Communiqués de presse

Etude IBM et Ponemon Institute : les coûts liés à la violation des données atteignent désormais 4 millions de dollars par incident

Les résultats montrent que le temps c'est de l'argent. Des équipes dédiées pour répondre aux incidents permettent des économies de coûts significatives

Paris - 15 juin 2016: La division sécurité d'IBM (NYSE: IBM) présente aujourd'hui les résultats d'une étude mondiale analysant l'impact financier des violations de données sur la rentabilité d'une entreprise. Commandée par IBM et réalisée par l'Institut Ponemon, l'étude révèle que le coût moyen d'une violation de données pour les entreprises interrogées a augmenté, atteignant 4 millions de dollars, ce qui représente une augmentation de 29% depuis 2013.

Les incidents liés à la cybersécurité continuent à croître en volume et en sophistication, avec 64% d'incidents de sécurité supplémentaires signalés en 2015 par rapport à 20141. Comme ces menaces deviennent plus complexes, le coût pour les entreprises continue à augmenter. En fait, l'étude révèle que les entreprises perdent 158 dollars par donnée compromise. Les violations de données dans les industries fortement réglementées étaient encore plus coûteuses, la santé atteignant 355 dollars par donnée – soit 100 dollars de plus qu'en 2013.

Un manque de réactivité et de planification coûte des millions aux entreprises

Selon l'étude, s'appuyer sur une équipe de réponse aux incidents était de loin le facteur le plus important pour réduire les coûts d'une violation de données permettant ainsi aux entreprises d'économiser près de 400 000 dollars en moyenne (soit 16 dollars par donnée). En fait, les activités de réponse aux incidents telles que la recherche de la cause, la communication, les dépenses juridiques et de remise en conformité représentent 59%2 du coût d'une violation de données. Ces coûts élevés sont en partie liés au fait que 70%3 des responsables de la sécurité américains signalent qu'ils ne disposent pas de stratégie de réponse aux incidents.

Le processus de réponse à une violation est extrêmement complexe et prend beaucoup de temps s'il n'est pas correctement planifié. Parmi les activités requises, une entreprise doit :

- Travailler avec le service informatique ou des experts en sécurité externes, afin d'identifier rapidement la source de la violation et arrêter la fuite de données
- Divulguer la violation aux entités gouvernementales/règlementaires adéquates, en respectant des délais spécifiques pour éviter les amendes potentielles

- Communiquer sur la fuite de données aux clients, partenaires et actionnaires
- Mettre en place toute assistance téléphonique et services de surveillance nécessaires pour les clients touchés

Chacune de ces étapes nécessite un temps d'engagement considérable de la part des membres du personnel, les éloignant de leurs responsabilités habituelles et gaspillant de précieuses ressources humaines pour l'entreprise.

Les équipes de réponse aux incidents peuvent accélérer et rationaliser le processus de réponse à une violation, en tant qu'experts de ce que l'entreprise doit faire quand elle est compromise. Ces équipes traitent tous les aspects des opérations de sécurité et du cycle de vie de la réponse aux incidents, de l'aide à la résolution de ce dernier, à la réponse aux problèmes de conformité tant sectoriels que légaux. De plus, les technologies de réponse aux incidents peuvent automatiser ce processus pour réduire les temps de réponse et améliorer l'efficacité.

L'étude révèle également que plus cela prend du temps de détecter et contenir une violation de données, plus sa résolution est coûteuse. Alors que les violations qui ont été identifiées en moins de 100 jours coûtent aux entreprises une moyenne 3,23 millions de dollars, les violations détectées après 100 jours coûtent 1 million de dollars de plus en moyenne (4,38 millions de dollars).

Le temps moyen pour identifier une faille est estimé à 201 jours, et le délai moyen pour contenir une violation de donnée est estimé à 70 jours.

L'étude révèle que les entreprises qui ont prédéfini des processus de gestion de la continuité des opérations (BCM : Business Continuity Management) trouvent et traitent les failles de sécurité plus rapidement, les découvrant 52 jours plus tôt et les traitant en 36 jours de moins que les entreprises sans BCM 4.

