BYOD : Incontournable, mais de nouveaux besoins en sÃ©curitÃ©
Internet
PostÃ© par : JPilo
PubliÃ©e le : 25/2/2013 11:30:00

Les Ã©quipements mobiles, quâ□□il sâ□□agisse de PC portables, de tablettes ou de Smartphones font partie intÃ©grante de notre quotidien. Alors que la frontiÃ¨re entre lâ□□utilisation professionnelle et personnelle de ces matÃ©riaux sâ□□affine, les problÃ©matiques liÃ©es Ã ce phÃ©nomÃ¨ne se renforcent. **Quelle politique adopter face au BYOD afin de sÃ©curiser les flux dâ□□informations ?**

La notion de Bring Your Own Device (BYOD) est dÃ©finie par le cabinet Gartner comme une stratÃ©gie alternative permettant aux employÃ©s, partenaires et autres utilisateurs, dâ□□utiliser leurs terminaux personnels pour se servir des applications dâ□□entreprise et accÃ©der aux donnÃ©es. Mais ces donnÃ©es, soumises Ã des rÃ¨gles de confidentialitÃ© pour certaines, sont Ã la merci de la moindre faille de sÃ©curitÃ©.

Ce concept, trÃ¨s Ã la mode, est la consÃ©quence directe du succÃ¨s des Smartphones et des tablettes dans la sphÃ¨re personnelle ; les nombreux utilisateurs de ces terminaux souhaitent, de maniÃ¨re naturelle, pouvoir les utiliser dans leur activitÃ© professionnelle.

Un phÃ©nomÃ¨ne qui sâ□□est imposÃ© de lui-mÃªme

Les entreprises Ã©tant par nature moins agiles que les consommateurs, elles doivent apprÃ©hender ces terminaux sans quâ□□elles en aient elles-mÃªmes dÃ©cidÃ© le dÃ©ploiement. Ce type de situations nâ□□est dâ□□ailleurs pas vraiment nouveau. Les DSI avaient dÃ©jÃ connu ces problÃ©matiques lors du dÃ©veloppement du Wi-Fi dans la sphÃ¨re privÃ©e, ou encore lors de lâ□□apparition du GSM, alors que la pression des utilisateurs Ã©tait forte pour lâ□□adoption des technologies dans le cadre professionnel.

LÃ encore, la technologie et les utilisateurs sont allÃ©s plus vite que prÃ©vu. Le cabinet dâ□□Ã©tudes Forrester estime ainsi que 74 % des salariÃ©s utilisent deux terminaux au minimum au travail, et 52 % en utilisent trois ou plus.

Points Ã©galement importants, plus de la moitiÃ© ont une utilisation mixte, personnelle et professionnelle, et un tiers des Ã©quipements utilisent un autre OS que Windows.

Le BYOD et la sÃ©curitÃ© de lâ□□accÃ¨s au SystÃ¨me dâ□□Information

Lâ□□ouverture du systÃ¨me dâ□□information est un fait, le BYOD est la partie Ã©mergÃ©e de lâ□□iceberg. Le besoin des utilisateurs dâ□□utiliser leurs Ã©quipements personnels, lâ□□accueil des prestataires ou des invitÃ©s, le besoin de visibilitÃ© sur les Ã©quipements connectÃ©s au rÃ©seau interne de lâ□□entreprise engendre beaucoup de problÃ©matiques pour les DSI. Il faut faire face Ã une multitude dâ□□Ã©quipements et de profils dâ□□utilisateurs.

Beaucoup dâ□□entreprises ne savent pas rÃ©pondre aux questions suivantes : Qui se connecte ? Par quel Ã©quipement ? Lâ□□Ã©quipement utilisÃ© est-il conforme ? Comment gÃ©rer les droits dâ□□accÃ¨s ? Comment donner accÃ¨s aux applications et donnÃ©es de maniÃ¨re simple et ergonomique ? Et surtout : Comment veiller au respect de la politique de sÃ©curitÃ© de lâ□□entreprise, sans Ãªtre intrusif ?

Pour rÃ©pondre Ã ces enjeux il existe des solutions hÃ©ritÃ©es des technologies de NAC. Les solutions de NAC de derniÃ¨re gÃ©nÃ©ration ont Ã©voluÃ©es et gagnÃ© en maturitÃ© afin dâ□□offrir les services permettant de rÃ©pondre aux challenges du BYOD. On va donc Ãªtre en mesure de donner un accÃ¨s au SI Ã un utilisateur (quâ□□il soit interne ou externe) en fonction du type dâ□□Ã©quipement quâ□□il va utiliser, de son profil, du mode de connexion, et mÃªme en fonction du crÃ©neau horaire. De plus les nouvelles fonctions de profiling vont apporter de la visibilitÃ© en catÃ©gorisant tous les Ã©quipements connectÃ©s au rÃ©seau. Les politiques dâ□□accÃ¨s vont donc pouvoir Ãªtre appliquÃ©es en fonction de ces catÃ©gories.

