Communiqués de presse

IBM Security dévoile de nouveaux outils d'aide à la conformité au RGPD

IBM Resilient aide ses clients à se préparer, répéter et adopter les procédures du règlement.

CAMBRIDGE, MA - 26 mai 2017:

IBM dévoile aujourd'hui de nouveaux outils de réponse aux incidents, qui seront intégrés à sa gamme de produits de sécurité IBM Resilient et aideront les entreprises à se conformer au nouveau Règlement général sur la protection des données (RGPD). Ces outils sont conçus pour permettre aux utilisateurs de se préparer, de répéter et d'adopter les nouvelles réglementations imminentes. Le RGPD, qui entrera en vigueur le 25 mai 2018, marquera le plus grand changement dans la législation sur la protection des données depuis plus de vingt ans.

Le RGPD peut imposer aux entreprises de nouvelles normes quant à la façon de réagir en cas de violation des données utilisateurs. Par exemple, toute organisation opérant sur le continent européen disposera dorénavant de 72 heures pour signaler une violation de données à l'autorité de surveillance, sous peine de recevoir une amende qui pourra aller jusqu'à 20 millions d'euros ou 4 % de son chiffre d'affaires global annuel. Une récente enquête menée par l'Institut Ponemon a révélé que 75 % des organisations admettent n'avoir déployé aucun plan de réponse formel aux incidents de cybersécurité (PRICS) touchant leur organisation, et que l'adoption du règlement RGPD pourrait s'avérer très compliquée pour elles. [1]

IBM Security vient pour cela de déployer sur sa plateforme Resilient Incident Response (IRP) des outils qui aideront les organisations à adopter les dispositions du RGPD, soit un an avant la date butoir du 25 mai 2018, afin de leur laisser tout le temps nécessaire pour se préparer et s'adapter. Ces nouvelles fonctionnalités incluent :

· **Guide de préparation au RGPD**. Un outil interactif qui indique, étape par étape, comment se préparer au RGPD. Le guide exploite la flexibilité de la plateforme Resilient IRP pour offrir une préparation et une planification interactives et dynamiques. Les tâches préconisées peuvent être modifiées ou assignées afin d'optimiser la conformité au RGPD à tous les échelons de l'organisation, au-delà de la notification des violations. Ce guide se penche de façon détaillée sur chaque aspect de la préparation, ce qui facilitera à l'avenir le suivi et la documentation des incidents.

· **Simulation du RGPD.** Une nouvelle fonction intégrée à la plateforme Resilient IRP aidera les analystes de la sécurité d'une organisation à répéter les actions qu'ils devront potentiellement peut-être entreprendre à

l’avenir en cas de violation, comme par exemple communiquer toute attaque dans la limite de 72 heures, évaluer les risques ou les dommages, et entrer en contact avec le Délégué à la protection des données (DPD) et une Autorité de protection des données (APD). Dans le cadre de cette simulation, les analystes devront définir un risque comme élevé, moyen ou faible, se conformer à la marche à suivre afin de notifier une violation à une APD, et ensuite signaler aux utilisateurs que des données ont été subtilisées. L’enquête de Ponemon a également révélé que le manque de cyber-résilience au sein d’une organisation est dû à une planification et une préparation insuffisantes ; les simulations au RGPD peuvent ainsi aider à résoudre ce type de problème.

· **Module de confidentialité adapté au RGPD.** IBM Security a intégré les normes du RGPD à son module de confidentialité global et continuera de le mettre à jour afin qu’à la date d’entrée en vigueur du RGPD, le 25 mai 2018, les clients d’IBM Resilient puissent accéder à la base d’informations sur le RGPD et les législations apparentées disponible sur la plateforme Resilient IRP. L’application extraterritoriale de ce règlement imposera également aux entreprises basées en dehors de l’UE mais qui vendent ou exploitent des données relatives à des entités européennes, de se conformer au RGPD. Néanmoins, malgré l’impact généralisé de ce dernier, l’étude de Ponemon indique qu’à peine la moitié des 4 268 professionnels de l’IT et de la sécurité IT interrogés ont commencé à se préparer à l’adoption du RGPD. [1]

