Etude IBM : Les organisations n'ont pas de plans de sécurité pour faire face à l'évolution du paysage

CAMBRIDGE, Mass., June 30, 2020 : IBM (NYSE: IBM) Security a annoncé aujourd'hui les résultats d'un rapport mondial examinant l'efficacité des entreprises à se préparer et à répondre aux cyberattaques.

Plus de la moitié des nouveaux employés travaillant à domicile depuis peu opèrent sans aucune nouvelle politique de sécurité pour les aider. Ceci signifie que les organisations doivent réagir, d'autant plus que les cybercriminels tirent parti de ces changements à leur avantage. Une étude d'IBM Security montre que les organisations doivent revoir et renforcer leurs plans de réponse aux incidents, non seulement pour les menaces actuelles, mais aussi pour celles à venir dans un climat commercial et de menaces en évolution rapide. En effet, **en France, seules 20%** des organisations interrogées disposent d'un plan de réponse aux incidents de cybersécurité qui est appliqué de manière cohérente dans l'ensemble de l'entreprise.

IBM et le Ponemon Institute dévoilent de nouvelles données mondiales sur la façon dont les organisations planifient leur réponse aux cyberattaques, ainsi que sur leur capacité à détecter et à contenir ces incidents - sur la base des réponses de plus de 3 400 professionnels de l'informatique et de la sécurité à travers le monde. Voici quelques-unes des principales conclusions :

- Si le nombre d'organisations adoptant des plans d'intervention officiels en matière de sécurité a lentement augmenté, près de **75 % d'entre elles sont encore sous-préparées** avec des plans qui sont soit ad hoc, soit appliqués de manière incohérente, soit inexistants.
- Plus de la moitié **(52 %)** n'ont jamais examiné ou n'ont pas fixé de délai pour examiner/tester ces plans de réponse. **En France, 35%** des entreprises interrogées n'ont pas de période fixe pour l'examen et la mise à jour de leur plan.
- Même parmi ceux qui disposent de plans de réponse aux incidents de cybersécurité (CSIRP) officiels, **seuls 33% ont des manuels pour des types d'attaques spécifiques.**
- Les meilleurs playbooks couvrent les attaques plus traditionnelles telles que les attaques DDoS (64 %) et les logiciels malveillants (57 %), et ceux qui couvrent les menaces émergentes sont encore moins nombreux. Seuls 45 % d'entre eux ont des playbooks pour les ransomwares, même si leur existence a augmenté de près de 70 % ces dernières années.

Pour en savoir plus : https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue

Contacts :

IBM

Gaëlle Dussutour

Tel. : + 33 (0)6 74 98 26 92

DUSGA@fr.ibm.com

Weber Shandwick pour IBM
Robin Legros / Morad Salehi
Tel. : + 33 (0)6 68 04 57 83

ibmfrance@webershandwick.com