www.informationweek.com /cyber-resilience/data-breaches-just-keep-piling-up

Les violations de données ne cessent de s'accumuler

Un nouveau rapport d'Apple indique que le nombre de violations de données a plus que triplé entre 2013 et 2022.

Carrie Pallardy :

Les violations de MOVEit et de GoAnywhere et une autre violation de T-Mobile ont fait la une des journaux cette année, mais ces incidents n'étaient que quelques-uns parmi tant d'autres en 2023.
Si vous avez l'impression que vous pouvez difficilement passer une journée sans voir des nouvelles d'une autre violation de données, ce n'est pas seulement votre imagination.
Les violations de données ont connu une augmentation fulgurante au cours de la dernière décennie.

Apple a commandé une étude indépendante pour se pencher sur les chiffres et les raisons derrière les milliards d'enregistrements qui ont été piratés au cours des deux dernières années.
Compte tenu de l'énorme quantité de données générées et des acteurs malveillants motivés, le nombre stupéfiant de violations sera-t-il tout simplement inévitable ?

Des milliards d'enregistrements

L'étude d'Apple, menée par Stuart Madnick, Ph.D., professeur au Massachusetts Institute of Technology, indique que plus de 2,6 milliards de dossiers personnels ont été piratés en 2021 et 2022.
Et cette tendance ne montre aucun signe de ralentissement.
Au cours des neuf premiers mois de cette année, le nombre de violations de données aux États-Unis a bondi de 20 % par rapport à l'ensemble de l'année 2022.

Il convient de noter que la quantité de données personnelles que les entreprises collectent et stockent a augmenté de manière exponentielle ces dernières années, et qu'il est peu probable qu'elle ralentisse compte tenu de la valeur de l'accès à des trésors de données.

« Les entreprises traitent de plus en plus d'informations personnelles, tant en interne que par l'intermédiaire de tiers.
Plus il y a d'informations personnelles qui sont traitées et/ou partagées avec des fournisseurs de services ou des tiers, plus elles amplifient le risque potentiel dans lequel les données peuvent être compromises », a déclaré Erin Illman, associée et avocate spécialisée dans la protection de la vie privée au cabinet d'avocats national Bradley, dans une interview par courriel.

À lire aussi :Questions de sécurité à poser après la violation de ZeroedIn

L'endroit où ces données sont stockées est un facteur important lors de l'évaluation des tendances en matière de violation.
Au total, 82 % des violations concernaient des données stockées dans le cloud : public, privé ou dans plusieurs environnements différents, selon le rapport sur le coût d'une violation de données 2023 d'IBM Security.

La migration vers le cloud a eu des avantages évidents, mais les acteurs de la menace sont clairement attentifs et capitalisent sur les vulnérabilités.
Sourya Biswas, directeur technique de la gestion des risques et de la gouvernance au sein du cabinet de conseil en sécurité NCC Group, souligne que les fournisseurs de services cloud fonctionnent selon un modèle de responsabilité partagée.
« Les fournisseurs de cloud sont responsables de la sécurité du cloud et les clients sont responsables de la sécurité dans le cloud », explique-t-il.

Les mauvaises configurations du cloud peuvent entraîner d'importantes violations de données.
Cette année, Microsoft AI a accidentellement exposé 38 téraoctets d'informations sensibles en raison d'une mauvaise configuration du cloud, selon TechCrunch.

À lire également :Limiter les dommages : remédier à l'atteinte à la réputation après une violation de données

La surface d'attaque augmente en grande partie en raison de la nature interconnectée de l'entreprise et de la technologie.
La plupart des organisations utilisent une variété de fournisseurs tiers pour fonctionner, et toute vulnérabilité et violation qui en résulte chez ces fournisseurs peut avoir un effet d'entraînement.
Presque toutes les entreprises (98 %) travaillent avec un fournisseur qui a fait l'objet d'une violation au cours des deux dernières années, selon le rapport d'Apple.

L'externalisation est souvent nécessaire, mais cela signifie que les organisations n'ont pas le contrôle total de leur sécurité.
Même si une organisation fait preuve de diligence raisonnable à l'égard d'un fournisseur, cela signifie-t-il que ce dernier maintient ses pratiques de sécurité ?
« Une fois que vous travaillez avec un fournisseur, il n'y a aucune garantie que ces pratiques de sécurité sont toujours respectées, à moins que vous ne disposiez d'un processus de surveillance très rigoureux », explique M. Biswas.

