Rapport Technical Insight

Déjouer les attaques par ransomware avec le stockage primaire

Par Krista Macomber, analyste senior

Mars 2022

Evaluator Group

Pour prendre les meilleures décisions en matière de technologie

Introduction

Nous le savons tous, les attaques par ransomware continuent d'augmenter et de gagner en virulence. Evaluator Group a constaté que les clients investissent pour se défendre face à cette menace. En effet, dans notre enquête Pulse de 2021 sur les ransomware, 87 % des personnes interrogées ont indiqué qu'elles avaient l'intention de dépenser, ou prévu de dépenser, une part de leur budget dans des technologies de prévention et de protection contre les attaques par ransomware au cours des 12 prochains mois. Plus précisément, nous avons remarqué que les clients achètent des technologies de protection des données, afin de s'assurer une reprise d'activité rapide. Dans notre enquête, 56 % des personnes interrogées ont indiqué avoir dépensé de l'argent pour la protection des données au cours des 12 mois précédents en raison de l'augmentation des attaques par ransomware.

Bien qu'il soit possible, dans certains cas, de restaurer les données à partir de sauvegardes, celles-ci ne sont pas aussi infaillibles qu'on le prétend souvent. D'ailleurs, les hackers le savent bien. Si leur victime peut récupérer ses données, elle ne va pas payer la rançon. Ils ont donc modifié leur approche pour cibler l'environnement de sauvegarde. En outre, la restauration à partir de sauvegardes implique quelques compromis : il faut du temps pour localiser la dernière copie valide, la restauration est longue et il manque parfois des données dans la copie de sauvegarde si le dernier point de récupération n'est pas assez récent. Par conséquent, il est essentiel d'instaurer des mesures de protection contre les ransomware dans l'environnement de stockage primaire.

Se protéger contre les attaques par ransomware avec le stockage primaire

Compte tenu de ces menaces et des défis inhérents à la récupération des données à partir de sauvegardes, Evaluator Group conseille aux clients de mettre en place une stratégie complète de défense contre les attaques par ransomware qui englobe la détection et la protection en plus de la récupération.

Les piliers d'une bonne défense contre les ransomware

- Prévention
- Détection
- Restauration

En intégrant des mesures de défense dans le stockage primaire, il est possible d'identifier plus rapidement une tentative d'attaque par ransomware et d'accélérer le délai de restauration.

Pour déjouer une attaque par ransomware, il faut savoir en permanence qui accède aux données, comment et pourquoi. Ainsi, il est possible de détecter les utilisateurs malveillants et de les empêcher d'accéder à l'environnement. En outre, l'équipe IT peut obtenir des informations sur les interactions entre les différents éléments de l'environnement tout au long du cycle de vie des données, pour détecter les éventuelles zones à risque. Cette visibilité est assortie de mesures de contrôle d'accès strictes qui permettent de superviser les accès de chaque utilisateur à chaque composant de l'environnement IT. Le chiffrement des données et la possibilité de rendre des données ou des objets immuables (verrouillés en mode lecture et inaltérables) et indélébiles (impossibles à supprimer) sont essentiels, notamment en cas d'infiltration, car le hacker ne pourra pas prendre le contrôle des données.

La visibilité et l'analytique jouent également un rôle dans la détection des attaques par ransomware en facilitant l'identification des activités malveillantes dès qu'elles se produisent. Dans les environnements de sauvegarde, les informations sont rétroactives, elles se basent sur des modifications qui ont déjà eu lieu dans l'environnement de production et qui ont été sauvegardées. De plus, pour analyser les données, il faut d'abord les extraire du système de sauvegarde. L'analyse des systèmes de production réduit leurs performances, mais il s'agit d'un compromis raisonnable sachant que vous pourrez détecter les attaques par ransomware plus tôt qu'avec l'analyse des données de sauvegarde. L'intégration d'autres outils tels que IBM QRadar, SecureX et Splunk permet ensuite de déployer les informations obtenues dans l'environnement IT dans son ensemble.

Afin d'assurer une reprise d'activité rapide et de réduire l'impact d'une attaque par ransomware sur l'entreprise, il est important de **raccourcir le délai de restauration**, en particulier pour les applications et services de base tels qu'Active Directory. La récupération des données à partir de sauvegardes allonge le délai de restauration, notamment en cas de corruption d'un système de fichiers, car l'équipe IT doit rechercher et identifier manuellement la dernière copie de sauvegarde valide.

Utiliser le stockage NetApp pour se protéger contre les ransomware

L'architecture de NetApp suit le principe de la « sécurité axée sur les données », c'est-à-dire la protection des données actives, au repos et en transit, dans les data centers, en périphérie et dans le cloud. Dans les paragraphes qui suivent, nous allons voir ce que cela signifie en termes de capacités techniques spécifiques, sous l'angle de la protection contre les attaques par ransomware : prévention, détection et restauration.

