RSSI : les 4 compétences clé…au delà de la sécurité

1 – Un sens aigu des affaires

Il n'y a pas si longtemps, le RSSI était chargé d'élaborer un plan de défense adapté au paysage informatique de sa société. Cette stratégie est aujourd'hui insuffisante, et l'approche moderne doit être en phase avec la vision de l'entreprise. C'est pour cette raison que la quasi-totalité des postes de RSSI à pourvoir exigent non seulement des connaissances pointues en matière de sécurité informatique et une liste de certifications, mais également un sens aguerri du business.

Résultat, le RSSI ne peut ni rejeter ni interdire une technologie que sa société souhaite mettre en œuvre. Il doit évaluer les risques y afférents et proposer la stratégie la plus sûre qui n'entravera pas le développement de l'entreprise. Si les employés doivent être en mesure d'accéder aux ressources de l'entreprise à partir de leurs propres appareils, le RSSI devra déployer une règle leur permettant de les connecter au réseau (BYOD).

Le meilleur conseil à donner à un RSSI est de devenir un gestionnaire de risques tout en apportant aide et conseil à l'entreprise.

2 – De bonnes capacités de communication et de présentation

Être dirigeant implique des interactions avec la « C-suite » et le Conseil d'administration. Mais compte tenu du nombre limité de cadres supérieurs disposant d'une formation en sécurité digne de ce nom, le défi est de taille, ce qui oblige le RSSI à développer une rhétorique permettant aux membres du CA de mesurer la gravité des risques.

La capacité à présenter des idées complexes sous une forme compréhensible est sans doute un cliché, mais la possibilité de traduire le langage de la cybersécurité dans des termes compris par les dirigeants d'entreprise peut permettre de résoudre ce problème de communication. Cette aptitude peut également s'avérer utile face au principal casse-tête rencontré par tout RSSI, à savoir justifier le budget de la sécurité informatique.

De solides compétences en communication, telles que la facilité à adapter l'information à un public novice et à avancer des arguments imparables (sanctions en cas de non-conformité, dommages provoqués par des attaques antérieures, rapports concernant les failles), démontreront que les avantages sont largement supérieurs aux coûts induits.

3 – Savoir gérer une crise

Selon une récente étude menée par Kaspersky Lab, 86 % des RSSI estiment que des failles de cybersécurité vont se produire tôt ou tard, ce qui signifie que les entreprises ne peuvent se permettre d'être mal préparées. Dans tous les bureaux, une procédure d'évacuation doit être observée par les employés en cas d'incendie. De la même manière, toute entreprise doit établir une stratégie pour contrer les failles de sécurité, dans la mesure où panique et désorganisation ne feront qu'aggraver la situation.

Mettre en œuvre un plan d'action ne consiste pas uniquement à modifier des mots de passe ou restaurer des systèmes agressés. Pour contrer une attaque rapidement, il est essentiel de déterminer qui est responsable de quelle action et d'identifier dans les autres services les personnes-ressources qu'il conviendra d'informer en priorité — équipes juridiques, service de presse ou de relations avec la clientèle — et qui, à leur tour, pourront intervenir pour résoudre la crise.

En cas de faille, il est essentiel que le RSSI soit en permanence tenu informé de l'évolution de l'incident et se positionne comme un interlocuteur privilégié entre les différents intervenants et dont la mission sera de coordonner les activités de l'équipe de sécurité informatique, d'informer l'entreprise et de gérer la situation à mesure de son évolution.

4 – Supervision et leadership

Actuellement, 62 % des RSSI déplorent une pénurie de talents en cybersécurité, et il est de plus en plus difficile de trouver de nouveaux spécialistes en la matière. Ce n'est toutefois que la partie visible de l'iceberg, le principal motif de préoccupation étant leur fidélisation.

Compte tenu du manque d'experts en sécurité, les spécialistes qui souhaitent changer d'emploi croulent sous les offres. La pénurie de main-d'œuvre en sécurité informatique accroît par ailleurs la charge de travail du personnel en place, ce qui suscite des inquiétudes supplémentaires pour les responsables de la sécurité. Face à la multiplication des tâches redondantes et banales, le burn-out des employés est-il aussi inévitable que la cybercriminalité ?

Le RSSI exerce une influence directe sur le personnel de sécurité et à ce titre, il doit jouer un rôle de leader que les employés pourront suivre — un rôle de mentor capable de diriger une équipe et de motiver les employés. Une telle motivation ne se borne pas à des incitations financières : elle peut se traduire par l'octroi d'une plus grande puissance de décision, par des possibilités de formation et de perfectionnement professionnel, voire par la simple reconnaissance du travail accompli.

Il ne fait aucun doute que le rôle du RSSI est complexe, dans la mesure où il requiert une combinaison unique de compétences humaines et de solide expertise technique. Pour être performant, un RSSI doit afficher des qualités de manager et de leader, mais également une bonne compréhension de l'IT, un sens aigu des affaires et une grande maîtrise de la cybersécurité.

Bien que les compétences techniques constituent le socle de ce rôle tel qu'il existe aujourd'hui, certains facteurs-clés continueront d'influer sur l'équilibre des compétences qui seront requises demain. Un jour viendra peut-être où les machines disposeront d'une meilleure expertise en cybersécurité que n'importe quel être humain et qu'elles seront capables d'exécuter des tâches

techniques. Mais les compétences « humaines » telles que la gestion des équipes, la maîtrise du temps et le sens des affaires des RSSI feront d'eux, à n'en pas douter des professionnels essentiels dans les entreprises de demain