

DIRECTION INFORMATIQUE

Accueil

Sécurité mobile : enjeu méconnu des organisations

Direction informatique invite, à chaque parution, un chroniqueur qui traite d'un thème lié aux technologies de l'information en entreprise. Pour l'édition d'octobre, Sylvain Nadeau, directeur de la pratique Sécurité chez Victrix, traite de la sécurité mobile.

Sylvain Nadeau | 10/7/2011 1:51:00 PM



Sylvain Nadeau. (Photo: Victrix)

Concept encore très jeune, la mobilité entraîne des problèmes de sécurité dont nous ne sommes pas toujours pleinement conscients. Des solutions évoluées peuvent aider en ce sens, mais les organisations doivent apprendre à bien les choisir en fonction d'une politique de sécurité clairement définie.

Une pratique actuellement répandue dans les organisations fait en sorte que les appareils mobiles, et particulièrement les tablettes, sont utilisés sans que l'on tienne compte des notions fondamentales de sécurité. L'attrait de la nouveauté et l'empressement à se doter d'une technologie de pointe de façon à accroître son efficacité ou à se donner un avantage concurrentiel incite les entreprises à utiliser ces dispositifs sans avoir évalué au préalable les risques et les conséquences possibles.

Les employés se servent à des fins personnelles des appareils mobiles fournis par leur employeur. Pareillement, ceux qui acquièrent un appareil mobile pour leurs besoins personnels souhaitent ultérieurement le brancher dans le réseau d'entreprise. Ce phénomène a été constaté depuis quelques années déjà avec les téléphones intelligents, mais s'accroît à l'heure où les tablettes sont massivement commercialisées par un nombre croissant de fournisseurs.

Tout récemment encore, on apprenait qu'à l'échelle mondiale, les ventes de tablettes ont quadruplé au deuxième trimestre de 2011 par rapport à la période correspondante l'an dernier.

Au début de l'année, un rapport de la firme Infinite Research prévoyait qu'il se vendrait quelque 147,2 millions de ces appareils en 2015, comparativement à 16,1 millions en 2010. Selon Gartner, les tablettes seront utilisées dans 80 % des entreprises dès 2013.

Cette adoption rapide entraîne des problèmes qui ne sont pas sans rappeler les incidents de sécurité qui, à compter de l'an 2000, se sont multipliés sur Internet. Comme à cette époque, les organisations deviennent victimes d'une mode. Il est relativement simple pour un utilisateur moindrement habile de débloquer (jailbreaker ou rooter) son appareil mobile. Les raisons qui poussent les gens à faire cela est pour personnaliser leur appareil et y installer gratuitement des applications offertes sur l'AppStore ou l'Android Market. Le risque encouru en téléchargeant ces applications « *crackées* » publiées sur Internet est qu'un code malveillant y soit inséré, sans parler des enjeux légaux d'une telle manipulation qui pourraient entacher la réputation de l'entreprise ou de son utilisateur.

Pareil code malicieux permet à un pirate de recueillir des renseignements personnels ou de l'information sur l'entreprise, données dont la vente peut rapporter. Souvent, ne sachant pas que son appareil a été piraté, l'utilisateur ne prend aucune mesure particulière. Dès lors, l'appareil demeure vulnérable, car les personnes mal intentionnées sont en mesure de détecter les postes piratés.

Gestion des appareils mobiles

Certes, il existe des moyens de sécuriser ces appareils qui, au départ, ne sont pas sécuritaires. Toutefois, nous avons vu que le marché des tablettes croît à la vitesse de l'éclair; divers modèles sont maintenant commercialisés, mais les solutions d'entreprise permettant de les sécuriser n'ont pas évolué aussi rapidement.

Par conséquent, il n'y a pas de solution pouvant protéger l'ensemble des plateformes et des pratiques pour l'instant. Avant de déployer toute solution de ce type, les entreprises auront peut-être à choisir les plateformes qu'elles autoriseront leurs employés à utiliser. Il est également recommandé de normaliser autant que possible les pratiques entourant l'utilisation des appareils mobiles.

Cela dit, les solutions de gestion des appareils mobiles (ou solutions MDM pour *Mobile Device Management*) peuvent grandement aider à gérer, à surveiller et à contrôler l'usage de ces appareils. Elles comprennent un agent que l'on installe dans le téléphone ou la tablette et que l'on se procure par courriel ou téléchargement. Il devient alors possible de recueillir de l'information sur chaque appareil utilisé par le personnel pour des motifs d'affaires – par exemple quel est le code identifiant l'appareil, quelle est la personne qui l'utilise et quelle est la version du système d'exploitation qui y est installée. Selon la solution choisie, on pourra également exécuter une série de fonctions à distance – verrouiller l'appareil, le retracer, en supprimer les données ou faire une sauvegarde notamment. En cas de perte ou de vol d'un appareil, ces fonctions peuvent se révéler fort utiles.

