DonnÃ©es d'entreprise et applications grand public : un mÃ©lange dangereux!
Internet
PostÃ© par : JulieM
PubliÃ©e le : 9/4/2014 13:00:00

Suite au rachat de WhatsApp par Facebook pour 16 milliards de dollars rÃ©cemment, un certain nombre de spÃ©cialistes ont fait remarquer que Facebook ne dÃ©boursait pas une telle somme uniquement pour acquÃ©rir 450 millions de nouveaux utilisateurs, mais plutÃ´t que le rÃ©seau social offrait 35 dollars pour rÃ©cupÃ©rer le rÃ©pertoire tÃ©lÃ©phonique de chacun de ces 450 millions d'individus.

Ã voluant dans le secteur de la mobilitÃ© professionnelle, je me suis immÃ©diatement posÃ© les questions suivantes : Â« Quels sont les noms et numÃ©ros qui figurent dans ces rÃ©pertoires ? Quel PDG, haut responsable ou personnalitÃ© importante permet Ã Facebook de contrÃ´ler son rÃ©pertoire de contacts ? Â» s'interroge *Nicko van Someren, Chief Technology Officer,* ***Good Technology***

L'ensemble des systÃ¨mes d'exploitation mobiles modernes et populaires ont Ã©tÃ© lancÃ©s aprÃ¨s que Facebook et Twitter soient fondÃ©s. Ces systÃ¨mes d'exploitation, ainsi que toutes les applications qui fonctionnent dessus, ont Ã©tÃ© crÃ©Ã©s pour un monde au sein duquel les utilisateurs souhaitent partager une grande partie de leur activitÃ© avec un grand nombre de gens.

WhatsApp n'utilise pas de subterfuge pour se procurer leurs carnets d'adresse ; ce sont les utilisateurs qui choisissent librement de livrer des donnÃ©es sensibles au service afin de profiter de capacitÃ©s indÃ©niablement utiles qui fonctionnent mieux lorsque l'application a accÃ¨s Ã ces donnÃ©es. En donnant sciemment son consentement, l'utilisateur est en mesure de fournir toutes les informations qu'il dÃ©tient, et les systÃ¨mes d'exploitation mobiles contemporains rendent cela facile.

Mais que se passe-t-il s'il utilise Ã©galement son tÃ©lÃ©phone pour travailler ? Si certaines donnÃ©es stockÃ©es sur l'appareil ne lui appartiennent pas ? Si la dÃ©cision de partager ces donnÃ©es ne lui appartient pas ?

Beaucoup d'entreprises sont confrontÃ©es aux problÃ¨mes posÃ©s par le contrÃ´le de leurs donnÃ©es une fois qu'elles permettent Ã leurs utilisateurs d'accÃ©der Ã ces donnÃ©es sur des appareils mobiles. Une approche possible pour rÃ©soudre ce problÃ¨me est d'utiliser des outils et des protocoles de gestion des appareils mobiles (MDM) tels que Exchange ActiveSync afin de synchroniser les donnÃ©es professionnelles sur l'appareil.

En cas de perte du terminal, les donnÃ©es peuvent en Ãªtre effacÃ©es, et si l'utilisateur quitte l'entreprise, il est possible d'effectuer une synchronisation spÃ©ciale provoquant la suppression des copies locales des donnÃ©es de l'entreprise prÃ©sentes sur l'appareil (mÃªme si, bien entendu, l'utilisateur disposera probablement d'une sauvegarde sur son ordinateur personnel Ã la maison).

La gestion des appareils peut Ãªtre un processus utile pour garder le contrÃ´ler des terminaux, mais en pratique, ce n'est pas une solution optimale pour garder le contrÃ´le des donnÃ©es. Ces outils permettent la gestion des appareils mobiles, et non pas des donnÃ©es mobiles.

Si une entreprise dÃ©ploie un parc d'appareils mobiles gÃ©rÃ©s par elle-mÃªme (auprÃ¨s de travailleurs sur le terrain ou sur des bornes interactives, par exemple) et qu'elle compte contrÃ´ler prÃ©cisÃ©ment les applications qui seront utilisÃ©es sur ces terminaux, alors les outils de gestion des appareils mobiles sont une excellente solution.

