Commvault

eBOOK

Guide de préparation à la cyber récupération

DÉCOUVREZ COMMENT VOTRE ENTREPRISE PEUT ÊTRE PRÊTE À RELEVER LES DÉFIS QUI SE PRÉSENTENT À ELLE.

TABLE DES MATIÈRES

Les équipes de sécurité, d'informatique et d'exploitation de nombreuses organisations considèrent que la cyber-récupération et la récupération après sinistre sont identiques. Toutefois, la cyber-récupération à la suite d'incidents récents a révélé quelques difficultés particulières par rapport à la récupération après sinistre classique. La variabilité des tactiques, des techniques et des procédures des attaquants a montré que les plans de cyber-récupération doivent être pris en compte :

- **Imprévisibilité et évolution des menaces :** Contrairement à une catastrophe naturelle, les cyberattaques sont malveillantes et les attaquants se sont donné beaucoup de mal pour tenter de dissimuler leurs actions et leur geste. Pour cette raison, il peut être difficile de déterminer exactement quand l'attaque a commencé, quels sont les systèmes touchés ou l'étendue des dégâts.
- **Attaques secondaires :** On a vu des attaquants planter du code pour lancer des attaques secondaires pendant le processus de récupération ou créer des portes dérobées persistantes qui s'ouvrent automatiquement lors d'une action de restauration.
- **Sauvegardes compromises :** Dans certains cas, les attaquants ont ciblé les sauvegardes spécifiquement pour s'assurer que les efforts de récupération soient inefficaces. La nécessité de payer une rançon pour récupérer les données de production devient alors plus réelle.
- **Contraintes de temps :** Les entreprises sont souvent confrontées à une pression énorme pour se remettre rapidement en ligne après une cyberattaque. Il a été démontré que les temps d'arrêt coûtent à une entreprise jusqu'à 12 millions de dollars par jour[1]. Et pour ne rien arranger, une récupération précipitée peut conduire à restaurer des systèmes déjà compromis, ce qui amplifie encore les dégâts.
- **La perte des ressources :** La cyber-récupération peut être un processus à forte intensité de ressources, nécessitant l'expertise d'équipes informatiques, de sécurité, juridiques, voire d'application de la loi. Cela peut mettre à rude épreuve les ressources déjà éprouvées d'une entreprise et détourner les équipes chargées de la sécurité et des opérations d'autres cybermenaces éventuelles.

En comprenant ces défis, les organisations peuvent utiliser certains éléments fondamentaux de la récupération après sinistre pour élaborer un plan de cyber-récupération qui anticipe ces difficultés et les aide à rebondir plus efficacement après une attaque.

Ce guide vous aidera à préparer votre organisation à la cyber-récupération en vous donnant les concepts, les idées et les processus nécessaires pour établir votre propre programme, tout en vous alignant sur certains cadres communément observés.

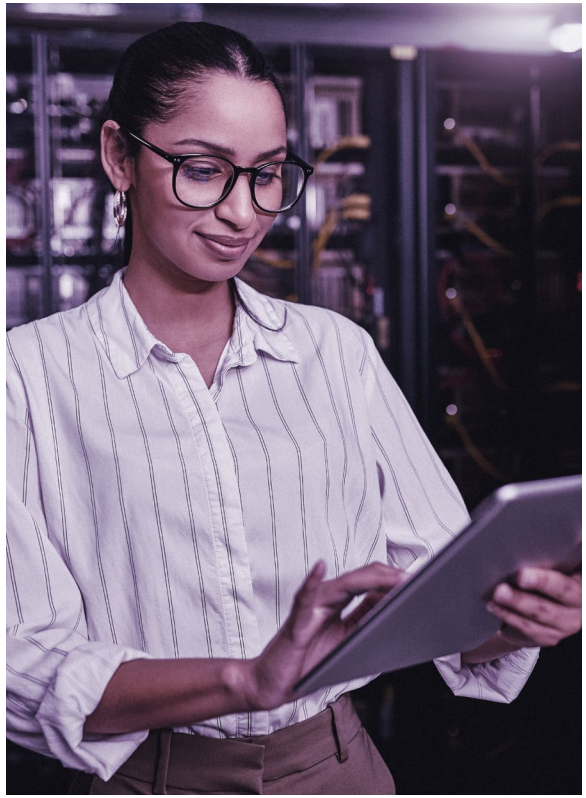
[1] SolarWinds : Pingdom Team, Average Cost of Downtime per Industry, 9 janvier 2023.

LE CADRE DE CYBERSÉCURITÉ DU NIST COMME GUIDE

Le cadre de cybersécurité du National Institute of Standards and Technology (NIST CSF) sert depuis longtemps de guide aux équipes de sécurité pour élaborer et aligner leurs programmes de sécurité et se défendre contre les nouvelles cybermenaces qui ne cessent d'évoluer.

Utiliser le cadre Identifier, Détecter, Protéger, Répondre et Récupérer pour expliquer comment s'appuyer sur chacun de ces éléments pour une cyber-récupération réussie.