Les solutions MDM permettent également de chiffrer les données contenues dans les

appareils mobiles. Elles forcent l'utilisation d'un mot de passe pour le déverrouillage de l'appareil et désactivent au besoin les appareils photo, des applications, le Wi-Fi ou le Bluetooth dont sont dotés les téléphones. En outre, elles détectent les appareils piratés et les applications installées sur chacun d'eux. Ainsi, devient-il possible de contrôler les applications utilisées et d'établir une liste de celles que l'on aura choisi d'interdire pour des raisons de sécurité ou tout autre motif. On peut même contrôler le téléchargement d'applications dans les appareils.

En plus des fonctions de sécurité, ces solutions comprennent des fonctions de gestion des appareils mobiles. Elles permettent ainsi de prendre le contrôle d'un appareil à distance afin d'effectuer une mise à niveau ou d'autres tâches de maintenance ou d'assistance technique. Par exemple, il est possible d'émettre des alertes à l'intention des administrateurs. On peut aussi établir des rapports d'utilisation grâce à diverses informations, notamment les appels effectués et les minutes d'utilisation pendant les heures de pointe et en dehors de ces heures. Dès lors, ces rapports permettent d'optimiser l'usage des appareils et de vérifier si les forfaits auxquels l'entreprise souscrit sont les plus avantageux, entre autres possibilités.

En outre, les fonctions administratives serviront à établir l'inventaire du parc d'appareils mobiles de l'organisation; à vérifier la durée de vie restante de la batterie de chaque appareil; à gérer le cycle de vie des appareils; à remplacer ceux qui sont moins performants; ou à décider s'il est temps ou non de renouveler le parc.

Sensibilisation nécessaire

Selon les politiques établies et les conditions d'utilisation mises en place, les organisations doivent choisir soigneusement la solution de gestion des appareils mobiles convenant le mieux à leurs affaires. Puisque plusieurs fournisseurs – grands et petits – proposent de telles applications, on doit comparer les différentes possibilités. Certaines solutions s'installent dans le réseau d'entreprise, d'autres sont offertes en mode infonuagique. Malgré la diversité de l'offre, ces applications demeurent relativement nouvelles et peu d'entreprises encore les utilisent.

Elles sont toutefois promises à un bel avenir; dans un récent sondage, 90 % des gestionnaires consultés disent vouloir mettre en œuvre de nouvelles applications mobiles en 2011. Près de la moitié d'entre eux croient que la gestion efficace de ces applications constitue une haute priorité. Selon la firme Research and Markets, la valeur du marché mondial des solutions MDM atteindra 391,3 millions de dollars en 2014.

Ces solutions se répandent cependant plus vite aux États-Unis qu'au Québec. Ici, un travail de sensibilisation important reste à faire. Déjà, les entreprises de services-conseils qui sont engagées de façon sérieuse dans ce domaine ont mené des bancs d'essai afin de déterminer quelles solutions sont les plus susceptibles d'aider leurs clients. Comme c'était le cas au moment où Internet a commencé à proliférer, les organisations doivent apprendre à définir des politiques d'utilisation et à composer avec les enjeux de la mobilité à l'aide de programmes de sensibilisation fermement appuyés par la haute direction.

À titre d'exemple, les dirigeants devront déterminer si les utilisateurs sont autorisés à se brancher sur un réseau non sécurisé; à activer le mode itinérance de leur téléphone lors de leurs déplacements; à utiliser sans restrictions les sites de téléchargement d'applications; à

établir des ponts entre différents appareils; ou à se servir de l'appareil photo ou des fonctions Bluetooth de leur appareil mobile. Il est nécessaire aussi de communiquer clairement et efficacement les directives pertinentes à l'ensemble du personnel.

On connaît aujourd'hui l'importance d'un coupe-feu et d'un antivirus en réseautique, mais cette reconnaissance a été chèrement acquise. Combien de virus ont infecté nos ordinateurs sans rencontrer de résistance avant que ne se généralise l'utilisation de mesures de sécurité fondamentales? La mobilité se trouve actuellement au même stade. Mieux vaut être proactif et éviter que des perturbations importantes ne viennent compromettre la bonne marche des affaires courantes par suite d'une utilisation négligente des appareils mobiles.

Accueil