Innovations

LEARNING SERIES

FOUNDATION EDITION

Partage d'expérience: récupérer après une attaque de ransomware

Dans ce guide

- La montée des ransomware, en variété et en quantité
- Savez-vous quelles sont vos vulnérabilités face au ransomware ?
- Comment garantir que votre entreprise survivra à une attaque de ransomware

ActualTech Media | rubrik

Partage d’expérience : récupérer après une attaque de ransomware

SOMMAIRE

ActualTech Media

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

www.actualtechmedia.com

Remerciements de l'éditeur

DIRECTEUR ÉDITORIAL
Keith Ward

DIRECTRICE DIFFUSION DE CONTENU
Wendy Hernandez

DIRECTRICE ARTISTIQUE
Olivia Thomson

DIRECTRICE PRINCIPALE CONTENU
Katie Mohr

PARTENAIRES ET VP CONTENU
James Green

AVEC LA CONTRIBUTION SPÉCIALE DE RUBRIK
Arushi Jain, Responsable principal Marketing produits

Damani Norman, Responsable de la gestion des produits techniques

James Knott, Senior Engagement Manager

Jonathan Hemming, Directeur technique, Réussite des clients

Introduction : la montée des attaques de ransomware

Alors que de plus en plus d'entreprises adoptent des stratégies basées sur les données pour accroître leur agilité, les données deviennent une cible toujours plus lucrative pour les cybercriminels. Malgré la mise en place de mécanismes de défense robustes, les attaques de ransomware ne cessent d'augmenter et parviennent à chiffrer les données de nombreuses organisations. Au premier semestre 2020, environ 2,5 millions de nouvelles attaques de ransomware ont été perpétrées, selon le *Rapport de McAfee Labs sur le paysage des menaces* de novembre 2020. Par ailleurs, SafetyDetectives a constaté que 54 % des moyennes et grandes entreprises aux États-Unis et 57 % au Royaume-Uni ont été touchées par des attaques de ransomware au cours de l'année dernière (voir **Figure 1**). Le nombre d'attaques de ransomware ciblant des établissements de soins de santé et de recherche médicale a également explosé, les cybercriminels cherchant à tirer profit de la pandémie de COVID-19. Des écoles et universités qui tentaient de fournir à leurs étudiants des moyens d'apprentissage en ligne ont aussi été ciblées.

LES BASES

Une statistique stupéfiante

Selon la Newsletter sur la cybersécurité du Bureau des droits civils (OCR) du département de la Santé et des Services sociaux des États-Unis publiée à l'automne 2019, le FBI estime que les cybercriminels encaisseront plus d'un milliard de dollars en rançons.

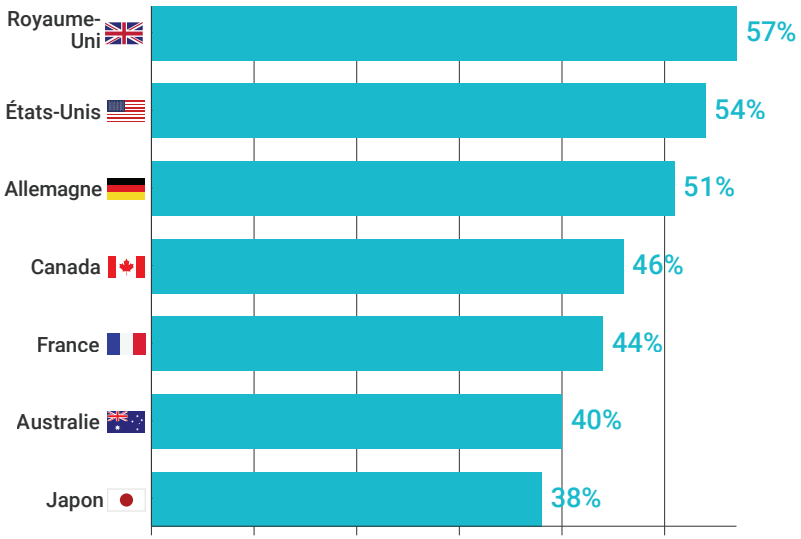

Figure 1 : pourcentage d'organisations ayant signalé des attaques de ransomware au cours de l'année dernière par pays (source : SafetyDetectives)

