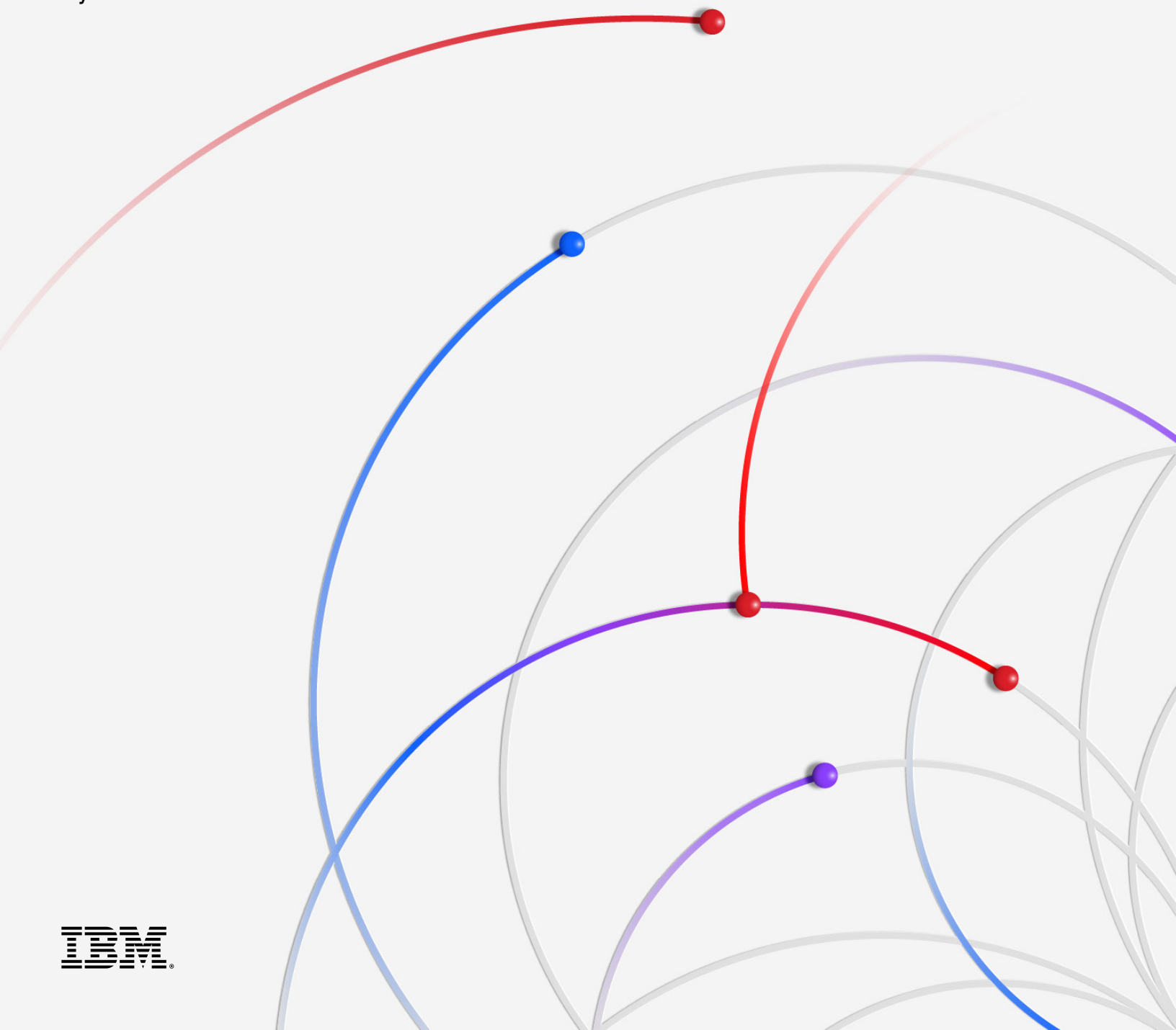
Rapport sur le coût d'une violation de données 2024

