Mitigación de ataque DDos

¿Qué es la mitigación de ataque de DDos? ¿Cómo se disminuye el riesgo? Las empresas de todos los tamaños corren el riesgo de verse afectadas por un ataque DDoS. El objetivo común de estos ataques es hacer que su aplicación o red no esté disponible, pero los ataques reales pueden diferir. Se trata, como no, de uno de las formas más comunes de «tumbar» un servidor o un sitio web, mediante el envío automatizado de miles de consultas o peticiones de recursos desde múltiples Ips en tiempo real.

Volumétrico

Consumen todo el ancho de banda disponible en el enlace de red que conecta una aplicación a Internet u otras redes.

Solicitudes de aplicaciones

Imitan las solicitudes de aplicaciones legítimas, pero intentan sobrecargar los recursos del servidor web, como la CPU o la memoria.

Recursos Computacionales

Intentan agotar los recursos de la infraestructura, como las tablas de estado del firewall, provocando un bloqueo o un rendimiento degradado.

¿Cómo funciona?

Prácticamente todo lo que esté conectado a Internet es un objetivo potencial. Lo mismo ocurre con la fuente de los ataques DDoS: los culpables comunes incluyen servidores web pirateados y dispositivos de «Internet de las cosas» como dispositivos inteligentes , enrutadores e incluso cámaras de

CCTV . Las causas pueden ser accidentales o intencionales. Pero ha crecido una gran industria delictiva que ofrece ataques DDoS como servicio. Existe un mercado para los ataques a sitios, incluidos los competidores que buscan empañar la reputación de otros y aquellos que niegan la presencia en línea por razones políticas.

Un ataque DDoS simplemente funciona así: un atacante utiliza varias máquinas en Internet (o lo que se llama una «red de bots»). Las máquinas envían un alto volumen de tráfico falso al sitio de destino, todo ello en un intento de hacer que los recursos del servidor se sobrecarguen y saquen al servidor online y lo pongan fuera de servicio.

Hay muchos tipos y tamaños de ataques DDoS y pueden ser devastadores independientemente de su tamaño. Incluso un ataque desde un solo sistema (DoS) puede paralizar un sitio, así que considere la despiadada eficiencia de un ataque multisistema a través de DDoS. Un DDoS poderoso puede ser tan pequeño como una solicitud por segundo y aún puede tener efectos devastadores en un sitio web.

Pasos para mitigar un ataque de denegación del servicio

Actualización de la infraestructura de seguridad de su red

En primer lugar, dado que los hackers astutos pueden explotar cualquier laguna, una empresa debe asegurarse de que las lagunas estén cerradas. En otras palabras, los profesionales de TI deben examinar su sistema de seguridad existente y mantenerlo actualizado en todo momento. Eso incluye el firewall, el software anti-malware y antivirus, y las herramientas anti-spam y anti-phishing. Parte del sistema de seguridad es la infraestructura subyacente. Si su infraestructura de red es básica y débil, es hora de actualizarla. Un primer paso es aumentar el ancho de banda. Hacer esto brinda a las redes y servidores la capacidad de manejar picos repentinos en el tráfico, muy similares a los que causan los ataques DDoS. Además, la solución de seguridad multicapa es imprescindible. Esto significa evitar la centralización del centro de datos y colocar componentes de infraestructura en diferentes ubicaciones. De esa manera, si un área es atacada, otras pueden manejar el tráfico regular sin interrupciones.

Adopción de mejores prácticas de seguridad de red

Más allá de los aspectos prácticos de la infraestructura, los piratas informáticos pueden aprovechar cualquier descuido en sus prácticas de seguridad, por lo que deben ser infalibles. Por ejemplo, muchos dispositivos de IoT todavía vienen con contraseñas predeterminadas débiles y una protección general débil. Esto los convierte en objetivos fáciles para los piratas informáticos que buscan expandir sus redes de bots, especialmente porque su número está aumentando rápidamente.

