Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

El papel del almacenamiento en el direccionamiento de los desafíos de garantizar la resiliencia cibernética

Por Scott Sinclair, director de la práctica ESG y analista senior y Monya Keane, analista de Investigación Senior ESG

Enero 2022

Este White Paper de ESG fue realizado por IBM y distribuido con la licencia de TechTarget, Inc.

Contenidos

Resumen Ejecutivo

El papel de los datos como un activo comercial transformador continúa creciendo. Gracias a las crecientes inversiones en desarrollo de aplicaciones, prácticas modernas de DevOps, y el aumento de las demandas de inteligencia comercial, análisis y aprendizaje automático, casi todas las empresas están acelerando la creación y el uso de datos. También, se están ampliando la cantidad de lugares que aprovechan los datos. Esta proliferación de datos combinada con la creciente presión para acelerar las operaciones ha llevado a un aumento en la complejidad tanto de la infraestructura de TI como de las operaciones de TI.

Dichos factores ponen a las organizaciones y sus infraestructuras en gran riesgo de sufrir ataques maliciosos, errores humanos y comportamiento negligente. Desafortunadamente, las estrategias heredadas no pueden garantizar adecuadamente que las operaciones comerciales continúen durante y después de este tipo de incidentes. Las empresas pueden tratar de entrelazar capacidades en un intento de prevenir ataques y otras infracciones; no obstante, las brechas funcionales, la integración deficiente y la complejidad de la administración hacen que cumplir los objetivos de seguridad sea difícil y requiera mucho tiempo.

Cambiar la mentalidad organizacional de la prevención a la preparación de incidentes, por ejemplo, implementar soluciones de almacenamiento con resistencia cibernética incorporada, es clave para proteger los activos de datos críticos y poder responder y recuperarse rápidamente tanto del ransomware como de otros ataques cibernéticos.

Introducción

TI se enfrenta a nuevos retos. Casi la mitad (46 %) de los encuestados de ESG dicen que la TI es más compleja hoy que hace dos años. Este aumento en la complejidad puede ser el resultado de iniciativas de transformación digital en curso (citadas por el 29 %), mayores volúmenes de datos (35 %), la rápida evolución del panorama de la seguridad cibernética (37 %) y/o esfuerzos para adherirse a la nueva norma de seguridad de datos. y normas de privacidad (32%).[1]

Simultáneamente, las organizaciones luchan por abordar una escasez problemática de habilidades críticas de TI. De hecho, el 48 % de las organizaciones encuestadas informan que no tienen suficientes especialistas en seguridad cibernética; fue el área de escasez citada con más frecuencia. Además, estas organizaciones están lidiando con la expansión de aplicaciones, dispositivos y trabajadores remotos/móviles, que están aumentando el tamaño y el alcance del perímetro de seguridad que TI tiene la tarea de proteger.[2]

Dada la complejidad de la TI moderna, la proliferación de datos y las amenazas de ciberataques en constante crecimiento, los equipos de TI a menudo tienen dificultades para mantener el ritmo. Tratar de abordar la complejidad solo con el personal interno es una batalla perdida. El éxito requiere modernizar la propia infraestructura subyacente. Sin embargo, al hacerlo, los encargados de tomar decisiones de TI deben buscar tecnologías que no solo satisfagan las necesidades de las aplicaciones o simplifiquen las operaciones. Alcanzar el verdadero éxito significa encontrar tecnología que pueda lograr esos objetivos y también mejorar la postura de resiliencia cibernética del entorno de la aplicación.

