

NAKIVO®

**Meilleures pratiques pour
protection et récupération en cas
d'une attaque par ransomware**

Table des matières

Aperçu	3
Notions de base sur les ransomwares	
Qu'est-ce qu'un ransomware ?	5
Ransomware en tant que service	5
Vecteurs d'infection par ransomware	6
Protection contre les ransomwares	
Qu'est-ce qu'un plan d'intervention en cas d'incident ?	8
Qu'est-ce qu'un incident dans l'ITIL ?	9
Étapes impliquées dans l'intervention en cas d'incident	9
Meilleures pratiques en matière de protection contre les ransomwares	11
Suivre la règle de sauvegarde 3-2-1	11
Utiliser de multiples destinations de sauvegarde	11
Utiliser la réplication pour la récupération après sinistre	11
Créer une stratégie de rétention appropriée	12
Protection et récupération en cas d'attaque par ransomware avec NAKIVO Backup & Replication	
Sauvegardes natives sans agent	13
Sauvegarde vers des destinations multiples	13
Sauvegardes à l'abri des ransomwares	13
Vérification instantanée de sauvegarde/réplica de VM	14
Récupération granulaire	14
Flash VM Boot	14
P2V Recovery	15
Réplication pour la récupération après sinistre	15
Orchestration et automatisation de la récupération après sinistre	15
Protection des données complète avec NAKIVO Backup & Replication	17
À propos de NAKIVO	17

Aperçu

La pandémie a changé la manière dont les petites entreprises et les multinationales opèrent. Elle a affecté non seulement la manière dont les employés travaillent et collaborent, mais également les interactions avec les clients et le service client. Les entreprises se sont tournées de plus en plus vers des services et des plateformes cloud pour assurer la continuité opérationnelle. Cette transition s'est accompagnée d'avantages considérables, allant d'une plus grande flexibilité à une meilleure visibilité. Mais parallèlement à ces avantages, les entreprises ont également été confrontées à la vulnérabilité des données due à un changement aussi soudain.

L'année dernière a été marquée par une hausse sans précédent des attaques par ransomware, les cybercriminels cherchant à exploiter à des fins lucratives ces nouveaux défis en matière de protection des données. Aux trois premiers trimestres de l'année 2020, 21 % des pertes de données sont le résultat d'attaques par ransomware¹. Cybersecurity Ventures a prévu qu'en 2021 une entreprise ferait l'objet d'une attaque par ransomware toutes les 11 secondes². Les attaques par ransomware constituent l'une des raisons principales pour lesquelles les entreprises perdent des données de manière définitive et cela se traduit par une perte de productivité, de revenu et de clients.

Les entreprises n'ayant pas élaboré de plan de protection contre les ransomwares deviennent souvent les otages des cybercriminels. Après avoir réussi leur attaque et s'être emparés de données, les pirates informatiques peuvent exiger des paiements pour restaurer l'accès aux données commerciales ou pour ne pas les diffuser. Sous la pression d'une perte de données potentielle, d'une exposition médiatique ou de nouvelles attaques, les entreprises cèdent souvent devant les exigences des pirates informatiques. Selon le dernier rapport The State of Ransomware 2021 de Sophos, 37 % des entreprises ont fait l'objet d'une attaque par ransomware en 2020, le coût moyen par attaque étant de 170 404 dollars US³. Et pourtant, même une fois la rançon versée, seulement 65 % en moyenne des données chiffrées ont été récupérées⁴.

Ces paiements de rançon élevés indiquent que les entreprises ne sont pas toujours préparées à gérer de manière proactive l'éventualité d'une attaque par ransomware. Une approche proactive doit couvrir les mesures de sécurité permettant de prévenir les attaques, les mesures à prendre en cas d'incident, ainsi qu'un plan de protection des données/récupération après sinistre. Et quelle que soit l'ampleur de l'attaque, payer les pirates n'est

1 Risk Based Security, 2020

https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020_Q3_Data_Breach_QuickView_Report.pdf

2 Cyber Security Ventures, 2019

<https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>

3 Sophos, 2021

<https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>

4 Sophos, 2021

<https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>

pas la bonne réponse. Leur verser la rançon peut avoir pour dangers une perte additionnelle de données, une sécurité compromise, une atteinte à la réputation et des pertes financières, sans compter le fait d'inciter les cybercriminels à perpétrer d'autres attaques.

Payer les cybercriminels peut également avoir des conséquences juridiques pour les entreprises. En octobre 2020, le Département américain du Trésor a émis un document consultatif soulignant les risques de sanction associés au règlement de sommes lié aux cyberattaques malveillantes⁵. Verser la rançon ne garantit pas la restauration de l'accès aux données commerciales et peut entraîner des pertes supplémentaires sous la forme de dépenses juridiques et d'amendes, lesquelles entravent davantage la restauration de l'accès aux données.

