Enterprise Strategy Group by TechTarget

Traducido por: redsis

FICHA TÉCNICA

El papel del almacenamiento para afrontar los desafíos de garantizar la ciberresiliencia

Por Scott Sinclair, director de práctica y analista sénior y Monya Keane, analista sénior de investigación.

Diciembre de 2022

Este informe técnico del Enterprise Strategy Group fue encargado por IBM y se distribuye bajo licencia de TechTarget, Inc.

Contenidos

Resumen Ejecutivo

El papel de los datos como activo empresarial transformador continúa creciendo. Gracias al aumento de las inversiones en desarrollo de aplicaciones, las prácticas modernas de DevOps y las mayores demandas de inteligencia empresarial, análisis y aprendizaje automático, casi todas las empresas están acelerando la creación y el uso de datos. También están ampliando el número de ubicaciones que los utilizan. Esta proliferación de datos, combinada con la creciente presión para acelerar las operaciones, ha provocado un aumento de la complejidad tanto de la infraestructura como de las operaciones de TI. Estos factores exponen a las organizaciones y sus infraestructuras a un gran riesgo de sufrir ataques maliciosos, errores humanos y comportamiento negligente. Desafortunadamente, las estrategias tradicionales no pueden garantizar adecuadamente la continuidad de las operaciones comerciales durante y después de este tipo de incidentes. Las empresas pueden intentar integrar capacidades para prevenir ataques y otras brechas de seguridad, pero las deficiencias funcionales, la integración deficiente y la complejidad de la gestión dificultan y hacen que el cumplimiento de los objetivos de seguridad sea lento. Cambiar la mentalidad organizacional, de la prevención a la preparación ante incidentes (por ejemplo, implementando soluciones de almacenamiento con ciberresiliencia integrada), es clave para proteger los activos de datos críticos y poder responder y recuperarse rápidamente del ransomware y otros ciberataques.

Introducción

El sector de TI se enfrenta a nuevos retos. Más de la mitad (53%) de los encuestados por el Grupo de Estrategia Empresarial (ESG) de TechTarget afirma que el sector de TI es más complejo hoy que hace dos años. Este aumento de la complejidad puede deberse a las iniciativas de transformación digital en curso (mencionadas por el 33%), el mayor volumen de datos (34%), la rápida evolución del panorama de la ciberseguridad (35%) y/o los esfuerzos para cumplir con las nuevas normativas de seguridad y privacidad de datos (34%).(1) Al mismo tiempo, las organizaciones tienen dificultades para abordar la problemática escasez de profesionales de TI críticos. De hecho, el 45% de las organizaciones encuestadas afirma no contar con suficientes especialistas en ciberseguridad; esta fue la escasez más frecuente. Además, estas organizaciones se enfrentan a una proliferación de aplicaciones, dispositivos y trabajadores remotos/móviles, lo que aumenta el tamaño y el alcance del perímetro de seguridad que el departamento de TI debe proteger. (2) Dada la complejidad del sector de TI moderno, la proliferación de datos y las crecientes amenazas de ciberataques, los equipos de TI a menudo tienen dificultades para mantener el ritmo. Intentar abordar la complejidad solo con personal interno es una batalla perdida. El éxito requiere modernizar la propia infraestructura subyacente. Sin embargo, al hacerlo, los responsables de TI deben buscar tecnologías que no solo satisfagan las necesidades de las aplicaciones o simplifiquen las operaciones. Alcanzar el verdadero éxito implica encontrar tecnología que pueda lograr esos objetivos y, además, mejorar la ciberresiliencia del entorno de aplicaciones.

