DELL Technologies

Día cero: cómo reforzar la ciberseguridad y la resiliencia con Dell Technologies

La amenaza en auge de los ataques de día cero

Los ataques de día cero se han convertido rápidamente en uno de los retos más extraordinarios de la ciberseguridad de hoy en día. Estos ataques aprovechan vulnerabilidades que los proveedores de software y los expertos en seguridad desconocen, lo que deja a las empresas desprotegidas. Todas las organizaciones, desde empresas sanitarias hasta financieras, son susceptibles de sufrir este tipo de ataques, que suelen provocar consecuencias graves a nivel económico y operativo.

La transformación digital se está acelerando rápidamente, y los ataques de día cero se han vuelto más frecuentes y sofisticados que nunca. La necesidad de encontrar protecciones adecuadas nunca había sido tan urgente. Dell Technologies es consciente de la importancia de estas amenazas, por lo que ofrece soluciones de defensa innovadoras y adaptables para combatir los ataques de día cero y recuperarse de ellos de forma efectiva.

¿Qué son los ataques de día cero?

En un ataque de día cero, los delincuentes aprovechan una vulnerabilidad de seguridad desconocida en el software o el hardware antes de que se encuentre un parche o una solución. Estos ataques suelen provocar interrupciones generales antes de que la vulnerabilidad pueda detectarse y arreglarse.

Cómo funcionan los ataques de día cero

1. **Detección de una vulnerabilidad:** los hackers identifican fallos de codificación o puertas traseras ocultas en aplicaciones o sistemas de software.
2. **Desarrollo de técnicas de ataque:** se crea malware para aprovechar las brechas de seguridad. Los atacantes pueden usar tácticas de phishing o infectar sitios web con malware.
3. **Ejecución del ataque:** se lleva a cabo el ataque, que pone en riesgo el sistema y, posiblemente, facilita el robo de datos o la interferencia operativa.

Técnicas comunes

- Las descargas involuntarias hacen que los usuarios instalen malware sin ser conscientes de ello.
- Los correos electrónicos de phishing envían enlaces o archivos payload maliciosos para aprovechar vulnerabilidades del sistema.
- Los ataques sin archivos pasan desapercibidos, ya que se ejecutan totalmente en la memoria de un sistema.

Estos vectores superavanzados convierten los ataques de día cero en algo sumamente peligroso, ya que las herramientas de detección tradicionales basadas en firmas no suelen identificarlos.

El impacto en las empresas

Los ataques de día cero conllevan riesgos significativos debido a su imprevisibilidad y al tiempo que se tarda en detectarlos. Las consecuencias pueden ser devastadoras en varios aspectos.

Pérdidas económicas

Un ataque de día cero exitoso puede costar grandes sumas de dinero, desde multas hasta pérdidas de ingresos durante los periodos de inactividad. Por ejemplo, una vulnerabilidad no identificada en una plataforma de comercio electrónico puede desactivar el proceso de compra, lo que afectaría directamente a las ventas.

Daños en la reputación

La percepción de una empresa en el mercado puede verse gravemente afectada. Cuando la información confidencial queda desprotegida o el funcionamiento falla, los clientes pierden su confianza en la compañía.

Interrupción operativa

Las vulnerabilidades sin solventar suelen paralizar los sistemas, lo que se traduce en una reducción de la productividad, retrasos en los proyectos y la pérdida de oportunidades de negocio.

Ejemplo real

Un importante proveedor de servicios sanitarios sufrió un ataque de día cero dirigido a software de dispositivos médicos sin parches. El ataque no solo interrumpió procesos importantes, sino que también expuso datos de pacientes y socavó la confianza de los clientes, y la organización perdió **millones** de dólares en costes de recuperación.

Estadísticas alarmantes

Según un estudio de Ponemon de 2023, el porcentaje de vulneraciones con ataques de día cero es de aproximadamente el 80 %.

Los ataques de día cero representan constantemente más del **70 %** de las brechas de seguridad

Fuente: “M-Trends” de Mandiant de 2024

Combatir los ataques de día cero con Dell Technologies

Dell Technologies ofrece soluciones líderes en el sector para ayudar a las empresas a protegerse activamente contra ataques de día cero, además de facilitar una recuperación rápida en caso de que se produzcan.

Soluciones de seguridad para servidores y almacenamiento

Las soluciones de seguridad para servidores y almacenamiento de Dell ofrecen un mayor nivel de protección:

- Los servidores seguros supervisan y bloquean los intentos de acceso no autorizados.
- Los sistemas de copias de seguridad y recuperación garantizan que, si llega a producirse un ataque, la información esencial se mantenga intacta y siga siendo accesible.

Puntos finales reforzados con Dell Trusted Devices

Los puntos finales son una vía de entrada clave para los atacantes. Dell Trusted Devices integra medidas de seguridad avanzadas para proteger los puntos finales contra amenazas no detectadas.

