Cybersécurité : RSSI et hackers éthiques, une relation à développer

La sécurité offensive gagne progressivement du terrain dans les entreprises en Europe, mais la majorité des RSSI interrogés hésitent encore à se tourner vers des hackers éthiques, selon une enquête européenne commandée par la plateforme de chasse aux bugs HackerOne.

Malgré la pénurie de professionnels de la cybersécurité, 57% des responsables de la sécurité des systèmes d'information (RSSI) interrogés (51% en France) disent ne pas faire appel à des hackers éthiques externes pour identifier des vulnérabilités logicielles dans leurs systèmes.

Par ailleurs, seuls 26% (23% en France) se disent prêts à accepter les soumissions de bugs de l'ensemble de la communauté de hackers. Toutefois, ce taux augmente nettement (jusqu'à 40% en France) lorsqu'il est question de collaborer uniquement avec des hackers « certifiés ».

Or, 64% des répondants (68% en France) estiment que leur équipe interne est insuffisamment dimensionnée pour suivre le rythme de développement de leur organisation.

Qu'en est il du ressenti concernant les tests d'instrusion ?

L'Europe peut mieux faire

En France, 21% des répondants estiment que les tests d'intrusion (pentests) fournissent des résultats suffisants pour soutenir la cadence du développement applicatif. Mais ils sont plus nombreux encore à penser le contraire (30% en France, 45% pour l'ensemble du panel).

Globalement, enfin, 35% des RSSI européens (30% en France) reconnaissent être freinés par un manque de budget et de compétences pour aller de l'avant.

« La sécurité offensive est encore un marché émergent en Europe et certains mythes subsistent. Il est donc primordial de poursuivre l'évangélisation et de démontrer les bénéfices du hacking éthique », a déclaré Hugues Masselin, consultant chez HackerOne.

« Ne pas chercher à trouver des vulnérabilités dans ses systèmes de manière proactive revient à appliquer la politique de l'autruche », a-t-il ajouté. Or « une vulnérabilité [ignorée] peut rester exploitée longtemps, à l'insu de l'organisation, et faire de nombreux dégâts. »

*L'enquête promue par HackerOne a été menée par Opinion Matters auprès de 600 RSSI et décideurs techniques en France, en Allemagne et au Royaume Uni entre le 31 décembre 2019 et le 7 janvier 2020.

(crédit photo © Shutterstock)