

Intervention de Jean-Philippe Trabichet à la journée du cloud computing de l'OPI, le 15 juin 2011

Bonjour, j'aimerais intituler ma courte présentation

Business in the cloud, quel impact sur la gouvernance de la sécurité ?

La sécurité des systèmes d'information (SI) fait clairement partie de la stratégie d'entreprise dès lors qu'elle contribue aux objectifs de création de valeur de l'entreprise. En termes de SI, les organisations doivent se doter de moyens qui leur permettent, dans une approche cohérente avec le dispositif global de sécurité, d'optimiser les processus et rationaliser des investissements. Le cloud computing offre, pour cet objectif, un cadre moderne et performant ayant toutefois un impact considérable sur le business. Il agit comme moteur de croissance mais modifie l'approche traditionnelle des risques dans toutes les dimensions (stratégique, managériale, organisationnelle, juridique et technique). Le département informatique de la HEG travaille à la fois sur l'impact business du cloud computing et sur la gouvernance de la sécurité des SI.

Première étape : le cloud computing une nouvelle méthode de gestion

Le cloud computing est à nouveau un de ces concepts qui prend forme spontanément en informatique profitant d'une conjonction d'évolutions technologiques et qui va modifier de façon notable les structures et même la culture de nos organisations. L'exemple le plus récent et le plus marquant de ce type est le WEB 2.0 qui qualifie, à un moment donné, une rupture dans l'utilisation de l'internet par les internautes. Dans ce cas, grâce à l'aboutissement de diverses technologies, les internautes ont tout à coup fondamentalement modifié leurs comportements sur le WEB.

Le cas du cloud computing ressemble un peu à cette situation. Nous sommes à une conjonction de l'état de la technologie réunissant, en particulier, la fiabilité et l'extension de l'infrastructure internet à laquelle on ajoute les derniers développements dans le cadre de la virtualisation des infrastructures et des plateformes informatiques et la disponibilité de ressources appartenant à de grands acteurs de l'internet comme Amazon ou Google. Ces éléments vont ensemble, sous l'appellation cloud computing, transformer nos organisations.

A l'instar du WEB 2.0, le cloud a donc un impact sur nos organisations, en tout cas d'un point de vue structurel. Les caractéristiques de ce nouveau concept d'architecture des SI vont se retrouver dans tous les processus métiers et la stratégie d'entreprise va devoir englober ce concept. A la HEG, nous avons posé comme hypothèse que les caractéristiques du cloud, à savoir, la répartition géographique, la synchronisation, la globalité, la virtualisation et l'élasticité, vont modifier et s'intégrer dans les méthodes de gestion.

Au niveau de la stratégie d'entreprise, il est maintenant possible d'optimiser et rationaliser les processus métiers en s'inspirant des caractéristiques du cloud computing. En effet, si on pose comme hypothèse que le système d'information est l'élément structurant de l'entreprise et que l'on admet que l'information est la ressource essentielle de cette stratégie alors nos méthodes de gestion d'entreprise vont réellement pouvoir s'inspirer du cloud et l'utiliser. C'est vraiment passionnant et nous travaillons beaucoup sur ces options avec mon équipe. Mais, et c'est le sujet du jour, la protection du patrimoine informationnel de l'entreprise est devenue un enjeu stratégique essentiel d'où la question qui revient toujours dans nos cas pratiques :

Le cloud computing est-il sûr ?

J'aime beaucoup cette question. C'est évidemment une question d'interprétation. Il faut s'entendre sur le sens de sécurité. C'est presque une question de philosophie. Il y a la sécurité type « Fort Nox » ou bien celle décrite par Edgar Alan Poe dans la « Lettre volée ». Le cloud computing n'est ni plus sûr, ni moins sûr que toute l'informatique.

Les ingénieurs mettent en place des systèmes de cryptage qui sont très sûrs, autant sur votre PC que sur le cloud. Mais on sait que la sécurité est une affaire d'organisation avant tout. **Qui a accès à quoi ? Qui est responsable de quoi ? Quelle politique de mot de passe avons-nous ? Quelle base de données est reliée à quelle autre ?** etc..

Alors, et sans écouter les ingénieurs système qui ne manqueront pas de vous dire ... « le cloud c'est mal ! », je répondrai : oui, il est parfaitement possible de sécuriser le cloud avec les mêmes techniques et la même organisation que le reste de l'informatique.

