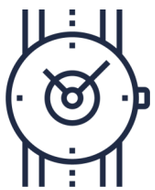
Élaboration d'un plan de reprise informatique personnalisé

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

JANVIER 2021 | ITSAP.40.004

Qu'il s'agisse d'une panne imprévue, d'une cyberattaque ou d'une catastrophe naturelle, tout peut survenir. Si votre organisme n'est pas prêt à faire face à ces éventualités, il pourrait subir une perte de données ou des temps d'arrêt qui perturbent ou même interrompent les fonctions opérationnelles pourtant essentielles. **Quelle que soit la cause d'une interruption imprévue, les répercussions sont coûteuses et peuvent avoir des effets à long terme sur les activités opérationnelles.** Pour assurer la continuité des activités après un temps d'arrêt minimal, il est indispensable que votre organisme intègre un plan de reprise informatique dans sa stratégie globale de continuité des activités. Dans ce plan, il est nécessaire de déterminer les processus, les applications et les données qui sont essentiels et d'indiquer la façon dont votre organisme pourra assurer la reprise des services TI qui appuient les opérations, les produits et les services.



L'intervention visant la reprise des activités doit être fondée sur de nombreux éléments et doit permettre d'indiquer clairement ce qui doit être récupéré, l'intervenant qui devra le faire, le moment et l'endroit de l'intervention dans un plan de reprise détaillé où tout doit être consigné. Dans la majorité des cas, ce sont deux types de plans que l'on doit envisager d'élaborer : le plan de reprise après sinistre et le plan d'intervention en cas d'incident. Ces deux plans tiennent compte de deux événements majeurs qui pourraient provoquer une panne imprévue et obliger un organisme à activer son plan d'intervention.

1. **Plan de reprise après sinistre :** ce plan vise principalement à assurer la continuité des activités en cas de panne ou d'interruption de service imprévue.
2. **Plan d'intervention en cas d'incident :** ce plan vise principalement à protéger les informations sensibles en cas d'infraction à la sécurité.

DÉTERMINEZ LA TOLÉRANCE DE VOTRE ORGANISME FACE AUX POSSIBLES PERTURBATIONS OPÉRATIONNELLES

Pour qu'un plan de reprise soit efficace, vous devez l'adapter en fonction des répercussions d'un incident ou d'une catastrophe sur votre organisme et en fonction du niveau de perturbation que votre organisme peut tolérer. Il existe trois principales mesures à intégrer dans votre plan : **le temps d'arrêt maximal tolérable, l'objectif du point de récupération et l'objectif du temps de récupération.**

Temps d'arrêt maximal tolérable : durée totale pendant laquelle un processus peut être interrompu sans causer de préjudice important à votre organisme.

Objectif de point de rétablissement : mesure de la perte de données que votre organisme peut tolérer.

Objectif de délai de rétablissement : temps prévu et niveau de service nécessaires pour répondre aux attentes minimales du propriétaire du système.

DÉTERMINEZ LES DONNÉES, LES APPLICATIONS ET LES FONCTIONS OPÉRATIONNELLES ESSENTIELLES

Pour élaborer un plan efficace, vous devez déterminer les données, les applications et les fonctions organisationnelles qui sont essentielles. Parmi les informations essentielles, il peut y avoir des dossiers financiers, des actifs exclusifs et des données personnelles. Quant aux applications essentielles, ce sont les systèmes qui exécutent les principales fonctions organisationnelles et qui sont indispensables aux opérations. Ce sont les systèmes qui doivent être rétablis immédiatement en cas de panne imprévue, afin d'assurer la continuité des activités. Pour déterminer les fonctions, les applications et les données organisationnelles qui sont essentielles, vous devez procéder à une évaluation des risques afin de cerner les menaces et les vulnérabilités. Examinez certains scénarios précis (par exemple, une cyberattaque, une panne de courant importante ou une catastrophe naturelle) pour vous aider à identifier les principaux intervenants et les parties prenantes, à gérer les risques importants, à élaborer des stratégies d'atténuation et à déterminer le temps et les efforts nécessaires à la reprise des activités.

Menez une analyse des répercussions pour prévoir la façon dont une perturbation ou un incident pourrait nuire à vos finances, à vos opérations de même qu'à vos processus et systèmes opérationnels. Dans cette analyse, vous devriez également évaluer les données que vous recueillez et les applications que vous utilisez afin de déterminer leur criticité et d'établir les priorités qui permettront un rétablissement immédiat.