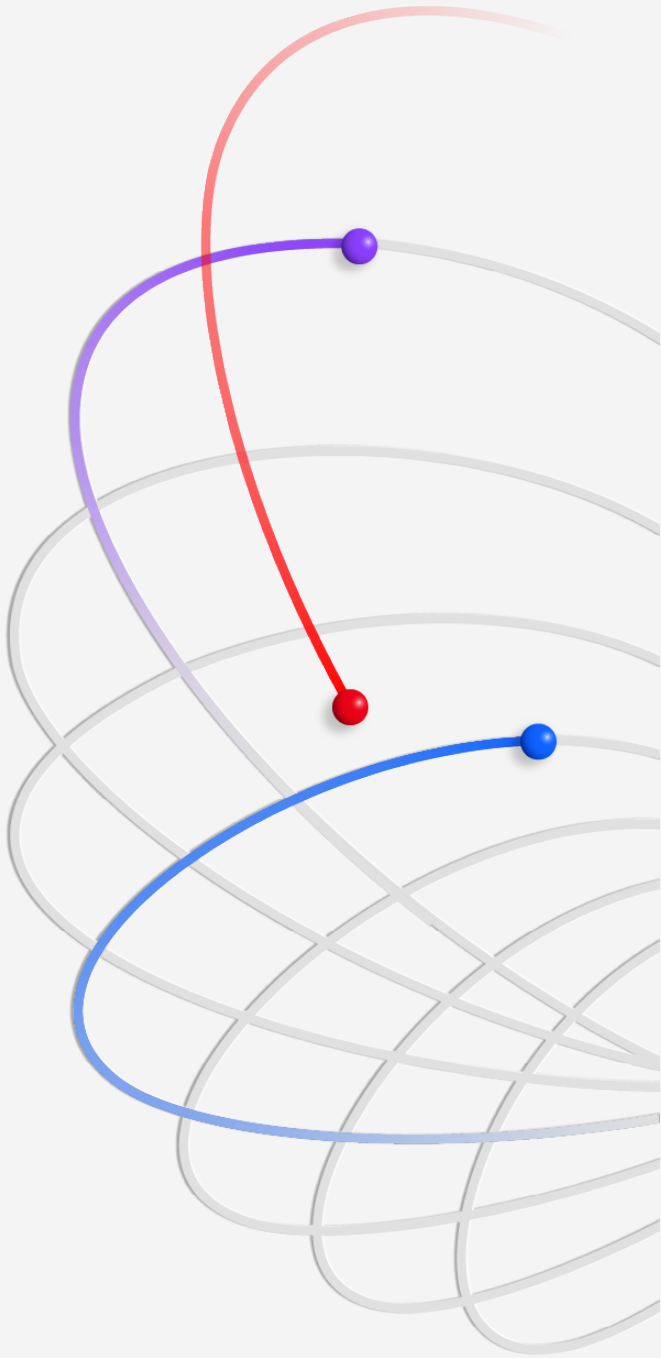
Synthèse



IBM

Table des matières

Synthèse



Le rapport IBM sur le coût d'une violation de données fournit aux responsables informatiques, de la gestion des risques et de la sécurité des données quantifiables et opportunes pour les guider dans leur prise de décision stratégique. Il les aide également à améliorer la gestion de leurs profils de risque et de leurs investissements en matière de sécurité. Cette 19e édition du rapport reflète les changements causés par les évolutions technologiques telles que l'essor des données cachées, qui font référence aux données résidant dans des sources de données non gérées, et l'ampleur et les coûts associés à la perturbation des activités découlant d'une violation de données.

L'étude a été réalisée de manière indépendante par le Ponemon Institute et commanditée, analysée et publiée par IBM. Elle porte sur 604 organisations victimes de violations de données survenues entre mars 2023 et février 2024. Les chercheurs se sont concentrés sur des organisations opérant dans 17 secteurs, dans 16 pays et régions, et sur des violations ayant compromis 2 100 à 113 000 enregistrements. Afin d'obtenir des informations sur le terrain, les chercheurs du Ponemon Institute ont interrogé 3 556 dirigeants et responsables de la sécurité en lien direct avec les incidents de violation de données au sein de leur organisation.

