Stocker dans le Cloud, c'est bien quand c'est sÃ©curisÃ©.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 27/6/2013 14:00:00

Stocker ses donnÃ©es d'entreprises dans **le Cloud, c'est pratique**, mais est-ce **aussi anecdotique d'un point de vue sÃ©curitÃ© ?**

Lorsque l'entreprise dÃ©cide de stocker ses donnÃ©es sur des serveurs Cloud prend-elle la mesure des menaces qui pÃ¨sent alors sur elle et sur ses donnÃ©es : risques de pertes de donnÃ©es Ã cause des serveurs, possibilitÃ© pour des tiers d'accÃ©der aux donnÃ©es, perte de gouvernance des donnÃ©es, problÃ¨me de souverainetÃ©.

La premiÃ¨re mesure de sÃ©curitÃ© Ã laquelle on pense pour protÃ©ger ses donnÃ©es dans le Cloud est dâ□□assurer un service de sauvegarde. Il s'agit certainement d'une nÃ©cessitÃ©, mais elle ne rÃ©sout pas tout. On ne craint pas uniquement la perte des informations quand on parle de problÃ¨mes de protection des donnÃ©es dans le Cloud mais Ã©galement du risque que des personnes qui ne devraient pas pouvoir lire ces donnÃ©es y accÃ¨dent.

Dans les faits, en choisissant un service de Cloud, vous ne savez pas rÃ©ellement oÃ¹ sont stockÃ©es vos donnÃ©es et surtout vous ne savez pas qui peut avoir accÃ¨s Ã celles-ci. De nombreux services de Cloud indiquent en effet dans leurs conditions gÃ©nÃ©rales qu'ils ont le droit d'accÃ©der Ã vos donnÃ©es Ã des fins de maintenance, bien sÃ»r, mais aussi pour leur usage propre, ce qui est beaucoup moins acceptable.

Comment se protÃ©ger ?

Deux solutions sâ□□offrent alors Ã vous. La premiÃ¨re : ne pas mettre toutes les donnÃ©es de lâ□□entreprise dans le Cloud. Cela implique de les classifier, câ□□est-Ã -dire de choisir celles quâ□□il faut protÃ©ger ou pas. Quels fichiers dans une entreprise ne sont pas assez confidentiels pour ne pas Ãªtre protÃ©gÃ©s ? Les brevets ? Les comptes fiscaux ? Et que penser des donnÃ©es personnelles des salariÃ©s ?

La seconde possibilitÃ© consiste Ã protÃ©ger les fichiers avant leur envoi sur le serveur dans le Cloud. Cela ne peut clairement s'envisager que si le tiers peut continuer Ã travailler, Ã effectuer les maintenances nÃ©cessaires sans avoir besoin d'enlever la protection mise par l'entreprise.

Lâ□□objectif est donc de pouvoir profiter des avantages du Cloud en conservant la gouvernance de ses propres donnÃ©es. Lâ□□entreprise doit Ãªtre la seule Ã pouvoir accÃ©der au contenu des fichiers stockÃ©s dans le nuage. Cela passe par un chiffrement mais pas nâ□□importe lequel et surtout pas nâ□□importe comment.

Tout dâ□□abord, il ne faut pas utiliser une solution de chiffrement non validÃ©e, ou qui potentiellement pourrait possÃ©der des Back-doors (voir article qui dit le FBI souhaite lâ□□installation dâ□□une Back-door lÃ©gale sur les principaux logiciels et sites web amÃ©ricains afin de pouvoir plus facilement accÃ©der aux donnÃ©es).

MÃ©fiez-vous aussi des solutions gratuites : comment vivent les sociÃ©tÃ©s qui mettent gratuitement ces logiciels Ã disposition ? Elles dÃ©veloppent des logiciels et les donnent sans contrepartie ? Et si elles avaient accÃ¨s Ã vos donnÃ©es et les revendaient ? Les exploitaient ?

Ensuite, il faut que cette solution de cryptage respecte l'Ã□tat de l'Art en matiÃ¨re de gestion des clÃ©s.

Si vous chiffrez vos donnÃ©es et que la clÃ© est stockÃ©e dans le Cloud, que le Â« Cloudeur Â» a accÃ¨s Ã vos clÃ©s de chiffrement, vous nâ□□Ãªtes plus protÃ©gÃ© contre ces Tiers qui ont potentiellement accÃ¨s Ã vos donnÃ©es. Le chiffrement doit se faire sur votre systÃ¨me avec la clÃ© conservÃ©e en interne. Les donnÃ©es ainsi chiffrÃ©es sont envoyÃ©es par le rÃ©seau sur les serveurs distants et elles doivent demeurer chiffrÃ©es dÃ¨s quâ□□elles sortent de votre pÃ©rimÃ¨tre.

Nous pourrions aussi Ã©voquer le problÃ¨me du Patriot Act qui permet au gouvernement amÃ©ricain et Ã ses instances dâ□□avoir accÃ¨s Ã nâ□□importe quelle donnÃ©e stockÃ©e sur un serveur hÃ©bergÃ© sur le sol amÃ©ricain. Si le Â« Cloudeur Â» en question possÃ¨de les clÃ©s de chiffrement, il sera dans lâ□□obligation de fournir les donnÃ©es en clair.

Si vous Ãªtes maÃ®tre de votre chiffrement et que vous envoyez dans le nuage des donnÃ©es chiffrÃ©es, le Â« Cloudeur Â» quel quâ□□il soit ne pourra fournir que les donnÃ©es quâ□□il a, sans que celles-ci soient nÃ©cessairement intelligibles, du moins pas sans un travail beaucoup plus complexe.

Pour profiter des avantages du Cloud, il faut prÃ©voir de mettre en place des solutions de sÃ©curitÃ©s adaptÃ©es et qui permettent de conserver la gouvernance des donnÃ©es et dâ□□Ãªtre certain quâ□□elles restent confidentielles. Cela passe par la mise en place d'un logiciel de chiffrement des donnÃ©es, renchÃ©rit **Xavier Dreux**, responsable marketing Prim.xTechnologies..