Akamai

WHITE PAPER

9 mitos sobre la defensa frente a DDoS

En los últimos dos años, se ha duplicado el tamaño de los ataques distribuidos de denegación de servicio (DDoS) y ha aumentado de forma significativa el número y la combinación de los vectores de ataque. En 2020, una organización sufrió un ataque de 809 millones de paquetes por segundo (Mpps), en lo que se convirtió en el mayor ataque de este tipo jamás registrado. Aunque algunas organizaciones pueden creer que son objetivos de bajo riesgo para un ataque DDoS, los servicios y las aplicaciones esenciales de todos los sectores son objetivos muy atractivos y dejan a las empresas expuestas a problemas de tiempo de inactividad y a una reducción del rendimiento si la infraestructura no está protegida.

La protección contra DDoS debe ser un principio clave de su estrategia de seguridad general, por lo que conocer los mitos al respecto puede ser fundamental para su estrategia de defensa.

Hay muchos mitos sobre la protección contra ataques DDoS. De hecho, algunos de ellos los fomentan los proveedores de seguridad.

Mito n.° 1: La capacidad total indica los recursos de mitigación disponibles

Una simple cifra de capacidad de red omite detalles importantes. Las preguntas que se deben responder son las siguientes: ¿Cuánta capacidad de red se dedica a consumir tráfico de ataques? ¿Cuántos recursos del sistema de mitigación se utilizan 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? La capacidad no solo se limita a la tecnología. En algún momento, si las tecnologías no funcionan de manera eficaz o no optimizan la mitigación, ¿qué capacidad humana específica se puede aprovechar para derivar el problema, gestionar la respuesta a incidentes y ajustar las medidas de mitigación?

Consejo: Profundice en las diferencias existentes entre la capacidad total de red y la estabilidad de la plataforma de un proveedor, la capacidad disponible para la mitigación de ataques y la utilización de la distribución de tráfico limpio.

Mito n.° 2: Todos los SLA de tiempo de mitigación son iguales

El tiempo de mitigación debe hacer referencia a la rapidez con la que se detiene o se bloquea el tráfico malicioso, sin que esto afecte al tráfico legítimo ni a los usuarios. Al parecer, 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. Por lo tanto, es posible que el temporizador del acuerdo de nivel de servicio (SLA) no comience hasta que ya hayan pasado cinco minutos del ataque. Eso significa que el periodo anunciado de 10 segundos de mitigación podría durar realmente cinco minutos o más. Otros proveedores definen el tiempo de mitigación como la rapidez con la que se puede implementar una regla de mitigación. A fin de cuentas, lo que le interesa es el tiempo necesario para que los activos orientados a internet vuelvan a funcionar con normalidad. 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 para detectar el ataque + tiempo para aplicar controles de mitigación + tiempo para bloquear el ataque + calidad de la mitigación = tiempo real para detener el ataque.

Mito n.° 3: El bloqueo del tráfico y la limitación de la velocidad son defensas admisibles

El bloqueo del tráfico es una respuesta defensiva muy frecuente entre algunos proveedores de mitigación de DDoS. Si un activo es objeto de un ataque y pone en riesgo a otros clientes, el proveedor puede tratar de evitar los daños colaterales al descartar el tráfico de ese recurso en un agujero negro virtual. ¿Eso le resulta útil? Desde la perspectiva de un atacante, el bloqueo del tráfico significa objetivo cumplido. De hecho, el activo en cuestión está sin conexión. En función de la infraestructura del proveedor, otros clientes pueden acabar sin conexión o experimentar un rendimiento degradado. Por otro lado, muchos proveedores también califican la limitación del tráfico de clientes como una contramedida dentro de los entornos compartidos. Sin embargo, la reducción del tráfico legítimo en un 20 %-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.

Consejo: Pregunte a su proveedor con qué frecuencia bloquea o limita el tráfico en "tiempos de paz" o cuando sufre un ataque. Determine en qué condiciones un proveedor bloquea el tráfico y qué criterios deberá cumplir usted para que se restablezcan sus servicios.

Mito n.° 4: 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 pornografía) también necesitan defensas de seguridad. 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 eso no le afecta. Sin embargo, si su empresa comparte una plataforma de seguridad 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 ya estén bloqueados o saturados, lo que dejaría a su organización expuesta.

Si su empresa comparte una plataforma de seguridad en la nube con una empresa ilegal o que sufre ataques frecuentes, existe una gran posibilidad de que se produzcan daños colaterales.

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.

