DELL Technologies

DDoS: fortalecer la seguridad y la resiliencia cibernéticas con Dell Technologies

El aumento de la amenaza de ataques DDoS

Los ataques de denegación de servicio distribuido (DDoS) se han convertido en una de las amenazas más comunes y perjudiciales de la era digital. Aprovechando numerosos dispositivos vulnerados, los ataques DDoS inundan ciertos sistemas, servidores o redes con un volumen inmenso de tráfico. Esta oleada incesante ralentiza las operaciones o las detiene, lo que a menudo paraliza a una empresa.

Ninguna organización, por pequeña o grande que sea, es inmune al auge de los ataques DDoS. Como las empresas dependen cada vez más de la infraestructura digital, estos ataques tienen consecuencias devastadoras, que van desde pérdidas financieras hasta daños a la reputación. Dell Technologies reconoce la importancia de este desafío y ofrece soluciones adaptables e innovadoras para reforzar las defensas de las empresas y poder hacer frente al problema.

¿Qué son los ataques DDoS?

Un ataque DDoS busca interrumpir el funcionamiento normal de una red, un servicio o un servidor con una sobrecarga de tráfico de múltiples orígenes. El ataque se lleva a cabo con botnets, que son redes de dispositivos infectados controlados de forma remota por los atacantes.

Cómo funcionan los ataques DDoS

1. **Captación de botnets:** Los ciberdelincuentes infectan miles o millones de dispositivos con malware para formar una botnet con la que atacar a una empresa y hacerla inoperable.
2. **Inundación de tráfico:** Los atacantes envían una avalancha de solicitudes al servidor objetivo a través de las botnets, lo que provoca que el sistema se ralentice, se bloquee o deje de estar disponible para los usuarios legítimos.
3. **Sobrecarga del sistema:** El sistema, superado por el tráfico ilegítimo, se vuelve incapaz de responder a las solicitudes legítimas, lo que provoca interrupciones del servicio o retrasos graves.

Técnicas comunes

- **Los ataques basados en el volumen** envían una avalancha de tráfico para agotar el ancho de banda de una red.
- **Los ataques de protocolo** aprovechan vulnerabilidades en protocolos, como el TCP/IP, para consumir recursos.
- **Los ataques a la capa de aplicación** se dirigen a aplicaciones específicas, como un sitio web o una base de datos, para interrumpir el funcionamiento.

Estos ataques evolucionan constantemente, por lo que son un gran desafío para las empresas que intentan proteger sus operaciones.

El impacto en las empresas

Agotamiento financiero

Un solo ataque DDoS puede costar millones en pérdidas de ingresos, tiempo de inactividad y gastos de recuperación. Incluso unos pocos minutos de interrupción pueden afectar gravemente a las empresas que dependen de las transacciones en tiempo real, como las plataformas de comercio electrónico o los servicios financieros.

Interrupción operativa

Las interrupciones causadas por un ataque DDoS reducen la productividad, retrasan los procesos críticos y dificultan el acceso a los servicios esenciales. En sectores como los de la sanidad o la fabricación, la inactividad operativa puede tener consecuencias de gran alcance.

Daño reputacional

Cuando las interrupciones en el servicio afectan a consumidores y clientes, su confianza disminuye. Los incidentes prolongados o repetidos pueden dañar la reputación de una organización a largo plazo, lo que lleva a la pérdida de clientes y a una menor confianza del mercado.

Ejemplo real

En 2020, ocurrió un caso destacado: una gran entidad financiera fue víctima de un ataque DDoS que desactivó sus servicios de banca digital durante varias horas. Las pérdidas de ingresos directos, combinadas con el desprestigio de la entidad, derivaron en daños por un valor de más de **50 millones de dólares.**

Estadísticas alarmantes

Según el informe sobre ataques DDoS que publicó Zayo Group (DDoS Insights, febrero de 2024), las organizaciones desprotegidas perdían un promedio de **6000 $** por minuto, lo que conllevó un coste promedio de unos **408 000 $** por incidente en 2023. Además, la frecuencia de estos ataques está aumentando, con más de **10 millones de ataques notificados al año**. Estas estadísticas ponen de relieve la necesidad urgente de contar con mecanismos preventivos sólidos.

