Communiqués de presse

Rapport IBM : Le coût d'une violation de données atteint un niveau record pendant la pandémie

Les violations de données coûtent en moyenne 4,24 millions de dollars par incident aux entreprises interrogées ; C'est le montant le plus élevé depuis la publication du premier rapport il y a 17 ans

L'adoption de l'intelligence artificielle, du Cloud hybride et de l'approche « zero trust » a permis de réduire les coûts liés aux violations de données

Armonk, le 28 juillet 2021 : IBM Security a annoncé aujourd'hui les résultats d'une étude mondiale qui révèle que les violations de données coûtent désormais 4,24 millions de dollars par incident en moyenne aux entreprises interrogées - le coût le plus élevé depuis la création du rapport il y a 17 ans. Basée sur une analyse approfondie des violations de données réelles subies par plus de 500 organisations, l'étude indique que les incidents de sécurité sont devenus plus coûteux et plus difficiles à contenir en raison de changements opérationnels drastiques pendant la pandémie, les coûts ayant augmenté de 10 % par rapport à l'année précédente.

Les entreprises ont été contraintes d'adapter rapidement leurs approches technologiques l'année dernière, de nombreuses sociétés encourageant ou imposant à leurs employés le télétravail et 60 % des organisations s'orientant davantage vers des activités basées sur le Cloud pendant la pandémie[1]. Les nouvelles conclusions publiées aujourd'hui montrent que la sécurité pourrait avoir pris du retard par rapport à ces changements informatiques rapides, entravant la capacité des organisations à réagir aux violations de données.

Le rapport annuel sur le coût d'une violation de données, réalisé par le Ponemon Institute, sponsorisé et analysé par IBM Security, a identifié les tendances suivantes parmi les organisations étudiées :

- **Impact du travail à distance** : Le passage rapide aux opérations à distance pendant la pandémie semble avoir entraîné des violations de données plus coûteuses. Les violations ont coûté plus d'un million de dollars de plus en moyenne lorsque le travail à distance a été indiqué comme un facteur de l'événement, par rapport à ceux de ce groupe sans ce facteur (4,96 contre 3,89 millions de dollars) [2].
- **Les coûts liés aux violations de données dans le secteur des soins de santé ont fortement augmenté** : Les secteurs qui ont dû faire face à d'énormes changements opérationnels pendant la pandémie (soins de santé, commerce de détail, hôtellerie et fabrication/distribution de biens de consommation) ont également connu une augmentation substantielle des coûts liés aux violations de données d'une année sur l'autre. Les violations dans le secteur de la santé sont de loin les plus coûteuses, avec 9,23 millions de dollars par incident, soit une augmentation de 2 millions de dollars par rapport à l'année précédente.
- **Des informations d'identification compromises ont conduit à des données compromises** : Le vol d'informations d'identification d'utilisateurs était la cause première la plus courante des violations dans l'étude. Dans le même temps, les données personnelles des clients (telles que le nom, l'adresse mail, le mot de passe) étaient le type d'informations le plus couramment exposé dans les violations de données - avec 44 % des violations comprenant ce type de données. La combinaison de ces facteurs pourrait provoquer un effet de spirale, les violations de noms d'utilisateur / de mots de passe fournissant aux attaquants un levier pour d'autres violations de données dans le futur.

- **Les approches modernes ont réduit les coûts** : L'adoption de l'IA, de l'analytique et du chiffrement ont été les trois principaux facteurs d'atténuation qui ont permis de réduire le coût d'une violation, permettant aux entreprises d'économiser entre 1,25 million et 1,49 million de dollars par rapport à celles qui ne les utilisaient pas de façon significative. Pour les violations de données basées sur le Cloud étudiées, les organisations qui avaient mis en œuvre une approche de Cloud hybride avaient des coûts de violation de données plus faibles (3,61 millions de dollars) que celles qui avaient une approche de Cloud principalement public (4,80 millions de dollars) ou de Cloud principalement privé (4,55 millions de dollars).