El creciente riesgo de las amenazas de ataques cibernéticos y de Ransomware

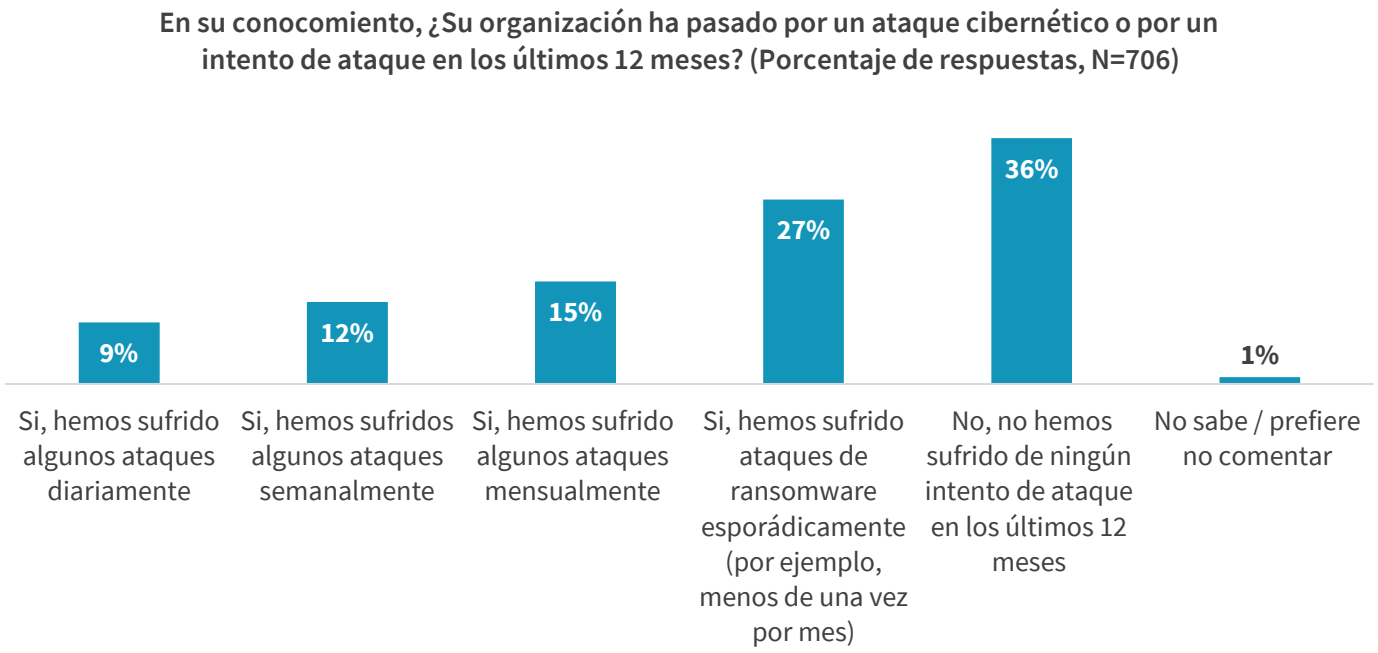
Las organizaciones se enfrentan a amenazas cibernéticas cada vez mayores, probablemente impulsadas por los crecientes incentivos financieros para los criminales cibernéticos. Por ejemplo, las quejas del público estadounidense en 2020 al Centro de Quejas de Delitos en Internet (IC3) del FBI aumentaron un 69 % desde 2019, con pérdidas reportadas que superan los $4100 millones. Además, en los últimos cinco años, el IC3 reporta pérdidas totales combinadas de $13,300

[1] Fuente: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, Novembro 2021.
[2] Ibid.

millones. A partir del cuarto trimestre de 2020 en los EE. UU., la duración promedio de la interrupción después de los ataques de ransomware en las empresas fue de 21 días. Claramente, el impacto negativo del ransomware en las operaciones comerciales es significativo

Existe una fuerte correlación entre la complejidad de las herramientas de TI y la vulnerabilidad de los ataques cibernéticos. A medida que la tecnología se vuelve más compleja, aumentará la frecuencia de ataques cibernéticos y tendrán un costo más alto.

Figura 1. Sesenta y tres por ciento de los participantes sufrieron un ataque de Ransomware en los últimos 12 meses



Fuente: ESG, a division of TechTarget, Inc.

El ransomware es una amenaza omnipresente que ataca el activo más valioso de una empresa: sus datos. El IC3 identificó 2474 incidentes de ransomware informados en 2020, y ESG descubrió que el 63 % de las organizaciones que participaron en el estudio sufrieron ataques de ransomware el año pasado. De hecho, el 9 % sufrió de ataques de ransomware diariamente (consulte la Figura 1).[3]

La protección contra ransomware requiere una estrategia tecnológica que se expanda más allá del ámbito de la seguridad cibernética tradicional; también, se deben aprovechar los avances en el almacenamiento y la protección de datos.

