Mobiles & Sécurité : quels sont les vrais risques pour les entreprises ?

La question de la sécurité des terminaux mobiles a brutalement refait la 'une' de l'actualité ces dernières semaines. Le 25 juin dernier, la police espagnole arrêtait le présumé créateur des deux principaux virus touchant les mobiles : Cabir et CommWarrior. Quasiment à la même date, une circulaire officielle demande à certains services de l'Etat français de bannir purement et simplement le BlackBerry. En cause : la sécurité des messages qui pourraient être interceptés lors de leur transit à travers les serveurs de RIM au Canada et en Angleterre.

L'organisation par le forum Atena d'un atelier sur la question le 28 juin dernier tombait donc à pic. Il a permis de refaire un point sur cette question sensible : quels sont les risques concrets pour les entreprises avec des mobiles toujours plus perfectionnés, s'approchant des fonctionnalités d'un PC mais aussi de ses failles ? Les smartphones et les PDA incluent désormais des outils de communication, de synchronisation, de stockage qui multiplient les risques.

Les participants ont très vite fait le distinguo entre risques grand public et risques en entreprises. François Paget, de McAfee Avert explique que *» les menaces planent sur le téléphone mobile, les virus se focalisent à 70% sur les environnement Symbian. Pour autant, l'activité virale a tendance à se calmer et ces virus sont avant-tout des 'proofs of concept' peu dangereux qui ont besoin de l'accord explicite de l'utilisateur pour s'installer »*.

Dans le domaine grand public, la tendance est aujourd'hui à la convergence des menaces. *« En effet, dans les années 2000 les créateurs de virus le faisaient pour le 'fun'. A l'heure actuelle on s'oriente vers une nouvelle cybercriminalité dont le but est de gagner de l'argent ou bien de nuire : contacter des numéros surtaxés, spam, phishing, spam SMS incitant à se connecter à un site pour vérifier ses gains, un bip avec un numéro surtaxé que l'on a tendance à rappeler, et enfin le SMishing contraction de SMS et de Phishing » ,* ajoute François Paget.

Mais ces risques impactent peu l'entreprise. Pour Jean-François Tesseraud, RSSI chez EADS/ITS, le danger vient de l'utilisation d'un PDA ou d'un smartphone pour se connecter au Système d'Information de l'entreprise.

Mails, applications métiers, accès aux bases de données etc., le mobile est aujourd'hui en relation étroite avec le SI. Les risques de détournement de données sont importants, *« au même titre que les laptops »*, insiste le responsable.

« Il est donc indispensable d'encadrer très précisément le déploiement d'une solution mobile », souligne le RSSI qui nous fait partager le processus en place dans son entreprise. Dans un premier temps, il s'agit de bien identifier les besoins de l'utilisateur : que veut-il ? Comment veut-il s'en servir ? A quoi et comment veut-il accéder ? Quelle est la criticité ? Ceci permet de définir les risques de la solution à mettre en oeuvre (Laptop, PDA..) ainsi que la politique de sécurité à associer.

Vient ensuite la définition et la mise en place de la solution (définition, mécanismes et règles d'utilisations), les règles d'administration, d'exploitation, la veille sécurité et enfin le service associé

à l'utilisateur et à la flotte d'appareils déployés. Un grand nombre de collaborateurs pouvant se trouver à l'étranger, le décalage horaire nécessite une assistance de tout instant.

Même tonalité de la part d'Olivier Caleff de Devoteam. *« Afin de limiter les risques, le RSI doit restreindre les droits de l'utilisateur et mettre en place une politique de sécurité adaptée à l'usage que l'utilisateur fait de son appareil. Il faut* ***sensibiliser*** *l'utilisateur sur les erreurs à ne pas commettre, être conscient que le chiffrement ne suffit pas. C'est une politique globale de sécurité qui doit être mise en place. Si les communications sont chiffrées vers l'entreprise via un VPN mais le PDA n'est pas verrouillé, c'est la porte ouverte vers le système d'information de l'entreprise »* explique-t-il.

Sécurité du BlackBerry : passe d'arme entre RIM et Microsoft Les récents déboires du BlackBerry avec les administrations françaises n'ont pas manqué de provoquer un flot de questions lors de cet atelier. Daniel Jouan directeur commercial de RIM a une nouvelle fois répété le discours officiel du constructeur : *« nos solutions sont cryptées de bout en bout et sont utilisées par de nombreux gouvernements (Canada, Etats-Unis…) » .* Pour répondre aux critiques à propos des serveurs de transit des messages situés à l'étranger, RIM souligne à nouveau que rien n'est stocké et que tout est chiffré. Mais pour Thierry Picq (Microsoft), implanter un serveur en France ne changerait rien, *« c'est l'infrastructure RIM qui pourrait ouvrir une backdoor ».* Pour Jean-François Tesseraud, RSSI chez EADS/ITS, *« le battage médiatique actuel est injuste car si à chaque fois que Microsoft avait une faille on interdisait l'utilisation de Windows ? ».* Mais un membre du ministère de l'Intérieur, présent dans la salle, ne semble pas partager cette opinion. *« Si on utilise une communication de RIM à RIM d'accord, mais si on envoie de RIM vers une adresse hotmail avec une personne qui relève son mail via le webmail d'un cybercafé, plus rien n'est sécurisé. Le chiffrement de bout en bout peut-être ; mais il faut bien savoir quels sont les bouts. »*