La division US-CERT (United States Computer Emergency Readiness Team) de la CISA (Cybersecurity and Infrastructure Security Agency) des États-Unis définit le ransomware comme suit :

Un type de logiciel malveillant, ou malware, conçu pour bloquer l'accès à un système informatique ou à des données jusqu'au paiement d'une rançon. Un ransomware s'introduit généralement par le biais d'e-mails d'hameçonnage ou lorsqu'un utilisateur consulte sans le savoir un site Web infecté.

Les types d'attaques de ransomware

L'idée derrière les attaques de ransomware est plutôt simple : bloquer l'accès d'utilisateurs autorisés à des données stratégiques, le plus souvent en chiffrant leurs fichiers, puis demander le paiement d'une rançon (typiquement en cryptomonnaie, comme le Bitcoin). Auparavant, les demandes de rançon initiales étaient relativement faibles (de l'ordre de dizaines de milliers de dollars), mais augmentaient rapidement si la victime tardait à payer, afin de pousser les victimes à payer la rançon. Toutefois, en raison du succès croissant de ces attaques, les rançons exigées atteignent aujourd'hui des centaines de milliers, voire plusieurs millions de dollars.

ANALYSE DÉTAILLÉE

Le ransomware revêt de multiples formes

Le ransomware se présente sous de multiples formes et par le biais de nombreux vecteurs d'attaque, notamment :

- **Ransomware à chiffrement :** chiffrement des fichiers personnels, des dossiers et des stockages réseau partagés. Les fichiers ciblés sont supprimés après avoir été chiffrés, et les utilisateurs trouvent généralement un fichier texte avec des instructions de paiement d'une rançon dans le dossier où étaient les fichiers devenus inaccessibles.
- **Ransomware ciblant les serveurs de stockage en réseau (NAS) :** chiffre et/ou supprime les fichiers sur un système NAS, y compris

les répertoires personnels, les sauvegardes d'hyperviseurs de machines virtuelles (MV), les volumes fictifs et les fichiers de sauvegarde.

- **Ransomware bloqueur d'écran :** verrouille l'écran d'ordinateur de l'utilisateur et exige un paiement, mais ne chiffre aucun fichier personnel. La récupération après une attaque de ransomware bloqueur d'écran est relativement simple et implique le redémarrage en mode sans échec et la suppression du verrouillage d'écran à l'aide d'outils de récupération anti-malware.
- **Bloqueur de matériel :** modifie l'enregistrement d'amorçage maître (MBR) de l'ordinateur de sorte à interrompre le processus d'amorçage normal, empêchant le système d'exploitation de démarrer correctement. La récupération nécessite soit de corriger le MBR, soit de restaurer les données sur un nouveau système.
- **Chiffrement des applications/serveurs Web :** chiffre des fichiers et serveurs Web par le biais des vulnérabilités des applications. Sur les serveurs Web, les fichiers index.php ou index.html sont remplacés par des instructions de rançon. La récupération nécessite de trouver les fichiers infectés et de les restaurer à leur état précédent.
- **Ransomware as a Service (RaaS) :** largement disponible sur le Dark Web, le RaaS permet à quasiment n'importe qui d'attaquer une organisation avec un ransomware qui gère tous les aspects de l'attaque, y compris la diffusion, l'infection, le chiffrement, la collecte du paiement et le déchiffrement, le tout contre un droit de licence ou une commission de faible montant.
- **Exfiltration de données :** lit des données stratégiques sur les systèmes attaqués et les copie vers l'attaquant. Ce type d'attaque de ransomware est souvent combiné avec d'autres attaques qui verrouillent les données stratégiques.

