Cybersécurité : divulguer une faille ou garder le secret ?

Les entreprises jugent satisfaisante leur approche de la cybersécurité. Malgré tout, elles redoutent l'expertise de hackers éthiques. C'est l'un des enseignements d'une enquête* internationale promue par HackerOne. 800 responsables de la sécurité des systèmes d'information ont été interrogés sur les choix de leur entreprise dans ce domaine.

Plus de 6 organisations sur 10 (66%) pensent être plus affûtées que la concurrence en matière de cybersécurité. 65% se disent même « irréprochables » sur ce plan. Cependant, 67% accepteraient certaines vulnérabilités logicielles plutôt que d'investir la sécurité participative (crowdsourced security).

Un autre frein apparaît. 1 hacker éthique sur 2 hésite à divulguer une faille identifiée du fait d'une précédente expérience négative (risque juridique) ou d'un manque d'appui pour un contact avec l'entreprise concernée dans un cadre légal.

Aussi, 57% des répondants peinent à diffuser une culture de la cybersécurité dans leur entreprise. 65% disent être confrontés au message : « la sécurité freine l'innovation ». 63% déplorent des violations de sécurité à la suite d'un contournement interne de mesures en la matière.

Quels sont les défis à relever ?

En finir avec la sécurité par l'obscurité

63% des RSSI considèrent que les critères liés aux meilleures pratiques de cybersécurité sont aussi importants que les coûts lorsqu'il est question de choisir un fournisseur. 62% iraient voir ailleurs si un fournisseur était victime d'une faille de sécurité. Enfin, 53% (52% en France) admettent avoir perdu des clients à la suite d'une faille de sécurité, selon l'enquête publiée par HackerOne.

Le spécialiste américain du bug bounty et promoteur du manifeste Corporate Security Responsibility (CSecR), recommande aux entreprises de se défaire d'une culture de « la sécurité par l'obscurité » et d'opter pour davantage de transparence en la matière. Autrement dit de faire appel à des hackers éthiques pour identifier des vulnérabilités logicielles dans leurs systèmes. Ces failles qui, autrement, pourraient échapper à leur vigilance et être exploitées par des organisations cybercriminelles ou des initiés.

*L'enquête « Le piège de la sécurité : de la culture du secret à la transparence » a été réalisée auprès de 800 responsables sécurité à travers le monde.

(crédit photo © Shutterstock)