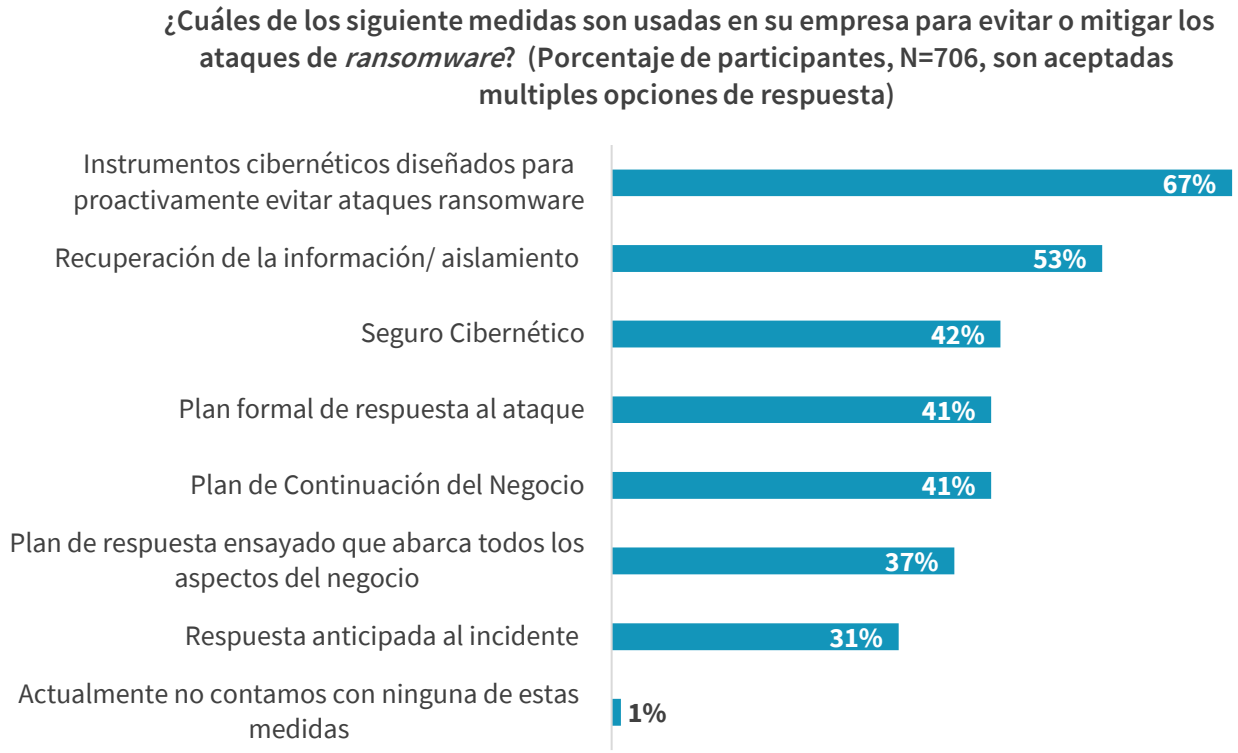
El papel del almacenamiento de datos en la resiliencia cibernética

Los sistemas de almacenamiento y los administradores de almacenamiento juegan un papel importante en la protección contra el ransomware. Cuando ESG preguntó a los responsables por la toma de decisiones de TI qué medidas habían

[3] Fuente: Resultados Completos del Estudio ESG, *2022 Technology Spending Intentions Survey*, November 2021.

implementadas sus organizaciones para combatir o mitigar los ataques de ransomware, el 67 % de los encuestados informó que utiliza herramientas cibernéticas para evitar el ransomware de forma proactiva, y el 53 % identificó capacidades de recuperación de datos como aislamiento (consulte la Figura 2).)[4] Esas dos respuestas comúnmente identificadas resaltan la importancia no solo de implementar medidas para evitar un ataque, sino también de invertir en soluciones para garantizar que la empresa esté preparada para recuperarse cuando inevitablemente ocurra un ataque. Es importante evitar simplemente configurar políticas para combatir o mitigar el ransomware y luego detenerse. Este enfoque "parcial" crea una falsa sensación de seguridad porque, si bien se hace un esfuerzo para mitigar los ataques, en realidad se hace poco o ningún esfuerzo para establecer un plan efectivo de recuperación de datos antes de que sea necesario.

