DELL Technologies

Defensa contra ciberataques a la cadena de suministro con Dell Technologies

Resumen ejecutivo

El carácter cada vez más global e interconectado de las operaciones empresariales ha expuesto a las organizaciones a más amenazas de ciberataques a la cadena de suministro. Estos sofisticados ataques aprovechan las vulnerabilidades del ciclo de vida del hardware, desde la fabricación hasta la implementación, así como el software de terceros, para que agentes maliciosos pongan en peligro sistemas enteros a través de aplicaciones o actualizaciones de confianza. Estos incidentes no solo tienen efectos desastrosos a nivel financiero, sino que también pueden dañar la reputación e interrumpir las operaciones a gran escala.

Las consecuencias de estas amenazas son graves. Los ataques a la cadena de suministro suelen pasar desapercibidos hasta que se producen daños significativos, por lo que las estrategias preventivas de defensa son esenciales. Gracias a la protección avanzada de puntos finales, la supervisión y las soluciones integrales de seguridad de datos y servidores, Dell permite a las empresas proteger toda su cadena de suministro. Mediante la tecnología, las colaboraciones y la experiencia, las organizaciones pueden desarrollar resiliencia y proteger sus ecosistemas de sus vulnerabilidades inherentes.

Aumento de las amenazas de ciberataques a la cadena de suministro

Los ataques a la cadena de suministro han aumentado considerablemente en los últimos años. Al manipular dispositivos físicos durante la producción, el envío o la implementación, o al detectar debilidades en los proveedores de software, los atacantes obtienen los medios para introducir componentes o código maliciosos, dañar sistemas o filtrar datos confidenciales. Las víctimas son empresas de todos los tamaños, desde pequeñas hasta globales, y entre las consecuencias están graves pérdidas financieras, confianza de los clientes en riesgo y repercusiones legales. Dell Technologies, consciente de peligro creciente, aboga por medidas preventivas para mitigar los impactos catastróficos de estos ataques.

Conocer los ciberataques a la cadena de suministro

Cómo funcionan los ataques a la cadena de suministro de hardware

1. **Fase de fabricación:** los atacantes introducen componentes maliciosos durante el montaje del hardware, a menudo aprovechando proveedores en riesgo.
2. **Fase de envío:** los dispositivos se interceptan durante el transporte y se modifican para incluir modificaciones dañinas de firmware o hardware.
3. **Fase de implementación y activación:** cuando el hardware comprometido entra en la red de la organización, los atacantes obtienen acceso a datos confidenciales o permiten operaciones de puerta trasera.

Cómo funcionan los ataques a la cadena de suministro de software

1. **Vulneración inicial:** un proveedor de software externo está en riesgo, a menudo debido al phishing, vulnerabilidades desprotegidas o amenazas internas.
2. **Manipulación de código:** los agentes maliciosos introducen elementos dañinos, como malware o puertas traseras, en el software destinado a la distribución.

© 2025 Dell Inc. o sus filiales.

3. **Propagación a los usuarios finales:** las empresas que instalan o actualizan software comprometido descargan componentes maliciosos de forma involuntaria.

Técnicas comunes: hardware

- **Manipulación del firmware:** introducción de código malicioso que se activa después de la implementación.
- **Implantación de hardware:** integración de componentes ocultos para supervisar o filtrar datos.
- **Explotación de proveedores de confianza:** aprovechamiento de proveedores externos con procesos menos seguros.

Técnicas comunes: software

- **Secuestro de componentes:** infección de bibliotecas o infraestructuras de terceros con código malicioso.
- **Introducción de actualizaciones:** modificación de las actualizaciones oficiales de software para introducir vulnerabilidades.
- **Confusión de dependencias:** aprovechamiento de la confianza de las organizaciones en dependencias de paquetes inseguras.

El impacto en las empresas

Consecuencias financieras

Los ataques dirigidos a las cadenas de suministro suelen generar costes relacionados con multas legales, gastos de recuperación del sistema y compensación a los clientes. Un incidente destacado causó pérdidas de más de 70 millones de dólares a una empresa global de gestión, lo que refleja los estragos financieros que pueden provocar estas vulneraciones.

Interrupción operativa

Los sistemas dañados o deshabilitados por la infiltración de malware a menudo provocan un tiempo de inactividad prolongado, y esto afecta la productividad de la organización y retrasa la finalización de los proyectos.

Consecuencias en la reputación

La confianza en los socios de software es fundamental para las empresas modernas. Una vulneración de la cadena de suministro vinculada a las ofertas de software de una organización puede manchar su reputación y erosionar la fidelidad de sus clientes.

Ejemplos reales: hardware y software

Un fabricante global de productos electrónicos descubrió componentes comprometidos en su cadena de suministro, lo que provocó fallos generalizados del sistema. El ataque tuvo un coste de más de **45 millones de dólares** en concepto de recuperación y honorarios legales, además de daños irreparables en las relaciones con los proveedores.

La vulneración de SolarWinds es uno de los ataques a la cadena de suministro de software más conocidos. Supuso el riesgo de que su producto Orion infectara organizaciones de todo el mundo, incluidas agencias gubernamentales y empresas de la lista Fortune 500. Las estimaciones de daños superaron **los 90 millones de dólares** y la vulneración destacó las consecuencias de gran alcance de las vulnerabilidades de la cadena de suministro.

La experiencia de Dell Technologies en la lucha contra los ataques a la cadena de suministro

La amplia cartera de soluciones de seguridad de Dell Technologies prepara a las empresas ante los riesgos cibernéticos en constante evolución.

