Akamai

WHITE PAPER

11 mitos sobre DDoS que no desaparecerán

Los ataques distribuidos de denegación de servicio (DDoS) han aumentado drásticamente de tamaño, escala, así como en su nivel de distribución y sofisticación en los últimos años, lo que se manifiesta en algunos ataques sin precedentes. Desafortunadamente, son muchas las organizaciones que siguen aferrándose a algunas ideas del pasado sobre cómo deben defenderse, y que asumen que sus defensas son suficientes o, lo que es peor, que es poco probable que se conviertan en objetivo. La verdad es que encontramos víctimas de estos ataques en todos los sectores clave, desde los servicios financieros, pasando por el comercio electrónico, y llegando a los videojuegos. De hecho, los ataques a infraestructuras públicas críticas, como la atención sanitaria, la energía y los servicios públicos, la enseñanza y el transporte, han sido motivo de especial preocupación. En 2023, Akamai protegió a un cliente de la región de Asia-Pacífico de un ataque masivo de 900 gigabits por segundo (Gbps). A finales del mismo año, Akamai evitó un ataque de 634 Gbps y 55 millones de paquetes por segundo (Mpps) donde se utilizaba una compleja combinación de vectores de ataque, convirtiéndose en uno de los mayores ataques jamás llevados a cabo contra un cliente de servicios financieros de EE. UU. A ello hay que sumar el mayor ataque DDoS que Akamai ha mitigado hasta la fecha: un ataque distribuido en todo el mundo, de 1,44 Tbps y 385 Mpps que duró casi dos horas. Estos hechos ponen de manifiesto que los ciberdelincuentes siguen atacando los pilares más importantes de la economía.

Aunque la escala de estos ataques puede llevar a algunas organizaciones más pequeñas a creer que tienen pocas posibilidades de convertirse en objetivo de un ataque DDoS, la realidad es que los servicios y las aplicaciones más importantes para la empresa de todos los sectores son blancos fáciles. El aumento del número de hacktivistas con motivaciones políticas e ideológicas, junto con el coste relativamente bajo de los ataques DDoS como servicio que ofrecen los grupos de ciberdelincuentes, como Killnet y Anonymous Sudan, han convertido a casi cualquiera en un posible objetivo. Y las organizaciones no solo deben preocuparse por el ataque inicial. Los agentes maliciosos utilizan los ataques DDoS cada vez más como una cortina de humo para distraer a las personas encargadas de la red y seguridad mientras lanzan ataques DDoS de ransomware simultáneos (RDDoS) u otros ataques malintencionados, como campañas de extorsión triple. Por último, la creciente y alarmante adopción de herramientas de inteligencia artificial para organizar ataques DDoS altamente distribuidos y sofisticados supone un importante desafío defensivo para las empresas y las instituciones públicas que necesitan garantizar una disponibilidad y un rendimiento constantes.

En un panorama en que las amenazas son cada vez más complejas y están cada vez más evolucionadas, lamentablemente siguen existiendo muchos mitos sobre la protección contra DDoS, algunos de ellos incluso fomentados por los proveedores de seguridad. La protección contra DDoS debe ser un principio clave de cualquier estrategia de seguridad, por lo que entender el peligro que suponen estos mitos resulta fundamental para su defensa contra DDoS.

MITO N.º 1

La capacidad total indica la cantidad total de recursos de mitigación disponibles

Aunque la capacidad total es importante, una simple cifra de capacidad de la red puede llevar a confusión si se omiten detalles importantes. Las organizaciones que estén pensando en adquirir soluciones tecnológicas de protección contra DDoS deben preguntarse:

- ¿Cuánta capacidad de red se dedica a consumir tráfico de ataques?
- ¿Cuántos recursos del sistema de mitigación **se utilizan explícitamente** para detener los ataques?
- ¿Cuántos recursos de red y del sistema están disponibles para distribuir tráfico limpio a todos los orígenes de clientes en esa plataforma y a cada uno de los inquilinos concretos?

Estas preguntas son esenciales porque si la capacidad total de la red incluye otros requisitos, como la distribución de contenido, la capacidad real de defensa contra DDoS podría suponer solo una parte de lo que el proveedor proclama.

La capacidad de defensa contra DDoS no solo se limita a la tecnología. En algún momento, si la tecnología deja de funcionar bien, ¿habrá recursos humanos específicos para derivar el problema, gestionar la respuesta a incidentes y ajustar las medidas de mitigación? La mitigación más sólida es capaz de combinar automatización e inteligencia artificial con experiencia humana para ofrecer una protección exhaustiva.

Consejo

Profundice en las diferencias existentes entre la capacidad total de red y la estabilidad de la plataforma de un proveedor, así como la capacidad que tiene para la mitigación de ataques y la distribución de tráfico limpio. Deberían considerarse segmentos distintos. Por ejemplo, debe haber una capacidad concreta para cada finalidad, como el enrutamiento del tráfico de ataque en la red, el bloqueo o la mitigación del tráfico de ataques y la devolución de tráfico limpio al centro de datos.

MITO N.º 2

Con la protección contra DDoS que ofrecen los proveedores de servicios de Internet o los proveedores de servicios en la nube es suficiente

Lamentablemente, son muchas las organizaciones que siguen pensando que la protección que les ofrece su proveedor de servicios de Internet (ISP) es lo único que necesitan. La verdad es que normalmente los ISP solo ofrecen protección frente a DDoS comercial, estándar pero reacondicionada para usar con un ancho de banda limitado. En la infraestructura de ellos y en la suya se usa el mismo hardware, lo que implica una capacidad y unos ciclos de CPU limitados. Los ataques DDoS actuales son tan masivos que pueden desbordar ambas infraestructuras. Los ISP redirigirán todo el tráfico a una ruta nula (o agujero negro) con el fin de evitar daños colaterales a otros recursos de producción. Al hacer esto, las empresas dejan de recibir el tráfico y los servicios legítimos de los usuarios finales, y los atacantes logran su objetivo , al dejar a la empresa inoperativa a todos los efectos prácticos.

Además, aunque los proveedores de servicios en la nube (CSP) a menudo permiten a los clientes establecer sus propios controles y mantener la soberanía sobre su estrategia de seguridad en el entorno de nube del CSP, la mayoría de estos últimos suelen rechazar cualquier responsabilidad y terminan cobrando a los clientes por el tráfico ilegítimo de DDoS. Esto puede suponer un sobrecoste considerable para las víctimas, teniendo en cuenta la escala y el tamaño de los ataques DDoS modernos.

Consejo

Analice detenidamente y negocie las cláusulas de protección contra DDoS con su ISP o CSP. Asimismo, decida si su ISP utiliza un hardware de protección contra DDoS sólido en el entorno local, con función de copia de seguridad en la nube para mitigar este tipo de ataques pequeños pero rápidos en ese entorno local, mientras se hace frente a los ataques volumétricos de gran volumen mediante un servicio de protección contra ataques DDoS en la nube.

MITO N.º 3

Todos los SLA de tiempo de mitigación son iguales

A veces los números pueden llevar a engaño. El tiempo de mitigación (TTM) es un número del que suelen alardear los proveedores de seguridad. El tiempo de mitigación hace referencia a la rapidez con la que se detiene o se bloquea el tráfico malicioso, sin que el tráfico ni los usuarios legítimos se vean afectados. Al parecer, aquí hay bastante margen para la interpretación. Por ejemplo, es posible que un proveedor no califique un aumento del tráfico como un ataque DDoS hasta que haya durado, al menos, cinco minutos consecutivos. Por lo tanto, es posible que el temporizador del acuerdo de nivel de servicio (SLA) no se ponga en marcha hasta que esté sufriendo ya el ataque. Si tenemos en cuenta que la duración media de los ataques es inferior a cinco minutos, resulta lógico entender por qué esto se ha convertido en un problema: significa que el periodo anunciado de 10 segundos de mitigación podría durar realmente más de cinco minutos.

Otros proveedores definen el tiempo de mitigación como la rapidez con la que se puede implementar una regla de mitigación. Aquí no se refleja la detención del ataque ni la calidad o regularidad con la que se activa ese control. Al fin de cuentas, lo que le interesa es el tiempo necesario para que los activos orientados a Internet estén protegidos y vuelvan a funcionar con normalidad, **con el menor impacto posible para los usuarios o servicios legítimos**. Asegúrese de leer atentamente la letra pequeña del SLA de su proveedor.

Consejo

Profundice en los detalles del tiempo de mitigación que figuran en un SLA. Debería reflejar la siguiente ecuación: tiempo real que importa = tiempo de detección del ataque + tiempo de aplicación de controles de mitigación + tiempo de bloqueo/detención del ataque + calidad/regularidad de la mitigación. Seleccione un proveedor que ofrezca un **SLA de cero segundos real** para mitigar los ataques DDoS sin que los usuarios legítimos lo noten.

MITO N.º 4

La redirección del tráfico hacia una ruta nula (o agujero negro) y la limitación de la velocidad son defensas admisibles

La redirección hacia una ruta nula (también conocida como enrutamiento hacia agujeros negros) es una respuesta defensiva muy básica utilizada por algunos proveedores de mitigación de ataques DDoS. Si un activo es objeto de un ataque y la capacidad de dicho ataque pone en riesgo a otros clientes o servicios, el proveedor puede tratar de evitar los daños colaterales al enviar el tráfico de ese recurso a un agujero negro virtual. ¿Eso le resulta útil? Desde la perspectiva de un atacante, la redirección del tráfico hacia agujeros negros significa objetivo cumplido. De hecho, el activo en cuestión está sin conexión. En función de la infraestructura del proveedor, otros clientes también pueden acabar sin conexión o experimentar un rendimiento degradado.

Otra respuesta básica de defensa contra DDoS que ofrecen muchos proveedores de seguridad incluye la imposición de límites de velocidad al tráfico de los clientes como una contramedida dentro de los entornos compartidos. Sin embargo, la reducción del tráfico legítimo entre un 20 % y un 40 % para dar la impresión de que el activo o el servicio sigue funcionando no es la mejor solución para el cliente que sufre un ataque. La limitación de velocidad es eficaz como contramedida secundaria o terciaria cuando se trata de ataques DDoS a las capas 3, 4 y 5. Al hacer frente a ataques DDoS a la capa 7, la limitación de velocidad puede ser más efectiva como primer control, pero siempre es más recomendable confiar primero en la mitigación de firmas. Merece que el 100 % de su infraestructura digital esté protegida eficazmente contra ataques DDoS, independientemente de la capa del modelo de interconexión de sistemas abiertos a la que estos afecten, y no solo el 60 % (o menos).

Consejo

Pregunte a su proveedor con qué frecuencia redirige el tráfico hacia agujeros negros o limita el tráfico en "tiempos de paz" y cuando sufre un ataque. Determine cuándo (en qué condiciones) un proveedor redirige el tráfico hacia agujeros negros y qué criterios deberá cumplir usted para que se restablezcan sus servicios.

MITO N.º 5

No importa quién comparta la plataforma en la nube

Toda organización requiere seguridad. Las empresas controvertidas que atraen ataques frecuentes (por ejemplo, mercados grises como los sitios web de apuestas y contenido para adultos) también necesitan defensas de seguridad contra DDoS. Incluso organizaciones que fomentan las actividades delictivas y los ataques terroristas han adquirido ciberseguridad de proveedores legítimos de servicios en la nube.

Es fácil pensar que esos sitios no le afectan. Sin embargo, si su empresa comparte una plataforma en la nube con una empresa ilegal o que sufre ataques frecuentes, existe una gran posibilidad de que se produzcan daños colaterales. Es posible que los recursos del proveedor estén bloqueados o saturados, lo que dejaría a su organización expuesta.

Consejo

Lea atentamente la política de uso aceptable de un proveedor de seguridad en la nube para confirmar que no compartirá los recursos de la plataforma de seguridad con objetivos de alto riesgo. Repase también los consejos que aparecen tras los mitos 1 y 2 en relación con la capacidad.

MITO N.º 6

Un firewall de aplicaciones web es suficiente para estar protegidos contra DDoS

Los firewalls de aplicaciones web (WAF), que a menudo se integran en el grupo de soluciones de protección de API y aplicaciones web (WAAP), ofrecen una protección eficaz contra DDoS para los ataques a la capa de aplicación (capa 7). Aunque ofrecen cierta protección básica en la capa de red (capa 3) o capa de transporte (capa 4), esta protección no es suficiente para incluir todas las direcciones IP, puertos y protocolos de manera exhaustiva.

Los ataques DDoS se producen con distintas apariencias y formatos, y pueden tener como objetivo las capas de infraestructura (capas 3 y 4), la capa de aplicación HTTP (capa 7) y la infraestructura del sistema de nombres de dominio (DNS). Además, los atacantes a menudo cambian de forma dinámica el tipo de ataque, por ejemplo, empezando por el DNS y, posteriormente, expandiéndose a otras capas o protocolos. La verdadera protección contra DDoS se obtiene con una estrategia de defensa en profundidad que adopte una plataforma de soluciones sólidas, con puntos fuertes y capacidades específicas para ofrecer protección a las capas 3, 4, 7 y del DNS. Cualquier solución por sí sola no será suficiente para cubrir todas las bases, además de que tal vez haga que su organización quede expuesta ante ataques y mayores niveles de riesgo mitigando, sin necesidad, tráfico o servicios legítimos.

Consejo

Asegúrese de que su solución de protección contra DDoS no se incline demasiado a evitar un determinado tipo de ataque DDoS o diseño de implementación. La mejor defensa se obtiene con un único proveedor que proporcione diversas soluciones de protección contra DDoS específicas, que consigan mantener la interoperabilidad y que estén respaldadas por un equipo unificado de servicios de seguridad capaz de ofrecer una respuesta rápida para proteger sus recursos de producción. La situación se vuelve compleja cuando estos activos se encuentran en redes híbridas y entornos alojados en la nube. Los servicios de protección deben ser independientes de la red o del modelo de implementación.

MITO N.º 7

Una plataforma de seguridad integral equivale a una mejor experiencia de seguridad

Algunos proveedores ofrecen una serie de servicios agrupados en una única plataforma en la nube. Aunque esto podría reducir la complejidad técnica a la hora de implementar e integrar controles de seguridad a corto plazo, el hecho de que varios servicios compartan las mismas redes e infraestructura de back-end los haría poder ser objeto de interrupciones de la plataforma, pudiendo sufrir daños colaterales y tener problemas de resistencia si se dañan otras partes del entorno. A menudo, los proveedores de servicios integrales de este tipo sacrifican las funcionalidades debido a las limitaciones de su enfoque de plataforma única.

Una red transparente de soluciones o plataformas de protección contra DDoS de CDN y DNS, diseñadas para resolver problemas técnicos y de seguridad específicos, implica una mitigación y un rendimiento de mayor calidad a escala para optimizar las estrategias defensivas.

Consejo

Recuerde que no es necesario compartir la misma infraestructura para lograr una experiencia de seguridad unificada. En un enfoque de defensa basado en la diversidad se utilizan las arquitecturas subyacentes para ofrecer una experiencia de usuario óptima, así como un servicio de mitigación de alto rendimiento.

MITO N.º 8

No se necesita protección contra DDoS para IPv6

Según Google, aproximadamente el 45 % del tráfico de Internet procede de dispositivos compatibles con IPv6. En términos de ataques DDoS, IPv6 supone algunas mejoras con respecto a IPv4, como un mayor espacio de direcciones y funciones de seguridad integradas como IPsec, pero no protege intrínsecamente contra estos tipos de ataques.

Los ataques DDoS pueden tener como objetivo tanto redes IPv4 como IPv6, saturándolas con un gran volumen de tráfico, aprovechando sus vulnerabilidades o utilizando distintos vectores de ataque independientes de la versión de IP. Los ciberdelincuentes ya han venido utilizando el espacio de IP cada vez mayor de IPv6 para provocar ataques DDoS volumétricos de mayor envergadura. En algunos casos, los atacantes han enviado tráfico a direcciones aleatorias de una red, lo que ha creado una tormenta de transmisiones en la capa de red física y ha acaparado y mantenido ocupados los recursos del router o de la red.

La fragmentación actual entre IPv4 y IPv6 hace que todo sea más complejo, ya que normalmente no podemos asumir que partimos de entornos IPv6 limpios.

Consejo

Para conseguir una protección contra DDoS para IPv6 se necesitan estrategias y tecnologías similares a las de IPv4, entre ellas la supervisión de la red, el filtrado del tráfico, la limitación de velocidad y el uso de servicios especializados de mitigación de DDoS.

MITO N.º 9

No necesita varias capas de defensa

La mayoría de las organizaciones no creen en este mito, aunque a veces desarrollan su estrategia de defensa como si fuera cierto. Al proteger su casa, cerrar con llave la puerta delantera no significa que pueda dejar la puerta trasera y las ventanas abiertas. La verdadera defensa frente a DDoS se consigue creando capas de seguridad que interactúen perfectamente para evitar que los atacantes logren su objetivo a la primera.

La mejor defensa frente a DDoS comienza con un firewall de nube de red que alivie la carga de los firewalls en el Edge de la red. A continuación, un modelo híbrido de protección contra DDoS incluirá protección local basada en dispositivos de hardware frente a ataques de este tipo, breves pero intensos, y recurrirá a la protección basada en la nube dedicada para ataques DDoS volumétricos, complejos y de gran tamaño. También es necesario proteger su infraestructura de DNS con una estrategia por capas similar que incluya el uso de un servicio de proxy capaz de implementar políticas de seguridad de forma dinámica en el Edge, así como añadirle una solución de DNS autoritativo, ya sea en modo primario o secundario. Por último, debe proteger todas sus aplicaciones y API con una solución WAAP definitiva que incluya funcionalidad WAF.

Consejo

Utilice un modelo por capas con las mejores tecnologías y soluciones, junto con diferentes puntos fuertes específicos, para diseñar una estrategia de defensa integral en profundidad que haga que a los ciberdelincuentes les resulte extremadamente difícil lograr los objetivos de sus ataques.

MITO N.º 10

Todos los centros de operaciones de seguridad ofrecen el mismo nivel de asistencia

Muchos proveedores anuncian que disponen de un centro de operaciones de seguridad (SOC) para ofrecer asistencia. Sin embargo, disponer de un SOC de forma ininterrumpida no es lo más importante. Lo que importa es el nivel de servicio y experiencia que puede esperar recibir cuando sus activos sufran un ataque. Debe tener en cuenta las siguientes consideraciones fundamentales al evaluar a los proveedores de mitigación de DDoS:

- ¿Qué tipo de asistencia y análisis recibiría antes, durante y después de un ataque?
- ¿El SOC cuenta con el personal necesario para garantizar que la defensa siga funcionando?
- Si se pone en contacto con el SOC, ¿la persona con la que habla es el analista real que realiza la mitigación o solo la persona de contacto?
- ¿Su proveedor cuenta con profesionales de seguridad con formación en mitigación o son simplemente "policías de tráfico" que dirigen el tráfico a un servicio de mitigación estándar?
- ¿Ofrecen un runbook personalizado?

El SOC de su proveedor de seguridad debe actuar como una extensión de su equipo de respuesta a incidentes para generar valor real.

Consejo

Evalúe la calidad de la asistencia que prevé recibir por parte del SOC del proveedor de servicios. Además de la detección y mitigación de ataques, determine si ofrecen integración y pruebas, resolución de incidentes, análisis posteriores (lecciones aprendidas) y asistencia con el diseño para reducir su superficie de ataque.

MITO N.º 11

Los ataques DDoS usan viejas tecnologías, por lo que será suficiente con la protección más barata

La máxima "nada sale gratis" es probablemente la que mejor se ajuste cuando hablamos de protección contra DDoS. Aunque un precio más bajo puede parecer atractivo, suele haber gastos ocultos.

Algunos proveedores ofrecen un precio bajo, pero restringen la cantidad o el tamaño de los ataques que mitigarán. Si es el objetivo de una gran cantidad de ataques, o de un ataque de gran magnitud, le pedirán que se cambie a un nivel de servicio más alto (y más caro) antes de detener el ataque. Todo esto mientras usted intenta que su negocio vuelva a estar online. Los proveedores conocidos de seguridad frente a DDoS ofrecen a los clientes la flexibilidad de elegir entre protección DDoS "siempre activa" y "bajo demanda", además de permitirles cambiar de una a otra de forma sencilla, para que los costes operativos se mantengan bajos y ofrecer la mejor protección de su clase. Al comparar proveedores y precios, asegúrese de que entiende las contrapartidas y su impacto en su estrategia de seguridad ante DDoS.

Consejo

Antes de firmar, asegúrese de que entiende todo lo que se incluye en el presupuesto.

La seguridad contra DDoS es un asunto complejo y, para garantizarla, se necesitan bastante tiempo y recursos en un panorama actual en constante cambio. Lo que funcionó ayer puede que no funcione ni hoy ni mañana. Mantenerse conectado con sus usuarios finales, clientes y empleados es la base del éxito de su negocio. No hay margen de error ni necesidad de afrontar el alto coste de hacerlo en solitario. Como plataforma de protección contra DDoS más completa, flexible y fiable, Akamai puede ayudarle.

Obtenga más información sobre las soluciones de seguridad contra DDoS de Akamai.

Acerca de la seguridad de Akamai

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado el 24 de octubre.