Sauvegarde – bonnes pratiques

Pour faire face aux risques d'attaque, il est impératif de prévoir une stratégie de sauvegarde robuste. En effet, pour réduire la perte de données potentielle, un bon système de sauvegarde permet de perdre un minimum de données et un minimum de temps pour un retour à la normal. Pour ce faire, il faut s'interroger et répondre aux questions qui vont suivre.

1. Commencez par une stratégie de sauvegarde

La meilleure pratique en matière de sauvegarde des données consiste à créer un plan détaillé qui expose les objectifs spécifiques de votre entreprise. Ce plan est souvent inclus dans un plan de continuité des activités (PCA) ou un plan de reprise d'activité (PRA).

PCA : Il s'agit de l'ensemble des mesures visant à assurer, selon divers scénarios de crise, le maintien des prestations de service essentielles à l'entreprise. Un plan de continuité d'activité comprend l'analyse des risques, afin de pouvoir faire face à plusieurs scénarios.
Le plan de continuité des affaires prévoit le maintien des prestations de services essentielles de l'entreprise, comme par exemple le travail de certains services sur un site de repli. Puis, la reprise planifiée des activités.

Soit la démarche est inscrite dans un processus globale de la société, soit elle est liée à un service critique ou central si l'entreprise n'est pas mature pour faire cette démarche.
Pour un service IT, cette démarche est centrale et pourra faire l'objet d'une prochaine synthèse.

PRA : Le PRA désigne l'**ensemble des procédures et moyens matériels, technologiques et humains** permettant de rétablir et de reprendre l'activité de l'entreprise après la survenue d'un incident.

Alors que le Plan de Continuité d'Activité (PCA) organise la poursuite des activités de l'entreprise en cas d'incident, le Plan de Reprise d'Activité anticipe une interruption de l'activité et prévoit les conditions de sa reprise. Ainsi, le PRA est complémentaire du PCA, et sera à privilégier en cas de crise soudaine. Il intègre des ajustements tels que l'activité en mode dégradé ou l'activité partielle.

Avant même de rentrer dans le comment, il faut réfléchir :

- Les risques de pertes de données diverses (rançon, etc.)
- Impact de ces événements sur diverses opérations (productivité, pertes financières, etc.)
- Les objectifs de restauration des données suffisamment rapide pour réduire le poids de cet impact (objectifs de points de récupération, objectifs de temps de récupération, etc.)

2. Objectif primordial : La continuité des activités !

Il convient de prendre la mesure de l'importance de la sauvegarde. Il faut se méfier des solutions de sauvegarde « légères » qui se contentent de répliquer vos données sur un disque externe ou un dossier cloud. Lorsque vous comparez vos options, tenez-vous en aux solutions qui assurent la continuité des activités, c'est-à-dire qui contribuent à maintenir votre entreprise en activité après un sinistre sur vos infrastructures informatiques.

La différence est qu'une simple sauvegarde des fichiers est inutile si toutes les applications et les systèmes d'exploitation sur lesquels elles fonctionnent, sont infectés par un logiciel de type rançon.
Ou, s'il faut des jours pour restaurer les données d'une sauvegarde, il pourrait être trop tard.

Les solutions de continuité des activités et de reprise après sinistre sont conçues pour offrir des options de reprise robustes, de sorte que les opérations critiques puissent se poursuivre avec un minimum d'interruption.

3. Sauvegarder fréquemment les données

Définir la fréquence des sauvegardes revient à définir le RPO (Recovery Point Objective) ou la PDMA (Perte de Données Maximale Admissible).

Selon la criticité du programme, on peut « accepter » une perte de données de X unités de temps.

Pour des données quasiment statiques, on peut accepter d'avoir une sauvegarde hebdomadaire par exemple. Pour des données d'exploitation de production, on peut accepter parfois 5 minutes de perte.

Il va falloir définir pour les différentes applications la fréquence optimale en fonction d'une grille de points objectifs comme :

- la criticité des données
- la fréquence de modification
- l'utilisation
- la sensibilité (données RGPD)
- …

Les points constituant la grille de définition sont à définir et doivent être pondérés en fonction des attentes finales du système de sauvegarde.

4. Utiliser le stockage à distance

Les sauvegardes sur site sont toujours la clé de la rapidité. Cependant, il est primordiale d'avoir une sauvegarde hors site.

En effet, en cas d'incendie ou d'inondation, si les sauvegardes sur site sont détruites, il n'y a aucun moyen de récupérer les données.

