Culture cybersécurité et culture d'entreprise ne doivent faire qu'un

La protection de l'entreprise et de sa valeur, ainsi que la réussite en matière de cybersécurité reposent en grande partie sur le facteur humain. Chaque collaborateur a un rôle à jouer pour protéger son entreprise. Pour y arriver, il est temps d'adopter la culture de la cybersécurité.

Les avantages des nouvelles technologies et les opportunités qu'ouvrent la connectivité sont évidents. Cependant, les risques de cyberattaques persistent et constituent une menace se?rieuse pour les entreprises. En effet, selon une étude du cabinet Deloitte, 63% des incidents de sécurité ayant lieu en entreprise proviendraient d'une erreur commise par un des employés. Si la sensibilisation et la formation des équipes aux risques informatiques sont essentielles, développer une véritable « culture de cybersécurité » en interne est indispensable pour aider à prévenir et à limiter les risques.

Intégrer la cybersécurité à la gestion d'entreprise

Les violations de donne?es cou?tent en moyenne 3,85 millions d'euros aux entreprises françaises et ce, outre les conséquences que ces attaques peuvent avoir sur leur valeur et leur image. En général, la valeur marché est impactée par la perte de données (d'autant plus si celles-ci sont à caractères personnelles) et les cyber-intrusions re?ussies re?duisent les investissements et accentuent l'endettement. Alors, plus les attaques sont nombreuses et couronnées de succès, plus les conséquences sont désastreuses pour les entreprises.

Historiquement, assurer la sécurité d'une entreprise consistait à utiliser des clés sécurisées et à fermer simplement la porte derrière soi. Dans le meilleur des cas, un groupe restreint de collaborateurs avait pour mission de maintenir la sécurité au sein de l'entreprise. Bien que la sécurité physique soit toujours importante, elle semble presque obsolète à l'heure du règne de la technologie. Compte tenu des événements de ces derniers mois et de l'adoption massive du télétravail, la cybersécurité est plus que jamais l'affaire de chacun d'entre nous. Il n'est plus question de la traiter de façon distincte, mais plutôt de l'intégrer à la culture d'entreprise. Mais comment assurer l'adhésion des collaborateurs à ce nouveau pan de la culture ?

Par ailleurs, un service dédié à la cybersécurité est primordial. Pour la gestion des équipes et des frais, il faut rester prudent. Ces investissements sont généralement mal compris et engendrent parfois une augmentation des coûts sans que de réels bénéfices n'en soient tirés en matière de gestion de risques. « Le plus est l'ennemi du bien » : un bon RSSI comprendra que des ressources correctement allouées seront beaucoup plus efficaces. D'autres éléments peuvent être mis en place comme par exemple la visibilité et la reconnaissance des CISO/CSO et de leurs aptitudes. Leur mention sur le site web d'une entreprise donne souvent une bonne indication des personnes décisionnaires ainsi que l'orientation stratégique. Compte tenu des nombreuses conséquences négatives d'une attaque réussie, les CISO et CSO devraient définitivement pouvoir participer aux discussions stratégiques d'une entreprise. Un premier travail est à mener dans les hautes sphères de l'entreprise. Même si la cybersécurité a tendance à s'imposer dans les discussions stratégiques et notamment au sein des conseils d'administration, seules 25% des entreprises ont rattaché leur service dédié à la sécurité au comité exécutif. Les conseils d'administration ont pourtant tout intérêt à adopter ces comportements, puisqu'ils permettront une meilleure compréhension des enjeux, une

mise en place d'une vision stratégique claire et l'implémentation de solutions de cybersécurité et de « remote working » adaptées.

Il est évident que toute entreprise, quel que soit son secteur d'activité? ou sa taille, est axée sur la technologie et dépend d'elle. Alors, si les entreprises sont technologiques, chacune d'entre elles doit également intégrer la cybersécurité dans son ADN.

La cybersécurité se doit d'être accessible et comprise de tous

Tout comme les solutions et les processus, les salariés sont les clés d'une cybersécurité performante. Guidé par les équipes IT, chaque directeur, responsable, doit insuffler les bonnes pratiques à leurs équipes. Que ce soit à travers actions quotidiennes simples ou encore l'utilisation de solution de protection, tous les collaborateurs sont responsables à la fois de leur propre cybersécurité mais aussi celle de l'entreprise.

Sensibiliser les employés au travers de sessions de formations et de tests de phishing ne saurait ni être suffisant ni permettre d'évaluer la situation eu sein des différents corps de métier. Pour que l'adoption de ces gestes devienne un acquis, la pédagogie, la communication et un rappel régulier des attentes sont nécessaires. Il ne s'agit pas d'ajouter une nouvelle pression aux salariés, déjà chargés par les évènements de ces derniers mois, mais de les accompagner dans la sureté de leurs missions au quotidien.

La cybersécurité doit être véhiculée et perçue comme un enjeu de premier ordre qui concerne tous les salariés. Chacun doit alors agir au quotidien et à son niveau, comme il le ferait pour d'autres dimensions comme la RSE. Il faut leur donner les moyens informatiques et organisationnels afin qu'ils adoptent les bons comportements, puissent réagir rapidement en cas de cyberattaque, et de savoir juger si une situation peut être potentiellement dangereuse. Cela s'illustre notamment par la mise en place de solutions adaptées au télétravail sécurisant l'ensemble des terminaux et basées sur l'authentification continue ou encore le Zero Trust.

À l'aide de solutions transparentes et simples d'utilisation, salariés et responsables doivent être en mesure de mieux cerner les subtilités de la cybersécurité, mais aussi de mesurer les risques qu'ils encourent si les normes ne sont pas respectées. Souvent, les plus grands ennemis de la cybersécurité ne sont pas les hackers, mais bel et bien l'ignorance des utilisateurs qui leur offre généralement une porte d'entrée. En empruntant la voie de la responsabilisation de chacun, il est possible de penser que d'ici quelques années, la cybersécurité ne sera plus une source d'angoisse mais une compétence acquise de tous au sein des entreprises.