Quelles que soient les mesures de cybersécurité mises en place, les pirates informatiques trouvent des moyens d'infiltrer les systèmes et de verrouiller les données de leur victime. Mais avec une approche holistique et une intervention rapide, les chances de récupérer entièrement les données sont assez élevées. Les entreprises doivent donc se tourner vers les méthodes éprouvées et efficaces de protection et de récupération en cas d'attaque par ransomware. Désormais, des fournisseurs tiers offrent des solutions complètes de sauvegarde et de récupération qui garantissent aux entreprises la continuité de leurs activités même si des agissements malveillants ont lieu et que la première ligne de défense échoue.

Les entreprises doivent envisager d'établir un plan d'intervention en cas d'incident (IRP, Incident Response Plan) pour gérer efficacement les attaques par ransomware. Un bon IRP couvre généralement une plage d'événements allant des attaques par ransomware à la perte de données et intègre les meilleures méthodes de protection et de récupération des données. Un plan d'intervention en cas d'incident et une solution de sauvegarde de pointe peuvent garantir l'accessibilité des données, la récupérabilité, ainsi que leur disponibilité à 99,999 %.

Les attaques par ransomware frappent les petites entreprises comme les grandes. Mais une chose est claire : toutes les entreprises doivent observer des pratiques intelligentes de protection et de récupération en cas d'attaque par ransomware afin d'éliminer toute menace externe potentielle. Ce document porte sur les dernières meilleures pratiques dans la protection et la récupération en cas d'attaque par ransomware pour les entreprises de tous les secteurs. Il couvre les ransomwares, les plans d'intervention en cas d'incident (IRP, Incident Response Plan), la protection des données, la récupération après sinistre et les stratégies de gestion des cybermenaces.

⁵ Department of the Treasury, 2020

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Notions de base sur les ransomwares

Qu'est-ce qu'un ransomware ?

Un ransomware est un type de logiciel malveillant qui chiffre ou verrouille les données d'une victime. Une fois les données rendues inaccessibles, le cybercriminel peut exiger un paiement pour les rendre à nouveau accessibles. Les deux types de ransomware principaux sont les suivants :

- **Crypto-ransomware.** Ce type de ransomware sélectionne les fichiers/dossiers puis les rend illisibles. Un crypto-ransomware brouille les données à l'aide d'un algorithme de chiffrement spécifique. Pour que les données soient à nouveau disponibles, la victime doit obtenir une clé de déchiffrement.
- **Ransomware de verrouillage.** Ce type de ransomware verrouille le système entier de l'entreprise ciblée. L'utilisateur voit alors son accès au système verrouillé. Un message apparaît sur son écran et peut afficher la somme et la date à laquelle un paiement doit être effectué pour retrouver l'accès.

Ces deux types de ransomware ont des approches différentes pour compromettre les données et les systèmes, mais le résultat est le même. Une fois les données critiques bloquées, de nombreuses victimes n'ont d'autre choix que de verser la rançon. Cependant, même après avoir été payés, les pirates informatiques ne respectent pas toujours l'entente. De ce fait, les entreprises ne sont pas en mesure de récupérer leurs données. Les attaquants acceptent souvent d'être payés en bitcoins ou dans une autre crypto-monnaie, ce qui leur permet de couvrir leurs traces et d'éviter les poursuites.

Ransomware en tant que service

Aujourd'hui, les pirates informatiques opèrent comme des entreprises. Ils font fonctionner des sites Web, embauchent des employés et publient même des communiqués de presse. En fait, un nouveau modèle de ransomware a récemment émergé, avec des développeurs de ransomwares offrant des programmes malveillants sur la base d'un abonnement. On appelle ce nouveau modèle commercial « ransomware en tant que service » (RaaS, Ransomware as a Service), un dérivé de « logiciel en tant que service » (SaaS, Software as a Service).

Le modèle RaaS fournit des ransomwares dans un logiciel qui permet à des cybercriminels peu expérimentés dans le développement de ransomwares de lancer des attaques malveillantes dans une courte période de temps. Les entreprises RaaS vendent souvent leurs produits sur le dark web aux attaquants à la recherche de solutions rapides et prêtes à l'emploi.

Que le ransomware soit développé par une personne, un acteur étatique ou via un modèle RaaS, tous les cybercriminels utilisent des tactiques et des vecteurs d'infection similaires en vue de l'extorsion. Ainsi, comprendre les vecteurs d'infection couramment utilisés et le comportement des ransomwares peut vous aider à prévenir et surmonter les incidents.

Vecteurs d'infection par ransomware

La majorité des attaques par ransomware sont amorcées à cause d'utilisateurs peu méfiants qui visitent des sites malveillants ou cliquent sur des liens malveillants. La sensibilisation des employés est donc une priorité dans toute stratégie de lutte contre les programmes malveillants.

Les vecteurs d'attaque les plus répandus sont le hameçonnage, les kits d'exploits, les botnets téléchargeurs et chevaux de Troie, l'ingénierie sociale et la distribution du trafic.

