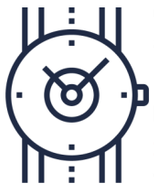
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

SAUVEGARDER ET RÉCUPÉRER VOS DONNÉES

OCTOBRE 2020 | ITSAP.40.002

Avoir une copie de sauvegarde des informations de votre organisation et l'une des nombreuses étapes que vous pouvez adopter pour améliorer la cybersécurité et la résilience de votre entreprise. Si vos réseaux, vos systèmes ou vos informations sont compromis par une menace comme un virus, ou endommagés lors de circonstances comme une catastrophe naturelle, une sauvegarde aidera votre organisation à reprendre ses activités plus rapidement.

POURQUOI AI-JE BESOIN DE SAUVEGARDES?



Certes, on ne souhaite jamais être victime d'une cyberattaque ou d'une catastrophe naturelle, mais ce sont des possibilités auxquelles nous devons nous préparer. Considérez les sauvegardes comme une sorte d'assurance. Si quelque chose arrive à votre organisation, vos sauvegardes sont essentielles pour deux raisons :

1. **Disponibilité :** Protéger la disponibilité des systèmes et des données est un élément essentiel de la cybersécurité. En cas de panne d'électricité, de catastrophe naturelle ou de cyberattaque, les sauvegardes font en sorte que vos employés, partenaires et clients peuvent continuer d'accéder à l'information dont ils ont besoin en temps opportun.
2. **Récupération :** La récupération est le processus qui consiste à restaurer vos systèmes et informations. En cas de panne, de catastrophe naturelle ou de cyberattaque, vous pouvez utiliser vos sauvegardes pour restaurer les systèmes, mettre votre entreprise en marche le plus rapidement possible et minimiser la quantité d'informations, de temps et d'argent qui pourraient être perdus en raison du temps d'arrêt.

QUAND AURAI-JE BESOIN DE MES SAUVEGARDES?

Voici quelques exemples de situation au cours desquelles une copie de sauvegarde des informations de votre organisation pourrait s'avérer extrêmement utile :

PANNE D'ÉLECTRICITÉ

Une panne d'électricité peut provoquer un arrêt du fonctionnement des systèmes et des appareils électroniques, entraînant des temps d'arrêt ou des pannes qui peuvent avoir un impact sur vos processus et activités d'entreprise. Les sauvegardes peuvent garantir que votre organisation ne perd pas d'informations critiques à la suite d'une panne, d'un arrêt soudain des systèmes ou d'une panne d'électricité imprévue.

RANÇONGICIELS

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. En ayant des sauvegardes, vous n'avez pas besoin de payer la rançon (de toute façon, dans certains cas, payer la rançon est inutile, car les données des victimes sont quand même détruites). 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, un auteur de cybermenace inonde une cible (p. ex. un serveur) de trafic pour causer une panne des systèmes et empêcher ainsi l'accès aux sites Web et services internes. Les auteurs de cybermenaces se servent de cette attaque pour interrompre les activités et les services des entreprises ciblées ou pour créer une distraction, par exemple pour voler des données lorsque votre organisation s'efforce de reprendre ses activités. 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 déluges et les tremblements de terre sont des choses qui arrivent. La plupart des entreprises ont des plans d'urgence pour savoir quoi faire 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 avoir des sauvegardes qui se trouvent à un autre emplacement (hors site ou dans le nuage) pourrait se révéler très utile pour la reprise de vos activités.

Il est important de noter que ces événements n'ont pas besoin de survenir directement dans votre organisation pour y 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 commerciales.

TYPES DE SAUVEGARDE

Vos données peuvent être sauvegardées de différentes façons :

- **Sauvegarde complète** : Il vaut mieux faire une sauvegarde complète de façon périodique (chaque semaine ou chaque mois) et avant chaque mise à niveau majeure du système. Une sauvegarde complète est l'option la plus coûteuse et la plus longue, selon la quantité d'informations sauvegardées et vos besoins en matière de stockage.
- **Sauvegarde différentielle :** Une sauvegarde différentielle consiste à faire seulement une copie des données qui ont changé depuis votre 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 incrément est sauvegardé en tant que volume incrémentiel. Toutefois, 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 afin que vous ne stockiez pas de données excédentaires ou redondantes. La déduplication réduit les coûts liés aux sauvegardes et fait en sorte que vous sauvegardez et stockez efficacement vos données.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

OÙ DOIS-JE STOCKER MES SAUVEGARDES?

vous permettent de reprendre vos activités efficacement en cas de cyberattaque. Il existe trois options de stockage des sauvegardes : **sur place** (ou sur le site), **hors site**, ou 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 à vos besoins opérationnels et à vos 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. De plus, vous devriez avoir plus d'une copie de vos sauvegardes et les stocker à deux emplacements différents afin de réduire les risques de pertes de données.

