Cloud : les points clés avant d'opter pour une solution
Accessoire
Posté par : JulieM
Publiée le : 9/7/2013 13:30:00

Le Cloud est dans l'air du temps et offre de nombreux avantages. Beaucoup d'entreprises optent pour des services de Cloud ou Infrastructures as a Service (mise en uvre de services dédiés à la demande) pour gagner de l'espace mais aussi en efficacité et en performance. Pourtant, avant de sauter le pas, **il est nécessaire de vérifier certains points clés, confirme Thomas Beerens, Directeur des Opérations de CloudSystem .**

1. Choisir une entreprise française avec des DataCenter en France : dès lors qu'une entreprise collabore avec une société basée aux Etats-Unis, elle est soumise au Patriot Act et aux lois américaines. Il est à présent reconnu publiquement que les services de renseignement américain ont tout pouvoir d'accéder aux données gérées par les infrastructures du Cloud des sociétés américaines. Cette surveillance, si elle est affichée, est faite dans le but de lutter contre le terrorisme peut s'avérer être utilisée à des fins stratégiques concurrentielles comme cela a déjà été démontré par le passé.

Quoi qu'il en soit, la souveraineté de l'Europe et de la France impose que les entreprises soient vigilantes autant au niveau économique qu'au niveau indépendance des libertés individuelles. La France sur ces sujets, notamment grâce à la CNIL qui veille au grain, est particulièrement rigoureuse sur ces sujets. Des infrastructures appartenant à une société française, hébergée en France, et utilisant des opérateurs français c'est la meilleure garantie du respect de cette déontologie de la confidentialité, culturelle.

2. S'assurer que les données déposées dans le Cloud restent confidentielles dans le contrat. Les données appartiennent aux clients et l'opérateur n'a aucun droit de regard sur celles-ci. Ces termes doivent être clairement spécifiés dans le contrat passé entre l'entreprise et le fournisseur de solutions de Cloud. Il faut également examiner attentivement les contrats proposés par le prestataire. Ils doivent respecter les principes français en matière de protection et de confidentialité des données personnelles (Loi du 6 janvier 1978 modifiée) et être conformes aux

recommandations de la CNIL :

a. Audit : La possibilité au client de demander un audit pour vérifier le respect par le prestataire des obligations contractuelles,

b. Réversibilité : Restitution des données dans un format lisible et destruction de celles-ci par la suite.

3. Choisir un Cloud à visage humain : Il est important d'avoir confiance dans l'opérateur de service Cloud. La confiance regroupe : la compétence, la fiabilité, le respect des engagements et la disponibilité de l'opérateur en cas de difficulté. Tisser un lien avec l'entreprise qui propose des services de Cloud est un gage de transparence. De plus, on trouve plus rapidement des réponses à ses interrogations lorsqu'une société est à taille humaine. Les interlocuteurs de proximité sont plus réactifs que ceux placés à différents niveaux et qui plus est, à l'étranger.

4. La sécurité ne doit pas être des options du contrat. La sécurité est un sujet complexe et doit garantir la confidentialité, l'intégrité et la disponibilité des données. C'est un métier auquel les services informatiques peuvent être en général mal préparés, sauf si elles disposent assez de moyens pour embaucher des experts en interne (la redondance de l'expert fait partie de la sécurité...).

Confier son infrastructure, c'est aussi confier une bonne partie de sa sécurité à des experts. L'opérateur de services Cloud doit donc avoir une forte compétence en sécurité, et être équipé des meilleures solutions de sécurité du marché pour garantir l'étanchéité des Cloud privés virtuels, réseaux privés virtuels, prévention d'intrusion, détection de trafic IP anormal sortant, détection d'activité de malware...

Tous les hébergeurs proposant des services de Cloud ne sont pas suffisamment avertis de ces problématiques. Afin de protéger les données de l'entreprise dans le Cloud, la sécurité doit être intégrée dans l'offre de base pour garantir la confidentialité des données. **Les échanges entre le DataCenter et les postes clients doivent pouvoir être chiffrés aux travers de tunnels sécurisés**. De la même manière, les environnements virtuels doivent être privés et protégés par des systèmes de firewalls pour garantir l'étanchéité entre les clients. Selon les accords définis, seul le client et son prestataire doivent pouvoir accéder aux données dans le Cloud.

Il ne faut pas confondre la disponibilité seule ne garantit pas la sécurité des données. Un Cloud peut être disponible à 99,9 % sans pour autant être protégé. Toutefois, certains Cloud permettent de gérer soi-même les paramètres de sécurité. Dans ce cas, seul le client accède à ses données et maîtrisent lui-même les paramètres de sécurité. Il devient alors responsable de la sécurité de son Cloud.

5. Demander à visiter les DataCenter : visiter le (s) lieu (x) où est (sont) hébergé (s) les données, c'est s'assurer que les données sont bien présentes en France et rencontrer le prestataire, c'est aussi s'assurer que celui-ci maîtrise bien le Cloud qu'il propose. L'entreprise est alors rassurée sur sa capacité à récupérer ses données, sur le support de son choix sans dépendance du lien Internet (sous réserve du respect du principe de réversibilité).