Instaurer la confiance dans le cloud

La perspective du secteur des services financiers à l'échelle mondiale

Selon notre étude, les établissements de services financiers sont plus susceptibles d'utiliser les services de cloud que les entreprises des autres secteurs. En effet, 99 % de ces entreprises ont recours à des fonctions fournies dans le cloud, tandis que la moyenne mondiale tous secteurs confondus n'est que de 93 %. Ce secteur compte un nombre particulièrement important d'entreprises ayant adopté une philosophie de priorisation du cloud : elles ne déploient un service interne qu'en l'absence d'une variante cloud appropriée. Ainsi, 87 % des entreprises du secteur ont déjà adopté cette philosophie, contre une moyenne de 82 % des entreprises mondiales tous secteurs confondus. Nous avons par ailleurs découvert que les architectures informatiques des entreprises de services financiers évoluent rapidement d'une infrastructure de centre de données en cloud privé, 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 14 mois en moyenne.

99 %

des entreprises de services financiers **ont recours à une forme ou l'autre de service de cloud**.

57 %

des entreprises de services financiers **utilisent des solutions de cloud public/privé hybrides**.

48 %

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

Cette analyse de l'adoption des services de cloud par les entreprises de services financiers, de leurs préoccupations et de leurs projets futurs s'appuie sur l'**étude 2016 sur l'état du cloud** d'Intel Security. Les participants à l'étude étaient des décideurs informatiques responsables de la sécurité du monde entier : Allemagne, Arabie saoudite, Australie, Brésil, Canada, Émirats arabes unis, États-Unis, France, Japon, Mexique, Royaume-Uni et Singapour.

Principales observations — Services financiers

Le secteur des services financiers est celui où l'adoption du cloud rencontre le plus grand succès (99 % des entreprises interrogées), uniquement égalé par le secteur des nouvelles technologies en pourcentage d'entreprises qui utilisent une forme ou l'autre de service de cloud. Les architectures de cloud de ces entreprises ont connu des bouleversements considérables au cours de l'année écoulée. La proportion d'entreprises utilisant des services de cloud privé exclusivement a chuté, passant de 50 % en 2015 à 26 % en 2016, à la suite de l'adoption croissante de solutions de cloud privé/public hybrides, désormais utilisées par 57 % du secteur.

Près de la moitié (48 %) des responsables interrogés ont mis un frein à l'adoption du cloud en raison d'un manque de compétences en cybersécurité au sein de leur équipe informatique. La pénurie de compétences et les préoccupations en matière de sécurité ralentissent l'adoption, mais la perception

54 %

des répondants du secteur des services financiers ont identifié une **application SaaS en tant que vecteur d'une infection par logiciel malveillant**.

64 %

des entreprises de services financiers **stockent tout ou partie de leurs données clients sensibles** dans des clouds publics.

39 %

des services de cloud sont **mis en service sans l'approbation du département informatique, qui ne dispose d'une visibilité que sur 45 %** d'entre eux.

et la confiance dans les services de cloud public continuent de progresser d'année en année. La plupart des entreprises de services financiers considèrent les services de cloud public comme aussi sûrs, voire plus sûrs, que les clouds privés. En outre, elles les jugent nettement plus susceptibles de réduire les coûts de possession et d'offrir une visibilité sur les données. D'après elles, le seul véritable avantage que peuvent offrir les clouds privés par rapport aux clouds publics réside dans la protection contre les pirates.

Les applications de cloud demeurent un vecteur de choix pour les cyberattaques. Plus de la moitié (54 %) des répondants du secteur des services financiers déclarent avoir identifié une application SaaS comme étant à l'origine d'une infection par logiciel malveillant. Cependant, ce secteur figure parmi les moins susceptibles d'avoir subi une perte de données ou une compromission (19 % contre une moyenne mondiale de 22 %).

Les entreprises de services financiers qui font confiance aux clouds publics sont désormais plus de deux fois plus nombreuses que celles qui s'en méfient. Ce renforcement de la confiance et de la perception, ainsi qu'une meilleure compréhension des risques de la part des cadres dirigeants, encouragent davantage d'entreprises à stocker des données sensibles dans le cloud public. Les entreprises de services financiers sont les plus susceptibles de stocker tout ou partie de leurs données clients sensibles dans le cloud public (64 %), probablement en raison de l'omniprésence des transactions financières et autres services en ligne.

Les responsables informatiques du secteur ont indiqué qu'ils sont plus susceptibles d'utiliser les services SaaS (64 %), suivis de près par les services IaaS (57 %). Les offres PaaS se classent en troisième place, mais loin derrière (38 %). Toutefois, leurs projets d'investissement pour l'année à venir s'orientent davantage vers les services IaaS. En effet, 69 % d'entre eux prévoient d'accroître leur activité dans ce domaine, tandis que 60 % projettent d'utiliser davantage de services SaaS, et 52 % prévoient une augmentation des investissements dans les services PaaS.

