Communiqués de presse

IBM et Ponemon Institute : le coût d'une violation de données a chuté de 10% dans le monde en 2017

Le coût aux États-Unis a continué à augmenter alors qu'il a baissé en Europe; Les différences réglementaires pourraient fortement impacter les coûts d'une violation

CAMBRIDGE, MA - 20 juin 2017: L'entité sécurité d'IBM a annoncé les résultats d'une étude mondiale explorant les implications et les effets des violations de données sur les entreprises d'aujourd'hui. Sponsorisée par IBM Security et menée par le Ponemon Institute, l'étude a révélé que le coût moyen d'une violation de données était de 3,62 millions de dollars dans le monde, soit une baisse de 10% depuis les résultats de 2016. C'est la première fois depuis la création de l'étude mondiale qu'il y a une baisse globale du coût. Selon l'étude, ces violations de données ont coûté, en moyenne, aux entreprises 141 dollars par donnée perdue ou volée.

En analysant les 11 pays et deux régions étudiés dans le rapport, l'entité sécurité d'IBM a identifié une corrélation étroite entre la réponse aux exigences réglementaires en Europe et le coût global d'une violation de données. Les pays européens ont affiché une diminution de 26% du coût total d'une violation de données par rapport à l'étude de l'an dernier. Les entreprises en Europe opèrent dans un environnement réglementaire plus centralisé, tandis que les entreprises aux États-Unis (U.S.) ont des exigences uniques, avec 48 des 50 États disposant de leurs propres lois sur les violations de données. Répondre à une multitude d'exigences réglementaires et les signaler à, potentiellement, des millions de consommateurs peut se révéler être une tâche extrêmement coûteuse et exigeant beaucoup de ressources.

Selon l'étude 2017 sur le coût d'une violation des données : vue d'ensemble, les « défauts de conformité » et les « pressions à notifier » figurent parmi les cinq principales raisons pour lesquelles le coût d'une violation a augmenté aux États-Unis. Une comparaison de ces facteurs laisse entendre que les activités réglementaires aux États-Unis pourraient coûter aux entreprises davantage par donnée qu'en Europe. Par exemple, les défauts de conformité coûtent aux entreprises américaines 48% de plus qu'aux entreprises européennes, tandis que la pression à notifier coûte aux entreprises américaines 50% de plus qu'aux entreprises européennes. En outre, les sociétés américaines ont déclaré avoir payé plus de 690 000 $ en moyenne pour les coûts de notification liés à une violation - soit plus du double du montant de n'importe quel autre pays interrogé dans le rapport.

« Les nouvelles exigences réglementaires telles que le GDPR en Europe représentent à la fois un défi et une opportunité pour les entreprises cherchant à mieux gérer leur réponse aux violations de données », a déclaré ***Wendi Whitmore, Global Lead, IBM X-Force Incident Response & Intelligence Services (IRIS). «*** *Identifier rapidement ce qui s'est passé, ce à quoi l'attaquant a accédé et comment contenir et supprimer son accès est plus important que jamais. En tenant compte de cela, il est essentiel d'avoir un plan complet de réponse aux incidents en place, afin qu'une organisation qui fait face à un incident, puisse répondre rapidement et efficacement. »*

Le coût d'une violation de données ne baisse pas partout

Dans l'étude mondiale de 2017, le coût global d'une violation de données a diminué pour s'établir à 3,62 millions de dollars, en baisse de 10% par rapport aux 4 millions de dollars de l'an dernier. Cependant, de nombreuses régions ont connu une augmentation d'une violation de données - par exemple, le coût d'une violation des données aux États-Unis était de 7,35 millions de dollars, soit une augmentation de 5% par rapport à l'année dernière. Cependant, les États-Unis n'étaient pas le seul pays à subir une augmentation des coûts en 2017.

- **Les pays non européens ont été confrontés à une augmentation des coûts :** les organisations au Moyen-Orient, au Japon, en Afrique du Sud et en Inde ont tous connu une augmentation des coûts en 2017 par rapport aux coûts moyens des dernières années.
- **Les pays européens ont connu une diminution majeure des coûts :** l'Allemagne, la France, l'Italie et le Royaume Uni ont connu des baisses significatives par rapport aux coûts moyens des quatre dernières années ainsi que l’Australie, le Canada et le Brésil.

Par rapport aux autres régions, les entreprises américaines ont connu les violations de données les plus coûteuses du rapport 2017.

- Le Moyen-Orient arrive juste derrière les Etats-Unis, avec un coût moyen d'une violation de données de 4,94 millions de dollars - augmentation de plus de 10% par rapport à l'année précédente.
- Le Canada était le troisième pays avec un coût moyen de violations de données de 4,31 millions de dollars.
- Au Brésil, en revanche, les violations de données étaient les moins coûteuses au global, puisqu’elles n’ont représenté que 1,52 millions de dollars.

Le temps c’est de l'argent : contenir les violations de données

Pour la troisième année consécutive, l'étude a révélé que le fait d’avoir une équipe de réponse aux incidents (IR) en place a considérablement réduit le coût d'une violation de données, en faisant économiser plus de 19$ par perte ou vol de donnée. La vitesse à laquelle une violation peut être identifiée et contenue est en grande partie due à l'utilisation d'une équipe IR et au fait d’avoir un plan formalisé de réponse aux incidents. Les équipes IR peuvent aider les organisations à faire face plus aisément aux difficultés rencontrées pour contenir une violation de données et par conséquent minimiser les pertes.

