Communiqués de presse

Étude IBM : Plus de la moitié des organisations disposant de plans de réponse aux incidents de cybersécurité omettent de les mettre à l'essai

L’utilisation de l'automatisation a amélioré la détection et le confinement des cyberattaques de près de 25% ; Près de la moitié des organisations ne sont pas conformes au RGPD

Cambridge, MA - 11 avr. 2019: L’entité sécurité d’IBM (NYSE: IBM) a annoncé aujourd'hui les résultats d'une étude mondiale sondant le niveau de préparation des organisations en matière de résistance à une cyberattaque et de récupération ensuite. L'étude, menée par le Ponemon Institute et sponsorisée par IBM Resilient, a révélé qu'une grande majorité des organisations interrogées ne sont toujours pas prêtes à répondre de façon adéquate aux incidents de cybersécurité, 77% des personne interrogées indiquant qu'ils n'ont pas de plan de réponse aux incidents de cybersécurité appliqué de manière cohérente dans l’ensemble de l'organisation.

Bien que des études montrent que les organisations qui peuvent réagir rapidement et efficacement pour contenir une cyberattaque dans un délai de 30 jours économisent en moyenne plus d'un million de dollars sur le coût total d'une violation de données1, les lacunes en matière de planification adéquate de la réponse aux incidents de cybersécurité sont restées constantes au cours des quatre dernières années de l'étude. Parmi les organisations interrogées qui ont un plan en place, plus de la moitié (54%) ne le mettent pas à l'essai régulièrement, ce qui peut les rendre moins prêtes à gérer efficacement les processus complexes et la coordination qui doivent être mis en œuvre suite à une attaque.

Les difficultés auxquelles sont confrontées les équipes de cybersécurité dans la mise en œuvre d'un plan de réponse aux incidents de cybersécurité ont également eu un impact sur la conformité des organisations au règlement général sur la protection des données (RGPD). Près de la moitié des personnes interrogées (46%) affirment que leur organisation n’est pas encore pleinement conforme au RGPD, alors même que le premier anniversaire de la législation approche à grands pas.

"Echouer à planifier est un plan pour échouer lorsqu'il s'agit de répondre à un incident de cybersécurité. Ces plans doivent faire l'objet de tests de résistance réguliers et ont besoin du soutien total du conseil d'administration pour investir dans les compétences, les processus et les technologies nécessaires pour maintenir un tel programme ", a déclaré **Ted Julian, Vice President of Product Management and Co-Founder, IBM Resilient**. *"Quand une bonne planification s'accompagne d'investissements dans l'automatisation, on voit des organisations capables d'économiser des millions de dollars pendant une violation."*

Voici d'autres points à retenir de l'étude :

- **L'automatisation de la réponse toujours émergeante** - moins d'un quart des personnes interrogées ont déclaré que leur organisation utilise de manière significative les technologies d'automatisation, telles que la gestion des identités et l'authentification, les plateformes de réponse aux incidents et les outils de gestion des informations et événements de sécurité (SIEM), dans leur processus de réponse.

- **Les compétences sont toujours insuffisantes** - seuls 30% des personnes interrogées ont indiqué que la dotation en personnel dans le domaine de la cybersécurité est suffisante pour atteindre un niveau élevé de cyber-résilience.

- **Confidentialité et cybersécurité sont étroitement liées** - 62% des personnes interrogées ont indiqué que l'harmonisation des rôles en matière de confidentialité et de cybersécurité est essentielle ou très importante pour assurer la cyber-résilience au sein de leurs organisations.

L'automatisation toujours émergeante

Pour la première fois, l'étude de cette année a mesuré l'impact de l'automatisation sur la cyber-résilience. Dans le contexte de cette recherche, l'automatisation fait référence aux technologies de sécurité permettant d'augmenter ou de remplacer l'intervention humaine dans l'identification et le confinement des cyber-exploits ou violations. Ces technologies reposent sur l'intelligence artificielle, le machine learning, l'analytique et l'orchestration.

Lorsqu'on leur a demandé si leur organisation tirait parti de l'automatisation, seuls 23% des personnes interrogées ont répondu qu'ils étaient des utilisateurs importants, tandis que 77% ont répondu que leur organisation n'utilisait l'automatisation que modérément, faiblement ou pas du tout. Les organisations qui utilisent l'automatisation de manière significative évaluent leur capacité à prévenir (69% contre 53%), à détecter (76% contre 53%), à répondre (68% contre 53%) et à contenir (74% contre 49%) une cyberattaque comme étant plus élevée que l'échantillon global des personnes interrogées.

Selon l'étude 2018 sur les coûts cachés liés aux violations de données, l'utilisation de l'automatisation est une occasion manquée de renforcer la cyber-résilience, car les organisations qui ont déployé pleinement l'automatisation de la sécurité économisent 1,5 million de dollars sur le coût total d'une violation de données, contrairement aux organisations qui n'exploitaient pas l'automatisation pour lesquelles ce coût est beaucoup plus élevé.

