Akamai

WHITE PAPER

Proteja su empresa contra ataques avanzados

La complejidad de los entornos de TI ha crecido en los últimos años, lo que ha hecho que los ciberataques evolucionen para adaptarse a las nuevas vulnerabilidades. El número de aplicaciones, API, microservicios y componentes crece constantemente, lo que está transformando la manera de desarrollar su actividad online. Pero, lamentablemente, estos avances vienen acompañados de nuevas vulnerabilidades y superficies de amenaza que los atacantes pueden explotar. Las soluciones de ciberseguridad deben abordar tanto las amenazas internas (protección de los datos propios) como externas (bloqueo de los ataques de ransomware, DDoS o agotamiento de recursos, por ejemplo).

Esto lo sabemos de primera mano porque los investigadores de Akamai analizan, de media, 788 TB de datos diariamente. Con el conocimiento adquirido, actualizamos continuamente nuestros productos para protegerles a usted y sus usuarios contra los atacantes más peligrosos y las campañas más avanzadas, incluso cuando los propios ataques evolucionan con el tiempo.

¿Cuáles son los ataques más dañinos que pueden afectar a su empresa y cómo debe prepararse para hacerles frente?

El ransomware sigue al alza

La pérdida de acceso a sus datos y a los de sus clientes es una de las mayores amenazas a las que se enfrenta su empresa. Entre el primer trimestre de 2022 y el primer trimestre de 2023, la cantidad de ataques de ransomware aumentó un 143 % en todo el mundo; en ellos, los atacantes aprovecharon vulnerabilidades de día cero y de primer día, según el informe de Akamai El ransomware en movimiento. Por suerte, puede disminuir la probabilidad y el impacto de los ataques avanzados a través de la segmentación.

Mientras que la segmentación es un enfoque arquitectónico que divide una red en segmentos más pequeños con el fin de mejorar el rendimiento y la seguridad, la microsegmentación es una técnica de seguridad que le permite fraccionar de manera lógica la red en segmentos que se corresponden con cargas de trabajo individuales. De este modo, los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único.

Akamai Guardicore Segmentation, que forma parte de la plataforma Akamai Guardicore para una seguridad Zero Trust, detiene los ataques en todos sus sistemas esenciales, lo que evita que se propaguen por sus activos (tráfico este-oeste) y además mejora la capacidad de respuesta y recuperación. De esta manera, le protege contra los daños a la reputación y las pérdidas de datos y de ingresos que provocan las filtraciones.

Al tratarse de una solución de microsegmentación sin agente, la plataforma Akamai Guardicore se implementa de manera rápida y sencilla, sin necesidad de realizar cambios físicos en su red ni de preocuparse por la ubicación de sus servidores y dispositivos. La plataforma genera una visión interactiva de todas las conexiones de su red, ayudándole a superar uno de los principales obstáculos de la implementación: la falta de visibilidad. Además, Akamai permite abordar activamente los cuellos de botella de rendimiento y los requisitos de cumplimiento, así como aplicar políticas para los diferentes tipos de infraestructura. Gracias a ello, tendrá una amplia visibilidad y podrá llevar un control detallado de todos sus entornos desde una sola plataforma.

Akamai ofrece una visibilidad inigualable del tráfico online a través de su red global ampliamente distribuida. Y la plataforma Akamai Guardicore aprovecha esta posición privilegiada para ofrecer una visibilidad detallada de su entorno, sus recursos tecnológicos, el acceso y los flujos de red. Con esta información en tiempo real, tendrá la tranquilidad de que su actividad empresarial no se verá interrumpida.

Aplicaciones y API bajo ataque

¿Cuántas aplicaciones utiliza su empresa? Probablemente más de las que se imagina. De media, las empresas utilizan más de 1000 aplicaciones. Asimismo, la gran dependencia de las API para casi cualquier transacción online y la creciente adopción de arquitecturas basadas en microservicios hacen que estas aplicaciones sean cada vez más complejas. Por desgracia, la presión de crecer rápidamente a través de la innovación a menudo lleva a las empresas a publicar aplicaciones antes de que su seguridad se haya probado rigurosamente, lo que supone un mayor riesgo para todo el ecosistema.

El reciente informe sobre el Estado de Internet de Akamai ha revelado que el 29 % de los ataques globales se dirigen a las API, que son el principal motor de la transformación digital. En Europa, Oriente Medio y África, la proporción fue de poco más del 47 %. Las API son un vector de ataque común para ciberdelincuentes que utilizan tanto técnicas tradicionales como específicas para API. También deben tenerse en cuenta los ataques distribuidos de denegación de servicio (DDoS), los de bots y los multivectoriales.

Al defender sus aplicaciones web con Akamai App & API Protector, estará protegiendo su flujo de trabajo, sus usuarios y su negocio frente a la actividad maliciosa y el fraude. Esta herramienta incluye protecciones de firewall configurables que pueden absorber los ataques dirigidos a la capa de la aplicación, incluidos aquellos lanzados a través de API. Con visibilidad en tiempo real del tráfico de bots, puede investigar los análisis web sesgados, evitar las sobrecargas de origen y personalizar los permisos para conceder acceso a bots externos sin obstrucción.

Pero volvamos a la pregunta original: ¿qué pasa si no conoce todas sus aplicaciones y API? La visibilidad es, nuevamente, la clave: Akamai API Security identificará todas sus API, evaluará los niveles de riesgo y responderá a los ataques. De esta manera, se impide que los atacantes accedan a sus datos, carguen archivos maliciosos en los servidores y ocasionen sobrecargas con picos de tráfico.

