Etude Gemalto & Ponemon : sécuriser les données dans le cloud reste un défi pour de nombreuses entreprises

- 40% des services cloud et des données corporate de l'entreprise stockées dans le cloud ne sont pas contrôlés par les départements IT
- 30% des données sensibles hébergées au sein d'applications basées dans le cloud sont chiffrées
- La moitié des entreprises ne dispose pas d'une approche proactive visant à respecter les règles de confidentialité et de sécurité des données transitant au sein des environnements cloud.

Paris, le 26 Juillet, 2016 - En dépit de l'intérêt croissant des entreprises pour le cloud computing, celles-ci n'ont pas encore adopté les mesures de gouvernance et de sécurité appropriées leur permettant de protéger les données sensibles stockées dans le cloud.
Il s'agit là des premières conclusions de l'étude intitulée « The 2016 Global Cloud Data Security Study », réalisée par le Ponemon Institute pour le compte de Gemalto (Euronext NL0000400653 GTO), leader mondial de la sécurité numérique. Se basant sur les réponses de plus de 3 400 spécialistes IT interrogés de par le monde (dont plus de 300 en France), elle fait état des tendances clés en matière de gouvernance des données et des pratiques de sécurité destinées aux services basés sur le cloud.

Pour 36% des répondants, les services et les plates-formes cloud sont considérés comme importants dans l'exécution de leurs opérations courantes, et 39% indiquent qu'ils devraient l'être plus encore au cours des deux prochaines années. Plus précisément, 24% déclarent que l'utilisation actuelle du cloud répond à leurs besoins en matière d'informatique et de traitement des données, un constat qui devrait augmenter à 51% d'ici deux ans.

Bien que le cloud joue un rôle de plus en plus important dans l'exécution des opérations informatiques et dans le déploiement des stratégies commerciales, la moitié des personnes interrogées estiment qu'aucune démarche de sécurité et de conformité avec les réglementations en matière de confidentialité des données dans les environnements cloud n'a été mise en place dans leur entreprise de façon proactive. Pour autant, 65% déclarent que celles-ci sont très engagées dans la protection des informations confidentielles ou sensibles. En outre, 62% pensent que leur entreprise se montre pourtant prudente concernant le partage d'informations sensibles dans le cloud avec des utilisateurs tiers tels que les partenaires, les intérimaires ou les fournisseurs.

« La sécurité du cloud reste un défi pour les entreprises, qui est accentué par la complexité des règlementations en matière de confidentialité et de protection des données », indique le Dr Larry Ponemon, président et fondateur du Ponemon Institute. « Pour s'assurer d'être conformes, les entreprises doivent déployer des technologies telles que le chiffrement, la tokenisation et d'autres solutions de cryptage visant à protéger les données sensibles transférées et stockées dans le cloud. »

« Les entreprises ont adopté le cloud afin de gagner en flexibilité et de rationaliser leurs coûts mais elles ont encore des difficultés à maintenir le contrôle et la conformité de leurs données au sein des environnements virtuels », souligne Jason Hart, vice-président et CTO pour la protection des données chez Gemalto. « Face à ces nouveaux challenges, les mesures de sécurité traditionnelles ne sont pas adaptées, car elles permettent de sécuriser des données uniquement présentes sur le réseau physique. C'est pourquoi les services IT doivent adopter une approche centrée sur les données, permettant de protéger aussi bien celles de leurs clients que leurs informations sensibles, circulant via les différents services cloud utilisés au quotidien par les employés et départements internes ».

Principales conclusions

Le Shadow IT, responsable de la complexité de la sécurité du cloud
Selon les répondants, plus de la moitié (49%) des services cloud sont déployés par des départements autres que le service IT de l'entreprise, et 42% des données en moyenne sont stockées dans des environnements cloud dont le contrôle et la gestion lui échappe. Cependant, le sentiment de disposer d'une forte visibilité quant à l'utilisation des services cloud est en hausse. Ainsi, 68% des personnes interrogées sont convaincues que le service IT dispose d'une vision à 360° sur l'ensemble des applications, services, plate-formes ou infrastructures cloud utilisées.