STOCKAGE SUR LA 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. Cela dit, si vous stockez toutes vos sauvegardes sur place, vous courez le risque de subir une perte de données si l'ensemble de vos installations sont touchées, par exemple, par un incendie ou une inondation. Nous vous recommandons de stocker une copie à un autre emplacement pour éviter de perdre vos données.

Voici différents dispositifs de stockage que vous pouvez utiliser :

Les supports de stockage amovibles (p. ex. bandes, CD, DVD, clés USB et disques durs externes) sont pratiques et relativement peu coûteux. Toutefois, ces supports peuvent être endommagés, volés ou perdus.

Les périphériques de stockage en réseau (NAS pour *Network-attached storage*) se connectent directement à votre réseau et permettent aux utilisateurs dont les périphériques ne sont pas connectés directement à un support de stockage amovible d'accéder aux données stockées. Cependant, ce type de périphérique peut faire l'objet d'une attaque par rançongiciel, ce qui mettrait en péril vos sauvegardes.

Quel que soit le type de périphérique de stockage que vous utilisez, vous devez vous assurer de le protéger, ainsi que les données qu'il contient, à l'aide d'autres contrôles de sécurité, comme le chiffrement, la détection de maliciels et une expurgation ou une élimination appropriée.

STOCKAGE HORS SITE

Le stockage des données essentielles à un emplacement distinct, situé à l'extérieur de vos installations peut aider votre organisme à prévenir la perte de données. 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 pour votre organisation.

Si vous envisagez de faire appel à un fournisseur pour le stockage hors site, assurez-vous qu'il dispose de mesures de sécurité, de processus de gestion des incidents et 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 des ressources dans votre organisation. Vous pouvez tirer parti de l'expertise d'un fournisseur de services d'infonuagique; de nombreux fournisseurs de services offrent des fonctionnalités de sécurité accrues 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 que vous sélectionnez peut prendre en charge vos exigences de sécurité avec des garanties appropriées.

Vous devez 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 politiques qui exigent que les données soient stockées au Canada.

SAUVEGARDES EN LIGNE OU HORS 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 (parfois appelées sauvegardes à froid) ne sont pas connectées aux systèmes de votre entreprise et y sont connectées uniquement lorsque cela est nécessaire. Puisque ces sauvegardes sont hors ligne, elles ne peuvent pas être touchées par les cybermenaces, comme les rançongiciels, qui pourraient sinon compromettre tous les systèmes et appareils connectés à votre réseau.

AUTRES ÉLÉMENTS À CONSIDÉRER

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

- Élaborez des politiques et procédures au sujet des sauvegardes (p. ex. fréquence, processus, tests, récupération).
- Tenez compte des politiques et exigences de votre organisme lorsque vous effectuez la gestion de vos sauvegardes.
- Déterminez quelles sont les données essentielles de votre entreprise et priorisez-les. De quoi avez-vous besoin pour fonctionner (le strict minimum)?
- Chiffrez les données sensibles afin de les protéger.
- Stockez vos sauvegardes ailleurs que dans votre ordinateur. Stockez-les dans un dispositif externe sur place ou dans une solution de stockage sur le nuage.
- Conservez plus d'une copie de vos sauvegardes et stockez ces copies à deux emplacements différents (p. ex. une copie dans le nuage et l'autre dans un disque dur externe).
- Connaissez les mesures de sécurité et les protocoles de vos fournisseurs de solutions — posez-leur les questions nécessaires et assurez-vous qu'ils peuvent répondre à vos besoins et exigences.
- **Testez vos sauvegardes** pour vous assurer qu'elles fonctionnent!

RESSOURCES SUPPLÉMENTAIRES

Consultez le site Web du Centre pour la cybersécurité (**cyber.gc.ca**) pour en savoir plus sur la cybersécurité et pour consulter nos publications, notamment :

- *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*

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada