problématiques sont automatiquement détectés. Une autre vise à éradiquer les vers informatiques du réseau, en détectant le fonctionnement anormal des ordinateurs qui en sont infectés. Un tel système permet de réduire le risque de plus en plus grand causé par le trop long intervalle existant entre le moment où apparaît un nouveau ver et celui où une rustine est diffusée afin de le contrer.

Bien que certaines organisations les aient mises à l'essai, aux États-Unis surtout, et qu'elles s'avèrent prometteuses, de telles solutions exigent pour le moment un investissement de plusieurs centaines de dollars par poste de travail. Heureusement, les mesures de protection fondamentales dont nous avons parlé demeurent économiques et efficaces, et peuvent être appliquées dès maintenant.