Enfin pour illustrer les possibilitÃ©s, prenons lâ□□exemple dâ□□un collaborateur du service ressources humaines. Lorsquâ□□il se connecte depuis son PC de bureau il aura accÃ¨s aux applications liÃ©es Ã son mÃ©tier ainsi que toutes les ressources partagÃ©es de lâ□□entreprise (Intranet, Internet, emailsâ□¦). Si le mÃªme utilisateur se connecte avec un Ipad de lâ□□entreprise on pourra lui donner les mÃªmes droits dâ□□accÃ¨s. Par contre, sâ□□il utilise son Smartphone personnel, le RSSI souhaitera peut Ãªtre diffÃ©rencier les droits dâ□□accÃ¨s et ne donner accÃ¨s quâ□□Ã Internet aux tÃ©lÃ©phones sous Android et peut Ãªtre donner accÃ¨s Ã Internet et Ã lâ□□Intranet aux tÃ©lÃ©phones sous iOS. Les possibilitÃ©s sont nombreuses et peuvent rÃ©pondre aux exigences des politiques de sÃ©curitÃ© adaptÃ©es aux nouveaux usages de lâ□□entreprise.

Il faut prÃ©ciser, que les utilisateurs finaux attendent des nouveaux usages de ce phÃ©nomÃ¨ne BYOD.

Ces attentes, sont notamment :

? de pouvoir accÃ©der au SI de lâ□□entreprise, avec leurs terminaux personnels, de la maniÃ¨re la plus simple et ergonomique possible

? mais Ã©galement de pouvoir bÃ©nÃ©ficier de leur terminal personnel pour leurs usages personnels, en parallÃ¨le, des usages professionnels auxquels ils aimeraient prÃ©tendre. Dans ce dernier cas, on parle essentiellement de lâ□□accÃ¨s aux emails, agenda, contacts, lâ□□intranet, voire de certains applications mobiles (apps) dÃ©diÃ©es Ã lâ□□entreprise.

Il faut souligner Ã©galement, que des contraintes lÃ©gales viennent sâ□□ajouter aux demandes des utilisateurs, notamment, la capacitÃ© de ne pas contrÃ´ler (visualiser ou modifier) les donnÃ©es privÃ©es sur lesquelles lâ□□entreprise nâ□□a pas le droit de regard.

Pour rÃ©unir ces diffÃ©rentes contraintes et rÃ©pondre Ã ces nouveaux besoins, il est alors souhaitable de disposer de fonctionnalitÃ©s suivantes :

- Reconnaissance automatique du type de terminaux (Â« corporate Â», personnel, Smartphone, tablette...)

- Proposition du mode de connexion le plus adaptÃ©

- Enregistrement du terminal et affectation Ã lâ□□utilisateur correspondant

- Affectation des droits dâ□□accÃ¨s associÃ©s Ã lâ□□utilisateur et Ã son type de terminal,

- SÃ©paration des donnÃ©es professionnelles et privÃ©es sur lâ□□Ã©quipement mobile,

- VisibilitÃ© et contrÃ´le des donnÃ©es professionnelles.

Avoir une vue globale des besoins

Bien entendu, on prendra soin de rÃ©pertorier ces besoins dans une politique de mobilitÃ©, elle-mÃªme dÃ©pendant de la politique de sÃ©curitÃ© du systÃ¨me dâ□□information, concÃ¨dent **NoÃ«l Chazotte**, Directeur Marketing et Innovation SÃ©curitÃ© et **Etienne Didelot**, marketing Infrastructure et Communications UnifiÃ©es.

Une fois cette matrice rÃ©alisÃ©e, il est possible de mettre en place une feuille de route pour lâ□□adoption du BOYD de lâ□□entreprise et dÃ©finir une architecture correspondante.

Lâ□□adoption du BYOD peut Ãªtre classÃ©e en diffÃ©rentes phases, reprÃ©sentant la maturitÃ© dâ□□une entreprise dans ce domaine (la majoritÃ© des entreprises se trouvent actuellement dans la phase Â« limitÃ©e Â» ou Â« simple Â») comme le montre lâ□□infographie ci-dessus.

Selon un sondage rÃ©cent rÃ©alisÃ©e par NetIQ, 56 % des entreprises franÃ§aises ont mis en place une politique de gestion du BYOD. Le chemin vers une intÃ©gration optimale du BYOD dans les entreprises franÃ§aises est encore long, mais elles commencent Ã prendre conscience de lâ□□ensemble des paramÃ¨tres dâ□□infrastructure et de sÃ©curitÃ© Ã prendre en compte pour faire du BYOD un rÃ©el atout pour le monde professionnel.