DELL Technologies

Cómo reforzar la ciberseguridad y la resiliencia con Dell Technologies

¿Qué es el ransomware?

El ransomware es un tipo de software malicioso (malware) que bloquea el acceso a un sistema o unos datos informáticos hasta que se pague un rescate. Se trata de uno de los ciberataques más perjudiciales que existen. El 50 % de las organizaciones mundiales se han visto afectadas por el ransomware al menos una vez en el último año. El tiempo de inactividad medio tras un ataque es de tres semanas, lo que conlleva importantes interrupciones operativas.

El aumento de la amenaza del ransomware

El ransomware es un tipo de software malicioso (malware) que bloquea el acceso a un sistema o unos datos informáticos hasta que se pague un rescate. Se trata de uno de los ciberataques más perjudiciales que existen. El 50 % de las organizaciones mundiales se han visto afectadas por el ransomware al menos una vez en el último año. El tiempo de inactividad medio tras un ataque es de tres semanas, lo que conlleva importantes interrupciones operativas.

Cómo funciona el ransomware

El ransomware suele infectar a las organizaciones cuando alguien hace clic en un enlace malicioso, abre un archivo adjunto infectado o visita un sitio web peligroso. A continuación, entra en los sistemas para cifrar los archivos y hacerlos ilegibles. En se momento, el programa de ransomware suele mostrar un mensaje exigiendo un pago (a menudo en criptomonedas) a cambio de una clave de descifrado. Si el rescate no se paga, el atacante puede amenazar con eliminar o publicar los datos. Un ataque de ransomware bastante conocido fue el de WannaCry de 2017, que se extendió rápidamente por todo el mundo y afectó a hospitales, empresas y agencias gubernamentales. Tuvo un impacto financiero masivo. El impacto económico global del virus WannaCry fue de entre 4 000 y 8 000 millones de dólares según Cyber Risk Management (CyRiM) y Lloyd's of London, con más de 200 000 sistemas afectados en 150 países en cuestión de días.

Dos de las principales empresas del mundo afectadas fueron FedEx, que informó de una pérdida de 300 millones de dólares debido a interrupciones en el servicio y limpieza, y Renault-Nissan, que tuvo que detener temporalmente la producción en varias plantas. Los costes ocultos de un ataque de ransomware pueden ser muchos, incluidos:

- Tiempo de inactividad y pérdida de productividad de la empresa
- Daño reputacional
- Coste de recuperación y aplicación de parches del sistema
- Multas legales y normativas

Cuando se enfrentan a un ataque de ransomware, las empresas deben tomar las siguientes medidas:

- No pagar salvo que sea absolutamente necesario: no hay garantía de que los atacantes vayan a restablecer e acceso.
- Restaurar los datos con una copia de seguridad en caso de tenerla.
- Denunciar el ataque a las autoridades.
- Reforzar la seguridad para prevenir infecciones en el futuro (por ejemplo: mantener el software actualizado, capacitar al personal, utilizar protección de puntos finales).

Combatir los ataques de ransomware con Dell Technologies

Dell Technologies proporciona a las organizaciones herramientas integrales y avanzadas diseñadas para frustrar las amenazas de ransomware antes de que causen daños.

Mejora de la seguridad de puntos finales con Dell Trusted Devices

Los puntos finales suelen ser los principales puntos de entrada de los ataques de ransomware, por lo que la seguridad de los puntos finales es un área de enfoque esencial. Dell Trusted Devices integran características de seguridad habilitadas para hardware que protegen los sistemas sin comprometer el rendimiento. Soluciones como Dell SafeBIOS y SafeID protegen los dispositivos de puntos finales contra el acceso no autorizado, mientras que Dell SafeData cifra los datos para proteger la información confidencial incluso fuera del firewall corporativo. Al integrar la seguridad directamente en los dispositivos, las empresas garantizan la protección a nivel de hardware, lo que ofrece a los atacantes menos oportunidades de afianzarse.

Detección proactiva con CrowdStrike

Los ataques de ransomware se pueden evitar si las organizaciones utilizan las herramientas adecuadas para detectar amenazas y responder a ellas en tiempo real. CrowdStrike, que se ofrece como parte de la cartera de soluciones de Dell, proporciona una plataforma de protección de puntos finales de última generación con tecnología de IA y análisis de comportamiento. Esta tecnología identifica y neutraliza la actividad sospechosa antes de que se convierta en un ataque. Al integrarse sin complicaciones con la infraestructura de Dell, CrowdStrike permite a los equipos de TI mantener la visibilidad de todo su entorno, lo que ofrece una respuesta inmediata y eficaz ante amenazas.

Protección de datos integral con Dell PowerProtect

Las soluciones Dell PowerProtect son vitales para la resiliencia de ransomware. Estas herramientas avanzadas de protección de datos están diseñadas para proteger los datos empresariales frente a amenazas internas y externas. Funciones como las copias de seguridad inmutables garantizan que sus datos no se puedan alterar, eliminar o cifrar mediante ransomware, lo que proporciona una red de seguridad fiable incluso ante ataques avanzados. El vault de Dell PowerProtect Cyber Recovery, por ejemplo, aísla los datos críticos de la red mediante tecnología con cámara de aire, lo que garantiza que permanezcan intactos incluso durante los ataques más sofisticados. Gracias a la detección automatizada de anomalías y los flujos de trabajo inteligentes, las organizaciones pueden detectar actividades maliciosas con antelación y responder antes de que se propague el ransomware.

