

Trois questions, **trois visions**

JEAN-FRANÇOIS FERLAND

Des responsables des technologies au sein d'organisations, des dirigeants d'entreprises de l'industrie des TIC et des observateurs répondent à trois questions liées à la thématique de notre dossier.



Nicolas Roberge
Consultant

Ovologic
Québec



Georges Cowan
Associé directeur

Business Continu-IT Partners
Montréal



Simon Castonguay
Directeur, risque, performance,
technologie et conformité

KPMG Montréal

1. L'informatique en nuage convient-elle à toutes les applications d'une organisation ?

Nicolas Roberge : Elle convient à toutes les applications informationnelles et de gestion, où les données sont documentaires. Elle est également utile lorsqu'il y a des besoins liés à la mobilité ou au télétravail, car il est plus facile d'y établir des applications que sous le modèle traditionnel. Cela peut devenir plus compliqué pour les applications industrielles, où il y a de la robotisation ou de l'impression de masse qu'il est préférable d'exécuter en interne.

Il faut avoir accès à une connectivité Internet abordable et de qualité, sinon un transfert volumineux de données risque d'entraîner une implantation coûteuse ou fréquemment non disponible. Aussi, il vaut mieux éviter d'établir des ponts critiques entre des applications en nuage et des applications en interne.

Georges Cowan : Il faut identifier les applications trop sensibles pour être envoyées à l'extérieur de l'organisation. L'application de courriel est souvent la première et la plus populaire à être envoyée dans le nuage. Cela permet d'externaliser l'information, mais aussi d'emmagasiner des informations à vocation variable - certaines données doivent être conservées et d'autres doivent être éliminées - afin de respecter une réglementation. En deuxième lieu, on retrouve les applications qui ont trait à la force de vente et à la gestion de la relation client.

Les applications les moins intéressantes à envoyer en nuage se trouvent du côté des finances et de la recherche et du développement, mais si c'est bien sécurisé et que les gens sont à l'aise avec l'approche, cela ne cause pas de problème.

Simon Castonguay : La décision d'aller dans le nuage - et jusqu'à quel point on veut y aller - doit reposer sur les informations en main. J'imaginerais mal qu'on mette dans le nuage des données confidentielles qui ont trait à la paie des employés. À l'inverse, les versions du site web de l'entreprise représentent très peu de risque. Entre ces deux extrêmes, il y a divers types de données pour lesquelles la décision de recourir au nuage doit être prise après avoir réfléchi à la nature des informations et au besoin à combler : obtient-on des avantages à les mettre dans le nuage ? Est-ce que ces avantages surpassent les inconvénients ?

D'autre part, des aspects légaux entrent en ligne de compte. Y a-t-il des lois spécifiques qui s'appliquent aux informations que l'on veut mettre dans le nuage ? Les critères relatifs au traitement de l'information continueront-ils d'être respectés dans le nuage ?

2. Comment optimise-t-on la sécurité du côté des utilisateurs d'une application en nuage ?

Nicolas Roberge : Les applications de qualité en logiciel service offrent par défaut des connexions de type HTTPS ou SSL. Cela permet aux utilisateurs d'accéder aux applications de n'importe où, que ce soit de leur domicile ou via des services Wi-Fi publics qui sont souvent non sécurisés. Cette mesure forcée par les applications Web réduit les risques d'usurpation des mots de passe.

Pour les serveurs virtuels, on peut en sécuriser l'accès afin qu'ils soient intégrés à notre réseau sans être visibles de l'extérieur, à l'aide d'une configuration semblable aux réseaux privés virtuels. Il s'agit d'une façon d'augmenter la sécurité de traitements dématérialisés ou externalisés sur Internet.

