THALES
Building a future we can all trust

COMMUNIQUÉ DE PRESSE
2 juin 2021
Paris La Défense

Thales constate une aggravation des cyberattaques en 2020 pour 47% des entreprises en télétravail

- Quatre entreprises sur cinq (82 %) se disent préoccupées par des risques de sécurité liés au télétravail, bien que plusieurs d'entre elles explorent des modèles potentiels de travail hybride
- Prêt de la moitié (47 %) font état d'une aggravation des cyberattaques en termes de nombre, de gravité et/ou de portée au cours des 12 derniers mois
- 41 % des entreprises ayant fait l'objet d'une brèche l'ont subie l'année passée. Ce chiffre a pratiquement doublé par rapport à 2019 (21%)
- Le secteur du commerce est le plus à risque. 61 % des entreprises du secteur ont subi une brèche ou un échec d'audit en 2020, suscitant ainsi des préoccupations aussi bien chez les fournisseurs que chez les consommateurs

©Thales

Après plus d'un an de télétravail et malgré une transition vers des modèles de travail hybrides à distance/au bureau, 82 % des entreprises se disent encore préoccupées par les risques de sécurité pour les employés en télétravail.

L'édition 2021 du Rapport de Thales sur les menaces mondiales pour les données, une étude réalisée par 451 Research, une société S&P Global Market Intelligence, indique une indéniable complexification de la gestion des risques de sécurité : près de la moitié (47 %) des entreprises constatent une hausse en termes de nombre, de gravité et/ou de portée des cyberattaques sur les 12 derniers mois.

Des attaques en hausse

Pour les entreprises ayant déjà subi une brèche, deux attaques sur cinq (41 %) se sont produites l'an dernier. Ce chiffre a pratiquement doublé par rapport à 2019 (21%), marquant ainsi un changement notable dans la menace posée.

Les malwares (54 %) sont la principale source d'attaques de sécurité, suivis par les rançongiciels (ransomware) (48 %) et l'hameçonnage (phishing) (41 %). Quelle que soit le type d'attaque, le

message est clair quant au mode opératoire des attaques : les menaces internes et les erreurs humaines restent la principale porte d'entrée des cybercriminels. Un tiers des entreprises a déclaré que les activités malveillantes en interne (35 %) et les erreurs humaines (31 %) représentent les risques les plus importants, suivis par les attaques externes (22 %).

Avec des risques de sécurité en explosion en raison du télétravail, près de la moitié (46 %) des entreprises reconnaissent que leur infrastructure de sécurité n'était pas prête pour traiter l'aggravation des risques entrainée par la Covid-19. Dans les faits, seulement une organisation sur cinq (20 %) estime avoir été préparée à cette tendance à la hausse.

Une multitude de secteurs à risque

Cette protection insuffisante semble frapper plus durement certains secteurs : un peu moins de deux tiers (61 %) des détaillants interrogés ont subi une brèche ou un échec d'audit impliquant des données ou des applications stockées sur le cloud durant l'année écoulée. C'est le pourcentage le plus élevé parmi les secteurs évalués. Plus de la moitié des organisations dans les secteurs juridique (57 %), des centres d'appels (55 %), des transports (54 %) et des télécommunications (52 %) ont connu les mêmes problèmes au cours des 12 derniers mois.

La complexité des environnements multi-cloud augmente les risques

Alors que le nombre d'attaques continue d'augmenter, les entreprises se tournent vers le cloud pour stocker leurs données dans un monde numérisé. La moitié d'entre elles (50 %) indiquent que plus de 40 % de leurs données sont stockées sur des environnements cloud externes mais seules 17 % ont chiffré la moitié ou plus de leurs données sensibles dans le cloud. La complexité liée à l'approche multi-cloud n'aide pas la sécurisation des données : de nombreux répondants (45 %) utilisent actuellement au moins deux fournisseurs de PaaS (plateforme en tant que service) et/ou deux fournisseurs d'IaaS (infrastructure en tant que service). Un quart (27 %) des entreprises utilise actuellement plus de 50 applications SaaS (logiciel en tant que service).

