Informe técnico

Combatir el ransomware con almacenamiento principal

Por Krista Macomber, analista sénior

Marzo de 2022

Introducción

No es ningún secreto que los ataques de ransomware no dejan de aumentar en número y que su impacto sobre las empresas es cada vez más grave. Evaluator Group ve que los clientes invierten para responder a esta amenaza. Según nuestra encuesta Ransomware Pulse Survey 2021, el 87 % de los participantes indicó que piensa gastar o presupuestar dinero para tecnologías de protección y prevención del ransomware en los próximos 12 meses. En concreto, vemos que los clientes invierten en tecnologías de protección de datos para asegurar su capacidad de recuperación. En nuestro estudio, el 56 % de los participantes indicó que había gastado dinero en protección de datos en los 12 meses anteriores debido al aumento de los ataques de ransomware.

Aunque en algunos casos puede ser posible recuperarse de un ataque mediante un backup, estos no son la póliza de seguros infalible que a veces se nos vende. Los atacantes saben que, si el cliente es capaz de recuperarse, no tiene por qué pagar el rescate, así que han modificado su estrategia para atacar el entorno de backup. Además, la recuperación desde un backup tiene sus problemas: se requiere un tiempo para localizar la última copia en buen estado conocida y luego ejecutar el proceso, y además podría dar lugar a la pérdida de datos si el punto de recuperación no es el más adecuado. Por estos motivos, la resiliencia ante el ransomware también debe afrontarse en el propio entorno de almacenamiento principal.

Afrontar la resiliencia ante el ransomware con almacenamiento principal

Especialmente al considerar estas amenazas y dificultades para la recuperación desde backups, Evaluator Group recomienda a los clientes que elaboren una completa estrategia de resiliencia que se extienda más allá de la capacidad de recuperación e incluya la posibilidad de detectar y defenderse del ataque de ransomware.

Pilares básicos de la resiliencia ante el ransomware

- Evitación
- Detección
- Recuperación

Afrontar la resiliencia con almacenamiento principal puede ayudar a identificar antes que se está produciendo un ataque de ransomware y así acelerar el tiempo de recuperación.

La prevención de los ataques de ransomware para que no lleguen a producirse pasa por saber quién accede a los datos, cómo lo hace y por qué, con el objetivo de detectar usuarios maliciosos e impedirles que accedan al entorno. Además, el departamento de tecnología puede obtener información sobre cómo interactúan los distintos elementos del entorno de tecnología a lo largo del ciclo de vida de los datos, con el fin de detectar áreas de riesgo que podrían quedar comprometidas. Esta visibilidad se complementa con fuertes medidas de control de acceso para supervisar quién tiene acceso a qué componentes del entorno de tecnología. El cifrado y la capacidad para establecer datos u objetos como inmutables (bloqueados en un modo de solo lectura, por lo que no pueden alterarse) e indelebles (bloqueados de modo que no puedan eliminarse) son importantes. De este modo, aunque un usuario malicioso logre colarse en el entorno, no puede tomar el control de los datos.

La visibilidad y el análisis también tienen su papel en la detección del ransomware, pues ayudan a identificar actividades maliciosas en el momento en que se producen. En un entorno de backup, la información es retroactiva y se basa en cambios que ya se han producido en el entorno de producción y de los que se ha hecho un backup. Por lo general, también es preciso sacar los datos del sistema de backup con el fin de analizarlos. El escaneado de los sistemas de producción afecta al rendimiento, pero puede ayudar a detectar que se está produciendo un ataque de ransomware antes que mediante el escaneado y análisis de los datos de backup. La integración con otras herramientas como IBM Qradar, SecureX y Splunk permite llevar esta información al entorno informático general.

Un **tiempo de recuperación rápido** es crucial para que la empresa vuelva a ponerse en funcionamiento lo antes posible, lo que reduce el impacto empresarial del ataque de ransomware. Esto es especialmente cierto en lo que respecta a aplicaciones y servicios básicos, como Active Directory. La recuperación desde un backup puede alargar el tiempo de recuperación, sobre todo si el sistema de archivos resulta dañado y, como resultado, el departamento informático debe buscar e identificar la última copia de backup en buen estado conocida.

Utilizar el almacenamiento de NetApp para aumentar la resiliencia ante el ransomware

Por su parte, la arquitectura de NetApp sigue la filosofía de «seguridad centrada en los datos», lo que significa que se protegen los datos en uso, en reposo y en tránsito, tanto en el núcleo como en el perímetro y el cloud. La siguiente sección explora lo que esto significa en cuanto a funcionalidades técnicas específicas y lo analiza con la mirada puesta en la resiliencia ante el ransomware: prevención, detección y recuperación.

Prevención

En un esfuerzo por prevenir que lleguen a producirse los ataques de ransomware, NetApp emplea una arquitectura de seguridad de confianza cero, múltiples niveles de inteligencia y verificación, y funcionalidades de registro y auditoría para prevenir el acceso de usuarios maliciosos. Además, su marco de notificación del acceso a archivos FPolicy supervisa y gestiona los eventos de acceso a archivos mediante los protocolos SMB y NFS v3 y v4.0. FPolicy actúa como una capa de control para el acceso a archivos, usuarios y volúmenes de almacenamiento. Permite al departamento de tecnología bloquear o restringir a determinados usuarios, además de controlar la actividad de lectura y escritura en el nivel del sistema de archivos y el volumen de almacenamiento. FPolicy puede integrarse con herramientas de terceros proveedores, por ejemplo, productos de gestión de eventos y seguridad de la información (SIEM) tales como Splunk, con el fin de proporcionar al departamento de tecnología una visibilidad adicional de la actividad maliciosa en toda la infraestructura. Estas funcionalidades se complementan con la validación de imagen de arranque y renovación.

Para prevenir aún más el acceso a los datos de backup por parte de usuarios maliciosos, NetApp emplea funciones de administración segura, como el control de acceso basado en roles (RBAC) y la autenticación multifactor (MFA). También es compatible con el marco REST Open API y ofrece un kit de desarrollo de software (SDK) «plug and play» que permite a los socios integrarse en la plataforma de seguridad de NetApp.

NetApp aplica diversas tecnologías de cifrado a los datos tanto en reposo como en tránsito. Entre ellas, se incluyen las siguientes:

- Cifrado de los datos en reposo mediante:
  - NetApp Storage Encryption (NSE), que proporciona un cifrado de almacenamiento en disco completo no disruptivo basado en hardware para los datos en reposo.
    - Más concretamente, NSE utiliza unidades de autocifrado (SED) FIPS 140-2 nivel 2 para cifrar los datos en reposo con independencia de la red y del sistema.
  - NetApp Volume Encryption (NVE), una función de cifrado para datos en reposo basada en software que permite a los clientes evitar el uso de SED.
    - NetApp Secure Purge «rasca» los datos de un volumen NetApp Volume Encryption (NVE) y los destruye criptográficamente, de modo que los archivos no puedan recuperarse desde el soporte de almacenamiento físico. De este modo se evita el derramamiento y se proporciona la funcionalidad de «derecho al borrado».
  - El uso conjunto de NSE y NVE para alimentarse el uno al otro otorga protección adicional gracias a NetApp Aggregate Encryption (NAE). NAE permite compartir las claves de cifrado de volúmenes agregados y aplicar deduplicación en dichos volúmenes, con el fin de aumentar la eficiencia del almacenamiento y la gestión.
  - El uso de NetApp CyptoMod, un módulo que proporciona operaciones criptográficas para NSE y el gestor de claves incorporado.
  - El uso del conjunto de cifrado Intel AES New Instructions (Intel AES-NI) SMB.
  - Puede invocarse la seguridad del Protocolo de Internet (IPsec), que proporciona autenticación de datos, integridad y cifrado entre dos extremos de una red IP conectados por cable.
- Compatibilidad con el protocolo TLS 1.2 para la transferencia de datos y el uso del plano de gestión con estos fines, entre otros:
  - Funcionalidad de replicación de datos de NetApp SnapMirror.
  - Creación con NetApp SnapVault de instantáneas de backup de solo lectura de varios sistemas en un sistema de almacenamiento secundario centralizado.
- Se admite Challenge Handshake Authentication Protocol (CHAP) para iSCI con el fin de autenticar usuarios y host de red.
- Se incluye compatibilidad con Key Management Interoperability Protocol (KMIP), el protocolo de comunicación de facto para la gestión de claves de cifrado.

NetApp crea instantáneas inmutables de solo lectura, mientras que su función SnapLock permite hacerlas indelebles y satisfacer así todos los requisitos. SnapLock tiene dos modos de funcionamiento:

- El modo Enterprise, que ofrece a los clientes una cierta flexibilidad en cuanto a la duración del periodo de bloqueo. El administrador puede controlar y modificar los ajustes de retención.
- El modo SnapLock Compliance, que satisface los requisitos de inmutabilidad, imposibilidad de borrado y retención de legislaciones como HIPAA. Una vez configurado, el período de retención no puede cambiarlo ningún usuario, ni siquiera los empleados de NetApp.

Para recuperar rápidamente las operaciones en línea, SnapMirror puede replicar las instantáneas inmutables en otro sitio.

Detección

NetApp utiliza patrones de actividad de archivos de carga de trabajo, cálculos de entropía de los datos y un motor de análisis integrado propio para identificar y bloquear a los usuarios maliciosos. También evalúa la entropía de los datos para comprender si se están utilizando de forma maliciosa. En concreto, esta funcionalidad está integrada en las siguientes funcionalidades y ofertas:

- Aplicación Active IQ de NetApp para la supervisión de operaciones de TI, que utiliza datos de telemetría basados en IA y aprendizaje automático. Desde el punto de vista de la protección de datos, Active IQ puede proporcionar a los clientes recomendaciones y directrices prescriptivas, además de acciones y remedios automatizados, con el fin de mejorar la disponibilidad y reducir la posición de riesgo de la organización.
- FPolicy, un marco de notificación del acceso a archivos para supervisar y gestionar los eventos de acceso mediante los protocolos SMB y NFS v3 y v4.0.
- NetApp Cloud Secure, que se integra con FPolicy para analizar y detectar comportamientos anormales de los usuarios, en concreto, patrones en el acceso a los datos y archivos. Esta funcionalidad ayuda a identificar el ransomware y otros ciberataques cuando se producen y ayuda a asegurar el cumplimiento de normativas. Cuando se identifica un evento anómalo, Cloud Secure activa automáticamente una instantánea de almacenamiento y bloquea el acceso a las cuentas de usuario para prevenir la exfiltración de datos. Es una función de NetApp Cloud Insights, una solución SaaS para la supervisión de la infraestructura tecnológica, tanto dentro como fuera de las instalaciones.
- Cloud Data Sense, que identifica, cartografía y documenta un amplio abanico de sistemas de archivos y soluciones de almacenamiento de objetos, tanto dentro como fuera de las instalaciones. Cloud Data Sense se controla mediante NetApp Cloud Manager. Aplica IA y automatización para las tareas de detección de datos, asignación, clasificación/categorización y gobernanza (p. ej., las solicitudes de borrado y acceso a los datos, lo que garantiza que los datos cumplan los requisitos de privacidad).

Recuperación

NetApp ofrece distintas funcionalidades para ayudar a los clientes a acelerar el proceso de recuperación del ransomware. Es posible realizar recuperación granular de archivos, lo que permite detectar y recuperar rápidamente archivos concretos, en vez de, por ejemplo, tener que recuperar una imagen entera. Además, las restauraciones rápidas pueden ejecutarse desde copias Snapshot locales o remotas.

La identificación de la última copia de datos en buen estado conocida es un problema que Evaluator Group recibe a menudo de las operaciones del departamento de tecnología. Para resolver esta necesidad, NetApp aumenta sus propias funcionalidades de análisis forense de los datos mediante asociaciones con proveedores como Catalogic y ProLion. La tecnología CryptoSpike de Catalogic identifica los usuarios y archivos infectados e impide a los primeros seguir accediendo a los archivos compartidos de NetApp. ProLion también supervisa los indicadores de amenaza para identificar y bloquear usuarios maliciosos y ataques.

Priorizar la recuperación de datos en función de su valor para la organización es importante de cara a poner en funcionamiento el backup de la empresa lo antes posible tras un ataque de ransomware. Active IQ de NetApp permite al departamento de informática buscar los volúmenes más utilizados de la organización, por ejemplo, aquellos con mayor actividad de lectura y escritura. Además, Cloud Insights indica cuáles son los datos a los que se accede con más frecuencia. Ambas herramientas pueden ayudar a determinar los datos más útiles de la organización. Con SnapMirror, los clientes pueden realizar recuperaciones rápidas y granulares basadas en instantáneas.

Conclusión

El diseño de un entorno de almacenamiento que mejore la resiliencia ante el ransomware (es decir, que prevenga y detecte los ataques, además de permitir la recuperación) es un proceso complejo y con múltiples aspectos. Situar el entorno de almacenamiento de producción como componente básico de la estrategia de resiliencia ayuda a prevenir y detectar con mayor velocidad los ataques, así como a recuperarse antes del ransomware.

El almacenamiento principal de NetApp cumple muchos de los requisitos importantes de la resiliencia ante el ransomware:

- Arquitectura de confianza cero, con auditoría y registro
- Control de acceso de varias facetas
- Cifrado (de los datos en reposo y en tránsito)
- Inmutabilidad, incluida la replicación de puntos de datos inmutables
- Imposibilidad de borrado
- IA/aprendizaje automático para la detección y detención de actividades maliciosas.
- Recuperación granular de archivos
- Recuperación rápida mediante instantáneas

Acerca de Evaluator Group

Evaluator Group Inc., una empresa de gestión de la información y análisis de almacenamiento de datos, lleva más de 20 años estudiando sistemas. Ejecutivos y gerentes de tecnología informática confían en nosotros para tomar decisiones informadas sobre el diseño y compra de sistemas que satisfagan sus objetivos de gestión de datos. Vamos más allá del entorno de tecnología actual, para lo cual definimos requisitos y proporcionamos información en profundidad sobre los productos y las complejidades que dictan las estrategias a largo plazo.