Mito n.° 5: Una plataforma de seguridad integral equivale a una mejor experiencia de seguridad

Algunos proveedores ofrecen una variedad de servicios agrupados en una única plataforma en la nube, lo que podría significar una reducción de la complejidad técnica para implementar e integrar controles de seguridad a corto plazo. Sin embargo, que varios servicios compartan la misma infraestructura y redes de back-end los deja expuestos a interrupciones de la plataforma, daños colaterales y problemas de resistencia si se dañan otras partes del entorno. A menudo, los proveedores de servicios integrales sacrifican la funcionalidad a causa de las limitaciones del diseño de un enfoque de plataforma única. Una red transparente de nubes de barrido de CDN, DNS y DDoS, diseñadas para resolver problemas técnicos y de seguridad específicos, implica una mayor calidad de mitigación y rendimiento a escala para optimizar las estrategias defensivas.

Consejo: Recuerde que no es necesario compartir la misma infraestructura para lograr una experiencia de seguridad unificada. Unas arquitecturas subyacentes diversas pueden ofrecer tanto una experiencia de usuario uniforme como una mitigación de alto rendimiento.

Mito n.° 6: Una solución local ofrece mayor control

Aunque una solución local permite a las organizaciones realizar sus propios ajustes, el control puede ser ilusorio. El eslabón más débil de cualquier solución local es, con frecuencia, el tamaño de la conexión a internet. A medida que los ataques DDoS aumentan en tamaño y complejidad (multivectoriales), incluso un ataque común de menos de 4 Gbps puede saturar la conexión a internet y denegar el servicio incluso a los centros de datos que cuentan con el mejor hardware local. En el caso de las implementaciones locales, básicamente se están ganando minutos para mitigar los ataques graves en la nube. Dado que el personal de seguridad no solo es escaso, sino que además está muy sobrecargado, las organizaciones externalizan la mitigación de DDoS a plataformas basadas en la nube, en lugar de desarrollar competencias internas para mitigación de DDoS.

Consejo: No puede tener el control si su red, su equipo de TI y el personal de respuesta a incidentes están desbordados. DDoS es un vector de ataque que los expertos en mitigación manejan con más facilidad. Refuerce lo que puede hacer internamente y externalice el resto a los expertos.

Mito n.° 7: No necesita varias capas de defensa

La mayoría de las organizaciones no creen en ello, aunque a veces desarrollan su estrategia de defensa como si fuera cierto. Por ejemplo, piense en el enfoque híbrido. Una organización que busca reforzar su solución de seguridad local puede ampliarla añadiendo una solución basada en la nube del mismo proveedor. La solución integral puede ser cómoda, pero no ofrece necesariamente una defensa en profundidad. Si se desarrollan varias capas de defensa sobre la misma tecnología subyacente, esas capas tendrán las mismas deficiencias y debilidades, dejándole igual de expuesto.

Consejo: Utilice las mejores tecnologías en capas con diferentes puntos fuertes y débiles, de modo que la defensa de una capa cubrirá deficiencias en la otra.

Mito n.° 8: Todos los centros de operaciones de seguridad (SOC) ofrecen el mismo nivel de asistencia

Muchos proveedores dan a conocer la asistencia del centro de operaciones de seguridad (SOC) en sus fichas técnicas. 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 el punto de contacto? ¿Su proveedor cuenta con profesionales de seguridad con formación en mitigación o son "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 9: La protección contra DDoS es integral

Aunque un precio más bajo puede parecer atractivo, podría implicar 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 costoso) antes de detener el ataque. Todo esto mientras usted intenta que su negocio vuelva a estar online. Al comparar proveedores y precios, asegúrese de que entiende las contrapartidas y su impacto en su estrategia de riesgo.

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

Si es el objetivo de una gran cantidad de ataques, o de un ataque de gran magnitud, algunos proveedores le pedirán que se cambie a un nivel de servicio más alto (y más costoso) antes de detener el ataque. Todo esto mientras usted intenta que su negocio vuelva a estar online.

La seguridad DDoS es compleja, requiere mucho tiempo y está en constante evolución. Mantenerse conectado con sus clientes, consumidores y empleados es la base de su negocio. No hay margen de error ni necesidad de afrontar el alto coste de hacerlo en solitario. Como plataforma de distribución en la nube de mayor tamaño y confianza para la seguridad web, Akamai puede ayudarle. Para obtener más información, visite www.akamai.com/secureapps.

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com, blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado el 20 de diciembre.