eBOOK

Guide de préparation à la cyber récupération

APPRENEZ COMMENT RESTER RÉSILIENT FACE AUX DÉFIS

Commvault®

TABLE DES MATIÈRES

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 $14,056 par minute. 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.

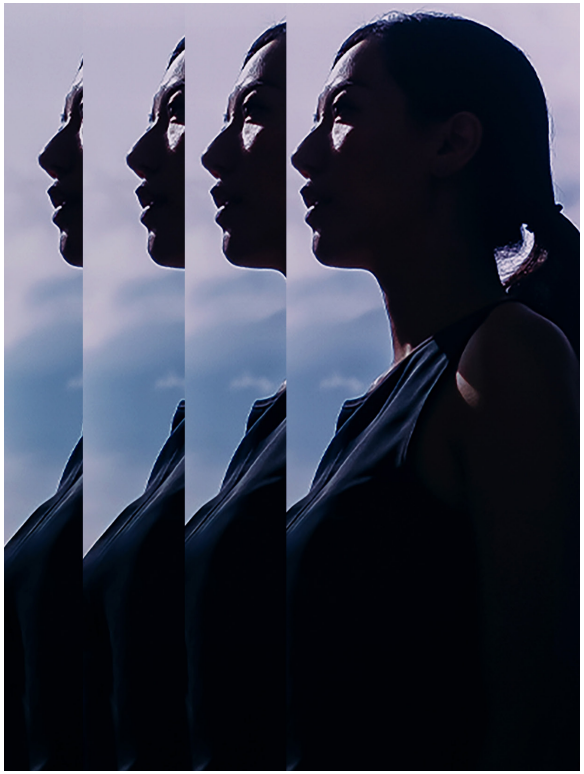
[1] Enterprise Management Associates, "IT outages: 2024 costs and containment," Valerie O'Connell, Research Director, April 2024.

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 cyberrécupération 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

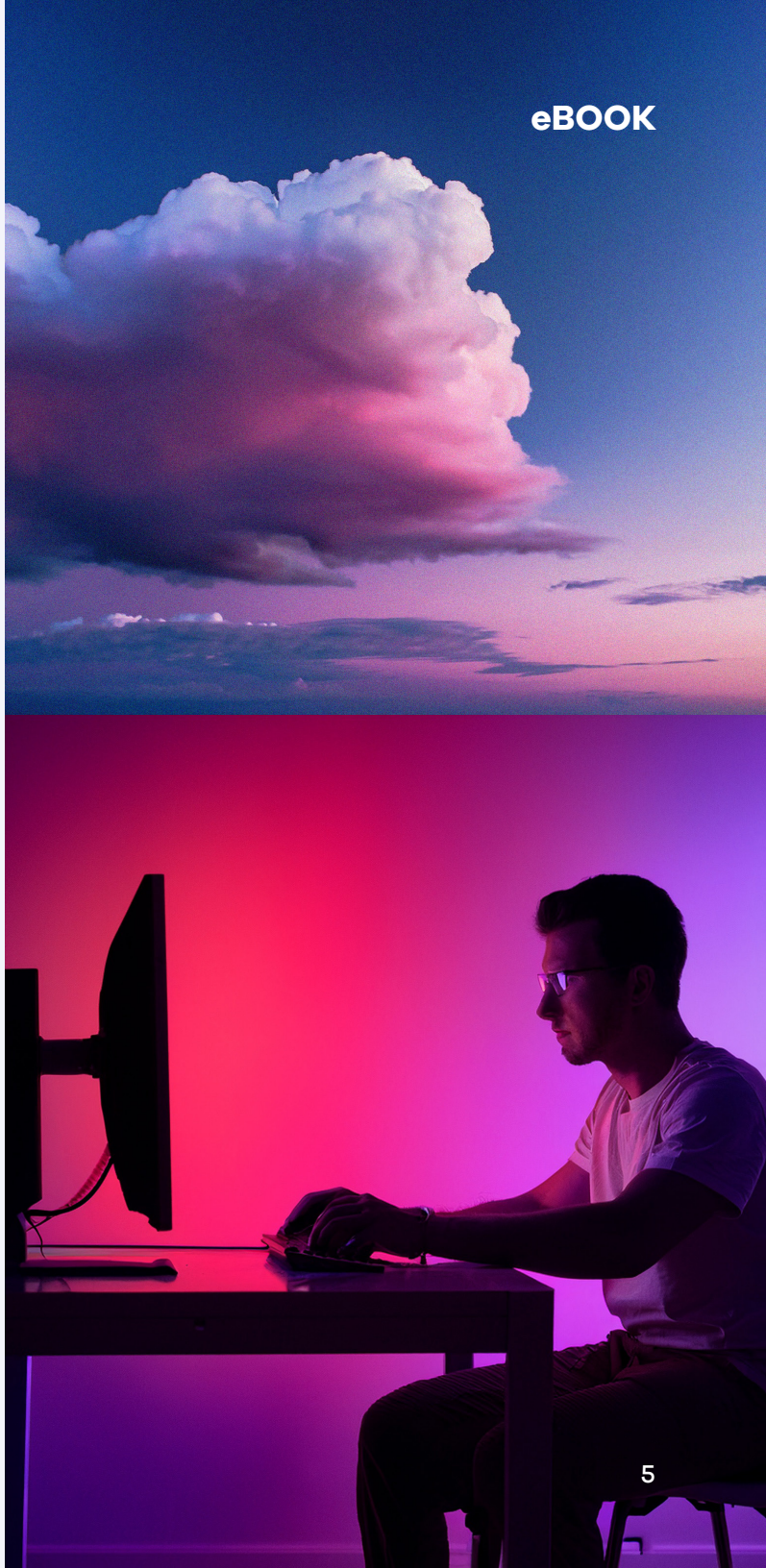
De par leur nature même, les cyberincidents sont souvent des attaques secrètes orchestrées en coulisses pendant des jours ou des semaines avant que les destructions ou les ravages ne se produisent.

