Cloud computing : la sécurité en question

Au moment où le cloud computing gagne du terrain, Christophe Auberger, Responsable technique chez Fortinet, s'explique sur les erreurs à ne pas commettre en matière de sécurité informatique.

« *Toutes les entreprises ont été ou seront attaquées informatiquement un jour ou l'autre, par hasard ou volontairement. Il faut savoir que l'argent généré par la cybercriminalité est plus important que celui du trafic de drogue !* » C'est l'avertissement de Christophe Auberger, Responsable technique chez Fortinet, société créée il y plus de dix ans, dont l'activité est la sécurité des réseaux informatiques. Celle-ci intervient aussi bien auprès des grands groupes que des PME et ceci dans pratiquement tous les domaines d'activité. D'ailleurs, pour le spécialiste, la sécurité doit être abordée de la même manière, quelle que soit la taille de la structure.

En réalité, il n'existe pas de chiffres fiables qualifiant la cybercriminalité. Les données disponibles varient du simple au triple et les évaluations sont sujettes à caution. Ne serait-ce que parce que les entreprises qui ont subi des attaques informatiques ne le crient pas sur les toits et ne peuvent déterminer précisément le préjudice financier d'un vol ou d'une perte de données. Et puis parce que nombre d'entre elles sont fournies par les prestataires

Christophe Auberger, responsable technique chez Fortinet.

de services comme Fortinet, ou des éditeurs d'anti-virus... Reste que le risque est là et, qu'à l'échelle mondiale, le coût de la cybercriminalité est sans doute de plusieurs centaines de milliards de dollars chaque année !

Les cinq erreurs à éviter

Alors, y a-t-il plus de risque de perdre ses données, ou d'être piraté si l'on adopte les services de cloud computing proposés désormais aux industriels et notamment bureaux d'études ? Des services qui logiquement améliorent la flexibilité et la productivité de l'entreprise tout en réduisant les coûts d'infrastructure. « *Pas plus que dans toute démarche d'externalisation. Vous devez évaluer les capacités de votre prestataire à assurer la sécurité de vos données. Mais c'est loin d'être simple, car il n'existe pas de références communes sur ce critère technique. Les bonnes*

pratiques se standardisent dans certains domaines d'activité comme la finance, mais l'industrie reste encore pauvre en la matière. Le passage au cloud est l'occasion pour l'entreprise qui se lance de se poser les bonnes questions sur la sécurité de la chaîne informatique mise en place. Et dans tous les cas, le niveau de celle-ci dépend de son maillon le plus faible. Il faut donc porter attention à cinq points majeurs... »

1. Ne pas opter pour le bon modèle de cloud

Les entreprises migrant vers le cloud peuvent choisir parmi les clouds publics, clouds privés, clouds communautaires ou clouds hybrides.

• Le cloud public : Il appartient à un fournisseur cloud et est accessible à un large public. Le principe est de payer à l'utilisation et la plateforme est partagée avec d'autres utilisateurs.

• Le cloud privé : Il appartient à une organisation et est déployé pour sa propre utilisation puisqu'elle en est la seule et unique propriétaire.

• Le cloud communautaire : Il est partagé en coopération par plusieurs organisations, souvent de la même industrie.

• Le cloud hybride : Il mixe les modèles de déploiement cloud énumérés ci-dessus, permettant aux applications et données de passer facilement d'un cloud à l'autre.

Chaque type de déploiement en matière de cloud a ses avantages. Les facteurs à considérer avant l'adoption sont : le niveau de criticité des applications que l'entreprise veut basculer dans le cloud ; les questions de réglementation et de conformité ; les niveaux de services (SLA) nécessaires ; les modes d'utilisation selon les charges de travail ; et la manière dont les applications doivent être intégrées aux autres fonctions de l'entreprise.

