Article

12 questions auxquelles tout dirigeant devrait pouvoir répondre pour prouver que ses données sont réellement récupérables

Les ransomwares, les menaces internes et les défaillances opérationnelles ne sont plus des événements rares. Ce sont des menaces constantes. Pourtant, la plupart des organisations sont encore incapables d'affirmer avec certitude qu'elles pourront récupérer leurs données au moment où cela compte le plus.

Ce décalage s'explique par une raison simple : les sauvegardes et les snapshots sont les données d'entrée, la capacité de récupération est la donnée de sortie.

Une protection continue des données, des sauvegardes périodiques, des snapshots et des contrôles de sécurité sont nécessaires. Cependant, ces derniers ne garantissent pas que les systèmes reviendront en ligne rapidement, sans problème et dans le bon ordre, sous une pression réelle. Nombre d'organisations ne découvrent leurs lacunes que lorsqu'elles tentent de se rétablir pendant un incident réel. Et à ce moment-là, il est trop tard pour y remédier.

La capacité de récupération permet de véritablement mesurer la résilience. Les dirigeants peuvent et doivent la tester dans des conditions réelles avant qu'une attaque, une interruption ou une erreur humaine ne révèle le problème au grand jour.

Cette liste de contrôle concise destinée aux dirigeants ne s'intéresse ni aux outils, ni à l'architecture. Elle est conçue pour révéler les lacunes le plus tôt possible, quand vous avez encore la possibilité d'y remédier. Si vous pouvez répondre clairement à ces douze questions, vous êtes sur la bonne voie pour mettre en place une stratégie axée sur la reprise alignée avec les menaces modernes et les réalités hybrides.

Que signifie réellement « récupérable » ?

Il semble utile de clarifier ce point avant de passer aux questions.

« Récupérable » signifie que vous pouvez restaurer :

— **À un point précis dans le temps** qui répond aux attentes de l'entreprise (RPO)

— **Assez rapidement pour assurer la continuité de l'activité** (RTO), non seulement pour les données, mais aussi pour les services prioritaires

— **Dans un environnement évitant tout réinfection immédiate**, grâce à un isolement et à une validation appropriés

Si l'un de ces éléments venait à faillir, la résilience deviendrait une revendication plutôt qu'un contrôle.

Comment utiliser cette liste de contrôle

Vous n'avez pas besoin de formuler des réponses parfaites dès le premier jour. L'objectif est de déceler les lacunes au plus tôt, tant que vous avez encore le choix.

Utilisez ces questions pour effectuer une auto-évaluation rapide :

— **Vert :** documenté, testé et mesuré

— **Jaune :** partiellement implémenté ou non testé

— **Rouge :** supposé, inconnu ou « je pense que oui »

Portez une attention particulière aux réponses rouges. Elles révèlent de potentielles lacunes en matière de délais et de risques de récupération.

Fréquence de protection (le b.a.-ba de la capacité de récupération)

Avoir confiance en sa capacité de récupération exige de comprendre le niveau de perte de données que votre entreprise peut réellement tolérer, et de vérifier que la fréquence de votre protection est adaptée à cette réalité.

1. **Quel RPO exigeons-nous pour les services de niveau 0 et de niveau 1, et pouvons-nous réellement l'atteindre, pas seulement en théorie ?**
   De nombreuses équipes peuvent réciter un RPO. Rares sont celles qui ont validé la capacité de leur modèle de protection actuel à l'atteindre sous pression.

2. **Nos points de reprise sont-ils suffisamment précis pour permettre une restauration jusqu'à quelques secondes avant l'impact sur les données, ou nous contentons-nous de la dernière sauvegarde planifiée ?**
   Lorsque des attaques ou des corruptions se produisent au fil du temps, les points de reprise approximatifs peuvent se traduire directement par une perte de données inacceptable.

3. **La fréquence de nos points de récupération est-elle cohérente sur les différentes plateformes sur site, cloud et SaaS ? Et comment les différences de fréquence affectent-elles notre stratégie de récupération ?**
   Dans les environnements hybrides, l'incohérence est un angle mort fréquent. Des lacunes en matière de protection apparaissent souvent là où les politiques divergent.

Signaux d'alarme :

« Nous ne connaissons pas notre RPO au niveau 0. »

« Nous avons une seule politique de sauvegarde standard pour tout. »

« Les charges de travail cloud sont traitées différemment, et de manière incohérente. »

Immuabilité et isolement (non négociables à l'ère des ransomwares)

L'immuabilité contribue à empêcher la suppression et le chiffrement des copies de récupération, mais elle ne suffit pas à elle seule. L'isolement et la discipline opérationnelle déterminent si les copies immuables peuvent survivre à une véritable attaque. La plupart des environnements ont besoin des deux.