194 jours, soit plus de six mois

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[1]

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] Cost of a Data Breach Report 2024, IBM.

VIABILITÉ MINIMUM : LA PREMIÈRE ÉTAPE DE LA RÉCUPÉRATION CYBER

Une fois que votre entreprise a été touchée par une cyberattaque, vous subissez une immense pression pour revenir à la normale le plus rapidement possible. La meilleure façon de reprendre les opérations rapidement ? Restaurer à la viabilité minimum les actifs les plus critiques dont vous avez besoin pour maintenir une activité continue. Ainsi, vous pouvez continuer à gérer les aspects les plus vitaux de votre organisation pendant que la restauration complète est en cours.

Une fois que vous avez identifié vos systèmes, actifs les plus critiques dont vous avez besoin pour maintenir une activité continu, vous devrez élaborer un plan pour les restaurer en cas d'incident. Vous devez comprendre l'impact des temps d'arrêt et vous devez tester et mettre à jour votre plan selon les besoins.

Lisez le Guide Ultime de la Viabilité Minimum pour en savoir plus sur les étapes pour restaurer vos opérations et nos pratiques recommandées.

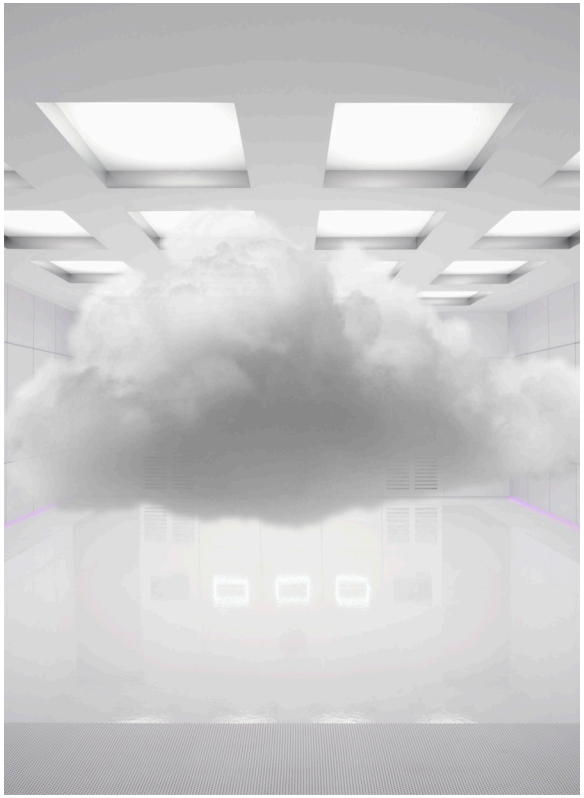
LA RÉCUPÉRATION CYBER LA PLUS RAPIDE ET LA PLUS COMPLÈTE

Commvault fournit des solutions pour protéger, tester et récupérer vos données, applications et charges de travail – offrant une récupération complète et une véritable résilience cyber.

Commvault® Cloud Cleanroom™ Recovery vous permet de tester et de récupérer dans un environnement cloud sûr, à la demande,[SG1] basé sur le cloud. Vous pouvez facilement récupérer des applications et des données, et mener des enquêtes après un événement. Vous disposerez d'un environnement de récupération isolé pour la continuité des activités en cas d'attaque.

Commvault Cloud Rewind permet une récupération quasi-instantanée et écrit automatiquement du code pour récupérer des données et reconstruire des applications, vous permettant de reprendre vos activités quelques minutes après une panne – tout cela sans intervention manuelle.

Commvault Cloud for Active Directory Enterprise Edition offre une récupération rapide pour les environnements AD et Entra ID. Il aide à automatiser et orchestrer la récupération des AD de niveau forêt après un incident, vous permettant de revenir rapidement à la viabilité minimum.



eBOOK

Une certitude en matière de cybersécurité : les acteurs malveillants continueront d'innover pour trouver des vulnérabilités. Gardez un temps d'avance avec un plan et une stratégie de récupération cyber bien pensés pour protéger vos actifs et maintenir une activité continue face aux menaces.

En savoir plus : **www.commvault.com/fr/minimum-viability**

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

Commvault®