Cybersécurité : quand les RSSI peinent à équilibrer les ressources

Les responsables de la sécurité des systèmes d'information (RSSI) redoutent de manquer de ressources (budgets et talents) pour faire face à la multiplication des menaces. C'est le principal enseignement d'une enquête* internationale réalisée par Forbes Insights avec le soutien de Fortinet.

Sous pression, 84% des RSSI interrogés pensent que les risques de cyberattaques vont augmenter. Or, 21% déplorent que les capacités des attaquants dépassent celles dont leur organisation dispose pour se protéger. Comment mieux se défendre ?

Le plus grand nombre (48%) déclare se concentrer sur l'intégration transparente de la sécurité des opérations réseau. 45% des responsables de la sécurité cherchent aussi à obtenir une meilleure visibilité de leurs environnements en s'appuyant sur des technologies d'analyse avancée. Par ailleurs, 44% disent adapter leur stratégie de cybersécurité à l'extension de la surface d'attaque.

Données clients et propriété intellectuelle

Protéger les données clients et la marque est citée comme la principale priorité par 36% du panel. La protection de la propriété intellectuelle de l'entreprise arrive ensuite (20%).

Cependant, les RSSI redoutent l'absence d'une stratégie de cybersécurité pleinement soutenue par le top management (citée par 35% des répondants) et largement diffusée dans l'entreprise (35% également).

Mais les budgets ne suivent pas toujours. Or, 36% des RSSI estiment que l'absence d'un budget adéquat a un impact significatif sur leur programme de cybersécurité.

Ils préféreraient d'ailleurs transférer des ressources de la prévention au renforcement de la détection et de la réponse aux incidents de sécurité (en y consacrant 40% de leur budget, plutôt que 36% en moyenne).

Selon une autre étude (NTT Security), le coût de la reprise d'activité après incident atteint en moyenne 1 million d'euros par entité dans le monde et 690 000 euros en France.

**L'enquête a été menée auprès de 209 RSSI de grandes entreprises (plus de 1 Md$ de CA). Amérique du Nord, régions EMEA et Asie-Pacifique sont concernées. (source : « Making tough choices: How CISOs manage escalating threats and limited resources. »)*