Des ransomwares sophistiqués ciblent désormais les sauvegardes, les modifient ou les effacent complètement, compromettant ainsi la dernière ligne de défense et optimisant les chances de paiement d'une rançon.

Bonnes pratiques de récupération après ransomware

Même si le FBI et d'autres agences de cybersécurité déconseillent fortement aux victimes de payer une rançon pour récupérer leurs données, plus du quart d'entre elles le font, selon les rapports récents de CrowdStrike et Sophos. Cependant, il n'existe aucune garantie de récupérer son argent, et d'après Sophos, les victimes qui payent une rançon doublent en fait le coût du traitement d'une attaque de ransomware, qui passe d'environ 730 000 $ à 1,4 millions de dollars.

Les bonnes pratiques suivantes vous aideront à vous préparer, à identifier et à corriger avec succès une attaque de ransomware visant votre organisation (voir **Figure 2**).

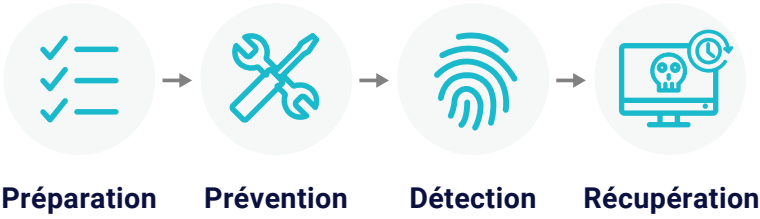

Figure 2 : la défense contre le ransomware comprend les bonnes pratiques en matière de préparation, de détection et de réponse et récupération

PRÉPARATION

Prendre le temps de se préparer à une attaque de ransomware est la clé d'une récupération réussie en cas d'attaque. Voici quelques bonnes pratiques :

- **Élaborer un plan :** commencez par développer une réponse au ransomware et un plan de reprise, ainsi qu'un manuel d'assistance. Le plan et le manuel doivent être revus et mis à jour périodiquement, et stockés d'une manière sécurisée qui les protège de toute attaque de ransomware (copie papier par exemple).
- **Identifier les parties prenantes et les membres de l'équipe d'intervention :** vous devez identifier les parties prenantes clés des équipes de direction, informatique, systèmes/applications et autres, et préciser qui sera responsable de l'exécution et de la gestion de la réponse aux incidents et du plan de reprise. Assurez-vous que chacun comprenne ses responsabilités individuelles et sache comment exécuter les activités qui lui sont affectées dans le plan de reprise.
- **Créer un plan de communication :** une communication interne rapide, précise et complète au sein de l'entreprise affectée est essentielle. Identifiez les méthodes de communication qui seront disponibles lors d'une attaque de ransomware. Les systèmes de messagerie et de téléphonie de l'entreprise pourraient être impactés et indisponibles. Fournissez des moyens de communication alternatifs à la fois en interne et avec les fournisseurs externes, les services de police, les clients et le public en général.
- **Prioriser les systèmes en fonction de leur importance pour l'entreprise :** identifiez le degré d'importance de chaque

système et des données associées pour l'entreprise. Le fait de savoir quels systèmes de l'entreprise requièrent votre attention en priorité et comment ils interagissent avec les autres systèmes de l'entreprise facilitera une récupération fluide et organisée. Sur la base du niveau d'importance de chaque système, documentez un plan de reprise qui identifie quels systèmes doivent être récupérés et dans quel ordre.

