

# points de vue sur la technologie

## À PROPOS DE CE DOCUMENT

Ce numéro de *Points de vue sur la technologie* de CGI traite de la question de la sécurité de l'information dans le contexte de l'informatique dans les nuages.

Il reprend en français l'essentiel d'un fichier balado enregistré en anglais sur ce sujet par Andy Pridham, CISSP\*, directeur du groupe Sécurité de l'information du bureau de CGI dans la région de la Capitale nationale.

Prenant du recul par rapport à l'engouement dont l'informatique dans les nuages fait présentement l'objet, M. Pridham décrit certains risques inhérents à cette formule et propose des stratégies de gestion de ces risques.

\* Certified Information Systems Security Professional

## Sécurité de l'information dans un contexte d'informatique dans les nuages

### Tout d'abord : qu'est-ce que l'informatique dans les nuages? Quels sont ses avantages et quels sont les enjeux en matière de sécurité qui y sont liés?

Dans son sens le plus simple, l'informatique dans les nuages est l'informatique faisant appel à des réseaux qui ne sont pas placés sous votre autorité et à des ressources dont vous ignorez la nature. Elle dépend du Web, dont elle est indissociable, ainsi que des technologies de virtualisation des ressources et des logiciels-services.

Il a été démontré que cette approche fondée sur le partage diminue les coûts en optimisant l'utilisation de l'espace physique, de la bande passante et des droits d'utilisation des logiciels. Elle exige toutefois de la souplesse en ce qui a trait à l'emplacement physique des données, choisi pour maximiser l'emploi des ressources communes. Nous savons depuis longtemps qu'il est avantageux de stocker les données et les applications sur des serveurs plutôt que sur chacun des micro-ordinateurs. L'informatique dans les nuages prolonge cette formule hors de l'organisation.

Clairement bénéfique sur le plan des coûts, l'informatique dans les nuages a acquis une popularité immédiate. Néanmoins, les inquiétudes en matière de sécurité ont freiné sa propagation. Il est possible que l'adoption intégrale de l'informatique dans les nuages ne soit pas opportune dans certains cas, pour des raisons de sécurité. Des méthodes susceptibles de diminuer les risques à un niveau acceptable ont toutefois été mises au point.

### Quels sont les pièges et les mesures de protection dont nos clients devraient tenir compte lorsqu'ils adoptent l'informatique dans les nuages?

L'absence d'autorité et d'information sur les ressources, inhérente à l'informatique dans les nuages, est contraire aux exigences de la sécurité. Voilà donc où le bât blesse : plus vous exigerez d'emprise et de connaissance, moins vous profiterez des avantages de cette formule. C'est donc une question de gestion des risques : il faut trouver le point d'équilibre entre les gains et les dommages potentiels.

Cinq dimensions devraient retenir votre attention. En les gérant bien, il est possible de réduire considérablement les risques liés à l'informatique dans les nuages.

Avant d'en parler, cependant, je tiens à souligner que la plupart des enjeux dont je traiterai ne sont pas propres à l'informatique dans les nuages : ils sont présents dans les autres contextes d'impartition et, de manière générale, dans tous les cas où une organisation confie ses actifs à un fournisseur externe. Ce qui distingue l'informatique dans les nuages, c'est l'absence presque complète de mécanismes de contrôle des lieux et des méthodes de stockage, de traitement et de transmission des données.

Il est entre autres indispensable d'obtenir des réponses satisfaisantes aux questions suivantes : Mes données seront-elles protégées comme il se doit? L'entente respectera-t-elle mes obligations juridiques?

### *Pensez tout d'abord à la conformité.*

Les certifications en disent long sur les organisations. Par exemple, une société peut détenir les certifications ISO 27002 et SAS70 pour ses méthodes et CISSP pour ses employés, et utiliser des critères normalisés de sélection des produits de sécurité. Votre fournisseur de services informatiques dans les nuages devrait respecter des normes internationales contrôlées périodiquement par des vérificateurs externes certifiés.

Par ailleurs – même si ce point ne touche pas uniquement la sécurité – il importe de déterminer la maturité de l'entreprise en examinant ses processus et en évaluant leur viabilité. Depuis combien de temps le fournisseur exerce-t-il ses activités? Qui sont ses clients? Combien de contrats a-t-il remporté? Les sociétés inscrites en bourse sont tenues de divulguer ces renseignements et d'attester leur véracité.

Enfin, votre entreprise est peut-être soumise à des exigences réglementaires touchant la sécurité. S'il n'est pas possible de les respecter dans un contexte d'informatique dans les nuages, il faudra renoncer à cette formule à moins de trouver une solution de rechange approuvée. Rappelez-vous que ces exigences s'appliquent à tout sous-traitant de votre fournisseur.

Plusieurs des sujets dont je parlerai sont traités dans le cadre des programmes de conformité. Il est néanmoins prudent de les approfondir davantage afin de respecter l'esprit et non seulement la lettre des lois.

### *Renseignez-vous ensuite sur le lieu de conservation des données.*

Savez-vous dans quels pays vos données seront – et ne seront pas – stockées et traitées? À certains endroits, les lois ou les pratiques des gouvernements ne garantissent pas la confidentialité que les clients exigent. Demandez : Comment assurera-t-on la séparation des données? Les données seront-elles conservées sur le même serveur que celles d'un concurrent ou d'un pays hostile? D'ailleurs, la loi et les règlements permettent-ils que les données soient stockées ou traitées dans tel ou tel pays?

Ceci donne un aperçu des dilemmes découlant des questions de sécurité. Pour contourner les obstacles, vous pourriez opter pour un « nuage privé » où certaines ou toutes vos données seraient stockées et traitées selon vos exigences. Il faudrait toutefois vous faire à l'idée qu'une telle solution de compromis diminuerait les avantages de la virtualisation des serveurs.

### *Troisièmement, examinez le contrôle de l'accès.*

Si vos données sensibles tombent entre de mauvaises mains, les conséquences pourraient être désastreuses. L'accès aux données doit donc être réservé aux personnes autorisées. Déterminez si les données seront chiffrées et les méthodes de gestion des clés de chiffrement. Examinez les autres mécanismes de contrôle de l'accès. Quand le contrat sera terminé, comment aurez-vous l'assurance que toutes les données et tous les artefacts auront été enlevés?

Vous devez admettre que certains administrateurs de systèmes auront des raisons légitimes d'accéder à vos données et que ces contacts intimes avec vos renseignements ouvrent la porte à des actes malveillants. Après avoir vérifié la compétence du fournisseur, vous devrez donc vous assurer qu'il est digne de confiance. Quelle est sa politique de vérification des antécédents des administrateurs de systèmes? Quels mécanismes utilise-t-il pour les surveiller? Quelles sont ses pratiques de vérification et de reddition de comptes?

## **CINQ DIMENSIONS À SURVEILLER POUR ASSURER LA SÉCURITÉ**

En gérant bien les cinq dimensions suivantes, il est possible de réduire considérablement les risques liés à l'informatique dans les nuages :

1. Vérifiez les certifications du fournisseur, ainsi que ses normes de conformité à la réglementation.
2. Examinez les enjeux liés à l'endroit où vos données seront conservées – pays, réglementation, concurrence.
3. Renseignez-vous sur les pratiques de contrôle de l'accès et de vérification.
4. Évaluez les processus et les systèmes de sauvegarde et de restauration du fournisseur.
5. Déterminez si le système de signalement et de résolution des incidents est satisfaisant.

*Évaluez ensuite les processus et les systèmes de sauvegarde et de restauration du fournisseur.*

La disponibilité des données est un facteur critique exigeant un examen approfondi. Elle figure d'ailleurs parmi les quelques critères objectifs qui font partie des ententes sur les niveaux de service et détermine dans une large mesure les prix négociés. Voici certaines questions que vous devriez poser à votre fournisseur de services informatiques dans les nuages :

- Quelle est la robustesse de son système?
- Comment l'architecture assure-t-elle la redondance?
- Où sont ses centres de secours et comment répondent-ils aux exigences mentionnées ci-dessus, en matière de conformité par exemple?
- Comment gère-t-il les pannes?
- Quelles sont ses pratiques en matière de sauvegarde et de restauration? Quelle est sa feuille de route?
- Comment est-il structuré pour détecter et riposter aux attaques?

*Ce qui nous amène au dernier sujet : le signalement et la résolution des incidents*

Le nombre d'entreprises sérieuses qui n'ont pas de système de signalement des incidents est étonnant. Et dans bien des cas, celles qui ont élaboré un plan ne l'ont pas communiqué efficacement à leurs équipes. Ainsi, quand un malheur arrive, les gestionnaires improvisent une réponse – comme si c'était le premier incident du genre. Une telle situation peut occasionner des pertes importantes et des périodes prolongées de non disponibilité.

Quel est le système de signalement et de résolution des incidents du fournisseur? Quelles sont ses méthodes d'investigation des incidents? Quelles sont les circonstances qui occasionneraient l'intervention d'organismes externes comme la police locale, par exemple? Quelle est la politique d'information du client en cas d'attaque réelle ou possible?

### **En terminant, quels sont les points à retenir, selon vous, sur la sécurité dans le contexte de l'informatique dans les nuages?**

Il y a toujours des risques, quels que soient les montants investis, les précautions prises ou les personnes à qui vous confiez vos actifs. Vous devez comprendre la valeur de vos données, ainsi que les exigences juridiques auxquelles vous êtes soumis, et prendre les mesures qui s'imposent. Quand vous choisissez un fournisseur de services informatiques dans les nuages – ou un impartiteur –, ne tenez rien pour acquis. Soyez méthodique lors de la sélection et exercez une surveillance rigoureuse par la suite.

Le dilemme, c'est que les plus grands avantages et les plus grandes menaces de l'informatique dans les nuages sont indissociables. En étant très vigilant lors de l'évaluation du fournisseur et en imposant des restrictions bien dosées, il peut être possible de profiter des avantages de l'informatique dans les nuages tout en assurant convenablement la protection des données.

### **PROFIL DE L'ENTREPRISE**

La satisfaction des clients est au premier plan des activités de CGI. Depuis 30 ans, nous sommes solidaires de nos clients et les aidons à faire face aux défis qu'ils rencontrent en leur offrant des services de qualité. Figurant parmi les chefs de file du secteur des services en TI et en gestion des processus d'affaires, CGI bénéficie d'un avantage concurrentiel grâce à ses 25 500 professionnels œuvrant à partir de plus de 100 bureaux dans le monde.

Par leur entremise, nous fournissons à nos clients la combinaison de valeur et de savoir-faire qui répond le mieux à leurs besoins en alliant judicieusement les partenariats à l'échelle locale et des options de prestation de services à l'échelle mondiale – à l'intérieur du pays, sur le continent et outre-mer.

CGI estime qu'elle a réussi quand elle a aidé ses clients à obtenir des résultats supérieurs et a surpassé leurs attentes.