CRÉEZ VOTRE PLAN DE REPRISE

1. Indiquez tous les intervenants, notamment les clients, les fournisseurs, les propriétaires fonctionnels, les gestionnaires et les propriétaires de systèmes.
2. Indiquez les membres de votre équipe d'intervention, ainsi que leurs rôles et responsabilités.
3. Faites l'inventaire de tous vos biens matériels et logiciels.
4. Déterminez les fonctions, les applications et les données opérationnelles qui sont essentielles et établissez leur ordre de priorité.
5. Fixez des objectifs de reprise clairs.
6. Définissez des stratégies de reprise et de secours.
7. Mettez votre plan à l'essai.
8. Élaborez un plan de communications pour informer les principaux intervenants.
9. Élaborez un programme de formation à l'intention des employés afin de vous assurer qu'ils comprennent leurs rôles, leurs responsabilités et le déroulement des opérations pendant une interruption non prévue.
10. Envisagez la possibilité de discuter avec vos fournisseurs de services gérés pour déterminer en quoi ils peuvent appuyer vos efforts de reprise (facultatif).

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

CHOISISSEZ VOTRE STRATÉGIE DE REPRISE.

Plusieurs options peuvent être considérées dans la mise en œuvre de votre stratégie de reprise, mais vous devez opter pour une stratégie de reprise qui répond à vos besoins opérationnels et à vos exigences de sécurité.

SITES CHAUDS, TIÈDES OU FROIDS

Site chaud : site de secours doté des mêmes serveurs et équipements que le site principal. Ce site fonctionne en permanence et de façon identique au site principal pour pallier une panne. La synchronisation des données s'effectue en quelques minutes ou en quelques heures, ce qui réduit le risque de perte de données.

Site tiède : site de secours doté d'une connectivité réseau. Certains équipements y sont installés. Il est nécessaire de procéder à des installations pour faire fonctionner ce site au même niveau que le site principal. La synchronisation des données est moins fréquente, ce qui peut entraîner une certaine perte de données.

Site froid : site de secours doté de peu d'équipements, voire aucun. Ce site nécessite plus de temps et de ressources pour l'installer et rétablir les activités opérationnelles. La synchronisation des données peut s'avérer être un processus long et difficile, car les serveurs doivent être transférés depuis le site principal, ce qui augmente le risque de perte de données.

ÉCRITURE MIROIR

L'écriture miroir permet de transférer les données sur deux disques durs ou plus. L'écriture miroir transfère automatiquement les données essentielles sur un réseau ou un serveur de rechange lorsque le système principal subit une interruption imprévue. Si vous ne parvenez pas à rétablir vos systèmes, vous pouvez utiliser la copie miroir. Il est important que la copie miroir soit sauvegardée sur un serveur séparé ou dans un emplacement qui n'est pas touché par l'interruption.

METTEZ VOTRE PLAN À L'ESSAI

La mise à l'essai est essentielle, car elle vous permettra de cerner les incohérences et d'améliorer les lacunes. Assurez-vous toutefois d'utiliser un environnement de test pour éviter d'interrompre vos activités opérationnelles. Voici quelques exemples de stratégies de mise à l'essai :

liste de contrôle : lisez et expliquez les étapes du plan de reprise;

explications détaillées : passez en revue les étapes du plan sans les mettre en œuvre;

simulation : appuyez-vous sur une catastrophe ou un incident simulé pour permettre à l'équipe chargée de la reprise de se familiariser avec ses rôles et responsabilités;

exploitation en parallèle : configurez les systèmes de reprise et mettez-les à l'essai pour déterminer s'ils peuvent effectuer des opérations et soutenir les principaux processus tout en maintenant les principaux systèmes en mode de production intégrale;

test de migration : configurez vos systèmes de reprise pour qu'ils prennent en charge toutes vos activités opérationnelles et déconnectez les systèmes primaires. Ce type de test provoque des interruptions opérationnelles et nécessite donc une planification préalable supplémentaire.

RÉPLICATION DU STOCKAGE

La réplication du stockage permet de copier les données en temps réel d'un endroit à un autre au moyen d'un réseau de stockage (SAN), d'un réseau local (LAN) ou d'un réseau étendu (WAN). Comme elle est réalisée en temps réel, on parle de **réplication synchrone**. Vous pouvez également utiliser la **réplication asynchrone**, qui crée des copies de données en fonction d'un calendrier défini.

REPRISE : SOLUTION EN NUAGE OU SUR PLACE

Grâce à une plateforme de récupération dans le nuage, vous pouvez vous connecter facilement, de n'importe où, au moyen d'une variété de dispositifs. Vous pouvez y sauvegarder vos données fréquemment, et cette option est moins coûteuse que l'achat et la maintenance d'une plateforme sur place, car vous payez uniquement l'espace dont vous avez besoin. L'utilisation du nuage peut également permettre de réduire, et même d'éliminer, le besoin d'avoir un site de reprise distinct.

APPRENEZ-EN DAVANTAGE!

Visitez le site web du Centre canadien pour la cybersécurité (**cyber.gc.ca**) pour en savoir davantage sur les sujets liés à la cybersécurité et trouver toute notre collection de publications, dont les suivantes :

- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Êtes-vous victime de piratage? (ITSAP.00.005)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Conseils de cybersécurité pour le télétravail (ITSAP.10.116)
- Sécurité de la chaîne d'approvisionnement pour les petites et moyennes entreprises (ITSAP.00.70)
- 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)
- Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)