Fiche-conseils

SAUVEGARDER SES DONNÉES SANS RISQUE

Les données sont un élément vital et un atout précieux de la société moderne. Leur perte peut non seulement causer des dommages importants, au niveau financier par exemple, mais également perturber les opérations commerciales ou bien encore les échanges.

Sauvegarder ses données - c'est-à-dire copier ou archiver des données pour les restaurer si elles sont perdues ou endommagées - est donc essentiel tant pour les entreprises que pour les particuliers, également confrontés à des enjeux de conservation.

Définition d'une sauvegarde performante

Une sauvegarde de données performante combine fiabilité, protection contre les menaces de sécurité et optimisation des ressources. Cette combinaison lui permet de garantir une restauration précise et rapide des données, en cas de perte.

1

Une sauvegarde fiable

Les données sauvegardées sont récupérables de manière cohérente et précise. Des sauvegardes régulières, une à plusieurs duplications d'une source principale vers un à plusieurs emplacements et supports de stockage secondaire sont indispensables.

2

Une sauvegarde sécurisée

Les données sauvegardées sont protégées contre tout accès non autorisé, leur intégrité est garantie et le cryptage et les contrôles d'accès - permettant d'empêcher les violations et la fuite de données - sont utilisés.

3

Une sauvegarde efficace

L'espace de stockage, la puissance de traitement pendant la sauvegarde ou la restauration et la bande passante du réseau sont autant de ressources qui doivent être optimisées.

FIABILITÉ + **SÉCURITÉ** + **EFFICACITÉ** = **SAUVEGARDE PERFORMANTE**

Pourquoi sauvegarder ?

Sauvegarder c'est résoudre quatre problèmes auxquels les entreprises ou organisations - au même titre que les particuliers - sont confrontées dans leurs activités quotidiennes :

- Tout ordinateur ou ses composants - tels que les disques durs - peuvent tomber en panne (panne logicielle ou matérielle).
- **Tout le monde peut faire des erreurs** (mauvaise manipulation ou suppression accidentelle de fichiers, etc.)
- **Tout le monde peut être victime d'une cyberattaque** (menaces de sécurité).
- **Les catastrophes surviennent toujours au moment où on s'y attend le moins** (sinistres ou catastrophe naturelle).

En cas de perte, suppression ou corruption de vos données, la sauvegarde est votre seule alliée.

restena
réseau · sécurité · .lu

Conseils pour mettre en place une sauvegarde performante

Une sauvegarde performante repose sur la mise en place d'objectifs de sauvegarde clairs basés sur une évaluation des données et la mise en place d'une stratégie de sauvegarde répondant à une série de questions incontournables. En entreprise, des politiques et obligations peuvent influencer cette stratégie, certaines, par exemple, n'autorisant pas la sauvegarde des données sur un *cloud* public. Posez vous donc les bonnes questions avant d'envisager une sauvegarde.

Quelles données doivent être sauvegardées ?

Toutes les données que vous possédez n'ont pas la même importance. Déterminez pour chacune d'entre elles si elle mérite d'être sauvegardée : sont-elles critiques et/ou des exigences réglementaires en matière de conservation de données s'appliquent-elles ?

À quelle fréquence sauvegarder les données ?

Les données à sauvegarder identifiées, définissez la fréquence à laquelle la sauvegarde doit être effectuée : une fois par semaine, par mois, par année ? C'est à vous de décider du rythme, mais il doit être cohérent, régulier, et constant.

Astuce !

Pour réduire le risque d'erreur humaine, pensez à automatiser vos sauvegardes grâce à des logiciels ou scripts de sauvegarde automatisés.

Combien de temps conserver les données ?

Le temps de conservation des données dépend de la nature des données. Les données à caractère personnel, par exemple, sont soumises au Règlement Général sur la Protection des Données (RGPD). Les documents généraux des entreprises, quant à eux, répondent aussi à des exigences légales de conservation qu'il convient de respecter.

Sur quel support stocker les données ?

Il existe deux grands types de support - la sauvegarde locale et la sauvegarde *cloud*. À vous de choisir celui qui vous convient le mieux.

SAUVEGARDE LOCALE

La sauvegarde locale est un stockage physique, de type disques durs externes, bandes magnétiques ou stockage en réseau.

Caractéristiques

Les données sont stockées sur le site principal d'une entreprise ou d'une organisation. Les sauvegardes sont fréquemment effectuées sur des disques durs internes ou externes.

Points forts

- Restauration des données rapide
- Contrôle des données
- Confidentialité garantie

SAUVEGARDE CLOUD

La sauvegarde *cloud* a recours à des solutions basées sur le *cloud*, de type *cloud* public, *cloud* privé ou '*cloud to cloud* (C2C).

Caractéristiques

Les données sont stockées sur un serveur ou un système de stockage situé hors site, généralement hébergé par un fournisseur de sauvegarde externalisé.

