La sécurité, point noir de la mobilité professionnelle ?

Progressivement, les solutions de mobilité professionnelle font leur entrée dans l'entreprise. Il y a d'abord eu le décollage massif de l'e-mail mobile avec des solutions comme le Blackberry. Aujourd'hui, les applications métiers mobiles, qui permettent véritablement de générer un retour sur investissement, commencent à être déployées, notamment dans les sociétés qui s'occupent de maintenance.

Toutes ces applications qui font gagner du temps aux salariés (et de l'argent à leurs entreprises) profitent de la montée en puissance des réseaux sans fil: GPRS/Edge/UMTS et Wi-Fi. Pour autant, le principe même de la mobilité professionnelle pose un problème de sécurité. Comment être sûr que les données échangées sont bien protégées, quelle confiance peut-on accorder à ces réseaux? Comment éviter les intrusions? Ces questions deviennent aujourd'hui prioritaires pour les chefs de projets et d'entreprise. Presque plus que le ROI pourtant longtemps considéré comme l'argument de choix numéro un. **Wi-Fi/WiMax: des passoires** Et il y a en effet de quoi s'inquiéter. Un gros doute pèse sur les réseaux et en particulier sur le Wi-Fi (et donc à terme le WiMax). Ce protocole utilisant les ondes radio a à de nombreuses reprises montré ses faiblesses. Pourtant, il est très massivement utilisé par les travailleurs nomades. Si à l'intérieur des bâtiments le Wi-Fi peut être parfaitement sécurisé, à l'extérieur, ce n'est pas la même affaire. Or le nombre de cadres qui utilisent le Wi-Fi pour échanger des datas avec leurs entreprises ne cesse de progresser, à mesure où les hot-spots (points d'accès) poussent comme des champignons. *« Il n'y a aucune sécurité sur les hot-spots d'Orange et de SFR »*, explique sans ambiguité Guy Pujolle, Directeur scientifique d'Ucopia, universitaire et expert reconnu dans le domaine des réseaux. Pas de doute, le Wi-Fi public (et donc le futur WiMax) est une passoire. *« C'est aux opérateurs de réagir, or ils estiment que le risque n'est pas important »*, ajoute-t-il. *« C'est une démarche dangereuse car les opérateurs sont responsables »*. De plus en plus de « pirates » tirent profit de ces accès mal sécurisés et s'y connectent à l'insu de leurs propriétaires pour mener à bien leurs actions illicites. Cette faiblesse peut aussi être exploitée par les virus mobiles. Des virus qui commencent à se développer. Il y a un an, un homme basé à Toronto a été arrêté en flagrant délit de « War Driving ». En voiture, muni de son ordinateur portable et d'une carte wireless, il sillonnait les rues à la recherche de réseaux Wi-Fi faillibles. **Manque d'information** Bien que de plus en plus d'équipements Wi-Fi intègrent des fonctionnalités de sécurité, elles sont rarement activées par défaut et peu mises en place par l'utilisateur. La cause est tout simplement la complexité de la sécurisation par un novice. Interrogé par le *New Scientist*, Bruce Schneier explique *« Quand le confort des utilisateurs et les fonctionnalités de sécurité sont en conflit, la sécurité se dégrade. A mesure que les réseaux Wi-Fi deviennent populaires, l'insécurité grandit »*. Même constat de la part de Guy Pujolle: *« Les utilisateurs sont mal informés, ils ne configurent pas la sécurité de leurs équipements. Il est indispensable d'établir des règles strictes de sécurité »*. Le Wi-Fi est tellement peu fiable que des grandes entreprises ont même décidé de lui tourner le dos. *« Au siège de France Télécom, le Wi-Fi destiné aux collaborateurs, et permettant un accès à l'Intranet, est purement et simplement interdit »*, révèle l'expert. L'opérateur offre bien un accès sans fil 'visiteur', mais il ne passe pas par l'Intranet ! Le déploiement de points d'accès répond malheureusement plus à une logique économique que sécuritaire. Car un hot-spot ne coûte pas cher: environ 50 euros. Mais la

sécurisation de ces accès multiplie la facture par 10! Et tous ne sont pas prêts à investir pour se mettre aux normes. Les exploitants de ces hot-spots ont tout intérêt à jouer la carte de la sécurité. D'autant que des solutions existent. Divers entreprises se sont positionnées sur ce marché: Aruba, Ucopia… Cette dernière propose par exemple des solutions logicielles qui permettent d'améliorer la protection: filtre, accès VPN… Des universités, des centres hospitaliers ou des collectivités ont déjà déployé ce type de solutions **Renforcer les terminaux** Pour autant, l'entreprise souligne n'avoir jamais reçu de témoignages d'utilisateurs Wi-Fi s'étant fait pirater. Mais peut-on s'apercevoir de telles intrusions? Une ombre plane donc sur ces réseaux sans fil. Mais aussi sur les terminaux (vulnérables lorsqu'ils fonctionnent ou lorsqu'ils sont perdus) et les infrastructures qui supportent la transmission de données. Ces terminaux renferment de plus en plus d'informations critiques qui sont échangées avec le SI de l'entreprise. *« Le risque est relatif mais il peut pénaliser l'essor de la mobilité professionnelle »*, explique Mikaël Taillepied, Sales Manager pour la France chez Extended Systems, un spécialiste de la protection des données et de la sécurité des échanges d'informations. Le risque est désormais bien connu. Les doutes autour du Blackberry, les données entreprise qui passent par un serveur extérieur…, ont alerté un grand nombre de professionnels. *« La demande est très importante, le sujet est abordé systématiquement »*, souligne le Sales Manager. Des entreprises comme la sienne ont donc le vent en poupe en proposant des solutions packagées permettant de sécuriser des flottes mobiles, qu'il s'agisse de 10 ou de 15.000 terminaux. Sa base de clients à été multipliée par deux en un an. *« Nous sommes capables de protéger des solutions d'e-mail mobile mais aussi celles supportant des applications métiers critiques »*, explique Mikaël Taillepied. La société a ainsi noué d'étroites relations avec les fabricants de terminaux et les éditeurs d'applications mobiles. Les géants du secteur ont également pris la mesure de la problématique. Microsoft vient par exemple de mettre à jour son tout nouveau Windows Mobile 5.0 afin de renforcer la sécurité des terminaux qui font tourner cet OS. Il s'agit par exemple d'empêcher à distance l'utilisation d'un PDA perdu et d'apporter de nouveaux outils d'authentification, comme les Certificats. Bref, le marché de la sécurité destinée à la mobilité professionnelle a de beaux jours devant lui.