- **Hameçonnage.** Le hameçonnage est un type d'attaque utilisant la messagerie pour arnaquer les utilisateurs. Les cybercriminels envoient des e-mails frauduleux prétendant provenir d'entités fiables. L'objectif est d'amener la victime à communiquer des informations personnelles telles que des données bancaires ou des identifiants de connexion, ou à cliquer sur un lien malveillant.
- **Kits d'exploits.** Il s'agit de jeux d'outils entièrement automatisés visant à exploiter discrètement les vulnérabilités de l'environnement ciblé (par exemple, un site Web compromis). Lorsqu'un visiteur accède au site, il se peut qu'il télécharge par inadvertance une charge utile malveillante, infectant ainsi son système. Les cybercriminels utilisent souvent des kits d'exploits pour diffuser des programmes malveillants en masse.
- **Botnets.** Les botnets sont des réseaux informatiques contrôlés par les cybercriminels pour diffuser des ransomwares et lancer des attaques par hameçonnage. Ils permettent de lancer des attaques par déni de service distribué (DDoS, Distributed-Denial-Of-Service).
- **Ingénierie sociale.** Au lieu d'utiliser des moyens techniques, l'ingénierie sociale utilise la manipulation psychologique pour convaincre les utilisateurs de communiquer leurs données de connexion ou autres informations sensibles. Les attaquants utilisent ces informations pour accéder au système et l'infecter par un ransomware.
- **Distribution du trafic** La distribution du trafic est un mécanisme malveillant qui permet d'orienter la victime vers un site Web infecté. Une action effectuée sur un tel site peut déclencher le téléchargement d'une charge utile malveillante.

Les vecteurs d'infection par ransomware varient d'élémentaires à sophistiqués, mais leur objectif principal est de déjouer la sécurité et de prendre le contrôle de la machine et des données de la victime. Une fois qu'un ransomware a déjoué la sécurité, il procède de l'une ou plusieurs des manières suivantes pour infecter l'environnement :

- **Persistance des charges utiles.** Les charges utiles sont similaires aux virus. Elles consistent en lignes de code diffusées avec des kits d'exploits et des tactiques de distribution du trafic. Les pirates informatiques utilisent les charges utiles pour établir des connexions avec l'appareil de la victime. Ils peuvent alors s'octroyer des privilèges d'administrateur et télécharger des fichiers malveillants dans le système de la victime. L'attaquant peut cacher le code (par exemple, un registre) à l'utilisateur. Ce bloc de code

lui permet de prendre entièrement le contrôle du système de la victime, y compris des données, des mots de passe et des activités du réseau⁶. Pour s'assurer que les charges utiles ne sont pas supprimées par un simple redémarrage du système, les pirates informatiques établissent la persistance des charges utiles⁷. Cette opération permet aux charges utiles de contourner le redémarrage. Ceci fait, la machine de la victime est à la disposition de l'attaquant à tout moment⁸.

- **Mappage d'environnement.** À la phase de configuration, le ransomware mappe votre environnement afin de s'assurer qu'il n'est pas limité à un sandbox. Un sandbox est un environnement virtuel qui imite l'environnement d'origine. Il est souvent utilisé comme mesure de sécurité face aux cyberattaques. Toutefois, certains ransomwares peuvent analyser l'environnement qu'ils infectent et déterminer s'ils ciblent un environnement réel ou un sandbox.
- **Élévation des privilèges.** Le plus souvent, les attaquants explorent le système ou le réseau dans le but d'obtenir un accès illimité à une machine ou à un compte utilisateur spécifique. Lorsqu'ils détectent des failles dans le code, ils profitent de cette opportunité et obtiennent les droits d'administration complets au niveau de la machine, de l'application, du réseau ou du compte utilisateur ciblé. Disposer d'un contrôle total d'un réseau ou de n'importe quel compte ou logiciel open source permet au pirate informatique de lancer son attaque sans être détecté⁹.
- **Restriction de la restauration du système.** Lorsqu'un pirate informatique obtient le contrôle des droits d'administration et du registre, il peut mettre en place des restrictions au niveau de la restauration du système et ainsi empêcher qu'un appareil soit restauré à son état précédent. Dans ce cas, la victime n'est pas en mesure de récupérer ses données et de supprimer la charge utile de son appareil.
- **Mode furtif.** Les ransomwares passent souvent en mode furtif pour éviter d'être détectés. Cela implique, entre autres actions, de masquer les communications, ce qui permet de transmettre des informations aux attaquants et de compliquer le suivi. Dans le mode furtif, un cybercriminel peut accéder à des données et établir des brèches sur le réseau sans être détecté par les systèmes de sécurité.^{10 11}

6 Hacking Articles, 2020

<https://www.hackingarticles.in/multiple-ways-to-persistence-on-windows-10-with-metasploit/>

7 A note on different types of ransomware attacks, IACR, 2019

<https://eprint.iacr.org/2019/605.pdf>

8 Vulnerabilities Assessments in Ethical Hacking, AJER, 2016

<http://www.ajer.org/papers/v5t05yA05050105.pdf>

9 TechGenix, 2004

<https://techgenix.com/registryhacktodisablestoreoptionfromxpstartmenuandcontrolpanel/>

10 Hackers Wikia

https://hackersthegame.fandom.com/wiki/Stealth_Programs

11 AFCEA, 2019

<https://www.afcea.org/content/stealth-attacks-require-stealth-responses>

Protection contre les ransomwares

Le cybercrime évolue en permanence et les cybercriminels trouvent de nouvelles vulnérabilités et de nouveaux moyens d'infiltrer les systèmes. Ils trouvent également de nouvelles manières de gagner de l'argent grâce au modèle RaaS et ciblent des entreprises importantes gérant des données extrêmement sensibles. C'est pourquoi la stratégie de protection contre les ransomwares doit couvrir la protection des données/récupération après sinistre, ainsi que les mesures de sécurité, les formations visant à sensibiliser les employés et la détection/l'endiguement.

Ce papier porte sur la protection des données et la récupération après sinistre dans le cadre d'un plan d'intervention en cas d'incident pour une récupération rapide et sûre face aux menaces externes.

Qu'est-ce qu'un plan d'intervention en cas d'incident ?

La protection et la récupération en cas d'attaque par ransomware consiste à garantir un fonctionnement continu des services informatiques. Quelle que soit le référentiel méthodologique utilisé, qu'il s'agisse d'ITIL (Bibliothèque pour l'infrastructure des technologies de l'information) ou autre, il vous incombe de vous assurer que les systèmes et les données sont disponibles et accessibles en temps voulu. Un plan d'intervention en cas d'incident indique les mesures que votre service informatique doit prendre pour détecter un incident de sécurité, y répondre et s'en remettre.

Avec ou sans contrat de niveau de service (SLA, Service Level Agreement) formel, un service informatique doit fonctionner pratiquement sans interruptions et les systèmes critiques doivent être disponibles 99,999 % du temps. Cette norme n'autorise que 5 minutes et 15 secondes de temps d'arrêt imprévu par an !

Atteindre le niveau de disponibilité exigé par votre entreprise implique de spécifier le temps nécessaire à la remise en marche des systèmes après un incident et la quantité de données que l'entreprise peut tolérer de perdre : en d'autres termes, déterminer votre objectif de temps de récupération (RTO, Recovery Time Objective) et votre objectif de point de récupération (RPO, Recovery Point Objective).

Définitions

RTO : délai durant lequel les opérations de l'entreprise doivent être restaurées pour éviter des conséquences négatives ou irréversibles.

RPO : quantité maximale de données pouvant être perdues au cours de l'incident sans dommages sérieux pour l'entreprise.

REMARQUE : La protection contre les ransomwares nécessite des sauvegardes régulières des charges de travail à une fréquence qui dépend de votre objectif de point de récupération (RPO).

Qu'est-ce qu'un incident dans l'ITIL ?

L'ITIL (Information Technology Infrastructure Library) est aujourd'hui l'une des méthodologies les plus utilisées dans l'exécution des services informatiques. Examinons la définition d'un incident et les instructions fournies par l'ITIL pour gérer les incidents, car ces instructions peuvent être appliquées même sans adoption formelle de l'ITIL.

L'ITIL fait la différence entre un incident, un problème et une requête.

Définitions

Un incident est une « interruption non prévue d'un service informatique, une baisse de qualité d'un service informatique ou un échec d'un composant de configuration n'ayant pas encore eu d'impact sur un service informatique (par exemple, la panne d'un disque d'un miroir de volume). »¹²

Selon l'ITIL, les principales tâches de gestion des incidents comprennent les suivantes :

- Restaurer au plus vite les services de l'entreprise
- Réduire l'impact négatif de l'incident sur l'entreprise
- Maintenir une qualité élevée de toutes les opérations¹³.

Étapes impliquées dans l'intervention en cas d'incident

Il est recommandé d'élaborer un plan d'intervention en cas d'incident efficace prenant en compte les besoins spécifiques ainsi que le RTO et le RPO de votre entreprise. Ce plan doit couvrir les mesures immédiates à prendre pendant et à la suite de l'attaque par ransomware. Le plan de base d'intervention en cas d'incident implique de communiquer l'incident, de contenir les dommages, de supprimer le logiciel malveillant et de récupérer les données :¹⁴

- Chaque entreprise doit déterminer la chaîne hiérarchique à suivre en cas d'incident de sécurité. La première étape consiste à informer la direction et le PDG de l'entreprise.
- Ceux-là peuvent estimer la sévérité de l'attaque et embaucher ou nommer des experts qualifiés pour résoudre la situation. Les mesures appropriées peuvent être prises une fois que la situation d'ensemble devient claire, par exemple lorsque le type de programme malveillant utilisé et les causes sous-jacentes sont connus.

