SECURECOM
Services Conseils inc.

BYOD en 2014 – Le Défi

Ces dernières années, le phénomène 'Apportez le vôtre' (aka. Bring your Own Device, BYOD) s'est imposé au sein des entreprises et auprès des salariés. Nous y sommes donc exposés quotidiennement. Que pouvons-nous faire maintenant pour s'y adapter et en tirer profit?

En 2005, un rapport Gartner, Inc. indiquait que la « consumérisation informatique » constituait « la tendance qui aura l'impact le plus important sur le secteur de l'informatique durant les dix prochaines années » … Et ils avaient raison.

Le BYOD, ou en bon français « Apporter le vôtre » a suivi la courbe de croissance des téléphones intelligents, tablettes et autres ordinateurs portables. La popularité et l'émergence rapide de ces nouvelles technologies forcent les entreprises à revoir l'approche en vigueur face aux appareils provenant de l'extérieur et pouvant accéder aux ressources de l'entreprise.

Il peut sembler normal d'interdire l'utilisation des appareils personnels sur les lieux de travail. Toutefois, la pression de vos utilisateurs sera si grande et le phénomène si important qu'il finira par s'imposer. Imaginez qu'un employé mécontent de ne pas pouvoir accéder aux données de l'entreprise avec son téléphone, décide de les rendre disponible sur un site d'hébergement de fichiers ou par courriel. Le risque encouru par l'entreprise est alors plus grand que lors d'une implémentation du BYOD avec la mise en place d'une politique et des mesures de sécurité adéquates.

L'entreprise peut tirer avantage (flexibilité, mobilité, réduction des coûts, etc) du phénomène mais certains facteurs très importants doivent être adressés. Les points suivant devraient être examinés pour guider les entreprises vers une implémentation du BYOD qui leur sera profitable.

- Identifier les actifs auxquels les utilisateurs de chaque groupe doivent accéder. Par ex : un vendeur doit pouvoir accéder à la base de données d'adresse et d'information des clients. Par contre ce besoin ne serait pas requis pour tous les employés œuvrant dans les autres départements de l'entreprise.
- Identifier les zones d'accès et réaliser une analyse de risques pour évaluer le niveau de criticité des actifs pour chacune des zones.
- Une fois que l'entreprise a identifié les actifs auxquelles elle désire donner l'accès aux BYOD et les risques associés à ces actifs, une politique claire qui encadre cette pratique doit être mise en vigueur. Les employés devront y adhérer afin d'accéder aux différentes zones offertes. Cette politique devrait répondre à certaines questions importantes à adresser dès le départ.
    - Quelle est la politique de l'entreprise concernant l'utilisation des terminaux personnels ?
    - Le contenu de la politique de sécurité de l'entreprise est-il adapté à la pratique du BYOD et la pratique du BYOD est-elle conforme à cette politique ?

Juillet 2014

- Existe-t-il une politique concernant le remboursement des frais d'utilisation des appareils mobiles des employés ?
- Les données professionnelles présentent sur les appareils doivent-elles être séparées des données personnelles ? L'utilisation du chiffrement est-elle obligatoire?
- Comment l'entreprise peut-elle gérer et garder une forme de propriété intellectuelle sur des données ayant été transférées sur les terminaux mobiles de ses employés. La politique BYOD devra préciser ce qui relève de la vie personnelle et professionnelle (modalités de contrôles, sanctions encourues, Propriétés des données stockées)
- Les contrats de travail doivent-ils faire l'objet d'une modification ?
- Comment gère-t-on les terminaux perdus ou volés ?
- Comment gère-t-on les départs des employés ?
- Par quel moyen les utilisateurs se connecteront-ils (Wifi vs réseau cellulaire) ?
- Quel sera le niveau de surveillance ?

Cette liste n'est pas exhaustive mais constitue un bon départ pour toute entreprise désireuse de régulariser l'accès à ses ressources par les différents appareils mobiles personnels. La façon dont les administrateurs abordent et gèrent la sécurité de leur réseau doit être adaptée à la réalité des technologies d'aujourd'hui. La segmentation en différentes zones ou sous-réseaux sécurisés selon une politique d'accès bien établie, demeure une façon efficace d'isoler ou de démocratiser certaines données.

Même avec une bonne expertise à l'interne, les compagnies auraient avantages, tout au long du projet, à faire appel aux services d'une firme spécialisé en sécurité pour obtenir un avis externe et des conseils précis tout au long des différentes phases.

Pour terminer ce bref survol sur les considérations et questions qu'engendre le « BYOD », un court mot sur une autre tendance, le « COPE » ou *Corporate Owned Personaly Enabled*. Similaire en plusieurs points au BYOD, la différence est que les appareils « personnel » sont fournis par l'entreprise. Ceci facilite grandement la notion d'appartenance des données présentes sur l'appareil. Le COPE rend les aspects légaux moins flous mais diminue quelque peu les avantages financiers liés au BYOD. Voici un lient vers un article intéressant qui compare les deux solutions ICI. Quelle que soit la solution choisie, chaque entreprise devra bientôt tenir compte des périphériques mobiles de toutes sortes, cherchant à s'y rattacher. Êtes-vous prêt?

Dany Ouellet OSCP, MCSA security, Comptia sec+

www.securecom.ca
T : 514 544-0442
Contact : info@securecom.ca

SECUREcom
Services Conseils inc.