1. **Identifier.** Comprenez vos données, y compris les données sensibles / critiques, où elles se trouvent et qui en est responsable.
2. **Détecter.** Utilisez les contrôles de sécurité et la technologie pour observer ce qui se passe dans votre environnement et vos données.
3. **Protéger.** Mettez en place des mécanismes pour verrouiller vos données sensibles ou critiques et préparez-les à la récupération.
4. **Répondre.** Éliminez l'attaquant de votre environnement et supprimez ou protégez le vecteur d'attaque utilisé pour infiltrer votre organisation. Si cela ne peut être fait rapidement, préparez un nouvel espace de travail, intact et non compromis, à restaurer et à utiliser pour poursuivre les opérations.
5. **Récupérer.** Reconstruisez une version non compromise de l'ensemble de votre environnement, y compris les données, les applications et l'infrastructure.



SE PRÉPARER À L'INATTENDU

De par leur nature même, les cyberincidents sont souvent des attaques secrètes orchestrées en coulisses pendant des jours ou des semaines avant que les destructions ou les ravages ne se produisent. Des études ont montré que la durée moyenne de séjour, c'est-à-dire le temps pendant lequel un attaquant est resté à l'intérieur d'une organisation lors d'une attaque, est de 204 jours, soit près de 7 mois.[1]

204 jours, soit près de 7 mois

la durée moyenne de séjour, c'est-à-dire le temps pendant lequel un attaquant est resté à l'intérieur d'une organisation lors d'une attaque

Les organisations effectuent depuis longtemps des tests de pénétration pour mettre en évidence les points faibles de leurs défenses et des exercices de simulation pour tester la récupération après sinistre. Mais avec la variabilité des cyberattaques, la pratique doit tenir compte du fait que presque rien ne peut être implicitement fiable dans un véritable scénario de cyber-récupération. Les sauvegardes doivent être analysées pour détecter les logiciels malveillants persistants. L'infrastructure doit être nettoyée pour confirmer que seuls les utilisateurs autorisés sont présents. Les applications et les données doivent quant à elles être vérifiées pour détecter les portes dérobées et être restaurées dans un état antérieur à l'attaque (ou à l'infiltration).

[1] 2023 IBM Ponemon Cost of a Data Breach Report, p14 Cost of a Data Breach Report 2023.pdf

LE COÛT DE LA REDONDANCE PEUT ÊTRE PROHIBITIF

Disposer de sites sombres supplémentaires pour assurer la redondance est une méthode précieuse pour protéger vos données, car elle vous permet de vous entraîner et de vous préparer aux cyberattaques. Mais, bien entendu, le fait de disposer d'un ensemble d'infrastructures supplémentaires représente un coût énorme.

Chaque site physique nécessite des dépenses importantes telles que la planification, l'immobilier, la construction, l'équipement, l'énergie, les taxes, le personnel et l'entretien courant. Ces coûts s'additionnent rapidement et peuvent atteindre des dizaines ou des centaines de millions de dollars par an, selon l'ampleur de l'entreprise, ce qui les rend hors budget – et hors de question – pour de nombreuses organisations.

RÉCUPÉRATION EN SALLE BLANCHE À LA DEMANDE

Avec l'arrivée de Commvault® Cloud Cleanroom™ Recovery, les entreprises peuvent éviter le coût et la complexité de la gestion des salles blanches sur site. La première et unique salle blanche pour la cyber-récupération vous permet de tester et de récupérer rapidement dans un environnement sûr, basé sur le cloud.

Cleanroom Recovery est une solution pratique et abordable, qui rend les tests et la récupération plus accessibles à un plus grand nombre d'entreprises. Il s'agit d'une solution qui est également facile à mettre en place à la demande et à tester selon les besoins, ce qui est pratique lorsque vous souhaitez apporter des modifications ou tester différents scénarios.

Vous pouvez facilement récupérer les applications et les données, et effectuer des analyses judiciaires après un événement. Vous disposerez d'un environnement de récupération isolé pour assurer la continuité des activités en cas d'attaque. Cleanroom Recovery comprend par ailleurs une intégration avec Microsoft Defender qui automatise l'analyse des menaces afin de confirmer que les données sont propres.

COMMENT LA RÉCUPÉRATION EN SALLE BLANCHE FOURNIT UN ENVIRONNEMENT CLOUD EXEMPT DE LOGICIELS MALVEILLANTS

Air-gapping (isolation physique)
Copies de données isolées, séparées des environnements sources.

Conception immuable
Sauvegardes avec contrôles d'accès Zero Trust à plusieurs niveaux.

Automatisation intégrée
Tirez parti de l'automatisation et de l'orchestration pour une mise en œuvre facile et des opérations simples.

Protection résiliente contre les ransomwares et sécurité de bout en bout
Détection d'anomalies intégrée, rapports et cryptage des données au repos et actives.

Validation de la récupération de l'application
Récupérabilité des données grâce à une validation orchestrée de la récupération des applications.

Analyse judiciaire sécurisée
Effectuer des analyses sécurisées avec du matériel exempt de logiciels malveillants dans des environnements en nuage isolés.

Une certitude en matière de cybersécurité : les acteurs malveillants continueront à innover pour trouver des failles. La meilleure façon de protéger votre entreprise contre les cyberattaques est de disposer d'un plan de récupération d'activité bien conçu et de le tester régulièrement. **Cleanroom Recovery offre un espace sûr et isolé pour tester votre plan et une récupération rapide en cas de problème.**

En savoir plus : **www.commvault.com/platform/cleanroom-recovery**

commvault.com | +33 1 73 13 00 23 | talktous@commvault.com

Commvault®