Cependant, si les appareils seront utilisÃ©s par les employÃ©s pour leurs activitÃ©s personnelles et professionnelles, alors il est nÃ©cessaire d'utiliser des outils permettant de gÃ©rer les donnÃ©es, et pas juste le terminal. Si les utilisateurs sont autorisÃ©s Ã installer WhatsApp ou autre application pouvant lÃ©gitimement solliciter l'accÃ¨s aux donnÃ©es prÃ©sentes sur l'appareil, il est essentiel de maintenir une sÃ©paration entre donnÃ©es personnelles et donnÃ©es professionnelles.

Notez bien que je n'ai pas Ã©voquÃ© le Â« BYOD Â» jusqu'ici. En effet, le besoin de sÃ©parer les donnÃ©es professionnelles des donnÃ©es personnelles ne se limite pas au cas oÃ¹ les utilisateurs amÃ¨nent leur propre appareil au travail. Le problÃ¨me n'est pas de savoir qui est lÃ©galement en charge de la gestion de l'appareil, mais de dÃ©terminer si l'utilisateur pense que l'appareil en sa possession lui appartient.

S'il l'amÃ¨ne avec lui en vacances, c'est qu'il considÃ¨re que l'appareil (qui contient ses photos, sa musique, ses vidÃ©os et surtout ses applications) est le sien. Ã moins que l'entreprise ait l'intention de restreindre complÃ¨tement l'appareil quant aux applications pouvant Ãªtre installÃ©es, il lui faudra alors prÃ©fÃ©rer une approche consistant Ã verrouiller l'accÃ¨s Ã ses donnÃ©es.

En effet, bien qu'il soit tout Ã fait concevable de verrouiller un appareil destinÃ© Ã Ãªtre utiliser sur une borne, ou qui sera rÃ©cupÃ©rÃ© au dÃ©but d'une journÃ©e de travail et rendu Ã la fin, en revanche, une telle protection peut Ãªtre extrÃªmement mal perÃ§ue, voire absolument inacceptable pour l'utilisateur si ce dernier considÃ¨re que l'appareil lui appartient.

Notons Ã©galement que les outils de gestion des appareils mobiles restent utiles pour les entreprises ayant adoptÃ© le BYOD comme pour celles gÃ©rant les appareils confiÃ©s Ã leurs employÃ©s, mais leur valeur rÃ©side dans la gestion des terminaux, et non pas des donnÃ©es.

Pouvoir s'assurer que les utilisateurs possÃ¨dent les identifiants pour se connecter au Wi-Fi d'entreprise, ont accÃ¨s au portefeuille d'applications nÃ©cessaires pour travailler, et disposent de versions des applications et du systÃ¨me d'exploitation Ã jour est un avantage trÃ¨s prÃ©cieux.

Mais en pratique, pour dÃ©ployer une stratÃ©gie de mobilitÃ© complÃ¨te, toute entreprise a besoin d'un ensemble d'outils complet afin de gÃ©rer les donnÃ©es, les appareils, les applications et les configurations ; pour contrÃ´ler la qualitÃ© de service ; et pour effectuer des analyses afin de s'assurer que tout fonctionne correctement.

Pour qu'une telle stratÃ©gie puisse Ãªtre dÃ©ployÃ©e, tous ces Ã©lÃ©ments doivent fonctionner de faÃ§on coordonnÃ©e plutÃ´t que de faÃ§on isolÃ©e. Il faut donc une solution de mobilitÃ© complÃ¨te et cohÃ©sive.

Par consÃ©quent, avant de laisser vos donnÃ©es d'entreprise sur un appareil mobile, posez-vous la question de savoir quels types d'applications pourraient Ãªtre exÃ©cutÃ©es dessus. Il ne s'agit pas simplement de faire attention aux logiciels malveillants ou Ã WhatsApp en particulier, mais de s'interroger plus gÃ©nÃ©ralement sur les applications pouvant Ãªtre installÃ©es et sur leur utilisation potentielle de vos donnÃ©es.

Dans certains cas, une fois ces applications installÃ©es sur votre appareil, vous disposerez de la rÃ©ponse Ã ces questions, et la gestion des appareils sera peut-Ãªtre appropriÃ©e. Mais si vous avez le moindre doute, il vous faudra mettre en place une solution des gestion des donnÃ©es.