Para evitar errores, los profesionales de TI deben implementar métodos de autenticación multifactor y cambiar todas las contraseñas de vez en cuando. Además, la compartimentación y los controles de acceso son las mejores prácticas, especialmente si una empresa tiene muchos empleados y una alta tasa de rotación. No todo el mundo necesita tener acceso a sus recursos e información más valiosos, y restringir el acceso puede evitar que los atacantes DDoS apunten fácilmente a estos componentes.

Cambio a sistemas en la nube

Durante el año pasado, las empresas han migrado a sistemas en la nube para desarrollar más flexibilidad y resistencia en sus operaciones de TI. Existen beneficios de seguridad, ya que las soluciones basadas en la nube fuera de las instalaciones generalmente tienen parches actualizados y siguen las mejores prácticas de la industria para ser seguras. Desde una perspectiva DDoS, los sistemas en la nube llevan la descentralización al siguiente nivel.

Las empresas pueden considerar un enfoque de múltiples nubes con diferentes proveedores de la nube o una solución híbrida que utiliza soluciones tanto fuera de las instalaciones como locales para la máxima protección DDoS flexible.

Supervisión periódica de la red

Otra forma importante de proteger los servidores de los ataques DDoS es monitoreando el tráfico de la red. Afortunadamente, existen muchas herramientas útiles que brindan monitoreo de red. Herramientas como Datadog Network Monitoring o Paessler PRTG Network Monitor monitorearán el tráfico y enviarán una alerta cuando ocurra un aumento en las solicitudes. Además, es importante comprender las señales de advertencia típicas de DDoS para garantizar una detección y una respuesta rápidas. Los síntomas comunes incluyen un comportamiento de tráfico inusual, ralentización de la red, incapacidad para acceder a las páginas web y una gran cantidad de correos electrónicos no deseados.

Desarrollar un plan de respuesta eficaz

Incluso si implementa todas las soluciones de seguridad descritas anteriormente, pueden ocurrir errores. Si un ataque DDoS realmente golpea un servidor, la mejor arma contra él es un plan de mitigación de DDoS efectivo. Las empresas deben formar un equipo de respuesta DDoS que sea técnicamente competente para ejecutar rápidamente un plan de recuperación. Este equipo debe desarrollar múltiples estrategias para la identificación y mitigación junto con las pautas exactas que el personal debe seguir.

Es posible que se necesiten diferentes estrategias dependiendo de la naturaleza crítica de los diferentes servidores que podrían ser atacados. Un plan de recuperación completo con múltiples opciones de conmutación por error puede mantener una empresa en funcionamiento durante un ataque DDoS.

Desafortunadamente, los ataques DDoS son cada vez más prominentes y no muestran signos de desaceleración. Además de volverse más sofisticados y destructivos, estos ataques ahora pueden ser ejecutados fácilmente, incluso por un hacker con un nivel relativamente bajo de conocimientos técnicos. La

protección adecuada contra los ataques DDoS es imprescindible para las empresas que operan en la economía digital. Mediante la construcción de una infraestructura moderna, la creación de una estrategia de seguridad sólida y el desarrollo de escenarios de recuperación ante desastres, las organizaciones pueden protegerse de los peores daños que pueden causar los DDoS.

Conclusión

Para detener el caos DDoS, las empresas continúan invirtiendo fuertemente en la implementación de las soluciones de mitigación híbridas más avanzadas; sin embargo, los atacantes aún logran eludirlos y crear interrupciones comerciales. El problema subyacente es que las empresas no se aseguran de que cada parte de su postura de mitigación de DDoS esté actualizada, integrada y ejecutando la configuración correcta para su entorno específico para bloquear los ataques DDoS. La implementación de la protección DDoS más eficaz requiere comprender las diferentes capacidades de los componentes de mitigación y cómo pueden satisfacer las necesidades del entorno y los requisitos comerciales.

Leer también: Ataques DDoS en litespeed web server, cómo los maneja; Protegernos de Ataques DDoS; Multicloud: cómo reducir la superficie de exposición a los riesgos de ciberseguridad