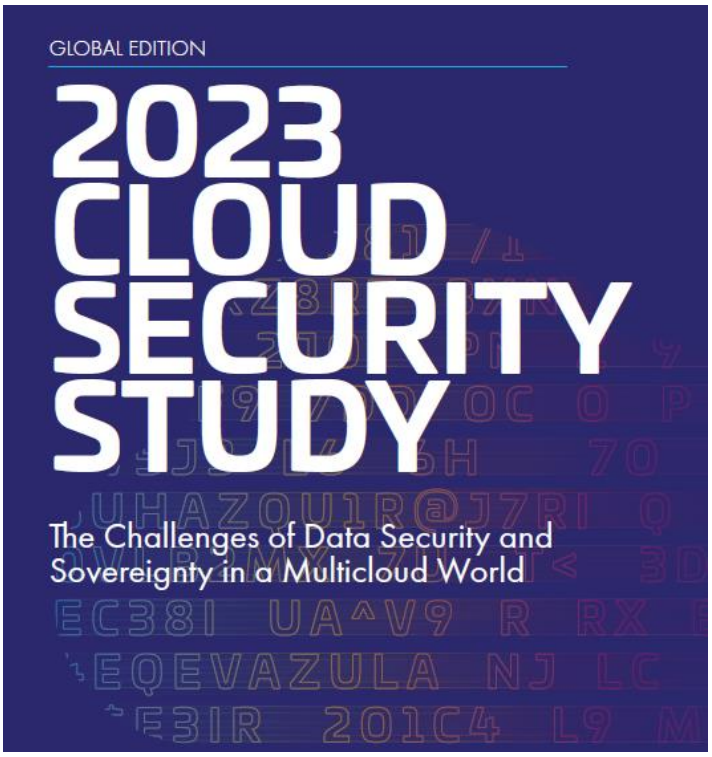
COMMUNIQUE DE PRESSE
5 Juillet 2023
Paris, La Défense, FRANCE

Alors que les violations de données se multiplient, les actifs dans le cloud deviennent les cibles principales de cyberattaques

- Depuis l'année dernière, 39 % des entreprises ont été victimes d'une violation de données dans leur environnement cloud l'année dernière, soit une hausse de 4 points par rapport à l'année précédente (35 %)
- On observe une augmentation de 26% du transfert de données stockées dans le cloud. 75 % des entreprises déclarent que plus de 40 % des données stockées dans le cloud sont des données sensibles.
- Malgré l'augmentation spectaculaire du nombre de données sensibles stockées dans le cloud, seules 45 % d'entre elles sont chiffrées en moyenne.



© Thales

C'est Thales a annoncé aujourd'hui le démarrage de l'édition 2023 de la Thales Cloud Security Study, une évaluation annuelle des toutes dernières menaces, tendances et risques émergents en matière de sécurité du cloud. Cette étude est basée sur une enquête menée auprès d'environ 3 000 professionnels de l'informatique et de la sécurité dans 18 pays.

L'étude de cette année a révélé que plus d'un tiers (39 %) des entreprises ont subi l'année dernière une violation de données dans leur environnement cloud, indiquant une hausse vis-à-vis des 35 % signalés en 2022. En outre, plus de la moitié (55 %) des personnes interrogées ont déclaré que l'erreur humaine était la principale cause des violations de données dans le cloud.

Cette augmentation intervient dans le cadre d'une hausse spectaculaire du volume de stockage de données sensibles dans le cloud. Les trois quarts (75 %) des entreprises ont déclaré que plus de 40 % des données stockées dans le cloud sont classées comme données sensibles, contre 49 % l'année dernière à la même époque.

Plus d'un tiers d'entre eux (38 %) considèrent que les applications SaaS (Software as a Service) sont la principale cible des pirates, suivies de près par le stockage dans le cloud (36 %).

L'absence de chiffrement et de contrôle des clés associées est une source de préoccupation concernant les données dans le cloud

Malgré la hausse signalée des données sensibles dans le cloud, l'étude a révélé une faiblesse des niveaux de chiffrement utilisés. Seul un cinquième (22 %) des professionnels de l'informatique ont indiqué avoir chiffré plus de 60% des données sensibles stockées sur un cloud. L'étude dévoile qu'en moyenne, seuls 45% des données sensibles sont chiffrées dans le cloud.

L'étude a également révélé une absence de contrôle des clés de chiffrement par les entreprises, puisque seulement 14 % des personnes interrogées ont déclaré qu'elles contrôlaient toutes les clés de leurs données chiffrées dans leurs environnements cloud. En outre, près des deux tiers (62 %) déclarent disposer de cinq systèmes de gestion des clés, ce qui augmente la complexité de la sécurisation des données sensibles.

Le multicloud, source de complexité opérationnelle

L'adoption du multicloud continue de progresser, avec plus de trois quarts (79 %) des organisations disposant de plus d'un fournisseur cloud.

