RSSI, un rôle en perpétuel changement

Qu'elles soient dues au progrès technologique, à l'hyperconnectivité, à des facteurs internes ou externes aux entreprises, à la transformation digitale rapide ou même, pour finir, à la récente pandémie Covid19, les cyber-menaces augmentent incontestablement.
Par conséquent, la cybersécurité est devenue une question d'intérêt général. Elle fait partie des éléments permettant de juger de la santé d'une entreprise, à l'instar des contrôles financiers et opérationnels.

Toutes les industries sont conscientes des risques et prennent des mesures contre les cyber-attaques. Les conseils d'administration sont plus regardants sur la manière dont les RSSI gèrent les cyber- menaces et sur les stratégies déployées pour sécuriser les organisations.

Un rôle multiple qui a rapidement évolué

À l'époque, les RSSI peinaient à se faire entendre et devaient s'efforcer de convaincre que la sécurité est importante. Aujourd'hui, le nouveau défi est d'être performant et de tenir ses promesses ! Le rôle des RSSI est en train de passer de l'influence et de la visibilité, à l'exécution sans relâche et à la garantie que les actifs sont protégés de la bonne manière.

De nos jours, le rôle d'un RSSI consiste à concevoir une stratégie de sécurité complète, comprenant politiques, gouvernance, cadres sans risque et évolutifs par nature, puis à l'intégrer dans la stratégie globale de son organisation. Un autre rôle est de promouvoir une culture de la sécurité.
Il doit également apporter une valeur ajoutée aux parties prenantes externes et internes, et définir et orienter les carrières des futurs professionnels de la cybersécurité.

Panorama global des nouvelles missions du RSSI

Nous constatons donc que le nouveau rôle du RSSI va bien au-delà de la gestion des risques.

– Le RSSI joue désormais un rôle très important dans l'adoption stratégique et sécurisée de technologies nouvelles et avancées, la perception de la marque, le maintien de la réputation et l'engagement des parties prenantes.

– Il est passé de la protection de l'entreprise à la création de valeur pour celle-ci. Cela peut se faire en rationalisant les fonctions liées à la sécurité et la conformité, en créant un mécanisme de défense impénétrable et en assurant la cyber-résilience et la continuité des activités.

– Afin d'instaurer une culture de la sécurité dans l'ensemble de l'organisation, le RSSI doit, contrairement à ce qui se faisait auparavant, être impliqué dans toutes les équipes. Les politiques de partage et d'autorisation d'accès doivent toutes être prises en charge à un niveau élevé.

– Le RSSI se trouve au cœur de la planification stratégique et de la prise de décision. Avec la transformation digitale, la complexité des technologies et des menaces a augmenté et il est donc important d'avoir une visibilité complète de l'architecture de sécurité et des décisions stratégiques

prises à tous les niveaux.

– Chaque année, il se trouve face à de nouveaux défis en raison des innovations et des révolutions rapides des technologies. On attend de lui qu'il se tienne au courant des derniers événements et qu'il renforce la sécurité de son organisation constamment.

– Sa capacité d'investigation est essentielle. Un RSSI doit connaitre les détails d'une attaque en précisant comment elle a eu lieu, qui en est responsable et comment elle a été gérée. Plus important, il doit être capable de déterminer rapidement si l'entreprise est toujours sous le coup de l'attaque ou si l'environnement est redevenu sûr.

Il est intéressant de constater l'évolution du rôle du RSSI au cours des dernières années. Il est désormais considéré comme un facilitateur, un stratège, un conseiller commercial essentiel qui s'efforce de créer une culture de la sécurité et préconise la « sécurité dès la conception ». Dans les temps à venir, nous verrons certainement de nombreux nouveaux aspects s'ajouter à ce rôle.