- **Stocker les sauvegardes dans un emplacement sécurisé :** déterminez où les copies de sauvegarde seront stockées, à la fois localement et/ou hors site. Les copies locales doivent être stockées sur une plateforme de stockage immuable (non modifiable). Ceci garantit que vos données de sauvegarde ne pourront pas être chiffrées ou modifiées en cas d'attaque de ransomware de sorte que vous pourrez récupérer rapidement (voir **Figure 3**). Des copies distantes de vos données seront requises si votre plan prévoit la récupération dans un site alternatif. Vous devez prêter une attention particulière à la façon dont les données sont stockées hors site. Les données stockées dans des archives hors site sont vulnérables aux attaques de ransomware car les plateformes de stockage sur lesquelles les sauvegardes sont conservées peuvent ne

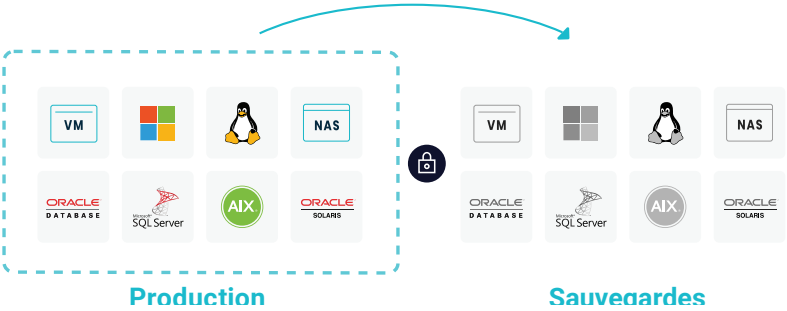

Figure 3 : les plateformes immuables empêchent les attaques de ransomware d'accéder à ou de chiffrer les systèmes de sauvegarde et les données en ligne

pas être immuables. Par ailleurs, la restauration depuis des sauvegardes hors site peut s'avérer complexe et extrêmement chronophage. Les archives dans le cloud peuvent également faire l'objet d'un accès externe si elles ne sont pas sécurisées correctement. Si le recours à des emplacements d'archivage est prévu pour la reprise après une attaque de ransomware, vous devez prendre les mesures nécessaires pour sécuriser ces emplacements.

- **Tester régulièrement les plans de reprise :** testez régulièrement la récupération des données afin d'être prêts à affronter un incident réel. Sans ces tests, vous ne pourrez avoir aucune certitude que le plan de reprise fonctionnera en cas d'attaque. Par ailleurs, les tests apportent aux équipes d'intervention et de récupération l'expérience nécessaire et la confiance en leur capacité à corriger rapidement et avec succès une attaque. Les tests doivent être aussi réalistes que possible, sans perturber les activités de l'entreprise, et doivent être conduits à la fois à intervalles planifiés et non planifiés. L'un des objectifs des tests est d'être préparé à l'imprévu.

Même si le FBI et d'autres agences de cybersécurité déconseillent fortement aux victimes de payer une rançon pour récupérer leurs données, plus du quart d'entre elles le font, selon les rapports récents de CrowdStrike et Sophos.

PRÉVENTION

Les bonnes pratiques de prévention des attaques de ransomware comprennent la formation en vue de sensibiliser les utilisateurs finaux afin de les aider à reconnaître les liens et les pièces jointes malveillants dans les e-mails, ainsi que les sites Web malveillants qui diffusent des ransomwares. Les courriers indésirables et d'hameçonnage, les mots de passe trop simples et les sites Web malveillants sont les méthodes les plus courantes d'infection par ransomware (voir **Figure 4**). La formation doit être interactive et engageante, similaire à la formation anti-hameçonnage que de nombreuses entreprises dispensent aujourd'hui. Les autres mesures de prévention consistent notamment à mettre à jour vos systèmes d'exploitation et applications en appliquant les correctifs, à activer les options de filtrage des liens et des pièces jointes dans les e-mails (par ex. Liens fiables et Pièces jointes fiables dans Office 365) et à vous assurer qu'un logiciel anti-malware est installé et à jour sur tous les terminaux.

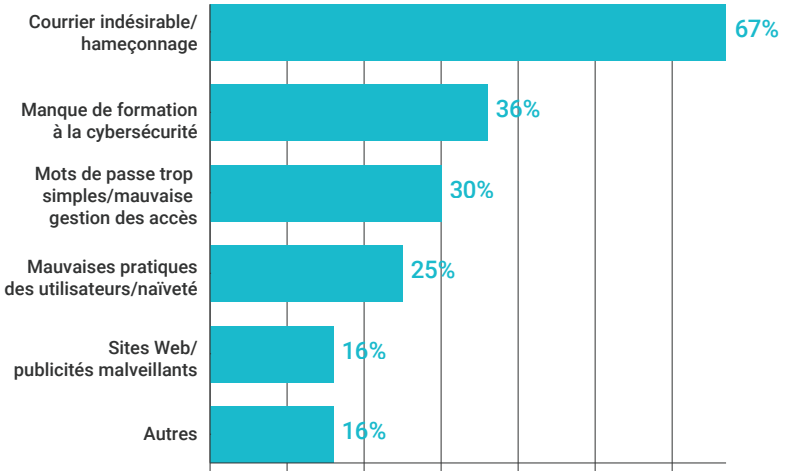

Figure 4 : méthodes d'infection par ransomware les plus courantes en Amérique du Nord (d'après les attaques sur des organisations signalées par les MSP) (Source : SafetyDetectives)

Les courriers indésirables et d'hameçonnage, les mots de passe trop simples et les sites Web malveillants sont les méthodes les plus courantes d'infection par ransomware.

DÉTECTION

Malheureusement, la prévention n'est pas toujours possible. L'industrie de la sécurité reconnaît de plus en plus qu'une posture de cybersécurité efficace doit combiner des capacités de prévention, de détection et de réponse. Au cas où un ransomware déjouerait vos efforts de prévention, vous devez avoir mis en place les processus et outils appropriés pour le détecter avant qu'il ne se soit pleinement activé. Les outils de détection et d'alerte en temps réel constituent votre première ligne de défense. Ces outils doivent également inclure la surveillance et l'analyse pour assurer l'intégrité et la disponibilité de votre dernière ligne de défense : vos données de sauvegarde. Voici quelques bonnes pratiques :

- **Aligner la protection avec les engagements de l'entreprise :** assurez-vous que tous les systèmes et données critiques sont protégés d'une manière qui garantisse que les RPO (Recovery Point Objectives) et RTO (Recovery Time Objectives) pourront être respectés. Prévoyez également une durée de conservation des données suffisante au cas où une infection par ransomware ne serait détectée qu'après plusieurs semaines ou mois.
- **Identifier les données affectées au niveau granulaire :** mettez en œuvre des outils capables d'identifier, au niveau

Au cas où un ransomware déjouerait vos efforts de prévention, vous devez avoir mis en place les processus et outils appropriés pour le détecter avant qu'il ne se soit pleinement activé.

Figure 5 : les outils qui évaluent automatiquement l'impact d'une attaque et identifient clairement quels applications et fichiers ont été chiffrés et où ils se situent permettent une récupération plus rapide au niveau granulaire qui minimise la perte de données

du fichier ou de l'objet, quelles données ont été infectées par le ransomware (voir **Figure 5**). Disposer de ces informations au moment d'une attaque est extrêmement précieux pour accélérer la récupération et préserver les données non infectées. Les innovations telles que le Machine Learning (ML) peuvent aider à identifier les tendances existantes parmi tous les échantillons de données de sauvegarde et classifier

les nouvelles données en fonction de leurs similitudes sans nécessité d'intervention humaine. Cette analyse est basée en grande partie sur l'analyse du comportement du système de fichiers et du contenu effectuée sur les métadonnées du système de fichiers. Elle examine des caractéristiques telles que le nombre de fichiers ajoutés, le nombre de fichiers supprimés, etc., afin de détecter des comportements inhabituels et d'alerter les équipes informatiques et de sécurité. Elle peut également fournir une couche d'intelligence supplémentaire pour la détection des anomalies dans vos données de sauvegarde, votre dernière ligne de défense.

RÉPONSE ET RÉCUPÉRATION

Lorsqu'une attaque de ransomware a été détectée, la notification rapide des parties prenantes et des membres de l'équipe d'intervention (y compris le service support des fournisseurs) aidera à s'assurer que les personnes appropriées sont engagées et mobilisées aussi vite que possible. La première étape d'une réponse efficace consiste à évaluer l'étendue de l'attaque et à isoler tout système suspecté d'avoir été infecté. Vous devez avoir un plan pour isoler les systèmes infectés afin d'empêcher le ransomware de s'étendre davantage sur le réseau. Vous devez également avoir un plan pour récupérer les systèmes et les données infectées que vous avez isolés du réseau. Lorsqu'il est impossible de neutraliser un ransomware en toute sécurité, il peut être nécessaire d'effectuer la récupération sur de nouveaux systèmes sur un réseau distinct. Voici quelques bonnes pratiques supplémentaires :

- **Déterminer quelles méthodes de récupération seront utilisées pour chaque type de récupération.** Des options telles que Live Mount pour des VM VMware permettent de récupérer

des systèmes en quelques minutes. Cependant, celles-ci restaurent des systèmes entiers à un point sûr dans le temps, de sorte que des données non infectées peuvent être perdues. La restauration des données infectées au niveau des fichiers ou des bases de données peut-être une meilleure option. La méthode appropriée doit être identifiée en amont afin de pouvoir être sélectionnée rapidement lors d'une attaque.

- **Exploiter l'automatisation afin d'accélérer la réponse et de réduire l'erreur humaine.** Un facteur clé de la récupération est l'automatisation, car elle minimise le risque d'erreur humaine. Par ailleurs, elle accélère la récupération et facilite le suivi de l'avancement. Votre fournisseur de sauvegarde et de restauration doit proposer un ensemble complet d'API et de SDK pour faciliter l'automatisation de la récupération. Ceux-ci peuvent être intégrés avec des outils d'automatisation comme Ansible, Terraform, Puppet, Chef, PowerShell et Python. Une fois que vous avez établi votre plan de reprise et vos priorités, l'automatisation est l'étape suivante du développement de capacités de récupération solides.

Lorsqu'un ransomware a été détecté, examinez avec soin les paramètres d'expiration des instantanés afin de vous assurer qu'aucun instantané valide susceptible d'affecter la récupération des données n'expire. Les accords de niveau de service (SLA) avec des politiques de conservation à court-terme doivent être étendus pour au moins un an pendant toute la durée de l'événement de ransomware. Veillez à noter les périodes de conservation d'origine afin de pouvoir les rétablir une fois que l'événement de ransomware est terminé.

Avant de démarrer le processus de récupération, il est important de savoir quel est le type de récupération nécessaire. Si le

Demandez à votre fournisseur s'il peut garantir des RTO proches de zéro pour les machines virtuelles, le partage de fichiers et les bases de données et exécuter une récupération instantanée des fichiers sans hydratation des données.

ransomware a seulement infecté des fichiers sur des serveurs ou des partages utilisateur sur un serveur NAS, une méthode de récupération sur la base des fichiers peut être utilisée. En revanche, si le ransomware a attaqué les images du disque virtuel d'un hyperviseur ou l'enregistrement d'amorçage maître (MBR) d'un système physique, une récupération du système complet peut être nécessaire. Voici quelques bonnes pratiques de récupération :