Les conclusions de l'étude ont été compilées dans un rapport de référence sur lequel les dirigeants et les responsables de la sécurité peuvent s'appuyer pour renforcer leurs défenses de sécurité et stimuler l'innovation, en particulier concernant l'adoption de l'IA dans la sécurité et de la sécurité pour leurs initiatives d'IA générative.

Le rapport de cette année est marqué par deux évolutions majeures. Tout d'abord, le coût moyen mondial d'une violation de données a augmenté de 10 % par rapport à l'année précédente, atteignant 4,88 millions de dollars USD, soit la plus forte hausse depuis la pandémie. Cette flambée des coûts s'explique par l'interruption des activités et par le support client et la résolution post-violation. Interrogées sur la gestion de ces coûts, plus de la moitié des organisations ont déclaré les répercuter sur les clients. Demander aux clients d'absorber ces coûts peut s'avérer problématique dans un marché concurrentiel déjà confronté aux pressions tarifaires imposées par l'inflation.

Deuxièmement, côté défenseurs, les chercheurs ont également constaté des bénéfices liés à l'application de la sécurité basée sur l'IA et de l'automatisation, qui a permis de réduire les coûts des violations de 2,2 millions de dollars USD en moyenne dans certains cas. Les solutions d'IA et d'automatisation réduisent la durée de vie nécessaire à l'identification et à l'endiguement d'une violation et des dommages qui en résultent. En d'autres termes, les défenseurs n'exploitant ni l'IA ni l'automatisation sont susceptibles d'avoir besoin de plus de temps pour détecter et contenir une violation, et risquent de voir les coûts s'envoler par rapport à ceux qui utilisent ces solutions.

Nous l'avons vu, les équipes de cybersécurité de tous les secteurs sont constamment en sous-effectif. L'étude de cette année a révélé que plus de la moitié des organisations victimes de violations étaient confrontées à de graves pénuries de personnel de sécurité, un déficit de compétences qui a été multiplié par deux chiffres par rapport à l'année précédente. Ce manque de personnel de sécurité formé s'accroît à mesure que le contexte des menaces s'élargit. La course continue pour adopter l'IA générative dans presque toutes les fonctions organisationnelles devrait entraîner des risques sans précédent et mettre davantage de pression sur ces équipes de cybersécurité.

Ce rapport fournit des informations et des recommandations issues de l'étude pour vous aider à réduire les dommages financiers potentiels et les atteintes à la réputation dont pourrait souffrir votre entreprise après une violation de données.

Nouveautés du rapport pour 2024

Chaque année, nous continuons à faire évoluer le rapport sur le coût d'une violation de données pour refléter les nouvelles technologies, les tactiques émergentes et les événements récents. Cette année, le rapport explore pour la première fois les éléments suivants :

- Si les organisations ont connu une perturbation opérationnelle à long terme, par exemple, l'incapacité de traiter les commandes client, un arrêt complet des installations de production, un service client inefficace ;
- Si la violation a touché des données issues de sources de données non gérées, également appelées données cachées ;
- Dans quelle mesure les organisations utilisent l'IA et l'automatisation dans chacun des quatre domaines d'opérations de sécurité : prévention, détection, examen et réponse ;
- La nature des attaques d'extorsion, par exemple, extorsion et ransomware ou extorsion et exfiltration de données uniquement ;
- Le temps nécessaire pour restaurer les données, les systèmes ou les services à leur état pré-violation ;
- Le temps nécessaire aux organisations pour signaler la violation lorsqu'elles étaient dans l'obligation de le faire ;
- Si les organisations qui ont impliqué les forces de l'ordre à la suite d'une attaque par ransomware ont payé la rançon.

Principales conclusions

Les principales conclusions présentées ici sont basées sur l'analyse réalisée par IBM à partir des données compilées par le Ponemon Institute.

