Communiqués de presse

Une étude d'IBM montre que le coût des violations de données est en hausse et que les répercussions financières sont ressenties depuis des années

Les violations présentent un risque croissant pour les petites entreprises, coûtant jusqu'à 5 % du revenu annuel

CAMBRIDGE, Massachusetts - 03 sept. 2019: L'entité Sécurité d'IBM (NYSE: IBM) a annoncé aujourd'hui les résultats de son étude annuelle sur l'impact financier des violations de données sur les organisations. Selon le rapport, le coût d'une violation de données a augmenté de 12 % au cours des cinq dernières années[1] et coûte désormais 3,92 millions de dollars en moyenne. Ces dépenses croissantes sont représentatives de l'impact financier pluriannuel des violations, de la réglementation accrue et du processus complexe de résolution des attaques criminelles[2].

Les conséquences financières d'une violation de données peuvent être particulièrement graves pour les petites et moyennes entreprises. Dans cette étude, les entreprises de moins de 500 employés ont subi des pertes de plus de 2,5 millions de dollars en moyenne - un montant qui peut potentiellement mettre à mal les petites entreprises, dont le revenu annuel est généralement inférieur ou égal à 50 millions de dollars.

Pour la première fois cette année, le rapport a également examiné l'impact financier à long terme d'une violation de données, concluant que ses effets se font sentir pendant des années.

Bien qu'en moyenne 67 % des coûts liés à une violation de données aient été engagés au cours de la première année suivant la violation, 22 % se sont accumulés au cours de la deuxième année et 11 % plus de deux ans après la violation. Les coûts à long terme étaient plus élevés au cours des deuxième et troisième années pour les organisations œuvrant dans des environnements hautement réglementés, tels que les soins de santé, les services financiers, l'énergie et les produits pharmaceutiques.

« La cybercriminalité représente beaucoup d'argent pour les cybercriminels et, malheureusement, cela représente des pertes considérables pour les entreprises », a déclaré **Wendi Whitmore, Global Lead for IBM X-Force Incident Response and Intelligence Services.** *« Face à la perte ou au vol de plus de 11,7 milliards d'enregistrements au cours des trois dernières années seulement, les entreprises doivent être pleinement conscientes de l'impact financier qu'une violation de données peut avoir sur leur résultat net et se concentrer sur les moyens de réduire ces coûts. »*

Sponsorisé par IBM Security et mené par le Ponemon Institute, le rapport annuel sur le coût d'une violation de données repose sur des entretiens approfondis avec plus de 500 entreprises du monde entier victimes d'une violation au cours de l'année écoulée[3]. L'analyse prend en compte des centaines de facteurs de coûts, dont les activités juridiques, réglementaires

et techniques, entraînant une perte de valeur de la marque, une perte de clients et de productivité des employés. Voici quelques-unes des principales conclusions du rapport de cette année :

- **Les violations malveillantes - plus courantes, plus coûteuses :** Plus de 50% des violations de données dans l'étude résultent de cyberattaques malveillantes et coûtent en moyenne 1 million de dollars de plus aux entreprises que celles d'origine accidentelle.

- **Les «méga-violations» entraînent des méga-pertes** : bien qu'elles soient moins courantes, les violations de plus d'un million d'enregistrements ont coûté aux entreprises 42 millions de dollars de pertes ; et celles de 50 millions d'enregistrements devraient coûter 388 millions de dollars aux entreprises.[4]

- **L'entraînement conduit à la perfection :** les entreprises dotées d'une équipe de réponse aux incidents qui ont également testé de manière approfondie leur plan de réponse aux incidents ont enregistré des coûts de violation de données inférieurs de 1,23 million de dollars en moyenne à ceux des entreprises n'ayant aucune mesure en place.

- **Les violations de données aux États-Unis coûtent 2 fois plus cher :** le coût moyen d'une violation aux États-Unis est de 8,19 millions de dollars, soit plus du double de la moyenne mondiale.

- **Les violations liées à la santé sont celles qui coûtent le plus cher :** Pour la 9ème année consécutive, les organismes de soins de santé ont enregistré le coût le plus élevé pour une violation - près de 6,5 millions de dollars en moyenne (plus de 60% de plus que les autres secteurs de l'étude).

Les violations malveillantes constituent une menace croissante ; Les violations accidentelles demeurent courantes

L'étude a révélé que les violations de données résultant d'une cyberattaque malveillante étaient non seulement la cause première d'une violation, mais aussi la plus coûteuse.

Les violations de données malveillantes coûtent en moyenne 4,45 millions de dollars aux entreprises de l'étude, soit plus d'un million de dollars de plus que celles provenant de causes accidentelles telles que des problèmes de système et des erreurs humaines. Ces violations constituent une menace croissante, car le pourcentage d'attaques malveillantes ou criminelles en tant que cause fondamentale des violations de données dans le rapport a grimpé de 42% à 51% au cours des six dernières années de l'étude (soit une augmentation de 21%).

Ceci dit, les violations involontaires dues à des erreurs humaines et à des problèmes de système étaient toujours à l'origine de près de la moitié (49%) des violations de données dans le rapport, coûtant respectivement 3,50 et 3,24 millions de dollars aux entreprises. Ces violations dues à des erreurs humaines et à des erreurs matérielles représentent une opportunité d'amélioration qui peut être adressée par le biais de formations de sensibilisation du personnel à la sécurité, d'investissements technologiques et de services de test permettant de détecter rapidement les violations accidentelles. L'un des principaux sujets de préoccupation est la mauvaise configuration des serveurs Cloud, qui a contribué à l'exposition de 990 millions d'enregistrements en 2018, représentant 43% de tous les enregistrements perdus cette année selon l'indice X-Force Threat Intelligence d'IBM[5].