¿Sabía que...?

Los ataques DDoS aumentaron un 50 % entre 2021 y 2023

Más del 60 % de los ataques DDoS en 2023 tenían un componente de DNS

Protéjase contra ataques DDoS y de agotamiento de recursos

Una de las amenazas online más importantes y conocidas es el ataque distribuido de denegación de servicio (DDoS). Desde que existe Internet, ha habido ataques DDoS y su impacto no hace sino evolucionar con el resto de avances tecnológicos. En los últimos años, los ataques DDoS han aumentado de tamaño, duración y sofisticación, con múltiples vectores y destinos de ataque. La cantidad de ataques DDoS altamente volumétricos se incrementó en un 50 % entre 2021 y 2023. Y más del 60 % del total afectó también a los sistemas de nombres de dominio (DNS) en 2023.

Incluso las empresas más grandes pueden verse afectadas por botnets hostiles que interrumpen el servicio para millones de clientes y cortan de raíz la actividad comercial. Los ciberdelincuentes con grandes recursos, los Estados nación y los hacktivistas con motivaciones geopolíticas utilizan botnets amplias y distribuidas para colapsar no solo las empresas más grandes, sino también instituciones públicas esenciales que van desde escuelas y hospitales hasta aeropuertos y proveedores de servicios. Los ataques DDoS y de agotamiento de recursos más dañinos se dirigen a todas las capas, puertos, protocolos de las instituciones y empresas, e incluso al sistema DNS.

Proteger una infraestructura contra ataques DDoS requiere de inteligencia contra amenazas en tiempo real. Los datos que recopilamos se utilizan para potenciar el rango de acción de Prolexic, nuestra solución de protección y mitigación contra ataques DDoS. La herramienta, capaz de proteger la infraestructura digital subyacente a las aplicaciones y experiencias digitales de una empresa, detiene los ataques en todos los puertos y protocolos, ya sea en la nube, en el entorno local o en ambas ubicaciones, antes de que afecten a su empresa.

En los últimos años, se ha producido un resurgimiento significativo de los ataques de agotamiento de recursos dirigidos a la infraestructura DNS. El sistema DNS es la base de la presencia online de una empresa. Si este sistema falla, la organización pierde la capacidad de operar en Internet. Edge DNS y Shield NS53 de Akamai reducen el tráfico de agotamiento de recursos DNS en el Edge y hacen que solo las consultas de DNS legítimas lleguen al origen del cliente.

Desde hace mucho tiempo, la defensa contra ataques DDoS es un requisito esencial para las empresas online, ya que el tamaño de los ataques se duplica cada dos años, con el consiguiente aumento de la complejidad. Para evitar la pérdida de ingresos y de la confianza del cliente, es necesario proteger todos los puntos de fallo potenciales.

¿Qué pasa cuando se produce un ataque?

Sin duda, si tiene presencia digital, en algún momento será el objetivo de un ataque. Uno de los propósitos de toda estrategia de seguridad es proteger antes de que se produzcan los ataques. Por eso se refuerza la seguridad de los recursos esenciales para disuadir a los atacantes y se mejora la visibilidad de la red para detectar los ataques desde el primer momento.

Pero ¿qué pasa si se produce un ataque de día cero, por ejemplo? Aquí es donde entra en juego el análisis de comportamiento, un aspecto fundamental para soluciones como Akamai App & API Protector.

Akamai combina soluciones altamente automatizadas con inteligencia artificial y la experiencia de más de 225 agentes del centro de control de operaciones de seguridad para proteger los datos, la infraestructura y las experiencias digitales de los usuarios finales.

Akamai revisa más de 13 billones de consultas de DNS al día y bloquea más de 12 000 millones de ataques a firewalls de aplicaciones web cada trimestre. Tenemos gran visibilidad del panorama gracias a lo que vemos con nuestros clientes y estos análisis de los ataques nos permiten ser más fuertes. En Akamai utilizamos esta inteligencia contra amenazas para hacer que nuestras soluciones sean más reactivas y eficaces.

No importa si todavía no utiliza las soluciones de seguridad de Akamai; si está sufriendo un ataque, puede ponerse en contacto con nosotros a través de nuestra línea directa para ciberamenazas. Un experto en seguridad le llamará con los pasos a seguir para mitigar el ataque.

Seguridad dondequiera que su empresa se conecte con el mundo

Igual que la muerte y los impuestos, los ciberataques son algo inevitable en la vida. No obstante, puede proteger su empresa y a sus clientes con soluciones de seguridad que utilizan inteligencia contra amenazas actualizada, obtener una gran visibilidad de sus aplicaciones y redes, y adaptarse al panorama de amenazas.

Akamai protege la experiencia de sus clientes, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. Gracias a la visibilidad de amenazas que tenemos en nuestra plataforma global, nuestra amplia cartera de soluciones ofrece una fiabilidad sin igual, para que pueda adelantarse a las amenazas y adaptarse rápidamente al cambiante panorama de seguridad.

Más recursos

Conozca los cinco pasos que debe seguir para romper la cadena de exterminio del ransomware

Desarrolle su estrategia de nube híbrida mientras se defiende de los ataques DDoS

Defienda los componentes básicos de su empresa con una seguridad de API adecuada

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. 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 en junio de 2024.