WHITEPAPER

CÓMO PROTEGER SUS DATOS DEL RANSOMWARE

The Register® | Lenovo

1. RESUMEN EJECUTIVO

En la última década, el ransomware pasó de ser un problema en gran medida teórico que afectó a un número limitado de desafortunadas víctimas a un problema generalizado para la mayoría de las organizaciones y una amenaza existencial para unos pocos desdichados.

Esto se debe a que el volumen de datos que generan y retienen las organizaciones se ha disparado, impulsado en parte por nuevas cargas de trabajo como IA, Machine Learning y análisis avanzados.

Mientras tanto, la pandemia ha dado a los malos actores la oportunidad de mejorar su juego. A medida que las empresas migraron al trabajo remoto e híbrido, los equipos de seguridad extendidos han dejado a los trabajadores y sus datos más expuestos.

Este whitepaper define la escala de la amenaza del ransomware, incluida la forma en que los invasores están ampliando sus objetivos más allá de las grandes empresas y de la infraestructura crítica, poniendo cada vez más a las pequeñas y medianas organizaciones en la línea de fuego.

También explica por qué las organizaciones necesitan adoptar una estrategia de defensa en profundidad para proteger sus activos más valiosos —sus datos e información de infraestructura—, así como sus negocios en general. Eso supone no solo centrarse en la prevención, sino también en la detección y mitigación y, lo que es más importante, en la recuperación para garantizar que puedan reanudar los negocios rápidamente.

También exploraremos el papel cada vez más importante que desempeña una infraestructura de almacenamiento subyacente, especialmente cuando se trata de la recuperación, para asegurar que un ataque de ransomware se reduzca a una mera molestia en lugar de un desastre total.

2. INTRODUCCIÓN

Las raíces del ransomware se remontan a la década de 1980, cuando un individuo sin escrúpulos se alió por primera vez con la idea de un troyano que encriptaría los nombres de los archivos para un esquema de extorsión. Pero no fue hasta mediados de la década de 1990 que los investigadores concibieron agregar una clave pública criptográfica a la mezcla, lo que aumentó la posibilidad de que las víctimas perdieran sus datos de forma permanente si no pagaban.

En el 2010, el ransomware era una amenaza viable, aunque el impacto en el mundo real quizá se haya visto eclipsado por los titulares hiperbólicos. Sin embargo, en los últimos años se ha visto un aumento constante en el impacto financiero de las pandillas de ransomware, impulsado en parte por el aumento de las pandillas de Ransomware-as-a-Service (RaaS) y, en parte, porque las criptomonedas han facilitado la recolección y el transporte de los rescates.

El ransomware es un problema para todos, no solo para las grandes empresas o para los operadores de infraestructuras críticas.

Como resultado, se ha incrementado la actividad de las pandillas de ransomware y los ataques de alto perfil, como los que sufrieron Colonial Pipeline y JBS USA en el 2021.

Todo esto contribuye a que el ransomware se convierta no solo en una preocupación técnica o comercial, sino también en una preocupación de seguridad nacional.

La Casa Blanca señala que las víctimas pagaron US$ 400 millones en rescates de ataques de ransomware en todo el mundo en el 2020, con US$ 81 millones en el primer trimestre de 2021[1]. El costo medio del rescate en el 2021 fue de US$ 170.404, según el informe Sophos State of Ransomware 2021. Pero el costo total de remediar un ataque ha aumentado de un promedio de US$ 761.106 en el 2020 a US$ 1,85 millones en el 2021. Esto se debe al tiempo de inactividad comercial, a la pérdida de pedidos y a los costos operativos.

Una investigación realizada por el gigante de seguros AIG predijo US$ 20.000 millones en costos de daños por ransomware para el 2021, en comparación con US$ 325 millones para el 2015. Según AIG, se espera que los costos globales totales de los daños causados por el ciberdelito alcancen los US$ 10,5 billones para el 2025. En los casos en que los datos son extraídos por hackers, AIG informó que los costos de rescate y extorsión se duplicaron[2].

AIG también señaló que las interrupciones de la red debido a los ataques de ransomware son cada vez más largas, con un plazo típico de siete a diez días. Y si bien los pedidos perdidos a corto plazo son un dolor de cabeza obvio, ¿cómo se calcula el impacto a largo plazo en la confianza del cliente? Asimismo, ¿cuál es el impacto en proveedores, inversionistas y otras partes interesadas?

El ransomware es un problema para todos, no solo para las grandes empresas o para los operadores de infraestructuras críticas. AIG declaró que ha visto un aumento del 150% en la frecuencia de quejas de ransomware y extorsión desde el 2018, y estas provienen de “empresas de todos los tamaños... en todo tipo de industrias”.

Un consejo conjunto de funcionarios de las autoridades de Estados Unidos y el Centro Nacional de Seguridad Cibernética del Reino Unido dijo, a principios de este año, que los atacantes se estaban “alejando de la ‘caza mayor’ en los Estados Unidos” y acercándose a organizaciones medianas. Sin embargo, la Agencia Europea para el escenario de amenazas a la ciberseguridad más reciente clasificó al ransomware como “la principal amenaza” para el momento.

NOTAS AL PIE DE PÁGINA

1. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

2. https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-ransomware-global.pdf

Por eso es importante comprender la amenaza, reconocer que cualquiera podría ser una víctima y asegurarse de que los sistemas estén preparados para detectar ransomware e implementar una estrategia de respuesta en caso de un ataque a sus defensas.

3. ¿HA SUFRIDO UN ATAQUE DE RANSOMWARE? ¿CUÁL ES EL MEJOR RESULTADO QUE PUEDE ESPERAR?

El ransomware es una amenaza omnipresente y continua, y puede parecer tentador adoptar una mentalidad de búnker como respuesta, confiando en un perímetro de fortaleza y vigilancia constante para mantener a los malos actores fuera de sus sistemas.

Pero esto es difícil de sostener en el entorno tecnológico actual. Pocos especialistas creen que el enfoque perimetral tradicional es suficiente, porque la estrategia de los invasores de ransomware es ingresar silenciosamente en sus sistemas y moverse lateralmente hasta que encuentran lo que buscan.

Los equipos de tecnología necesitan detección y escaneo automatizados para que, si los intrusos superan las defensas externas, puedan desenmascararlos y detenerlos antes de que dañen o filtren datos

Un mejor enfoque es adoptar la defensa en profundidad, como recomiendan agencias gubernamentales como el NCSC3 del Reino Unido y la Agencia de Infraestructura de Seguridad y Ciberseguridad de Estados Unidos.

Esto significa que las organizaciones deben practicar la "higiene" de seguridad básica para prevenir ataques en primer lugar. Lo que incluye la corrección y la actualización de sistemas y aplicaciones para minimizar las vulnerabilidades; educar a los usuarios sobre el phishing y otras amenazas; y requerir otros tipo de defensas como la autenticación multifactor, contraseñas fuertes, etc.

Pero la lucha contra el ransomware no termina ahí. Algunos ataques pasarán, y aquí es donde entran en juego la detección y la mitigación. Los equipos de tecnología necesitan escaneo y detección automatizados, de modo que si los intrusos superan las defensas externas, puedan ser desenmascarados y detenidos antes de dañar o filtrar datos. Y deben considerar acciones a nivel de red, como segmentación, cifrado de punta a punta y privilegios mínimos.

Y, por supuesto, necesitan aumentar su enfoque en la remediación y recuperación. La detección contará poco si la empresa está fuera de línea y no puede hacer negocios durante horas, días o más. Las estrategias de recuperación deben implementarse y probarse mucho antes de cualquier ataque, con el equipo entrenado exactamente en lo que tiene que hacer.

¿QUÉ DATOS CORREN MAYOR RIESGO?

El primer paso es analizar las principales fuentes de datos y sus riesgos asociados. ¿Qué impacto tendría perder el acceso a un cierto almacenamiento de datos en la capacidad de la organización para hacer negocios?

Grandes conjuntos de datos históricos pueden ser esenciales para entrenar algoritmos de Machine Learning, pero puede que no

3. https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

4. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

sea inmediatamente necesario hacer una copia de seguridad de estos datos y ejecutarla justo después de un ataque.

Por otra parte, reanudar los negocios puede requerir una cantidad de datos relativamente pequeña en el primer ejemplo: los líderes necesitan saber exactamente qué es esto. Por ejemplo, el primer pensamiento de una empresa financiera podría ser garantizar que sus registros de transacciones estén seguros. A su vez, una empresa de fabricación puede querer que sus datos de PLM (Product Lifecycle Management) sean prioridad en cualquier restauración.

Y un ataque puede tener un impacto limitado si se detecta a tiempo. Las empresas necesitan herramientas que les permitan identificar rápidamente el radio de explosión, para restaurar solo los archivos que realmente se necesitan.

¿CÓMO AFECTA ESTO A SU RECUPERACIÓN?

Los enfoques de copia de seguridad tradicionales, normalmente con cinta como destino final, se centraban en producir un registro completo de todos los datos de la empresa, que se realizaría fuera del sitio. Si bien es integral, este enfoque puede ser difícil de manejar para una restauración de negocios rápida.

