Communiqués de presse

Étude IBM : répondre aux incidents de cybersécurité reste un défi majeur pour les entreprises

77% des entreprises interrogées ne disposent pas de plans de réponse aux incidents appropriés ; alors que 69% déclarent que le financement pour la cyber-résilience est insuffisant

CAMBRIDGE, MA - 15 mars 2018: L'entité sécurité d'IBM (NYSE: IBM) a annoncé aujourd'hui les résultats d'une étude mondiale explorant les facteurs et les défis d'une entreprise cyber résiliente. L'étude a été réalisée par le Ponemon Institute et sponsorisée par IBM Resilient. Elle a révélé que 77% des personnes interrogées admettent ne pas avoir de plan formel de réponse aux incidents de cybersécurité (CSIRP) appliqué uniformément dans l'ensemble de leur entreprise. Près de la moitié des 2800 personnes interrogées ont indiqué que leur plan de réponse aux incidents est soit informel / ad hoc, soit totalement inexistant.

Malgré ce manque de planification officielle, 72% des entreprises déclarent se sentir plus cybers résilientes aujourd'hui qu'elles ne l'étaient l'an dernier. Les entreprises fortement résilientes (61%) attribuent leur confiance à leur capacité d'embaucher du personnel qualifié - mais les entreprises ont besoin à la fois de la technologie et des personnes pour être cyber résilientes.

En fait, 60% des personnes interrogées considèrent le manque d'investissement dans l'intelligence artificielle et le machine learning comme le principal obstacle à la cyber résilience.

Cette confiance peut sembler déplacée, l'analyse révélant que 57% des personnes interrogées ont déclaré que le temps de résolution d'un incident a augmenté, tandis que 65% ont indiqué que la gravité des attaques avait augmenté. Ces domaines représentent certains des facteurs clés ayant une incidence sur la cyber-résilience globale. Ces problèmes sont aggravés par le fait que seulement 31% des personnes interrogées disposent d'un budget adéquat consacré à la cyber résilience et qu'ils rencontrent des difficultés pour retenir et embaucher des professionnels de la sécurité informatique (77%).

« Les entreprises peuvent se sentir plus cyber résilientes aujourd'hui, et la principale raison en est le fait d'embaucher du personnel qualifié », a déclaré **Ted Julian, Vice-Président Product Management et cofondateur d'IBM Resilient.** *« Avoir le bon personnel en place est essentiel, mais les équiper des outils les plus modernes pour améliorer leur travail est tout aussi important. Un plan de réponse qui orchestre l'intelligence humaine avec l'intelligence artificielle est la seule façon pour les équipes de sécurité d'anticiper la menace et d'améliorer globalement la cyber résilience ».*

L'absence de CSIRP cohérent est une tendance persistante chaque année, en dépit d'une constatation clé tirée de l'étude d'IBM sur le coût d'une violation de données de 2017. Le coût d'une violation de données a été inférieur de près de 1 million de dollars en moyenne lorsque les entreprises ont pu contenir la violation en moins de 30 jours – ce qui démontre la valeur et

l'importance d'avoir un CSIRP efficace.

Réalisée par le Ponemon Institute et sponsorisée par IBM Resilient, "The 2018 Cyber Resilient Organization" (« L'entreprise cyber résiliente de 2018 ») est la troisième étude de référence annuelle sur la Cyber Résilience - la capacité d'une entreprise à maintenir son objectif principal et son intégrité face aux cyberattaques. L'enquête mondiale présente des informations provenant de plus de 2 800 professionnels de la sécurité et de l'informatique du monde entier, notamment des États-Unis, du Royaume-Uni, de la France, de l'Allemagne, du Brésil, de l'Asie-Pacifique, du Moyen-Orient et de l'Australie.

« Se concentrer sur quelques domaines cruciaux peut faire une grande différence en ce qui concerne la cyber résilience », a déclaré le **Dr Larry Ponemon***. « S'assurer que la fonction de sécurité est dotée d'un plan de réponse aux incidents, du personnel et d'un budget adéquats mènera à une meilleure posture de sécurité et à une meilleure cyber résilience globale. »*

Vous pouvez télécharger le résumé de ces résultatsici.

Les autres points à retenir de l'étude sont les suivants :

- **La dotation en personnel pour les activités liées à la cyber résilience est inadéquate**
  - Le deuxième plus grand obstacle à la cyber résilience était le manque de personnel qualifié dédié à la cybersécurité.
  - 29% des personnes interrogées ont déclaré avoir une dotation idéale pour atteindre la cyber résilience.
  - 50% affirment que l'actuel RSSI ou responsable de la sécurité dans leur entreprise est en place depuis trois ans ou moins. 23% déclarent ne pas avoir de RSSI ou de responsable de la sécurité.

- Les entreprises ne sont pas prêtes pour le RGPD
  - Le Règlement Général sur la Protection des Données (RGPD) entre en vigueur en mai 2018 et obligera les entreprises à mettre en place un plan de réponse aux incidents.
  - 77% des personnes interrogées n'ont pas de plan de réponse aux incidents appliqué de manière cohérente dans l'ensemble de l'entreprise.
  - La plupart des pays déclarent ne pas avoir confiance dans leur capacité à se conformer au RGPD.

Télécharger les rapports complets et s’inscrire au webinar

Pour en savoir plus sur les résultats complets de l'étude, téléchargez"The Third Annual Study on the Cyber Resilient Organisation"

Inscrivez-vous à notre prochain webinar :“Growing Your Organization’s Cyber Resilience in 2018,”qui aura lieu le 27 mars 2018 à 16h00.

A propos d'IBM Resilient

IBM Resilient est le leader de l'industrie pour accompagner les entreprises à faire face à toute cyberattaque ou crise métier. La plateforme IRP (Incident Response Platform) éprouvée d'IBM Resilient permet aux équipes de sécurité d'analyser, d'atténuer et de remédier aux incidents plus rapidement, plus intelligemment et plus efficacement. L'IRP Resilient est la seule plateforme complète d'orchestration et d'automatisation IR du secteur, permettant aux équipes d'intégrer et d'aligner les personnes, les processus et les technologies dans un seul et même centre de réponse aux incidents. Avec Resilient, les équipes de sécurité peuvent disposer des meilleures capacités de réponse. IBM Resilient compte 300 clients mondiaux, dont 60 des sociétés du Fortune 500, et des centaines de partenaires dans le monde. Pour en savoir plus : www.resilientsystems.com.

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 8000 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

Amélie Chipaux Tél. : + 33 (0) 6 62 49 20 50amelie.chipaux@text100.fr