Les pratiques de sécurité classiques ne sont pas applicables au cloud
54% des répondants estiment qu'il est plus difficile de protéger des informations sensibles en ayant recours à des services cloud. Les problématiques liées au contrôle et à la restriction de l'accès des utilisateurs représentent 67% des inquiétudes des répondants. Les autres défis majeurs incluent l'incapacité à pouvoir sécuriser des données de manière classique au sein des environnements cloud (pour 64%) et l'impossibilité de s'assurer que les fournisseurs de services cloud sont bien conformes en matière de sécurité (pour 76%).

Plus les données clients sont stockées dans le cloud, plus elles sont à risque
Selon l'enquête, les informations clients et celles liées aux paiements, les e-mails, les profils des consommateurs et les dossiers des employés, sont les types de données le plus souvent hébergés dans le cloud. Le taux d'informations clients présentes dans le cloud est de 59%. Des données qui sont considérées comme étant, de ce fait, à risque par 51% des personnes interrogées.

Les services IT sont tenus à l'écart des achats de services cloud
Seulement 10% des répondants indiquent que les équipes sécurité sont systématiquement impliquées dans le choix des applications ou plates-formes cloud. 50% d'entre eux précisent également que leur entreprise ne dispose pas de politique impliquant l'utilisation de mesures de sécurité, telles que le chiffrement, pour pouvoir utiliser certaines de ces applications.

Les solutions de chiffrement se développent, mais ne sont pas encore omniprésentes dans le cloud
80% des répondants considèrent comme important le fait de pouvoir chiffrer ou tokéniser des données sensibles ou confidentielles, et 91% pensent même que cela devrait l'être plus encore au cours des deux prochaines années. Bien que le recours aux solutions cryptographiques se généralise, elles ne sont pas encore assez largement déployées dans le cloud. Par exemple, pour les plateformes du type SaaS, qui sont les plus répandues, seulement 30% des personnes interrogées indiquent que le chiffrement et la tokénisation se font directement depuis les applications basées sur le cloud.

De nombreuses entreprises ont encore recours aux mots de passe pour sécuriser l'accès des utilisateurs aux services cloud
La gestion de l'identité des utilisateurs est jugée par 60% des répondants comme étant plus difficile à sécuriser dans le cloud que sur site. Toutefois, bon nombre d'entreprises n'ont pas encore adopté de mesures permettant de renforcer cette sécurité. 32% d'entre elles n'ont pas recours à des solutions d'authentification multi-facteurs pour sécuriser l'accès des employés ou d'utilisateurs tiers, aux applications et données stockées dans le cloud. Cela signifie qu'elles sont encore nombreuses à se baser uniquement sur le nom et le mot de passe de l'utilisateur pour valider leur identité. Les

données sont ainsi plus à risque, avec 55% des répondants indiquant que des utilisateurs tiers ont accès aux informations de leur entreprise via le cloud.

Quelques recommandations pour les services IT

- Définir des politiques globales en termes de gouvernance des données et de conformité, mettre en place des directives claires en matière de sourcing des services cloud, et établir des règles quant aux données pouvant ou ne pouvant pas être stockées dans le cloud.

- Assurer la protection des données de l'entreprise tout en limitant le phénomène de « Shadow IT » en ayant recours à des solutions telles que le chiffrement.

- Renfoncer les contrôles d'accès des utilisateurs par l'authentification multi-facteurs.

À propos de l'étude

L'enquête a été menée par le Ponemon Institute pour le compte de Gemalto et a interrogé 3,476 spécialistes IT aux États-Unis, au Brésil, au Royaume-Uni, en Allemagne, en France, en Russie, en Inde, au Japon et en Australie, dont les entreprises ont recours à des services de cloud public et privé. Les secteurs ici représentés sont les services financiers, le commerce, les technologies et les logiciels, le secteur public, la santé et le pharmaceutique, l'énergie, l'éducation, le transport, la communication, les médias, et les métiers de réception.

Ressources connexes

- Report: Gemalto 2016 Global Cloud Data Security Study
- Infographic: Gemalto Cloud Data Security Infographic
- Web Site: Gemalto 2016 Global Cloud Data Security Study Findings
- Video: Gemalto Cloud Security Solutions Overview
- Web Site: You Can't Secure the Cloud with Old School Technology

Contacts Presse :

Gemalto Peggy Edoire, Europe et CEI +33 4 42 36 45 40
peggy.edoire@gemalto.com

LEWIS
Natacha Kalasa / Célia Casabianca +33 1 55 31 75 63
gemaltofrance@teamlewis.com