4,88 millions de dollars US

Coût total moyen d'une violation
Le coût moyen d'une violation de données est passé de 4,45 millions de dollars US en 2023 à 4,88 millions de dollars US, soit un pic de 10 % et la plus forte hausse depuis la pandémie. Celle-ci s'explique par l'augmentation du coût lié à la perte d'activité, comprenant les temps d'arrêt opérationnels et la perte de clients, ainsi que par celle du coût des interventions en réponse aux violations, comme le recrutement de personnel pour le centre d'assistance du service client et le paiement d'amendes réglementaires plus élevées. Au total, ces coûts s'élèvent à 2,8 millions de dollars US, le montant cumulé le plus important de ces six dernières années lié à la perte d'activité et aux activités post-violation.

2,2 millions de dollars US

Économies réalisées grâce à l'utilisation intensive de l'IA dans la prévention
Deux tiers des organisations interrogées ont déclaré déployer l'IA et l'automatisation de sécurité dans leur centre d'opérations de sécurité, soit un bond de 10 % par rapport à l'année précédente. Les organisations ayant déployé à grande échelle les workflows de prévention (gestion de la surface d'attaque (ASM), red-teaming et gestion de la posture) ont en moyenne réduit de 2,2 millions de dollars US les coûts des violations par rapport à celles dont le même workflow n'utilise pas l'IA. Il s'agit là de la plus grande économie de coûts révélée dans le rapport 2024.

26,2 %

Augmentation du déficit de cyber compétences
Plus de la moitié des organisations victimes de violations sont confrontées à des niveaux élevés de pénurie de personnel de sécurité. Ce problème a connu une hausse de 26,2 % par rapport à l'année précédente, une situation qui correspond à une augmentation moyenne de 1,76 million de dollars US des coûts de violation. Bien qu'une organisation sur cinq déclare avoir utilisé une forme d'outils de sécurité d'IA générative (censés aider à pallier la pénurie en boostant la productivité et l'efficacité), ce déficit de compétences reste problématique.

1 sur 3

Part des violations impliquant des données cachées
35 % des violations ont impliqué des données cachées, montrant que la prolifération des données complexifie le suivi et la protection. Le vol de données cachées a été corrélé à une augmentation de 16 % du coût d'une violation. Les chercheurs ont constaté que le stockage de données dans plusieurs environnements était une stratégie de stockage courante, représentant 40 % des violations. Il a également fallu plus de temps pour identifier et contenir ces violations. En revanche, les données stockées dans un seul type d'environnement ont été moins souvent victimes de violations, que cet environnement soit un cloud public (25 %), sur site (20 %) ou un cloud privé (15 %).

4,99 millions de dollars US

Coût moyen d'une attaque par initié malveillant
Par rapport à d'autres vecteurs, les attaques par initié malveillant ont entraîné les coûts les plus élevés, avec une moyenne de 4,99 millions de dollars US. Parmi les autres vecteurs d'attaque coûteux figurent la compromission des adresses e-mail professionnelles, le phishing, l'ingénierie sociale et le vol ou la compromission d'identifiants. L'IA générative est susceptible d'être impliquée dans la création de certaines de ces attaques de phishing. Par exemple, l'IA générative facilite même plus que jamais la rédaction de messages de phishing grammaticalement corrects et plausibles par des non-anglophones.

46 %

Part des violations impliquant des données personnelles de clients
Près de la moitié des violations ont impliqué des informations personnelles identifiables (PII) de clients, qui peuvent inclure des numéros d'identification fiscale , des adresses e-mail, des numéros de téléphone et des adresses personnelles. Les enregistrements de propriété intellectuelle arrivent en deuxième position (43 % des violations). Le coût lié aux enregistrements de propriété intellectuelle a considérablement augmenté par rapport à l'année dernière, passant de 156 dollars US par enregistrement dans le rapport de l'année dernière à 173 dollars US par enregistrement dans celui de cette année.

1 M $

Économies réalisées lorsque les forces de l'ordre sont impliquées dans des attaques par ransomware
Les deux tiers des organisations ayant subi des attaques par ransomware et fait appel aux forces de l'ordre n'ont pas payé la rançon. Ces organisations ont également fini par réduire le coût de l'attaque de près d'un million de dollars US en moyenne, en excluant le coût de toute rançon payée. La participation des forces de l'ordre a également permis de réduire le temps nécessaire pour identifier et contenir les violations de 297 à 281 jours.

