

risques du cloud : ouvrir le parapluie

Plébiscité pour des raisons économiques, le cloud computing soulève de légitimes interrogations sur sa sécurité. Constitue-t-il un risque pour ses données ? Est-il l'avenir des échanges ? Enquête.

éstimé à 846 millions d'euros en 2011, le marché français du cloud public en entreprise ne connaît pas la crise. Il en tire même profit, les raisons financières constituant la première des motivations pour migrer vers ce type d'hébergement. Avec 93 % de ses entreprises connaissant, évaluant ou ayant mis en place des services cloud, la France est le pays d'Europe qui présente la plus forte pénétration européenne de ce phénomène (1).

Comment expliquer cette spécificité nationale ? Pour Pascal Colin, directeur général de Keynectis, éditeur spécialisé dans le domaine de la sécurité des échanges numériques, « les entreprises françaises avaient un retard important sur l'externalisation en général. Elles profitent de la maturité de l'offre cloud pour le combler. Cela montre d'ailleurs que le cloud correspond à une vraie économie, car faire autant avec moins - ou plus avec autant - est le critère principal d'investissement des entreprises en ce moment ». Thomas Luquet, responsable produit sur les offres cloud et datacenters chez Nec, complète l'explication par les particularités du tissu économique français et notamment la prédominance des PME : « Les primo adoptants du cloud aujourd'hui sont les entreprises fournissant des services de cloud public - voire privé [voir encadré] -, avec une cible clairement identifiée, les PME-

PMI, plus enclines à basculer vers une externalisation de leur informatique, pour se concentrer sur leur cœur de métier et ne pas avoir à gérer des investissements matériels et humains qui peuvent peser sur l'entreprise ».

bénéfices et risques

Le cloud computing soulève par conséquent une problématique propre à l'externalisation, avec ses bénéfices, mais aussi ses risques. Renaud Bidou, directeur technique de **Deny All**, entreprise

un certain nombre de précautions en terme de sécurité », explique Thomas Luquet. Il convient d'abord de distinguer le cloud public du cloud privé. Dans le premier cas, le client n'a aucune maîtrise de l'infrastructure en dehors des données et des applications. Elle est mutualisée et la principale problématique réside dans la segmentation et la sécurisation de ces données d'un client à l'autre, ainsi que dans la qualité de sauvegarde opérée par le prestataire. Le cloud privé repose lui sur une infras-



« ne pas avoir à gérer des investissements matériels et humains qui peuvent peser sur l'entreprise »

Thomas Luquet, Nec

spécialisée dans la sécurité informatique, résume : « Il s'agit de confier à un tiers tout ou une partie du stockage et du traitement des données d'une entreprise, sachant que ce tiers fait lui-même probablement appel à d'autres acteurs, plus ou moins visibles ».

Mais le cloud n'est pas que de l'externalisation. « Le cloud repose sur les mêmes concepts, sur les mêmes technologies que les services d'infogérance, mais pousse l'approche encore plus loin puisque ces services externalisés deviennent automatisés, gérables par le client lui-même via des portails web d'administration, et proposent peu à peu des services hybrides. Cette approche nécessite néanmoins de prendre

structure virtualisée, mais propre au client ; ce sont toutes les données (bases de données, serveurs, etc.) et systèmes de l'entreprise qui sont à sécuriser.

degré de sensibilité des données

Que ce soit pour le cloud public ou privé, des technologies existent, mais qu'il est indispensable de mettre en oeuvre au sein de bonnes pratiques, à commencer par une rigoureuse analyse des besoins, c'est-à-dire des données et applications à migrer. Il convient d'abord de définir le degré de sensibilité des données, que ce soit dans leur dimension régle-



mentaire, stratégique ou commerciale. Il est ensuite capital d'examiner attentivement les contrats de service proposés : ne pas hésiter à négocier certaines clauses avant de s'engager. Patrick

