Prévention des ransomwares

LISTE DE CONTRÔLE

Les entreprises qui contrent le mieux les attaques par ransomware privilégient **cinq mesures essentielles de préparation aux ransomwares :**

1 | Protéger les données et les systèmes de sauvegarde

- ☐ Mettre en place des sauvegardes régulières, alignées sur les exigences de l'entreprise et sur les règles de conformité, et automatisées en tant que stratégies de protection.
- ☐ Sauvegarder en permanence les charges de travail, même après la défaillance d'un composant matériel ou logiciel.
- ☐ Appliquer régulièrement des correctifs aux logiciels et analyser les systèmes existants pour réduire les vulnérabilités.
- ☐ Donner de la visibilité sur les lacunes de sécurité dans les configurations des systèmes et les conceptions opérationnelles.
- ☐ Concilier une sécurité renforcée avec des RTO/RPO plus rapides qui respectent les SLA de l'entreprise numérique.
- ☐ Investir dans une solution robuste de sécurité et de gestion des données réputée pour protéger les données sauvegardées contre les attaques par ransomware.

CAPACITÉS CLÉS :

Snapshots inaltérables

WORM

Chiffrement des données

Audit et analyse de la configuration

Tolérance aux pannes

Isolation des données moderne et flexible

2 | Réduire les risques d'accès non autorisés

- ☐ Sensibiliser les employés aux dangers des attaques par hameçonnage et des identifiants compromis.
- ☐ Appliquer les principes du Zero Trust, notamment le principe du moindre privilège et le MFA, dans la solution de sécurité et de gestion des données.
- ☐ Mettre en place un système d'approbation multi-utilisateurs pour les opérations et les modifications critiques.
- ☐ Comprendre les capacités de sauvegarde (existantes et nouvelles) qui empêchent les accès non autorisés aux données de l'entreprise, et donc qui protègent contre les ransomwares et les menaces internes.

CAPACITÉS CLÉS :

Authentification multifacteur (MFA)

Modification surveillée

Contrôle d'accès basé sur les rôles (RBAC) granulaire

3 | Voir et détecter les attaques pour stopper les intrusions

- ☐ Classifier les données et identifier les informations sensibles susceptibles d'être menacées.
- ☐ Fournir une visibilité approfondie des données et des applications pour identifier les vulnérabilités logicielles et les cyber-vulnérabilités.
- ☐ Intégrer l'IA/le ML pour détecter les anomalies susceptibles d'indiquer une menace ou une attaque par ransomware.
- ☐ Détecter les indicateurs de compromission (IOC) en analysant régulièrement les menaces sur les données de sauvegarde.

CAPACITÉS CLÉS :

Alimenté par l'IA/le ML

Détection d'anomalies en temps quasi réel

Alertes automatisées

Découverte des cyber-vulnérabilités

COHESITY

4 | Renforcer sa posture de sécurité grâce une plateforme extensible

CAPACITÉS CLÉS :

- ☐ S'assurer qu'une solution de sauvegarde ou de gestion des données prend en charge les intégrations de sécurité, en particulier vers les solutions SOC, pour détecter les ransomwares et y remédier plus rapidement.
- ☐ Améliorer la collaboration en supprimant les silos entre les personnes, les processus et la plateforme de données.
- ☐ Comprendre les API des produits et plateformes de sécurité de premier plan.
- ☐ Établir des flux de travail transparents dans les sauvegardes pour extraire des informations tout en préservant la sécurité des données.

Intégrations préconçues

Intégrations personnalisables

Interopérabilité des applications à valeur ajoutée

5 | Garantir une récupération rapide des données à grande échelle

CAPACITÉS CLÉS :

- ☐ Déterminer si une solution de sauvegarde ou de gestion des données existante peut récupérer les données rapidement, proprement et de manière prévisible à grande échelle.
- ☐ Tenir compte des exigences de protection des données et de souveraineté propres à chaque pays.
- ☐ Évaluer les capacités à récupérer rapidement à n'importe quel point dans le temps et à n'importe quel emplacement.
- ☐ Comprendre l'état de santé d'un snapshot et récupérer les données non structurées sans investissement supplémentaire.
- ☐ Identifier comment récupérer sur place des données non structurées afin de réduire les temps d'arrêt.

Récupération instantanée à grande échelle

Récupération propre

Récupération sur place

Téléchargez le guide complet de préparation aux ransomwares

COHESITY

© 2023 Cohesity Inc. Tous droits réservés.

Cohesity, le logo Cohesity, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, le logo Helios, DataGovern, SiteContinuity et les autres marques Cohesity sont des marques commerciales ou déposées de Cohesity, Inc. aux États-Unis et/ou dans d'autres pays. Les noms d'autres sociétés et produits peuvent être des marques commerciales des sociétés respectives auxquelles elles sont associées. Ce document (a) est destiné à vous fournir des informations sur Cohesity, son activité et ses produits ; (b) est réputé exact et à jour au moment de sa rédaction, mais est susceptible de modification sans préavis ; et (c) est fourni « TEL QUEL ». Cohesity rejette toutes les conditions, représentations et garanties expresses ou implicites de quelque nature que ce soit.

Cohesity.com/fr | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110, États-Unis

9100074-002-FR 7-2023