20,5 millones

Ataques DDoS bloqueados en el primer trimestre de 2025

Fuente: Informe de Cloudflare sobre las amenazas DDoS, 2024

Dell Technologies y la lucha contra los ataques DDoS

Dell Technologies ofrece un conjunto avanzado de soluciones para ayudar a las empresas a prevenir y detectar incidentes DDoS y a recuperarse de ellos.

Puntos finales reforzados con Dell Trusted Devices

Los puntos finales son puntos de entrada cruciales para las amenazas relacionadas con DDoS. La gama de Dell Trusted Devices cuenta con potentes funciones de seguridad integradas en el hardware, como el BIOS seguro y SafeID, que protegen contra el acceso no autorizado y mantienen la integridad del sistema.

Seguridad en los servidores

Las soluciones de servidores de Dell están equipadas con medidas de seguridad integradas, como su tecnología de Dell Trusted Server, que incluye:

- **Raíz de confianza de hardware:** Esta función garantiza que los componentes de hardware del servidor se verifiquen en el momento del arranque, lo que proporciona una capa básica de seguridad contra manipulaciones o modificaciones no autorizadas.
- **Características de seguridad integradas:** Los servidores Dell incluyen unidades de autocifrado y verificación de arranque integral, que protegen contra el acceso no autorizado e infunden confianza en la integridad de los datos.
- **Ciberresiliencia:** El enfoque incluye capacidades para detectar anomalías, vulneraciones y operaciones no autorizadas, lo que permite a las organizaciones recuperarse rápidamente de los ciberincidentes.
- **Protección de datos integral:** Las soluciones de servidor fiables de Dell cuentan con mecanismos de seguridad integrados que protegen los datos en reposo y en tránsito. Esto incluye técnicas de cifrado avanzadas y opciones de recuperación automatizada para garantizar la continuidad del negocio.

Gracias a estas capacidades, los servidores pueden soportar aumentos de tráfico y mantener la estabilidad operativa. Las soluciones de almacenamiento aseguran la disponibilidad y la integridad de los datos críticos durante un ataque, lo que minimiza las interrupciones.

Protección para el almacenamiento

Dell Storage ofrece protección contra los ataques DDoS a través de diversas medidas de seguridad integradas y tecnologías avanzadas diseñadas para minimizar las vulnerabilidades, detectar antes las amenazas y garantizar una recuperación rápida si se produce un ataque. Entre las medidas clave se incluyen las siguientes:

- **Detección proactiva de amenazas:** Las soluciones de almacenamiento de Dell utilizan supervisión inteligente y detección de anomalías basada en IA para identificar patrones de acceso inusuales que podrían indicar un ataque DDoS. Estas herramientas proporcionan información sobre seguridad en tiempo real y pueden activar respuestas automatizadas ante amenazas para mitigar el impacto de un ataque.
- **Arquitectura de raíz de confianza:** Está integrada en los controladores de almacenamiento, garantiza la autenticidad del firmware y evita modificaciones no autorizadas, lo que mejora la seguridad del hardware de almacenamiento y reduce las posibilidades de vulneración durante un ataque DDoS.
- **Autenticación multifactor (MFA) y controles de acceso:** La implementación de MFA y el control de acceso basado en funciones (RBAC) ayuda a evitar el acceso no autorizado a los sistemas de almacenamiento, lo que aumenta la protección contra las amenazas asociadas a los ataques DDoS.
- **Microsegmentación y aislamiento de red:** Al aislar los sistemas de almacenamiento y restringir el acceso entre cargas de trabajo, Dell minimiza los posibles vectores de ataque y protege los sistemas de almacenamiento del movimiento lateral en caso de vulneración.
- **Instantáneas seguras y registros inmutables:** Estas funciones, que proporcionan las soluciones de almacenamiento de Dell, garantizan la integridad de los datos y ayudan a las organizaciones a recuperarse rápidamente de los ataques DDoS. Además, facilitan el análisis forense y la investigación de incidentes, lo que permite a los equipos de TI detectar y analizar los vectores de ataque.
- **Vault de Cyber Recovery:** Soluciones como Dell PowerMax y el vault de PowerProtect Cyber Recovery crean copias de seguridad aisladas que quedan inmutables y protegidas contra los incidentes de ransomware y otros ataques. Estas copias de seguridad se pueden restaurar para garantizar la continuidad del negocio sin riesgo de reinfección.

