DELL Technologies

Filtración de copias de seguridad: reforzar la ciberseguridad y ganar resiliencia con Dell Technologies

Resumen ejecutivo

La filtración de copias de seguridad cada vez amenaza más a empresas de todos los sectores. Son una vía para explotar las vulnerabilidades de sistemas que se han diseñado precisamente para proteger información crítica. Estos ataques ponen en peligro los sistemas de recuperación de datos, socavan la confianza y arriesgan las operaciones. Las consecuencias de un ataque de este tipo pueden ser severas y comprenden desde importantes pérdidas financieras a largos de tiempos de inactividad o daño reputacional.

Dell Technologies ofrece una serie integral de defensas para proteger datos confidenciales y evitar las filtraciones. Entre ellas están Dell Trusted Devices, la infraestructura de confianza de Dell y más capacidades de seguridad integradas en el resto de nuestras soluciones. Con nuevas colaboraciones estratégicas y servicios profesionales, Dell ayuda a las organizaciones a establecer marcos de seguridad multicapa resistentes para detectar filtraciones de copias de seguridad. impedirlas y recuperarse de ellas de manera eficiente.

Gracias a las innovadoras soluciones de Dell y a la asistencia de sus expertos, los negocios pueden prepararse mejor para proteger sus infraestructuras y mantener la continuidad operativa.

La creciente amenaza de las filtraciones de copias de seguridad

Las copias de seguridad son esenciales para la continuidad de las empresas. Son un instrumento clave de recuperación ante cualquier incidente informático, como los ataques de ransomware o los fallos de hardware. Por desgracia, lo que constituye una herramienta útil y necesaria, también es un objetivo cada vez más interesante para los ciberdelincuentes. La filtración de estas copias acaba en una corrupción o en la eliminación de datos almacenados para que no se pueda acceder a ellos cuando sean necesarios.

Para hacer frente a estas amenazas en constante evolución hay que implantar medidas proactivas. De lo contrario, se comprometen las operaciones y se ponen en peligro los datos confidenciales. Empresas de todos los tamaños, desde pequeñas a multinacionales, son objetivos potenciales de estos ataques. Y, entre ellas, son las de los sectores de la salud, las finanzas y la fabricación las que más expuestas quedan a estos riesgos.

En Dell Technologies sabemos que hay que reforzar la seguridad de estos entornos urgentemente y ofrecemos una serie de avanzadas herramientas y directrices para hacer frente a estos ataques sofisticados.

Ataques de filtración de copias de seguridad

Se produce una filtración de copia de seguridad cuando los ciberdelincuentes explotan las vulnerabilidades de un sistema de copias para comprometer, destruir o cifrar datos de recuperación críticos. Estos ataques sofisticados pueden ir acompañados de otros incidentes, como amenazas de ransomware o malware, que agravan las consecuencias financieras y operativas.

Cómo funcionan los ataques a copias de seguridad

1. **Brecha inicial:** los atacantes acceden de manera no autorizada a la red. Suelen conseguirlo sirviéndose del phishing, de credenciales poco seguras o de otras vulnerabilidades de seguridad.
2. **Desplazamiento lateral:** una vez dentro de la red, los atacantes utilizan herramientas para moverse sigilosamente hasta dar con los repositorios de copias de seguridad y otros conjuntos de datos críticos.
3. **Ataque sobre la copia:** las principales tácticas son, entre otras, el cifrado de archivos, la eliminación de puntos de recuperación o la corrupción de datos.

© 2025 Dell Inc. o sus filiales.

Técnicas comunes

- **Robo de credenciales** para acceder a cuentas administrativas, a través de las que entrar en sistemas de copias de seguridad.
- **Ataques de ransomware** para cifrar datos reales y copias de seguridad y luego exigir un pago a cambio de su decodificación.
- **Corrupción gradual** para comprometer las copias de seguridad escalonadamente. Así el ataque pasa desapercibido y la empresa queda expuesta cuando necesita recuperar sus datos.

Estas técnicas ponen de relieve la sofisticación y la gravedad de estas amenazas y evidencian la necesidad de acciones preventivas.

El impacto en las empresas

Pérdida financiera

La filtración de copias de seguridad aumenta los costes de recuperación y lapsos de inactividad, y suelen duplicar o triplicar los costes de la respuesta. La recuperación de copias de seguridad cifradas o comprometidas puede exigir pagos a atacantes, nuevas infraestructuras o gastos en consultoría.