Figure 2. Medidas comunes para combatir o mitigar los ataques de Ransomware



Fuente: ESG, a division of TechTarget, Inc.

Es importante recordar que luchar contra un ataque es bastante diferente de la recuperación de datos tradicional. Por lo general, las organizaciones casi siempre desean recuperar sus datos utilizando la copia más reciente. Sin embargo, con el ransomware, TI normalmente no sabe qué copia es "útil"; por lo tanto, la recuperación suele ser más riesgosa y puede llevar mucho más tiempo. Algunos ataques de ransomware no solo se dirigen a los datos, sino también a la propia infraestructura de copia de seguridad. Esta es la razón por la cual las capacidades de almacenamiento avanzadas son fundamentales para una recuperación efectiva de un ataque de ransomware.

La adopción de las medidas identificadas en la Figura 2 es inteligente y debe aumentar, las organizaciones deben comprender que ninguna defensa única es 100 % efectiva para la recuperación de un ataque ransomware. Si bien es importante considerar herramientas que se especialicen en identificar y evitar ransomware, así como en recuperar datos,

[4] Ibid.

eso es solo parte del esfuerzo. Incluso con la mejor defensa, es posible que un ataque pase. Las organizaciones deben prepararse para esa eventualidad y evaluar cómo pueden minimizar el impacto comercial al recuperarse lo más rápido posible. Para minimizar la exposición general al ransomware, las organizaciones deben buscar formas de acelerar la rapidez con la que pueden identificar los ataques, la rapidez con la que pueden mitigar cualquier daño y la rapidez con la que pueden recuperarse con una copia en buen estado.

Aquí es donde entran en escena las fuertes estrategias de resiliencia cibernética, teniendo en cuenta todos los componentes de manejo de datos, es decir, hardware, software, personas y procesos. Al desarrollar una postura de resiliencia cibernética, las organizaciones deberían dejar de preguntarse "¿Cómo protegemos?" y comenzar a preguntarse “Si nos ataca un ransomware, ¿Qué tan rápido podemos recuperarnos? ¿Qué tan rápido puede nuestro negocio volver a la normalidad?”

Almacenamiento de Datos y Protección de Datos: Saber dónde concentrarse para reducir los riesgos derivados de un ataque Ransomware

Ransomware recovery is a form of disaster recovery, but the effects of ransomware are quite different from those of a fire or a flood. After all, you can generally tell when a fire is fully extinguished. Ransomware is more like a hidden spark inside a wall that could potentially reignite at any time. Storage admins need to focus on certain areas to help reduce the risks associated with ransomware. Because speed is essential, they should determine how quickly their organization can:

La recuperación de un ataque de ransomware es una forma de recuperación ante desastres, pero los efectos del ransomware son muy diferentes a los de un incendio o una inundación. Después de todo, generalmente se puede saber cuándo un incendio se ha extinguido por completo. El ransomware es más como una chispa oculta dentro de una pared que podría volver a encenderse en cualquier momento. Los administradores de almacenamiento deben concentrarse en ciertas áreas para ayudar a reducir los riesgos asociados con el ransomware. Debido a que la velocidad es esencial, deben determinar qué tan rápido la organización puede:

- Identificar una amenaza.
- Medir los daños causados.
- Contener el daño identificando una copia segura, recuperándose usando esta copia y restaurando las operaciones.

Adoptar un enfoque de "esto no nos pasará" es, en el mejor de los casos, una postura arriesgada. Las organizaciones deben ser proactivas e implementar una solución efectiva de protección y almacenamiento de datos, antes de que realmente la necesiten.

Cambiando de seguridad cibernética a resiliencia cibernética con IBM

Con su amplia experiencia en ciberseguridad y gestión de riesgos, IBM es un líder reconocido en resiliencia cibernética y ofrece un conjunto completo de soluciones avanzadas de almacenamiento y protección de datos, que incluyen:

- IBM FlashSystem, IBM Cloud Object Storage, y IBM Spectrum Scale,. soluciones de almacenamiento básicas que vienen con funciones de encriptación e inalterabilidad de datos.
- IBM Tape Storage, que también admite la inalterabilidad y criptógrafa los datos, así como brinda protección por medio del aislamiento.

