Cyber-résilience : la moitié des entreprises dans le flou

La fréquence irrégulière de tests de sécurité IT – cyber-résilience – peut coûter cher aux entreprises.

Pourtant, la majorité des organisations testent rarement, voire pas du tout, leurs capacités de résistance aux cyberattaques. C'est ce que montrent les résultats d'une enquête internationale commandée par IBM Security au Ponemon Institute.

77% (82% dans l'Hexagone) des professionnels IT interrogés* ont déclaré ne pas appliquer de manière uniforme dans l'entreprise de plan de réponse aux incidents de sécurité (CSIRP, computer security incident response plan).

Cyber-résilience : les tests sont trop rares

De surcroît, parmi les organisations qui gèrent un CSIRP d'envergure, 54% (53% en France) ne réalisent pas de test de résistance régulièrement.

Plus d'une organisation sur deux reconnaît avoir été la cible d'un incident ou d'une violation de données ces douze derniers mois.

Or, selon une autre étude Ponemon/IBM, les entreprises qui ont contenu une violation de données en moins de 30 jours auraient économisé plus de 1 million de dollars sur le coût total de l'incident.

Par ailleurs, 46% des entreprises ne sont pas encore pleinement en conformité avec le règlement européen sur la protection des données (RGPD).

Qu'en est-il de l'automatisation pour les RSSI ?

Prévention–détection

77% des organisations disent utiliser l'automatisation modérément, faiblement ou pas du tout.

Les 23% qui l'adoptent de manière significative estiment que l'automatisation renforce leurs capacités à : prévenir (69% contre 53% pour l'ensemble du panel), détecter (76% contre 53%), répondre (68% contre 53%) et contenir (74% contre 49%) une cyberattaque.

La cyber-résilience est considérée comme un moyen de conforter la prévention–détection.

*3655 professionnels IT et sécurité, dont 298 en France, ont été interrogés.

(crédit photo : Ecole polytechnique / Paris / France on Visual hunt / CC BY-SA)