12 ITIL Service Operation, United Kingdom: The Stationery Office, 2011

13 ITSM Process Description - Incident Management

https://www.alaska.edu/files/oit/ITSM_Program/Incident-Management-Process-Description-v1.pdf

14 Cyber Security Incident Management Guide

<https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FN.pdf>

- À l'étape de la suppression du programme malveillant, tous les outils utilisés par l'attaquant doivent être supprimés des systèmes. Il est vital d'éliminer le programme malveillant, de supprimer les comptes utilisateur compromis et les fichiers spécifiques, de bloquer les e-mails de hameçonnage et d'exécuter des analyses de sécurité pour s'assurer que tous les problèmes ont bien été éliminés. Il est également recommandé d'examiner toutes les machines susceptibles d'être affectées par l'incident et de vérifier qu'elles ne sont pas infectées.
- Selon l'ampleur de l'attaque et si l'entreprise dispose d'un site secondaire de récupération après sinistre, il est possible de basculer vers ce site. Basculer les charges de travail vers un site de récupération après sinistre réduit les temps d'arrêt et permet à l'entreprise de poursuivre ses opérations. Une fois l'attaque contenue et les systèmes purgés, une restauration du site de production peut avoir lieu.
- Un processus de récupération peut être lancé lorsque les machines et les systèmes ont été purgés. Une récupération rapide nécessite des sauvegardes rapides et de qualité. Dans le cadre du plan d'intervention en cas d'incident, des stratégies de sauvegarde efficaces doivent être élaborées et maintenues à jour avant toute attaque. Si l'entreprise ne dispose pas de sauvegardes précédentes ou suffisantes, le processus de récupération est plus complexe. Il peut être nécessaire de reconstruire l'environnement de travail en entier, ce qui peut s'avérer long et coûteux. Par exemple, certaines entreprises continuent à travailler avec des versions arrêtées d'anciens fichiers. Dans ce cas, il est toujours possible que certains des programmes malveillants soient restés dans le système.

Liste de contrôle

Questions auxquelles répondre avant de formuler un plan d'intervention en cas d'incident :

- Combien de temps votre entreprise peut-elle survivre sans ses systèmes critiques ?
- Quel est le nombre maximal d'utilisateurs pouvant être affectés par l'incident ?
- Quelles sont les machines prioritaires pour la sauvegarde et la réplication vers un site secondaire ? Quels sont les RTO et les RPO de ces machines ?
- Quelles sont les données les plus essentielles pour les sauvegardes prioritaires et à la récupération instantanée ?
- Quelles sont les responsabilités du personnel pendant l'incident ?
- Quelle quantité de données est générée par l'entreprise ? Ces données changent-elles souvent ? Quelle est leur importance ?

Meilleures pratiques en matière de protection contre les ransomwares

Dans le cadre de leurs processus de travail et avant que ne survienne une activité non désirée, les entreprises sont invitées à observer les meilleures pratiques en matière de protection contre les ransomwares. La conservation des données dans plusieurs emplacements et une compréhension des meilleures pratiques sont essentielles à une récupération sans heurts pendant et après un incident de ransomware.

Suivre la règle de sauvegarde 3-2-1

Il est important de garder à l'esprit que même le fait de verser la rançon ne garantit pas que les cybercriminels fourniront les clés de déchiffrement. De ce fait, la sauvegarde doit demeurer au cœur de la planification de la récupération après sinistre. Et l'approche adéquate de la sauvegarde réside dans l'observation de la règle 3-2-1. Selon cette règle, vous devez disposer d'au moins trois copies de vos données. Deux d'entre elles doivent résider sur des supports différents tandis que la troisième doit être stockée hors site.

Bien que la sauvegarde principale puisse se trouver au même emplacement physique que les données de production, assurez-vous qu'elle est stockée sur un type de support différent. Même si les deux sauvegardes ne sont plus disponibles, vous pouvez récupérer vos données critiques à partir de la sauvegarde hors site. Pour améliorer encore vos chances de réussir la récupération des données, créez des copies de sauvegarde supplémentaires. Plus vous disposez de copies de vos données, plus vous aurez de chances de réussir la récupération de vos données.

Utiliser de multiples destinations de sauvegarde

Pour mettre en pratique la règle 3-2-1, stockez vos sauvegardes sur des supports différents tels que des partages réseaux locaux, le stockage cloud, des serveurs hors site, des appliances de déduplication, des bandes magnétiques et des appliances NAS. Le choix du support de stockage doit reposer sur le type et la taille de votre infrastructure et sur vos contraintes budgétaires. Il en va de même pour le nombre de copies de sauvegarde que vous créez, qui ne doit pas être inférieur à trois. Gardez à l'esprit que des copies de sauvegarde multiples peuvent protéger vos données non seulement contre les ransomwares, mais aussi contre une panne d'un appareil de stockage, laquelle n'est pas un événement rare.

Utiliser la réplication pour la récupération après sinistre

Même le temps d'arrêt le plus court peut diminuer la productivité et les revenus d'une entreprise. C'est pourquoi, outre des sauvegardes fiables, vous pouvez avoir recours à la réplication pour réduire les RTO et les RPO à un minimum pendant et après une attaque par ransomware. Créez des répliques de vos VM et conservez-les hors site dans un emplacement secondaire. Bien entendu, tout dépend du nombre de sites et du budget dont votre entreprise dispose. Mais cette approche peut apporter une couche de protection supplémentaire lorsqu'elle est possible.

Si votre site de production principal n'est pas opérationnel en raison d'une attaque par ransomware sévère, il vous suffit de basculer vers le réplica et de reprendre vos opérations. Vous pouvez revenir à votre site principal une fois qu'il a été purgé et qu'il fonctionne à nouveau.

