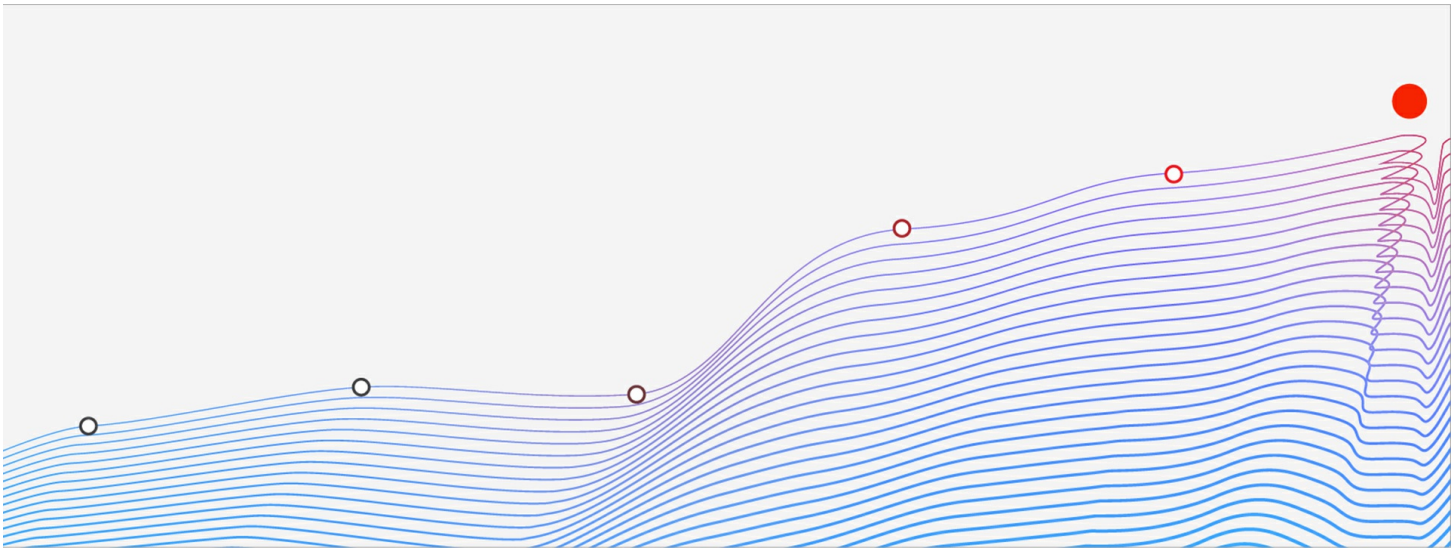
Communiqués de presse

Rapport IBM : La moitié des organisations victimes d'une violation ne prévoient pas d’augmenter leurs dépenses de sécurité malgré la montée en flèche du coût des violations

L'IA et l'automatisation ont permis de réduire le cycle de vie des violations de 108 jours ; 470 000 dollars de coûts supplémentaires pour les victimes de ransomware qui échappent aux autorités ; seul un tiers des organisations ont détecté la violation par leurs propres moyens



IBM annonce aujourd'hui les résultats de l’édition 2023 de son rapport annuel "Cost of a Data Breach" sur les coûts liés aux violations de données.

Voici l’extrait des données clés pour la France (le communiqué de presse ci-après présente les chiffres au niveau mondial) :

En France, le rapport 2023 sur le coût d'une violation de données est basé sur une analyse approfondie des violations de données réelles subies par **35 organisations** entre mars 2022 et mars 2023.

En 2023, le coût moyen d’une violation de données en France est de 3,75 millions d’€ (soit une baisse d’environ 5% par rapport à 2022).

Les secteurs les plus touchés restent :

- Les services financiers
- L’industrie pharmaceutique
- La technologie

Le coût total moyen et la fréquence des violations de données par vecteur d'attaque initial est le suivant :

- Hameçonnage ou Phishing (12 %, 4,18 millions d'€)
- Compromission des emails professionnels (9 %, 4,15 millions d'€)
- Compromission de la sécurité physique (8 %, 4,01 millions d'€)
- Perte accidentelle de données ou appareils perdus ou volés (6 %, 3,98 millions d'€)

Il faut en France en moyenne **210 jours pour identifier une violation et 72 jours pour la contenir** (soit respectivement une baisse de 19 et 6 jours par rapport à 2022), contre respectivement 207 et 77 jours au niveau mondial.

Une organisation ayant déployé largement l'IA et l'automatisation met **50 jours de moins** pour identifier une violation, **16 jours de moins** pour la contenir et subit un coût de violation de données **inférieur de 40%** par rapport à une organisation n'utilisant pas ce type d'approche, ce qui représente la plus grande économie de coûts identifiée par l'étude.

36 % des violations de données étudiées ont entraîné la **perte de données dans plusieurs environnements**, notamment dans les Clouds publics, les Clouds privés et en local, ce qui représente un coût de 4,12 millions d'€.

