BYOD, CYOD, Cloud, tÃ©lÃ©travail : La synchronisation met les donnÃ©es en danger
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 27/11/2013 13:30:00

BYOD (Bring Your Own Device), CYOD (Chose Your Own Device), travail Ã domicile, hausse des dÃ©placements... Les habitudes de travail sont en pleine mutation, les tablettes et les Smartphones sont devenus des outils de travail communs
Bien que la France ait pris du retard sur l'adoption de ces nouvelles formes de travail, les professionnels sont de plus en plus nombreux Ã nÃ©cessiter un accÃ¨s permanent et souvent distant Ã leurs donnÃ©es.

Dans ce but, nombres de services Cloud ont vu le jour pour permettre d'accÃ©der aux donnÃ©es et de les sauvegarder Ã distance. Souvent, les fichiers sont synchronisÃ©s avec le terminal mobile pour assurer un accÃ¨s immÃ©diat et rapide aux collaborateurs. Ces applications, qui sont pour la plupart initialement prÃ©vues pour les particuliers, ont rencontrÃ© Ã©galement un grand succÃ¨s auprÃ¨s des professionnels mobiles qui y trouvent un moyen simple et efficace de rÃ©pondre Ã leurs besoins en termes de mobilitÃ©. Mais ces applications gratuites ou faciles d'accÃ¨s n'offrent la plupart du temps qu'un cryptage des donnÃ©es de faible qualitÃ©.

Â

Elles mettent ainsi en danger les donnÃ©es de l'entreprise.

Depuis le rÃ©cent scandale d'espionnage commis par la NSA, de nombreux professionnels remettent en cause les applications et services qu'ils utilisent dans le cadre des accÃ¨s et sauvegardes Ã distance de leurs fichiers. Mais, l'espionnage et le piratage dans le Cloud sont loin d'Ãªtre les seuls dangers auxquels les donnÃ©es sont soumises lorsque dÃ©placÃ©es ou consultÃ©es Ã l'extÃ©rieur de l'infrastructure de l'entreprise.

Pour protÃ©ger correctement ses donnÃ©es il faut Ãªtre conscient que chaque information prÃ©sente sur le moindre terminal mobile est en danger. D'une part, la donnÃ©e disparaÃ®tra ou

sera dÃ©tournÃ©e en cas de perte du terminal, mais surtout, en cas de tentative d'espionnage, il ne faudra que quelques secondes Â« aux malfaiteurs Â» pour faire une Â« image Â» du tÃ©lÃ©phone et pouvoir ainsi rÃ©cupÃ©rer tout son contenu, y compris les donnÃ©es critiques qui s'y trouvent.

Les entreprises se heurtent donc Ã deux problÃ©matiques : d'un cÃ´tÃ© il est indispensable de pouvoir accÃ©der aux donnÃ©es depuis un terminal mobile, mais de l'autre l'accÃ¨s et la synchronisation des donnÃ©es sur ces mÃªmes terminaux reprÃ©sentent un danger de taille.

La solution est donc d'effectuer une synchronisation intelligente. Il est en effet, nÃ©cessaire de sÃ©curiser au maximum le terminal mobile et les transferts de fichiers via un chiffrage militaire, voire la mise en place de dates d'expirations des fichiers critiques synchronisÃ©s. Les donnÃ©es utilisÃ©es frÃ©quemment qui comportent peu de risque pourront quant Ã elles Ãªtre synchronisÃ©es automatiquement. L'utilisateur pourra de la sorte facilement y accÃ©der, travailler dessus, les modifier et les partager Ã souhait depuis son terminal sans aucun risque pour l'entreprise.

En revanche les donnÃ©es critiques doivent Ãªtre traitÃ©es avec plus d'attention. Elles devront ainsi Ã©viter d'Ãªtre conservÃ©es sur le terminal mobile pour diminuer les risques de fuites en cas de perte ou de vol du matÃ©riel. De plus leur accÃ¨s devra Ãªtre soumis au contrÃ´le de l'administrateur informatique qui pourra ainsi dÃ©cider cas par cas des accÃ¨s, synchronisation et partage dudit fichier depuis le mÃªme terminal mobile.
Â

Laurent Dedenis, PrÃ©sident et Directeur GÃ©nÃ©ral, Ventes et Marketing chez Acronis