Créer une stratégie de rétention appropriée

Une stratégie de rétention de sauvegarde vous aide à gérer vos données efficacement. Elle vous permet de conserver les sauvegardes jusqu'à un point spécifique dans le temps et de les archiver ou de les supprimer après une certaine période. La stratégie de rétention de sauvegarde vise à obtenir le plus de points de récupération tout en utilisant un espace minimal. Une stratégie de rétention bien pensée vous permet d'économiser l'espace de stockage en remplaçant les anciens points de récupération par de nouveaux, vous permettant ainsi de récupérer la version de données dont vous avez besoin. Gardez suffisamment de points de récupération pour chaque sauvegarde et effectuez des rotations quotidiennes, hebdomadaires, mensuelles et annuelles de ces points en fonction du modèle de rétention « grand-père - père - fils » (GFS, Grandfather-Father-Son), par exemple.

Une fois vos stratégies de rétention définies et vos données sauvegardées, vous disposez de plusieurs options de récupération pour effectuer des restaurations de points de vos données dans le temps. Si un ransomware frappe votre entreprise, utilisez les sauvegardes pour récupérer vos données sans verser la rançon.

Contrôler l'accès aux données de sauvegarde

Il est vital d'empêcher l'accès non autorisé à vos sauvegardes et à vos réplicas. Pour ce faire, appliquez le principe du moindre privilège (PoLP, Principle of Least Privilege). Selon ce principe, vous n'accordez que le strict minimum en termes d'autorisations pour permettre aux utilisateurs de faire leur travail. Pour appliquer le principe du PoLP, vous pouvez utiliser le contrôle d'accès basé sur les rôles (RBAC, Role-Based Access Control). Le RBAC est essentiel car il offre une protection contre les employés malveillants et les erreurs humaines. Grâce au contrôle d'accès, seuls les utilisateurs autorisés et authentifiés peuvent accéder à vos données de sauvegarde.

Vérifier les capacités de récupération des sauvegardes et des réplicas

Sauvegarder vos VM n'est pas le but final en soi. L'objectif est de pouvoir restaurer les données après une attaque par ransomware. À cette fin, vérifiez régulièrement vos sauvegardes et vos réplicas en exécutant des tests de récupération. Un mécanisme de sauvegarde et de récupération testé en continu est la solution numéro un pour gérer les menaces liées à la sécurité et aux désastres. Des sauvegardes rapides et bien planifiées peuvent vous aider à conserver les versions de données dont vous avez besoin et favoriser un processus de récupération efficace.

Protection et récupération en cas d'attaque par ransomware avec NAKIVO Backup & Replication

NAKIVO Backup & Replication est une solution de protection des données pouvant être utilisée dans le cadre d'un plan d'intervention en cas d'incident et de récupération après sinistre. Cette solution offre toutes les fonctionnalités pour assurer une protection et une récupération simples et fiables en cas d'attaque par ransomware. Cette section couvre les principales fonctionnalités de la solution.

Sauvegardes natives sans agent

NAKIVO Backup & Replication fournit une sauvegarde basée sur les images et cohérente avec les applications pour les VM VMware vSphere, Microsoft Hyper-V et Nutanix AHV, les instances Amazon EC2 et les serveurs et stations de travail Windows/Linux. Grâce à la fonctionnalité App-ware Mode, les sauvegardes de données d'application dans Microsoft Exchange Server, Microsoft Active Directory et Microsoft SQL Server sont cohérentes en termes de transactions. Vous pouvez ainsi récupérer instantanément des objets et des fichiers tels que des e-mails dans Microsoft Exchange ou des utilisateurs dans Active Directory directement à partir d'un référentiel de sauvegarde compressé et déduplicé.

Pour créer des sauvegardes et des répliques cohérents de VM VMware et Hyper-V basées sur Windows, NAKIVO Backup & Replication fait appel au service VSS (Volume Shadow Copy) de Microsoft qui fonctionne dans les VM. Et si votre application ne prend pas en charge VSS ou s'exécute sous Linux ? NAKIVO Backup & Replication peut exécuter des scripts pré-gel et post-dégel personnalisés pour permettre une sauvegarde de VM cohérente avec les applications.

Sauvegarde vers des destinations multiples

NAKIVO Backup & Replication permet de mettre en pratique la règle 3-2-1 et de stocker des sauvegardes sur des supports multiples. Les options de stockage prises en charge par la solution sont les dossiers locaux, le partage CIFS, le partage NFS, le cloud (Amazon S3, Azure, Wasabi), les bandes magnétiques, ainsi que les appliances NAS et les appliances de déduplication tels que HPE StoreOnce et EMC Data Domain. La solution fournit également une fonction de copie de sauvegarde. Vous pouvez créer autant de copies de sauvegarde que nécessaire et les stocker sur différents supports pour améliorer vos chances de récupérer vos données après une attaque par ransomware.

