Cybersécurité : des RSSI à bout de souffle ?

Les responsables de la sécurité des systèmes d'information révisent leurs priorités pour se concentrer sur la protection des postes et des outils de télétravail, sans grever les budgets. C'est l'un des enseignements d'une enquête* estivale publiée par HackerOne.

En France, 70% des RSSI (contre 64% pour l'ensemble du panel) estiment que leur entreprise est plus exposée aux violations de données qu'elle ne l'était avant la crise sanitaire. Ce taux est supérieur de 6 points à la moyenne du panel.

Les RSSI français sont également plus nombreux (36%) que la moyenne (30%) à rapporter une augmentation des cyber-attaques contre les systèmes d'information de leur organisation par rapport à la période pré-pandémique.

Posture de sécurité

70% des répondants en France (66% en moyenne) déclarent que la pandémie de Covid-19 les pousse à renforcer davantage leur posture en matière de sécurité.

Or, plus d'un quart des RSSI (30% en France, contre 25% en moyenne) estiment que les budgets de sécurité sont négativement impactés par la crise. Pour faire face, 33% des RSSI français (contre 30% en moyenne) se déclarent plus enclins que par le passé à accepter les rapports de vulnérabilité de sécurité émanant de chercheurs tiers.

HackerOne, plateforme collaborative de chasse aux bugs, surfe sur la vague.

« La pression pour répondre aux exigences du travail à distance et aux demandes des clients en matière de services numériques a considérablement élargi les surfaces d'attaque, laissant les équipes de sécurité à bout de souffle », a déclaré Marten Mickos, CEO de HackerOne. Dans ce contexte, de plus en plus d'organisations prennent conscience de l'avantage que représente le recours à une communauté de hackers, selon lui.

*L'enquête a été menée par Opinion Matters pour HackerOne. 1400 RSSI et décideurs informatiques ont été interrogés en juillet 2020. France, Allemagne, Royaume-Uni, Canada, États-Unis, Singapour et Australie sont couverts.

(crédit photo © Shutterstock)