Communiqués de presse

Rapport IBM : La compromission des comptes d'employés a entraîné les violations de données les plus coûteuses au cours de l'année écoulée

Les données personnelles des clients exposées dans 80 % des violations analysées ; l'IA et l'automatisation réduisent considérablement les coûts

CAMBRIDGE, Massachusetts, le 29 juillet 2020 : IBM Security a annoncé aujourd'hui les résultats d'une étud mondiale examinant l'impact financier des violations de données, révélant que ces incidents coûtent au entreprises 3,86 millions de dollars en moyenne par violation et que la compromission de comptes d'employés e est la cause première la plus coûteuse. Selon une analyse approfondie des violations de données subies par plus d 500 organisations dans le monde, 80 % de ces incidents ont entraîné l'exposition d'informations personnelle identifiables (PII) de clients. Parmi tous les types de données exposées dans ces violations, les données PII de clients étaient également les plus coûteuses pour les entreprises.

Alors que les entreprises accèdent de plus en plus à des données sensibles par le biais de nouvelles méthodes d travail à distance et l'usage du Cloud, le rapport met en lumière les pertes financières que peuvent subir le organisations si ces données sont compromises. Une autre étude d'IBM a révélé que plus de la moitié des employé qui travaillent à domicile depuis peu en raison de la pandémie n'ont pas reçu de nouvelles directives sur la manièr de gérer les PII des clients, malgré l'évolution des risques engendrés par ce changement.

Sponsorisé par IBM Security et réalisé par le Ponemon Institute, le rapport 2020 Cost of a Data Breach Repor (rapport 2020 sur le coût d'une violation de données) est basé sur des entretiens approfondis avec plus de 3 20 professionnels de la sécurité dans des organisations ayant subi une violation de données au cours de l'anné passée.[1] Voici quelques-unes des principales conclusions du rapport de cette année :

- **La Smart Tech réduit de moitié le coût des violations :** Les entreprises qui ont pleinement déployé de technologies d'automatisation de la sécurité (qui utilisent l'Intelligence Artificielle, l'analytique e l'orchestration automatisée pour identifier les événements de sécurité et y répondre) ont subi moins de l moitié des coûts liés aux violations de données par rapport à celles qui n'ont pas déployé ces outils - 2,4 millions de dollars contre 6,03 millions de dollars en moyenne.

- **Une peine supplémentaire pour les informations d'identification compromises :** Dans les cas où de attaquants ont accédé à des réseaux d'entreprise en utilisant des informations d'identification volées o compromises, les entreprises ont vu les coûts liés aux violations de données augmenter de près d'un millio de dollars par rapport à la moyenne mondiale - atteignant 4,77 millions de dollars par violation de données L'exploitation des vulnérabilités de tiers a été la deuxième cause la plus coûteuse des violations malveillante (4,5 millions de dollars) pour ce groupe.

- **Une méga brèche[2] coûte des millions :** Les violations lors desquelles plus de 50 million d'enregistrements ont été compromis ont fait grimper les coûts à 392 millions de dollars, contre 388 million l'année précédente. Les violations où 40 à 50 millions d'enregistrements ont été exposés ont coûté au

entreprises 364 millions de dollars en moyenne, soit une augmentation des coûts de 19 millions de dollars pa rapport au rapport de 2019.

- **Attaques des États nations - Les violations les plus dommageables :** Les violations de données don on pense qu'elles proviennent d'attaques d'États nations ont été les plus coûteuses, par rapport aux autre types de cybercriminels examinés dans le rapport. Les attaques sponsorisées par les États ont coûté e moyenne 4,43 millions de dollars en coûts de violations de données, dépassant à la fois les cybercriminel dont la motivation est financière et les hacktivistes.