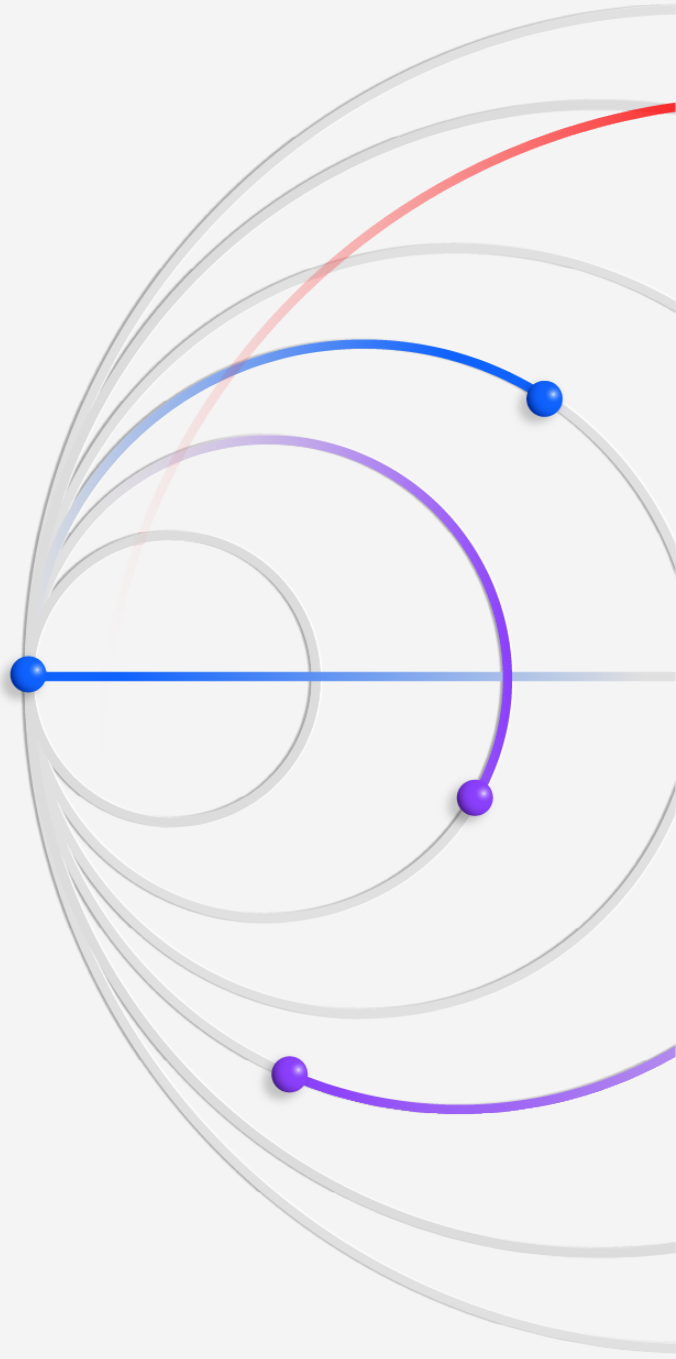
292

Jours pour identifier et contenir les violations impliquant le vol d'identifiants
Les violations impliquant le vol ou la compromission d'identifiants sont celles ayant nécessité le plus de temps pour être identifiées et contenues (292 jours) de tous les vecteurs d'attaque. Des attaques similaires menées en profitant d'employés et de l'accès des employés ont également nécessité un temps considérable pour être résolues. Par exemple, les attaques de phishing ont duré en moyenne 261 jours, tandis que les attaques d'ingénierie sociale ont duré en moyenne 257 jours.