2. Ne pas intégrer la sécurité cloud dans sa politique de sécurité d'entreprise

Vos politiques de sécurité cloud et sécurité d'entreprise doivent être intégrées. Au lieu de créer une nouvelle politique de sécurité pour le cloud, renforcez plutôt celles qui existent en considérant cette plateforme supplémentaire. Pour modifier vos politiques cloud, vous devez tenir compte des facteurs suivants : où sont stockées les données ? Comment sont-elles protégées ? Qui y a accès ? Mais aussi la conformité avec les règlementations, et les niveaux de services SLA.

Lorsqu'elle est correctement effectuée, l'adoption du cloud computing peut être une occasion d'améliorer vos politiques de sécurité et votre position globale de sécurité.

3. Compter sur la sécurité de son fournisseur de services cloud

Ne pensez pas que vos données soient automatiquement sécurisées parce que vous utilisez un fournisseur

« Toutes les entreprises ont été ou seront attaquées informatiquement un jour ou l'autre, par hasard ou volontairement. »

de services. Vous devez faire un examen complet de la technologie et des processus de sécurité du fournisseur, et vérifier la manière dont ils sécurisent vos données et leurs infrastructures. Plus précisément, vous devez examiner :

• La transportabilité des données et applications : votre fournisseur vous permet-il d'exporter les applications, données et processus existants dans le cloud ? Pouvez-vous les importer de nouveau aussi facilement ?

• La sécurité physique des centres de données : comment les fournisseurs de services protègent-ils leurs centres de données physiques ? Utilisent-ils des centres de données certifiés aux normes SAS 70 Type II ? Comment leurs opérateurs de centres de données sont-ils formés et qualifiés ?

• La sécurité des accès et des opérations : comment votre fournisseur contrôle-t-il l'accès aux machines physiques? Qui peut accéder à ces machines, et comment sont-elles gérées ?

• La sécurité du centre de données virtuel : l'architecture cloud est la clé de l'efficacité. Sachez comment les parties individuelles telles que les nœuds de traitement, nœuds du réseau et nœuds de stockage sont-elles architecturées, et comment sont-elles intégrées et sécurisées.

• La sécurité des données et des applications : Pour mettre vos politiques en application, la solution cloud doit vous permettre de définir des groupes et rôles avec un contrôle d'accès basé sur le rôle précis, des règles de mots de passe et un cryptage des données appropriées (en transit et à l'arrêt).

Y a-t-il plus de risque de perdre ses données ou d'être piratés si l'on adopte les services de cloud computing ?

4. Supposer que vous n'êtes plus responsable de la sécurisation des données

Ne pensez jamais que l'externalisation de vos applications ou systèmes signifie que vous n'êtes plus responsable en cas de violation de données. Certaines PME ont cette fausse idée, mais sachez que votre entreprise est toujours au bout du compte responsable vis-à-vis de ses clients et de tout autre partie prenante lorsqu'il s'agit d'inviolabilité des données. Autrement dit, c'est votre CEO qui risque d'aller en prison, et non le fournisseur cloud...

5. Ne pas savoir quelles lois locales s'appliquent

Les données qui sont en sécurité dans un pays peuvent ne pas l'être dans un autre. Cependant, dans de nombreux cas, les utilisateurs des services cloud ne savent pas où sont stockées leurs informations. Actuellement, dans le processus d'harmonisation des lois sur les données de ses états membres, l'Union Européenne favorise la protection très stricte de la vie privée, tandis que les lois américaines, telles que l'US Patriot Act, permettent au gouvernement et autres organismes d'avoir un accès quasi illimité aux informations appartenant aux entreprises.

Sachez toujours où sont vos données. Si nécessaire, stockez-les dans plusieurs endroits. Il est conseillé de choisir une juridiction qui vous permette d'accéder à vos données même si votre contrat avec votre fournisseur cloud se termine de manière inattendue. Le fournisseur de services devrait également vous donner l'option de choisir l'endroit où vos données seront stockées.

Pour conclure, l'adoption du cloud passe par des démarches de réductions des risques, et il est important que les entreprises se chargent de bien planifier et de veiller au respect de ces mesures dès le début, de sorte que les retours sur investissements en matière de cloud soient maximisés.