Visiblement, l'infrastructure n'est pas la seule à connaître cette croissance. L'utilisation d'applications SaaS est également en forte hausse. En 2021, 16 % des personnes interrogées ont déclaré que leur entreprise utilisait entre 51 et 100 applications SaaS différentes, tandis qu'en 2023, ce pourcentage passera à 22 %.

Malgré l'expansion de l'utilisation du cloud, une difficulté de taille demeure. Plus de la moitié des personnes interrogées (55 %) ont déclaré que la gestion des données dans le cloud était plus complexe que dans les environnements sur site, contre 46 % l'année précédente. La souveraineté numérique est également au cœur des préoccupations des personnes interrogées. 83 % d'entre elles ont exprimé des inquiétudes concernant la souveraineté des données, et 55 % ont reconnu que la confidentialité et la conformité des données dans le cloud se sont complexifiées.

Vers une meilleure sécurité dans le cloud

La gestion des identités et des accès (IAM) est une mesure cruciale pour contenir les violations de données, soulignant ainsi l'importance de mettre en place une de sécurité solides. Il est encourageant de constater que l'adoption d'une authentification multifactorielle robuste est passée à 65 %, indiquant des progrès dans le renforcement des contrôles d'accès.

Il est curieux de constater que seules 41 % des organisations ont mis en place des modèles de sécurité à confiance nulle (zero trust / build your own trust) dans leur infrastructure cloud, et qu'un pourcentage encore plus faible (38 %) utilise ces modèles de sécurité au sein de leurs réseaux dans le cloud. Ces statistiques soulignent la nécessité de prioriser l'adoption de mesures de sécurité complètes qui parviennent à protéger efficacement les données sensibles et améliorer la résilience globale en matière de cybersécurité.

« L'étude montre que les organisations fonctionnent dans un paysage multicloud dynamique, exigeant un accès transparent et efficace à l'infrastructure et aux services informatiques à la demande », a déclaré ***Sebastien Cano, vice-président senior de la protection du cloud et des activités de concession de licences chez Thales.***

« Traiter les environnements cloud comme une extension de l'infrastructure existante tout en conservant le contrôle exclusif et la sécurité des données, en particulier des données sensibles, est la clé de la sécurité du cloud. Le contrôle des clés de chiffrement par le client est essentiel car il permet aux organisations d'exploiter l'évolutivité, la rentabilité et l'accessibilité du cloud tout en garantissant l'intégrité et la confidentialité absolues de leurs précieuses informations ».

A propos du rapport Thales Cloud Security de 2023

Le rapport Thales Cloud Security de 2023 s'appuie sur une enquête mondiale menée par S&P Global Market Intelligence et commandée par Thales auprès de 3 000 cadres supérieurs environ ayant une responsabilité ou une influence sur la sécurité informatique et la sécurité des données. Les personnes interrogées étaient originaires de 18 pays : Allemagne, Australie, Brésil, Canada, Corée du Sud, Émirats arabes unis, États-Unis, France, Hong Kong, Inde, Italie, Japon, Mexique, Nouvelle-Zélande, Pays-Bas, Royaume-Uni, Singapour et Suède.

Les organisations représentaient une vaste gamme de secteurs, avec un accent particulier sur les services de santé, les services financiers, la vente au détail, la technologie et le gouvernement fédéral. Les titres des postes allaient des cadres dirigeants (C-level), notamment le PDG, le directeur financier, le directeur des données, le RSSI, le scientifique en chef des données et le directeur des risques, aux SVP/VP, administrateurs informatiques, analystes de la sécurité, ingénieurs de la sécurité et administrateurs de systèmes. Les personnes interrogées représentaient des organisations de toutes tailles, la majorité d'entre elles comptant entre 500 et 10 000 employés. L'enquête a été menée en novembre et décembre 2022.

À propos de Thales

Thales (Euronext Paris : HO) est un leader mondial des hautes technologies dans trois domaines : défense & sécurité, aéronautique & espace, identité & sécurité numériques. Le Groupe développe des produits et solutions qui rendent le monde plus sûr, plus vert et plus inclusif.

Le Groupe investit près de 4 milliards d'euros par an dans la recherche et le développement, en particulier dans des secteurs clés comme les technologies quantiques, le Far Edge computing, la 6G et la cybersécurité.

COMMUNIQUE DE PRESSE
5 Juillet 2023
Paris, La Défense, FRANCE

Thales emploie 77 000 personnes dans 68 pays. En 2022, le Groupe a réalisé un chiffre d'affaires de 17,6 milliards d'euros.

Le texte du communiqué issu d'une traduction ne doit d'aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine. La traduction devra toujours être confrontée au texte source, qui fera jurisprudence.

CONTACT PRESSE

Thales, Media Relations
Security & Cybersecurity
Marion Bonnet
+33 (0)6 60 38 48 92
marion.bonnet@thalesgroup.com

EN SAVOIR PLUS

Thales Group

Cloud Protection & Licensing Solutions | Thales Group

Cybersecurity Solutions | Thales Group