- IBM Spectrum Copy Data Management el software gestiona y protege copias de datos.
- IBM Spectrum Protect Suite para protección adicional. El almacenamiento definido por software de Spectrum Protect puede colocar datos en flash, disco, almacenamiento de objetos y cinta física o virtual. Después, detecta la actividad de malware y ransomware al identificar grandes desviaciones de los patrones de acceso normales.
- QRadar y Storage Insights Las soluciones ayudan a acelerar la detección de amenazas potenciales utilizando capacidades optimizadas de IA.

Resiliencia cibernética con IBM Cyber Vault

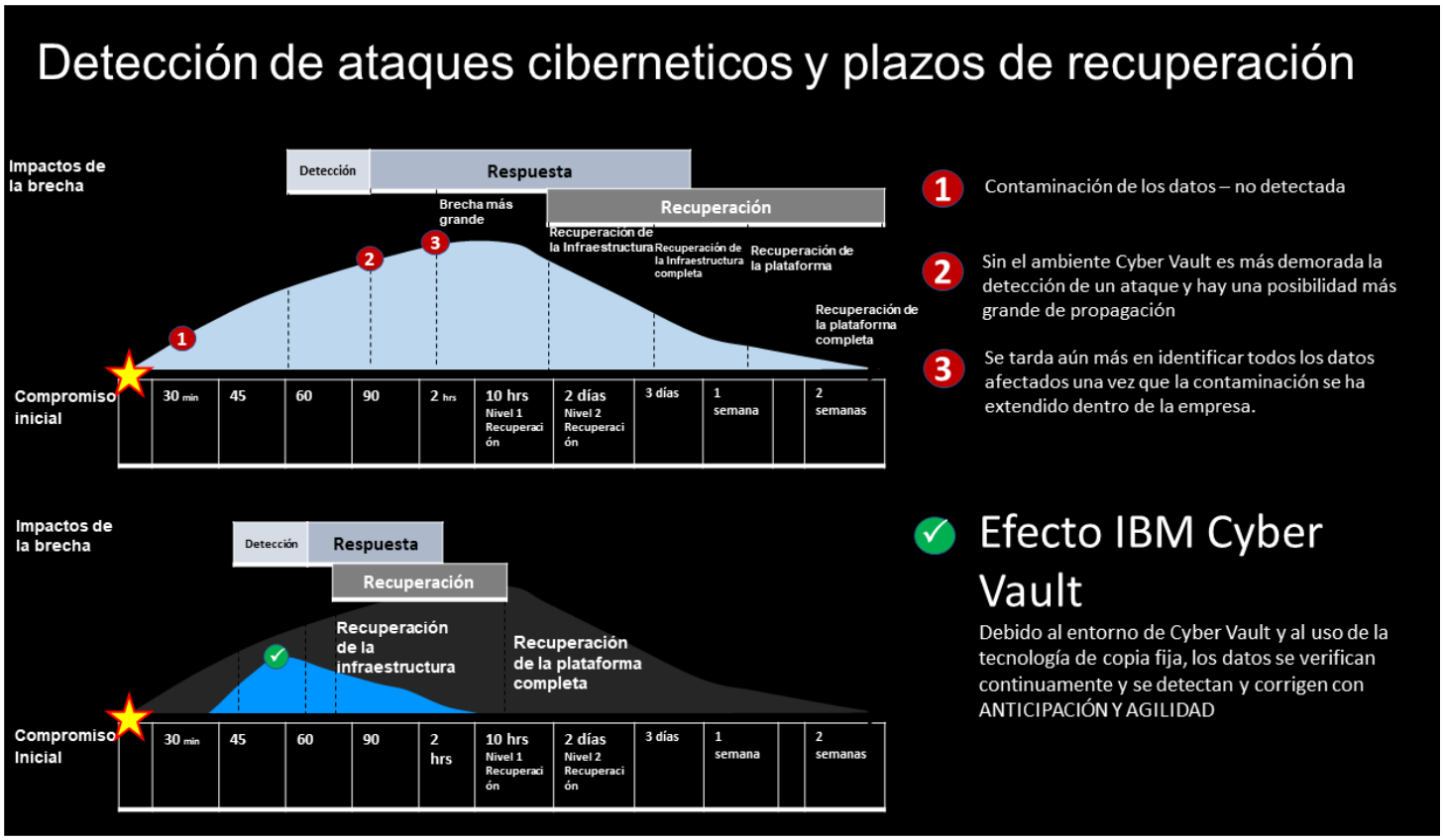
Es difícil exagerar el papel del almacenamiento en la protección contra el ransomware. El software de almacenamiento está viendo los cambios realizados en los datos primarios, y debido a que está viendo esos cambios, está en una excelente posición para identificar cuándo comienza un ataque. Es la tecnología la que también toma y protege las copias secundarias, lo que hace que el almacenamiento sea de vital importancia para ayudar con la recuperación. Con estos hechos en mente, quizás una de las herramientas más útiles de todas en la caja de herramientas de resiliencia cibernética de IBM es IBM Cyber Vault.

IBM Cyber Vault es una metodología de seguridad para la recuperación rápida de un ataque cibernético. Se basa en el IBM Safeguarded Copy, una tecnología para crear regularmente instantáneas aisladas e inmutables. Cyber Vault analiza estas instantáneas en busca de cambios potencialmente maliciosos, lo que podría indicar la presencia de ransomware. IBM Cyber Vault también se integra con IBM QRadar e IBM Storage Insights para una detección aún más rápida. Su validación de copias inalterables permite a los administradores identificar rápidamente una buena copia, probarla y luego restaurarla.

Para mejorar específicamente la velocidad, IBM Cyber Vault ayuda a los administradores de almacenamiento a acelerar:

- Identificación—La integración del QRadar e ideas de almacenamiento que ofrecen una mejor detección y facilitan el seguimiento.
- Mitigación y cuantificación de daños — La detección temprana y automática de ataques obviamente permite una recuperación más rápida de los mismos.
- Identificación de una copia segura— La automatización de copias inalterables de datos ocurre si se detecta una amenaza.
- Restauración de las operaciones— La recuperación rápida es posible en cuestión de horas, en lugar de días o semanas. (ver Figura 3).

Figura 3. Cómo el IBM Cyber Vault acelera la recuperación cibernética



Source: IBM

La gran verdad

Las infraestructuras de TI continúan volviéndose más complejas, lo que aumenta la posibilidad de que ocurran errores humanos, fallas del sistema o negligencia. Simultáneamente, los criminales, tanto dentro como fuera de la organización, son implacables en sus esfuerzos por buscar y explotar los vínculos débiles.

Sin duda, ocurrirán incidentes de seguridad. Este hecho debería impulsar un cambio en la mentalidad organizacional de reactiva a proactiva, de intentar fervientemente prevenir un ataque a prepararse y responder a las fallas de seguridad cuando ocurren. Esta es la transformación que las organizaciones deben emprender a medida que pasan de la seguridad cibernética a la resiliencia cibernética.

Muchas organizaciones están modelando sus estrategias de resiliencia cibernética siguiendo la guía proporcionada por el marco de seguridad cibernética del NIST, que recomienda que las organizaciones identifiquen recursos críticos, protejan esos recursos, detecten fallas e infracciones y planifiquen la respuesta y la recuperación de incidentes cibernéticos. Las organizaciones líderes están prestando especial atención a las capacidades de la infraestructura de TI que pueden mejorar su resiliencia cibernética a través de capacidades como el descubrimiento de datos, la gestión de copias, el cifrado, el control de acceso y el almacenamiento inmutable, al tiempo que mantienen múltiples opciones de recuperación de datos.

Para los líderes empresariales y de TI, la resiliencia cibernética se trata de tomar las decisiones tecnológicas y comerciales correctas, con el objetivo de mantener el negocio funcionando.

El Enterprise Strategy Group es una empresa que integra análisis, investigación y estrategia de tecnología para ofrecer inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad mundial del mercado de TI.

www.esg-global.com contact@esg-global.com 508.482.0188