La creciente amenaza de los ciberataques y el ransomware

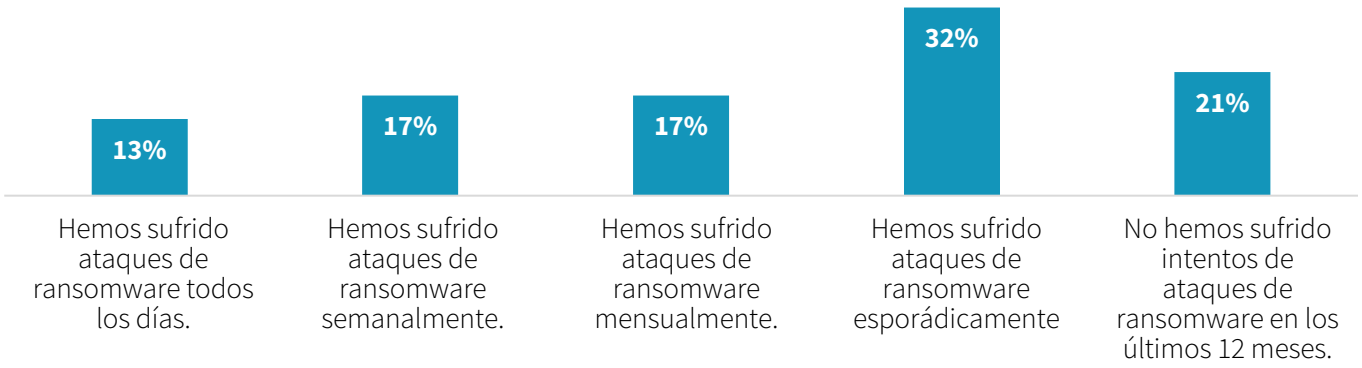
Las organizaciones se enfrentan a crecientes amenazas de ciberseguridad, probablemente impulsadas por el aumento de los incentivos financieros para los ciberdelincuentes. Por ejemplo, las quejas del público estadounidense ante el Centro de Quejas de Delitos en Internet (IC3) del FBI aumentaron un 69 % en 2020 con respecto a 2019, con pérdidas reportadas que superaron los 4100 millones de dólares.(3) Además, en los últimos cinco años, el IC3 reporta pérdidas totales combinadas de 13 300 millones de dólares.(4) En el cuarto trimestre de 2020, en EE. UU., la duración promedio de la interrupción tras los ataques de ransomware a empresas fue de 21 días.(5) Es evidente que el impacto negativo del ransomware en las operaciones comerciales es considerable.

[1] Fuente: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, Noviembre 2022.
[2] Ibid.
[3] Fuente: Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*.
[4] Ibid.
[5] Fuente: Coveware Blog, *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*, Febrero 2021.

Existe una fuerte correlación entre la complejidad de TI y la vulnerabilidad a los ciberataques. A medida que la TI se vuelve más compleja, los ciberataques aumentarán en frecuencia y tendrán un mayor costo.
El ransomware es una amenaza generalizada que ataca el activo más valioso de una empresa: sus datos. El IC3 identificó 2474 incidentes de ransomware reportados en 2020, y Enterprise Strategy Group (ESG) descubrió que el 63 % de las organizaciones encuestadas sufrieron ataques de ransomware el año pasado. De hecho, el 13 % experimentó ataques de ransomware a diario (véase la Figura 1). (6)
La protección contra el ransomware requiere una estrategia tecnológica que vaya más allá del ámbito de la ciberseguridad tradicional; también debe aprovechar los avances en el almacenamiento y la protección de datos.

Figura 1. El setenta y nueve por ciento sufrió ataques de ransomware en los últimos 12 meses

Según su conocimiento, ¿ha sufrido su organización algún intento de ataque de ransomware (con o sin éxito) en los últimos 12 meses? (Porcentaje de encuestados, N=620)



Fuente: Enterprise Strategy Group, a division of TechTarget, Inc.

Entre las organizaciones encuestadas que sufrieron un ataque de ransomware, el 73 % indicó que al menos uno de ellos tuvo éxito. En respuesta a una pregunta de seguimiento a las víctimas de un ataque de ransomware exitoso, más de la mitad (56 %) indicó que su organización pagó el rescate.

Sin embargo, pagar el rescate no solía ser una estrategia eficaz. ESG descubrió que, entre las organizaciones que pagaron un rescate, el 87 % se enfrentó a intentos de extorsión adicionales para pagar tarifas adicionales a la exigida originalmente, y solo el 14 % afirmó haber recuperado el 100 % de sus datos tras pagar el rescate.

