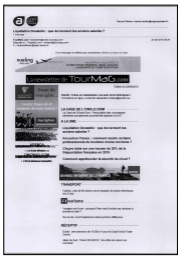

Comment appréhender la sécurité du cloud ?

un système en pleine démocratisation

La mode est d'avoir la tête dans le nuage. Pour les entreprises le Cloud apporte une flexibilité et une réduction des coûts de fonctionnement. En externalisant ses données les structures se libèrent de nombreuses contraintes opérationnelles mais ne doivent pas pour autant être moins vigilante. La sécurité du Cloud est un enjeu majeur pour rassurer les dirigeants encore réticents à l'idée de se séparer d'informations sur leur activité ou leur clientèle. Comment doivent-ils appréhender ce système en pleine démocratisation ? La protection des données est un sujet central et d'actualité, d'où l'importance d'être sensibilisé.

© Natalia Merzlyakova - Fotolia.com

Selon les prévisions de Salesforce, précurseur du système, d'ici 2020, le marché du Cloud computing devrait dépasser les 241 milliards de dollars.

Inévitable ? Probablement. Aujourd'hui ce qui porte préjudice au nuage, c'est la sécurité.

Sept entreprises sur 10 y sont encore réfractaires. Ce déficit de confiance est légitime au vue de l'actualité. Les récentes révélations faites sur la NSA et la CIA n'ont fait que renforcer les craintes.

Aujourd'hui les entreprises utilisent le Cloud pour gérer leur relation clients (CRM/GRC), leurs ressources humaines (RH), leur comptabilité et même des applications métiers. Des données parfois très sensibles, voire vitales pour les structures.

Définir le cloud pour mieux le protéger

Le Cloud, c'est un centre de données partagé, situé à l'extérieur de l'entreprise et lui permettant de réaliser toutes sortes de tâches sans avoir les contraintes souvent liées à leur utilisation.

Par exemple pour le grand public, Gmail archive vos mails dans un centre de données, ils ne sont pas sur votre ordinateur.

Grâce à un identifiant et un mot de passe vous pouvez les consulter où que vous soyez, simplement avec une connexion internet.

Le Cloud peut être privé, c'est-à-dire spécialement créé pour une seule société, ou public, standardisé pour que

des centaines de milliers de sociétés puissent l'utiliser simultanément. Il existe également des services de cloud hybrides que nous évoquerons plus bas.

Les bénéfices des solutions Cloud

Le dirigeant d'entreprise veut travailler en sécurité et de partout dans le monde. L'avantage économique est aussi indéniable, il peut passer d'un modèle d'investissement à un modèle de charge.

Le Cloud permet une consommation à la demande, tout comme les télécoms. C'est ce qui intéresse les PME: je sécurise mon exploitation, je partage l'information de façon dynamique et je réserve ma capacité d'investissement pour mon cœur de métier.

Selon une étude Aberdeen Group publiée par Salesforce, les PME bénéficient du meilleur temps de récupération de données en cas de soucis. Les pertes ou les problèmes matériels ne sont plus fatals et le nuage leur permet un accès à des nouvelles technologiques jusque-là inabordables.

« Aucun investissement, quel que soit son montant, ne peut protéger complètement les organisations de cyberattaques très sophistiquées », explique Art Gilliland, vice-président senior et directeur général de la division HP Enterprise Security Products

Mais alors pourquoi les dirigeants peinent à adopter le "nuage" ?

Selon une étude Ponemon Institute pour Netscape, 84% des patrons de TPE/PME doutent d'être notifiés immédiatement par leur fournisseur d'accès au Cloud en cas de fuite de propriétés intellectuelles ou d'infos confidentielles.

Et 64% pensent que le Cloud réduit la capacité d'une entreprise à protéger ses données.

Luc d'Urso, PDG de Wooxo comprend cette réticence : *« A partir du moment où l'on va externaliser une partie de ses données, de ces infrastructures et de ses applications, il faut intégrer que l'on a délégué une partie de sa sécurité.*

Avec les offres 100% Cloud public ou privé on doit se poser des questions, sur la territorialité par exemple, en France aux états unis ou en Finlande c'est tout à fait différent. La juridiction qui va s'appliquer est celle de la localisation des données. Si l'entreprise à un problème aux USA, cela implique le patriot Act.

La NSA et le FBI ont toutes les autorisations légales pour consulter des données. En cas de litige il ne faut pas oublier non plus que le procès aura lieu à l'étranger et pour les petites structures cela peut être très impactant ».

Mais a contrario, **penser que conserver toutes ses données au même endroit, et en interne, est une solution fiable, est une grossière erreur.**

Les entreprises mettent en danger leur données en accordant beaucoup de ressources sur la menace externe, pour contrer les cybercriminels, et pas suffisamment de moyens pour faire face au risque lié au facteur humain et à la menace interne.

Selon une étude Cisco publiée le 20 octobre 2014, 77% des salariés français pensent que leur comportement n'a pas d'incidence sur la sécurité des données de leur entreprise.

Les fournisseurs d'accès au Cloud ont des responsabilités, leurs clients aussi

Bien informer les entreprises est crucial pour rétablir la confiance. La transparence cassera cette réticence à adopter le Cloud.

Pour Luc Delpha, directeur de l'offre gestion des risques et Sécurité des Systèmes d'information chez Provadys, *« il est crucial d'informer les clients sur la nature des services qui leurs sont proposés. Il est donc de la responsabilité des entreprises d'informer leurs clients et de privilégier la transparence.*

Il est important de noter que même si l'entreprise a recours à des fournisseurs de type Cloud et externalise le traitement des données de ses clients, il reste responsable de leur protection.

En effet, l'un des enjeux fondamentaux est le respect des obligations légales et contractuelles (CNIL, PCIDSS, ...) applicables et il n'est pas possible de s'en affranchir complètement en ayant recours au Cloud ».

Mais attention, il ne faut pas oublier que l'entreprise qui paye un service Cloud a aussi une responsabilité envers ses clients. Le vol de certaines données collectées peut porter de gros préjudices, comme les données bancaires par exemple.

Elle a des contraintes légales d'informer ses clients et il est dorénavant possible d'assurer ses données partagées, Luc Delpha ajoute . *« Plus qu'un cadre juridique, sur lequel je ne saurais me prononcer, je recommande aux entreprises d'avoir recours à une assurance spécialisée pour couvrir ce type de défaut de fournisseurs essentiels »*.

Des solutions d'encadrement commencent à voir le jour

L'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) a mis au point un référentiel permettant d'auditer et de certifier la sécurité pour l'état et les entreprises.

Il a le mérite d'avoir formalisé les questions à se poser. Mais comme la plupart des PME et des TPE ont peu de ressources pour se plonger sur ce type de projet, Luc d'Urso reste dubitatif sur la capacité de ce document à trouver un écho pour les petites et moyennes structures : *« Il le trouvera certainement pour les plus grosses Cela demande une organisation que les TPE n'ont pas »*.

Cette solution n'en est qu'à ses balbutiements, le temps nous dira si elle est efficace.

Rédigé par Nicolas Pasquier le Jeudi 23 Avril 2015

Tags : cloud, nouvelles technologies, sécurité informatique