- **Bonnes pratiques de récupération générales** (s'appliquent à tous les scénarios de récupération) :
    - *Récupérer en toute sécurité :* ne commencez les opérations de récupération qu'une fois le ransomware neutralisé. Cela peut signifier que les données devront être récupérées de manière isolée ou sur de nouveaux systèmes. Si vous restaurez des systèmes ou des données avant que le ransomware n'ait été neutralisé, ceux-ci risquent d'être infectés de nouveau. S'il est impossible d'isoler et de neutraliser le ransomware rapidement, il convient de récupérer les systèmes en les isolant à un emplacement où ils ne peuvent pas être réinfectés.
    - *Récupération isolée en local :* les attaques de ransomware sont souvent tellement invasives que la récupération à l'emplacement d'origine se traduit par des infections

secondaires. Le meilleur moyen d'éviter une infection secondaire est la récupération vers un environnement local isolé de l'environnement infecté. La planification durant la phase de préparation (abordée précédemment) doit inclure l'identification et les tests de la récupération locale dans un environnement isolé.

- *Récupération priorisée :* comme prévu à la phase de prévention, la récupération s'effectuera en fonction des priorités établies pour les applications et les lignes métiers. Assurez-vous que les services fondamentaux nécessaires au fonctionnement de base, tels que le DNS, le DHCP et l'authentification, fonctionnent ou sont restaurés en priorité. Sans ces services fondamentaux, les systèmes récupérés pourraient ne pas fonctionner correctement.

- **Bonnes pratiques de récupération des fichiers seulement** (s'appliquent aux scénarios où seuls des fichiers et répertoires doivent être récupérés) :

  - *Vérifier le système d'exploitation :* vérifiez que le système d'exploitation sous-jacent est fiable et n'a pas été compromis lors de l'attaque de ransomware.

  - *Récupérer sur un système propre :* si le système d'origine n'est pas fiable, récupérez les fichiers sur un système reconnu en bon état. Il peut s'agir d'un système nouvellement créé isolé de l'environnement de production

  - *Identifier les fichiers à récupérer :* utilisez des outils automatisés pour identifier les fichiers infectés par le ransomware et les récupérer.

- **Bonnes pratiques de récupération des machines virtuelles et bases de données** (s'appliquent lorsque la MV elle-même

ne peut pas être utilisée, ce qui arrive notamment lorsque le stockage NAS sur lequel la VM s'exécute a été compromis, ou si le ransomware empêche le démarrage de la MV). Tous les fournisseurs n'offrent pas des capacités de récupération instantanée. Un fournisseur de solutions de protection des données modernes comme Rubrik fournit ces capacités, permettant ainsi des restaurations rapides et précises :

- *Restaurer des ensembles de données plus petits :* les capacités de récupération instantanée permettent aux machines virtuelles (VM) et aux bases de données d'être montées directement à partir du stockage, économisant le temps nécessaire pour copier les sauvegardes sur le stockage principal avant que les ressources soient de nouveau disponibles. Une fois montées, les VM peuvent être transférées sur le stockage principal en arrière-plan tout en fournissant leurs services habituels. Les bases de données peuvent être exécutées jusqu'à ce qu'une interruption planifiée puisse être programmée afin de les replacer sur le stockage principal.

- *Exporter directement vers le stockage principal :* les solutions de protection des données modernes comprennent une fonction d'exportation permettant de récupérer ou de copier une machine virtuelle ou une base de données directement sur le stockage principal. Une fois copiée, la VM ou la base de données peut-être remise en ligne. Cette méthode affiche la vitesse de transfert de données vers le stockage principal la plus rapide et est idéale pour récupérer de nombreuses machines virtuelles.

- *Associer récupération instantanée et exportation :* il est possible de lancer simultanément les charges de travail de récupération instantanée et d'exportation, mais cela doit être fait avec une extrême prudence. Les exportations utiliseront pleinement les ressources du cluster de stockage pour transférer les données vers le stockage principal. La récupération instantanée pourrait être forcée de composer avec le trafic en cours de récupération. Cela pourrait dégrader les performances au niveau des machines virtuelles et des bases de données restaurées avec la récupération instantanée. La récupération avec charge de travail mixte doit être évaluée au cas par cas.

