Instaurer la confiance dans le cloud

La perspective du secteur des soins de santé à l'échelle mondiale

Probablement stimulée par les économies potentielles et la numérisation rapide des informations médicales, l'utilisation des services de cloud par le secteur des soins de santé est légèrement supérieure à la moyenne mondiale. Le cloud est en effet adopté par 96 % des organisations de ce secteur, contre une moyenne mondiale de 93 % tous secteurs confondus. À l'instar de leurs homologues dans d'autres secteurs, 81 % des établissements de soins de santé ont adopté une philosophie de priorisation du cloud : ils ne déploient un service interne qu'en l'absence d'une variante cloud appropriée. Par conséquent, les architectures informatiques des établissements de soins de santé évoluent progressivement 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 15 mois en moyenne.

Cette analyse de l'adoption des services de cloud par les établissements de soins de santé, de leurs préoccupations et de leurs projets futurs s'appuie sur l'**étude 2016 d'Intel Security sur le cloud**. 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.

96 %

Ce taux d'adoption place le secteur des soins de santé dans le **trio de tête** en matière d'adoption du cloud.

24 %

des établissements de soins de santé utilisent des services de cloud **public exclusivement** (SaaS, IaaS ou PaaS).

Principales observations — Soins de santé

Selon notre étude, le secteur des soins de santé fait partie des trois secteurs où l'adoption du cloud rencontre le plus grand succès (96 %). Il est dépassé uniquement par le secteur des services financiers (99 %) et le secteur des nouvelles technologies (99 %) en pourcentage d'entreprises qui utilisent une forme ou l'autre de service de cloud. Le nombre moyen de services de cloud utilisés dans les établissements de soins de santé est passé de 41 en 2015 à 33 en 2016, ce qui représente une baisse inférieure à la moyenne mondiale, passée de 43 à 29 services, mais suggère néanmoins une possible consolidation des fournisseurs ou services de cloud.

Les architectures de cloud ont connu des bouleversements considérables, évoluant d'un modèle dominé par le cloud privé en 2015 vers un modèle essentiellement hybride de cloud privé/public, bien que le secteur des soins de santé compte le nombre d'utilisateurs d'architecture hybride le plus faible. Étonnamment, les établissements de soins de santé figurent parmi les plus grands utilisateurs de services de cloud exclusivement public (SaaS, IaaS ou PaaS), enregistrant un taux d'utilisation de 24 %, bien supérieur à la moyenne mondiale de 19 %. Les responsables informatiques du

46 %

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

60 %

des établissements de soins de santé **stockent des données de patients** dans des clouds publics.

52 %

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

38 %

des services de cloud utilisés dans les établissements de soins de santé sont **mis en service sans l'approbation du département informatique, qui ne dispose d'une visibilité** que sur la moitié d'entre eux.

secteur des soins de santé affirment qu'ils sont presque deux fois plus susceptibles d'utiliser des services SaaS que des offres IaaS ou PaaS. Les services SaaS représentent également leur principale priorité pour l'année à venir puisque 67 % d'entre eux prévoient d'augmenter leurs investissements dans ce domaine.

Près de la moitié (46 %) des responsables interrogés ont mis un frein à l'adoption du cloud en raison d'un manque de compétences en cybersécurité. Ce constat est particulièrement vrai lorsqu'ils sont interrogés spécifiquement sur leurs préoccupations liées aux services IaaS. Les compétences requises par le personnel de sécurité informatique constituaient la principale préoccupation des répondants du secteur des soins de santé en matière de services IaaS. Ce facteur devance les contrôles de sécurité cohérents et intégrés, qui dominent par contre les préoccupations liées aux services IaaS si l'on considère l'ensemble des répondants à l'échelle mondiale.

La pénurie de compétences en sécurité ralentit l'adoption, mais la perception et la confiance dans les services de cloud public continuent de progresser d'année en année auprès des organismes de soins de santé. La plupart d'entre eux considèrent les services de cloud public comme aussi sûrs, voire plus sûrs, que les clouds privés. En outre, ils les jugent nettement plus susceptibles de réduire les coûts de possession et d'offrir une visibilité globale sur les données que les clouds privés. Les entreprises qui font confiance aux clouds publics sont désormais plus de deux fois plus nombreuses que celles qui s'en méfient. Le renforcement de la confiance et de la perception, ainsi qu'une meilleure compréhension des risques de la part des cadres dirigeants, encouragent davantage d'établissements de soins de santé à stocker des données sensibles dans le cloud public. Cela peut être dû à leur niveau de préoccupation supérieur à la moyenne (37 % contre une moyenne mondiale de 30 %) en matière d'accès non autorisé aux données sensibles dans un cloud privé. Les établissements de soins de santé sont parmi les plus susceptibles de stocker tout ou partie de leurs données sensibles dans le cloud public, en particulier les données des patients (60 %) et les données du personnel (54 %) — un phénomène probablement dû à la généralisation des dossiers médicaux électroniques et de la nature interconnectée du système de soins de santé.

Cependant, les applications de cloud demeurent un vecteur de choix pour les cyberattaques. Plus de la moitié (52 %) des répondants du secteur des soins de santé déclarent avoir identifié une application SaaS comme étant à l'origine d'une infection par logiciel malveillant. Ils sont également parmi les plus susceptibles d'avoir subi une perte de données (25 % contre une moyenne mondiale de 22 %) ou un incident lié à un logiciel malveillant (13 % contre une moyenne mondiale de 10 %) pouvant être imputé à leurs fournisseurs de services de cloud.

L'informatique de l'ombre demeure un problème pour les départements informatiques du secteur des soins de santé, comme dans la plupart des secteurs. Les services SaaS utilisés dans les établissements de soins de santé n'ont pas forcément reçu l'approbation du département informatique. Les responsables interrogés indiquent que les services de cloud adoptés sans l'approbation du département informatique représentent 38 % de l'utilisation de services, et qu'ils ne disposent de visibilité que sur la moitié de ces applications. Lors de l'identification d'une application non approuvée, la réponse la plus probable consiste à bloquer entièrement l'accès à l'application. Dans l'ensemble, les responsables informatiques du secteur des soins de santé sont très préoccupés par l'informatique de l'ombre, 63 % d'entre eux affirmant que ce phénomène interfère avec leur capacité à préserver la sécurité du cloud.

Si les établissements de soins de santé adoptent de plus en plus volontiers les services SaaS et font état d'une utilisation exclusive des services de cloud public supérieure à la moyenne, 26 % d'entre eux continuent d'utiliser uniquement des services de cloud privé, alors que 50 % 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 légèrement inférieur à la moyenne mondiale (51 % contre 52 %), et le secteur des soins de santé figure parmi les plus grands utilisateurs de conteneurs selon nos répondants. La majorité d'entre eux (76 %) 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 soins de santé est plus susceptible d'utiliser et de faire confiance aux applications SaaS que les autres secteurs. Les établissements de soins de santé se situent dans la moyenne en termes d'utilisation des clouds privés, tandis que leur taux d'adoption des clouds hybrides est parmi les plus bas. Que cela soit dû à l'utilisation du cloud public, à la valeur croissante de leurs données ou à une combinaison de ces deux facteurs, ces établissements subissent davantage de cyberattaques, d'incidents liés à un logiciel malveillant et de pertes de données que leurs homologues de la plupart des autres secteurs.

Les clouds sont désormais solidement ancrés dans le paysage informatique, et les responsables des opérations de sécurité ne doivent pas se laisser dépasser par cette adoption enthousiaste afin de protéger leur établissement. 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.

Selon le **Rapport de McAfee Labs sur le paysage des menaces – Décembre 2016**, les établissements de soins de santé et leurs dossiers médicaux de grande valeur ont attiré l'attention des cybercriminels versés dans les attaques par ransomware. Parallèlement, les professionnels de la santé adoptent activement les nouvelles technologies qui permettent d'améliorer la qualité et l'efficacité des soins dispensés aux patients. Les cybercriminels continueront de rechercher les 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.

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. 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 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