« L'augmentation des coûts liés aux violations de données est une dépense supplémentaire pour les entreprises dans le sillage des changements technologiques rapides qui ont eu lieu pendant la pandémie », a déclaré **Chris McCurdy, Vice President and General Manager, IBM Security***. « Alors que les coûts liés aux violations de données ont atteint un niveau record au cours de l'année dernière, le rapport a également montré des signes positifs concernant l'impact des tactiques de sécurité modernes, telles que l'IA, l'automatisation et l'adoption d'une approche « zero trust » - ce qui pourrait s'avérer payant en réduisant le coût de ces incidents plus tard. »*

Impact du travail à distance et du passage au Cloud sur les violations de données

La société s'appuyant davantage sur les interactions numériques pendant la pandémie, les entreprises ont adopté le travail à distance et le Cloud pour s'adapter à ce monde de plus en plus connecté. Le rapport a révélé que ces facteurs avaient un impact important sur la réponse aux violations de données. Près de 20 % des organisations étudiées ont déclaré que le travail à distance avait joué un rôle dans la violation de données, et ces violations ont fini par coûter 4,96 millions de dollars aux entreprises (près de 15 % de plus qu’une violation moyenne).

Les entreprises de l’étude qui ont subi une violation lors d’un projet de migration vers le Cloud ont eu un coût supérieur de 18,8 % à la moyenne. Cependant, l'étude a également révélé que celles qui étaient plus avancées dans leur stratégie globale de modernisation du Cloud (stade « mature ») étaient en mesure de détecter et de répondre aux incidents plus efficacement - 77 jours plus rapidement en moyenne que celles qui étaient en phase d'adoption précoce. En outre, pour les violations de données basées sur le Cloud étudiées, les entreprises qui avaient mis en œuvre une approche de Cloud hybride avaient des coûts de violation de données plus faibles (3,61 millions de dollars) que celles qui avaient une approche de Cloud principalement public (4,80 millions de dollars) ou de Cloud principalement privé (4,55 millions de dollars).

Les informations d'identification compromises constituent un risque croissant

Le rapport met également en lumière un problème croissant : les données des consommateurs (y compris les informations d'identification) sont compromises lors de violations de données, et peuvent ensuite être utilisées pour propager d'autres attaques. Avec 82 % des personnes interrogées qui admettent réutiliser le même mot de passe sur plusieurs comptes, les informations d'identification compromises représentent à la fois une cause

et un effet majeurs des violations de données, créant un risque aggravant pour les entreprises.

- **Données personnelles exposées** : Près de la moitié (44 %) des violations analysées ont exposé des données personnelles de clients, telles que le nom, l'adresse mail, le mot de passe ou même des données relatives à la santé, ce qui représente le type de données ayant subi une violation le plus courant dans le rapport.
- **Les données personnelles d'identification des clients sont les plus coûteuses** : la perte des données personnelles d'identification (PII) des clients est également la plus coûteuse par rapport aux autres types de données (180 dollars par enregistrement perdu ou volé contre 161 dollars pour la moyenne générale par enregistrement).
- **Méthode d'attaque la plus courante** : Les informations d'identification d'utilisateur compromises ont été la méthode la plus utilisée comme point d'entrée par les attaquants, représentant 20 % des violations étudiées.
- **Plus long à détecter et à contenir** : Les violations résultant de la compromission d'informations d'identification ont été les plus longues à détecter - il a fallu en moyenne 250 jours pour les identifier (contre 212 pour une violation moyenne).

Les entreprises qui se sont modernisées ont eu des coûts de violation moins élevés

Alors que certains changements informatiques pendant la pandémie ont augmenté les coûts liés aux violations de données, les organisations qui ont déclaré n'avoir mis en œuvre aucun projet de transformation numérique afin de moderniser leurs opérations métier pendant la pandémie ont en fait subi des coûts de violation de données plus élevés. Le coût d'une violation de données était supérieur de 750 000 dollars à la moyenne dans les organisations qui n'avaient procédé à aucune transformation numérique en raison de la COVID-19 (16,6 % de plus que la moyenne).

Les entreprises étudiées qui ont adopté une approche de sécurité « zero trust » étaient mieux placées pour faire face aux violations de données. Cette approche part du principe que les identités des utilisateurs ou le réseau lui-même peuvent déjà être compromis, et s'appuie plutôt sur l'IA et l'analytique pour valider en permanence les connexions entre les utilisateurs, les données et les ressources. Les organisations dotées d'une stratégie « zero trust » mature avaient un coût moyen de violation de données de 3,28 millions de dollars, soit 1,76 million de dollars de moins que celles qui n'avaient pas du tout déployé cette approche.