La creación de estas copias de seguridad es una tarea que requiere mucho tiempo y puede interferir en las cargas de trabajo. Peor aún, puede llevar días o semanas realizar una restauración.

Comprender la importancia de las fuentes de datos específicos significa que la organización puede pensar con qué rapidez desea restaurar sus datos y qué datos —si los hay—, puede permitirse perder. Puede que no sea necesario tener estos datos históricos para funcionar de inmediato. Para los datos históricos con fines de cumplimiento, los enfoques de copia de seguridad tradicionales pueden ser aceptables, incluso si la recuperación se mide en semanas.

$81m Pagos de ransomware globalmente en el primer trimestre del 2020, La Casa Blanca.

$170k Costo medio de ransomware en el 2021, Sophos.

$1.85m Costo medio de remediar un ataque en el 2021, Sophos.

$20bn Costos de ransomware previstos en el 2021, AIG.

$10.5tn Costos globales totales de daños por ciberdelitos para el 2025, AIG.

Pero si se pierden los datos de producción, se afectará la capacidad de la organización para hacer negocios ahora. La víctima querrá recuperar sus datos minutos o incluso segundos antes de la interrupción.

SNAPSHOTTING

La respuesta al dilema de copia de seguridad/ restauración es el snapshotting. Un snapshotting captura el estado del sistema de archivos en el momento en que se obtiene, creando un volumen de imagen de solo lectura. La grabación de snapshots subsiguientes solo cambia los snapshots anteriores.

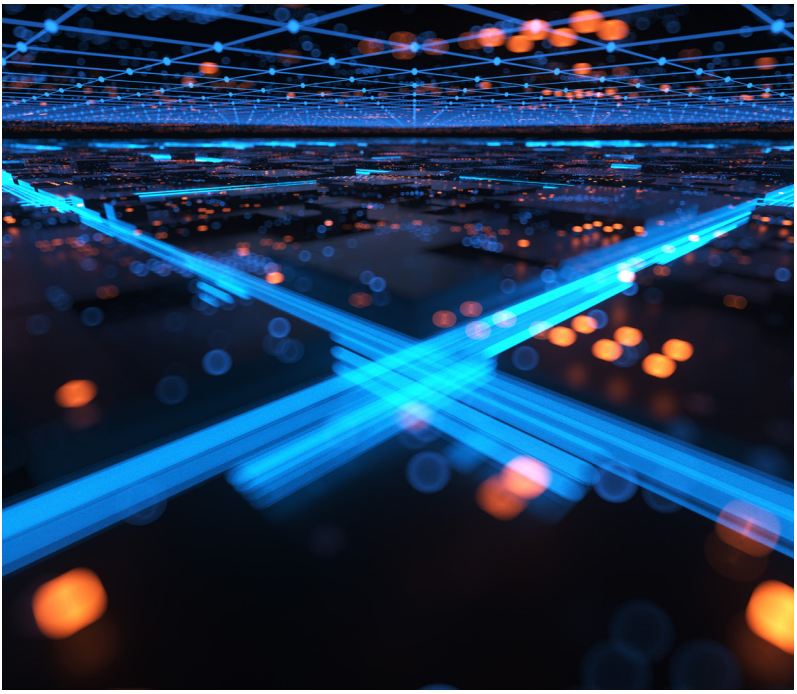
Esto proporciona la base para un registro inmutable de datos en varios momentos, lo que permite a los administradores guardar versiones anteriores en el cofre antes de un incidente, como un ransomware. También permite la recuperación no solo de volúmenes completos, sino también de “LUNS” o archivos individuales.

Es importante entender que no todos los snapshots se crean iguales. El snapshot en sí mismo puede ser un desafío de gestión de datos, con organizaciones que potencialmente buscan hacer 100s o 1000s snapshots al día. En algunos sistemas, el snapshot se añade de manera efectiva y se agrega sobre la estructura de la base del bloque. Es poco probable que sea eficiente con relación al tiempo o espacio con snapshots integrados en el sistema operativo.

Del mismo modo, los clientes deben considerar la forma en que la capacidad de snapshotting y su infraestructura de datos se integran con otras partes de su pila de copia de seguridad y recuperación, como Veeam, Veritas o Commvault. Esto podría implicar volver a examinar las opciones de copia de seguridad y recuperación ante al aumento del ransomware, pero eso no significa necesariamente que las inversiones y asociaciones existentes deban desperdiciarse.

¿Y EL AIR GAPPING?