Seguridad de red avanzada y microsegmentación con Dell PowerSwitch Networking y SmartFabric OS

La segmentación de red avanzada, los controles de acceso estrictos y los análisis de tráfico en tiempo real en toda la infraestructura fortalecen las defensas contra ataques de día cero.

Recuperación a escala con los servicios de protección de datos de Dell

Dell entiende que, aunque la prevención es fundamental, la recuperación es un factor igual de importante a la hora de prepararse para ataques de ransomware. Los servicios de protección de datos de Dell no solo ofrecen soluciones automatizadas de copia de seguridad y recuperación, sino también consultorías dirigidas por expertos para garantizar que las empresas puedan recuperarse rápidamente y minimizar el tiempo de inactividad. Servicios como la recuperación remota de datos y las respuestas ante incidentes ofrecen a las organizaciones la asistencia necesaria en momentos cruciales de crisis. Este enfoque integral permite preservar la integridad de los datos y reducir los tiempos de recuperación, lo que evita las interrupciones operativas.

Estos son solo algunos ejemplos de la gama de soluciones que puede ofrecer Dell contra amenazas maliciosas internas.

La fuerza de las colaboraciones

El enfoque colaborativo de Dell amplía su protección más allá de su tecnología exclusiva. A través de colaboraciones con empresas líderes en ciberseguridad, como CrowdStrike y Secureworks, Dell ofrece un ecosistema de soluciones integradas que abordan todos los posibles vectores de ataque. Juntas, estas soluciones proporcionan una cobertura de seguridad integral, lo que permite a las empresas crear varias capas de protección adaptadas a sus diferentes perfiles de riesgo.

¿Por qué elegir Dell?

Dell Technologies es más que un proveedor de tecnología: es un socio de confianza en la lucha contra el ransomware. Combinando innovación, conocimiento y el compromiso de ofrecer soluciones a las empresas, Dell proporciona a las organizaciones las herramientas necesarias para afrontar las amenazas en constante evolución. Ya sea protegiendo puntos finales, salvaguardando datos críticos o haciendo posible una recuperación rápida, los productos y servicios de Dell garantizan la continuidad operativa y la tranquilidad.

Un futuro a prueba de ataques

Los ataques de ransomware siguen evolucionando, pero con Dell Technologies las empresas van un paso por delante. Al aprovechar hardware, software y servicios avanzados, las organizaciones pueden crear una infraestructura de ciberseguridad resiliente, adaptable y fiable. Proteja sus datos y sus operaciones y prepare su empresa para el futuro hoy mismo con las soluciones integrales de Dell contra el ransomware.

Para garantizar la resiliencia de su empresa, es fundamental comprender las amenazas que existen actualmente y estar al tanto de las nuevas. Los expertos en ciberseguridad de Dell Technologies supervisan constantemente los nuevos vectores de ataque (¿cómo llamamos esto?) y trabajan para abordar de manera proactiva las posibles brechas en nuestros productos y servicios. Esto nos permite ofrecerle la última protección frente a las amenazas de ransomware en constante evolución.

Además de mantenerse informadas, las empresas también deben crear un enfoque de seguridad multicapa. Esto significa implementar una amplia gama de medidas de seguridad, como firewalls, software antimalware, sistemas de detección de intrusiones y copias de seguridad de datos. Al diversificar sus estrategias de defensa, puede minimizar el impacto de cualquier ataque y garantizar la operatividad de su empresa incluso ante un intento de ransomware exitoso.

También es importante probar y actualizar periódicamente las medidas de seguridad (aplicar parches a los sistemas y actualizar las políticas). Los hackers buscan constantemente nuevas formas de burlar las medidas de seguridad tradicionales, por lo que es fundamental que las empresas se mantengan a la vanguardia probando sus defensas cada cierto tiempo y actualizándolas según sea necesario. Esto incluye hacer periódicamente evaluaciones de vulnerabilidades, pruebas de penetración y gestión de parches.

Otro aspecto clave para proteger su empresa frente al ransomware es formar a sus empleados para que conozcan los procedimientos de ciberseguridad recomendados. Muchos ataques de ransomware se inician a través de tácticas de ingeniería social, como correos electrónicos de phishing o enlaces maliciosos. Al enseñar a sus empleados a detectar y evitar estas amenazas, puede reducir en gran medida la probabilidad de que un ataque tenga éxito.

Además, contar con un plan de recuperación ante desastres puede mitigar en gran medida el impacto de un ataque de ransomware. Este plan debe incluir copias de seguridad periódicas de datos y sistemas importantes, así como un procedimiento claro de respuesta y recuperación ante un ataque.

Además de estas medidas proactivas, también es importante contar con un plan consolidado de respuesta ante incidentes. Esto incluye definir claramente las funciones y responsabilidades necesarias para gestionar un ataque de ransomware, así como establecer protocolos de comunicación para notificar a las partes interesadas y mitigar los daños.

Por último, estar al día de las últimas tendencias y novedades en ataques de ransomware puede ayudarle a prevenir posibles amenazas. Al revisar periódicamente los informes y las actualizaciones de expertos en seguridad del sector puede implementar proactivamente nuevas medidas de seguridad para proteger su empresa.

Recuerde que ninguna empresa es inmune a los ataques de ransomware, pero con las estrategias y las herramientas adecuadas, es posible minimizar su riesgo e impacto. Al implicarse de forma proactiva en la ciberseguridad, no solo protege su empresa, sino que también genera confianza con sus clientes y partes interesadas.

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

Más información sobre las soluciones Dell

Póngase en contacto con un experto de Dell Technologies

Consulte más recursos

Únase a la conversación con #HashTag

DELL Technologies