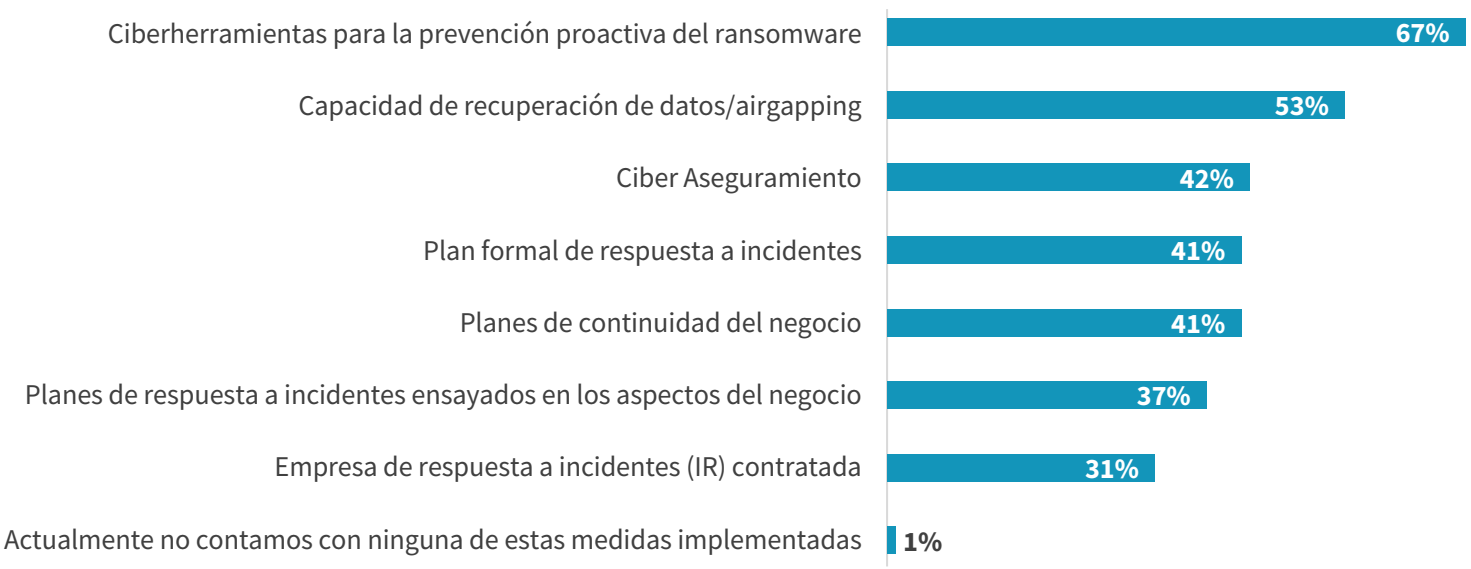
[6] Fuente: Enterprise Strategy Group Complete Survey Results: *The Long Road Ahead to Ransomware Preparedness,* Junio 2022.

El papel del almacenamiento de datos en la ciberresiliencia

Tanto los sistemas como los administradores de almacenamiento desempeñan un papel clave en la protección contra el ransomware. Cuando ESG preguntó a los responsables de la toma de decisiones de TI qué medidas usan para combatir o mitigar los ataques de ransomware, el 67 % de los encuestados indicó utilizar herramientas cibernéticas para la prevención proactiva del ransomware, y el 53 % identificó capacidades de recuperación de datos como la separación de datos (véase la Figura 2).7 Estas dos respuestas comunes destacan la importancia no solo de implementar medidas para evitar un ataque, sino también de invertir en soluciones que garanticen que la empresa esté preparada para recuperarse cuando inevitablemente ocurra un ataque. Es importante evitar simplemente establecer 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 de recuperación de datos eficaz antes de que sea necesario.

Cuando Enterprise Strategy Group preguntó a los responsables de la toma de decisiones de TI qué medidas implementan sus organizaciones para combatir o mitigar los ataques de ransomware, el 67 % de los encuestados indicó utilizar herramientas cibernéticas para la prevención proactiva del ransomware, y el 53 % identificó capacidades de recuperación de datos, como el aislamiento físico.

Figura 2. Medidas comunes implementadas para combatir o mitigar el ransomware



Fuente: Enterprise Strategy Group, a division of TechTarget, Inc.

