La sauvegarde des données dans les PME

En cas de perte de données – suite à une attaque malveillante, à une erreur ou autre incident fortuit, toute PME doit pouvoir les récupérer rapidement et de la manière la plus complète possible. Il s'agit là d'une protection de base qui suppose la mise en place d'un processus efficace de sauvegarde des données.

Principaux conseils à suivre pour les entreprises :

- Établissez un inventaire de votre système informatique et de vos données et déterminez un seuil de tolérance maximal en cas de panne ou de perte.
- Sur la base de cet inventaire, constituez des classes de protection pour des éléments présentant le même niveau de risque, puis définissez un concept de sauvegarde des données pour chaque classe de protection.
- Définissez et mettez en place un processus de sauvegarde des données dans votre PME.
- Vérifiez régulièrement que les données sont correctement sauvegardées (conformément à la stratégie de sauvegarde établie) et qu'elles peuvent être restaurées.

Le processus de sauvegarde des données

Face à la digitalisation croissante, les PME sont confrontées à une augmentation constante de leurs systèmes informatiques et des données à traiter. Pour ces entreprises, cela se traduit par une dépendance accrue à l'égard de la disponibilité illimitée des systèmes et données informatiques.

Une perte de données importante – telle qu'elle pourrait se produire à la suite d'une cyberattaque, d'un problème technique, d'une catastrophe naturelle ou tout simplement à la suite d'une mauvaise manipulation informatique – peut avoir des conséquences très lourdes pour une PME, au point d'en menacer son existence même. La capacité de sauvegarder puis de restaurer rapidement et de la manière la plus complète possible les données d'une entreprise représente donc un élément de protection de base essentiel.

Cela passe par la mise en place d'un processus de sauvegarde des données conforme à la stratégie établie, sachant qu'il est tout aussi important de vérifier que les données sauvegardées puissent ensuite être restaurées.

Les classes de protection

Tous les systèmes informatiques d'une PME n'ont pas la même importance pour le fonctionnement d'une entreprise. Il convient donc d'établir des priorités entre les différents systèmes et types de données informatiques qui nécessiteront des niveaux de protection différents. Il faut donc commencer par établir un inventaire actuel de tous les systèmes et données informatiques qui permettra d'obtenir une vue d'ensemble mais aussi d'ordonner les différents éléments par classe de protection.

Exemple de classification sur la base de différents critères

CP	Dénomination	Risque	Seuil de tolérance max. en cas de panne/ perte	Délais de restauration	Délais de conservation
I	Protection normale	Faible	> 1 jour	< 1 semaine[/av_cell]> 1 semaine	
II	Protection forte	Moyen	1 jour	1 jour	> 1 mois
III	Protection très forte	Important	< ½ jour[/av_cell]> 1 an		

En plus des facteurs de risque mentionnés plus haut, d'autres critères sont également à prendre en considération, tels que l'évaluation de la durée maximale tolérée en cas de panne des systèmes informatiques et du volume des pertes pouvant être supporté, ainsi que les délais de restauration nécessaires.

C'est de cette manière que pourront se dégager des groupes de systèmes et de données informatiques nécessitant les mêmes niveaux de protection. Ces groupes vont ainsi former des classes de protection (CP). À chaque classe de protection on fera correspondre une stratégie de sauvegarde des données appropriée avec des dispositions bien précises.

La stratégie de sauvegarde des données

Pour chaque classe de protection, la stratégie de sauvegarde des données définit les modalités organisationnelles et techniques de la sauvegarde. Parmi les modalités de type organisationnel, citons en particulier :

1. le volume des données à sauvegarder (scope)
2. la périodicité de la sauvegarde (quotidienne, hebdomadaire, mensuelle...)
3. le moment auquel elle doit avoir lieu (fin de journée, week-end, fin de mois...)
4. les délais de conservation des données sauvegardées (schéma Grand-père-père-fils)
5. les délais de restauration requis (durée maximale tolérée de la panne)

À partir de là, on définit les détails techniques de la mise en œuvre de la stratégie, à savoir :

1. le type de sauvegarde (complète, différentielle, incrémentielle)
2. le support de stockage (disques durs, bandes, etc.)
3. la conservation des média de stockage (sur site, support physique ou en ligne sur le cloud, etc.)

Une perte de données importante – suite à une cyberattaque, à un problème technique, à une catastrophe naturelle ou à une mauvaise manipulation informatique – peut avoir des conséquences très lourdes pour une PME, au point d'en menacer sa survie.

Un mode de sauvegarde des données intelligent peut toutefois minimiser le risque et permettre une restauration rapide et la plus complète possible des données perdues.

Pour aller plus loin

Le **volume des données à sauvegarder** (scope) définit les données ou les sources de données devant effectivement faire l'objet de la sauvegarde. En établissant un inventaire réfléchi et structuré des données à sauvegarder, vous ferez en sorte de ne pas oublier de données vitales pour l'entreprise. Il importe également de vérifier que les données ou sources de données à sauvegarder sont effectivement disponibles au moment prévu (ex. extinction des ordinateurs pendant le week-end).