Le manque de compétences impacte toujours la cyber-résilience

Le manque de compétences en cybersécurité semble compromettre encore davantage la cyber-résilience, car les organisations ont signalé que le manque de personnel les empêchait de gérer correctement leurs ressources et leurs besoins. Les participants à l'enquête ont déclaré ne pas disposer des effectifs nécessaires pour maintenir et tester correctement leurs plans de réponse aux incidents et qu'il leur restait de 10 à 20 postes à pourvoir dans les équipes de cybersécurité. En fait, seuls 30% des personnes interrogées ont indiqué que le personnel affecté à la cybersécurité est suffisant pour atteindre un niveau élevé de cyber-résilience. En outre, 75% des personnes interrogées estiment que leur difficulté à recruter et à retenir du personnel qualifié dans le domaine de la cybersécurité est moyennement élevée à élevée.

En plus du défi lié aux compétences, près de la moitié des personnes interrogées (48%) ont admis que leur organisation déploie trop d'outils de sécurité distincts, ce qui a pour effet d'accroître la complexité opérationnelle et de réduire la visibilité sur la sécurité globale.

La protection de la vie privée : une priorité croissante

Les organisations reconnaissent enfin que la collaboration entre la protection de la vie privée et la cybersécurité peut améliorer la cyber-résilience, 62% d'entre elles indiquant qu'il est essentiel d'aligner ces équipes pour atteindre cette résilience. La plupart des personnes interrogées estiment que le rôle de la protection de la vie privée prend de plus en plus d'importance, en particulier avec l'émergence de nouveaux règlements comme le RGPD et le California Consumer Privacy Act, et accordent la priorité à la protection des données dans leurs décisions d'achat IT.

Lorsqu'on leur a demandé quel était le principal facteur qui justifiait les dépenses en matière de cybersécurité, 56% des personnes interrogées ont répondu qu'il s'agissait des pertes ou vols d'information. Cela est d'autant plus vrai que les consommateurs exigent des organisations qu'elles fassent davantage pour protéger activement leurs données. Selon un récent sondaged'IBM, 78% des personnes interrogées affirment que la capacité d'une organisation à préserver la confidentialité de leurs données est extrêmement importante, et seuls 20% font entièrement confiance aux organisations avec lesquelles ils interagissent pour préserver la confidentialité de leurs données.

De plus, la plupart des personnes interrogées ont également indiqué avoir employé un responsable de la protection des données personnelles, 73% d'entre elles déclarant avoir un Chief Privacy Officer, ce qui prouve que la confidentialité des données est devenue une priorité absolue dans les organisations.

A propos de l’étude

Menée par le Ponemon Institute et sponsorisée par IBM Resilient, "The 2019 Cyber Resilient Organization" (« L'organisation cyber-résiliente de 2019 ») est la quatrième étude annuelle de référence sur la cyber-résilience : la capacité d'une organisation à maintenir son objectif principal et son intégrité face aux cyberattaques. L'enquête mondiale présente les points de vue de plus de 3 600 professionnels de la sécurité et IT du monde entier, notamment de la France, des États-Unis, du Canada, du Royaume-Uni, de l'Allemagne, du Brésil, de l'Australie, du Moyen-Orient et de l'Asie Pacifique.

Données concernant la France :

- La taille finale de l'échantillon des participants à l'étude en France était de 298 personnes.
- Au cours des deux dernières années, 54% des organisations interrogées ont subi une violation de données et 54% ont déclaré avoir été victimes d'un incident de cybersécurité.
- 82% des personnes interrogées ont déclaré NE PAS disposer d'un Computer Security Incident Response Plan : CSIRP (plan de réponse aux incidents de sécurité informatique) appliqué de manière uniforme dans l'ensemble de l'organisation.
- Parmi les organisations ayant un CSIRP en place, 53% ne testent pas les plans régulièrement, voire pas du tout.
- Seuls 24% ont déclaré utiliser l'automatisation de manière significative dans leur organisation.

Parmi les organisations ayant un CSIRP en place, 53% ne testent pas les plans régulièrement, voire pas du tout.

Seuls 24% ont déclaré utiliser l'automatisation de manière significative dans leur organisation.

Pour en savoir plus sur les résultats complets de l'étude, téléchargez l'étude "The 2019 Study on the Cyber Resilient Organization."

Inscrivez-vous à notre prochain webinaire : "Leaders & Laggards: The latest findings from the Ponemon Institute's study on the Cyber Resilient Organization", qui se tiendra le 30 avril de 18h à 19h.

A propos d'IBM Security

IBM Security offre l'une des gammes de produits et services de sécurité pour organisations 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 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] Source : Etude IBM/Ponemon Institute sur les coûts liés aux violations de données

Contact(s) relations externes

IBM

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

Weber Shandwick pour IBM

Eric Chauvelot / Julie Fontaine + 33 (0) 1 47 59 56 57 / 33 (0) 1 47 59 56 24ibmfrance@webershandwick.com