Interrupción operativa

Sin copias de seguridad viables, las empresas se enfrentan a largos tiempos de recuperación que interrumpen sus servicios, retrasan proyectos y detienen funciones críticas.

Daños en la reputación

La pérdida permanente de datos o los tiempos de inactividad prolongados merman la confianza de los clientes y perjudican la viabilidad de las empresas a largo plazo.

Un caso real

Un proveedor de servicios sanitarios global descubrió que sus copias de seguridad habían sido vulneradas durante un ataque de ransomware. A pesar de pagar el rescate, se perdieron permanentemente 3 semanas de datos de pacientes. Eso se tradujo en un retraso en las cirugías programadas y en posteriores demandas. Los costes totales de recuperación superaron **los 50 millones de dólares.**

Estadísticas alarmantes

En estudios recientes se ha estimado que las consecuencias financieras de un sistema de copias de seguridad vulnerado se sitúan, de media, en los **4,45 millones de dólares**[1], incluidas las sanciones, los tiempos de inactividad y otros costes de recuperación. Igual de alarmante es que estos incidentes se estén dando cada vez con más frecuencia. Los informes globales indican que hay un aumento del **39 %** de estas amenazas relacionadas con copias de seguridad de año a año.

El 57 %
de los ataques dirigidos a copias de seguridad consiguen perpetuarse con éxito

Fuente: 2024: Index Engines

Hacer frente a las filtraciones de copias de seguridad con Dell Technologies

Dell Technologies proporciona un sólido conjunto de herramientas y servicios con los que abordar los retos únicos que plantean las filtraciones de copias de seguridad para ayudar a las empresas a prevenirlas, detectarlas y recuperarse de ellas de forma eficaz.

Soluciones de seguridad para servidores y almacenamiento

Las soluciones de almacenamiento y servidores de Dell ofrecen una resiliencia inigualable contra los ataques dirigidos a copias de seguridad. Las funciones que llevan integradas garantizan una mayor seguridad tanto de la copia como de las instantáneas.

- **Las copias de seguridad e instantáneas inmutables** crean puntos de recuperación a prueba de manipulaciones.
- **La recuperación con espacio de aire** aísla los datos de las redes activas para evitar su corrupción.

[1] Ponemon, "Cost of a Data Breach Report 2024"

© 2025 Dell Inc. o sus filiales.

Reforzar la seguridad con dispositivos Dell Data Protection

Los dispositivos Dell Data Protection cuentan con capacidades como SafeBIOS de Dell para una mayor integridad de firmware y SafeData para un cifrado seguro con el que proteger las copias de seguridad de los ataques. Se trata de soluciones con autenticación de doble factor (MFA), control de acceso basado en funciones (RBAC) y autenticación doble para mantener a raya a los ciberdelincuentes.

Detección de amenazas avanzadas con CrowdStrike

La integración entre CrowdStrike y Dell Data Protection se centra en mejorar la seguridad y la supervisión de los entornos de protección de datos a través de un conjunto de capacidades avanzadas.

1. **Protección de datos y puntos finales:** con estas soluciones de protección de datos, Dell integra la seguridad de puntos finales de CrowdStrike y una detección y respuesta ampliadas (EDR/XDR). Y eso incluye la recopilación de telemetría de PowerProtect Data Manager y PowerProtect Data Domain de Dell, junto con información de seguridad de la consola CrowdStrike Falcon y el software SIEM de última generación
2. **Supervisión y respuesta:** el servicio Managed Detection and Response (MDR) de Dell gestiona el software CrowdStrike por los clientes, recopilando registros e investigando cualquier indicador de riesgo (IOC) o anomalía detectada. Esta integración permite a Dell ofrecer una supervisión continua y colaborar con los centros de operaciones de seguridad de los clientes para brindar soluciones rápidas y efectivas ante las amenazas
3. **Visibilidad en tiempo real y control de movimiento de datos:** la plataforma CrowdStrike Falcon Data Protection ofrece visibilidad en tiempo real del movimiento de datos a través de diversas fuentes y canales, y clasifica los datos por contenido y contexto. Esto ayuda a prevenir el robo de datos y a garantizar que las políticas de protección de datos se aplican de forma eficaz mediante la combinación de contenido con análisis contextuales
4. **Gestión unificada e implementación simplificada:** la integración permite que una sola plataforma y un agente gestionen la protección de datos y los puntos finales, lo que reduce la complejidad y la sobrecarga operativa. A ello contribuye el enfoque ligero y nativo de cloud de la plataforma CrowdStrike, que permite una implantación rápida y sin interrupciones

La integración entre CrowdStrike y Dell Data Protection aprovecha las capacidades avanzadas de EDR/XDR, la supervisión en tiempo real y la gestión integral de datos para mejorar la seguridad y la resiliencia generales de los entornos de protección de datos.

