eBOOK

Cyber Récupération 101

Votre guide pour construire une entreprise résiliente et axée sur le cloud

Commvault®

CONTENTS

© 2024 Commvault

Aperçu

Il est rare qu'une semaine passe sans que les gros titres ne parlent d'une nouvelle violation de données affectant les clients d'une autre entreprise.

Tandis que les consommateurs surveillent leurs comptes pour évaluer les dommages personnels, l'organisation s'efforce de minimiser l'impact sur les opérations commerciales, les données des clients, des employés et de l'entreprise, la réputation de la marque et le résultat financier. Chaque aspect d'une entreprise est en danger face à une cyberattaque, rendant la cyber-résilience non seulement un luxe, mais une nécessité. Les organisations doivent être préparées à résister et à se remettre des menaces cybernétiques pour assurer la continuité des activités. Ce guide présente des stratégies efficaces pour atteindre cette cyber-résilience, de la définition de la cyber-récupération à l'aide à la construction d'un plan de récupération efficace.

© 2024 Commvault

Cyber Récupération

vs.

La cyber récupération se concentre sur les actions et stratégies spécifiques nécessaires pour se remettre des incidents liés à la cybersécurité, tels que les violations de données, les attaques de logiciels malveillants et les ransomwares. Elle implique la restauration des données, des systèmes et des opérations affectés par les menaces cybernétiques.

Reprise après Sinistre

La reprise après sinistre, en revanche, est un concept plus large qui englobe tous les types de catastrophes, y compris les catastrophes naturelles, les pannes matérielles et les erreurs humaines. Elle vise à rétablir les opérations normales après tout type d'événement perturbateur.

Votre entreprise doit être prête à réagir et à répondre à toutes les menaces qui se présentent. Bien qu'elles soient souvent discutées ensemble, la cyber récupération et la reprise après sinistre ne sont pas identiques. Comprendre les différences est crucial pour élaborer une stratégie de récupération efficace. Bien que les deux soient essentielles, la cyber récupération est un sous-ensemble spécialisé de la reprise après sinistre, conçu pour répondre aux défis uniques posés par les menaces cybernétiques. Vous pouvez en apprendre davantage à ce sujet dans notre ebook "Au-delà de la Reprise après Sinistre : Pourquoi Vous Avez Besoin d'une Stratégie Différente Lorsque les Cyberattaques Frappent" et notre infographie "Reprise après Sinistre ≠ Cyber Récupération".

© 2024 Commvault

Élaboration d'un Plan de Cyber Récupération Efficace

Un plan de cyber récupération complet est essentiel pour toute organisation visant à être cyber-résiliente. Voici ce qu'un tel plan implique et ce qu'il ne doit pas inclure, ainsi qu'un modèle d'exemple détaillé. En élaborant votre plan de cyber récupération, il est important d'évaluer les besoins de votre organisation. **Cela signifie que vous devez :**

✕ CE QU'UN PLAN DE CYBER RÉCUPÉRATION NE DOIT PAS INCLURE

Aussi complet que votre plan de cyber récupération doit être, il est important de noter qu'il y a des domaines qui ne doivent pas en faire partie. Cela inclut les tâches routinières de votre département informatique et la maintenance générale, les processus liés aux opérations quotidiennes de votre entreprise, et les procédures de reprise après sinistre pour les catastrophes naturelles et les pannes matérielles.

Identifier les actifs critiques :

Liste tous les systèmes, données et applications critiques ainsi que les membres de l'équipe qui nécessitent une protection.

Effectuer une évaluation des risques :

Évaluez les risques et vulnérabilités potentiels associés à ces actifs. Assurez-vous que votre plan inclut des moyens de traiter les vulnérabilités et de réduire les risques.

Identifier les équipes et membres clés :

Définissez les rôles et responsabilités pour toutes les équipes qui géreront la réponse et la récupération au sein de votre organisation.

Établir des procédures de récupération :

Créez des étapes détaillées pour la récupération des données, des systèmes et des opérations.

Créer un plan de communication :

Décrivez comment communiquer avec les parties prenantes, les employés, les clients, les fournisseurs et les médias pendant et après un incident.

Effectuer des tests et des formations :

Testez régulièrement votre plan et formez le personnel sur leurs rôles. Fournissez une formation régulière en cybersécurité aux employés sur des sujets comme le phishing, et encouragez-les à signaler immédiatement tout incident suspect.

© 2024 Commvault

Modèle de Plan de Cyber Récupération

Utilisez ce modèle pour créer votre propre plan de cyber récupération – ou pour vérifier que votre plan inclut toutes les étapes nécessaires pour atténuer les effets d'une cyberattaque.

Identifier les actifs critiques :

- **Systèmes :** CRM, ERP, Serveur de messagerie
- **Données :** Informations clients, Données des employés, Enregistrements financiers, Propriété intellectuelle
- **Applications :** Logiciel de vente, Logiciel de comptabilité, Système de gestion des ressources humaines, Applications orientées client

Effectuer une évaluation des risques

- **Risques :** Violations de données, attaques de ransomware, attaques DDoS
- **Vulnérabilités :** Logiciels obsolètes, mots de passe faibles, manque de formation des employés
- **Actions :** Mettre à jour les logiciels, imposer des mots de passe plus robustes, établir une cadence régulière de formation

Identifier les équipes clés

- **Équipes :** Équipe de réponse et de récupération en cas de violation, Équipe réglementaire et juridique, Équipe de préparation des affaires
- **Rôles :** Responsable des incidents, Responsable technique, Responsable de la communication, Conseiller juridique
- **Responsabilités :** Coordonner la réponse, restaurer les systèmes, communiquer avec les parties prenantes, assurer la conformité

Établir des procédures de récupération

- **Étape 1 :** Isoler les systèmes affectés pour éviter toute propagation supplémentaire.
- **Étape 2 :** Identifier la source et le type d'attaque.
- **Étape 3 :** Restaurer les données à partir des sauvegardes.
- **Étape 4 :** Réinstaller et mettre à jour les logiciels.
- **Étape 5 :** Tester les systèmes restaurés pour vérifier leur fonctionnalité

Créer un plan de communication

- **Communication interne :** Informer les employés de l'incident et de l'avancement de la récupération.
- **Communication externe :** Informer les clients, les partenaires et les organismes de réglementation si nécessaire.

Effectuer des tests et des formations

- **Tests :** Effectuer des exercices et des simulations réguliers pour tester le plan de récupération. Réaliser des restaurations complètes des données dans des environnements temporaires pour valider le processus et l'intégrité des données.
- **Formation :** Fournir une formation continue pour les équipes de réponse aux incidents et tous les employés.

En suivant ce guide, votre organisation peut créer un plan de cyber récupération solide qui améliore considérablement votre cyber-résilience, vous préparant ainsi à faire face à tout incident cyber.

En savoir plus sur la manière dont Commvault peut vous aider ici.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®

© 2024 Commvault. See here for information about our trademarks and patents. 10_24