7 consideraciones fundamentales para elegir un proveedor de seguridad en la nube

Para mantener sus datos seguros, debe aplicar un enfoque avanzado a la ciberseguridad. Descubra cómo puede aumentar su infraestructura in situ existente con medidas de seguridad en la nube que refuercen la seguridad web.

¿Qué es la nube y por qué es importante?

La nube es una red de servidores que alojan datos, software y servicios. Normalmente, a los servicios en la nube se accede a través de Internet, en vez de utilizar un centro de datos local.

Las empresas dependen cada vez más de la nube para la seguridad cibernética, principalmente por dos razones:

1. El cambiante panorama de las amenazas hace que se necesiten mayor escalabilidad, precisión, experiencia e inteligencia colectiva. Estos recursos están fuera del alcance de la mayoría de las organizaciones internamente.
2. Las aplicaciones de mitigación de hardware in situ y los centros de datos empresariales presentan limitaciones importantes a la hora de proteger frente a ataques distribuidos de denegación de servicio (DDoS) y ataques web.

Cuestión de números: un ejemplo real

Los ataques reales mitigados en la plataforma de Akamai confirman la importancia de la escalabilidad. Uno de los peores ataques DDoS mitigado por Akamai alcanzó los 623 Gigabits por segundo (Gbps) y estaba dirigido a un solo cliente. Dicho esto, el tamaño medio de los ataques DDoS observado en 2016 fue de poco más de 5 Gbps.

Incluso si su hardware de mitigación de DDoS alcanza una capacidad superior a los 100 Gbps, seguramente no sea suficiente. Un ataque DDoS de un tamaño medio de 5 Gbps es capaz de saturar rápidamente la mayoría de canales de red, haciendo inservible cualquier solución basada en aplicaciones que tenga en su centro de datos.

En definitiva, resulta un blanco fácil para los ciberataques maliciosos.

Elegir la solución idónea de ciberseguridad basada en la nube: varias capas de protección, tecnología de primer nivel y conocimiento de los recursos

Es improbable que un solo software, hardware o servicio unidimensional pueda proteger de forma efectiva frente a ciberataques. La mejor protección la proporcionan los enfoques de varias capas que combinan soluciones basadas en la nube con recursos humanos cualificados.

Estos son los siete factores principales que debe tener en cuenta a la hora de elegir un proveedor de seguridad en la nube:

1. Escalabilidad y capacidad

El actual panorama de las amenazas exige disponer de una escalabilidad extrema y, en consecuencia, adoptar soluciones de seguridad basadas en la nube. Sin embargo, puede resultar difícil determinar cuál es la escalabilidad necesaria. Muchos proveedores afirman tener capacidad para hacer frente a los mayores ataques DDoS, pero esto no siempre es cierto. Es necesario ir más allá de los números que muestre el proveedor para entender realmente si esa capacidad que afirma tener estará disponible cuando usted lo necesite.

2. Soluciones flexibles, adaptables y personalizables

Barrido de DDoS frente a servicios de seguridad basados en redes de distribución de contenido (CDN, por sus siglas en inglés): ¿qué solución o combinación de soluciones es más adecuada para su empresa? Tenga en cuenta que la distribución regional de los centros de barrido puede afectar al rendimiento, por lo que es importante preguntar por las ubicaciones exactas antes de optar por un proveedor.

3. Precisión

Comparar la precisión que cada proveedor sostiene que ofrece (en lo que respecta, por ejemplo, a falsos positivos o falsos negativos) no es tarea sencilla. No tiene sentido basarse únicamente en los números, a menos que se apliquen los mismos criterios. Muchas veces los proveedores muestran los altos niveles de precisión obtenidos en un test realizado por una empresa externa, sin indicar que todos los demás proveedores han obtenido también buenas calificaciones. En conclusión, asegúrese de no comparar peras con manzanas.

4. Inteligencia colectiva

Los proveedores basados en la nube afirman a menudo que proporcionan inteligencia colectiva, pero, en realidad, la inteligencia útil solo puede proceder de un enorme universo formado por clientes de todos los tamaños, muchas redes y un megatráfico. Este tipo de inteligencia y la investigación constante de amenazas permite a Akamai mantener el conjunto de reglas Kona continuamente actualizado y aprovechar los incidentes detectados en un solo cliente para proteger a todos los demás.

5. Reputación de IP

Las direcciones IP se evalúan teniendo en cuenta el comportamiento pasado, como los ataques DDoS, los ataques web o la actividad de escaneo o extracción de información. La visibilidad sin precedentes que tiene Akamai sobre el tráfico web, su heurística avanzada y los algoritmos que aplica generan una puntuación de reputación de gran precisión para cada dirección IP que pasa por la plataforma.

6. Tiempo de mitigación garantizado

Debe buscar acuerdos de nivel de servicio (SLA) que incluyan de forma específica la velocidad y calidad de la mitigación. Un SLA de tiempo de respuesta únicamente garantiza que el proveedor empezará a indagar el ataque rápidamente. No determina el tiempo que tardará en mitigar el ataque una vez que empiecen a investigarlo.

7. El factor humano: comparación de centros de operaciones de seguridad (SOC)

Los SOC están formados por el personal que le atenderá cuando sufra un ataque. La calidad del servicio que recibe está directamente relacionada con la calidad de estos centros. Pidiendo la información correcta, conseguirá comparar de forma más precisa dos centros de operaciones de seguridad distintos. Averigüe cuánta gente trabaja en el SOC, con cuántas instalaciones cuentan y cómo organizan los turnos de trabajo. Por ejemplo, el SOC de Akamai es una red global formada por cinco centros y 150 expertos que gestionan los problemas de seguridad a nivel técnico y organizativo. Nuestro SOC mitiga más ataques que nadie y desde hace más tiempo, nada menos que 12 años.

Conclusiones

El enfoque ideal para la seguridad en la nube consiste en superponer las mejores tecnologías, una sobre otra. Esto ofrece múltiples capas de defensa con distintos puntos fuertes y débiles, lo que hace que a los atacantes les resulte más difícil penetrar en sus datos y aplicaciones.

Una seguridad multicapa auténtica, que sería el enfoque recomendado del sector, implica incorporar tecnología punta basada en la nube, como la de Akamai. Nuestra nube de seguridad puede complementar cualquier solución in situ que ya tenga.

Obtenga más información en nuestro ebook gratuito,

Why Cloud: The Buyer's Guide to Cloud Security" (¿Por qué la nube? Guía de seguridad en la nube para compradores) ▸

Akamai FASTER FORWARD

Como líder mundial en servicios de redes de distribución de contenido (CDN, por sus siglas en inglés), Akamai ofrece a sus clientes una Internet más rápida, fiable y segura. Gracias a sus soluciones avanzadas de rendimiento web y móvil, seguridad en la nube y distribución de contenido, Akamai está revolucionando la manera en que las empresas optimizan las experiencias de clientes, empresariales y de entretenimiento desde cualquier dispositivo y desde cualquier lugar. Para obtener más información sobre cómo las soluciones de Akamai y su equipo de expertos en Internet están ayudando a otras empresas a avanzar más rápido, visite www.akamai.com o blogs.akamai.com, y siga a @Akamai en Twitter.

Akamai tiene su sede central en Cambridge, Massachusetts (Estados Unidos), con operaciones en más de 57 oficinas de todo el mundo. Nuestros servicios y reconocida atención al cliente permiten a las empresas ofrecer una experiencia en Internet incomparable a sus clientes de todo el mundo. Podrá encontrar las direcciones, números de teléfono e información de contacto de todas nuestras oficinas en www.akamai.com/locations.