Es importante recordar que combatir un ataque es muy diferente a la recuperación de datos tradicional. Normalmente, las organizaciones casi siempre buscan recuperar sus datos utilizando la copia más reciente. Sin embargo, con el ransomware, el equipo de TI no suele saber qué copia "buena" usar; por lo tanto, la recuperación suele ser más arriesgada y puede tardar mucho más. Algunos ataques de ransomware no solo atacan los datos, sino también la propia infraestructura de respaldo. Por eso, las capacidades de almacenamiento avanzadas son fundamentales para una recuperación eficaz del ransomware.

[7] Fuente: Enterprise Strategy Group Research Report, *2022 Technology Spending Intentions Survey*, Noviembre 2021.

Si bien adoptar las medidas identificadas en la Figura 2 es inteligente y debe incrementarse, las organizaciones deben comprender que ninguna defensa por sí sola es 100 % efectiva para la recuperación. Si bien es importante considerar herramientas para identificar y evitar el ransomware, así como en la recuperación de datos, esto es solo una parte del esfuerzo. Incluso con la mejor defensa, es posible que un ataque logre infiltrarse. Las organizaciones deben prepararse para esta esoy evaluar cómo minimizar el impacto en el negocio recuperándose lo más rápido posible. Para minimizar la exposición general al ransomware, las organizaciones debe acelerar la identificación de ataques, la mitigación de daños y la recuperación con una copia de seguridad confiable.

Las organizaciones deberían pasar de preguntarse "¿Cómo nos protegemos?" a "¿Si nos ataca un ransomware, con qué rapidez nos recuperaremos? ¿Con qué rapidez podrá nuestro negocio volver a la normalidad?".

Aquí es donde entran en juego estrategias sólidas de ciberresiliencia, considerando todos los componentes del manejo de datos: hardware, software, personas y procesos. Al desarrollar una estrategia de ciberresiliencia, las organizaciones deben pasar de preguntarse "¿Cómo nos protegemos?" a "¿Si nos ataca un ransomware, con qué rapidez podemos recuperarnos? ¿Con qué rapidez puede nuestro negocio volver a la normalidad?".

Almacenamiento y protección de datos: sepa cómo minimizar el riesgo de ransomware

La recuperación de ransomware es una forma de recuperación ante desastres, pero sus efectos son muy diferentes a los de un incendio o una inundación. Al fin y al cabo, generalmente se puede saber cuándo un incendio está completamente extinguido. El ransomware es más bien como una chispa oculta dentro de una pared que podría reaparecer en cualquier momento. Los administradores de almacenamiento deben centrarse en ciertas áreas para ayudar a reducir los riesgos asociados al ransomware. Dado que la velocidad es esencial, deben determinar con qué rapidez su organización puede:

- Identificar un riesgo.
- Cuantificar el daño causado.
- Mitigar el daño con la copia correcta, usándola para la recuperar y restaurar las operaciones.

Adoptar una actitud de "esto no nos pasará a nosotros" es, en el mejor de los casos, arriesgado. Las organizaciones deben ser proactivas e implementar una solución eficaz de almacenamiento y protección de datos, antes de que la necesiten.

Pasando de la ciberseguridad a la ciberresiliencia con IBM

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

- **IBM FlashSystem y DS8000**, soluciones de almacenamiento principal que incluyen funciones de inmutabilidad y cifrado de datos, que pueden automatizarse o suscribirse como servicio.
- **IBM Storage Scale**, IBM Storage Scale System e IBM Storage Ceph, soluciones de almacenamiento de archivos y objetos con funciones de inmutabilidad y cifrado de datos, que pueden automatizarse o suscribirse como servicio.
- **IBM Tape Storage**, que también admite la inmutabilidad y el cifrado de datos, y proporciona protección mediante el aislamiento físico.

- **IBM Spectrum Sentinel** es una solución prediseñada creada para ayudar a las organizaciones a simplificar y mejorar la detección y recuperación de ransomware mediante la integración de la programación, el escaneo y la identificación de posibles copias de recuperación. Está disponible actualmente para SAP HANA y Epic Healthcare Systems.
- **IBM Spectrum Copy Data Management** gestiona y protege las copias de datos.
- **IBM Spectrum Protect Suite** ofrece protección adicional. El almacenamiento definido por software Spectrum Protect puede almacenar datos en memoria flash, disco, almacenamiento de objetos y cinta física o virtual. Detecta la actividad de malware y ransomware al identificar grandes desviaciones de los patrones de acceso normales.
- **Las soluciones IBM QRadar e IBM Storage Insights** ayudan a acelerar la detección de posibles amenazas mediante capacidades mejoradas con IA.

