MyCercle
ESPACES DE PARTAGE ET DATA ROOMS

DÉVELOPPÉ & HÉBERGÉ EN FRANCE

8 décembre 2018

Entrepreneurs, une check-list de vos risques numériques et le moyen de les maîtriser

Faites un audit rapide de votre entreprise en passant en revue 14 risques liés aux pertes de données, à leur diffusion inappropriée ou à leur vol.

Les risques numériques auxquels une entreprise s'expose sont nombreux et diffus. Longtemps la bonne solution a été de ne rien numériser de confidentiel ; puis de ne rien partager numériquement. Mais la première puis la seconde stratégie sont devenues intenables depuis des années. Il n'est plus possible de conduire une activité professionnelle sans recours au numérique. Dès lors, la question devient : quels sont les risques liés à mes partages professionnels avec clients et collègues et comment les maîtriser au mieux ?

Maîtriser les risques numériques est complexe car on doit arbitrer entre deux dangers : celui de mal protéger les données partagées, ce qui n'est pas acceptable ; et celui de les protéger si bien qu'elles sont inaccessibles à vos interlocuteurs et qu'il n'y a plus de partage, quand rapidité et proximité sont essentielles.

A partir de notre expérience et de celle de nos abonnés nous avons défini une typologie des principaux risques auxquels est exposé une entreprise cabinet dans ses partages numériques ; et comment ces risques peuvent être éliminés ou fortement réduits. Ce peut être une check-list utile pour un audit rapide de votre propre structure.

Les 14 risques identifiés peuvent être regroupés en trois catégories :

- 3 risques se traduisent par des pertes de données : vous perdez l'accès à des données pourtant essentielles pour votre activité.
- 6 risques conduisent à la diffusion inappropriée de données : des données sont accessibles à des gens qui n'aurait pas dû y avoir accès.
- Enfin 5 risques concernent des vols de données : un facteur aggravant du cas précédent, puisque les voleurs feront mauvais usage de ces informations.

Cette typologie n'est pas figée : une diffusion inappropriée peut conduire à un vol, et celui-ci peut ou non s'accompagner d'une perte.

LES PERTES DE DONNEES

1. Perte de données par ransomware : un virus bloque votre ordinateur et tous les appareils liés et crypte tous vos documents les rendant inaccessibles. C'est l'un des risques les plus importants puisqu'il peut complètement bloquer l'activité de votre entreprise.

La course virus/anti-virus va continuer, avec périodiquement de nouvelles attaques de plus en plus vicieuses, et une amélioration des logiciels anti-virus. Une certitude : aucun virus n'est jamais entré par un extranet sécurisé (qui est l'architecture de MyCercle). Et si vos correspondants principaux envoient leurs documents par cet intermédiaire, le risque que vous ou un de vos collègues ouvriez naïvement un faux message de l'un d'eux (phishing) est très réduit. Néanmoins, cela ne servira à rien si vous continuez d'ouvrir des pièces jointes de correspondants inconnus, ou de brancher sur votre ordinateur des clés USB non contrôlées.

2. Perte de données par mauvaise manipulation de vous ou un de vos collaborateurs. Un risque impossible à éviter : tout le monde fait une mauvaise manipulation un jour.

Ce risque est fortement limité si votre extranet prévoit des sauvegardes systématiques et régulières, sans que vous ayez à vous en préoccuper.

3. Perte de données par panne informatique de votre entreprise : un serveur ou un ordinateur qui tombe en panne et est irréparable.

Des solutions techniques existent à base de sauvegardes régulières. Mais ces sauvegardes reposent souvent sur des processus humains : qui n'oublie jamais une sauvegarde ? Avoir ses données chez soi peut donc s'avérer beaucoup plus dangereux que les avoir sur un extranet, qui s'appuie sur un professionnel de l'hébergement chez qui ces processus de sauvegarde sont industrialisés.

LES VOLS DE DONNEES

4. Vol de données pendant leur transfert sur internet : quand votre entreprise les envoie, ou quand elle les reçoit en collecte de clients ou de partenaires.

La solution est désormais simple et bien connue : crypter les données pendant leur transmission (protocole HTTPS). Mais on oublie que cette sécurité n'est pas présente dans un échange par messagerie mail traditionnelle. Elle est bien entendu intégrée par un extranet sécurisé.

5. Vol de données dans votre entreprise ou chez un prestataire. Le problème n'est pas propre au numérique, mais le numérique permet d'emmener avec un disque dur des millions de pages.

