4 défis de la sécurité du nuage en 2021 et comment les affronter

ELLES NOUS RENSEIGNENT SUR CE QUE NOUS VOULONS SAVOIR EN UN COUP D'ŒIL

Il est difficile (même un peu imprudent) de tirer des conclusions sur les 18 derniers mois. Tout semble incertain, maintenant, mais une chose est sûre : de plus en plus d'entreprises passent au nuage.

Un sondage de la Cloud Security Alliance a révélé que 41 % des entreprises ont recours à des services infonuagiques contre 25 % avant la pandémie en 2019. D'ailleurs, 21 % des entreprises prévoient déplacer entre 80 % et 100 % de leur travail vers le nuage en 2021.

Cette réorganisation a inévitablement un impact sur les budgets. La majorité des répondants d'un sondage de Gartner prévoit maintenir ou augmenter leurs dépenses en solutions infonuagiques au cours des 12 prochains mois. Le PDG du fournisseur de sécurité Valtix, Douglas Murray, a affirmé : « En 2020, les dépenses consacrées aux infrastructures infonuagiques publiques ont dépassé les dépenses sur site. Le nuage est en train de prendre sa vitesse de croisière et je ne vois aucun ralentissement à l'horizon. »

La sécurité du nuage s'améliore

Un sondage mené par Coalfire en 2019 auprès d'environ 400 000 professionnels de l'informatique révélait que les deux plus grands obstacles à l'utilisation du nuage sont liés à la sécurité. La possibilité de fuites de données (54 %) et la confidentialité des données (62 %) inquiétaient les répondants. Ces résultats s'inscrivent dans la même lignée que ceux obtenus dans les recherches menées par la Cloud Security Alliance, selon lesquelles 73 % des entreprises affirment que les problèmes de sécurité freinent leurs projets.

Même s'il reste encore des défis majeurs à résoudre en matière de sécurité (on les explore plus en détail dans ce billet de blogue), il n'en reste pas moins que la sécurité du nuage est nettement plus solide et fiable aujourd'hui qu'elle ne l'était auparavant. Plusieurs facteurs expliquent cette situation :

- Les fournisseurs de services infonuagiques surveillent constamment la sécurité et effectuent des tests d'intrusion et de vulnérabilité. La plupart des entreprises, en particulier les PME, n'ont pas les moyens d'effectuer ce genre de tests. L'ancien vice-président directeur de chez Salesforce et actuel directeur de l'exploitation chez Sprinklr, Vivek Kundra, affirmait de son côté : « Les technologies infonuagiques sont souvent plus sécuritaires que les technologies informatiques traditionnelles, parce que des entreprises comme Google et Amazon ont la capacité d'attirer des professionnels en cybersécurité plus qualifiés que les agences gouvernementales. »
- Contrairement aux systèmes sur site qui reposent essentiellement sur des pare-feux, les systèmes sur le nuage déploient plusieurs couches de sécurité, dont de l'IA et de l'apprentissage profond afin de gagner en intelligence.
- Les données dans le nuage peuvent être effacées à distance en cas de vol ou de violation. D'ailleurs, la plupart des services infonuagiques possèdent des fonctionnalités de sécurité intégrées comme l'authentification basée sur les rôles et la capacité d'arrêter n'importe quelle partie d'un système à la moindre détection d'une menace.
- Le stockage des données dans le nuage peut aider à réduire la fréquence et la gravité des menaces internes. Des recherches menées par le Ponemon Institute ont révélé qu'entre 2018 et 2020, le coût mondial moyen des menaces internes a augmenté de 31 % pour atteindre 11,45 millions de dollars. La fréquence des incidents a augmenté de 47 %.

- Les systèmes infonuagiques stockent les données dans plusieurs emplacements, ce qui protège les informations contre les pannes matérielles et la corruption. D'ailleurs, les temps de récupération sont 4 fois plus rapides pour les PME qui utilisent des services infonuagiques par rapport à celles qui ne les utilisent pas.

Les défis à venir pour la sécurité du nuage

La sécurité du nuage a le potentiel d'être nettement plus robuste que les solutions sur site conventionnelles. Il reste toutefois quelques défis importants à relever pour garantir une expérience sure et rentable.

Voici donc les quatre plus grands défis de sécurité en nuage pour 2021 et comment les affronter :

1. La prévention des violations de données

Sans surprise, la prévention des violations de données est, et sera probablement toujours, le défi numéro un en matière de sécurité. Pour répondre au problème, l'ingénieur en solutions de sécurité au Software Engineering Institute (SEI) du Carnegie Mellon Institute, Donald Faatz, conseille aux entreprises d'adopter une approche intégrée incluant les aspects suivants :

- Avoir une diligence raisonnable tout au long du cycle de vie des applications et des systèmes déployés (planification, développement, déploiement, opération et mise hors service).
- Identifier et authentifier les utilisateurs, attribuer des droits d'utilisateur et instaurer des politiques de contrôle d'accès aux ressources.
- Activer l'accès aux données critiques en cas d'erreurs et de pannes.
- Éviter que des données à supprimer soient accidentellement divulguées.
- Surveiller et défendre les systèmes et les applications créés avec les services infonuagiques.
- Collaborer avec les fournisseurs de services infonuagiques pour enquêter et répondre aux incidents de sécurité potentiels, de manière conforme aux réglementations de confidentialité.

2. La conformité à la réglementation

Certaines entreprises pensent à tort qu'à l'instant où elles font le transfert vers le nuage, elles délèguent toute la responsabilité de la conformité aux fournisseurs. Ce n'est pas tout à fait ça. En réalité, les entreprises sont

toujours tenues de s'assurer que les données et les applications sont sécurisées d'une manière conforme aux réglementations en vigueur (RGPD, PCI-DSS-CCPA, etc.).

Face à ce défi, la solution la plus pratique est de vérifier que les fournisseurs respectent les normes réglementaires pertinentes. À titre d'exemple, Devolutions a obtenu l'accréditation SOC 2 ainsi que la certification ISO/IEC 27001. Nous sommes conformes à la norme PCI-DSS et utilisons un modèle de sécurité et un chiffrement de haut niveau pour protéger les données inactives ou en transit, et respectons un ensemble de pratiques de développement de logiciels sécurisés rigoureuses. Pour en savoir plus, visitez le https://devolutions.net/fr/legal/security.

3. Le manque d'expertise interne

Selon le sondage Cloud Adoption Practices & Priorities de la Cloud Security Alliance, 34 % des entreprises ne déploient pas leurs charges de travail dans le nuage par manque d'expertise à l'interne. Le problème risque d'ailleurs d'empirer dans les années à venir. Comme le rapporte Forbes : « Les compétences avancées en matière de sécurité sont recherchées plus que jamais, mais il y a un manque important de main-d'œuvre qualifiée et compétente pour soutenir l'engouement pour le progrès. »

Bien que certaines entreprises aient de plus gros budgets que d'autres pour recruter les meilleurs talents, ce n'est pas le cas pour de nombreuses PME. Travailler avec un fournisseur de services gérés peut être une solution abordable, stratégique et efficace pour combler le manque de talents à l'interne. Pour plus de conseils sur la façon de choisir le bon fournisseur, cliquez ici.

4. Les problèmes de migration vers le nuage

Les trois enjeux de sécurité liés à la migration vers le nuage les plus courants, et coûteux, auxquels font face les entreprises sont la migration trop rapide, les mauvaises configurations et les vulnérabilités des API.

Vouloir se dépêcher à accomplir une tâche est un phénomène courant, particulièrement parmi les cadres qui désirent tout migrer vers le nuage le plus rapidement possible. Les entreprises devraient, au contraire, adopter une approche « pas à pas » et hiérarchiser soigneusement les données et les applications qui doivent faire partie de leur migration. Comme le soulignait l'entreprise de cybersécurité Check Point : « Essayer de tout faire en même temps est une erreur majeure. Le processus de migration doit être séparé en plusieurs étapes afin de réduire le risque d'erreurs critiques qui pourraient corrompre les données ou entrainer des vulnérabilités. »

Pour minimiser le risque d'une mauvaise configuration, les entreprises doivent utiliser une journalisation et des rapports complets afin de détecter et de régler rapidement les problèmes. Une autre stratégie intéressante

consiste à configurer les restrictions d'accès et les autorisations pendant le processus de migration au lieu de le faire une fois qu'il est terminé et que le réseau est prêt. D'ailleurs, auditer toutes les ressources, les actifs et les paramètres est une étape très importante à faire avant la migration. En 2018, une brèche chez FedEx a rendu publics plus de 150 000 documents, incluant des données sensibles dont des passeports et des permis de conduire. Plus tard, on a découvert que le compartiment de stockage qui a déclenché la violation a été exposé avant que FedEx n'achète l'entreprise qui possédait les données auparavant. En d'autres mots, FedEx a hérité de cette vulnérabilité. Pendant plusieurs années, le risque n'avait pas été traité.

Les API non sécurisés sont à l'origine de plusieurs violations de données médiatisées, comme celles qui se sont produites récemment du côté de Venmo (grattage de masse de 200 millions de dossiers), de Facebook (qui a affecté 6,8 millions d'utilisateurs et 1 500 applications), de USPS (grattage de masse de 60 millions de dossiers), de la Fédération des industries de l'État de São Paulo (exposition des données de 130 000 entreprises) et de JustDial (exposition des données de 100 millions d'utilisateurs). C'est essentiel : les entreprises doivent s'assurer que les fournisseurs de services infonuagiques disposent d'API hautement sécurisées et mises à jour en continu. Et cela s'étend au-delà des solutions principales : ça concerne aussi les outils et modules complémentaires. Par exemple, chez Devolutions, nous avons récemment renforcé la sécurité de l'API qui intègre Remote Desktop Manager à Devolutions Web Login. Pour en savoir plus sur cette mise à jour, cliquez ici.

En direct du bureau de notre Chef de la sécurité Martin Lemay

Tout ce qui vient d'être mentionné est essentiel, mais le plus important pour la majorité des entreprises est d'avoir sous la main des experts du nuage qualifiés et expérimentés. Avec l'expertise adéquate, ces entreprises sont davantage en mesure de :

- *Prévenir les violations.*
- *Se conformer aux régulations et aux normes.*
- *Effectuer des migrations avec un minimum de risques.*

De plus, certains fournisseurs d'hébergement infonuagique offrent uniquement des déploiements de machines virtuelles. Il s'agit de systèmes exposés sur le Web sans souci de la sécurité. Ainsi, travailler avec des experts de la sécurité du nuage (il y a des différences notables avec les experts TI traditionnels) est primordial. La comparaison entre les deux groupes est que les experts de la sécurité du nuage disposent d'outils avancés, et ils sont mieux équipés et formés pour comprendre et aborder la sécurité. Ils fournissent également des directives stratégiques, et aident les entreprises à produire un meilleur rendement du capital investi sur les coûts d'exploitation tout en réduisant les risques.

Pour conclure

Un nombre grandissant d'entreprises passent au nuage. Une étude prédit que le marché mondial du nuage va se développer à un taux de croissance annuel composé (TCAC) jusqu'en 2023 pour une valeur estimée à 623 milliards de dollars. Bien qu'il y ait des récompenses et des avantages significatifs, les risques demeurent présents. Identifier et aborder les défis de la sécurité décrits plus haut contribuera pour beaucoup à un avenir prospère et sûr.