- **SafeBIOS** protege el firmware contra manipulaciones y garantiza la integridad del sistema en todos los niveles.
- **SafeID** protege las credenciales de los usuarios reforzando los procesos de autenticación.
- **SafeData** cifra los datos confidenciales en tránsito y en reposo, de forma que, si se interceptan o se extraen, los atacantes no pueden aprovecharlos.

Detección preventiva de amenazas con CrowdStrike

CrowdStrike utiliza análisis avanzados e IA para supervisar la actividad de los puntos finales y detectar actividades sospechosas que puedan ocultar ataques de día cero. La detección preventiva de amenazas garantiza una respuesta rápida antes de que se aprovechen las vulnerabilidades y se produzcan daños generales.

Por ejemplo, un proveedor de telecomunicaciones que utilizaba CrowdStrike pudo detectar rápidamente anomalías en el tráfico de red y evitar un potencial ataque de día cero en los servidores de los clientes.

Soluciones Dell PowerProtect

Dell PowerProtect ofrece copias de seguridad sólidas e inmutables y opciones de recuperación aisladas. Así, las empresas pueden restablecer sus operaciones rápidamente y de forma eficiente tras un ataque de día cero, garantizando la continuidad del negocio y protegiendo datos críticos de clientes.

Por ejemplo, una importante cadena de comercio al detalle utilizó PowerProtect para recuperar archivos cifrados que se habían visto afectados por un ataque de ransomware a causa de una vulnerabilidad de día cero. Esta acción evitó un largo periodo de inactividad.

Seguridad de red avanzada y microsegmentación con las redes de Dell PowerSwitch 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.

La importancia de una seguridad de varias capas

Un buen sistema de seguridad requiere más de una solución. Las estrategias de varias capas permiten crear infraestructuras de seguridad integrales combinando innovaciones tecnológicas con el establecimiento de procesos y la participación humana.

Acciones clave para reforzar la defensa

- **Adopte los principios de confianza cero:** verifique todos los intentos de acceso a la red, sean de personas o de dispositivos.
- **Implemente un cifrado avanzado:** utilice protocolos de cifrado para proteger los datos en tránsito y en reposo.
- **Forme a su personal:** ofrezca sesiones de formación detalladas a sus empleados para enseñarles a reconocer ataques de phishing y tácticas de ingeniería social.
- **Pruebe los sistemas con regularidad:** realice pruebas regulares de penetración y análisis de vulnerabilidades para comprobar que las defensas se adapten a las nuevas amenazas.

Dell Technologies combina estas prácticas con sus soluciones de seguridad avanzadas para que las empresas puedan afrontar de forma efectiva los ataques de día cero.

Colaboraciones que refuerzan la ciberseguridad

La colaboración de Dell con **Microsoft**, **CrowdStrike** y **Secureworks**, líderes en el sector, permite ofrecer conocimientos y herramientas de seguridad de última generación a los clientes.

- **Microsoft** se integra fácilmente con las soluciones de Dell, así que garantiza la compatibilidad en todo el sistema, además de ofrecer mecanismos de protección preventiva.
- **CrowdStrike** proporciona inteligencia avanzada sobre amenazas de puntos finales para detectar posibles vulnerabilidades de día cero.
- **SecureWorks** ofrece una supervisión constante y soluciones expertas para poder reaccionar a ataques en tiempo real.

Sacar el máximo partido a Dell Professional Services

Dell Professional Services ofrece una gama integral de servicios de consultoría, implementación y recuperación para ayudar a las empresas a afrontar y mitigar los riesgos relacionados con ataques de día cero. Desde respuestas a incidentes hasta planes de ciberseguridad, Dell fomenta la resiliencia a largo plazo para cualquier organización.

Un futuro a prueba de ataques

Dell Technologies no solo le ofrece tecnología de última generación, sino también una mayor tranquilidad. A través de soluciones pioneras, colaboraciones estratégicas y una experiencia inigualable, Dell ayuda a las empresas no solo a detectar los ataques de día cero más sofisticados, sino también a anticiparse a ellos y a recuperarse en caso de que se produzcan.

Póngase en contacto con Dell Technologies hoy mismo para proteger su empresa, mantener su reputación a salvo y seguir creciendo en un entorno digital imprevisible. Dell fortalece su futuro frente a las amenazas del mañana.

Gracias a sus soluciones y servicios de seguridad diseñados para proteger lo más importante, Dell Technologies inspira confianza y permite que las empresas se mantengan un paso por delante frente a las amenazas de día cero en constante evolución.

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

Más información acerca de las soluciones Dell

Póngase en contacto con un experto de Dell Technologies

Consulte más recursos.

Únase a la conversación con #HashTag.

DELL Technologies