

La souveraineté des données : une priorité de l'agenda des DSI !

Internet

Posté par : JPilo

Publié le : 8/10/2013 11:00:00

Les révélations concernant la surveillance des données par les États, en particulier les États-Unis d'Amérique ont mis en haut de l'agenda des DSI la question de la souveraineté des données à côté de **connaître la localisation physique des données**.

Pour NTT Communications, **Len Padilla**, Directeur de la Stratégie Produit en Europe et **Sylvain Defix**, Senior Consultant chez NTT Com Security, nous donnent leurs opinions et offrent quelques observations.

Un nombre croissant de DSI et de services informatiques se tournent vers le Cloud pour les aider à acquies un avantage concurrentiel pour leur entreprise, réduire les coûts et faire plus avec moins. Près des trois quarts des DSI que nous avons interrogés en mai de cette année ont convenu qu'ils utilisaient déjà du cloud. Selon l'étude, un des principaux avantages est de fournir un véritable accès universel (de n'importe où, à partir de n'importe quel appareil) aux données de l'entreprises au travers des applications métiers. C'est en effet le plus grand avantage du Cloud par rapport à l'infrastructure informatique maison ; mais c'est aussi sa plus grande faiblesse, comme les évolutions récentes l'ont mis en évidence.

En effet, les révélations faites par Edward Snowden sur le programme de surveillance « PRISM » du gouvernement américain, ont incité de nombreuses entreprises à repenser leurs investissements dans le cloud. Parmi toutes ses allégations, Snowden affirme que les entreprises technologiques américaines étaient de connivence avec le gouvernement US pour fournir un accès sur demande aux données détenues dans leurs systèmes. De nombreux fournisseurs l'ont nié, mais le mal a été fait. Ainsi, tout d'un coup, la souveraineté des données à côté de le lieu physique où les données sont stockées et la nature des organisations qui les stocke devient cruciale pour les DSI. Avoir ses données dans des DataCenter d'un pays, où les autorités peuvent y accéder ou les contrôler, sans même un consentement, constitue un risque commercial important.

La possibilité de choisir l'endroit où les données se trouvent, et même de les transférer d'un pays à un autre, à volonté, est désormais une préoccupation majeure.

Les décideurs politiques en Europe ont prêté leur voix à cette préoccupation. Ainsi, le ministre allemand de l'Intérieur, **Hans -Peter Friedrich**, a dit : *«Quiconque craint que ses communications ne soient interceptées, doit alors utiliser des services de cloud qui ne passent pas par les serveurs américains. »*

Ou encore, Fleur Pellerin, Ministre d'Économie et de l'Économie numérique au sein du gouvernement français, qui prend acte : *«Nous prenons aujourd'hui conscience, peut-être un peu tard, de la nécessité d'être moins dépendants des infrastructures, des plates-formes ou des points d'accès à Internet autres qu'européens. La nécessité d'avoir un Cloud souverain se pose avec une grande acuité.»*

Ces propos ont atteint durement les fournisseurs de Cloud américains de 21 à 35 milliards de dollars de pertes prévues, selon la fondation ITIF (voir le **rapport** daté 2013). Bien sûr,

toute personne, qui externalise des données à un tiers, doit accepter de perdre le contrôle total sur ses données et dans le même temps de faire confiance à l'opérateur choisi. Mais la question ici est de savoir si la confiance accordée à votre fournisseur doit s'étendre au gouvernement dont il dépend.

Cependant, le seul choix de localisation des données et des applications dans le Cloud ou chez soi n'est pas la réponse au problème. En effet, les plateformes de Cloud aident les entreprises à devenir plus agiles et à stimuler l'innovation technologique, mêmes chez les entreprises les plus frileuses. Aussi, les DSI doivent trouver un chemin pour bénéficier des avantages du Cloud, tout en protégeant sans aucun compromis - leur entreprise et ses données.

Tout d'abord, scruter les réseaux internationaux et les DataCenter des fournisseurs de Cloud ainsi que les implantations de leurs sièges sociaux est la première étape, cruciale. Puis, seconde étape tout aussi importante est de vérifier s'il est possible pour un client de déplacer les données à sa demande pour accompagner l'implantation de nouvelles filiales dans un pays, par exemple. Or, ceci est très difficile techniquement, car l'ensemble du réseau, des serveurs et de l'infrastructure de stockage doivent être virtualisés et automatisés. Fournir des services de Cloud Computing aux entreprises dans le monde entier sans toucher à aucune infrastructure américaine s'avère encore plus compliqué. L'acheminement des données transitant par Internet est automatisé, il n'y a donc aucun moyen de prédire quel chemin vont prendre les données et de savoir si elles vont traverser les Etats-Unis ?

Alors, comment cela affecte le «CLOUD» ? Fini le temps, où vous pouviez visiter un DataCenter et vous faire pointer du doigt le serveur, où vos informations étaient stockées. Toutefois, la souplesse du Cloud permet aux données d'être placées où le fournisseur veut les mettre, par exemple, en se limitant à un pays (ou plusieurs) ou à un DataCenter (ou plusieurs) ou même à un ensemble de serveurs dans un DataCenter. Mais où les données sont stockées, les fournisseurs ne vous donneront sans doute pas les droits d'auditer vous-même la sécurité mise en place. Par conséquent, lorsque vous choisissez un fournisseur de Cloud, lorsque vous sélectionnez les applications à déplacer vers le Cloud, vous devez sérieusement envisager les questions suivantes:

☞ Votre fournisseur de Cloud est-il assujéti au Patriot Act ?

☞ Est-ce que votre fournisseur possède de bonnes références en matière de sécurité ?

☞ La solution de votre fournisseur permet-elle de s'inscrire dans votre stratégie d'entreprise de gestion de risque ?

☞ Pouvez-vous faire le choix de l'implantation géographique des données avec votre fournisseur ?

☞ Est-ce que votre fournisseur vous permet de l'auditer ?

☞ Est-ce que votre fournisseur vous garantit qu'à votre demande les données seront réellement et non pas logiquement détruites ?

☞ Est-ce que votre fournisseur de cloud a l'expérience de la gestion de données sensibles, telles que les données bancaires ?

L'appel du Cloud a été entendu par les DSI, qui ont été séduits par ses promesses de plus grande flexibilité et de meilleure maîtrise des coûts. Bien que le Cloud ne soit pas une garantie contre les activités d'espionnage et contre l'interception de communications, il

permet une flexibilité et un niveau de sécurité, nécessaires aux entreprises qui font face à une expansion internationale.

Len Padilla ajoute : « Quel dommage que ce soient des organisations de sécurité nationale d'un pays qui jettent le discrédit sur le Cloud, discrédit dont il faudra se débarrasser ! Nous espérons que l'affaire PRISM se résoudra vite juste un ralentissement temporaire du mouvement d'adoption massif du Cloud Computing par le marché. Pour l'instant, les DSI doivent mesurer leurs décisions d'aller vers le Cloud Computing, à l'aune de la souveraineté des données. »

Sylvain Defix précise que l'actualité récente montre qu'il faut bien peser d'un point de vue métier les risques d'introduction du modèle Cloud avec les risques de ne pas s'y engager, sur la base d'une gestion du risque éclairée.

Il ajoute : « Transparence dans la localisation des données et des équipes opérationnelles, clarification des pratiques de certification chez le fournisseur de Cloud sont des exigences essentielles, auxquelles j'ajouterai la lisibilité et la flexibilité des services de sécurité associés telle que l'offre de sécurité managée WideAngle MSS, pour laquelle nous avons développé un moteur SIEM de nouvelle génération. »