Chambet, responsable du centre de sécurité du groupe de Bouygues, souligne un autre aspect relevant aussi de la sécurité, la protection des données personnelles. « Méfiez-vous si le fournisseur de cloud ne sait pas dire où sont hébergées les données, avertit-il. Cela a de fortes chances de signifier que la plateforme est hébergée hors des pays du groupe de l'article 29, c'est-à-dire

tion de bonnes pratiques. Il conseille : « Bien planifier la démarche, à commencer par le choix soigneux des données que l'on conserve et de celles que l'on va mettre en cloud, puis procéder progressivement et non migrer l'ensemble en une fois. Il convient ensuite d'être attentif aux mesures de sécurité disponibles dans ces solutions : mise en place d'authentification et de différents profils, chiffrement des données qui du coup ne sont accessibles que par le client. Enfin, en termes de traçabilité, le fournisseur de cloud doit transmettre sur demande les logs de connexion. Il est conseillé également de contrôler régulièrement la robustesse de l'ensemble à l'aide d'outils automatisés ».

« le choix soigneux des données que l'on conserve et de celles que l'on va mettre en cloud »

Patrick Chambet, Bouygues



virtualisation et étanchéité

Chambet, responsable du centre de sécurité du groupe de Bouygues, souligne un autre aspect relevant aussi de la sécurité, la protection des données personnelles. « Méfiez-vous si le four-

nisseur de cloud ne sait pas dire où sont hébergées les données, avertit-il. Cela a de fortes chances de signifier que la plateforme est hébergée hors des pays du groupe de l'article 29, c'est-à-dire

« dans un pays ne possédant pas de Cnil ou d'équivalent en terme de protection des données personnelles ».

La sécurité du cloud public, pour Patrick Chambet, est avant tout une question de bonnes pratiques. Il conseille : « Bien planifier la démarche, à commencer par le choix soigneux des données que l'on conserve et de celles que l'on va mettre en cloud, puis procéder progressivement et non migrer l'ensemble en une fois. Il convient ensuite d'être attentif aux mesures de sécurité disponibles dans ces solutions : mise en place d'authentification et de différents profils, chiffrement des données qui du coup ne sont accessibles que par le client. Enfin, en termes de traçabilité, le fournisseur de cloud doit transmettre sur demande les logs de connexion. Il est conseillé également de contrôler régulièrement la robustesse de l'ensemble à l'aide d'outils automatisés ».

Les solutions techniques sont à prendre en compte selon trois axes. Premier axe, celui de la disponibilité des systèmes et des données. Il n'a rien d'insurmontable





repères

grâce « au savoir-faire des hébergeurs qui ont l'expertise, les solutions et les process », explique Thomas Luquet. Même si concrètement « les solutions techniques ne sont pas toujours mises en œuvre, car pas toujours adaptées à des environnements multisite, ce qui fait aussi la différence, généralement, entre les gros faiseurs et les data centers de taille moyenne ».

Seconde problématique de sécurité à laquelle la technologie apporte une réponse, l'étanchéité entre clients. Concernant le cloud public, cette problématique est prise en charge par les technologies de virtualisation de réseau, « permettant non seulement de pouvoir créer des réseaux virtuels en garantissant une étanchéité parfaite entre clients, mais permettant également de gérer les plans de reprise d'activité intersite, ce qui reste plus compliqué aujourd'hui, à moins d'opter pour des solutions propriétaires et relativement figées, poursuit Thomas Luquet. La technologie OpenFlow par exemple est une solution open source très intéressante qui pourrait bien apporter des réponses concrètes à la brique de base du cloud, à savoir le réseau ».

Dernier axe, celui des malwares, virus et autres intrusions. Le cloud ne soulève pas de nouvelles problématiques, comme le souligne le spécialiste en offres cloud et data center de Nec : « On parle toujours de réseaux, de serveurs, de firewall, etc. à sécuriser. Les technologies sont matures, encore faut-il qu'elles soient bien implémentées ».