4. **Conservons-nous au moins une copie de récupération immuable et isolée de l'identité et des réseaux de production ?**
   Si des attaquants peuvent accéder à vos données de récupération en utilisant les chemins qu'ils ont pris pour accéder à l'environnement de production, l'immuabilité seule sera insuffisante.

5. **L'immuabilité est-elle appliquée dès la conception, ou une identité d'administrateur compromise peut-elle modifier les protections associées à la conservation ou à la suppression ?**
   Dans de nombreux cas, ce sont les identifiants, et non les programmes malveillants, qui sont à l'origine du problème. Les mécanismes de récupération doivent tenir compte de cette réalité.

6. **Si les attaquants ciblent d'abord les données de récupération, qu'est-ce qui les empêche de découvrir, de chiffrer ou de saboter nos chemins de récupération ?**
   Cette question met souvent en lumière des hypothèses sur la « sécurité par l'obscurité » qui ne résistent pas aux tactiques de menace modernes.

Un état d'esprit utile

Si votre plan de récupération part du principe que les attaquants ne comprendront pas votre environnement, il est déjà obsolète.

Discipline de test (la récupération n'est réelle que si elle est testée)

Les plans de récupération non testés n'échouent pas discrètement. Ils échouent aux moments les plus stressants qu'une organisation puisse traverser.

7. **Quand avons-nous effectué pour la dernière fois un test de restauration d'applications de niveau 0 à une échelle réaliste, et avons-nous mesuré le délai de restauration ?**
   Les tests partiels et de petite envergure ne reflètent pas la complexité des scénarios de reprise réels.

8. **Vérifions-nous systématiquement l'intégrité des sauvegardes et des ressources de restauration avant d'en avoir besoin ?**
   Découvrir des sauvegardes corrompues lors d'un incident transforme un problème technique en crise commerciale.

9. **Peut-on effectuer une restauration dans un environnement isolé à des fins de validation forensique avant de reconnecter le système à la production ?**
   Restaurer rapidement est important. Restaurer proprement est essentiel.

La dure vérité

Une récupération sans entraînement, c'est de l'improvisation.

Contrôles d'identité et hiérarchisation de la restauration (la vitesse en dépend)

La vitesse de récupération ne dépend pas uniquement du stockage ou de l'infrastructure. Elle est souvent limitée par les systèmes d'identité, les contrôles d'accès et des priorités floues.

10. **Les contrôles de protection et de récupération des données sont-ils protégés par la MFA, le principe du moindre privilège et la séparation des rôles ? Et ces contrôles sont-ils résilients même en cas de compromission d'Active Directory ou de l'IAM ?**
    Lorsque les systèmes d'identité tombent, l'autorité de la récupération suit souvent le mouvement.

11. **Avons-nous un ordre de restauration documenté pour les services de niveau 0, et a-t-il été testé ?**
    Par défaut, l'identité, le réseau, le DNS, les plateformes principales et les données ne sont pas remis en ligne simultanément. L'ordre a son importance.

12. **À quelle vitesse pouvons-nous restaurer les applications stratégiques à partir d'une copie immuable ? Et quelles dépendances ralentissent le délai de mise en service, et pas seulement le délai d'accès aux données ?**
    Pour les dirigeants, les interruptions représentent une perte de capacité, et non une perte de fichiers. Les plans de récupération doivent tenir compte de cette réalité.

De la liste de contrôle aux mesures concrètes

Cette évaluation ne consiste pas à vous attribuer une note. L'idée est de concentrer les efforts là où ils réduisent rapidement les risques.

Prochaine étape :

— Identifiez les **trois principales réponses rouges** et désignez clairement des responsables.

— Établissez un **calendrier de tests de restauration** et publiez des résultats, pas des promesses.

— Concevez un plan de récupération pour **les situations hostiles**, en supposant que les attaquants comprennent votre environnement.

Prouver sa capacité de récupération ne nécessite pas d'acheter de nouveaux outils ou de cocher telle ou telle case. Cela exige un entraînement à la restauration des éléments essentiels, vers un point optimal connu, dans le respect des délais de service cibles mesurés.

Pour en savoir plus

HPE.com/data

Visiter HPE.com

Live Chat

a00155955FRE

HEWLETT PACKARD ENTERPRISE

hpe.com