Sauvegardes à l'abri des ransomwares

NAKIVO Backup & Replication s'intègre à la fonctionnalité S3 Object Lock pour protéger vos données de sauvegarde stockées dans Amazon S3 contre les ransomwares et autres suppressions malveillantes ou accidentelles. Pour activer S3 Object Lock, indiquez directement dans l'interface de la solution pendant combien de temps vos sauvegardes doivent rester immuables.



Une fois S3 Object Lock activé, les objets sont stockés dans le mode S3 Compliance selon le modèle WORM (write-once-read-many). Ni un administrateur ni un tiers ne peut écraser ou modifier les objets avant l'expiration de la période de rétention. De même, personne ne peut modifier ou raccourcir la période de rétention. En plus d'offrir une protection contre les ransomwares, la fonctionnalité S3 Object Lock d'Amazon permet également de préserver des données importantes à des fins de conformité.

Vérification instantanée de sauvegarde/réplica de VM

NAKIVO Backup & Replication offre une fonctionnalité automatisée de vérification instantanée des sauvegardes. À l'issue de votre tâche de sauvegarde, la solution peut procéder à un test de récupération de votre sauvegarde de VM Hyper-V ou VMware et effectuer une capture d'écran du système d'exploitation initialisé. Vous pouvez afficher les résultats de la vérification dans l'interface de la solution ou via e-mail. Vous pouvez ainsi tester vos sauvegardes Hyper-V ou VMware et vous assurer que vos sauvegardes de VM sont valides et peuvent démarrer.

Récupération granulaire

Avec la récupération granulaire, vous n'avez pas besoin d'effectuer une récupération complète pour restaurer un ou plusieurs éléments sauvegardés. Il vous suffit à la place de rechercher ou de parcourir vos sauvegardes pour trouver les objets, les fichiers ou les dossiers dont vous avez besoin. Une fois l'élément sélectionné, vous pouvez le restaurer vers la source ou vers un emplacement personnalisé, avec toutes les permissions des fichiers restaurés.

NAKIVO Backup & Replication vous permet de créer jusqu'à 4 000 points de récupération pour chaque sauvegarde, vous offrant ainsi une flexibilité de choix pour récupérer vos données. La solution fait appel au modèle « grand-père - père - fils » (GFS, Grandfather-Father-Son) et effectue une rotation quotidienne, hebdomadaire, mensuelle ou annuelle de vos points de récupération, en fonction de vos préférences.

Flash VM Boot

Si un ransomware rend vos VM principales inaccessibles, vous pouvez récupérer des VM entières grâce à la fonctionnalité Flash VM Boot. Celle-ci vous permet de démarrer les VM directement à

partir de sauvegardes compressées et dédoublées. Une fois les VM démarrées, vous pouvez les migrer vers la production pour une récupération définitive, si nécessaire. La fonctionnalité est entièrement opérationnelle et ne nécessite aucune configuration spécifique. Avec Flash VM Boot, vous pouvez restaurer une VM entière à son dernier état ou à n'importe quel point dans le temps.

La VM restaurée contient toutes les données pertinentes, y compris la configuration, le système d'exploitation, les applications, les données associées et l'état du système. La solution permet également de récupérer plusieurs VM en une seule tâche. Lorsque vous exécutez la récupération d'une VM, une nouvelle VM est créée. La VM source n'est pas restaurée à l'état précédent ni remplacée par la nouvelle VM. La fonctionnalité vous permet également d'accéder à des fichiers, des dossiers et des objets d'application sur n'importe quel système d'exploitation.

P2V Recovery

Dans les environnements physiques/virtuels mixtes, la récupération après une attaque par ransomware peut être un processus simple et rapide grâce à la récupération d'un environnement physique vers un environnement virtuel. Imaginez un scénario dans lequel il vous faut récupérer une machine physique à la suite d'une attaque par ransomware. Votre serveur source est infecté et vous n'en avez pas d'autre à utiliser pour la récupération. Dans ce cas, vous pouvez récupérer la machine physique comme une VM, sans utiliser d'utilitaires de conversion tiers. Cette tâche peut s'effectuer directement à partir de l'interface de la solution. NAKIVO Backup & Replication permet de démarrer facilement des serveurs/stations de travail Linux ou Windows physiques en tant que VM VMware vSphere. Cette fonctionnalité peut être utilisée pour les récupérations P2V temporaires ou définitives.

Réplication pour la récupération après sinistre

Les sauvegardes ne sont pas l'unique moyen de récupérer après une attaque par ransomware. Vous pouvez également utiliser NAKIVO Backup & Replication pour créer des répliques de vos charges de travail sur un site secondaire. Ainsi, vous pouvez reprendre vos opérations en basculant simplement vers les répliques de VM si votre site principal n'est plus disponible.

Avec NAKIVO Backup & Replication, vous pouvez créer et maintenir des répliques exacts de vos VM. La solution vous permet également de répliquer vos VM directement à partir de sauvegardes afin de décharger l'environnement de production et de libérer les ressources système. NAKIVO Backup & Replication offre également d'autres fonctionnalités de réplication pour simplifier le processus et assurer la récupération. Par exemple, vous pouvez utiliser la fonctionnalité d'automatisation de la récupération pour automatiser entièrement la réplication des VM Hyper-V et VMware et des instances Amazon EC2.