Philippe Rondel, directeur technique France de Check Point Software, précise ce paradigme : « Pour les entreprises qui utilisent des offres de cloud public, il leur suffit de valider le fait que les infrastructures as a service qu'elles utilisent permettent d'héberger les mêmes solutions de sécurité que celles employées en interne », permettant l'application des mêmes procédures de sécurité quelles que soient les données et où qu'elles soient. Il convient cependant de ne pas oublier l'essentiel, les données elles-mêmes via « l'utilisation de logiciels qui vont les analyser, afin de trier

quel cloud

- Le principe du cloud public est d'héberger des applications, mais aussi des données sur une plateforme web mutualisant les ressources informatiques entre plusieurs utilisateurs, plusieurs organisations. Un de ses usages les plus courants réside dans les solutions de type SaaS (software as a service).
- Le principe du cloud privé est de transformer l'infrastructure interne d'une organisation par le biais de technologies de virtualisation et d'automatisation, ce qui permet de délivrer données et services à la demande.

Le cloud public n'offre donc pas le même sentiment de sécurité vis-à-vis des données sensibles d'une entreprise qu'un cloud privé. Il convient pour elle de bien prendre conscience que le cloud privé lui permet d'avoir la main sur son infrastructure informatique, ses données et applications, aussi virtualisées soient-elles. Concrètement, clouds public et privé sont complémentaires, selon le type d'application concernée. Patrick Chambet, responsable du centre de sécurité du groupe Bouygues Telecom, témoigne : « Tout n'est pas encore dans le cloud chez Bouygues Telecom, car nous avons un SI très étendu et complexe. On pratique l'implémentation du cloud en interne, il s'agit donc de cloud privé, avec un double but : pour nos propres besoins et pour proposer ces ressources à nos clients. Nous utilisons aussi du cloud public pour des applications peu sensibles comme du CRM ou des applications à disposition de nos acheteurs ».

L'utilisation combinée de clouds public et privé, dite cloud hybride, constitue l'approche privilégiée par un nombre croissant d'entreprises à l'heure actuelle (1). Thomas Luquet, responsable produit sur les offres cloud et data centers chez Nec, décrit : « Dans le cas d'une grande entreprise avec des données sensibles, on privilégiera effectivement le cloud hybride, consistant à conserver en cloud privé les systèmes les plus critiques et externaliser toutes les données non ou moins sensibles, comme on le voit de plus en plus avec la messagerie par exemple ».

(1) 43 % des entreprises françaises privilégient une approche hybride, étude IDC France datée du 15 décembre 2011.

celles qui sont confidentielles et nécessitent un haut niveau de protection et celles qui ne le sont pas. Pour cela, on utilise des solutions de DLP (data loss prevention) », explique le directeur.

pas de norme dédiée, mais des certifications indispensables

Traditionnels garants de sécurité, standards et normes brillent par leur absence dans le monde du cloud computing. Ils seraient pourtant appréciables : « Ce serait quelque chose de pertinent à mettre en place, à plus forte raison dans le cadre actuel d'une démarche de sensibilisation et de pédagogie vis-à-vis du cloud », estime Patrick Chambet. « On demande des normes – Iso 27001 par exemple (2) – à nos fournisseurs, mais pas réellement de certification

dédiée au cloud ». Pour Philippe Rondel, la certification constitue un élément essentiel pour les entreprises, leur permettant de s'assurer de la bonne mise en œuvre des procédures de sécurité, mais cela ne suffit pas, « ensuite les entreprises doivent s'assurer du niveau de sécurité de leur système en effectuant des tests d'intrusion et de vulnérabilité. Tous les clients ne peuvent pas se le permettre, c'est pourquoi les fournisseurs font de plus en plus tester leur sécurité par des auditeurs tiers et présentent les résultats obtenus à leurs clients ».

Guillaume Nuttin

(1) Étude IDC France datée du 15 décembre 2011.

(2) Publiée en 2005, elle est intitulée Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences.