Cybersécurité : quand la multiplication d'outils dessert les entreprises

IBM Security a publié les principaux résultats de l'édition 2020 d'un rapport* international sur la cyber-résilience des entreprises (Cyber Resilient Organisation Report). Plus de 3400 professionnels IT et sécurité ont été interrogés par le Ponemon Institute.

La proportion d'entreprises qui adoptent des plans de réponse aux incidents de sécurité (CSIRP, computer security incident response plan) a progressé, passant de 18% en 2015 à 26% cette année. Toutefois, 51% des répondants disent encore aujourd'hui ne pas appliquer de manière uniforme dans l'entreprise ces plans d'intervention ou, plus préoccupant encore, s'appuyer sur un plan « informel », voire ad hoc.

Parmi les organisations qui s'appuient sur un plan formel, un tiers (33%) dispose de playbooks (un ensemble de sripts décrivant des étapes à suivre pour améliorer la sécurité). Ces guides concernent avant tout des cyberattaques « classiques » de type DDoS (64%) ou celles utilisant des logiciels malveillants (malwares) (57%). Les playbooks dédiés aux attaques par rançongiciels (ransomwares) arrivent ensuite (45%).

Par ailleurs, 7% seulement des organisations concernées disent réviser ces plans tous les trimestres. Un taux stable sur cinq ans. Plus surprenant, 40% des organisations interrogées n'ont pas fixé de délai pour évaluer et mettre à jour ces plans.

Automatiser

Pour faire face, les solutions de cybersécurité de fournisseurs ne manquent pas. En moyenne, les organisations déploient 45 outils de cybersécurité pour protéger leurs réseaux et systèmes d'information.

Toutefois, selon le rapport, la multiplication d'outils affaiblit la cyber-résilience. Ainsi, l'opportunité de détecter des cyberattaques baisserait de 8%, et celle d'y répondre de 7%, chez les organisations qui s'appuient sur plus de 50 outils, par rapport à celles qui utilisent une quantité plus modérée de solutions et services dédiés à la sécurité informatique.

Pour Wendi Whitmore, vice-présidente d'IBM X-Force Threat Intelligence, les organisations ont également intérêt à « se concentrer sur les tests, la pratique et la réévaluation de leur plan de réponse aux incidents de sécurité », pour en déterminer la pertinence. Sans bouder pour autant les technologies interopérables et l'automatisation.

*3439 professionnels IT et sécurité ont été interrogés au printemps 2020. France, Allemagne, Royaume-Uni, États-Unis, Canada, Inde, Brésil, Japon, Australie, Moyen-Orient et région ASEAN sont concernés.

(crédit photo via Pexels)