***Sebastien Cano, Vice-président pour les activités Coud Protection & Licensing chez Thales, déclare** : « Des équipes du monde entier ont été confrontées à d'immenses défis de sécurité l'an passé, tandis que les entreprises ont accéléré leur transformation numérique et leurs initiatives d'adoption du cloud. Au moment de migrer vers des solutions multi-cloud, la complexité liée à la gestion des données peut rapidement entraîner une perte de contrôle. Les organisations risquent non seulement de ne plus savoir où sont stockées leurs données au sein d'environnements de cloud multiples, mais aussi de ne pas parvenir à protéger leurs données sensibles dans le cloud. Avec des quantités record de données stockées et utilisées dans le cloud, il est crucial pour les entreprises de déployer une stratégie de sécurité éprouvée et s'appuyant sur la découverte, la protection et le contrôle des données. »*

Feuille de route et défis à venir

Les entreprises ont pris conscience des défis qui les attendent et tentent de les relever avec des stratégies Zero Trust. Plus de trois quarts (76 %) des stratégies dans le cloud des répondants reposent dans une certaine mesure sur une sécurité de type Zero Trust. Près de la moitié (44 %) des répondants ont retenu un accès réseau Zero Trust (ZTNA)/un périmètre défini par logiciel (SDP) comme priorité d'investissement technologique durant la pandémie, suivi par la gestion des accès basée sur le cloud (42 %) et l'accès conditionnel (41 %). Près d'un tiers (30 %) des répondants indique disposer d'une

véritable stratégie Zero Trust et, fait intéressant, les entreprises l'ayant déployée sont moins nombreuses à avoir signalé une brèche dans leurs données.

Toutefois, malgré les initiatives prises par les entreprises pour contrecarrer les menaces actuelles, les défis des années à venir continuent d'inquiéter : 85 % des répondants se disent préoccupés par les menaces liées à l'informatique quantique, un risque sans doute exacerbé par la complexité grandissante des environnements cloud.

Eric Hanselman, analyste en chef chez 451 Research, une société S&P Global Market Intelligence, ajoute : *« Les contrôles natifs et les protections disponibles sur les environnements cloud couvrent un ensemble de capacités de base, mais s'avèrent bien souvent insuffisants au moment de fournir des protections efficaces pour les données et les charges de travail sensibles, en particulier dans le domaine de la conformité réglementaire, comme le RGPD et les ramifications du règlement Schrems II. Les organisations doivent avoir recours au chiffrement et s'assurer de tirer pleinement parti des avantages qui en découlent, en contrôlant les clés qui protègent leurs données via des approches BYOK (Bring Your Own Key), HYOK (Hold Your Own Key) ou BYOE (Bring Your Own Encryption). Les organisations doivent également effectuer des changements internes pour garantir que leur personnel comprenne, à tous les niveaux, les défis liés à la sécurité, et pour ajuster leurs priorités d'investissement en conséquence. Les équipes de direction doivent acquérir une compréhension plus globale des diverses strates de risques et d'attaques auxquels le personnel de première ligne est confronté. »*

Thales et 451 Research présenteront plus en détail les conclusions du rapport durant le prochain Crypto Summit organisé par Thales le 16 juin 2021 prochain. Pour y participer, rendez-vous sur la page d'inscription.

À propos du rapport 2021 de Thales sur les menaces mondiales pour les données

Le rapport 2021 de Thales sur les menaces mondiales pour les données s'appuie sur une étude de 451 Research mandatée par Thales et réalisée auprès de plus de 2 600 dirigeants ayant des responsabilités directes ou indirectes en matière de sécurité informatique ou des données. Les répondants proviennent de 16 pays : Allemagne, Australie, Brésil, Corée du Sud, Émirats arabes unis, États-Unis, France, Hong Kong, Inde, Japon, Mexique, Nouvelle-Zélande, Pays-Bas, Royaume-Uni, Singapour et Suède. Les organisations ont représenté un éventail d'industries, avec un accent mis sur les soins de santé, les services financiers, le commerce, la technologie et les gouvernements fédéraux. Les fonctions occupées allaient de postes de direction (PDG, directeur financier, responsable des données, RSSI, scientifique des données et responsable de la gestion des risques) à celles de VP principal/VP, administrateur TI, analyste de la sécurité, ingénieur de la sécurité et administrateur de systèmes. Les répondants ont représenté des organisations de tailles variées, la majorité d'entre elles ayant entre 500 et 10 000 employés. L'étude a été menée en janvier et février 2021.

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 17 milliards d'euros.

CONTACT PRESSE

Thales, Relations médias
Sécurité
Constance Arnoux
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

EN SAVOIR PLUS

Thales Group
Identité & Sécurité numériques
Télécharger les photos

@Thalesgroup