Prévention

Pour stopper les hackers et bloquer les attaques par ransomware, NetApp utilise une architecture de sécurité « zéro confiance », plusieurs niveaux d'intelligence et de vérification, ainsi que des fonctionnalités de journalisation et d'audit. En outre, sa structure de notification d'accès aux fichiers FPolicy surveille et gère les événements d'accès aux fichiers via les protocoles d'accès SMB et NFS v3 et v4.0. Le composant FPolicy sert de couche de contrôle pour l'accès aux fichiers, aux utilisateurs et aux volumes de stockage. Il permet à l'équipe IT de bloquer certains utilisateurs ou de restreindre leurs accès, et de contrôler l'activité de lecture et d'écriture sur les systèmes de fichiers ainsi qu'au niveau du volume de stockage. FPolicy peut alimenter les outils de fournisseurs tiers, y compris les produits de gestion des informations et des événements de sécurité (SIEM) tels que Splunk, afin de fournir au personnel IT une meilleure visibilité sur les activités malveillantes dans l'ensemble de l'infrastructure. Ces fonctionnalités sont assorties d'un processus de validation des images au démarrage et lors de la mise à niveau des systèmes.

Pour renforcer la protection des données de sauvegarde, NetApp utilise des fonctions d'administration sécurisées, notamment le contrôle d'accès basé sur des rôles (RBAC) et l'authentification multifacteur (MFA). NetApp prend également en charge une structure d'API REST ouverte et offre un kit de développement logiciel (SDK) prêt à l'emploi afin que les partenaires puissent s'intégrer dans sa structure de sécurité.

NetApp exploite plusieurs technologies pour chiffrer les données au repos et à la volée, notamment :

- Le chiffrement des données au repos, facilité par :
  - NetApp Storage Encryption (NSE), qui fournit des capacités de chiffrement matériel du stockage sur disque pour les données au repos.
    - Plus précisément, NSE utilise des disques autochiffrés (SED) conformes à la norme FIPS 140-2 de niveau 2 pour chiffrer les données au repos indépendamment du réseau et du système.
  - NetApp Volume Encryption (NVE), une fonction de chiffrement logiciel pour les données au repos qui permet aux clients de se passer de disques autochiffrés.
    - NetApp Secure Purge élimine les données d'un volume NetApp Volume Encryption (NVE) en détruisant les fichiers de manière chiffrée afin qu'ils ne puissent pas être récupérés à partir de leur support de stockage physique. Ceci empêche les fuites de données et constitue un excellent mécanisme de suppression.
  - L'association de NSE et NVE pour renforcer la protection à l'aide du chiffrement d'agrégat NetApp, qui permet de partager des clés de chiffrement pour les volumes agrégés et d'appliquer la déduplication sur les volumes agrégés, afin d'améliorer l'efficacité du stockage et de la gestion.
  - NetApp CryptoMod, un module qui fournit des opérations de chiffrement pour NSE et le gestionnaire de clés intégré.
  - Le jeu d'instructions pour le chiffrement SMB Intel AES-NI (Intel AES New Instructions).
  - L'invocation d'IPsec, pour l'authentification des données, l'intégrité et le chiffrement entre deux terminaux via le réseau IP.
- La prise en charge du protocole TLS 1.2 pour le transfert de données et l'utilisation du plan de gestion, y compris pour :
  - La fonctionnalité de réplication des données NetApp SnapMirror.
  - NetApp SnapVault, qui permet la sauvegarde sur un système de stockage central secondaire des Snapshots en lecture seule issus de plusieurs systèmes.
- Le protocole CHAP (Challenge Handshake Authentication Protocol) est pris en charge pour iSCSI pour l'authentification des utilisateurs ou des hôtes réseau.
- La prise en charge du protocole KMIP (Key Management Interoperability Protocol), le protocole de communication par excellence pour la gestion des clés de chiffrement, est incluse.

NetApp crée des copies Snapshot en lecture seule et immuables, et sa fonction SnapLock répond aux exigences des clients en matière d'indélébilité. SnapLock propose deux modes de fonctionnement :

- Le mode Enterprise : le client choisit la durée du verrouillage et l'administrateur garde la main sur les paramètres de conservation.

- Le mode SnapLock Compliance : répond aux critères d'immuabilité, d'indélébilité et de conservation établis par les lois telles que la Loi HIPAA. Une fois définie, la période de conservation ne peut plus être modifiée par un utilisateur, ni même par les employés NetApp.

Pour assurer une reprise rapide de l'activité, SnapMirror peut répliquer des copies Snapshot immuables sur un autre site.

Détection

NetApp utilise des modèles d'activité de fichier de workload, des calculs d'entropie des données et un moteur d'analytique intégré et personnalisé pour identifier et bloquer les utilisateurs malintentionnés. NetApp évalue également l'entropie des données pour détecter l'exploitation malveillante des données. Plus précisément, cette fonction est intégrée dans les fonctionnalités/offres suivantes :

- L'application NetApp Active IQ pour la surveillance des opérations IT qui utilise l'IA et le ML basés sur des données de télémétrie. En matière de protection des données, Active IQ fournit aux clients des conseils/recommandations normatifs ainsi que des actions/mesures correctives automatisées pour améliorer la disponibilité et réduire les risques pour l'entreprise.
- FPolicy, une structure de notification d'accès aux fichiers pour la surveillance et la gestion des événements d'accès aux fichiers sur les protocoles d'accès SMB et NFS v3 et v4.0.
- NetApp Cloud Secure, qui s'intègre avec FPolicy pour analyser et détecter les comportements anormaux des utilisateurs, en particulier les modèles d'accès aux fichiers/données. Cette fonctionnalité permet d'identifier les ransomware et autres cyberattaques dès qu'elles se produisent et d'assurer la conformité. Lorsqu'un événement anormal est identifié, Cloud Secure déclenche automatiquement un Snapshot de stockage et bloque l'accès aux comptes utilisateur pour empêcher les fuites de données. Il s'agit d'une fonctionnalité de NetApp Cloud Insights, une solution SaaS pour la surveillance de l'infrastructure IT sur site et hors site.
- Cloud Data Sense, qui assure l'identification, le mappage et le reporting sur de nombreux systèmes de fichiers et solutions de stockage objet, sur site et hors site. Contrôlé via NetApp Cloud Manager, Cloud Data Sense applique l'IA et l'automatisation aux tâches de détection, de mappage, de classification/catégorisation et de gouvernance des données (par exemple, la suppression des données et les demandes d'accès aux données) afin d'assurer le respect des exigences de confidentialité des données.

Restauration

NetApp propose plusieurs fonctionnalités pour accélérer la reprise suite à une attaque par ransomware. Les clients peuvent effectuer des restaurations de fichiers granulaires, ce qui permet d'identifier et de restaurer rapidement des fichiers spécifiques, au lieu de récupérer, par exemple, une image entière. En outre, ils peuvent exécuter des restaurations rapides à partir de copies Snapshot locales ou distantes.

Evaluator Group a constaté que les équipes d'exploitation évoquent souvent les difficultés qu'elles rencontrent à identifier la dernière copie valide des données. Pour les aider, NetApp enrichit ses capacités d'analyse des données en établissant des partenariats avec des fournisseurs tels que Catalogic et ProLion. La technologie CryptoSpike de Catalogic identifie les utilisateurs et les fichiers infectés, et bloque l'accès aux partages de fichiers NetApp à ces utilisateurs. ProLion surveille les indicateurs de menace afin d'identifier et de stopper les utilisateurs malveillants ainsi que les attaques.

Il est important de hiérarchiser la récupération des données en fonction de leur valeur pour l'entreprise afin d'accélérer la reprise d'activité après une attaque par ransomware.
NetApp Active IQ permet au personnel IT de retrouver les volumes les plus utilisés dans l'entreprise, par exemple en recherchant l'activité de lecture et d'écriture la plus élevée. En outre, Cloud Insights fournit aux équipes IT des informations, notamment sur les données les plus fréquemment utilisées. Ces deux outils peuvent aider l'entreprise à identifier plus précisément les données les plus utiles. Avec SnapMirror, les clients peuvent ensuite effectuer des restaurations granulaires rapides, basées sur des Snapshots.

Conclusion

Il n'est pas simple de concevoir un environnement de stockage résistant aux ransomware, c'est-à-dire qui soit capable de détecter les attaques, de les déjouer et, si besoin, de restaurer les données. En plaçant l'environnement de stockage de production au centre de votre stratégie de lutte contre les ransomware, vous donnez aux équipes d'exploitation IT les outils nécessaires pour se défendre contre les attaques, et accélérer leur détection et la reprise d'activité.

Le stockage primaire de NetApp remplit de nombreux critères essentiels à l'établissement d'une stratégie anti-ransomware efficace :

- Architecture « zéro confiance » avec audit et journalisation
- Contrôle d'accès multifacette
- Chiffrement (données au repos et à la volée)
- Immuabilité, y compris la réplication de points de données immuables
- Indélébilité
- IA/ML pour la détection et le blocage des activités malveillantes
- Restauration de fichiers granulaire
- Restaurations rapides à partir de Snapshots

À propos d'Evaluator Group

Spécialisé dans la gestion des informations et le stockage des données, le cabinet d'analyse Evaluator Group Inc., propose ses services depuis plus de 20 ans. Les dirigeants et les responsables IT font appel à nous pour prendre des décisions éclairées en matière d'architecture et d'achat de systèmes capables de soutenir leurs objectifs de gestion des données. Au-delà du domaine technologique, nous définissons les exigences et avons développé une connaissance approfondie des produits ainsi que des subtilités qui dictent les stratégies efficaces à long terme.