« En ce qui concerne la capacité des entreprises à atténuer l'impact d'une violation de données, nous commençon à voir un net avantage détenu par les entreprises qui ont investi dans les technologies automatisées », a déclar **Wendi Whitmore, Vice President, IBM X-Force Threat Intelligence** *. « À l'heure où les entreprises étender leur empreinte numérique à un rythme accéléré et où la pénurie de talents dans le secteur de la sécurité persiste les équipes peuvent être submergées par la sécurisation d'un plus grand nombre de dispositifs, de systèmes et d données. L'automatisation de la sécurité peut aider à résoudre ce problème, en permettant non seulement d réagir plus rapidement aux violations, mais aussi de manière beaucoup plus économique ».*

Les informations d'identification d'employés et les Clouds mal configurés - Point d'entrée de choix des attaquants

Le vol ou la compromission des identifiants et les erreurs de configuration du Cloud sont les causes les plu fréquentes d'une violation malveillante pour les entreprises figurant dans le rapport, représentant près de 40 % de incidents malveillants. Avec plus de 8,5 milliards d'enregistrements exposés en 2019 et des attaquants utilisant de e-mails et des mots de passe précédemment exposés dans une brèche étudiée sur cinq, les entreprises devraien repenser leur stratégie de sécurité en adoptant une approche zero-trust (zéro confiance) - en réexaminant l manière dont elles authentifient les utilisateurs et l'étendue des accès qui leur sont accordés.

De même, la lutte des entreprises contre la complexité de la sécurité - un facteur de coût important en cas d violation - contribue probablement à ce que les mauvaises configurations du Cloud deviennent un problème d sécurité croissant. Le rapport 2020 a révélé que les attaquants utilisaient les mauvaises configurations du Clou pour pénétrer les réseaux dans près de 20 % des cas, ce qui augmente les coûts des violations de plus d'un demi million de dollars pour atteindre 4,41 millions de dollars en moyenne - ce qui en fait le troisième vecteur d'infectio initial le plus cher examiné dans le rapport.

Les attaques sponsorisées par les États sont les plus graves

Bien qu'ils ne représentent que 13 % des violations malveillantes étudiées, les cybercriminels soutenus par un Éta sont le type d'adversaire le plus nuisible selon le rapport 2020, ce qui suggère que les attaques motivées par de raisons financières (53 %) ne se traduisent pas nécessairement par des pertes financières plus élevées pour le entreprises. La nature hautement tactique, la longévité et les manœuvres furtives des attaques soutenues pa l'État, ainsi que les données de grande valeur ciblées, entraînent souvent une compromission plus importante de environnements des victimes, ce qui augmente les coûts des violations à une moyenne de 4,43 millions de dollars.

En fait, les personnes interrogées au Moyen-Orient, une région qui connaît historiquement une proportion plu élevée d'attaques sponsorisées par un État que d'autres parties du monde[3], ont vu leur coût moyen de violatio augmenter de plus de 9 % par an, ce qui les place au deuxième rang des 17 régions étudiées (6,52 millions d dollars). De même, le secteur de l'énergie, l'une des industries les plus fréquemment ciblées par les États-nations a connu une augmentation de 14 % des coûts de violation d'une année sur l'autre, pour une moyenne de 6,3 millions de dollars.

Les technologies de sécurité avancées s'avèrent intelligentes pour les entreprises

Le rapport souligne le fossé grandissant en matière de coûts des violations entre les entreprises qui mettent e œuvre des technologies de sécurité avancées et celles qui sont à la traîne, révélant une différence d'économie d 3,58 millions de dollars pour les entreprises ayant pleinement déployé l'automatisation de la sécurité par rapport celles qui n'ont pas encore déployé ce type de technologie. L'écart de coût s'est accru de 2 millions de dollars alors qu'il était de 1,55 million de dollars en 2018.

Les entreprises ayant participé à l'étude et disposant d'un système de sécurité entièrement automatisé on également fait état d'un temps de réponse beaucoup plus court aux violations, un autre facteur clé de réductio des coûts liés aux violations, selon l'analyse. Le rapport a montré que l'Intelligence Artificielle, le machine learning l'analytique et d'autres formes d'automatisation de la sécurité ont permis aux entreprises de réagir aux violation plus de 27 % plus rapidement que les entreprises qui n'ont pas encore déployé l'automatisation de la sécurité - ce dernières ont besoin en moyenne de 74 jours supplémentaires pour identifier et contenir une violation.