Gracias a la integración de estas características y tecnologías integrales de seguridad, las soluciones de Dell Storage y de ciberresiliencia ayudan a las organizaciones a defenderse de los ataques DDoS y a garantizar la resiliencia y la seguridad de los entornos de TI.

Supervisión proactiva con CrowdStrike

La supervisión en tiempo real y los análisis avanzados son vitales para detectar patrones de tráfico anormales antes de cualquier incremento. CrowdStrike se integra con el ecosistema de Dell para utilizar análisis de comportamiento e información basada en IA para diferenciar la actividad legítima del tráfico de ataque, lo que permite una corrección rápida.

Dell PowerProtect protege la integridad de los datos

Dell PowerProtect garantiza que los datos críticos permanezcan seguros y accesibles durante un ataque DDoS. La capacidad de hacer copias de seguridad inmutables y los entornos de recuperación aislados permiten a las empresas restaurar los sistemas y minimizar el tiempo de inactividad tras un incidente.

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.

Aplicación en un caso real

Recientemente, una plataforma global de comercio electrónico utilizó las soluciones PowerProtect de Dell junto con las capacidades de detección proactiva para evitar un sofisticado ataque DDoS. Al aislar los sistemas críticos e implementar procesos de recuperación de emergencia, la empresa reanudó todas las operaciones en tiempo récord, lo que mitigó las pérdidas financieras y preservó la confianza de sus clientes.

Enfoque de seguridad multicapa

Las defensas estratificadas y adaptativas son la clave para protegerse de los ataques DDoS. Dell aboga por las siguientes estrategias para complementar sus ofertas tecnológicas:

Pasos clave para fortalecer sus defensas

- **Arquitectura de confianza cero:** Implemente un modelo que consista en no confiar nunca y comprobar siempre para examinar a cada usuario y dispositivo
- **Cifrado avanzado:** Cifre la comunicación a todos los niveles para proteger los datos confidenciales transmitidos durante posibles intentos de ataque.
- **Formación:** Forme al personal en la identificación de actividades sospechosas y el seguimiento de protocolos seguros para evitar vulneraciones involuntarias.
- **Pruebas periódicas del sistema:** Realice comprobaciones rutinarias, como pruebas de penetración y de carga, para evaluar si el sistema está preparado para grandes volúmenes de tráfico.

Estas acciones, combinadas con las soluciones de Dell Technologies, crean un sólido mecanismo de defensa contra amenazas sofisticadas.

Partners que refuerzan la ciberseguridad

Para ampliar sus capacidades, Dell Technologies colabora con líderes del sector, como **Microsoft**, **CrowdStrike** y **Secureworks**. Estas colaboraciones proporcionan más capas de protección, integrando la mejor inteligencia contra amenazas y metodologías de detección avanzadas en toda la infraestructura de Dell.

Ventajas de Dell Professional Services

Más allá de la tecnología, Dell Professional Services ofrece orientación experta a las empresas que se enfrentan a los retos de DDoS. Desde la respuesta ante incidentes hasta las consultas personalizadas sobre arquitectura de seguridad, el equipo de Dell garantiza una recuperación rápida y refuerza las defensas para el futuro.

Un futuro a prueba de ataques

Dell Technologies es más que un proveedor de tecnología; es un partner que se compromete a proteger a su empresa de la amenaza en constante evolución de los ataques DDoS. Con tecnología de vanguardia, una colaboración estrecha e información práctica, Dell ayuda a las empresas a proteger sus operaciones, a mantener la confianza de los clientes y a perseguir activamente el crecimiento.

Dé el primer paso hacia la resiliencia hoy mismo. Póngase en contacto con Dell Technologies para reforzar su empresa frente a las amenazas de DDoS y proteger su futuro.

Dell Technologies permite a las empresas superar los retos de ciberseguridad relacionados con el DDoS, y demuestra que priorizar la seguridad es la clave del éxito en un mundo interconectado.

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.

DELL Technologies