Le mode de stockage hors site peut s'opérer de diverses façon allant de la récupération d'un support de stockage le soir par un représentant de l'informatique, à des sauvegardes Cloud.

Le stockage à distance ne doit pas être utilisé comme une alternative au stockage sur site. Les meilleures solutions de sauvegarde actuelles pour les petites entreprises offrent une protection hybride, qui conserve les sauvegardes sur site et dans le Cloud pour la plus grande assurance contre tous les scénarios de catastrophe.

5. Temps de conservation des sauvegardes

Une réflexion sur la durée de conservation des sauvegardes doit être entreprise en fonction de chaque applicatifs.
On doit prendre en compte le point 3 mais pas seulement.
Certaines données doivent légalement être conserver pendant une durée déterminée, la sauvegarde doit donc le prendre en compte.

À titre d'exemple, voici à quoi pourrait ressembler une configuration de conservation des données pour une entreprise utilisant des solutions de sauvegardes optimisées.

- *Sauvegardes locales : conservées pendant 3 mois*
- *Sauvegardes intra-journalières : conservées pendant 7 jours*
- *Sauvegardes quotidiennes : conservées pendant 2 semaines*
- *Sauvegardes hebdomadaires : conservées pendant 1 mois*
- *Sauvegardes mensuelles : conservées jusqu'à la suppression des sauvegardes locales*

6. Les sauvegardes ne doivent pas permettre l'accès à Internet

Un dispositif de sauvegarde doit être capable de transmettre des données, mais il ne doit pas permettre de communication entrante. Le dispositif doit être déployé dans un environnement LAN sécurisé et même les communications sortantes doivent être limitées à celles qui sont nécessaires au dispositif pour effectuer les sauvegardes dans le cloud. Toutes les autres communications doivent être refusées pour garantir une sécurité maximale.

7. Chiffrement des sauvegardes

Il est primordiale que les données soient chiffrées (le terme crypté peut être utilisé). En effet, les sauvegardes non chiffrées peuvent être récupérées et clairement lisibles.

Le chiffrement doit être opérant tant pendant le transit qu'au repos. Cela signifie que les données restent cryptées lorsqu'elles sont téléchargées vers le cloud, ainsi que lorsqu'elles sont stockées sur le dispositif de sauvegarde et/ou dans le centre de données.

Le cryptage AES (256) est simple à mettre en œuvre et reste à ce jour considéré comme inviolable.

8. Tester régulièrement les sauvegardes

Ce n'est pas parce que vous avez une sauvegarde qu'elle peut être restaurée. Les sauvegardes incrémentielles traditionnelles sont réputées pour la corruption des données, en raison de la façon dont les erreurs se produisent dans la chaîne de sauvegarde à chaque ajout d'une nouvelle sauvegarde incrémentielle.

Les sauvegardes doivent être testées régulièrement pour s'assurer qu'elles peuvent être restaurées. Idéalement, votre système de sauvegarde devrait disposer d'un processus automatisé qui valide automatiquement chaque nouvelle sauvegarde et vous avertit en cas de problème.

Selon la taille de vos bases de données et le SGBD choisit, une sauvegarde complète et systématique peut être envisagée.

La volumétrie et la capacité de stockage est la clé pour un choix éclairé.

9. Restaurer les données en fonction de la catastrophe

Suivant la solution de sauvegarde mise en place, vous aurez de nombreuses possibilités de restauration des données, en fonction de la situation. Vous ne devriez pas avoir besoin de faire une restauration complète de sauvegarde simplement parce qu'un seul dossier critique a disparu.

Pour les fichiers et dossiers individuels, une restauration au niveau du fichier sera le moyen le plus rapide et le plus efficace de restaurer les données perdues.

Pour les pertes de données plus importantes, vous voudrez probablement revenir au point de récupération le plus récent, ou utiliser des options de restauration incrémentales, qui ne restaure que les fichiers qui ont été modifiés depuis la dernière sauvegarde.

Dans les cas où une machine protégée n'est plus amorçable, une restauration à nu peut s'avérer nécessaire. Le choix de l'option de restauration appropriée est essentiel pour minimiser l'impact de la perturbation et récupérer les données perdues aussi rapidement et efficacement que possible.

Source originale : https://www.flexmarket.fr/blog/tests-produits/les-bonnes-pratiques-de-la-sauvegarde-dossier-pour-les-tpepme