Rapport IBM : La moitié des organisations victimes d'une violation ne prévoient pas d'augmenter leurs dépenses de sécurité malgré la montée en flèche du coût des violations

L'IA et l'automatisation ont permis de réduire le cycle de vie des violations de 108 jours ; 470 000 dollars de coûts supplémentaires pour les victimes de ransomware qui échappent aux autorités ; seul un tiers des organisations ont détecté la violation par leurs propres moyens

CAMBRIDGE, Mass, le 24 juillet 2023 : IBM (NYSE : IBM) Security a publié aujourd'hui son **rapport annuel sur le coût d'une violation de données**[1], montrant que le coût moyen mondial d'une violation de données a atteint 4,45 millions de dollars en 2023 - un record historique pour le rapport et une augmentation de 15 % au cours des trois dernières années. Les coûts de détection et d'escalade ont bondi de 42 % au cours de cette même période, ce qui représente la part la plus élevée des coûts de violation, et indique une évolution vers des

travaux d’investigation plus complexes sur les violations.

Selon le rapport 2023 d'IBM, les entreprises sont divisées sur la manière dont elles prévoient de gérer le coût et la fréquence croissants des violations de données. L'étude révèle que si 95 % des entreprises étudiées ont subi plus d'une violation, les entreprises victimes de violations sont plus susceptibles de répercuter les coûts des incidents sur les consommateurs (57 %) que d'augmenter leurs investissements en matière de sécurité (51 %).

Le rapport 2023 sur le coût d'une violation de données est basé sur une analyse approfondie des violations de données réelles subies par 553 organisations dans le monde entre mars 2022 et mars 2023. La recherche, sponsorisée et analysée par IBM Security, a été menée par Ponemon Institute et a été publiée pendant 18 années consécutives. Voici quelques-unes des principales conclusions du rapport 2023 d'IBM :

- **L'IA aide à être plus rapide** - L'IA et l'automatisation ont eu le plus grand impact sur la vitesse d'identification et d'endiguement des violations pour les organisations étudiées. Les entreprises ayant largement recours à l'IA et à l'automatisation ont connu un cycle de vie des violations de données plus court de 108 jours par rapport aux organisations étudiées n'ayant pas déployé ces technologies (214 jours contre 322 jours).

- **Le coût du silence** - Les victimes de ransomware dans l’étude qui ont fait appel aux autorités ont économisé 470 000 dollars en coûts moyens de violation par rapport à celles qui ont choisi de ne pas y faire appel. Malgré ces économies potentielles, 37 % des victimes de ransomware étudiées n'ont pas fait appel aux autorités lors d'une attaque par ransomware.

- **Lacunes en matière de détection** - Seul un tiers des violations étudiées ont été détectées par l'équipe de sécurité de l'organisation, alors que 27 % ont été divulguées par un pirate. Les violations de données divulguées par un pirate coûtent en moyenne près d'un million de dollars de plus que celles des organisations étudiées qui ont identifié elles-mêmes la violation.

« Tout est une question de temps ... Plus on met de temps à détecter une intrusion grave, plus l’impact est fort et coûteux, il faut donc mettre en œuvre de nouvelles approches » a déclaré **Stéphanie Talaud, Directrice IBM Security Software France***. « Il n’est plus suffisant de réagir, il faut pouvoir prédire au mieux et anticiper pour agir plus vite, de manière proactive et Les solutions d’IA et d’automatisation peuvent s’avérer être un atout majeur pour cela ».*

Chaque seconde coûte

Selon le rapport 2023, les organisations étudiées qui déploient pleinement l'IA et l'automatisation dans le domaine de la cybersécurité ont vu leur cycle de vie des violations raccourci de 108 jours en moyenne par

rapport aux organisations qui ne déploient pas ces technologies - et ont connu des coûts d'incident nettement inférieurs. Les organisations étudiées qui ont largement déployé l'IA et l'automatisation dans le domaine de la sécurité ont constaté, en moyenne, une réduction de près de 1,8 million de dollars des coûts liés aux violations de données par rapport aux organisations qui n'ont pas déployé ces technologies, ce qui représente la plus grande économie de coûts identifiée par l'étude.

Dans le même temps, les adversaires ont réduit le temps moyen nécessaire pour mener à bien une attaque par ransomware. Et comme près de 40 % des organisations étudiées n'ont pas encore déployé l'IA et l'automatisation appliquées à la cybersécurité, il existe encore des possibilités considérables pour les organisations d'améliorer les vitesses de détection et de réponse.

Comment réduire le coût d'un ransomware facilement ?

Certaines organisations étudiées hésitent encore à faire appel aux autorités lors d'une attaque par ransomware, car elles pensent que cela ne fera que compliquer la situation. Pour la première fois cette année, le rapport d'IBM a examiné cette question de plus près et a trouvé des preuves du contraire. Les organisations participantes qui n'ont pas fait appel aux autorités ont connu des cycles de vie des violations plus longs de 33 jours en moyenne que celles qui l'ont fait - et ce silence a eu un prix. Les victimes de ransomware étudiées qui n'ont pas fait appel aux autorités ont payé en moyenne 470 000 dollars de plus que celles qui l'ont fait.