- **Bonnes pratiques de récupération du gestionnaire de l'hyperviseur** (coordonnez la récupération des vCenters ou autres hyperviseurs avec l'équipe d'assistance appropriée pour assurer une récupération fluide) :

  - *Récupération d'un vCenter :* il convient d'être prudent lorsque le vCenter doit être récupéré, ou lors de la récupération de machines virtuelles dans un nouveau vCenter. La duplication ou la réutilisation de l'ID d'objet géré (MOID) VMware peut engendrer des problèmes lors de la récupération des machines virtuelles. Si le vCenter a été compromis, il est préférable de le restaurer à partir de la sauvegarde plutôt que de créer un nouveau vCenter vide et de récupérer les machines virtuelles dans ce dernier.

  - *Récupération et/ou réinstallation de gestionnaires d'hyperviseur non-vSphere :* lorsque des gestionnaires d'hyperviseur tels que Microsoft System Center Virtual Machine Manager (SCVMM) ou Nutanix Prism sont protégés à l'aide d'instantanés, contactez votre

fournisseur de sauvegarde et de restauration pour connaître les options de récupération. Lorsque le gestionnaire d'hyperviseur est protégé par des méthodes de sauvegarde intégrée, contactez le fournisseur de l'hyperviseur en plus du fournisseur de sauvegarde et de restauration.

Récupérez plus vite et plus facilement

Les ransomwares continuent de proliférer et coûtent des millions de dollars aux entreprises. Par ailleurs, ils ont évolué et deviennent de plus en plus sophistiqués. Les ransomwares ne font pas que bloquer l'accès au système, ils chiffrent ou suppriment des données actives, y compris des sauvegardes sur les systèmes vulnérables.

Lorsque la prévention d'une attaque de ransomware échoue, il est vital pour récupérer de disposer d'une sauvegarde immuable qui ne peut être ni supprimée, ni chiffrée. La capacité à identifier intelligemment et à corriger les données chiffrées facilite et accélère les efforts de récupération tout en réduisant les pertes de données et les temps d'arrêt.

Rubrik aide les organisations à récupérer plus rapidement des attaques de ransomware grâce à des applications innovantes comme Rubrik Instant Recovery, Rubrik Radar pour l'analyse d'impact détaillée et la détection des anomalies, et Rubrik Sonar pour la découverte des données sensibles. Pour en savoir plus, rendez-vous sur https://rubrik.com/ransomware-recovery.

À propos de Rubrik

Rubrik aide les entreprises à maîtriser les données afin de favoriser leur résilience, leur mobilité dans le cloud et leur conformité règlementaire. Rubrik comble le fossé entre l'infrastructure sur site et le cloud en découplant les données du datacenter à l'aide d'une matrice définie par logiciel et en offrant un plan de gestion unique pour l'ensemble des données, qu'elles soient sur site ou dans le cloud. La gestion complète des données est fournie grâce à un accès instantané, l'orchestration automatisée, une protection des données et une résilience exceptionnelle.

À propos d'ActualTech Media

ActualTech Media est une entreprise de marketing technologique B2B qui connecte les fournisseurs IT d'entreprise aux acheteurs par le biais de programmes innovants de génération de prospects et de services de contenu personnalisés attrayants.

L'équipe d'ActualTech Media s'adresse à l'audience IT d'entreprise parce qu'il s'agit du secteur auquel nous appartenons.

Composée d'anciens DSI, responsables IT, architectes, experts dédiés et professionnels du marketing, notre équipe de direction aide les clients à limiter le temps qu'ils consacrent à la formation aux outils pour se focaliser sur la création de stratégies porteuses de croissance.

Vous êtes responsable informatique et vous souhaitez obtenir votre propre titre personnalisé Gorilla Guide® ou Innovations Learning Series pour votre société, rendez-vous sur https://www.gorilla.guide/custom-solutions/