Hausse des violations de données et de la complexité des environnements cloud selon le dernier rapport Cloud Security de Thales

Le 2022 Thales Cloud Security Report, réalisé par 451 Research, une société S&P Global Market Intelligence, indique que 45% des entreprises ont fait l'objet de violations de données ou ont échoué à un audit durant les 12 derniers mois, soit une hausse de 5% par rapport à l'année précédente[1], faisant planer des préoccupations encore plus lourdes sur la protection des données sensibles contre la cybercriminalité.

Ce communiqué de presse contient des éléments multimédias. Voir le communiqué complet ici : https://www.businesswire.com/news/home/20220607005061/fr/

©Thales

Au niveau mondial, l'adoption du cloud, et plus particulièrement multicloud, reste en hausse. En 2021, les organisations du monde entier utilisaient en moyenne 110 applications SaaS[2], contre seulement huit en 2015, témoignant ainsi d'une augmentation étonnamment rapide. Une expansion notable a été observée dans l'utilisation de multiples fournisseurs IaaS, avec près des trois quarts (72%) des entreprises qui utilisent plusieurs fournisseurs IaaS, contre 57% l'année précédente. L'utilisation de multiples fournisseurs a pratiquement doublé en un an, avec une personne interrogée sur cinq (20%) indiquant utiliser trois

fournisseurs ou plus.

Malgré cette prévalence et utilisation croissante du cloud, les entreprises ont des préoccupations communes concernant la complexité grandissante de ses services, avec la majorité (51%) des professionnels IT s'accordant à dire qu'il est devenu plus complexe de gérer la confidentialité et la protection des données sur le cloud. En outre, la transition vers le cloud devient elle aussi plus compliquée, avec le pourcentage de personnes interrogées indiquant prévoir une approche « lift and shift », la plus simple des stratégies de migration, passant de 55% en 2021 à 24% actuellement.

Défis de sécurité liés à la complexité multicloud

Cette complexité croissante s'accompagne d'un besoin encore plus impérieux de disposer d'une cybersécurité solide. À la question de savoir quel pourcentage de leurs données sensibles est stocké sur le cloud, une large majorité (66%) indique entre 21 et 60%. Toutefois, seulement un quart (25%) des personnes interrogées se disent capables de classer toutes leurs données.

De plus, près d'un tiers (32%) des répondants admettent rencontrer des difficultés pour transmettre une notification de violation à une agence gouvernementale, un client, un partenaire ou aux employés. Cet aspect préoccupant devrait être traité par les entreprises disposant de données sensibles, en particulier dans les secteurs hautement réglementés.

Les cyberattaques présentent également un risque continu pour les applications et données sur le cloud. Les personnes interrogées font état d'une prévalence grandissante des attaques, avec un quart (26%) signalant une hausse des logiciels malveillants, 25% des rançongiciels et un cinquième (19%) des attaques par hameçonnage/harponnage.

Protéger les données sensibles

En ce qui concerne la sécurisation des données dans des environnements multicloud, les professionnels IT considèrent le cryptage comme un contrôle crucial pour la sécurité. La majorité des personnes interrogées citent le cryptage (59%) et la gestion des clés (52%) comme les technologies de sécurité qu'ils utilisent actuellement pour protéger leurs données sensibles sur le cloud.

Toutefois, à la question de savoir quel pourcentage de leurs données sur le cloud est encodé, seulement un dixième (11%) des personnes interrogées indiquent entre 81 et 100%. De plus, la prolifération des plateformes de gestion des clés pourrait constituer une difficulté pour les entreprises. Seulement 10% des personnes interrogées utilisent une ou deux plateforme(s), 90% en utilisent trois ou plus, et près d'une sur cinq (17%) admet utiliser huit plateformes ou plus.

L'encodage devrait être un domaine prioritaire pour les entreprises au moment de sécuriser les données sur le cloud. Dans les faits, 40% des personnes interrogées indiquent avoir pu éviter le processus de notification de violation car leurs données volées ou divulguées étaient encodées ou tokénisées, illustrant ainsi la valeur concrète des plateformes de cryptage.

En outre, il est encourageant d'observer des signes montrant que les entreprises adoptent l'approche Zero Trust et investissent en conséquence. Près d'un tiers des personnes interrogées (29%) déclare déjà exécuter une stratégie Zero Trust, un quart (27%) déclare étudier ou prévoir ce

type de stratégie, et 23% déclare en envisager une. Il s'agit là d'un résultat positif, mais il reste encore du chemin à parcourir.

Sebastien Cano, SVP Cloud Protection & Licensing, Thales*: « On ne soulignera jamais assez la complexité de la gestion d'environnements multicloud. En outre, l'importance croissante de la souveraineté des données soulève de plus en plus de questions pour les responsables de la sécurité des systèmes d'information et de la protection des données au moment d'élaborer leur stratégie, gouvernance et gestion des risques sur le cloud. Ce défi concerne non seulement le lieu où les données sensibles sont stockées, mais aussi qui a accès aux données sensibles au sein de l'organisation.*

Il existe diverses solutions, comme le cryptage et la gestion des clés. Dernier point, mais non des moindres, il sera essentiel de continuer à adopter une stratégie Zero Trust pour sécuriser ces environnements complexes, contribuant ainsi à garantir la protection de leurs données par les organisations et répondre aux futurs enjeux. »

Thales et 451 Research aborderont plus en détail ces conclusions à l'occasion d'un webinaire le 23 juin 2022. Pour y participer, veuillez visiter la page d'inscription.

À propos de l'étude Thales Global Cloud Security 2022

À l'heure où les organisations sortent des mesures d'urgence de ces deux dernières années, elles se retrouvent aux prises avec la sécurisation d'environnements plus complexes dans lesquels elles évoluent dorénavant. L'édition mondiale de l'étude Thales Cloud Security Study 2022 se penche sur divers aspects de ces impacts en s'appuyant sur une vaste enquête menée auprès de professionnels de la sécurité et de dirigeants exécutifs sur des thèmes tels que l'accélération de la transformation numérique, la migration vers le cloud, et les complexités liées à la gestion de la sécurité dans des environnements multicloud. L'étude Thales Cloud Security 2022 se base sur les données d'une enquête réalisée auprès de quasiment 2 800 professionnels de la sécurité et dirigeants exécutifs. Cette étude a été faite selon une approche observationnelle et ne formule aucun lien de causalité.

A propos de Thales

Thales (Euronext Paris: HO) est un leader mondial des hautes technologies qui investit dans les innovations du numérique et de la « deep tech » – connectivité, big data, intelligence artificielle, cybersécurité et quantique – pour construire un avenir de confiance, essentiel au développement de nos sociétés. Le Groupe propose des solutions, services et produits qui aident ses clients – entreprises, organisations, Etats – dans les domaines de la défense, de l'aéronautique, de l'espace, du transport et de l'identité et sécurité numériques, à remplir leurs missions critiques en plaçant l'humain au cœur des décisions.

Thales compte 81 000 collaborateurs dans 68 pays. En 2020, le Groupe a réalisé un chiffre d'affaires de 16,2 milliards d'euros.

VEUILLEZ VISITER

Groupe Thales

Sécurité

[1] https://cpl.thalesgroup.com/cloud-security-research

[2] https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/