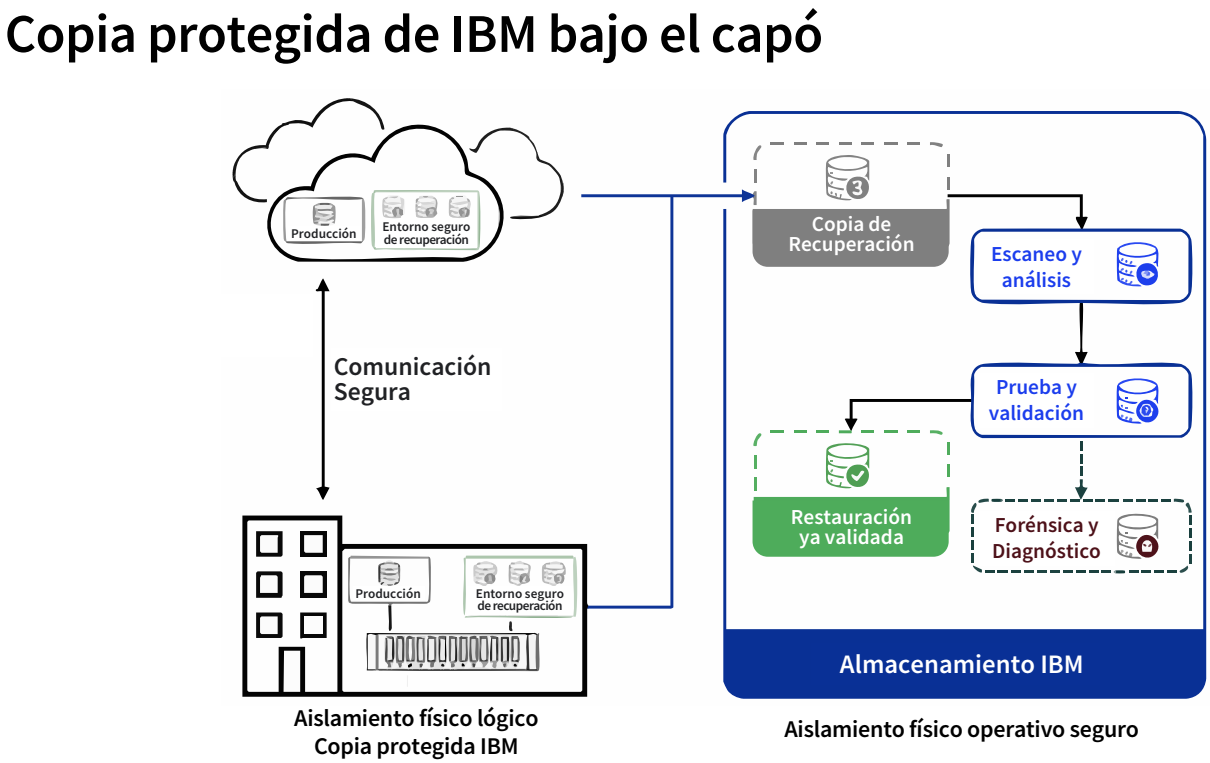
Construyendo una base de resiliencia cibernética con IBM Safeguarded Copy

IBM Safeguarded Copy permite a los usuarios crear copias granulares puntuales de datos de producción activos. Estas copias son copias protegidas e inmutables, inalterables e inalterables. Los usuarios deben tener los privilegios de acceso adecuados para modificar la configuración de caducidad de Safeguarded Copy, lo que facilita la separación de funciones en las operaciones y la gestión. Por último, Safeguarded Copy aprovecha el software de gestión de copias existente para realizar pruebas y facilitar la recuperación de copias. La Figura 3 ofrece más información sobre IBM Safeguarded Copy.

