Cyberconseils : Politiques de sauvegarde

VICTOR

Les données sont la partie la plus précieuse d'un système informatique et peuvent être irremplaçables si elles sont perdues à cause d'une attaque par logiciel de rançon ou d'une défaillance matérielle, ou si elles sont corrompues. Les conseils suivants vous aideront à planifier et à préparer une politique de sauvegarde en cas d'incident, au cas où le pire se produirait.

Qu'est-ce qu'une politique de sauvegarde?

Une politique de sauvegarde est un plan bien pensé pour atténuer la perte de données qui pourrait survenir en raison d'une attaque par logiciel de rançon, d'une défaillance matérielle, d'une corruption des données ou de tout autre événement préjudiciable. Si elle est bien mise en œuvre, elle peut aider une organisation à reprendre ses activités plus rapidement et plus facilement.

La complexité de la politique de sauvegarde dépendra de la taille de l'entreprise, du nombre d'applications et de bases de données qu'elle utilise et de la quantité de données à sauvegarder. Elle dépendra également de la politique de l'entreprise et des obligations réglementaires applicables à l'organisation.

Comment mettre en œuvre une pratique exemplaire en matière de politique de sauvegarde?

1 Déterminez vos données les plus critiques et planifiez en conséquence

En déterminant les données les plus critiques pour votre entreprise, des ressources peuvent être allouées pour garantir que ces données sont protégées et classées par ordre de p riorité. Les copies de sauvegarde peuvent être adaptées en conséquence à ces données particulières.

2 Faites des copies de sauvegarde fréquentes

Si vous disposez de données critiques, vous devez prêter attention à la fréquence des copies de sauvegarde effectuées.

3 Utilisez l'approche 3-2-1 pour les copies de sauvegarde

Créez trois copies de vos données en plus du fichier original, en utilisant deux types de supports de sauvegarde différents stockés localement et une copie stockée à distance.

Les copies de sauvegarde doivent être isolées ou isolées du réseau lorsqu'elles ne sauvegardent pas activement les données. Les supports de copie de sauvegarde ne doivent jamais être connectés en permanence physiquement ou sur le réseau.

4 Utilisez des versions de données

Les copies de sauvegarde doivent contenir d'anciennes versions de vos données, pas seulement les versions actuelles des fichiers sauvegardés le plus récemment. C'est important en cas de corruption de fichiers ou de logiciel de rançon qui peuvent se cacher dans les copies de sauvegarde de données actuelles.

5 Testez périodiquement l'intégrité de vos copies de sauvegarde

Les données devraient être vérifiées régulièrement pour s'assurer qu'elles sont accessibles et lisibles.

Autres considérations pour votre politique de sauvegarde

- Les données doivent être cryptées lorsqu'elles sont sauvegardées. Cela permettra d'éviter tout accès non autorisé.
- Pensez à rendre vos copies de sauvegarde immuables, afin qu'elles ne puissent pas être modifiées par vous ou par des cybercriminels.
- Envisagez d'utiliser le stockage à distance. Le stockage dans le nuage peut être une option rentable si elle est gérée correctement.
- Automatisez les sauvegardes lorsque cela est possible. Ainsi, la pratique de la sauvegarde de vos données fera partie de vos activités quotidiennes.
- Tenez compte de la durée de conservation de vos copies de sauvegarde. Ceci est particulièrement important si vous utilisez des services en nuage pour sauvegarder vos données. Les coûts de stockage des données dans le nuage peuvent s'accumuler. Déterminez donc une durée de conservation raisonnable dans votre politique de sauvegarde – et tenez compte des obligations légales et réglementaires.
- Réfléchissez à votre politique de conservation des données. Avez-vous réellement besoin de toutes les données que vous stockez et sauvegardez? Souvent, les données sont stockées inutilement, ce qui ajoute un coût inutile et entraîne des charges de sécurité supplémentaires si elles sont exposées.

Renseignements supplémentaires

- Gouvernement du Canada – Centre canadien pour la cybersécurité
  - › Sauvegarder et récupérer vos données
  - › Sauvegarder et chiffrement des données
- Ressources cybernétiques de Victor
  - › Assurance contre les cyber-risques de Victor
  - › Guide : Risques liés à la cyber-responsabilité : Comment vous protéger, ainsi que votre entreprise
  - › Guide : Cybersécurité : Travailler en toute sécurité depuis son domicile
  - › Infographie : Les cyberattaques : Une menace pour toutes les entreprises
  - › Vidéo : Une journée dans la vie d'un propriétaire d'entreprise dans un cybermonde
  - › Vidéo : Les experts de Victor partagent les mesures préventives alors que les cyberattaques se multiplient

#LaMenaceEstRéelle

Visitez assurancevictor.ca/cyber.