830 000 dollars US

Plus forte augmentation moyenne des coûts parmi tous les secteurs
Le secteur industriel a connu l'augmentation la plus coûteuse de tous les secteurs, avec une augmentation moyenne de 830 000 dollars US par violation par rapport à l'année dernière. Cette flambée des coûts pourrait signaler aux organisations industrielles le besoin de se préparer à intervenir plus rapidement, car les entreprises de ce secteur sont très sensibles aux temps d'arrêt opérationnels. Pourtant, le temps nécessaire à l'identification et à l'endiguement d'une violation de données dans les organisations industrielles était supérieur aux secteurs médians, avec 199 jours pour identifier les violations et 73 jours pour les contenir.

Recommandations pour aider à réduire le coût d'une violation de données



Nos recommandations comprennent des approches de sécurité gagnantes associées à une réduction des coûts d'identification et d'endiguement des violations.

Comprendre son environnement informatique

La plupart des organisations distribuent les données dans plusieurs environnements, y compris les référentiels de données sur site, les clouds privés et les clouds publics. Cependant, bon nombre d'entre elles disposent d'inventaires de données incomplets ou obsolètes, ce qui retarde les efforts visant à découvrir les données ciblées par les violations ainsi que leur degré de sensibilité ou de confidentialité. Ces retards peuvent compliquer l'intervention et augmenter le coût de la violation.

Les équipes de sécurité doivent s'assurer de disposer d'une visibilité complète sur tous ces environnements, afin de pouvoir surveiller et protéger les données en permanence, quel que soit leur emplacement. Les organisations peuvent appliquer la gestion de la posture de sécurité des données (DSPM) et d'autres solutions, telles que la gestion des identités et des accès et la gestion de la surface d'attaque, dans tous ces environnements pour garantir la cohérence et l'exhaustivité de leur protection.

Les équipes de sécurité doivent accorder une attention particulière aux environnements hybrides et aux clouds publics. 40 % des violations de données ont impliqué des données stockées dans plusieurs environnements. En outre, lorsque les données violées étaient stockées dans des clouds publics, leur violation entraînait le coût moyen le plus élevé avec 5,17 millions de dollars US. Les équipes de sécurité doivent impérativement mieux comprendre les risques et les contrôles spécifiques à chaque service cloud qu'elles utilisent.

La gestion des données sur différents environnements est davantage compliquée par l'impact des données non gérées. Plus d'un tiers des violations de données impliquent des données cachées. Les équipes de sécurité doivent désormais partir du principe que leur organisation dispose de sources de données non gérées. Les données non chiffrées, notamment celles liées aux workloads d'IA, exacerbent encore le risque. Les stratégies de chiffrement des données doivent tenir compte du type des données, de leur utilisation et de leur emplacement afin de réduire les risques en cas de violation.

Renforcer les stratégies de prévention grâce à l'IA et à l'automatisation

L'adoption de modèles d'IA générative et d'applications tierces dans l'ensemble de l'organisation, ainsi que l'utilisation continue d'appareils de l'Internet des objets (IdO) et d'applications SaaS, étendent la surface d'attaque et contribuent à exercer une forte pression sur les équipes de sécurité.

L'application de l'IA et de l'automatisation pour soutenir les stratégies de prévention de la sécurité, y compris dans les domaines de l'ASM, du red-teaming et de la gestion de la posture, peut souvent être prise en charge par les services de sécurité gérés. L'étude de cette année révèle que les organisations ayant constaté le plus grand impact de leurs investissements dans l'IA sont celles qui ont appliqué l'IA et l'automatisation à la prévention de la sécurité par rapport à trois autres domaines de sécurité : détection, examen et intervention. Elles ont économisé en moyenne 2,22 millions de dollars US par rapport aux organisations n'ayant pas déployé l'IA dans les technologies de prévention.

Adopter une approche de l'adoption de l'IA générative axée sur la sécurité

Alors que les organisations adoptent rapidement l'IA générative, seuls 24 % des projets d'IA générative sont sécurisés. Le manque de sécurité menace d'exposer les données et les modèles de données à des violations, risquant ainsi de compromettre les avantages que de tels projets sont censés offrir.

