RESUMEN DE LA SOLUCIÓN

Pare en seco los ataques de *ransomware* con InfiniGuard® InfiniSafe®

EL DESAFÍO

El *ransomware* es un software malicioso que "secuestra" su información mediante el cifrado de sus datos.

Tradicionalmente, las empresas con un proceso de copia de seguridad eficaz podían restaurar los datos válidos de los sistemas de producción afectados. Sin embargo, el código del *ransomware* es cada vez más sofisticado y hoy en día también suele atacar las copias de seguridad. Con un ataque de *ransomware* cada 11 segundos de media en las empresas[1], ya no resulta suficiente aplicar el enfoque tradicional de restaurar la copia de seguridad en caso de un ataque.

Las empresas víctimas de estos ataques, tienen pocas opciones. Algunas optan por pagar y tienen la suerte de conseguir la clave de cifrado, pero muchas otras, incluso pagando, no tienen respuesta alguna. Algunas recurren a costosos servicios de reparación del cifrado, y otras utilizan trailers, literalmente, para recuperar los cartuchos de cinta en modo "offline", al tiempo que se preparan para un arduo proceso de recuperación.

¿El coste? IDC estima que solo los ataques de *ransomware* cuestan a las empresas 20.000 millones de USD al año. Esta cifra aumenta si se añaden las pequeñas y medianas empresas como objetivos del *ransomware*.

El *ransomware* en la actualidad

A principios de 2021, el proveedor de ciberseguridad BlackFog[2] informó de algunos de los mayores incidentes de ciberataques: un ataque al distrito escolar Victor Central School District de Nueva York cifró datos y sistemas y bloqueó a los usuarios. Todas las escuelas del distrito se vieron obligadas a cerrar. En marzo, el fabricante de ordenadores Acer fue víctima de un ataque de *ransomware* que les supuso un coste de 50 millones de dólares para evitar que los hackers publicaran datos sensibles.

Un hackeo aún más reciente es el infame ataque de *ransomware* sufrido por Colonial Pipeline, que suministra hasta el 45 % del combustible de la costa este de Estados Unidos. El ataque fue llevado a cabo por un grupo de hackers rusos y obligó a este operador de oleoductos y gasoductos a apagar rápidamente sus sistemas para contener la propagación del ataque. Aun así, las gasolineras de gran parte del país tuvieron dificultades para abastecerse de combustible.

Las empresas más pequeñas también son víctimas de estos ataques. La empresa de seguridad Infrascale estimó que el 46 % de las pequeñas empresas ha sufrido ataques de *ransomware*, y el 73 % informó que había pagado por recuperar sus datos[3]. Puede que estas peticiones de rescate no lleguen a 50 millones de USD, pero son costosas y no garantizan que los hackers cumplan su dudosa palabra.

La copia de seguridad al rescate – ¡probablemente no!

Sin duda, es mejor que su copia de seguridad sobreviva al ataque, pero los intrusos han aprendido y ahora apuntan primero a los sistemas de copia de seguridad. Los métodos tradicionales de copia de seguridad y recuperación de desastres no son aplicables a la recuperación cibernética y, por tanto, sus planes deben tener en cuenta las necesidades específicas de recuperación cibernética

Algunas de las principales características y ventajas de InfiniGuard InfiniSafe son:

- Restauraciones rápidas a escala de petabytes
- Protección de las copias de seguridad contra los ciberataques con snapshots inmutables que no se pueden eliminar, cifrar ni modificar
- Demostración del cumplimiento normativo con copias de seguridad consolidadas y snapshots inmutables
- Admisión de varias operaciones simultáneas de copia de seguridad y recuperación sin afectar al rendimiento
- Validación del entorno de recuperación
- Motores de deduplicación redundantes en una configuración activa/activa/pasiva que protegen los datos y evitan fallos en las operaciones de copia de seguridad y recuperación
- Reducción de los costes energéticos y de los gastos generales de gestión mediante la consolidación de copias de seguridad de hasta 50PB*
- Escalabilidad extrema y soporte multiprotocolo para VTL, NFS, CIFS, OST, RMAN y DB/2
- Minimización de la pérdida de ingresos y de reputación restaurando los datos de forma prácticamente instantánea y segura
- Recuperación de los datos sin comprometer su integridad, independientemente de la causa: ciberataques, fallos técnicos, desastres naturales o errores humanos

[1] Cybersecurity Ventures https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[2] BlackFog https://www.blackfog.com/the-state-of-ransomware-in-2021

INFINIDAT

Tradicionalmente, los equipos de TI aumentan la velocidad de las copias de seguridad adoptando copias sintéticas con almacenamiento deduplicado de las copias. La recuperación a gran escala en el caso de un ciberataque requiere ensamblar los datos a partir de múltiples copias de seguridad, lo que da lugar a un patrón de lectura altamente aleatorio en el almacenamiento, provocando una recuperación lenta con consecuencias graves para el negocio.

LA SOLUCIÓN: InfiniGuard con InfiniSafe

InfiniSafe se incluye en la solución de protección y recuperación de datos InfiniGuard de Infinidat. InfiniSafe se suma a la arquitectura de protección de datos de InfiniGuard, que permite una recuperación casi instantánea a una fracción del coste de otros sistema de la competencia. InfiniGuard usa InfiniBox como "backend" y añade una innovadora capa de software para optimizar la disposición de los datos y lograr así una rápida recuperación, sin sacrificar la velocidad de las copias de seguridad.

La innovadora tecnología de InfiniGuard utiliza una gran cantidad de memoria DRAM como caché principal, junto con una mayor cantidad de memoria SSD como caché secundaria. El uso de las redes neuronales y TRIE (un árbol de nodos en lugar de uno binario o el uso de tablas hash) predicen los patrones de IO, almacenando en cache los datos para acelerar el tiempo de copia y de recuperación.

En lugar de intentar recuperar datos de varios "appliances" de copia de seguridad, tipos de medios y sitios de almacenamiento, InfiniGuard consolida varias copias de seguridad en un único "appliance" fácil de gestionar que se amplía a 2 PB de capacidad utilizable y a hasta 50 PB de capacidad efectiva.

Un análisis más exhaustivo de InfiniSafe

Las capacidades nativas de InfiniGuard InfiniSafe llevan la protección y la recuperación aún más lejos. InfiniSafe protege contra los efectos de los ataques de ransomware con cuatro tecnologías fundamentales que son clave para una solución de ciberrecuperación:

1.- Snapshots inmutables

Los snapshots inmutables no se pueden borrar ni modificar. El soporte experto de Infinidat le ayudará a configurar los snapshots inmutables de su sistema para cubrir sus necesidades de ciberseguridad, incluyendo los ajustes de retención, los horarios y las políticas asociadas. No es posible que un miembro del equipo de IT modifique o elimine, bien voluntariamente o accidentalmente, un snapshot inmutable existente.

2.- Protección Air-Gap

Garantizar que los datos que se protegen están aislados de otras áreas del sistema es de suma importancia. Otras soluciones requieren que los datos se trasladen mediante copia o replicación a un sistema separado, lo que añade coste

InfiniGuard con InfiniSafe permite proteger todo el almacenamiento de copias de seguridad mediante los snapshots inmutables de Infinidat. Cada motor de deduplicación (DDE) puede restaurarse a un punto en el tiempo por separado. InfiniSafe o las pruebas de descubrimiento también pueden activarse sobre la instancia de espera.

[3] Infrascale 2020 survey https://www.infrascale.com/press-release/infrascale-survey-revealsclose-to-half-of-smbs-have-been-ransomware-attack-targets

y complejidad. La tecnología InfiniSafe lo hace localmente, ahorrando costes y eliminando la complejidad.

3.- Red forense cercada

Una red completamente privada para la validación y la recuperación

4.- Recuperación casi instantánea

Disponer de los datos lo más rápidamente posible es fundamental cuando se trata de restaurar en caso de ataque. InfiniSafe le permite recuperar todos sus datos conocidos y validados y ponerlos a disposición para su restauración en cuestión de minutos, independientemente del tamaño del repositorio de copias de seguridad, aunque se trate de petabytes.

La recuperación debe ser sistemática, rápida y verificable, con una recuperación casi instantánea desde cualquier momento del tiempo. Un entorno de pruebas aislado y fácil de usar permite a las empresas verificar los datos antes de restaurarlos. Además, este entorno admite la validación rutinaria de las copias de seguridad sin interrumpir las operaciones diarias de copia de seguridad, todo ello sin usar sistemas secundarios y sin movimiento de datos.

RESUMEN

Los ciberataques son una amenaza real y creciente, y las organizaciones no deben subestimar las consecuencias potencialmente dolorosas. Está comprobado que los ciberataques se dirigen en primer lugar a su entorno de copia de seguridad, reduciendo así su capacidad de respuesta efectiva y ganando ventaja para sus demandas. Sea más inteligente. Implemente InfiniGuard con InfiniSafe para protegerse de una gama de amenazas que van desde los ciberataques, las averías técnicas y las catástrofes hasta el mero error humano. InfiniGuard con InfiniSafe le da la confianza que necesita para recuperar rápidamente sus datos y hacer que su organización vuelva a funcionar.