Malgré les efforts déployés par les autorités pour collaborer avec les victimes de ransomware, 37 % des personnes interrogées ont choisi de ne pas les faire intervenir. De plus, près de la moitié (47 %) des victimes de ransomware étudiées auraient payé la rançon. Il est clair que les organisations devraient abandonner ces idées fausses sur les ransomwares. Le fait de payer une rançon et d'éviter les autorités ne peut qu'augmenter les coûts de l'incident et ralentir la réponse.

Les équipes de sécurité découvrent rarement les violations elles-mêmes

La détection et la réponse aux menaces ont progressé. Selon l'indice 2023 Threat Intelligence Index d'IBM (rapport sur le paysage mondial des menaces), les défenseurs ont réussi à stopper une plus grande proportion d'attaques par ransomware l'année dernière. Cependant, les attaquants trouvent encore des moyens de passer à travers les mailles du filet de la défense. L'étude indique que seule une violation étudiée sur trois a été détectée par les propres équipes ou outils de sécurité de l'organisation, tandis que 27 % de ces violations ont été révélées par un attaquant et 40 % par une tierce partie neutre telle que les autorités.

Les organisations interrogées qui ont découvert elles-mêmes la violation ont subi des coûts inférieurs de près d'un million de dollars à ceux des organisations dont la violation a été révélée par un pirate (5,23 millions de dollars contre 4,3 millions de dollars). Les violations divulguées par un pirate ont également eu un cycle de vie plus long de près de 80 jours (320 contre 241) par rapport à ceux qui ont identifié la violation en interne. Les importantes économies de temps et d'argent réalisées grâce à la détection précoce montrent que l'investissement dans ces stratégies peut s'avérer payant à long terme.

Parmi les autres conclusions du rapport 2023 d'IBM, on peut citer :

- **Violation de données dans plusieurs environnements** - Près de 40 % des violations de données étudiées ont entraîné la perte de données dans des environnements IT variés, notamment dans les Clouds publics, les Clouds privés et en local, ce qui montre que les attaquants ont pu compromettre plusieurs environnements tout en évitant d'être détectés. Les violations de données étudiées qui ont touché plusieurs environnements à la fois ont également entraîné des coûts de violation plus élevés (4,75 millions de dollars en moyenne).

- **Les coûts des violations dans le secteur de la santé continuent de grimper en flèche** - Les coûts moyens d'une violation étudiée dans le secteur de la santé ont atteint près de 11 millions de dollars en 2023, soit une augmentation de 53 % par rapport à 2020. Les cybercriminels ont commencé à rendre les données volées plus accessibles aux victimes en aval, selon le rapport 2023 X-Force Threat Intelligence Report. Avec les dossiers médicaux comme levier, les acteurs de la menace amplifient la pression sur les organisations victimes de violations pour qu'elles paient une rançon. En fait, dans tous les secteurs d'activité étudiés, les informations d'identification personnelle des clients sont le type d'enregistrement le plus fréquemment violé et le plus coûteux.

- **L'avantage DevSecOps** - Les organisations étudiées dans tous les secteurs d'activité ayant un niveau élevé de DevSecOps ont vu le coût moyen global d'une violation de données inférieur de près de 1,7 million de dollars à celui des organisations étudiées ayant un niveau faible de DevSecOps ou n'utilisant pas ce type d’approche.

- **Les coûts de violation des infrastructures critiques dépassent les 5 millions de dollars** - Les organisations étudiées ayant des infrastructures critiques ont connu une augmentation de 4,5 % des coûts moyens d'une violation par rapport à l'année dernière - passant de 4,82 millions de dollars à 5,04 millions de dollars - soit 590 000 dollars de plus que la moyenne mondiale.

Sources additionnelles :

- Pour télécharger une copie du rapport 2023 sur le coût d'une violation de données : https://www.ibm.com/security/data-breach.
- Pour en savoir plus sur les principales conclusions du rapport, consultez le blog d'IBM Security Intelligence.
- Inscrivez-vous au webinaire 2023 sur le coût d'une violation de données, qui aura lieu le **mardi 1er août 2023, à 17 h 00** en cliquant ici.

- Contactez l'équipe IBM Security X-Force pour une présentation personnalisée des conclusions du rapport : https://ibm.biz/book-a-consult.
- Pour une analyse plus approfondie des recommandations du rapport : Cost of a Data breach Action Guide.

À propos d'IBM Security

IBM Security aide à sécuriser les plus grandes entreprises et les gouvernements du monde entier grâce à un portefeuille intégré de produits et de services de sécurité, infusé de capacités dynamiques d'IA et d'automatisation. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de prévoir les menaces, de protéger les données à mesure qu'elles se déplacent et de réagir avec rapidité et précision sans entraver l'innovation commerciale. Des milliers d'organisations font confiance à IBM en tant que partenaire pour l'évaluation, la stratégie, la mise en œuvre et la gestion des transformations en matière de sécurité. 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

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com

---

[1] The 2023 Cost of a Data Breach Report, conducted by Ponemon Insitute, is sponsored and analyzed by IBM Security.