Instaurer la confiance dans le cloud

Les services de cloud font désormais partie intégrante des opérations informatiques et sont utilisés par plus de 90 % des entreprises à travers le monde. De nombreuses entreprises ont adopté une philosophie de priorisation du cloud, en choisissant de ne déployer un service interne qu'en l'absence de variante de cloud appropriée. Par conséquent, les architectures informatiques évoluent rapidement vers un modèle de cloud privé/public hybride. Les répondants s'attendent à ce que 80 % de leur budget informatique soit consacré à des solutions de cloud d'ici 15 mois en moyenne.

93 %

des entreprises **utilisent des services de cloud** sous une forme ou l'autre.

49 %

des répondants ont **mis un frein à l'adoption du cloud** en raison d'un manque de compétences en cybersécurité.

62 %

des entreprises ont déclaré **stocker les informations personnelles de clients** dans des clouds publics.

En septembre 2016, Intel Security a interrogé plus de 2 000 responsables informatiques pour produire ce compte-rendu annuel de l'état de l'adoption du cloud, qui représente un large éventail de secteurs, pays et tailles d'entreprises. Face à la pénurie persistante de personnel de sécurité qualifié, l'impact de ce déficit de compétences sur l'adoption du cloud était une des priorités du rapport de cette année. Les autres objectifs consistaient à comprendre l'adoption des différents modèles d'utilisation du cloud, à identifier les principales préoccupations liées aux services de cloud privé et public, ainsi qu'à examiner l'impact grandissant de l'informatique de l'ombre.

Les participants à l'étude étaient des décideurs techniques issus de petites (500 à 1 000 employés), moyennes (1 000 à 5 000 employés) et grandes entreprises (plus de 5 000 employés) situées en Allemagne, en Australie, au Brésil, au Canada, aux États-Unis, en France, dans les pays du Golfe (Arabie saoudite et Émirats arabes unis), au Japon, au Mexique, au Royaume-Uni et à Singapour.

Principales observations

- Les services de cloud sont largement utilisés sous une forme ou l'autre. Ainsi, 93 % des entreprises recourent à des offres de services de logiciels (SaaS, Software-as-a-Service), d'infrastructure (IaaS, Infrastructure-as-a-Service) ou de plate-forme (PaaS, Platform-as-a-Service).
- Le nombre moyen de services de cloud utilisés dans une entreprise est passé de 43 en 2015 à 29 en 2016, ce qui suggère une possible consolidation des fournisseurs ou des solutions de cloud. Les architectures de cloud ont également considérablement évolué : alors qu'elles étaient majoritairement privées en 2015, l'adoption croissante du cloud public a entraîné l'apparition d'une infrastructure essentiellement hybride (privée/publique) en 2016.
- Près de la moitié (49 %) des professionnels interrogés ont déclaré avoir mis un frein à l'adoption du cloud en raison d'une pénurie de compétences en cybersécurité, un manque qui se fait particulièrement ressentir au Japon, au Mexique et dans les pays du Golfe.
- La confiance dans les services de cloud public, de même que leur perception, continuent à s'améliorer d'année en année. La plupart des entreprises considèrent les services de cloud comme aussi sûrs, voire plus, que les clouds privés, et comme bien plus susceptibles de réduire les coûts de possession et d'offrir une visibilité globale sur les données. Les entreprises qui font confiance aux clouds publics sont désormais plus de deux fois plus nombreuses que celles qui s'en méfient.

intel Security

52 %

des répondants ont identifié une **application SaaS comme étant à l'origine d'une infection par logiciel malveillant**.

40 %

des services de cloud **sont mis en service sans l'intervention du service informatique**.

65 %

des responsables informatiques estiment que **le cloud de l'ombre interfère** avec leur capacité à garantir la sécurité du cloud.

2 ans

Délai dans lequel les répondants prévoient de migrer vers un **centre de données entièrement défini par logiciel (SDDC)**

- Le renforcement de la confiance et de la perception, ainsi qu'une meilleure compréhension des risques par la direction, encouragent davantage d'entreprises à stocker des données sensibles dans le cloud public. Les informations personnelles des clients sont le type de données le plus susceptible d'être stocké dans les clouds publics, si l'on en croit les réponses fournies par 62 % des répondants.
- Les applications de cloud demeurent un vecteur de choix pour les cyberattaques. Plus de la moitié (52 %) des répondants déclarent avoir identifié une application SaaS comme étant à l'origine d'une infection par logiciel malveillant.
- L'informatique de l'ombre suscite toujours plus d'inquiétudes dans le chef du service informatique. Face au ralentissement de l'adoption de l'informatique ou à l'acceptation généralisée des clouds, près de 40 % des services de cloud sont mis en service sans intervention du service informatique. En conséquence, 65 % des responsables informatiques estiment que ce phénomène interfère avec leur capacité à garantir la sécurité du cloud.
- La virtualisation des architectures de centres de données privés est en progression. En moyenne, 52 % des serveurs de centre de données d'une entreprise sont virtualisés. En outre, la plupart des entreprises prévoient de migrer vers un centre de données entièrement défini par logiciel (SDDC) au cours des deux prochaines années.

Conclusions et recommandations

Les entreprises confient aux services de cloud un large éventail d'applications et de données, pour la plupart sensibles ou stratégiques. Les données sont envoyées là où elles sont nécessaires et où elles seront les plus efficaces. Des mécanismes de sécurité doivent dès lors être mis en place suffisamment à l'avance pour détecter rapidement les menaces, protéger l'entreprise et neutraliser les tentatives de compromission des données. Les économies de temps et d'argent offertes par les services de cloud sont bien réelles, et la diversité des offres permet de choisir les services les mieux adaptés à l'entreprise. Les éditeurs de solutions de sécurité proposent des outils visant à répondre aux principales préoccupations en matière de sécurité, telles que la protection des données en transit, la gestion des accès des utilisateurs et la mise en place de stratégies cohérentes entre plusieurs services.

La migration des données sensibles vers le cloud public risque d'attirer les cybercriminels. En effet, ceux-ci sont en permanence à la recherche des cibles les plus faciles, où qu'elles se trouvent. Les solutions de sécurité intégrées ou unifiées constituent une défense efficace contre ces menaces, en offrant aux opérations de sécurité une visibilité sur tous les services utilisés par l'entreprise et sur les ensembles de données autorisés à les traverser.

Les attaques cibleront le plus probablement les identifiants des utilisateurs, en particulier ceux des administrateurs. Les entreprises doivent dès lors s'assurer d'adopter les meilleures pratiques en matière d'authentification, comme des mots de passe distincts, l'authentification multifacteur et la biométrie, lorsque disponible.

Malgré la croyance générale selon laquelle l'informatique de l'ombre met l'entreprise en péril, les technologies de sécurité telles que la prévention des fuites de données, le chiffrement et les intermédiaires de sécurité de l'accès au cloud (CASB) demeurent sous-utilisées. L'intégration de ces outils à un système de sécurité existant améliore la visibilité, permet la découverte des services de l'ombre et met à disposition des options de protection automatique des données sensibles inactives et en mouvement dans n'importe quel type d'environnement.

S'il est possible d'externaliser le travail à des tiers, il n'en va pas de même des risques. Les entreprises doivent donc évoluer vers une approche de la sécurité des informations basée sur la gestion et la réduction des risques. Pourquoi dès lors ne pas envisager une stratégie de priorisation du cloud qui encourage l'adoption de services de cloud de façon à réduire les coûts et à améliorer la flexibilité, de même qu'à placer les opérations de sécurité dans une position proactive plutôt que réactive.

Pour télécharger le rapport complet, **cliquez ici**.

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com