Concernant l'utilisation des services SaaS, leur préoccupation principale était identique à celle des autres entreprises, c'est-à-dire la protection des données sensibles qui circulent entre l'entreprise et le cloud. En matière d'offres IaaS, leurs principales préoccupations étaient liées au maintien de la conformité et aux accès non autorisés potentiels dans un cloud public multiclient, tandis que les responsables des entreprises des autres secteurs étaient davantage préoccupés par le maintien de la cohérence des contrôles de sécurité. Le nombre moyen de services de cloud utilisés dans les entreprises de services financiers est passé de 40 en 2015 à 29 en 2016, ce qui suggère une possible consolidation des fournisseurs de cloud.

L'informatique de l'ombre représente un problème pour les départements informatiques du secteur des services financiers, comme dans la plupart des secteurs. Les responsables informatiques indiquent que les services de cloud adoptés sans l'approbation du département informatique représentent 39 % de l'utilisation de services, et qu'ils disposent de visibilité sur moins de la moitié de ces applications (45 %). La plupart des entreprises de services financiers s'appuient sur les pare-feux de nouvelle génération pour surveiller l'utilisation des services de cloud qui n'ont pas été approuvés par le département informatique (59 %). Lors de l'identification d'une application non approuvée, les réponses les plus probables consistent à bloquer entièrement l'accès à l'application (28 %) ou à s'en remettre à une solution de gestion des identités et des accès (27 %) pour limiter l'accès. Étonnamment au vu de leur préoccupation supérieure à la moyenne en ce qui concerne la protection des données qui circulent entre l'entreprise et le cloud public, les entreprises de services financiers ont indiqué une utilisation légèrement inférieure à la moyenne des outils de chiffrement et de prévention des fuites de données. Dans l'ensemble, les responsables informatiques des services financiers sont parmi les plus préoccupés par l'informatique de l'ombre, 72 % d'entre eux ayant déclaré que ce phénomène interfère avec leur capacité à préserver la sécurité du cloud.

Si les entreprises de services financiers adoptent de plus en plus volontiers le cloud public, 26 % d'entre elles continuent d'utiliser uniquement des services de cloud privé, alors que 57 % ont recours à un mélange hybride de cloud public et privé. En termes de cloud privé, le pourcentage actuel de virtualisation des serveurs de centre de données est supérieur à la moyenne mondiale (55 % contre 52 %), et l'adoption des conteneurs dans ce secteur correspond au taux moyen de 80 % à l'échelle mondiale. La majorité d'entre eux (73 %) prévoient de compléter la migration vers un centre de données entièrement défini par logiciel (SDDC) dans les deux ans.

Conclusions et recommandations

Il apparaît que le secteur des services financiers fait partie des secteurs où l'adoption du cloud rencontre le plus grand succès, et où la sécurité a atteint la plus grande maturité. En effet, les entreprises de ce secteur ont fait état d'une utilisation supérieure du cloud, mais d'un nombre inférieur de compromissions par rapport à leurs homologues des autres secteurs.

Les clouds sont désormais solidement ancrés dans le paysage informatique, et les responsables des opérations de sécurité mettent tout en œuvre pour s'aligner sur ce taux d'adoption très important. La grande variété des offres de cloud disponibles permet de choisir la mieux adaptée aux besoins de l'entreprise, tant en termes de coûts que de sécurité. Les éditeurs de solutions de sécurité proposent les outils nécessaires pour 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.

Les entreprises de services financiers disposent d'informations de paiement de grande valeur et constituent depuis longtemps une cible privilégiée des cybercriminels. Ceux-ci continueront de rechercher les cibles les plus faciles, qu'elles se trouvent dans les clouds publics, privés ou hybrides. 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.

Selon le rapport de McAfee Labs **Prévisions 2017 en matière de menaces**, les identifiants, en particulier ceux des administrateurs, représenteront les vecteurs d'attaque les plus probables. Veillez à mettre en place une protection appropriée sur tous les terminaux, y compris les tablettes et les smartphones. Les meilleures pratiques en matière d'authentification, telles que l'utilisation de mots de passe distincts, l'authentification multifacteur et, si possible, des solutions biométriques, participent des stratégies préventives essentielles qui réduisent considérablement le risque d'infection ou de compromission.

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. Si ce n'est pas déjà fait, il serait bon d'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 plus d'informations, lisez le rapport complet, **Instaurer la confiance dans le cloud**.

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