Georges Cowan : Chez les petites entreprises qui utilisent davantage l'informatique en nuage, à l'étape de la planification il faut identifier les risques, voir à l'implantation de contrôles, procéder à une mesure pour s'assurer que les résultats sont probants, puis valider que tout est bien fait. Il faut s'assurer que les informations envoyées vers le fournisseur de service en nuage sont chiffrées. Pour la grande entreprise, un service récent permet de gérer la sécurité chez le fournisseur d'informatique en nuage tout en gardant en interne l'information liée à cette gestion. Pour une somme raisonnable, on peut établir des pare-feux jusqu'à l'impartiteur. Un principe qui doit prévaloir en sécurité est la possibilité de recouvrement des éléments versés dans un service en nuage. Dans la majorité des cas, le fournisseur de service en nuage permet de rapatrier les données dans un délai beaucoup plus court que chez l'impartiteur traditionnel.

Simon Castonguay : La sécurité ne sera jamais mieux dans le nuage qu'elle ne le sera à l'intérieur de l'entreprise. Si la gouvernance de la sécurité de l'information a des lacunes en interne, forcément les politiques, les procédures, l'utilisation et la gestion de l'information en auront. Si on fait affaire avec un fournisseur de service en nuage sans avoir pris conscience de ces lacunes, il y a de fortes chances que les services demandés ou que les critères élaborés pour définir si les services répondront aux besoins refléteront ces lacunes.

En fait, on peut avoir dans le nuage la transposition virtuelle des problèmes qu'on connaît dans l'entreprise - les problèmes y sont juste plus imposants, parce que ça touche plus de gens et moins d'infrastructure.

3. Que doit-on valider avant de recourir à un fournisseur situé hors du pays ?

Nicolas Roberge : Il faut surtout s'assurer que les lois applicables dans le pays où se trouve le fournisseur ressemblent à celles du Canada. Dans l'ensemble des pays industrialisés, les lois criminelles, de confidentialité et de protection de la vie privée sont similaires.

On entend souvent parler du *Patriot Act* aux États-Unis qui pourrait être un élément dissuasif en matière d'hébergement de données, mais des analyses démontrent que la loi canadienne est pratiquement identique. Le *Patriot Act*, qui permet au gouvernement américain de fouiller des serveurs, existe surtout pour les enquêtes liées au terrorisme. Une entreprise légitime et honnête ne devrait pas se soucier d'un tel risque, au même titre que le risque d'affaires que représenterait la police pour les opérations de la compagnie.

Georges Cowan : Il y a un besoin d'évaluation des risques lorsque l'information est envoyée à l'extérieur du pays. Au niveau de la conformité, il faut prendre en compte des éléments afin de respecter des règles comme Sarbanes-Oxley. Il faut aussi s'assurer qu'il y a bien une ségrégation de données : y a-t-il des barrières qui assurent que personne ne peut y toucher ?

En informatique en nuage, le contrôle ne s'externalise pas. Comme on donne des lignes directrices à son comptable, il faut établir des paramètres afin que l'information soit bien traitée. Toutefois, l'envoi des données hors du pays comporte une problématique : comme les grands fournisseurs de services en nuage veulent avoir une grande capacité de déplacement des données, ils peuvent exiger des montants plus élevés s'ils n'ont pas une facilité à transférer vos données à l'extérieur du pays afin d'accroître la capacité de leur nuage.

Simon Castonguay : L'environnement légal compte pour beaucoup, mais il ne faut pas partir à la chasse aux sorcières pour autant. Lorsque le *Patriot Act* est apparu, beaucoup d'entreprises ont craint de mettre leur informations aux États-Unis parce qu'elles seraient espionnées par l'État. [...] Si on n'a rien à se cacher, ce n'est pas parce qu'un État intercepte des documents qu'ils seront rendus publics ou mettront à mal les activités de l'entreprise.

Néanmoins, il faut penser aux impacts de l'application des lois. Une récente directive européenne peut entraîner des pénalités substantielles si un protocole n'est pas respecté lorsque de l'information transite ou est détenue par des personnes ou des serveurs hors de l'Union européenne. Dans la mesure où le nuage est international, la question de l'extraterritorialité de l'information devient cruciale. ■