Points forts

- Stockage hors site
- Reprise après sinistre simplifiée

La règle de sauvegarde 3-2-1

Pour assurer une sauvegarde optimale, conservez plusieurs copies de sauvegarde.

- **3** copies de vos données d'origine (données originales incluses)
- **2** copies de sauvegarde sur des supports différents
- **1** copie stockée 'hors site', c'est-à-dire dans un autre emplacement (un autre bâtiment, un autre environnement informatique, tel que le *cloud*, etc.)

La copie 'hors site' permet notamment de se prémunir contre les catastrophes physiques - telles qu'incendies, inondations ou vols - qui pourraient intervenir sur le site principal de conservation des données.

N'attendez pas que vos données disparaissent pour mettre en place votre plan de sauvegarde !

Protéger les sauvegardes des cyberattaques

Même si elle constitue la meilleure solution face aux attaques *ransomware* (ou rançongiciel); des attaques qui prennent en otage les données présentes sur l'ordinateur de leurs victimes contre une rançon monétaire; la sauvegarde est elle aussi la cible de cette technique employée par les cybercriminel-le-s.

Isoler physiquement les supports de stockage

L'isolation physique consiste à déconnecter les supports de stockage du réseau. Le support de stockage étant totalement hors ligne, il reste protégé contre les *malwares* (ou logiciels malveillants), virus ou *ransomwares* qui pourraient se propager à travers les systèmes connectés.

Assurer l'immuabilité des sauvegardes

Une sauvegarde immuable est une copie de données qui ne peut être en aucun cas altérée, supprimée ou modifiée. Dans un tel cas, même les administrateurs-rices système, les utilisateurs-rices, les applications ou systèmes qui ont créé ces données ne peuvent les altérer.

Chiffrer les données

Chiffrer les données protège contre les utilisations abusives et les fuites de données exfiltrées (*data exfiltration / data leaks*). Même si cela n'offre pas de protection contre le (re)cryptage par *ransomware*, cela garantit que vos données sont inutilisables. Grâce au chiffrement, les données sont converties d'un format lisible à un format codé et ne peuvent être lues que par le propriétaire des données ayant la bonne clé de chiffrement.

Exemple : La vulnérabilité de la recherche et l'éducation

La nature diversifiée des données, la variété des systèmes utilisés et la nécessité d'une protection solide des informations sensibles posent des défis uniques au secteur de la recherche et de l'éducation. Ce secteur est particulièrement vulnérable de par ses sources de données distribuées, le type d'informations sensibles et exclusives - allant des dossiers des étudiants aux résultats de recherche de pointe - qu'il traite, la diversité et la complexité des structures de données et plateformes et systèmes technologiques auxquelles il est confronté.

Ces défis nécessitent d'être relevés grâce à des solutions adaptées incluant plans de sauvegarde robustes, formations sur les meilleures pratiques, investissement dans des outils de sauvegarde conviviaux, méthodes de chiffrement appropriées et plan complet de reprise après sinistre.

Recommandations et responsabilités

Définissez des stratégies claires et documentées.

Identifiez vos besoins en matière de protection des données puis documentez votre stratégie de sauvegarde, et les éventuelles procédures associées, pour garantir une compréhension claire des processus et responsabilités.

Respectez la sécurité et la conformité règlementaire des données.

Assurez-vous que vos pratiques de sauvegarde sont conformes aux réglementations en vigueur en matière de protection et de confidentialité des données et qu'elles respectent d'éventuelles politiques de sécurité mises en place dans votre organisation.

Révisez, testez et améliorez régulièrement votre plan de sauvegarde.

Régulièrement ou à chaque changement dans la structure des données, les avancées technologiques, les besoins et obligations de stockage, passez en revue votre plan de sauvegarde – sans oublier de tester le processus de restauration des données – et adaptez-le si nécessaire.

→ ***Vos sauvegardes doivent être fiables et fonctionnelles à tout instant. Au moindre doute, revoyez et adaptez votre plan de sauvegarde.***

Offre de services

Grâce à son équipe de réponse aux incidents de sécurité informatique (Restena-CSIRT), la Fondation Restena aide la communauté luxembourgeoise de la recherche et de l'éducation confrontée à des incidents de sécurité informatique. Elle réalise également des campagnes de phishing et de sensibilisation sur mesure sur des sujets d'actualité, et co-organise des conférences, telles que CyberDay.lu et Data Privacy Day.

Pour plus d'informations sur ce service, rendez-vous sur restena.lu/CSIRT

Co-funded by the European Union

Cette fiche-conseils est l'une des activités de sensibilisation mises en place dans le cadre du projet européen LuCySe4RE, financé par le programme Digital Europe de l'Union européenne (DIGITAL) dans le cadre de la convention de subvention n° 101127864.

restena
réseau · sécurité · .lu