Sauvegarder et récupérer vos données

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Juin 2024 | ITSAP.40.002

La sauvegarde des informations organisationnelles est l'une des mesures que vous pouvez prendre pour améliorer la cybersécurité et la résilience de votre organisation. Si vos réseaux, vos systèmes ou vos informations sont compromis, une copie sauvegarde permettra à votre organisation de reprendre ses activités plus rapidement.

Pourquoi les sauvegardes sont-elles nécessaires?

Des incidents imprévus, comme des cyberattaques ou des catastrophes naturelles, peuvent se produire. Vos sauvegardes constituent en quelque sorte une police d'assurance. En cas d'incident, vos sauvegardes sont essentielles pour deux raisons.

- **Disponibilité :** Protéger la disponibilité des systèmes et des données est un élément essentiel de la cybersécurité. Les sauvegardes permettent au personnel, aux partenaires et à la clientèle de continuer à accéder à l'information requise en temps opportun.
- **Récupération :** C'est le processus qui consiste à restaurer les systèmes et informations. En cas d'incident, vous pouvez :
  - utiliser vos sauvegardes pour rétablir vos systèmes;
  - assurer la reprise des activités de votre organisation le plus rapidement possible;
  - réduire au minimum la perte d'informations, de temps et d'argent causée par la période d'indisponibilité.

Types de sauvegarde

- **Sauvegarde complete :** Il vaut mieux faire une sauvegarde complète régulièrement (chaque semaine ou mois) et avant toute mise à niveau majeure. C'est l'option la plus coûteuse et la plus longue, selon la quantité d'informations à sauvegarder et les besoins en matière de stockage.
- **Sauvegarde différentielle :** Ce type de sauvegarde consiste à faire seulement une copie des données qui ont changé depuis la dernière sauvegarde complète
- **Sauvegarde incrémentielle :** Ce type de sauvegarde consiste à stocker uniquement les données qui ont changé depuis la dernière sauvegarde complète ou différentielle. Chaque nouvelle sauvegarde est enregistrée en tant que volume incrémentiel. Concrètement, si vous devez restaurer des données, vous devez traiter chaque incrément, ce qui peut prendre du temps.

Votre processus de sauvegarde doit inclure la déduplication des données pour éviter de stocker des données excédentaires ou redondantes. La déduplication réduit les coûts liés aux sauvegardes et permet de sauvegarder et de stocker efficacement les données.

Quand une sauvegarde est-elle nécessaire?

Voici quelques exemples de cas où une sauvegarde de l'information organisationnelle s'avère extrêmement utile.

Panne d'électricité

Une panne d'électricité peut causer l'arrêt du fonctionnement des systèmes et appareils électroniques, des temps d'arrêt ou des pannes qui peuvent avoir des répercussions sur les activités et les processus opérationnels. Les sauvegardes peuvent garantir que votre organisation ne perd pas de données critiques à cause d'une panne, d'un arrêt soudain des systèmes ou d'une panne d'électricité imprévue.

Rançongiciel

Un rançongiciel est un type de logiciel malveillant qui vous empêche d'accéder à vos systèmes, appareils et fichiers jusqu'à ce que vous payiez une rançon à l'auteur de la cybermenace. Grâce aux sauvegardes, vous n'aurez probablement pas besoin de payer la rançon (le paiement de la rançon peut aussi être inutile, car il ne garantit pas la restitution de vos données). Notez bien que les sauvegardes peuvent vous aider à restaurer vos systèmes et vos informations, mais qu'elles n'empêcheront pas un auteur de cybermenace de vendre ou de divulguer les données volées.

Attaque par déni de service

Lors d'une attaque par déni de service, les auteurs de cybermenace inondent la cible (p. ex., un serveur) de trafic pour causer une panne des systèmes et empêcher l'accès aux sites Web et services internes. Les auteurs de menace utilisent ce type d'attaque pour perturber les services et les activités opérationnelles ou pour créer une diversion et voler des données pendant les efforts de récupération. Avec des sauvegardes et un plan de reprise des activités, vous pouvez minimiser les temps d'arrêt pendant la récupération.

