Cloud et sécurité : le point sur 7 questions qui fâchent

	Cloud et sécurité : le point sur 7 questions qui fâchent

Le nuage informatique est à la mode chez les grands comptes, mais aussi chez les PME et TPE qui n'hésitent plus, parfois, à y déverser des données sensibles. La prudence reste pourtant de mise.

En France, le marché du "cloud" n'est pas encore mature », confie Henry-Michel Rozenblum, délégué général d'EuroCloud France, l'association des fournisseurs français de « cloud » liée à la fédération européenne Eurocloud. Ce qui signifie qu'il n'y a pas de standard de sécurité spécifique. L'approche consiste plutôt à s'appuyer sur les bonnes pratiques traditionnelles de la sécurité informatique. Notamment la certification ISO 27001, qui, si elle est délivrée par un grand cabinet d'audit, est la seule garantie qui fait foi. Autrement, pas de véritable sécurité. *« Même si le discours marketing prétend le contraire »,* souligne Gérôme Billois, expert sécurité au Cercle européen de la sécurité et des systèmes d'information.

Les pirates s'adaptent

Il existe sur Internet, des « black markets » électroniques (places de marché pirates), où des logiciels clefs en main s'échangent sans contrôle. Ils permettent de mener des attaques complexes contre un « cloud », sans même avoir besoin de solides compétences en informatique. Leur nom : des « hyperkits ». *« En quelques clics, ils permettent de prendre le contrôle d'un serveur physique à partir du serveur virtuel »,* prévient Jean-Paul Smets, PDG de Vifib, un offreur de « cloud » distribué. *« L'unique manière de s'en protéger est de maintenir son système à jour et de combler systématiquement les failles de sécurité. »*

Un risque systémique

En dehors des attaques, rappelons que le **cloud est, lui-aussi, sensible aux bugs, pannes et erreurs humaines…** *« Comme une poignée d'opérateurs de "cloud" domine le marché, le moindre problème prend une ampleur démesurée »,* explique Gabriel Chadeau, directeur commercial chez Vision Solutions, spécialiste de la récupération de données. Normal : lorsque le nuage « plante », des milliers d'entreprises n'accèdent plus à leurs services. Pour se protéger, il faut se demander quels services externaliser dans le « cloud » et quels autres garder chez soi. *« Je déconseille de mettre ses applications métiers dans le cloud. Pour des raisons de disponibilité et de confidentialité »,* souligne Gérôme Billois.

Une confidentialité illusoire

Pour de nombreux acteurs, la **confidentialité est le point noir du cloud computing**. Les fournisseurs américains sont particulièrement visés par les critiques. Car le **Patriot Act les oblige ainsi que leurs filiales situées en dehors des Etats-Unis à remonter des données vers leurs autorités**. En novembre 2012, le rapport « cloud computing » dans l'enseignement supérieur et les instituts de recherche et le Patriot Act américain, rédigé par des juristes de l'université d'Amsterdam, expliquait qu'il s'agissait d'un droit *« extraterritorial »* et qu'il ne s'embarrasse pas des lois nationales ou européennes… En ce moment, l'Europe légifère sur le sujet. En attendant, mieux vaut se rabattre sur un offreur cloud français.

De l'espionnage en interne

Reste qu'un fournisseur français n'est pas un gage de sécurité en soi. *« Parce que, lorsqu'une donnée circule dans le nuage, des centaines de techniciens y ont accès. Par le jeu de la sous-traitance, plus de la moitié d'entre eux ne sont pas en France »,* assure Hervé Schauer, membre du Club de la sécurité de l'information français (Clusif) et expert en sécurité des systèmes d'information. *« Si l'une de ces personnes est corrompue, il n'y a plus de confidentialité dans le cloud. »* Pour se prémunir, il faut obliger son fournisseur à apporter des garanties concrètes. *« Il doit pouvoir expliquer comment son architecture est techniquement cloisonnée et comment les droits sont gérés »,* explique Matthieu Bennasar, consultant sécurité au Lexsi, un cabinet spécialisé en sécurité informatique et gestion des risques.

Chiffrement faible

A défaut d'obtenir ces garanties, il faut vivre avec la crainte d'être mis sur écoute, dans le nuage. Et le bon vieil argument qui veut que le chiffrement protège efficacement les données contre les regards malveillants ne tient en réalité pas la route. C'est un écran de fumée. *« Aucun chiffrement n'est infaillible »,* rappelle Patrick Debus-Pesquet, directeur technique chez Numergy, un des deux opérateurs de cloud souverain. Ce qu'il faut faire, souvent, c'est auditer son cloud afin de déceler la présence de sondes et de logiciels espions.

Pas d'audit par défaut

Mais encore faut-il pouvoir auditer son cloud ! Tous les offreurs ne le permettent pas. *« Il faut négocier en amont une clause d'auditabilité, c'est indispensable »,* martèle Philippe Hervias, directeur sécurité à l'Institut français de l'audit et du contrôle interne (Ifaci).

Réversibilité impossible

Dans tous les cas, négocier avec son fournisseur est une stratégie gagnante. Dans le cas inverse, le risque est de se retrouver piégé avec un mauvais prestataire. Et de ne pas pouvoir en changer, parce qu'il est difficile – voire impossible – de réinjecter ses données dans un nouveau système d'information. *« Je n'ai jamais vu un tel principe mis en œuvre »,* admet Pierre-Josée Billotte, président du conseil d'administration d'Eurocloud France. Il faut donc redoubler de vigilance au moment de signer son contrat. Ou choisir exclusivement des applications SaaS à base de logiciels libres que l'on peut répliquer gratuitement sur une autre plate-forme.

Article original de GUILLAUME PIERRE

Réagissez à cet article

Original de l'article mis en page : Cloud et sécurité : le point sur 7 questions qui fâchent – Les Echos Business