Les 10 recommandations du Cesin pour maîtriser le Cloud

L'externalisation massive de données dans le Cloud n'est pas sans risques pour les entreprises. Elles peinent encore à trouver le bon équilibre. Selon un sondage OpinionWay pour le Cesin, 85 % des entreprises stockent des données dans le Cloud. Et, selon une autre enquête publiée par Intel Security, une minorité de RSSI et décideurs IT en France pense que leurs dirigeants mesurent complètement les risques de sécurité qui pèsent sur les services Cloud. Le Shadow IT (les services informatiques déployés sans contrôle de la DSI et utilisés par les métiers) renforce les inquiétudes.

Sécurité et souveraineté

Pour Alain Bouillé, RSSI de la Caisse des Dépôts et président du Cesin (Club des experts de la sécurité de l'information et du numérique), *« l'arbitrage des opportunités versus risques doit être pris au niveau le plus haut de l'entreprise »*. Si les grands groupes ont les moyens d'assurer l'encadrement contractuel et juridique des prestations de Cloud, les organisations de taille moyenne n'ont pas la même marge de manoeuvre. *« En même temps, le Cloud peut offrir un niveau de sécurité parfois bien supérieur à ce que ces entreprises sont à même de s'offrir en interne »*, tempère le dirigeant interrogé par la rédaction.

Mais la localisation de données proposée par de grands acteurs du Cloud basés aux États-Unis ne suffit pas à assurer l'équilibre entre opportunités et risques. Outre les fuites et vols potentiels de données par un tiers ou un initié, la menace d'un accès *« secret »* ou mandaté par un État tiers existe. En témoigne, le différend opposant Microsoft à l'Etat fédéral américain sur l'accès aux données de messagerie d'un client de la firme de Redmond stockées en Irlande. On l'aura compris, la localisation de données *« n'est bien évidemment pas suffisante car le Patriot Act s'applique [aux entreprises américaines et à leurs filiales] indépendamment des frontières »*, ajoute Alain Bouillé. *« Mais cela permet tout de même de répondre à certaines contraintes réglementaires »*. Des contraintes renforcées par la directive européenne sur la protection des données personnelles.

10 recommandations du Cesin

Pour mieux gérer le risque et bénéficier des opportunités du Cloud, le Cesin propose donc 10 recommandations aux entreprises. Ces recommandations sont le fruit d'une consultation réalisée par le Cesin auprès de ses membres, de juristes et de représentants de la Cnil et de l'Anssi.

1- Estimez la valeur des données que vous comptez externaliser ainsi que leur attractivité en termes de cybercriminalité.

2- S'il s'agit de données sensibles voire stratégiques pour l'entreprise, faites valider par la DG le principe de leur externalisation.

3- Evaluez le niveau de protection de ces données en place avant externalisation.

4- Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offre en fonction du résultat du point 1.

5- Effectuez une analyse de risque du projet en considérant les risques inhérents au cloud comme la localisation des données, les sujets de conformité et de maintien de la conformité, la ségrégation ou l'isolement des environnements et des données par rapport aux autres clients, la perte des données liée aux incidents fournisseur, l'usurpation d'identité démultipliée du fait d'une accessibilité des informations via le web, la malveillance ou erreur dans l'utilisation, etc. Sans oublier les risques plus directement liés à la production informatique : la réversibilité de la solution et la dépendance technologique au fournisseur, la perte de maîtrise du système d'information et enfin l'accessibilité et la disponibilité du service directement lié au lien Internet avec l'entreprise.

6- Outre ces sujets, exigez un droit d'audit ou de test d'intrusion de la solution proposée.

7- A la réception des offres analysez les écarts entre les réponses et vos exigences.

8- Négociez, négociez.

9- Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français.

10- Faites un audit ou un test d'intrusion avant démarrage du service (si cela est possible) et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps.

Lire aussi :

Sécurité du Cloud : le flou demeure entre l'IT et les métiers

Alain Bouillé, Cesin : « sans sécurité, la transformation numérique est un non-sens »