En resumen, IBM Safeguarded Copy ofrece:

- **Copias protegidas de los datos que ofrecen un mayor nivel de seguridad**, cumpliendo con las normativas del sector y las empresas. Las copias de seguridad de Copias Protegidas son inmutables, lo que significa que están ocultas, no se pueden direccionar, no se pueden modificar ni eliminar, y solo se pueden utilizar tras la recuperación.
- **Automatización** para establecer y gestionar políticas, como el número de copias o el periodo de retención, para simplificar y acelerar la gestión y la restauración.
- **Separación de funciones.** Las funciones tradicionales de copia de seguridad y restauración no suelen proteger contra ataques intencionados (por ejemplo, de empleados deshonestos) ni involuntarios. Al impedir el acceso a la configuración de caducidad de Copias Protegidas, las copias de seguridad ofrecen mayor protección contra ataques internos.

Figura 3. Copia protegida de IBM



Fuente: IBM

Ciberresiliencia con IBM Cyber Vault

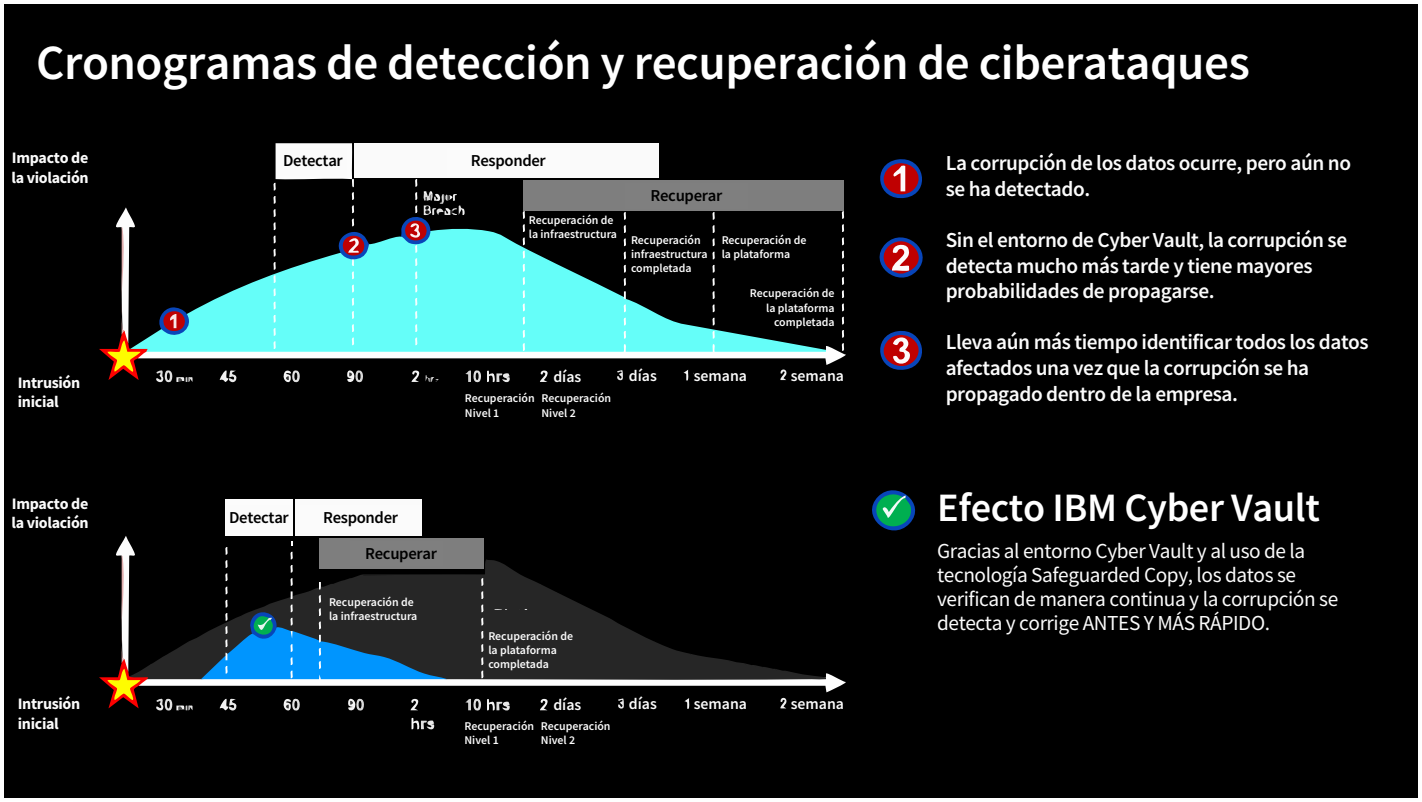
Es difícil sobreestimar el papel del almacenamiento en la protección contra el ransomware. El software de almacenamiento detecta los cambios realizados en los datos primarios y, gracias a ello, está en una posición ideal para identificar cuándo se inicia un ataque. Es la tecnología que también toma y protege las copias secundarias, lo que hace que el almacenamiento sea crucial para facilitar la recuperación. Con esto en mente, quizás una de las herramientas más útiles de IBM para la ciberresiliencia sea IBM Cyber Vault.