Une **périodicité de sauvegarde** rapprochée assure certes des pertes de données de moindre importance, mais accroît fortement la charge de la sauvegarde. Il peut arriver par exemple que le réseau se trouve bloqué en raison des grandes quantités de données à sauvegarder tous les jours. D'où l'importance de bien évaluer les différents besoins en protection.

Le **moment de la sauvegarde des données** doit être choisi en fonction du mode de fonctionnement de l'entreprise, en tenant compte du risque de perte de données entre deux sauvegardes. Beaucoup d'entreprises optent pour la fin de journée, à un moment où les sauvegardes ne risquent pas de perturber les activités quotidiennes et où elles peuvent au contraire utiliser les ressources libérées pendant la nuit.

En cas de perte de données, l'entreprise peut généralement récupérer la dernière sauvegarde effectuée. Mais il peut s'avérer nécessaire, pour différentes raisons, de restaurer des données sauvegardées précédemment. Voilà pourquoi il convient d'établir des **délais de conservation pour les données sauvegardées**. Un système de rotation réfléchi (basé sur le schéma « grand-père-père-fils ») adapté aux volumes de données traitées et aux besoins de protection de l'entreprise permet de conserver plusieurs sauvegardes successives sur un minimum de supports. Avec une sauvegarde quotidienne des données (lun-ven) et 20 supports de stockage seulement, il est possible de restaurer les sauvegardes des quatre derniers jours de la semaine (lun-jeu), des 13 derniers week-ends (vendredi), des deux dernières fins de mois et de la dernière fin d'année.

Le **délai de restauration requis** correspond au laps de temps qui s'écoule entre le moment où l'on constate la perte des données et le moment où celles-ci sont de nouveau accessibles. Plus ce délai est court, plus les exigences techniques et organisationnelles du processus de sauvegarde sont élevées. Pour le définir, il faut tenir compte du temps nécessaire à l'identification des données à restaurer, à leur localisation dans le catalogue de sauvegarde, à l'accès aux supports de stockage et à la restauration effective des données.

Il peut arriver que le temps à disposition (p. ex. la nuit) ne soit pas suffisant pour sauvegarder toutes les données d'une certaine classe de protection conformément à la périodicité définie. Pour pallier le problème, on détermine également le **type de sauvegarde** (sauvegarde complète, différentielle, incrémentielle). Dans le cas d'une sauvegarde **complète**, on réalise une copie complète de toutes les données répertoriées dans le scope sur le médium de sauvegarde. Cette méthode est très gourmande en espace de stockage et nécessite également beaucoup de temps. Dans le cas de la sauvegarde **différentielle**, il s'agit en revanche de sauvegarder uniquement les données modifiées ou ajoutées depuis la dernière sauvegarde complète. Cette méthode permet de réduire considérablement le volume des données à sauvegarder dans la mesure où les données non modifiées ne sont sauvegardées qu'une seule fois. La restauration des données se fait dans ce cas en deux étapes : la restauration de la dernière sauvegarde complète dans un premier temps, puis celle de la sauvegarde différentielle souhaitée. La sauvegarde **incrémentielle** réduit encore ultérieurement le volume des données à sauvegarder puisqu'il s'agit dans ce cas de sauvegarder uniquement les données modifiées ou ajoutées depuis la dernière sauvegarde effectuée (indépendamment

du type). Pour récupérer les données sauvegardées, il est nécessaire de restaurer la dernière sauvegarde complète, la dernière sauvegarde différentielle ainsi que toutes les sauvegardes incrémentielles successives.

Lorsque l'on parle du **médium de sauvegarde**, on fait référence au matériel qui assure le stockage des données sauvegardées. Dans les cas les plus simples, il peut s'agir d'un simple fichier au format spécial ou d'un support de stockage physique (disques durs, supports optiques, bandes magnétiques, etc.) inséré dans un système de sauvegarde dédié. Le choix du médium de sauvegarde dépend en premier lieu des exigences organisationnelles (volume, périodicité, délais de conservation et de restauration). Les bandes magnétiques sont le plus souvent utilisées pour le stockage à long terme (archivage) de grosses quantités de données.

Le choix des média de sauvegarde et leur **conservation** revêtent une importance cruciale dans le processus de sauvegarde. Au moment d'évaluer les risques, il convient de tenir compte d'un certain nombre de facteurs tels que la protection physique, les conditions de stockage, la disponibilité, l'accessibilité, etc. En règle générale, les sauvegardes doivent être protégées le plus possible contre les agents extérieurs. Si l'on considère les risques liés aux rançongiciels par exemple, mieux vaut s'assurer que les sauvegardes restent hors de leur portée, c'est-à-dire hors ligne.