La préparation à la réponse aux incidents (RI) continue également à influencer fortement les conséquence financières d'une violation. Selon le rapport, les entreprises qui ne disposent pas d'une équipe de réponse au incidents ou qui ne testent pas leurs plans de réponse aux incidents supportent des coûts moyens de 5,29 million de dollars en cas de violation, alors que les entreprises qui disposent d'une équipe de réponse aux incidents et qu réalisent des exercices de simulations pour tester leurs plans de réponse aux incidents supportent des coûts de millions de dollars de moins en cas de violation - réaffirmant que la préparation permet un retour su investissement important en matière de cybersécurité.

Voici quelques autres conclusions du rapport de cette année :

- **Le risque lié au travail à distance aura un coût :** Avec des modèles de travail hybrides créant des environnements moins contrôlés, le rapport a constaté que 70 % des entreprises étudiées qui ont adopté le télétravail dans le contexte de la pandémie s'attendent à ce que cela exacerbe les coûts liés aux violations de données.

- **Les RSSIs responsables des violations, malgré un pouvoir de décision limité :** 46 % des personnes interrogées ont déclaré que le RSSI est responsable en dernier ressort de la violation, alors que seulement 27% d'entre elles ont déclaré que le RSSI est le décideur en matière de politique de sécurité et de technologie. Le rapport a révélé que la nomination d'un RSSI était associée à une économie de 145 000 dollars par rapport au coût moyen d'une brèche.

- **La majorité des entreprises assurées contre les risques cyber utilisent les demandes d'indemnisation pour les frais de tiers :** Le rapport a révélé que les violations commises dans les organisations étudiées ayant une cyberassurance coûtent en moyenne près de 200 000 dollars de moins que la moyenne mondiale de 3,86 millions de dollars. En fait, parmi ces organisations qui ont utilisé leur cyberassurance, 51 % l'ont appliquée pour couvrir les honoraires de consultation de tiers et les services juridiques, tandis que 36 % des organisations l'ont utilisée pour les frais de dédommagement des victimes. Seulement 10 % ont utilisé les demandes de remboursement pour couvrir le coût du ransomware ou de l'extorsion.

- **Perspectives régionales et industrielles** : Alors que les États-Unis continuent de connaître les coûts les plus élevés au monde en matière de violations de données, soit 8,64 millions de dollars en moyenne, le rapport a constaté que la Scandinavie a connu la plus forte augmentation d'année en année des coûts liée aux violations, observant une hausse de près de 13 %. Le domaine de la santé a continué à subir les coût moyens de violation les plus élevés, avec 7,13 millions de dollars, soit une augmentation de plus de 10 % pa rapport à l'étude de 2019.

À propos de l'étude

Le rapport annuel sur le coût d'une violation de données est basé sur une analyse approfondie des violations de données réelles survenues entre août 2019 et avril 2020, en tenant compte de centaines de facteurs de coût, don les activités juridiques, réglementaires et techniques, la perte d'image de marque, de clients et de productivité de employés.

Pour télécharger une copie du rapport 2020 sur le coût des violations de données : ibm.com/databreach

Inscrivez-vous au webinaire "2020 Cost of a Data Breach Report" le mercredi 12 août 2020 à 17 h 00 : https://ibm.biz/BdqhMf

A 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 70 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.

---

[1] Report analyzes data breaches occurring between August 2019 and April 2020. Limitations of the report's methodology can be found in the report.

[2] The 2020 Cost of a Data Breach Report examines the cost of a mega breach, namely breaches involving the loss or theft one million records or more, based on a separate analysis of a specific sample.

[3] According to the IBM 2020 X-Force Threat Intelligence Index: https://ibm.biz/downloadxforcethreatindex

Contacts : IBM Gaëlle Dussutour Tél. : + 33 (0)6 74 98 26 92 DUSGA@fr.ibm.com Weber Shandwick pour IBM Robin Legros / Morad Salehi Tél. : + 33 (0)6 68 04 57 83 ibmfrance@webershandwick.com