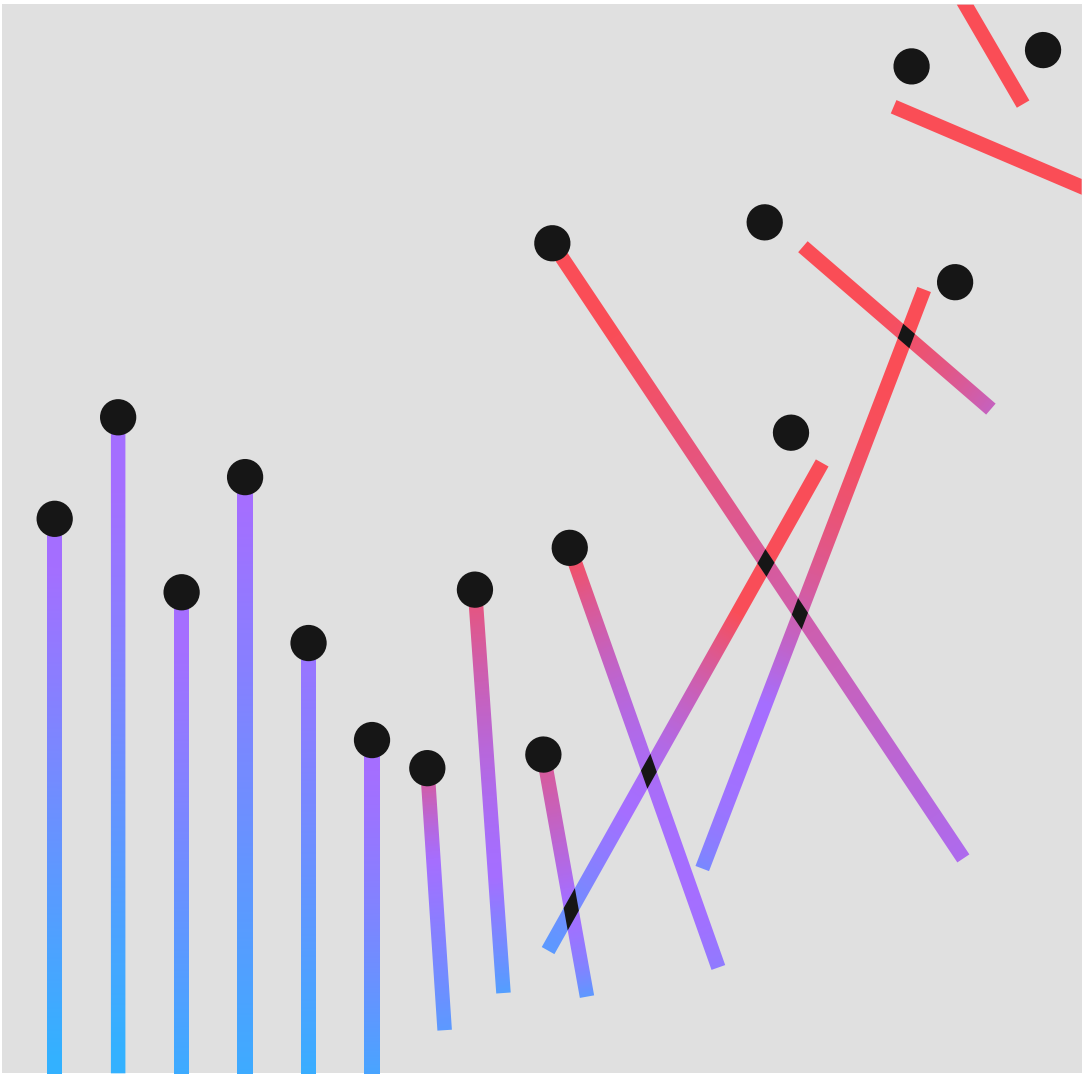
IBM **Security**

Rapport 2022 sur le coût d'une violation de données : Résumé analytique



IBM

Sommaire

Résumé analytique

Le Rapport sur le coût d'une violation de données offre aux responsables de l'informatique, de la gestion des risques et de la sécurité une vision des facteurs qui peuvent accentuer ou atténuer le coût des violations de données.

Maintenant dans sa 17e année, cette étude indépendante réalisée par le Ponemon Institute et parrainée, analysée et publiée par IBM Security®, porte sur 550 entreprises victimes de violations de données survenues entre mars 2021 et mars 2022. Les violations se sont produites dans 17 pays et régions et dans 17 secteurs d'activité différents.

