

« Les dix aspects les plus souvent oubliés dans la mise en place d'un plan de reprise d'activité »

Les responsables informatiques sont conscients de l'importance de disposer d'un plan efficace de reprise d'activité. Les entreprises qui ne possèdent pas de plan approprié risquent de faire faillite rapidement après un sinistre majeur. La situation est encore plus grave lorsqu'il s'agit de PME, car la plupart de ces entreprises se fient à des plans de sauvegarde et de restauration archaïques qui ne leur permettent pas de survivre aux sinistres ou à la fréquence des incidents quotidiens qui pèsent sur leur informatique.

Les entreprises souhaitant se prémunir en cas de sinistre connaissent déjà certainement les principes de base d'un plan solide. Il est néanmoins possible d'éviter un grand nombre d'obstacles et de pièges. Après avoir collaboré avec des milliers de clients, nous avons pu établir la liste des dix oublis les plus couramment constatés. Examinez-la et vérifiez que vous n'avez pas oublié une étape cruciale qui pourrait faire toute la différence entre survie ou faillite !

Il y a de fortes chances que votre entreprise ne connaisse jamais de sinistre majeur. Mais si vous disposez d'un plan de reprise d'activité efficace et d'une documentation satisfaisante, si vous effectuez les tests appropriés et si votre personnel est bien formé, vous augmentez vos chances de survie en cas de catastrophe mineure ou majeure.

Vous souhaitez en savoir plus sur l'effet positif que peut avoir la virtualisation VMware sur la survie de votre entreprise ?

Découvrez-en davantage sur le site www.vmware.com/smb.

1. Non-identification des éléments susceptibles de nuire à l'infrastructure et aux données vitales pour votre entreprise.

Outre les menaces habituelles (virus, chevaux de Troie, vers, etc.), vous devez identifier les phénomènes propres à votre région. Vivez-vous dans une zone sujette aux tremblements de terre ou aux inondations ? Votre région connaît-elle fréquemment des interruptions de courant dues aux tempêtes ou de longues coupures d'électricité ? Examinez bien ces éventualités avant de créer votre plan ou de choisir le lieu d'implantation de votre infrastructure de reprise.

2. Création d'un plan avec un personnel qualifié trop restreint.

Il arrive parfois qu'une entreprise crée un plan de reprise d'activité qui dépend d'un seul informaticien muni d'un pager. Que se passe-t-il si cette personne n'est pas disponible ? Vous devez constituer une équipe et la doter de compétences transversales pour que ses membres puissent répondre aux urgences. Il est préférable de répartir cette équipe sur plusieurs lieux pour le cas où une catastrophe naturelle toucherait tous les employés d'un site.

3. Recours à des processus manuels pour avertir le personnel lors d'un sinistre.

Si votre site est victime d'une coupure de courant et que personne n'est présent pour le signaler, le personnel chargé de la reprise d'activité va-t-il être informé ? Vous devez créer un système automatisé pour avertir votre personnel informatique en cas de sinistre ou d'interruption du service. Vous pouvez également passer un accord avec un prestataire de services qui sera chargé de surveiller votre site et d'informer un groupe établi de personnes, capables d'exécuter votre plan de reprise d'activité.

4. Absence d'alimentation de secours.

Si votre site est touché par une catastrophe naturelle de grande envergure, vous risquez de vous retrouver sans électricité pendant une longue période. Faites l'acquisition d'un dispositif d'alimentation sans coupure très puissant et à longue durée de vie. Dotez-vous ensuite de batteries de secours supplémentaires pour garantir une alimentation continue.

5. Non-hiérarchisation des ressources à restaurer en priorité.

Quelles sont les applications informatiques auxquelles vous devez accéder en premier ? Est-ce que vous pouvez attendre un jour ou deux pour certaines d'entre elles sans nuire à vos activités ? Vous devez déterminer l'ordre dans lequel vous remettrez en ligne les applications et les services après un sinistre. Vous pouvez, par exemple, décider de réactiver le système de messagerie de l'entreprise avant de restaurer les serveurs de fichiers des divers départements. Afin d'éviter les « moi d'abord ! », usez de toute votre diplomatie et veillez à ce que cette décision ait obtenu l'adhésion de tous.

6. Manque de documentation appropriée pour votre plan de reprise d'activité.

Après avoir créé un plan de reprise, préparez des instructions détaillées sur son mode d'exécution. Veillez à ce que chaque processus soit bien documenté. Décrivez l'emplacement de toutes les ressources système nécessaires à la récupération. N'oubliez pas de ranger la documentation dans plusieurs endroits et vérifiez que le personnel concerné puisse y accéder facilement.

7. Utilisation de sauvegardes.

Si vos données sont obsolètes, stockées dans un emplacement touché par le sinistre ou corrompues, le meilleur plan de reprise d'activité sera vain. Effectuez des sauvegardes à intervalles fixes et réguliers pour préserver l'intégrité des informations. Vous pouvez également faire appel à une technologie telle que la virtualisation VMware pour implanter un site distant avec machines virtuelles répliquées afin d'accélérer la récupération.

8. Plan de reprise d'activité non testé.

Vous devez vous assurer que votre plan de reprise fonctionne correctement en cas d'urgence ! Même si cela semble évident, de nombreuses entreprises oublient de tester leur plan. Simulez régulièrement des alertes sur les données pour tester tous les scénarios possibles, qu'il s'agisse d'une simple coupure de courant ou d'un événement catastrophique susceptible de provoquer des dégâts pendant des mois. Là aussi, grâce à la virtualisation VMware et la possibilité de provisionner n'importe quel serveur avec les machines virtuelles nécessaires, votre plan de reprise d'activité sera parfaitement testé en quelques minutes.

9. Sécurisation des mots de passe.

Même si la protection par mot de passe est un facteur clé pour la sécurité des données, vous devez stocker vos mots de passe système dans au moins deux emplacements distincts et sûrs. Veillez à ce que plusieurs personnes du département informatique aient accès à la totalité des mots de passe et des codes. Et n'oubliez pas de changer immédiatement ces mots de passe dès qu'un membre du personnel concerné quitte la société.

10. Plan de reprise non actualisé.

Effectuez des mises à jour fréquentes de votre plan de reprise d'activité. Une fois votre plan créé, réexaminez-le au moins tous les trimestres. Dressez la liste de tous les motifs qui doivent entraîner la modification du plan (changement de personnel, de matériel, d'emplacement ou d'application, entre autres). Non seulement votre personnel informatique pourra actualiser ses compétences, mais c'est aussi l'occasion d'améliorer les procédures si vous détectez des failles dans votre plan ou de rationaliser vos procédures.