La course cambrioleurs / coffres-forts va continuer. Une certitude : le stockage des informations sous forme cryptée chez un hébergeur sécurisé décourage tous les cambrioleurs et l'immense majorité des hackers.

6. Vol de données par vol/perte d'un de vos terminaux pendant un déplacement : portable oublié dans un train ou clé USB perdue dans un taxi… Le problème est bien plus ancien que le numérique, mais le numérique l'aggrave puisque vous pouvez perdre ou vous faire voler des centaines de dossiers en quelques secondes.

Il est encore plus recommandé aujourd'hui qu'hier d'éviter de transporter ses données avec soi. Un extranet évite d'avoir à le faire : vous retrouvez vos dossiers partout, sur n'importe quel terminal.

7. **Détournement de données** par un de vos collaborateurs.

Ce problème est aggravé par le numérique : un collaborateur malhonnête ou mécontent peut en quelques secondes siphonner l'équivalent de toute une armoire de documents. Vous pouvez limiter fortement ce risque si votre extranet, comme MyCercle, vous permet de facilement fixer (et modifier) qui a accès à quels dossiers.

8. Rediffusion de données confidentielles par la personne autorisée à les consulter.

Ce risque n'existe que dans certaines situations très particulières, du type audit d'acquisition. Votre extranet MyCercle intègre une option « data room » avec verrouillage des téléchargements, filigrane confidentiel dynamique et tracé de toutes les consultations. L'élément important est que la simplicité et le faible coût de cette data room permet de l'utiliser y compris pour de petites opérations. Alors qu'aujourd'hui la réalité est que seules les très grosses opérations bénéficient d'outils de protection « état de l'art ». Les autres opérations -l'immense majorité en nombre- sont gérées par des pièces jointes à des messages électroniques ou des portails gratuits qui n'apportent pas de garanties de sécurité.

LES CAPTATIONS INAPPROPRIEES DE DONNEES

9. Captation de données par votre prestataire informatique. Grands réseaux ou grands portails ont une attitude ambigüe sur la protection de vos données, ou de vos méta données (avec qui vous échangez) surtout dans leurs versions gratuites.

Un extranet sécurisé comme MyCercle vous garantit un engagement de confidentialité total.

10. Accès de tiers aux données par injonction d'une loi étrangère notamment la loi américaine (le Patriot Act et les lois qui ont pris sa suite).

Le risque est maintenant bien connu. La solution est également connue : un prestataire comme MyCercle vous garantit un hébergement en France.

11. Accès d'un tiers aux données par erreur de diffusion (de vous ou d'une autre partie à l'échange). C'est une erreur humaine, donc éternelle, mais qui devient très facile avec un outil comme la messagerie numérique, qui vous propose des adresses dont on n'a tapé que les premières lettres, ou encourage à répondre à des messages dont on n'a pas vérifié que la liste des destinataires en copie était toujours correcte.

Un extranet comme MyCercle a une approche par espaces homogènes qui limite au maximum les erreurs de diffusion, dans les deux sens. Vous et vos collègues contrôlez à chaque instant qui a accès à quoi dans un espace. Et vos invités dans cet espace n'ont aucun choix, donc aucune erreur possible : leur message ira automatiquement (selon votre paramétrage) à vous seulement ou à tous les participants à l'espace.

12. Violation involontaire par votre entreprise du Règlement européen de protection des données (RGPD).

Votre responsabilité est entière dans ce domaine et nul ne peut s'y substituer. Mais un extranet adapté au RGPD vous permet de limiter fortement vos risques et de le faire savoir à vos interlocuteurs.

13. Accès d'un tiers à des données qui auraient dû être supprimées.

« Internet n'oublie rien » et il est difficile de ne pas laisser de traces. Un extranet sécurisé comme MyCercle vous garantit que les données que vous effacez sont définitivement effacées de ses systèmes. Et que si vous ne renouvelez pas votre abonnement, tous vos informations sont détruites dans un délai d'un mois.

14. (Cas particulier des cabinets d'avocats) Accès des autorités à la correspondance de vos clients sans respect de l'article 56-1 du code de procédure pénale. Ce problème est bien plus ancien que le numérique, simplement le numérique accélère la possibilité de saisir des données puis de les explorer méthodiquement.

Un prestataire comme MyCercle vous garantit contractuellement qu'il se soumettra bien entendu à d'éventuelles réquisition d'autorités française mais qu'il aura bien le réflexe de demander le bénéfice de l'article 50 pour ses abonnés avocats.