Verificación de componentes seguros (SCV)

La verificación de componentes seguros (SCV) es una parte clave de la estrategia de seguridad de la cadena de suministro de Dell Technologies, diseñada para garantizar la autenticidad y la integridad de los componentes de hardware en varias soluciones de Dell. SCV proporciona validación criptográfica de los componentes del sistema desde la fabricación hasta la entrega y la implementación. Dell Technologies proporciona una seguridad férrea a la cadena de suministro, lo que garantiza que los sistemas no se manipulen y sean seguros desde la fábrica hasta la implementación. Esto mejora la seguridad, la fiabilidad y el rendimiento generales de los clientes de Dell.

© 2025 Dell Inc. o sus filiales.

Protección de puntos finales con Dell Trusted Devices

Dell Trusted Devices integra la seguridad a nivel de hardware y firmware para crear sistemas a prueba de manipulaciones.

- **SafeBIOS** garantiza la integridad del firmware en la puesta en marcha, lo que evita cambios no autorizados en la configuración y verifica la integridad del firmware en el arranque para evitar que se inicien sistemas en riesgo.
- **SafeID** protege las credenciales de autenticación a nivel de hardware al impedir el acceso no autorizado y proteger las credenciales de inicio de sesión mediante el cifrado de las claves de autenticación y el bloqueo de usuarios no autorizados.
- **SafeData** permite el cifrado integral de archivos empresariales confidenciales para bloquear los intentos de filtración de datos de relevantes.

Detección preventiva de amenazas con CrowdStrike

CrowdStrike se integra con las tecnologías de Dell para ofrecer información en tiempo real sobre el comportamiento de software malicioso.

- **Análisis de detección de amenazas de comportamiento:** supervisa los comportamientos de hardware y firmware en busca de signos de manipulación y detecta actividades de software inusuales para evitar la implementación de malware.
- **Herramientas de respuesta inmediata:** la IA aísla los sistemas en riesgo para impedir el movimiento lateral dentro de la red.
- **Corrección de amenazas basada en IA:** identifica y aísla activamente las amenazas para evitar la propagación lateral dentro de los sistemas empresariales.
- **Capacidades de integración:** los entornos híbridos y de multicloud están protegidos de forma integral con las herramientas de Dell y CrowdStrike.

Seguridad reforzada a través de las soluciones de servidor y almacenamiento de Dell

La familia de servidores Dell PowerEdge incorpora protección avanzada para las plataformas de software esenciales. Los sistemas de almacenamiento como Dell PowerStore ofrecen un cifrado líder del sector para aplicaciones y datos.

- **Firmware del servidor seguro:** supervisa y bloquea los cambios no autorizados a nivel de hardware.
- **Supervisión de red aislada:** detecta anomalías que indican manipulaciones en la cadena de suministro.
- **Copias de seguridad inmutables:** protege los puntos de recuperación incluso cuando el almacenamiento principal está comprometido.
- **Vaults de recuperación:** los entornos aislados protegen frente a fallos consecutivos iniciados en sistemas comprometidos.

Enfoque multicapa para mitigar los riesgos

Dell anima a las empresas a adoptar estrategias integrales que combinen tecnología, prácticas de personal y procesos actualizados.

Medidas estratégicas

- **Mejore la visibilidad de la cadena de suministro:** exija a todos los proveedores que cumplan los rigurosos estándares de seguridad y que certifiquen el hardware en cada etapa.
- **Implemente el cifrado avanzado:** proteja los datos a todos los niveles mediante protocolos avanzados para limitar la accesibilidad incluso en hardware comprometido.
- **Adopte políticas de confianza cero:** ningún dispositivo, aplicación o usuario se considera fiable automáticamente sin verificación.
- **Aplique estándares de codificación seguros:** aplique directrices estrictas para plugins, API e integraciones al colaborar con socios de software.
- **Supervise la actividad y audite periódicamente:** las auditorías de visibilidad frecuentes garantizan la integridad de los servicios de terceros.
- **Realice pruebas periódicas:** implemente pruebas de penetración y evaluaciones del firmware para validar continuamente la integridad de los dispositivos.
- **Forme al personal:** prepare a los equipos para que reconozcan los componentes o paquetes con comportamientos sospechosos.

© 2025 Dell Inc. o sus filiales.

Cómo Dell Professional Services garantiza la resiliencia empresarial

Dell Professional Services asesora a las empresas en la implementación de defensas férreas en la cadena de suministro. Equipos de expertos en ciberseguridad con experiencia proporcionan evaluaciones, formación y estrategias de respuesta ante amenazas adaptadas a las necesidades únicas de la organización.

- **Guía de implementación:** alinea estratégicamente las prácticas de los proveedores auditados y de confianza cero en sus entornos.
- **Respuestas ante incidentes:** garantiza que las empresas se recuperen rápidamente tras incidentes maliciosos.

Sistemas empresariales preparados para el futuro con Dell

Los ciberataques a la cadena de suministro muestran la sofisticación de las amenazas modernas. Las empresas necesitan una protección que no solo evite las vulneraciones, sino que garantice una recuperación rápida cuando se produzcan incidentes. Trabajar con Dell Technologies proporciona acceso a herramientas de vanguardia, conocimientos estratégicos y una red de partners de confianza.

Dé el siguiente paso

Proteja los activos confidenciales y aumente la fiabilidad operativa mediante la implementación de procedimientos recomendados con tecnología de Dell Technologies. Contáctenos hoy mismo para tener una reunión personalizada y prepararse para proteger sus sistemas empresariales.

Dell Technologies es sinónimo de confianza, adaptabilidad e innovación a medida que evoluciona la ciberseguridad de la cadena de suministro. El compromiso de hoy garantiza el éxito del mañana.

Un futuro más seguro y protegido comienza con Dell Technologies. Confíe en nosotros para proteger lo más importante.

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.

© 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