El Air Gapping (espacio de aire) ha sido una parte esencial de las estrategias de copia de seguridad y recuperación. La regla tradicional era 3-2-1, lo que significa tres copias de los datos, en dos medios diferentes, con una copia guardada fuera de la oficina.



Pero ¿qué significa esto en el mundo moderno? Los medios separados físicamente y sin conexión a la red mantenidos fuera del sitio obviamente serán inaccesibles para los invasores. Pero, como no se puede monitorear, tampoco permiten que los profesionales de datos garanticen que los sistemas de interés de una organización se vuelvan a instalar y que estén funcionando en cuestión de minutos.

Entonces querrán considerar lo que constituye un "espacio de aire virtual". Las copias inmutables en el lugar serán parte de ello: si un invasor alcanza los datos, no será capaz de cambiarlos, conservando la capacidad de restaurarlos instantáneamente.

La capacidad off-premise en forma de copias inmutables mantenidas en una nube privada, pública o híbrida aportará más seguridad y tranquilidad a sus datos. Una vez más, aquí entra en juego la capacidad de una plataforma para integrarse con otros servicios.

LOS ATACANTES SE PREOCUPARON POR SUS DATOS SUS SISTEMAS DE PROTECCIÓN TAMBIÉN

A lo largo de este proceso, los equipos de tecnología deben tener en cuenta cuál es su objetivo final. En la gran mayoría de los casos, será volver a funcionar en minutos, sin perder negocios, sin perder datos y sin pagar el rescate.

Los atacantes también lo saben. Son conocidos por analizar la infraestructura de datos de sus víctimas, identificar posibles deficiencias en los procedimientos de recuperación y definir sus exigencias de rescate en consecuencia.

Si una pandilla de ransomware puede estar segura de que una organización confía en una cinta de copia de seguridad separada físicamente, sabrá que la perspectiva de pagar un rescate considerable puede ser más palpable que iniciar un proceso de restauración de datos que llevará días o semanas, y que la pandilla puede no tener éxito. Y si encuentran el camino hacia una copia de seguridad conectada, podrás garantizar que la tirarán a la basura antes de la posibilidad de que la detección bloquee los datos de producción, garantizando virtualmente un pago aún mayor.

4. EL ALMACENAMIENTO PRIMARIO DEBE JUGAR EN SU DEFENSA EN UNA ESTRATEGIA DE PROFUNDIDAD

El destino final de un invasor de ransomware es la infraestructura de almacenamiento local de la organización. Si esta no ofrece el rendimiento o los recursos necesarios para respaldar su estrategia de defensa en profundidad, incluido el snapshot y las herramientas de copia de seguridad apropiadas, así como la capacidad de restauración rápida, todas sus otras precauciones podrán resultar inútiles.

La serie DM de matrices all-flash de Lenovo abarca el nivel básico para soluciones NVMe de última generación. El galardonado CRN DM5100F All-Flash Array, en particular, es similar a los bloques de construcción de plástico en la medida en que ofrece flexibilidad para que las empresas comiencen pequeñas y desarrollen la capacidad para satisfacer la mayoría de las necesidades. Este proporciona un camino desde una única solución SAN para escalar hasta un borde unificado para la plataforma en la nube con recursos de clase empresarial. Un solo dispositivo se escala hasta 88 PB de capacidad bruta, con hasta 12 dispositivos en un solo clúster[5].

La serie DM brinda a las organizaciones de todos los tamaños acceso a la ordenación de resiliencia de datos y gestión que antes eran exclusivos para preservar los sistemas empresariales de alta gama.

SNAPSHOTTING EN SU CORAZÓN

La serie DM es alimentada por el sistema operativo ONTAP, que tiene la capacidad de snapshotting en su corazón. Como hemos visto, algunos sistemas brindan la capacidad de snapshotting como complemento, lo que tiene implicaciones para la eficiencia del espacio, la facilidad de gestión e integración con otros sistemas de respaldo y tecnologías y servicios de recuperación.

La capacidad de snapshotting de la serie DM admite hasta 1023 snapshots por volumen. Los snapshots son de solo lectura y brindan protección contra la corrupción por un ataque de ransomware. Un snapshot tarda menos de un segundo en crearse y en proporcionar la base para restauraciones instantáneas con matrices basadas en flash, ya sea en el caso de una eliminación accidental, ya sea en el caso de un ataque de ransomware completo. Las restauraciones pueden ser en archivo, LUN o a nivel de volumen completo. Obviamente, esta es una opción más rápida que una restauración o copia de seguridad completa usando una arquitectura tradicional.

Los snapshots se pueden programar, pero también pueden ser activados por el propio sistema host integrado con los recursos de seguridad.

La serie DM brinda a las organizaciones de todos los tamaños acceso al tipo de resiliencia y gestión de datos que antes eran exclusivos para preservar los sistemas empresariales de alta gama.

INTEGRACIÓN

La serie DM de Lenovo ofrece integración con Veeam, Veritas, Commvault y otros proveedores, que ofrecen snapshotting y copia de seguridad para VMs. Así, los administradores pueden gestionar su protección de datos y copias de seguridad para diversos tipos de datos y aplicaciones en una sola plataforma. La serie DM tiene soluciones basadas en socios para la detección de ransomware integrada adicional y

5. https://www.lenovoxperience.com/newsDetail/283yi044hzgcdv7snkrmmx9okesnwqxuzayrlke1e8sv4ubs

protección como CryptoSpike de ProLion, que utiliza IA para monitorear el comportamiento del sistema de archivos y bloquear firmas de ransomware y tipos de archivos conocidos. Brinda a los administradores la capacidad de rastrear el archivo "entropía" y los cambios, alertándolos sobre actividades sospechosas que podrían ser precursoras de un intento de ransomware.

Pocas organizaciones existen como una isla. La serie DM tiene integraciones con proveedores clave de nube empresarial, incluidos AWS, Microsoft, Google e IBM, lo que permite a los clientes migrar y replicar capas de datos en múltiples nubes, proporcionando el espacio de aire necesario para garantizar una protección completa contra los invasores cibernéticos.

SIEMPRE ACTUALIZADO

La serie DM está disponible bajo licencia del programa Lenovo TruScale Infinite Storage. Esto significa que la infraestructura se puede comprar sobre la base de OPEX, lo que proporciona una mayor rentabilidad y un beneficio inmediato para la seguridad operativa.

El programa incluye verificaciones periódicas del estado de salud y garantiza que las actualizaciones y los parches se apliquen automáticamente para que su almacenamiento cuente con la seguridad más reciente y las actualizaciones para brindar la protección más actualizada.

Con TruScale Infinite Storage, la infraestructura de almacenamiento local se implementa con la garantía de actualizaciones de tecnología que son transparentes para las operaciones del cliente y eliminan las migraciones de datos que consumen mucho tiempo. De esa forma, las organizaciones pueden concentrarse en gestionar sus datos con la última tecnología y evitar las limitaciones del hardware antiguo y los riesgos de seguridad asociados.

5. CONCLUSIÓN

El ransomware es un peligro claro y presente, y la mayoría de las organizaciones son conscientes de las repercusiones de que un invasor que se apodere con éxito del control de sus datos.

Con los atacantes yendo más allá de la "caza mayor", las organizaciones medianas deben comprender que también están en la línea de fuego.

Pueden pensar que las empresas y organizaciones de primer nivel luchan por contener la ola de ransomware y recuperarse mientras los invasores avanzan: en ese sentido, ¿qué esperanza hay para ellos? Pueden imaginar que aquellas simplemente no tienen los recursos para detectar y mitigar las amenazas.

Pero pueden estar equivocados. Ellas pueden garantizar seguir las mejores prácticas de prevención, detección y mitigación y recuperación. Pueden tener una idea clara de cuáles son los datos más críticos para ellas y estar seguros de que comprenden las funciones específicas de sus datos y cómo funcionan las infraestructuras para protegerlas de los ataques.

Al combinar las prácticas correctas, la infraestructura de almacenamiento y las herramientas apropiadas, pueden minimizar las posibilidades de ser atacadas en primer lugar, maximizar las posibilidades de volver a operar rápidamente, y eliminar la necesidad de negociar un "rescate" como un costo de hacer negocios.

6. ACERCA DE LENOVO

Lenovo Infrastructure Solutions Group (ISG) es un proveedor de soluciones de infraestructura más inteligentes para organizaciones de todos los tamaños. Nuestra tecnología e insights fortalecen el corazón de los Data-Centered del comercio minorista más inteligente, de la fabricación más inteligente, de las ciudades más inteligentes, de la salud más inteligente, de las finanzas más inteligentes y mucho más. Por medio de la computación de borde y nube, el analytics, la inteligencia artificial y la Infraestructura como Servicio por medio de TruScale, ofrecemos tecnologías más inteligentes para todos. Somos el único proveedor de data center con producción de punta a punta. Contamos con toda nuestra cadena de suministro para todo lo que construimos, para brindar un nivel de seguridad y perfección que nadie más puede ofrecer en cualquier lugar del mundo.