Livre Blanc*

CONTINUITE D'ACTIVITE
4 Points de Vigilance pour les Dirigeants

BCDR Business Continuity and Disaster Recovery
ou **Plan de Continuité d'Activité / Plan de Reprise d'Activité informatique**

* Source Datto Corporate

En tant que DIRIGEANT proactif, vous savez que la mise en œuvre d'une continuité et récupération/reprise d'activité informatique solide est essentielle pour votre entreprise.

Après tout, compte tenu de votre position, pourquoi risquer une perte de données , pourquoi mettre en danger votre entreprise quand la prévention est si facile?

Bien que certains DIRIGEANTS n'accordent pas l'attention que mérite le PCA/PRA, vous n'êtes peut-être pas forcement concernés.

Mais si quelqu'un vous le demande, voici quatre raisons, recommandations essentielles pour lesquelles il faut se soucier de la continuité d'activité et reprise après sinistre.

1. Vigilance parce que les TEMPS D'ARRÊT sont coûteux

Si vos employés ou clients perdent l'accès à des applications et à des données critiques, il y aura un impact direct sur votre productivité et vos revenus. Bien que cela semble évident, de nombreuses entreprises ne prennent pas en compte les coûts réels de temps d'arrêt. Pour mieux comprendre ce coût, considérons l'exemple suivant en utilisant le Calculateur RTO de Datto. Considérons que votre entreprise compte 100 employés, en moyenne le revenu horaire est de 1 500 euros et le jeu de données de sauvegarde de 2 To. Compte tenu de ces paramètres, une restauration complète à partir d'une sauvegarde locale prendrait plus de 8 heures. Les coûts d'indisponibilité associés se traduiraient par une perte de revenus de 34 000 €. Certains produits modernes de BCDR offrent la possibilité d'exécuter des applications à partir d'une sauvegarde opérationnelle sur serveur virtuel. Cela permet aux utilisateurs de continuer leurs activités pendant que les serveurs d'applications principaux sont restaurés. Choisir une solution de BCDR visant à réduire les temps d'arrêt peut être économiquement pertinente.

2. Vigilance parce que la SAUVEGARDE seule ne suffit pas

Vous auriez du mal à trouver aujourd'hui une entreprise qui ne fait pas ses sauvegardes de données. Mais que se passera-t-il si une inondation détruit votre serveur de sauvegarde primaire ? L'envoi d'une copie des données hors site est également être considéré comme essentiel pour la récupération après sinistre. Historiquement, on envoyait des cartouches dans lieu secondaire. Comme mentionné précédemment, avec le BCDR d'aujourd'hui les produits peuvent exécuter les applications à partir d'instances de sauvegarde sur serveurs virtuels, et certains peuvent étendre cette possibilité dans le cloud. Cette approche est fréquemment appelé Cloud DR ou Disaster Recovery As a Service (DRaaS). **Pouvoir accéder aux applications dans le Cloud tandis que l'infrastructure sur site est restaurée est vraiment un avantage en cas de reprise après sinistre.** En tant que Dirigeant, vous ne voulez pas de la technologie de sauvegarde d'hier. La sauvegarde et le PCA/PRA ne sont pas la même chose, votre entreprise a besoin des deux.

3. Vigilance parce que les CATASTROPHES peuvent prendre plusieurs formes

Nous n'avons pas connaissance de toutes les catastrophes via les médias. **La plupart des temps d'arrêts informatiques sont le résultat d'actions quotidiennes courantes comme une suppression accidentelle (ou intentionnelle) de données, des pannes de matériels ou des comportements inappropriés liés à la sécurité.** Par exemple, une enquête récente d'OWI Labs a révélé que 81% des répondants se connectent occasionnellement ou régulièrement au réseau wifi public, malgré les risques de sécurité. Une attaque de ransomware ou un virus peut interrompre votre activité aussi facilement qu'une tempête ou une surtension. Ces petites catastrophes sont généralement le résultat d'erreurs humaines inévitables. Avoir la bonne technologie qui permet à votre entreprise de poursuivre son activité après ces catastrophes causées par l'homme est tout aussi important, sinon plus, que de se protéger contre une catastrophe naturelle. Cela peut, ou pas, frapper votre entreprise.

4. Vigilance parce que TOUT LE MONDE EST CONCERNE

Assurer l'accès aux applications et aux données après un sinistre n'est qu'une pièce du puzzle BCDR. **Évaluer la capacité de votre entreprise à restaurer l'informatique peut être un bon point de départ pour en mesurer sa capacité à poursuivre son activité. Mais une bonne planification d'un BCDR doit porter sur l'ensemble de l'entreprise et le but final devrait être de développer sa résilience.** En fait, la planification pour la mise en œuvre du BCDR doit commencer par effectuer une analyse d'impact ou une évaluation des risques - Ces études peuvent révéler des faiblesses dans la capacité de votre entreprise à poursuivre ses activités qui vont bien au-delà de l'informatique. Vous savez qu'une catastrophe (naturelle ou autre) peut arriver à tout moment et dans l'entreprise que vous dirigez, tout le monde va trouver son intérêt dans le BCDR.

Conclusion

La continuité d'activité et la reprise après un sinistre relèvent de la responsabilité de l'entreprise et ne pas protéger votre entreprise contre les erreurs humaines, les pannes matérielles et/ou les catastrophes naturelles peuvent être préjudiciables et avoir un impact sur chaque partie prenante.
Une fois que vous avez mis en place un plan BCDR solide, vous dormirez beaucoup plus sereinement la nuit sachant que vous êtes parfaitement préparé à toute catastrophe qui pourrait survenir dans votre quotidien.

Pour plus d'information:

Quietic
Nous gérons, vous grandissez.

HUB CREATIC, 6 rue Rose Dieng Nantes, 44300
www.quietic.fr
Téléphone:02 85 52 88 00
Email: contact@quietic.fr

Contactez-nous pour bénéficier de
l'AUDIT GRATUIT
de votre système d'information.