Le rapport indique également que les entreprises sont plus nombreuses à déployer l'automatisation de la sécurité par rapport aux années précédentes, ce qui permet de réaliser d'importantes économies. Environ 65 % des entreprises interrogées ont déclaré qu'elles déployaient partiellement ou totalement l'automatisation dans leurs environnements de sécurité, contre 52% il y a deux ans. Les organisations ayant une stratégie d'automatisation de la sécurité « entièrement déployée » ont enregistré un coût moyen de violation de 2,90 millions de dollars, tandis que celles qui n'ont pas mis en place d'automatisation ont enregistré un coût plus de deux fois supérieur, soit 6,71 millions de dollars.

Les investissements dans les équipes et les plans de réponse aux incidents ont également réduit les coûts liés aux violations de données parmi les entreprises étudiées. Les entreprises disposant d'une équipe de réponse

aux incidents qui ont également testé leur plan de réponse aux incidents ont eu un coût moyen de 3,25 millions de dollars, tandis que celles qui n'avaient ni l'un ni l'autre en place ont eu un coût moyen de 5,71 millions de dollars (soit une différence de 54,9 %).

Les autres conclusions du rapport 2021 sont les suivantes :

- **Temps de réponse** : Le temps moyen pour détecter et contenir une violation de données était de 287 jours (212 pour détecter, 75 pour contenir), soit une semaine de plus que dans le rapport de l'année précédente.
- **Méga-violations** : Le coût moyen d'une méga-violation était de 401 millions de dollars, pour des violations comprises entre 50 et 65 millions d'enregistrements[3]. Ce coût est presque 100 fois plus élevé que celui de la majorité des violations étudiées dans le rapport (qui se situaient entre 1 000 et 100 000 enregistrements).
- **Par secteur d'activité** : Les violations de données dans le secteur de la santé ont été les plus coûteuses (9,23 millions de dollars), suivies par le secteur financier (5,72 millions de dollars) et le secteur pharmaceutique (5,04 millions de dollars). Bien que les coûts globaux soient moins élevés, le commerce de détail, les médias, l'hôtellerie et le secteur public ont connu une forte augmentation des coûts par rapport à l'année précédente.
- **Par pays/région** : Les États-Unis ont enregistré les violations de données les plus coûteuses avec 9,05 millions de dollars par incident, suivis du Moyen-Orient (6,93 millions de dollars) et du Canada (5,4 millions de dollars).

Méthodologie et statistiques supplémentaires sur les violations de données

Le rapport 2021 sur le coût d'une violation de données d'IBM Security et du Ponemon Institute est basé sur une analyse approfondie des violations de données réelles de 100 000 enregistrements ou moins, subies par plus de 500 organisations dans le monde entre mai 2020 et mars 2021. Le rapport prend en compte des centaines de facteurs de coûts impliqués dans les incidents de violation de données, des activités juridiques, réglementaires et techniques à l’atteinte à l’image de marque, la perte de clients et de productivité des employés.

Pour télécharger un exemplaire du rapport 2021 sur le coût d'une violation de données : ibm.com/databreach.

Pour vous inscrire au webinaire 2021 sur le rapport sur le coût d'une violation de données, du **18 août à 17h** : ibm.biz/CODBwebinar

À propos d’IBM Security

IBM Security offre aux entreprises l’une des gammes de produits et services de sécurité les plus performantes

et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère plus de 150 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur https://www-03.ibm.com/security/fr-fr/, suivez IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

Contacts presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0) 6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Robin Legros

Tél. : + 33 (0)6 68 04 57 83

ibmfrance@webershandwick.com

---

[1] IBM Institute for Business Value: COVID-19 and the future of business

[2]Average cost of $4.96 million for those surveyed where remote work was a factor vs. $3.89 million when remote work was not a factor

[3] The 2021 Cost of a Data Breach Report examines the cost of a mega breach based on a separate analysis of a specific sample involving loss or theft of one million records or more. The mega breach sample is not included in the overall average data breach report calculations, which examines data breaches ranging from 1,000-100,000 records.