Selon l'étude, la rapidité avec laquelle une organisation peut contenir des incidents de violation de données a un impact direct sur les conséquences financières. Le coût d'une violation des données était en moyenne près d'un million de dollars inférieur pour les entreprises capables de contenir une violation de données en moins de trente jours par rapport à celles qui ont mis plus de temps. La rapidité de réponse va devenir de plus en plus critique avec le GDPR qui sera mis en œuvre en mai 2018, et qui exigera que les organisations qui ont des activités en Europe signalent des violations de données dans les 72 heures au risque de faire face à des amendes allant jusqu'à 4% de leur chiffre d'affaires global annuel.

Compte-tenu de ces économies considérables, l'étude a révélé qu'il y a une marge d'amélioration pour les entreprises en ce qui concerne le temps d'identification et de réponse à une violation. En moyenne, les organisations ont pris plus de six mois pour identifier une violation et plus de 66 jours supplémentaires pour la contenir une fois découverte.

Autres principales conclusions issues du rapport 2017 sur les violations de données

- **Par industrie, les infractions liées au domaine de la santé sont les plus coûteuses :** pour la septième année consécutive, le domaine de la santé est en haut de la liste en tant qu'industrie qui subit des violations de données les plus coûteuses. Les violations de données de santé coûtent aux organisations 380$ par donnée, plus de 2,5 fois la moyenne mondiale dans les industries (141 $ par donnée).
- **Principaux facteurs augmentant le coût d'une violation :** l'implication de tiers dans une violation des données a été le principal facteur contribuant à une augmentation du coût d'une violation des données, qui a cru de 17$ par donnée. Les entreprises doivent évaluer la posture de sécurité de leurs fournisseurs tiers - de la paie aux fournisseurs de cloud en passant par le CRM - afin d'assurer la sécurité des données des employés et des clients.
- **Les principaux facteurs réduisant le coût d'une violation :** la réponse aux incidents, le cryptage et la formation ont été les facteurs qui se sont révélés avoir le plus d'impact sur la réduction du coût d'une violation de données. Le fait d'avoir une équipe de réponse aux incidents en place a entraîné une réduction de 19$ du coût par donnée perdue ou volée, vient ensuite l'utilisation étendue du cryptage (réduction de 16$ par donnée) et la forte sensibilisation des employés (réduction de 12,50$ par donnée).
- **L'impact positif de l'orchestration de la résilience :** les programmes de continuité des opérations réduisent considérablement le coût d'une violation de données. Le coût global moyen d'une violation de données par jour est estimé à 5 064$ dans l'étude de cette année. Les entreprises qui ont un processus de reprise d'activité après sinistre manuel ont eu un coût moyen estimé à 6 101 $ par jour. En revanche, les entreprises qui déploient un processus automatisé de reprise d'activité après sinistre qui fournit une orchestration de résilience ont eu un coût moyen beaucoup plus bas par jour de l'ordre de 4 041$. Cela représente une différence nette de 39% (ou une économie de coûts de 1 699$ par jour).

Révélation du coût d'une violation de données

L'étude annuelle sur le coût d'une violation de données examine les coûts à la fois directs et indirects pour les entreprises dans le cas d'un incident unique de violation de données. Grâce à des entretiens poussés avec plus de 410 entreprises dans 13 pays ou régions, l'étude tient compte des coûts associés aux activités de réponse à la violation, ainsi que les dommages à la réputation et la valeur du chiffre d'affaire perdue.

« Les violations de données et les implications associées continuent à être une triste réalité pour les entreprises d'aujourd'hui », a déclaré le ***Dr Larry Ponemon****. « D'année en année, nous constatons l'énorme fardeau financier auquel les entreprises sont confrontées suite à une violation de données. Les détails du rapport illustrent les facteurs qui influent sur le coût d'une violation de données et, dans le cadre de la stratégie globale de sécurité d'une organisation, les entreprises devraient tenir compte de ces facteurs car ils impactent la stratégie globale de sécurité et les investissements continus dans la technologie et les services. »*

Télécharger les rapports complets et inscrivez-vous au webinar

Pour télécharger l'étude 2017 sur le coût d'une violation des données : vue d'ensemble : https://www.ibm.com/security/data-breach/

Des rapports spécifiques aux différents pays sont également disponibles pour la France, les États-Unis, le Royaume-Uni, l'Allemagne, l'Australie, le Brésil, le Japon, l'Italie, l'Inde, la péninsule arabique (Émirats arabes unis et Arabie Saoudite), le Canada, l'Afrique du Sud et, pour la première fois, la région de l'Asie du Sud-Est (Singapour, Indonésie, Philippines et Malaisie).

Pour explorer et interagir avec les résultats du rapport 2017, accédez à IBM Security Data Breach Calculator, un outil interactif qui vous permet de manipuler les données du rapport et de visualiser le coût d'une violation de données à travers les sites et les industries et de comprendre comment différents facteurs influent sur les coûts liés à la violation.

Pour vous inscrire au webinar IBM Security et Ponemon Institute "Comprendre les violations de sécurité actuelles : l'étude sur le coût d'une violation de données 2017 du Ponemon Institute" qui se tiendra le 26 juin 2017 à 17h00 heure française : [URL à venir]

A propos d'IBM Security

IBM Security offre l'une des gammes de produits et services de sécurité pour entreprises les plus performantes 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 35 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 3000 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.

Contact(s) relations externes

IBM

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

Text100 pour IBM

Sophie Barnabé Tél. : + 33 (0) 6 68 58 85 31Sophie.barnabe@text100.fr