Les données personnelles sont précieuses pour les auteurs de menaces, et ils continuent de cibler les organisations qui protègent ces informations par le biais d'attaques par rançongiciel.
Plus tôt cette année, les attaques par ransomware étaient en baisse, mais il semble qu'il s'agisse d'une accalmie temporaire.
Le rapport d'Apple note que les attaques par ransomware ont bondi de 70 % au cours des trois premiers trimestres de cette année par rapport aux trois premières années de 2022.

Les groupes de rançongiciels sont de plus en plus organisés et ciblent les organisations qui stockent des informations sensibles dans le but d'obtenir des gains financiers.

À lire également :La FTC exigera davantage de signalements de violations de données et un plan de sécurité

« Vraiment, c'est trompeur de les appeler des groupes.
Ce sont des entreprises entreprenantes qui disposent de ressources suffisantes, qui disposent de chaînes d'approvisionnement entières de tiers (tels que des courtiers d'accès initial et des fournisseurs de négociation de ransomwares) et qui réussissent à générer des bénéfices », a déclaré Heather Gantt-Evans, RSSI de la société d'émission de cartes et de solutions de paiement Marqeta, à InformationWeek par courriel.
« Il n'est pas surprenant que ce modèle d'affaires réussi soit reproduit.

Impact individuel

Avec des milliards de dossiers personnels exposés, il peut être facile d'oublier qu'une violation de données, en particulier une violation impliquant des informations sensibles, peut causer un préjudice individuel.
Les informations compromises peuvent avoir des conséquences qui ont un impact sur les finances, la vie privée et la sécurité personnelle d'une personne.

Plus tôt cette année, des pirates informatiques ont volé et divulgué des données de la société de tests génétiques 23andMe, affirmant qu'ils avaient rassemblé une liste de personnes d'origine juive ashkénaze.
D'autres informations ont été révélées et les pirates ont accédé aux informations personnelles d'environ 5,5 millions de personnes, selon TechCrunch.

Le rapport d'Apple a également fait état d'une violation des écoles publiques de Minneapolis en mars.
L'atteinte à la vie privée a révélé plus de 300 000 fichiers sensibles, qui comprenaient des informations incroyablement privées sur les agressions sexuelles, la vie familiale abusive et la santé mentale.

Les individus peuvent avoir le contrôle sur les renseignements personnels qu'ils partagent dans certaines circonstances, mais souvent ils ne le font pas.

Les gens ont besoin de recevoir des soins de santé, par exemple, et ils doivent partager des données sensibles qui ont le potentiel d'être balayées par une violation.

Protection des données

La prolifération des données, les acteurs malveillants motivés qui cherchent à exploiter les vulnérabilités et une surface d'attaque tentaculaire font de la protection des données un défi.
Mais il existe des moyens pour les défenseurs d'évoluer et de réduire le nombre de violations.

Par exemple, les entreprises peuvent évaluer leurs politiques de sécurité du cloud afin d'empêcher le déploiement et l'exploitation ultérieure d'erreurs de configuration.
En outre, le rapport d'Apple souligne l'importance du chiffrement de bout en bout pour améliorer la sécurité des données dans le cloud.

« En plus de chiffrer les données au repos et en mouvement, il existe des solutions émergentes qui fournissent un stockage décentralisé de données fragmentées et chiffrées qui n'ont aucune valeur pour les attaquants, mais qui sont automatiquement réassemblées lorsque les utilisateurs autorisés l'exigent », explique M. Gantt-Evans.

Les solutions émergentes comme celles-ci peuvent être des outils puissants, mais la protection efficace des données nécessite une approche holistique qui englobe non seulement les solutions techniques, mais aussi la formation, la réponse aux incidents et l'adhésion de toutes les parties prenantes.

« Afin de mettre en œuvre avec succès les mécanismes nécessaires pour ...
La protection des données, l'éducation des décideurs et le soutien aux initiatives de conformité doivent être abordés au sommet de l'organisation avec des processus de mise en œuvre clairs dans l'ensemble de l'entreprise », explique M. Illman.

À propos de l'auteur (s)

Journaliste collaborateur

Carrie Pallardy est une rédactrice et rédactrice indépendante qui vit à Chicago.
Elle écrit et édite dans divers secteurs, notamment la cybersécurité, les soins de santé et les finances personnelles.

Recherche et mise en page par:
Michel Cloutier
CIVBDL

20231215

"C'est ensemble qu'on avance"