IBM Cyber Vault es una metodología de seguridad para una rápida recuperación ante un ciberataque. Se basa en IBM Safeguarded Copy, una tecnología que crea periódicamente instantáneas aisladas e inmutables. Cyber Vault analiza estas instantáneas en busca de cambios potencialmente maliciosos que podrían 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 inmutables permite a los administradores identificar rápidamente una copia válida, probarla y restaurarla.

En términos de mejora de la velocidad, IBM Cyber Vault ayuda a los administradores de almacenamiento a acelerar:

- **Identificación:** La integración de QRadar y Storage Insights ofrece una detección y una monitorización mejoradas.
- **Mitigación y cuantificación de daños:** Este es un proceso automatizado. La detección temprana y automática de ataques permite, obviamente, una recuperación más rápida.
- **Identificación de una copia correcta:** La automatización de copias inmutables de datos se produce si se detecta una amenaza.
- **Restauración de operaciones:** La recuperación rápida es posible en cuestión de horas, en lugar de días o semanas (véase la Figura 4).

Figura 4. Cómo IBM Cyber Vault acelera la recuperación cibernética



Fuente: IBM

IBM Cyber Vault está disponible para los usuarios como una oferta de servicios de IBM, donde expertos de IBM trabajan con organizaciones para adaptar la solución a las necesidades de su entorno de aplicación específico. Para entornos de aplicación específicos, como SAP HANA o EPIC Healthcare Systems, IBM ofrece Spectrum Sentinel, que ofrece las funcionalidades de IBM Cyber Vault en una implementación llave en mano prediseñada, diseñada para simplificar y acelerar la implementación.

La verdad más grande

Las infraestructuras de TI son cada vez más complejas, lo que aumenta la probabilidad de errores humanos, fallos del sistema o negligencia. Simultáneamente, actores maliciosos, tanto dentro como fuera de la organización, buscan y explotan constantemente los puntos débiles.

Sin duda, los incidentes de seguridad ocurrirán. Esto debería impulsar un cambio en la mentalidad organizacional, de reactiva a proactiva: de esforzarse por prevenir un ataque a prepararse y responder ante las fallas de seguridad cuando ocurren. Esta es la transformación que las organizaciones deben emprender en su transición de la ciberseguridad a la ciberresiliencia.

Muchas organizaciones están modelando sus estrategias de ciberresiliencia según las directrices del Marco de Ciberseguridad del NIST, que recomienda que las organizaciones identifiquen los recursos críticos, los protejan, detecten fallos y brechas, y planifiquen la respuesta y la recuperación ante incidentes cibernéticos. Las organizaciones líderes están prestando especial atención a las capacidades de la infraestructura de TI que pueden mejorar su ciberresiliencia mediante funciones como el descubrimiento de datos, la gestión de copias, el cifrado, el control de acceso y el almacenamiento inmutable, manteniendo al mismo tiempo múltiples opciones de recuperación de datos.

Para los líderes de TI y de negocios, la ciberresiliencia tiene que ver con tomar las decisiones tecnológicas y comerciales correctas, con el objetivo de mantener el negocio operativo.

Traducido por:

Vea más información sobre IBM Flash System y cómo podemos ayudarlo:
https://redsis.co/soluciones/infraestructura-ti/almacenamiento/ibm-flash-system/

Enterprise Strategy Group es una empresa integrada de análisis, investigación y estrategia tecnológica que brinda inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad global de TI.

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