Laurent Heslault (Symantec) : « prendre conscience des vrais problèmes du cloud »

Dans son étude mondiale « *Avoiding the Hidden Costs of Cloud – 2013* », Symantec a révélé ce qu'il qualifie de « *vrais problèmes du cloud computing* » (lire notre article « La réalité du cloud : coûts cachés et données en danger »).

Une étude aux résultats inquiétants, que **Laurent Heslault**, directeur stratégie sécurité chez Symantec France et membre de la Cloud Security Alliance (CSA), a commenté pour nous.

Silicon.fr : Par certains aspects, les résultats de l'étude sont plutôt effrayants…

Laurent Heslault : L'arrivée du cloud est un changement, et comme tout changement il supprime des risques, mais il en crée de nouveaux. Nous suivons le même schéma que lors de l'explosion sauvage de la virtualisation. Les entreprises montrent des intérêts évidents pour le cloud, en particulier financiers. L'étude met les problèmes en lumière.

Silicon.fr : On se demande où est la DSI ?

Le cloud est plus moderne, moins cher, plus rapide. Et il court-circuite la DSI. D'ailleurs, les vendeurs de cloud ne s'adressent pas à la DSI !

En moyenne, nos clients ont une demi-douzaine de services cloud dont la DSI n'a pas conscience. En fait, dans les usages, le cloud ne fait pas beaucoup mieux que l'hébergement interne. Et les fournisseurs ont tendance à surbooker.

Silicon.fr : Le problème ne vient-il pas justement des fournisseurs ?

Le problème, c'est que les clients ne font pas d'analyse et de gestion du risque. La qualité du fournisseur de services va faire la différence. Encore faut-il tester le PRA. Mais le client prend trop souvent le risque du moins-disant.

Nous retrouvons cela dans la différence entre les données applicatives en mode SaaS (*Software as a Service*) et IaaS (*Infrastructure as a Service*). L'IaaS permet par exemple d'exploiter sa propre solution de backup.

En fait, la capacité du fournisseur de services dépend du type de cloud.

Silicon.fr : Votre étude met également l'accent sur les problématiques de conformité. Ne serait-ce pas une question de coût ?

De conformité et de gouvernance du cloud… Tant qu'il n'y a pas de volumes considérables, les coûts restent raisonnables. Nous constatons également un manque de proactivité sur la sécurité et la gestion des données.

Qu'il s'agisse des grandes entreprises ou des PME, nous pensons que nous allons tous finir en cloud hybride. Et c'est aux providers de fournir les solutions de sécurité. Mais beaucoup n'ont pas

de certification ! Certes 27001 a démontré son sérieux. En revanche, il n'y a pas un client SSL qui n'a pas perdu des données !

Les données et les accès sont aujourd'hui hors de l'entreprise, c'est pourquoi il faut valider la personne et le documentaire. Cela entraine le besoin d'un tiers de confiance et d'un certificat. Et c'est vrai qu'un SSL mal fait peut être vite très cher.

Il faut donc se poser les bonnes questions, en particulier celles de la PKI en mode SaaS.

Silicon.fr : N'est-il pas inquiétant de constater que peu d'entreprises se préoccupent de valider la sécurité offerte par leurs fournisseurs de cloud ?

Symantec a publié une étude il y a un an dont le paradoxe était que le cloud ne préoccupait pas les entreprises sur la sécurité des données, car elles estiment que le niveau de SLA du fournisseur est supérieur à celui qu'elles peuvent obtenir en interne.

La difficulté aujourd'hui c'est qu'il ne faut plus parler du cloud mais des clouds, avec autant de factures, de logins, d'interfaces. Il manque en particulier un cloud broker, pour fournir des services d'intégration des offres de clouds à destination des PME.

C'est là que peut prendre place la solution d'authentification de Symantec, qui permet un seul login, avec une vision de l'administrateur sur qui accède à quoi. Il faut redonner un niveau de contrôle au DSI, qui pourrait bien devenir un Cloud Interface Officer (CIO).

Silicon.fr : Quels conseils donneriez-vous aux entreprises qui veulent tenter l'expérience du cloud ?

D'abord, le cloud hybride est inéluctable, ainsi que la notion de cloud broker.

Le cloud est l'occasion de se poser ou reposer les bonnes questions sur la gestion de son système d'information et de ses informations. Se poser les questions que l'on ne s'est jamais posées. C'est une opportunité de repartir dans la gestion du risque, de la démystifier, de se poser la question « et si ? ».

Tout le monde sera attaqué et perdra des données, le risque zéro n'existe pas. Il faut mettre en place des passerelles, un système qui soit le plus 'cyber résilience'. La norme ISO 27001 offre des pages de bon sens, de même que les documents de la CSA (*Cloud Security Alliance*) ou de l'ENISA (*European Network and Information Security Agency*).

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes