22% des réseaux sans fil ne seraient pas sécurisés à Paris

On le sait, le protocole Wi-Fi ne présente pas une sécurité maximum. Et la problématique devient critique dans le cadre professionnel. Même avec l'utilisation du réseau sans fil interne à l'entreprise: le signal passe à travers les murs. Le risque est connu: risque d'intrusion ou de vols de données par des pirates extérieurs adeptes du »

drive-hacking« . Afin de mesurer le risque, RSA Security mène depuis plusieurs années des études dans les grandes villes. Elle consiste à parcourir les principaux quartiers de chaque ville afin de détecter les réseaux sans fil et d'en évaluer la perméabilité aux intrusions extérieures. Une conclusion s'impose d'emblée: le risque est important mais il faiblit d'années en années. A Paris, RSA affirme que 22% des réseaux sans fil professionnels ne sont pas sécurisés contre 32% il y a deux ans. L'amélioration est significative. Elle a été rendue possible, comme dans d'autres villes, par l'adoption régulière des systèmes de protection WEP. RSA souligne que *« la sécurité a été plus prise au sérieux à mesure que le nombre d'utilisateurs a augmenté »*. En effet, la sécurisation des réseaux sans fil est d'autant plus appréciable que le nombre de ces derniers a augmenté de 120% dans la capitale entree 2004 et 2006. Selon RSA on en dénombre 573 contre 261 il y a deux ans. Pour autant, 22%, cela fait encore beaucoup: plus de 120 réseaux sans fil de la capitale seraient ainsi vulnérables. Sans compter les milliers de réseaux domestiques (les fameuses box) qui dans la grande majorité des cas ne sont pas protégés par les utilisateurs. Il suffit parfois d'allumer un PC dans la rue pour s'étonner du nombre de réseaux Wi-Fi personnels ouverts comme des moulins. *« Sans dramatiser les résultats de cette étude, il est encore nécessaire d'alerter les consommateurs et les organisations pour les inciter fortement à crypter leurs communications sans fil et à changer les configurations par défaut des boîtiers de connexion qu'ils utilisent [NDLR: 21% des réseaux observés à Paris sont paramétrés par défaut, constate l'étude]. Les conséquences d'une utilisation d'informations privées est encore trop grave pour être négligée »*, souligne Tim Pickard, Vice-Président en charge du Marketing chez RSA Security. **Hot-spot illégaux** La modification des données SSID (Service Set Identifier), de l'adresse MAC (Media Access Control) et l'utilisation de clés WEP sont indispensables. Autant pour l'administrateur réseau en entreprise, que pour le consommateur lambda chez lui. Mais Paris est, selon l'étude, la ville la mieux sécurisée en matière de Wi-Fi face à Londres (26% de réseaux non sécurisés) ou New-York (25%) où des études similaires ont été menées. Enfin, l'étude de RSA souligne encore une fois le danger potentiel des points d'accès publics (hot-spots) dans le cadre d'une utilisation professionnelle. Ouverts au plus grand nombre, ces points d'accès sont donc peu protégés. D'ailleurs, les hotspots 'illégaux' apparaissent comme la dernière menace à la mode, souligne RSA. Les hotspots illégaux sont des points d'accès sans fil installés de manière temporaire dont l'interface ressemble à de véritables hotspots afin de recueillir des informations personnelles sur les utilisateurs). Capgemini a ainsi mené une expérience dans ses bureaux en Grande-Bretagne en installant un système d'accès à Internet à partir d'un PC portable qui simule un hotspot. La société a ainsi observé que des personnes venaient se connecter sur son hotspot en présumant qu'il s'agissait d'un hotspot public. Ces hotspots frauduleux permettent en effet d'accéder à Internet tout en divulguant son numéro de carte de crédit. Le risque est très élevé si on considère que ce procédé permet de recueillir une somme d'informations personnelles plus importante que via un e-

mail lancé par une attaque dephishing. *« Les hotspots frauduleux constituent actuellement une menace à prendre au sérieux. Ils sont faciles à installer et les pirates sont pratiquement certains de recueillir des informations fiables dans un délai restreint »*, commente Phil Cracknell, de Capgemini UK Security Consulting Practice.