Orchestration et automatisation de la récupération après sinistre

Grâce à la fonctionnalité de récupération de site de NAKIVO Backup & Replication, vous disposez d'une orchestration et d'une automatisation de la récupération après sinistre de niveau entreprise. Au lieu de procéder à un basculement de VM manuel, activez la

fonctionnalité VM Failover, qui permet une récupération facile en cas d'attaque par ransomware et offre les RTO les plus stricts. Voici comment opère cette fonctionnalité :









- Répliquez vos VM vers un emplacement de basculement où vous pourrez les démarrer après une attaque par ransomware. Vous pouvez soit répliquer toutes vos VM en une seule tâche, soit utiliser plusieurs tâches pour différents groupes de VM et les exécuter selon des planifications distinctes.
- Créez une tâche unique de basculement de VM et reliez vos tâches de réplication de VM à cette tâche. Ceci fait, vous pouvez effectuer instantanément le basculement de VM.

Notez que les nouvelles VM ajoutées aux tâches de réplication sont automatiquement incluses dans la tâche de basculement. Vous pouvez même automatiser davantage la récupération après sinistre grâce à des règles de mappage de réseau. Lors du basculement, vos VM passent d'un réseau à un autre en observant des règles précédemment préconfigurées. De même, créez des règles Re-IP de VM pour changer l'adresse IP de vos répliques de VM après le basculement.

Pour empêcher l'infection de se diffuser, mettez automatiquement hors tension vos VM source avant que les répliques de VM ne soient en ligne. Vous pouvez également tester les séries complexes d'étapes d'un plan de récupération après sinistre sans perturber votre environnement de production ni exécuter de tâches de protection des données. Grâce aux tests, vous optimisez également votre plan de récupération après sinistre pour garantir un processus de récupération après sinistre sans heurs et à l'épreuve des défaillances. Ainsi, si un événement de ransomware paralyse votre site principal, vous pouvez bénéficier de temps d'arrêt minimum et une perte de données nulle.

Protection des données complète avec NAKIVO Backup & Replication

NAKIVO Backup & Replication est une solution de protection des données destinée aux environnements virtuels, physiques, cloud et SaaS. Elle permet la sauvegarde, la réplication, la récupération granulaire instantanée et la récupération après sinistre à partir d'un seul et même écran.

-  **Déploiement en moins d'une minute**
VA VMware vSphere préconfigurée, VA ou AMI Nutanix AHV ; déploiement en un clic sur ASUSTOR, QNAP, Synology, NETGEAR, FreeNAS et WD NAS ; programme d'installation Windows en un clic , programme d'installation Linux en une commande.
-  **Protégez vos données à travers les plateformes**
Sauvegarde prenant en charge les applications native, sans agent et basée sur les images pour VMware vSphere, Microsoft Hyper-V, Amazon EC2, Nutanix AHV ; serveurs et stations de travail physiques Windows/Linux ; Microsoft 365 ; Oracle Database.
-  **Simplifiez la protection des données**
Protégez automatiquement les machines qui correspondent à des règles de politique basées sur le nom des machines, les balises, la taille, l'emplacement, etc.
-  **Augmentez la vitesse de sauvegarde**
Déduplication globales des sauvegardes, compression ajustable des sauvegardes.
-  **Réduisez la taille de la sauvegarde**
Sauvegardes incrémentielles avec CBT/ RCT/CRT, transfert de données sans LAN, accélération réseau et performances jusqu'à 2 fois supérieures en cas d'installation sur un NAS.
-  **Simplifiez la gestion**
Interface simple, rapide, facile à utiliser, accessible à tout moment et de n'importe où- même à partir d'un appareil mobile.
-  **Garantissez une capacité de récupération**
Vérification instantanée des sauvegardes avec captures d'écran des VM restaurées pour les tests ; copies de sauvegarde hors site, sur bande magnétique ou vers des clouds AWS/Azure.
-  **Réduisez les temps de récupération**
Récupération instantanée des VM, des fichiers et des objets d'application (Exchange, Active Directory et SQL) ; récupération de site ; récupération P2V quasi instantanée.

À propos de NAKIVO

NAKIVO est une société basée aux États-Unis dédiée au développement de la solution ultime de sauvegarde, de protection contre les ransomwares et de reprise après sinistre pour les environnements virtuels, physiques, cloud et SaaS. NAKIVO est l'un des fournisseurs de logiciels de sauvegarde et de récupération qui connaît la croissance la plus rapide du secteur et a enregistré une croissance à deux chiffres pendant 24 trimestres consécutifs, des avis 5 étoiles de la part de la communauté en ligne et un taux de satisfaction de 98 % de la part de ses clients en matière de support. NAKIVO dispose d'un réseau comptant plus de 7 000 partenaires dans le monde. Plus de 22 000 clients dans 171 pays font confiance à NAKIVO pour la protection de leurs données, y compris de grandes entreprises comme Coca-Cola, Honda, Siemens et Cisco. En savoir plus sur www.nakivo.com