Une bonne hygiène des données pour protéger la santé de l'entreprise

Environ 60% cesseraient d'acheter auprès d'une entreprise qui ne protège pas leurs données, tandis que 59% dépenseraient davantage pour des marques qui en prennent soin. En résumé, prendre à la légère la protection des données s'apparente à un coup de canif dans le contrat entre le client et l'entreprise.

Le concept d'hygiène des données définit la façon dont une entreprise traite ses données. Il décrit comment elles sont gérées et organisées et si elles sont correctement classifiées, stockées et protégées. Il s'applique aussi aux process et aux salariés. Un collaborateur qui ne stocke pas dans un endroit sécurisé les données sensibles et personnelles d'un client peut être accusé de ne pas prendre soin des données.

Il est dans l'intérêt de l'entreprise, aussi bien commercialement que pour son image, de promouvoir la responsabilité des données. Cependant, mettre en œuvre une bonne hygiène des données ne s'accomplit pas en une nuit.

Cela nécessite une stratégie claire, des processus robustes et une attention constante pour s'assurer que les standards sont bien respectés. Surtout, une bonne hygiène des données s'articule autour de deux axes majeurs : culturel et technologique. En résumé, les salariés doivent aussi bien avoir la volonté que les moyens technologiques de protéger les données de leurs clients et l'image de leur entreprise.

Beaucoup de données conduisent à de grandes responsabilités

Mettre en place une politique de conformité est une chose mais s'assurer qu'elle est bien appliquée, en est une autre.

La conformité n'est possible qu'avec l'engagement des collaborateurs de l'entreprise. Ces derniers sont généralement le talon d'Achille de la sécurité des données des entreprises. Selon une étude menée en 2018 par le Ponemon Institute, 60% des entreprises ayant été victimes d'une faille de données ont pointé du doigt une négligence humaine (provenant d'un salarié ou d'un prestataire).

Un manque de connaissance ou de motivation en matière de sécurité peut conduire à des données non nettoyées ou une mauvaise sauvegarde des informations sensibles sur les dispositifs personnels, abandonnant ainsi les données importantes dans des environnements non protégés.

L'un des enseignements les plus surprenants de GDPR est la façon dont la réglementation a encouragé les consommateurs à prendre le contrôle de leurs informations personnelles. Un an après l'application du règlement, les amendes se font plutôt rares, mais les demandes d'accès aux données sont en augmentation.

Une fois qu'une demande est faite, il ne reste plus qu'un mois pour se montrer conforme, ce qui peut être très difficile si les informations examinées ont été perdues dans le système ou mal identifiées.

Pourtant, le danger est plus important qu'il n'y parait. Il serait très facile pour un client ou un employé mécontent de faire valoir le droit de demande pour faire vaciller une entreprise ou une marque. Par exemple, un ancien employé qui aurait été congédié ou qui n'aurait pas été promu peut forcer l'entreprise à partager tous les renseignements qui ont servi à prendre cette décision.

Le demandeur est parfaitement dans son droit, mais un retard ou une incapacité à répondre – car les données pertinentes ne sont pas faciles à trouver – ne fait que complexifier et accroître les dangers auxquels font face les entreprises qui ne gèrent pas correctement les informations personnelles.

Les données désorganisées rendent les entreprises vulnérables et les exposent à des risques d'une atteinte à la protection des données très dommageable. Il suffit qu'un seul employé clique sur la mauvaise pièce jointe pour que tout le réseau soit infiltré. Les informations sensibles des clients – dossiers médicaux, coordonnées bancaires ou adresses – sont alors prêtes pour être recueillies si elles sont mal protégées.

L'approche de la carotte et du bâton

Il est facile de blâmer les employés mais ce n'est souvent qu'un symptôme révélateur d'un manque de leadership au sein de l'entreprise. La responsabilité des données doit concerner tous les niveaux et ce sont les dirigeants qui doivent décider des politiques de données et les mettre en place.
Aussi, de la même manière que les entreprises sont responsables des données de leurs clients, elles sont également responsables du comportement de leurs employés. Elles ont le devoir de veiller à ce que les bonnes pratiques soient appliquées par tous.

Heureusement, nombreuses sont celles qui commencent à prendre plus au sérieux leurs responsabilités en matière de données. Une de nos récentes études montre qu'elles s'adaptent en ajoutant des dispositions de conformité aux contrats des salariés, en prenant des mesures disciplinaires en cas de non respect des politiques et en éduquant les employés sur les avantages de la conformité. Les entreprises encouragent également les bons comportements en les intégrant dans le processus d'évaluation et en accordant des avantages aux bons élèves.

Une approche qui récompense les bons comportements et punit les mauvais est un bon point de départ, mais les entreprises ont également besoin de politiques qui intègrent la bonne gestion des données dans les habitudes de travail au quotidien – et pas seulement quand l'employé pense que quelqu'un pourrait le surveiller.

Une mauvaise hygiène des données n'est pas toujours due à la paresse, elle est souvent le résultat de la difficulté à garder les données organisées dans les environnements informatiques complexes et fragmentés d'aujourd'hui. Une considération plus pratique consiste à s'assurer que les employés disposent des bons outils de gestion pour faciliter les efforts de conformité.

Les données sont difficiles à protéger lorsqu'elles sont réparties dans une multitude d'environnements informatiques différents. Lorsqu'elles sont cloisonnées, elles sont facilement oubliées, exclues des dernières politiques de sécurité et deviennent vulnérables aux attaques.

A l'aide d'une plate-forme unique et centralisée, les employés pourraient comprendre de quelles informations ils disposent et où elles se trouvent. Cela leur garantirait également un accès chaque fois qu'ils en ont besoin.

Une bonne hygiène des données exige également que, si quelque chose tourne mal, ces dernières soient récupérables et que des solutions de sauvegarde fiables soient bien en place pour s'assurer que rien ne soit perdu.

Une bonne hygiène des données n'est pas facile à réaliser, mais elle est de plus en plus nécessaire. En fin de compte, cet objectif ne peut être atteint qu'en donnant aux équipes les encouragements, les incitations et les capacités technologiques nécessaires pour gérer et organiser correctement les informations dont elles disposent.
Les entreprises qui estiment avoir une hygiène des données irréprochable, observent une meilleure fidélisation de la clientèle, une augmentation des revenus et une vraie différenciation concurrentielle.