COHESITY

Rapport 2022 sur l'état de la sécurité et de la gestion des données

En bref

Le premier **rapport annuel sur l'état de la sécurité et de la gestion des données** repose sur une enquête menée en 2022 par Censuswide auprès de plus de 2 000 décideurs des domaines de l'informatique et de la sécurité (répartis presque à parts égales entre les deux groupes), dans des entreprises des États-Unis, du Royaume-Uni, d'Australie et de Nouvelle-Zélande.

L'enquête a révélé que les attaques par ransomware se multiplient dans le monde entier. Près de la moitié des personnes interrogées ont en effet déclaré que leur entreprise avait été touchée au cours des six derniers mois. Il est apparu que les stratégies de sécurité présentaient deux lacunes importantes qui mettaient les entreprises en danger.

- Les entreprises qui dépendent d'une infrastructure de sauvegarde et de récupération obsolète et ancienne pour gérer et protéger leurs données ne sont pas prêtes à faire face aux cyberattaques sophistiquées qui les frappent dans le monde entier.
- Le manque de collaboration entre les équipes informatiques et de sécurité rend les entreprises vulnérables aux cyberattaques et risque de compromettre la sécurité des données.

VOICI D'AUTRES FAITS MARQUANTS :

La dépendance envers les technologies traditionnelles affaiblit la capacité de réponse des entreprises aux ransomwares. Près de la moitié (46 %) des personnes interrogées ont déclaré que leur entreprise s'appuyait sur une infrastructure primaire de sauvegarde et de récupération conçue au minimum en 2010. À la question de savoir quels étaient les principaux obstacles à la reprise des activités après une attaque par ransomware réussie, 34 % des personnes interrogées ont répondu l'absence d'un système automatisé de reprise après sinistre, et 32 % des systèmes de sauvegarde et de récupération obsolètes.

Moderniser les capacités de gestion, de protection et de récupération des données permet de renforcer les postures de sécurité et les opérations multi-cloud. Voici les quatre mesures « incontournables » que les personnes interrogées demanderaient à leur direction en 2022 :

- Intégration entre les plateformes modernes de gestion et de sécurité des données, et alertes alimentées par l'IA en cas d'accès anormal aux données afin de signaler rapidement les attaques en cours (34 %)
- Plateforme extensible aux applications tierces pour les opérations de sécurité et la réponse aux incidents (33 %)
- Reprise après sinistre automatisée des systèmes et des données (33 %)
- Mise à niveau des systèmes de sauvegarde et de récupération existants (32 %)

Partager la responsabilité de la sécurité. Plus de quatre personnes interrogées sur cinq (81 %) sont plutôt ou tout à fait d'accord pour dire que les équipes informatiques et de sécurité devraient partager la responsabilité de la stratégie de sécurité des données de leur entreprise. Et bien que la menace des cyberattaques ait augmenté, le niveau de collaboration est resté le même.

La pénurie actuelle de talents techniques complique la situation. À la question de savoir si la pénurie de talents affectait la collaboration entre les équipes informatiques et de sécurité, 78 % des personnes interrogées ont répondu par l'affirmative.

Lisez le rapport complet pour en savoir plus sur les résultats et l'analyse de l'enquête, et pour découvrir comment les autres entreprises préviennent une attaque par ransomware et/ou s'en remettent.

Lire le rapport