À mesure que l'adoption de l'IA générative se répand, les organisations ont besoin d'un cadre d'exigences destiné à sécuriser les données, les modèles et l'utilisation de l'IA générative, ainsi qu'à établir des contrôles de gouvernance de l'IA. Il leur faudra sécuriser les données d'entraînement en les protégeant contre les vols et la manipulation. Les organisations peuvent associer découverte et classification des données pour identifier les données sensibles utilisées pour l'entraînement ou le réglage fin. Elles peuvent également mettre en place des contrôles de sécurité des données pour le chiffrement, la gestion des accès et le contrôle de la conformité.

Avec l'IA générative, les organisations sont confrontées au risque lié aux données cachées et à leur croissance, mais aussi aux modèles cachés. Elles doivent ainsi étendre la gestion de leur posture aux modèles IA eux-mêmes pour protéger les données d'entraînement sensibles de l'IA, gagner en visibilité sur l'utilisation de modèles d'IA non approuvés ou *cachés*, ainsi que sur l'utilisation abusive de l'IA ou la fuite de données.

La sécurisation du développement de modèles d'IA générative nécessite de rechercher les vulnérabilités dans le pipeline, de renforcer les intégrations et d'appliquer des politiques et des règles d'accès. Pour sécuriser l'utilisation des modèles d'IA générative, les équipes de sécurité doivent surveiller les entrées malveillantes, telles que les injections de prompts, et les sorties contenant des données sensibles. Elles doivent également mettre en œuvre des solutions de sécurité de l'IA capables de détecter et de neutraliser les attaques la ciblant, telles que l'empoisonnement des données, l'exfiltration et l'extraction de modèles. L'élaboration de protocoles de réponse pour restreindre les accès, mettre en quarantaine et déconnecter les modèles compromis est également impérative.

L’expansion du contexte des menaces liée à l’IA générative et à d’autres initiatives informatiques implique la nécessité de proposer des formations de sécurité aux praticiens non spécialisés en sécurité, comme par exemple les data scientists et les ingénieurs de données travaillant dans des équipes d’IA.

Améliorer la formation en matière de cyber réponse

La façon dont une organisation réagit et communique pendant et après une violation, avec les dirigeants de l’entreprise, les régulateurs et les clients, est plus importante que jamais. 75 % de l’augmentation des coûts moyens des violations dans l’étude de cette année peut être imputée au coût lié à la perte d’activité, comprenant les temps d’arrêt, la perte de clients et de commandes, et l’acquisition de nouveaux clients. Cette hausse s’explique également par les activités d’intervention post-violation, comme la mise en place d’un centre d’assistance client, la fourniture de services de surveillance gratuits aux clients touchés et le paiement d’amendes réglementaires. En somme, investir dans sa préparation à l’intervention post-violation peut contribuer à réduire les coûts liés aux violations de données.

Les organisations doivent compléter leurs capacités de réponse technique par une planification stratégique permettant de couvrir l’impact commercial, de protéger les clients et de maintenir la continuité opérationnelle. Mettre en place une gouvernance et prendre des décisions à l’avance peut aider les dirigeants à prévoir la gestion des perturbations affectant fortement l’activité et à rationaliser les actions qui profiteront à l’organisation en cas d’attaque.

Pour améliorer leur capacité à gérer des attaques à fort impact, les organisations peuvent développer leur mémoire musculaire de réponses aux violations en participant à des exercices de simulation de cyber crise à distance. Ces exercices s’adressent aux équipes de sécurité ainsi qu’aux chefs d’entreprise, afin que l’ensemble de l’organisation améliore sa capacité à détecter, contenir et répondre aux violations. Les responsables de la sécurité doivent préalablement travailler avec les fonctions commerciales de leur organisation et les équipes de communication pour élaborer des plans d’intervention et les tester. L’expansion du contexte des menaces liée à l’IA générative et à d’autres initiatives informatiques implique la nécessité de proposer des formations de sécurité aux praticiens non spécialisés en sécurité. Ces praticiens comprennent des data scientists et des ingénieurs de données travaillant dans des équipes de machine learning et d’IA ainsi que ceux chargés de la continuité des workloads d’IA des actifs sur site et cloud.