Recientemente, una institución financiera líder implementó PowerProtect Cyber Recovery y pudo impedir que unos atacantes accedieran al 90 % de sus copias de seguridad críticas durante una brecha. Tras el incidente, pudo recuperarse sin problemas ni pagos de rescate.

Soluciones Dell PowerProtect para la integridad de las copias de seguridad

Dell PowerProtect ofrece una protección integral de copias de seguridad que aprovecha la inmutabilidad, el aislamiento y la compresión para evitar riesgos en el sistema de copias de seguridad. Al integrarse con las herramientas de detección de ransomware, PowerProtect garantiza que los cambios sospechosos activen alertas para reaccionar de forma inmediata.

El enfoque de seguridad multicapa

La protección de los datos requiere estrategias de seguridad coordinadas y polifacéticas. Dell ayuda a las empresas a implementar los procedimientos recomendados del sector para crear un entorno de copia de seguridad resiliente.

Pasos clave para mejorar la defensa

- **Adoptar principios de confianza cero:** valide continuamente todos los usuarios, dispositivos y procesos para reducir el riesgo de acceso no autorizado.
- **Cifrar todas las copias de seguridad:** asegúrese de que los datos permanezcan ilegibles si se ven comprometidos, tanto en tránsito como en reposo.
- **Formar a la plantilla:** enseñe a su personal a reconocer los intentos de phishing y otras tácticas de ingeniería social que provocan brechas iniciales.
- **Pruebas de vulnerabilidad periódicas:** al realizar pruebas frecuentes podrá identificar puntos débiles y trabajar en ellos antes de que los atacantes los aprovechen.

Dell combina estas prácticas con soluciones avanzadas para crear una infraestructura sólida y con capacidad de respuesta lista para afrontar los retos.

© 2025 Dell Inc. o sus filiales.

Colaboraciones estratégicas que mejoran la seguridad

Dell colabora con líderes en ciberseguridad como Microsoft, CrowdStrike y Secureworks. Cada una de estas asociaciones mejora las soluciones de Dell y ofrece a los clientes capacidades de protección inigualables, como inteligencia de amenazas avanzadas, supervisión de puntos finales y estrategias de respuesta integrales.

Sacar el máximo partido a Dell Professional Services

Los servicios profesionales de Dell Technologies proporcionan conocimientos y orientación a las empresas para ayudarlas a abordar retos de ciberseguridad complejos de forma eficaz. Desde la creación de planes de respuesta ante incidentes hasta la implementación de arquitecturas de confianza cero, los especialistas de Dell garantizan que los entornos del cliente sigan siendo resilientes frente a amenazas sofisticadas como las filtraciones de copias de seguridad.

Crear resiliencia empresarial con Dell

Dell Technologies capacita a las empresas para superar ataques sofisticados y seguir operando con normalidad. A través de la innovación, la colaboración y el conocimiento, Dell ayuda a los negocios a prevenir, detectar y recuperarse incluso de los ataques de filtración de copias de seguridad más severos.

Dé el siguiente paso

Póngase en contacto con Dell Technologies hoy mismo para proteger su empresa. Juntos, mantendremos la seguridad de sus activos críticos, protegeremos su reputación y crearemos un futuro resiliente.

En Dell, tenemos el firme compromiso de ofrecer confianza a las empresas en la era digital brindándoles las herramientas, los conocimientos y la asistencia que necesitan para operar de forma segura y prosperar.

La resiliencia de las copias de seguridad comienza con Dell Technologies. Póngase en marcha hoy y genere verdadera confianza con operaciones listas para el futuro.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **Dell.com/SecuritySolutions**

Más información sobre Soluciones de Dell

Póngase en contacto con un experto de Dell Technologies

Consulte más recursos.

Únase a la conversación con #HashTag.

© 2025 Dell Inc. o sus filiales. Todos los derechos reservados. Dell y otras marcas comerciales pertenecen a Dell Inc. o sus filiales. Otras marcas comerciales pueden pertenecer a sus respectivos propietarios.

DELL Technologies