Nous avons réalisé plus de 3 600 entretiens avec des employés d'entreprises ayant été victimes de violations de données. Au cours des entretiens, nous avons posé des questions en vue de déterminer les coûts encourus par les entreprises pour les différentes activités se rapportant directement à la réponse immédiate et à long terme aux violations de données.

Comme dans les rapports précédents, les données de cette année donnent un aperçu de l'impact de dizaines de facteurs sur les coûts qui continuent de grimper après une violation de données. En outre, le rapport examine les causes profondes, les conséquences à court et à long terme des violations de données, ainsi que les facteurs atténuants et les technologies qui ont permis aux entreprises de limiter les pertes.

Principales conclusions

Les principales conclusions présentées ici sont basées sur l'analyse réalisée par IBM Security à partir des données compilées par le Ponemon Institute.[1]

4,35 millions de dollars

Coût total moyen d'une violation de données

Le coût d'une violation de données s'élevait en moyenne à 4,35 millions de dollars en 2022, un niveau record. Ce chiffre représente une augmentation de 2,6 % par rapport à l'année précédente, lorsque le coût moyen d'une violation était de 4,24 millions de dollars. En outre, il représente une augmentation de 12,7 % par rapport au coût moyen en 2020, à savoir 3,86 millions de dollars.

83 %

Pourcentage d'entreprises ayant été victimes de plus d'une violation

Quatre-vingt-trois pour cent des entreprises étudiées ont subi plus d'une violation de données, et seulement 17 % ont déclaré qu'il s'agissait de leur première violation. Soixante pour cent des entreprises étudiées ont déclaré avoir augmenté le prix de leurs services ou produits en raison d'une violation de données.

4,82 millions de dollars

Coût moyen d'une violation de données affectant une infrastructure critique

Le coût moyen d'une violation de données pour les entreprises d'infrastructures critiques étudiées s'élevait à 4,82 millions de dollars, soit 1 million de dollars de plus que le coût moyen pour les entreprises d'autres secteurs. Les entreprises d'infrastructures critiques étaient issues des secteurs des services financiers, de l'industrie, de la technologie, de l'énergie, des transports, des communications, des soins de santé, de l'éducation et du secteur public. Vingt-huit pour cent ont subi une attaque destructrice ou été victime d'un ransomware, tandis que 17 % ont subi une violation en raison d'un partenaire commercial compromis.

3,05 millions de dollars

Économies moyennes associées au déploiement complet de l'IA et de l'automatisation pour la sécurité

Les violations dans les entreprises ayant déployé des solutions complètes d'IA et d'automatisation pour la sécurité coûtent 3,05 millions de dollars en moins que les violations dans les entreprises n'ayant pas mis en œuvre de telles solutions. Cette différence de 65,2 % dans le coût moyen d'une violation (à savoir 3,15 millions de dollars avec déploiement complet contre 6,2 millions de dollars sans déploiement) représentait la plus grande économie de coûts constatée dans l'étude. En moyenne, le délai pour identifier et contenir la violation, appelé « cycle de vie de la violation », dans les entreprises disposant de solutions complètes d'IA et d'automatisation pour la sécurité était 74 jours plus court que dans les entreprises ne disposant pas de telles solutions, à savoir 249 contre 323 jours. L'utilisation de l'IA et de l'automatisation pour la sécurité a augmenté de près d'un cinquième en deux ans, passant de 59 % en 2020 à 70 % en 2022.

1. Les montants dans ce rapport sont exprimés en dollars américains (USD).

4,54 millions de dollars

Coût moyen d'une attaque par ransomware, sans compter le coût de la rançon elle-même

Les attaques par ransomware représentaient 11 % des attaques étudiées, en hausse par rapport à 2021 où elles représentaient 7,8 % des violations, soit un taux de croissance de 41 %. Le coût moyen d'une attaque par ransomware a légèrement diminué, passant de 4,62 millions de dollars en 2021 à 4,54 millions de dollars en 2022. Ce coût était légèrement supérieur au coût total moyen global d'une violation de données, à savoir 4,35 millions de dollars.

19 %

Fréquence des violations causées par des identifiants volés ou compromis

L'utilisation d'identifiants volés ou compromis reste la cause la plus fréquente de violation de données. Les identifiants volés ou compromis étaient le principal vecteur d'attaque dans 19 % des violations recensées dans l'étude de 2022, contre 20 % en 2021. Les violations causées par des identifiants volés ou compromis ont coûté en moyenne 4,5 millions de dollars. Elles comptaient le cycle de vie le plus long : 243 jours pour identifier la violation et 84 jours supplémentaires pour la contenir. Deuxième cause la plus fréquente de violation, l'hameçonnage représentait 16 % des violations. Avec un coût moyen par violation de 4,91 millions de dollars, son coût était également le plus élevé.

59 %

Pourcentage d'entreprises n'ayant pas opté pour l'approche Zero Trust

Seulement 41 % des entreprises étudiées ont déclaré avoir déployé une architecture de sécurité Zero Trust. Pour les 59 % restants qui n'ont pas adopté le Zero Trust, le coût d'une violation est en moyenne 1 million de dollars plus élevé. Parmi les entreprises d'infrastructures critiques, un pourcentage encore plus élevé, soit 79 %, n'a pas adopté le Zero Trust. En moyenne, le coût d'une violation pour ces entreprises s'élevait à 5,4 millions de dollars, soit plus de 1 million de dollars de plus que la moyenne mondiale.

1 million de dollars

Écart de coût moyen entre une violation où le télétravail a joué un rôle et une violation où il n'a pas été un facteur

Lorsque le télétravail était un facteur à l'origine de la violation, les coûts étaient en moyenne supérieurs de près de 1 million de dollars à ceux des violations où le télétravail n'était pas un facteur, à savoir 4,99 contre 4,02 millions de dollars. En moyenne, les violations liées au télétravail coûtent environ 600 000 de dollars de plus que la moyenne mondiale.

45 %

Pourcentage des violations survenues dans le cloud

Quarante-cinq pour cent des violations étudiées se sont produites dans le cloud. Néanmoins, les violations qui se sont produites dans un environnement de cloud hybride ont coûté en moyenne 3,8 millions de dollars, contre 4,24 millions de dollars pour les violations dans les clouds privés et 5,02 millions de dollars pour les violations dans les clouds publics. L'écart de coût était de 27,6 % entre les violations dans un cloud hybride et les violations dans un cloud public. Les entreprises dotées d'un modèle de cloud hybride affichaient également des cycles de vie de violations plus courts que celles ayant seulement adopté un modèle de cloud public ou privé.

2,66 millions de dollars

Économies moyennes associées à une équipe de réponse aux incidents (RI) et à un plan de RI testé régulièrement

Près des trois quarts des entreprises étudiées ont déclaré avoir un plan de RI et 63 % d'entre elles ont affirmé qu'elles le testaient régulièrement. Le fait d'avoir une équipe de RI et un plan de RI testé régulièrement a permis de réaliser d'importantes économies. En moyenne, les coûts de violations étaient inférieurs de 2,66 millions de dollars dans les entreprises disposant d'une équipe de RI ayant testé leur plan de RI par rapport à celles n'ayant pas d'équipe de RI et ne testant pas leur plan de RI. La différence entre 3,26 millions de dollars et 5,92 millions de dollars représente une économie de coûts de 58 %.

29 jours

Réduction du temps de réponse pour les entreprises disposant de technologies de détection et de réponse étendues (XDR)

Les technologies XDR ont été mises en œuvre par 44 % des entreprises. Celles-ci ont constaté des avantages considérables en termes de temps de réponse. Elles ont raccourci le cycle de vie des violations d'environ un mois, en moyenne, par rapport aux entreprises ne disposant pas de technologies XDR. Plus précisément, celles disposant de technologies XDR ont mis 275 jours pour identifier et contenir une violation, contre 304 jours pour celles ne disposant pas de telles technologies. Ce chiffre représente une différence de 10 % dans les temps de réponse.

12 ans

Années consécutives durant lesquelles le secteur de la santé a connu le coût moyen d'une violation le plus élevé

Les coûts des violations affectant le secteur des soins de santé ont atteint un nouveau record. Le coût moyen d'une violation dans ce secteur a augmenté de près de 1 million de dollars pour atteindre 10,1 millions de dollars. Au cours des 12 dernières années, le secteur des soins de santé a affiché les coûts de violations les plus élevés, ceux-ci ayant augmenté de 41,6 % depuis le rapport de 2020. Le secteur des finances se plaçait en deuxième position, avec des coûts de 5,97 millions de dollars en moyenne, suivi du secteur pharmaceutique (5,01 millions de dollars), du secteur technologique (4,97 millions de dollars) et du secteur de l'énergie (4,72 millions de dollars).

9,44 millions de dollars

Coût moyen d'une violation aux États-Unis, le plus élevé de tous les pays

Les cinq principaux pays et régions affichant le coût moyen d'une violation de données le plus élevé étaient les États-Unis (9,44 millions de dollars), le Moyen-Orient (7,46 millions de dollars), le Canada (5,64 millions de dollars), le Royaume-Uni (5,05 millions de dollars) et l'Allemagne (4,85 millions de dollars). Les États-Unis sont en tête de liste depuis 12 ans d'affilée. Entre-temps, le Brésil affichait le taux de croissance le plus rapide par rapport à l'année précédente, soit une augmentation de 27,8 %, passant de 1,08 million à 1,38 million de dollars.

Recommandations pour minimiser l'impact financier d'une violation de données

Dans cette section, IBM Security décrit les mesures que les entreprises peuvent prendre pour réduire les coûts financiers et les conséquences sur la réputation d'une violation de données. Ces recommandations comprennent des approches de sécurité réussies adoptées par les entreprises étudiées.

Adoptez un modèle de sécurité Zero Trust pour empêcher tout accès non autorisé aux données sensibles.
Les résultats de l'étude ont montré que bien que 41 % seulement des entreprises aient mis en œuvre une approche de sécurité Zero Trust, un déploiement mature pourrait leur permettre d'économiser 1,5 million de dollars en coûts de violations. Alors que les entreprises intègrent le télétravail et les environnements multicloud hybrides, une stratégie Zero Trust peut protéger les données et les ressources en limitant leur accessibilité et en exigeant du contexte.

Les outils de sécurité capables de partager des données entre des systèmes disparates et de centraliser les opérations de sécurité des données peuvent aider les équipes de sécurité à détecter les incidents dans des environnements multicloud hybrides complexes. Vous pouvez obtenir des analyses plus approfondies, atténuer les risques et accélérer la réponse grâce à une plateforme de sécurité ouverte qui peut faire progresser votre stratégie Zero Trust. Dans le même temps, vous pouvez utiliser vos investissements existants tout en laissant vos données là où elles se trouvent, aidant ainsi votre équipe à devenir plus efficace et à mieux collaborer.

Protégez les données sensibles dans les environnements cloud à l'aide de règles et du chiffrement.
Étant donné que la quantité et la valeur des données hébergées dans les environnements cloud augmentent sans cesse, les entreprises doivent prendre des mesures pour protéger leurs bases de données hébergées dans le cloud. La mise en œuvre de pratiques de sécurité cloud matures était associée à une réduction des coûts de violations de 720 000 dollars. Utilisez le schéma de classification des données et les programmes de rétention pour gagner en visibilité et réduire le volume d'informations sensibles vulnérables à une violation. Protégez les informations sensibles à l'aide du chiffrement des données et du chiffrement entièrement homomorphe. L'utilisation d'un cadre interne pour les audits, l'évaluation des risques dans l'ensemble de l'entreprise et le suivi de la conformité aux exigences de gouvernance peuvent vous permettre de mieux détecter une violation de données et d'intensifier vos efforts de confinement.

Investissez dans l'orchestration, l'automatisation et la réponse aux incidents de sécurité (SOAR) et dans les technologies XDR pour améliorer les temps de détection et de réponse.
Avec l'IA et l'automatisation pour la sécurité, les fonctionnalités XDR peuvent contribuer à réduire considérablement les coûts moyens des violations de données et les cycles de vie des violations. Selon l'étude, les entreprises ayant déployé des solutions XDR ont raccourci le cycle de vie des violations de 29 jours en moyenne par rapport à celles qui ne l'ont pas fait, ce qui se traduit par une économie de 400 000 dollars. Les technologies SOAR, les logiciels de gestion des informations et des événements de sécurité (SIEM), les services gérés de détection et de réponse et les technologies XDR peuvent aider votre entreprise à accélérer la réponse aux incidents grâce à l'automatisation, à la normalisation des processus et à l'intégration avec vos outils de sécurité existants.

Utilisez des outils pour la protection et la surveillance des terminaux et des télétravailleurs.
L'étude a montré que lorsque le télétravail est un facteur à l'origine d'une violation, celle-ci coûte près de 1 million de dollars de plus que lorsqu'il n'est pas un facteur. Les produits et services de gestion unifiée des terminaux (UEM), de détection et de réponse des terminaux (EDR) et de gestion des identités et des accès (IAM) peuvent offrir aux équipes de sécurité une visibilité plus poussée sur les activités suspectes. Cette surveillance couvre les dispositifs personnels (BYOD, Bring your own device) et les ordinateurs portables, les ordinateurs de bureau, les tablettes, les appareils mobiles et les dispositifs IdO de l'entreprise, y compris les terminaux auxquels l'entreprise n'a pas accès physiquement. L'UEM, l'EDR et l'IAM accélèrent l'investigation et le temps de réponse pour isoler et contenir les dommages lorsque le télétravail est un facteur.

Créez et testez des manuels de réponse aux incidents pour renforcer votre cyber-résilience.
La création d'une équipe de réponse aux incidents (RI) et des tests approfondis du plan de RI sont deux des moyens les plus efficaces pour réduire le coût d'une violation de données. Les violations survenues dans les entreprises disposant d'une équipe de RI qui teste régulièrement son plan ont coûté 2,66 millions de dollars de moins que celles survenues dans les entreprises sans équipe de RI ou qui ne testaient pas leur plan de RI. Les entreprises peuvent réagir rapidement pour contenir les retombées d'une violation en élaborant un manuel détaillé pour les cyberincidents. Testez régulièrement ce plan par le biais d'exercices de simulation ou exécutez un scénario de violation dans un environnement simulé tel qu'un cyber-range.

Les exercices de simulation d'adversaire, également appelés exercices « Red Team », peuvent améliorer l'efficacité des équipes de RI en découvrant les voies et techniques d'attaque qui pourraient leur échapper et en identifiant les lacunes dans leurs capacités de détection et de réponse. Une solution de gestion de la surface d'attaque peut aider les entreprises à améliorer leur posture de sécurité en localisant des points d'exposition auparavant inconnus grâce à la simulation d'une expérience d'attaque authentique.

Les pratiques de sécurité recommandées le sont à titre éducatif et les résultats ne sont pas garantis.

À propos du Ponemon Institute et d'IBM Security

Ponemon Institute

Le Ponemon Institute se consacre à la recherche et à l'éducation indépendantes pour proposer des pratiques de gestion responsable de la vie privée et des informations à destination du gouvernement et des entreprises. 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.

Le Ponemon Institute respecte des normes strictes en matière de confidentialité des données, de vie privée et de recherche éthique, et ne recueille aucune information qui permettraient d'identifier les personnes ou les entreprises participant à ses études. De plus, nos normes de qualité strictes sont la garantie qu'aucune question superflue, non pertinente ou inappropriée ne sera posée aux participants.

IBM Security

IBM Security propose l'un des portefeuilles de produits et services de sécurité d'entreprise les plus avancés et les plus intégrés. Ce portefeuille, soutenu par l'équipe de recherche IBM Security X-Force® de renommée mondiale, fournit des solutions de sécurité pour aider les entreprises à intégrer la sécurité au sein de leurs activités afin de prospérer en dépit d'un environnement imprévisible.

IBM dirige des opérations de recherche, de développement et de prestation dans le domaine de la sécurité qui figurent parmi les plus vastes et les plus complètes du marché. IBM surveille plus de 4 700 milliards d'événements par mois dans plus de 130 pays et détient plus de 10 000 brevets de sécurité. Pour en savoir plus, rendez-vous sur ibm.com/fr-fr/security. Prenez part à la conversation dans la communauté IBM Security.

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
À l'attention de : Research Department
2308 US 31 North
Traverse City
Michigan 49686, États-Unis

1.800.887.3118
research@ponemon.org

Passez à l'étape suivante

Solutions de sécurité Zero Trust
Assurez la sécurité de chaque utilisateur, de chaque appareil et de chaque connexion.
En savoir plus

Gestion des identités et des accès
Connectez chaque utilisateur, API et appareil à toutes les applications en toute sécurité.
En savoir plus

Sécurité des données
Découvrez, classez et protégez les données sensibles de l'entreprise.
En savoir plus

Orchestration, automatisation et réponse aux incidents de sécurité
Accélérez la réponse aux incidents grâce à l'orchestration et à l'automatisation.
En savoir plus

Gestion des informations et des événements de sécurité
Gagnez en visibilité pour détecter, enquêter et répondre aux menaces.
En savoir plus

Sécurité cloud
Intégrez la sécurité dans votre parcours vers le multicloud hybride.
En savoir plus

Sécurité des terminaux
Protégez les appareils, les utilisateurs et l'entreprise contre les attaques sophistiquées.
En savoir plus

Services de cybersécurité
Réduisez les risques grâce aux services de conseil, de cloud et de sécurité gérés.
En savoir plus

Réponse aux incidents et renseignements sur les menaces
Gérez et répondez de manière proactive aux menaces à la sécurité.
En savoir plus

Programmez une consultation individuelle avec un expert IBM Security X-Force
Réserver maintenant

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique
Juillet 2022