En investissant dans la préparation aux interventions, les organisations peuvent contribuer à réduire les effets coûteux et perturbateurs induits par les violations de données, à soutenir la continuité opérationnelle et à préserver leurs relations avec les clients, les partenaires et les autres parties prenantes clés. De plus, répéter les interventions permet de rassurer les employés et de réduire le stress, l’angoisse et les frictions en interne, car les stades les plus graves des attaques sont gérés, contrôlés et signalés par une équipe de direction bien préparée.

À propos d'IBM et de Ponemon Institute

Ponemon Institute

Fondée en 2002, le Ponemon Institute est un institut indépendant spécialisé dans la recherche et la formation, dont le but est de promouvoir des pratiques responsables de gestion de l'information et de la confidentialité dans le secteur public et privé. Notre mission est de réaliser des études empiriques de haute qualité portant sur des questions critiques affectant la gestion et la sécurité des informations sensibles sur les personnes et les organisations.

Dans le cadre de ses enquêtes commerciales, le Ponemon Institute respecte strictement la confidentialité des données et des personnes et les règles éthiques propres aux études et ne collecte pas d'informations personnelles identifiables auprès des personnes, ni d'informations identifiant une société. De plus, nous respectons des normes de qualité très strictes qui garantissent qu'aucune question superflue, non pertinente ou inappropriée ne sera posée aux participants.

Si vous avez des questions ou des commentaires au sujet de ce rapport, y compris pour obtenir la permission de citer ou de reproduire son contenu, veuillez nous contacter par courrier, téléphone ou e-mail aux coordonnées suivantes :

Ponemon Institute LLC
Research Department
1-800-887-3118
research@ponemon.org

IBM

L'un des principaux fournisseurs mondiaux de cloud hybride, d'IA et de services métier, IBM aide ses clients dans plus de 175 pays à tirer parti des informations issues de leurs données, à rationaliser les processus métier, à réduire leurs coûts et à obtenir un avantage concurrentiel dans leurs secteurs. Ces capacités s'appuient sur l'engagement légendaire d'IBM en faveur de la confiance, de la transparence, de la responsabilité, de l'inclusion et du service. Pour plus d'informations, rendez-vous sur www.ibm.com/fr-fr.

En savoir plus sur l'amélioration de votre posture de sécurité : Rendez-vous suribm.com/fr-fr/security

Participez à la conversation de la Communauté IBM Security

© Copyright IBM Corporation 2024

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produit aux Etats-Unis d'Amérique
Juillet 2024

IBM et le logo IBM sont des marques ou des marques déposées d'International Business Machines Corporation, aux États-Unis et/ou dans d'autres pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur ibm.com/fr-fr/trademark.

Le présent document est à jour à la date de publication initiale et est susceptible d'être modifié par IBM à tout moment. Certaines offres mentionnées dans le présent document ne sont pas disponibles dans tous les pays où la société IBM est présente.

LES INFORMATIONS CONTENUES DANS LE PRÉSENT DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, NOTAMMENT SANS AUCUNE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET AUCUNE GARANTIE OU CONDITION D'ABSENCE DE CONTREFAÇON. Les produits IBM sont garantis conformément aux dispositions des contrats qui régissent leur utilisation.

Déclaration sur les bonnes pratiques de sécurité : Aucun système ni produit informatique ne doit être considéré comme entièrement sécurisé, et aucun produit, ni service, ni mesure de sécurité ne peut être totalement efficace pour empêcher des accès non autorisés. IBM ne garantit pas qu'un système, produit ou service, quel qu'il soit, est à l'abri, ou mettra votre entreprise à l'abri, de la conduite malveillante ou illégale de quelque partie que ce soit.

Il incombe au client de respecter l'ensemble des lois et réglementations applicables. IBM ne fournit pas de conseils juridiques et ne déclare ni ne garantit que ses services ou ses produits mettront le client en conformité avec la législation ou la réglementation en vigueur.