Catastrophe naturelle

Les incendies, les inondations et les tremblements de terre sont des choses qui arrivent. La plupart des entreprises ont des plans d'urgence en cas de catastrophe et la sauvegarde des informations devrait toujours faire partie de ces plans. Les catastrophes naturelles peuvent endommager les édifices et les biens physiques, ce qui pourrait vous empêcher d'y avoir accès. C'est pourquoi des sauvegardes qui se trouvent à un autre emplacement (hors site ou dans le nuage) pourraient être très utiles pour la reprise des activités.

Équipement perdu ou volé

La perte ou le vol d'un appareil, comme un téléphone ou un ordinateur portable, peut entraîner la perte complète des données non sauvegardées. La sauvegarde des données organisationnelles permet d'assurer la reprise des activités rapidement.

Même s'ils ne touchent pas directement votre organisation, ces événements peuvent avoir un impact. Par exemple, si une catastrophe naturelle ou un cyberincident touche votre fournisseur de services liés au nuage, votre organisation pourrait connaître un temps d'arrêt qui aurait des répercussions sur vos activités.

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, [2024]

Canada

No de cat. D97-1/40-002-2024F-PDF ISBN 978-0-660-70857-7

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Juin 2024 | ITSAP.40.002

Où peut-on stocker les copies sauvegardes

Un processus de sauvegarde adéquat améliore la résilience organisationnelle. Il permet ainsi une reprise efficace des activités après une cybermenace. Trois options de stockage sont possibles :

- sur site (dans les locaux);
- hors site;
- dans le nuage.

Toutes ces options ont des avantages et des inconvénients. En fin de compte, il faut choisir l'option qui correspond le mieux aux besoins organisationnels et aux exigences en matière de sécurité. Lorsque vous prenez votre décision, tenez compte du niveau d'importance des systèmes et des données et de la rapidité avec laquelle vous auriez besoin de les restaurer.

Stockage sur place

Avec le stockage sur place, vous stockez vos sauvegardes dans l'espace physique de votre organisation. Le stockage sur place est pratique et peut être rapide. Les sauvegardes sont facilement disponibles si vous devez lancer votre processus de récupération.

Toutefois, la perte de données est toujours possible si les sauvegardes sont stockées uniquement sur place. Ce serait le cas, par exemple, si l'ensemble de vos locaux sont incendiés ou inondés. Nous vous recommandons de stocker une copie à un autre emplacement, hors site, pour éviter la perte des données.

Il y a divers types d'appareil de stockage que vous pouvez utiliser pour stocker vos données sur place.

Le support de stockage amovible est pratique et relativement économique. Toutefois, ces supports peuvent être endommagés, volés ou perdus. Le support doit être retiré de votre appareil après la sauvegarde afin de le protéger contre toute attaque sur votre réseau. Exemples de supports de stockage amovibles :

- Ruban magnétique
- CD
- DVD
- Clés USB à mémoire flash
- Disques durs externes

Les périphériques de stockage en réseau (NAS pour Network-attached storage) se connectent directement au réseau et permettent aux utilisateurs autorisés d'accéder aux données stockées en passant par le réseau au lieu d'une connexion directe au support. Cependant, les auteurs de menaces peuvent attaquer les périphériques NAS et les rançongiciels peuvent se propager à ces périphériques, ce qui compromettrait les sauvegardes.

Quel que soit le type de périphérique de stockage, vous devez vous assurer de le protéger et de protéger les données qu'il contient. Le périphérique de stockage doit être doté de contrôles de sécurité, tels que :

- Chiffrement
- Analyses de maliciels
- Processus adéquat d'expurgation et d'élimination

Stockage hors site

Le stockage des données essentielles à un emplacement distinct, situé à l'extérieur de vos installations, peut aider à prévenir la perte de données organisationnelles. Si vous avez besoin de plus d'espace de stockage et que vous avez le budget nécessaire, les solutions hors site peuvent être un bon choix.

