Comment bien protéger ses données

Vous êtes entrepreneur ? Maddyness vous a concocté un véritable kit des différentes étapes à suivre pour créer, faire grandir et même vendre votre startup. Du recrutement à la protection de votre marque en passant par le financement de votre innovation, vous retrouverez astuces et bonnes pratiques pour vous sortir de ce labyrinthe qu'est l'entrepreneuriat. Dans cette fiche : quelques conseils pour protéger correctement les données de votre entreprise.

Temps de lecture : minute

---

26 août 2019

TL;DR : ce qu’il faut retenir

- L’idéal est de prendre en compte la protection des données dès la conception de votre activité.
- Les mesures à prendre dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d’incident.
- Vos collaborateurs doivent eux aussi être sensibilisés et formés à la protection des données de l'entreprise
- N'hésitez pas à vous faire accompagner par un sous-traitant et une compagnie d'assurance.

Évaluer le niveau de sécurité de vos données.... et les risques potentiels

Ça n'est plus une surprise : toutes les entreprises, quelle que soit leur taille, sont aujourd'hui concernées par un véritable besoin de protection de leurs données, que celles-ci concernent des personnes tierces ou non. Entre perte de données, attaque informatique, virus et vol de matériel, les occasions sont nombreuses pour voir, du jour au lendemain, son entreprise en difficulté.

Avant toute chose, il vous faudra évaluer le niveau de sécurité des données disponibles
dans votre entreprise afin de définir le périmètre de ce qu'il vous faudra protéger. Posez-vous les bonnes questions : les comptes utilisateurs internes et externes sont-ils suffisamment protégés, notamment par des mots de passe d’une complexité suffisante ? Les accès aux locaux sont-ils assez sécurisés ? Existe-t-il une procédure de sauvegarde et de récupération des données en cas d’incident ? Quelles mesures ont déjà été prises pour assurer la sécurité des données collectées ou stockées ?

Une fois analysés les points les plus importants liés à la protection de vos données, identifiez les menaces réalisables ainsi que la gravité et la vraisemblance de ces risques, avant de déterminer les mesures existantes ou prévues qui permettraient de traiter chaque risque : contrôle d’accès,
sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation, etc.

Sensibiliser puis former ses collaborateurs à la data

L’élément humain est l'une des plus grosses faiblesses de la sécurité informatique d’une entreprise. Avant de se lancer dans un plan de formation concernant l'intégralité de vos collaborateurs, commencez donc par sensibiliser vos équipes à la data afin de leur faire prendre conscience de l'importance des données dans votre entreprise. Pourquoi ? Car si pour certains corps de métiers l'enjeu est évident, comme dans chaque transformation majeure des usages, le tournant data ne peut pas correctement être pris si ces nouveaux outils sont imposés, sans en donner les raisons, et sans acculturation préalable de ses équipes.

L’idée n’est donc pas d’imposer un outil et de nouvelles pratiques en interne mais d’accompagner les transformations culturelles liées à l’utilisation de la data. Si les collaborateurs d’une entreprise peuvent consulter et comprendre les chiffres et les données utilisées ou produites par l’entreprise, cela amène à plus de transparence, et un engagement facilité dans la prise en main de la data.

Une fois que vos équipes sont en mesure de comprendre en quoi la sécurité des données produites ou stockées par votre entreprise est un enjeu des plus importants, vous pourrez les former aux démarches à mettre en place en cas de perte ou de vol de matériel professionnel, de virus, de crash d'un disque dur, etc.

Enfin, la rédaction d’une charte informatique permet d'encadrer l'utilisation de vos réseaux et outils mais aussi sensibiliser et responsabiliser leurs utilisateurs aux bonnes pratiques de l’informatique.

Se doter d'outils de protection performants

Si certains rechignent encore à investir dans ces techniques de protection, réparer une perte ou un vol de données coûte à ce jour bien plus cher que d'anticiper. Des outils de sauvegarde interne et externe aux logiciels de gestion des données en passant par les logiciels de contrôle, les outils qui permettent aujourd'hui d'assurer la sécurité des données des entreprises ne manquent pas.

Attention cependant à s’informer sur les techniques utilisées par les pirates informatiques afin de pouvoir faire évoluer les moyens de protection mis en place dans votre entreprise.

Si vous le pouvez, faire appel à un sous-traitant reste une solution intéressante pour les entreprises n'ayant pas les capacités internes de gérer la sécurité de leurs données. Ceux-ci sont en effet en mesure de conseiller leurs clients sur la marche à suivre quant à la mise en œuvre de certaines obligations du RGPD.

S'assurer

Enfin, n'hésitez pas à vous renseigner auprès des compagnies d'assurance sur d'éventuelles solutions et services (responsabilité civile, dommages couverts…) qui pourraient vous permettre de sortir la tête de l'eau en cas de crise.

Article écrit par Iris Maignan