La réponse après violation demeure le plus gros économiseur de coût

Au cours des 14 dernières années, le Ponemon Institute a examiné les facteurs qui augmentent ou réduisent le coût d'une violation et a constaté que la rapidité et l'efficacité avec laquelle une entreprise répond à une violation ont un impact significatif sur le coût global.

Le rapport de cette année a révélé que le cycle de vie moyen d'une violation était de 279 jours, les sociétés prenant 206 jours pour identifier une violation après son apparition et 73 jours supplémentaires pour la contenir. Toutefois, les entreprises de l'étude qui ont réussi à détecter et contenir une violation en moins de 200 jours ont dépensé 1,2 million de dollars de moins sur le coût total d'une violation.

En mettant l'accent sur la réponse à incidents, on peut réduire le temps de réponse des entreprises. L'étude a révélé que ces mesures avaient également une corrélation directe avec les coûts globaux. Avoir une équipe de réponse à incidents en place et faire des tests approfondis des plans de réponse à incidents figuraient parmi les trois principaux facteurs de réduction des coûts examinés dans l'étude. Les entreprises qui appliquaient ces deux mesures avaient en moyenne 1,23 million de dollars de moins en coût total pour une violation de données que celles qui n'en avaient aucune en place (3,51 millions de dollars contre 4,74 millions de dollars).

Parmi les autres facteurs ayant une incidence sur le coût d'une violation pour les entreprises de l'étude, notons :

- Le nombre d'enregistrements compromis : les violations de données coûtent aux entreprises environ **150 dollars par enregistrement** perdu ou volé.

- Les entreprises qui ont entièrement déployé des **technologies d'automatisation de la sécurité** ont divisé le coût d'une violation par 2 (moyenne de 2,65 millions de dollars) par rapport à celles qui n'avaient pas déployé ces technologies (moyenne de 5,16 millions de dollars).

- **Le recours généralisé au chiffrement** constituait également un facteur de réduction des coûts considérable, réduisant de 360 000 dollars le coût total d'une violation.

- **Les violations émanant d'une tierce partie -** telle qu'un partenaire ou un fournisseur - coûtent aux entreprise 370 000 dollars de plus que la moyenne, soulignant la nécessité pour les sociétés de contrôler de près la sécurité des sociétés avec lesquelles elles font affaire, d'aligner les standards de sécurité et de surveiller activement l'accès des tiers.

Les tendances régionales et sectorielles

L'étude a également examiné le coût des violations de données dans différents secteurs et régions, en concluant que les violations de données aux États-Unis sont beaucoup plus onéreuses - coûtant 8,19 millions de dollars, soit plus du double de la moyenne des entreprises mondiales étudiées. Le coût des violations de données aux États-Unis a augmenté de 130% au cours des 14 dernières années de l'étude ; comparativement à 3,54 millions de dollars dans l'étude de 2006.

En outre, les organisations du Moyen-Orient ont enregistré le nombre moyen le plus élevé d'enregistrements volés avec près de 40 000 enregistrements volés par incident (comparé à une moyenne mondiale d'environ 25 500).

Pour la 9ème année consécutive, les organisations de soins de santé incluses dans l'étude présentaient les coûts les plus

élevés associés aux violations de données. Le coût moyen d'une violation dans le secteur des soins de santé s'élevait à près de 6,5 millions de dollars, soit 60% de plus que la moyenne intersectorielle.

Données françaises

- 10 ans de données historiques
- Au total, 32 entreprises françaises ont participé à l'étude de cette année
- 3,85 millions d'euros : c'est le coût total moyen d'une violation de données, ce qui représente une augmentation de 8,39% par rapport à l'année précédente
- 145 euros : c'est le coût par enregistrement perdu ou volé, ce qui représente une augmentation de 3,51% par rapport à l'année précédente
- L'origine de 56% des violations de données était des attaques malveillantes ou criminelles
- Le délai moyen d'identification d'une violation de données est passé de 210 à 225 jours
- Le délai moyen pour contenir une violation de données est passé de 75 à 87 jours

Télécharger le rapport complet et s'inscrire au webinaire

Cliquez ici pour afficher le rapport completdu coût d'une violation de données pour 2019 (glisser vers le bas de la page avec la souris et cliquer sur « Explore the full findings »).

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] Comparaison du coût global moyen d'une violation de données entre le rapport de 2014 et le rapport de 2019.

[2] Analyse d'IBM basée sur les données du rapport "Coût d'une violation de données".

[3] Les limites du rapport et les méthodologies employées se trouvent dans le rapport complet.

[4] Les calculs du coût des violations majeures étendent l'analyse de 14 entreprises en appliquant une approche de Monte-Carlo pour généraliser ces résultats.

[5] Indice IBM X-Force Threat Intelligence 2019

Contact(s) relations externes

IBM

Gaëlle Dussutour Tel. : + 33 (0)1 58 75 17 96 dusga@fr.ibm.com

Weber Shandwick pour IBM

Eric Chauvelot / Morad Salehi Tél. : + 33 (0) 1 47 59 56 57 / 33 (0) 6 89 59 12 54 ibmfrance@webershandwick.com