Si vous prévoyez retenir les services d'un fournisseur pour le stockage hors site, assurez-vous qu'il :

- a pris des mesures de sécurité, comme le chiffrement des données;
- dispose de processus de gestion des incidents;
- dispose d'un plan de reprise après sinistre.

Stockage dans le nuage

Le stockage dans le nuage peut comporter de nombreux avantages. Le fait qu'un fournisseur de services s'occupe de vos sauvegardes libère les ressources de votre organisation. Vous pouvez également profiter de l'expertise du fournisseur de services infonuagiques. De nombreux fournisseurs offrent des caractéristiques de sécurité améliorées que vous n'avez peut-être pas à l'interne.

Notez que votre organisation est en tout temps légalement responsable de la protection de ses données. Vous devez vous assurer que le fournisseur de services choisi peut prendre en charge vos exigences de sécurité et offrir des garanties appropriées.

Vous devriez également envisager la résidence des données, ce qui fait référence à l'emplacement géographique où vos données sont stockées. Il est possible que votre organisation ait des exigences réglementaires et stratégiques qui exigent que les données soient stockées au Canada.

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, [2024]

Canada

No de cat. D97-1/40-002-2024F-PDF ISBN 978-0-660-70857-7

Sauvegarder et récupérer vos données

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Juin 2024 | ITSAP.40.002

Stockage de sauvegardes hors ligne et en ligne

Nous vous recommandons d'avoir une copie de sauvegarde stockée hors ligne. Les sauvegardes en ligne sont stockées sur un serveur ou un ordinateur distant connecté à votre réseau. Contrairement aux sauvegardes en ligne, les sauvegardes hors ligne (ou « sauvegardes à froid ») ne sont pas connectées aux systèmes organisationnels, sauf en cas de nécessité. Ces sauvegardes étant hors ligne, elles ne peuvent pas être la cible de cybermenaces, comme les rançongiciels, qui peuvent compromettre tous les systèmes et appareils connectés au réseau.

Éléments à considérer

Voici quelques éléments que vous devez considérer lorsque vous effectuez la sauvegarde de vos systèmes et données :

- Élaborer des politiques et des procédures qui traitent des sauvegardes, notamment :
  - déterminer la fréquence à laquelle les sauvegardes sont effectuées (quotidiennement, hebdomadairement, mensuellement);
  - élaborer des processus et des politiques qui décrivent comment les sauvegardes sont mises en œuvre et gérées;
  - tester le processus de reprise avec la sauvegarde;
  - décrire l'exécution du processus de reprise, y compris les rôles et les responsabilités.
- Considérer les politiques et exigences organisationnelles concernant la gestion des sauvegardes.
- Déterminer les données essentielles (données requises pour fonctionner avec le strict minimum) et établir les priorités.
- Chiffrer les données sensibles pour les protéger.
- Adopter la règle 3-2-1 pour le stockage des données, soit trois copies des données (une copie originale et deux copies de sauvegarde), sauvegardées sur deux types de supports différents, dont une copie hors site.
- Garder les sauvegardes séparées de l'ordinateur en les stockant sur un appareil externe sur place ou dans une solution de stockage en nuage protégée par un mot de passe fort ou une phrase de passe et une authentification multifactorielle.
- Connaître les mesures de sécurité et les protocoles des fournisseurs de solutions, poser les questions nécessaires et s'assurer qu'ils peuvent répondre aux besoins et exigences.
- Tester les sauvegardes pour vérifier le fonctionnement.

Pour en savoir plus

Appuyez-vous sur les conseils suivants pour approfondir vos connaissances sur les sauvegardes et le stockage :

- Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Nettoyage et élimination d'appareils électroniques (ITSAP.40.006)
- Avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre organisation (ITSE.50.060)
- Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)
- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035)

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, [2024]

No de cat. D97-1/40-002-2024F-PDF ISBN 978-0-660-70857-7

Canada