« Avec le RGPD, les législations européennes en matière de confidentialité des données connaîtront leurs plus gros changements des vingt dernières années, notamment en matière de politiques et de documentation, qui sont des aspects difficiles à optimiser à l’aide de la technologie, explique John Bruce, PDG et co-fondateur d’IBM Resilient. La plateforme de réponse aux incidents IBM *Resilient (IRP) est conçue pour aider les entreprises à se conformer au RGPD. Elle indique les étapes à suivre, guide les utilisateurs et veille à ce que les processus et outils technologiques réagissent de façon spécifique aux violations de données.»*

La plupart des organisations ont déjà aujourd’hui beaucoup de difficultés à répondre aux cyber-incidents. Selon une autre étude menée par Ponemon, 66 % des professionnels interrogés se disent dubitatifs quant à la capacité de leur organisation à récupérer d’un cyber-incident. En outre, 41 % indiquent que le temps requis pour résoudre un cyber-incident a augmenté au cours des 12 derniers mois. [2]

« Le RGPD sera synonyme de nouveaux défis pour la plupart des organisations, confie Larry Ponemon, Président et fondateur de l’Institut Ponemon. *Notre enquête révèle qu’une grande partie des entreprises mondiales doutent de leur capacité à répondre aux nouvelles normes en matière de notification des violations de données. Pour pouvoir faire face à ces challenges, les organisations devront se montrer proactives en élaborant des procédures et stratégies qui assureront la conformité aux nouvelles exigences. »*

Le module de confidentialité, basé sur le RGPD, vise à réduire drastiquement la complexité et le temps nécessaire pour notifier une violation de données conformément à la nouvelle réglementation. Par exemple, une entreprise basée aux Etats-Unis avec une clientèle internationale pourrait être victime d'un vol de données appartenant à des clients situés en Allemagne et dans le Massachusetts, en Californie et à New York. Si elle ne dispose pas de la plateforme Resilient IRP, cette entreprise devra se renseigner sur la procédure à suivre et les personnes à contacter en Europe afin d'être conforme au RGPD pour ses clients allemands, mais aussi connaître les personnes à contacter et les procédures à respecter selon les lois applicables aux Etats du Massachusetts, de Californie et de New York.

La plateforme Resilient IRP fait partie du système IBM Security, qui aide les clients à contrecarrer les menaces intelligentes grâce à des technologies de pointe en matière cognitive, cloud et collaborative.

Pour découvrir le rapport d'IBM Resilient sur la réponse aux violations de données post-RGPD ou en savoir plus sur les outils RGPD d'IBM Security, cliquez ici.

A propos d'IBM Resilient

La mission d'IBM Resilient est d'aider les organisations à réagir efficacement en cas de cyberattaque ou de crise organisationnelle. La plateforme de réponse aux incidents (Incident Response Platform - IRP), leader de son marché, permet aux équipes de sécurité d'analyser, réagir et atténuer les incidents plus rapidement, plus intelligemment et plus efficacement. Resilient IRP est la seule plateforme capable d'offrir une orchestration et une automatisation des réponses aux incidents de bout-en-bout, permettant ainsi aux équipes de regrouper et harmoniser les utilisateurs, les processus et les technologies en un pôle central de réaction aux incidents. Grâce à Resilient, les équipes de sécurité peuvent bénéficier des meilleures performances actuelles en matière de réponse aux incidents. IBM Resilient compte plus de 200 clients mondiaux, dont 50 sont membres du Fortune 500, et plusieurs centaines de partenaires aux quatre coins du monde. Pour en savoir plus, rendez-vous sur **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 3000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous

sur www.ibm.com/security, suivez @IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

[1] Institut Ponemon et IBM Resilient, « The Cyber Resilient Organization » 2016

[2] Institut Ponemon et Citrix, « The Need for a New IT Security Architecture » 2017

Pour plus d'information, veuillez contacter :

Morgane Leonard / Anne-Hélène Lagadeuc

Finn Partners pour IBM Resilient

Contact(s) relations externes

Finn Partner

Morgane Leonard / Anne Hélène Lagadeuc 01 53 43 51 62IBMResilientFR@finnpartners.com