Mais le cloud computing, c'est aussi l'usage de data centres. Cette notion même de regroupement de données inquiète et la question suivante est toujours la même :

N'est-ce pas une aubaine pour les criminels de disposer d'autant de données au même endroit ?

On peut reprendre mon image de « Fort Nox ». Il y a beaucoup de données au même endroit, mais elles sont plus sécurisées que partout ailleurs. Aucune entreprise ne peut s'offrir un tel degré de sécurité. Un data center est effectivement concentré, mais on va avoir les moyens de le sécuriser. Les banques sont moins souvent cambriolées que les ménages.

Par contre, le cloud computing met en jeu **un paradoxe intéressant**, oui les données sont **centralisées** mais elles sont aussi **réparties**.

Le cloud computing permet de varier les stratégies de sécurité à l'instar du personnage de Poe qui avait trompé le détective en changeant les règles de la logique de cachette. Si vous partez en vacances en famille, préférez-vous répartir l'argent entre les membres ou tout cacher dans votre ceinture sécurisée.

Vos fichiers sur le cloud sont répartis, pris en charge par des professionnels alors que vos fichiers sur votre propre PC sont sous votre seule responsabilité.

En premier constat très simple, on peut rappeler qu'il y a deux vues de la sécurité par rapport à deux risques :

- **Perte de données**
Pour ce risque-ci, le cloud est beaucoup plus sûr que toutes vos politiques de sauvegarde maison.
- **Vol de données**
Pour ce risque-là, le cloud n'est pas différent des autres organisations informatiques.

J'aime à dire aux patrons d'entreprise qui se posent la question, qu'il y a de nombreux avantages à être sur le cloud. Les mêmes que ceux qui consistent à se libérer des tâches informatiques pour se

concentrer sur son propre métier. Il faut tenir compte, par contre, de certaines contraintes en partie légales dans certains mandats.

Il convient, en clair et en résumé, de décliner l'analyse des risques de l'appropriation du cloud en termes de

1. Sécurité physique
 - Cryptage
 - Anonymisation
 - Garantie selon ISO
2. Aspects légaux
 - CH-LPD
 - Ge-Lipad
 - International- USA Patriot act-(NSA) vie privée pas même concept aux USA.
3. Dépendance
 - Qualité du prestataire / accès qu'il donne à ses employés
4. SLA
 - Actuellement point faible largement décrié du cloud computing.

Selon Eugene Schultz, directeur technique d'Emagined Security, une entreprise de conseil installée à San Carlos, en Californie : « Mal ficeler les accords de niveau de service (SLA) ou partir du principe que le Cloud c'est mal et que tout contrôle sera perdu dès qu'il sera adopté, font partie des erreurs que les entreprises devraient essayer d'éviter lorsqu'elles se penchent sur la question de la sécurité des services de Cloud Computing. »

Justin Drain, responsable sécurité des données de la Fremont Bank, surenchérit en reconnaissant que le Cloud Computing représente un avenir certain : « tout le monde cherche à faire des économies. Et si je ne comprends pas les questions de sécurité que pose le Cloud Computing, je ne fais pas mon boulot. »

Ceci dit, il ne faut pas se faire d'illusion, que l'on le veuille ou non, que l'on sécurise drastiquement son SI, que l'on bannisse le cloud, celui-ci entre par la petite porte si on ne lui ouvre pas la grande. **Combien d'employés avez-vous qui se tournent vers Gmail lorsque la messagerie de votre entreprise est trop à l'étroit ? Combien d'employés avez-vous qui n'ont pas encore compris que Skydrive ou Dropbox permet d'échanger des documents avec des partenaires ? Ou bien, encore plus malicieux, combien d'employés utilisent des outils comme Google Cloud Connect ou EverNote ou encore Catch note ?**

En conclusion, le centre de compétence pour la sécurité de l'information des entreprises de la HEG a clairement exposé dans sa stratégie de gouvernance que le cloud computing modifie l'approche traditionnelle des risques dans toutes les dimensions :

stratégique,
managériale,
organisationnelle,
juridique et technique.

Seule une approche globale permet de piloter ces éléments.

Pour terminer, une petite réflexion à votre sagacité :

L'internet est une révolution, car le contenu n'est plus dans la bibliothèque, avec le cloud c'est carrément tout le poste de travail qui se retrouve sur l'internet ... une bonne question reste ouverte :
« est-ce bientôt l'utilisateur qui sera translaté sur l'internet ? »

Merci de votre attention.