Le nouvel Economiste

Problème avant tout culturel

Les enjeux de la sécurité

Pourquoi les entreprises ne prennent pas la pleine mesure des réels enjeux du numérique

©Freepik

Smart data, Anne-Tania Desmettre, Black Tiger

Les cyber-incidents se multiplient. Le géant mondial du courtage d'assurance et de réassurance, Aon, en a répertorié 3 718 dans le monde au premier semestre 2019. Ce nombre de cyber-incidents est déjà supérieur aux niveaux des années 2015 (3 391) et 2016 (3 252) entières. La sévérité des sinistres est aussi en augmentation.

La hausse continue des failles de sécurité est antinomique avec la nouvelle législation européenne, qui impose un niveau de vigilance nettement plus élevé aux pratiques du passé. Il est évident qu'il n'y aura pas de ralentissement dans l'utilisation du numérique dans nos vies personnelles et professionnelles. Les entreprises continueront de collecter et d'exploiter un volume de données personnelles de plus en plus important. La combinaison de ces deux facteurs ne peut que mener à une augmentation du risque quant aux failles de sécurité.

Il est donc incompréhensible que les entreprises ne parviennent pas à prendre la pleine mesure du contexte numérique. Pourquoi sont-elles toujours aussi défaillantes ? Trois raisons majeures sont à avancer : un problème culturel, un manque organisationnel et une mauvaise appréhension de la data.

La sécurité délaissée par les Directions générales

Tout d'abord, sur le plan culturel, le RSSI se retrouve, au sein de l'entreprise, souvent seul à porter le sujet de la sécurité. Cette dernière n'intéresse pas les Directions Générales. D'une part, elle est probablement considérée comme un sujet trop technique. D'autre part, n'ayant pas les compétences technologiques pour l'appréhender, les Directions générales s'en réfèrent alors aveuglément au RSSI isolé.

> "Les entreprises n'engagent aujourd'hui que 2% du budget global IT dans la protection des données et des réseaux. Un pourcentage bien insuffisant"

Seconde raison majeure, sur le plan organisationnel, pour qu'il ne soit pas isolé, le RSSI devrait posséder sa propre cellule et reporter directement au chef d'entreprise. Cette séparation des pouvoirs obligerait le CEO à écouter et comprendre les risques et enjeux rattachés aux manquements sécuritaires, et donc, à être pleinement responsable des décisions et des budgets engagés. Selon le cabinet Canalys, les entreprises n'engagent aujourd'hui que 2% du budget global IT dans la protection des données et des réseaux. Un pourcentage bien insuffisant.

Enfin, sur le plan de l'appréhension de la data, tant que les entreprises ne traitent pas la donnée comme un sujet en soi et équivalent aux produits stratégiques de l'entreprise, il n'existe alors pas d'approche globale relative à l'exploitation de la donnée dont les enjeux sécuritaires.

Un manque de responsabilisation partagée

La sécurité des données nous concerne tous. Il existe une absence de responsabilisation dans les usages des réseaux sociaux. Il y a un manque de responsabilisation partagée entre les citoyens et les entreprises en raison du côté abstrait de la cyber-sécurité. Le manque de sécurité n'étant pas physique au premier abord, la grande difficulté de ce sujet est qu'il ne génère pas de sentiment d'insécurité, sauf peut-être, pour les entreprises qui y ont été confrontées.

A lire également

Les enjeux de la transformation numérique
Le legacy IT, un frein à la transformation numérique
Anne-Tania Desmettre : "La donnée personnelle est d'abord un sujet de CEO"

Smart data - Les chroniques d'Anne-Tania Desmettre

Publié le 04/06/2021

Catégories :
Informatique & Technologies / Smart data /