Analyse du coût d'une violation de données

L'étude sur le coût annuel de la violation de données examine à la fois les coûts directs et indirects pour les entreprises qui font face à une seule violation de données. Grâce à des entretiens approfondis auprès de 400 entreprises à travers le monde, l'étude présente les coûts associés aux activités de réponse aux violations, ainsi

que les dommages sur la réputation et le coût des pertes commerciales.

« Au cours des nombreuses années passées à étudier la violation de données de plus de 2000 entreprises de tous secteurs, nous voyons qu'elles ont maintenant un coût commercial, ce qui est conforme à l'ère de la cybercriminalité actuelle », déclare le ***Dr Larry Ponemon****. « C'est un coût permanent que les entreprises doivent être prêtes à traiter et à intégrer dans leurs stratégies de protection des données.»*

Pour plus de détails sur l'étude, le rapport complet est disponible sur IBM X-Force Research Library.

Des rapports par 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 région arabe (Emirats Arabe Unis et l'Arabie Saoudite), le Canada et l'Afrique du Sud.

Cette année, IBM a augmenté son investissement sur le marché de la réponse aux incidents avec l'acquisition de Resilient Systems. La plateforme de réponse aux incidents de Resilient (IRP : Incident Response Platform) permet aux équipes de sécurité d'analyser, de réagir et d'atténuer les incidents plus rapidement et plus efficacement. La nouvelle version de la plateforme, annoncée aujourd'hui, comprend Resilient Incident Vizualisation, qui affiche graphiquement les relations entre les indicateurs de compromis (IOCs : Indicators of compomise) et les incidents qui ont lieu dans l'environnement d'une entreprise.

« Le temps, les efforts et les coûts auxquels sont confrontés les entreprises à la suite d'une violation de données peuvent être dévastateurs, et malheureusement la plupart d'entre elles ne disposent pas encore d'une stratégie pour faire face à cela de manière efficace », déclare ***Ted Julian, Vice-President Resilient an IBM Company****. « Tandis que le risque est inévitable, avoir une stratégie coordonnée et automatisée de réponse aux incidents, ainsi qu'un accès aux bonnes ressources et compétences, peut influer sur l'importance de l'impact d'un événement de sécurité sur une entreprise. »*

IBM a également lancé récemment IBM X-Force Incident Response Services, qui comprend des services de conseil et de gestion de la sécurité pour aider les clients à gérer tous les aspects des réponses à une violation de données.

[1] X-Force IBM Cyber Security Intelligence Index, April 2016

2 2016 Cost of Data Breach Study: Global Analysis, June 2016

3 The Cyber Resilient Organization: Learning to Thrive Against Threats, Ponemon Institute, 2015

4 2016 Cost of Data Breach Study: Impact of Business Continuity Management

A propos d'IBM Security

IBM Security propose un portefeuille de solutions de sécurité pour les entreprises parmi les plus avancés et les plus intégrés. Ce portefeuille est supporté par IBM X-Force, organisation de recherche connue mondialement et permet aux organisations de gérer efficacement les risques et de se défendre contre les menaces émergentes. IBM dispose d'une organisation de recherche et développement et de mise en œuvre parmi les plus importantes au monde, gère 20 milliards d'événements de sécurité par jour dans plus de 130 pays et possède plus de 3000 brevets de sécurité.

Pour plus d'informations : www.ibm.com/security/fr/fr

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

A propos d'IBM Resiliency Services

IBM Resiliency Services propose un portefeuille novateur de solutions et services de résilience, incluant la gestion de la continuité des opérations, qui aborde concrètement tous les aspects liés à la perturbation des opérations. Aujourd'hui, plus de 6000 professionnels d'IBM Resiliency construisent, déploient et gèrent des capacités cloud de pointe pour vous aider à maintenir la continuité des opérations et à améliorer la résilience globale de votre organisation. Pour plus d'informations, visitez le site http://ibm.co/1cqLDOz et suivez @IBMServices.