Historia de cliente de Akamai

La empresa de telecomunicaciones más importante de Asia protege las API de las amenazas

La empresa ha logrado obtener visibilidad de todas las API de su infraestructura y protegerlas

Detección de API no gestionadas

Protección de API mejorada

Protección de datos confidenciales

Con el aumento del número de dispositivos móviles, el sector de las telecomunicaciones de Asia empezó a invertir grandes cantidades en el desarrollo de nuevas tecnologías y la expansión de redes para satisfacer la demanda de los clientes de disponer de mejores servicios digitales. Entre bastidores, las API proporcionan:

- La conectividad necesaria para transformar el sector de las telecomunicaciones, además de acelerar los procesos de los equipos de DevOps
- La base para proporcionar servicios de telefonía móvil, acceso a Internet y otros productos de telecomunicaciones a clientes de todo el continente
- La capacidad de ofrecer soluciones más personalizadas y, en última instancia, mejorar la experiencia del cliente

Una de las principales empresas de telecomunicaciones de la región vio la gran oportunidad que ofrecían las API, específicamente para ofrecer nuevas soluciones digitales de voz y datos. Por otro lado, a medida que la era del 5G se acercaba, la empresa empezó a mirar más allá de la telefonía y fijó sus objetivos en el big data, la IA, el Internet de las cosas (IoT) y otras aplicaciones digitales emergentes. Sin embargo, también era consciente de que al tiempo que las API proliferaban, también lo hacían los riesgos que conllevaban. Al haber presenciado otros grandes proveedores de telecomunicaciones sufrir los efectos de ataques a las API en 2022 y 2023, la empresa se puso en contacto con Noname Security (ahora una empresa de Akamai).

Telecommunications Company

Ubicación

Asia

Sector

Operador de red

Solución

Akamai API Security

Akamai

Necesidad de obtener visibilidad de todas las API y sus riesgos

Como ocurre en muchas empresas, la falta de visibilidad de las API y sus riesgos es un problema frecuente de los equipos de seguridad. Según nuestra investigación, solo 4 de cada 10 organizaciones con inventarios de API completos saben cuáles de sus API devuelven datos confidenciales. Gracias al módulo de detección de nuestra solución de seguridad de API, descubrimos que nuestro cliente de telecomunicaciones se había enfrentado a un reto similar.

Antes de trabajar con Akamai, los controles de seguridad de API del cliente consistían principalmente en una plataforma de gestión de API heredada y un firewall de aplicaciones web (WAF). Desde el punto de vista de la seguridad de las aplicaciones y la distribución de API, esto tenía sentido. Sin embargo, ninguna de las dos soluciones lograba proporcionar el nivel necesario en cuanto a controles de seguridad y capacidad de observación para proteger de forma integral las API de los métodos de ataque actuales. La razón principal es que no todas las API se enrutan a través de un proxy, como un WAF o una puerta de enlace de API, y estas API no gestionadas son objetivos atractivos para los atacantes.

Incluso con una auditoría precisa de su inventario de API, la empresa aún necesitaba otras funciones para proteger las API durante su funcionamiento habitual de operación y gestión de las solicitudes. En pocas palabras, sería inviable que el equipo de seguridad de una organización identificara los comportamientos maliciosos de su entorno de forma manual.

Hay cientos, si no miles, de terminales de API que deben protegerse en tiempo real. Las soluciones de seguridad de aplicaciones que se utilizan habitualmente no pueden seguir el ritmo de todas las llamadas a las API en el entorno de un cliente. Si no se cuenta con las funciones de protección del tiempo de ejecución de API adecuadas, el entorno de TI de una empresa podría ser vulnerable a los ciberataques.

Soluciones para ver todas las API y protegerse frente a las amenazas

Durante la primera fase de la colaboración, se realizó una implementación piloto para localizar las API internas de la empresa, evaluar las configuraciones y comprender los tipos de datos que pasan por ellas. El cliente quedó inmediatamente impresionado con la velocidad de detección, la precisión de los resultados del inventario y la exposición de datos confidenciales que identificó la herramienta.

Debido a los resultados del proyecto piloto, el cliente decidió ampliar el alcance de la plataforma de seguridad de API de Noname (ahora parte de Akamai API Security) a todas sus API internas y externas. Este ejercicio también reveló más API de producción ocultas, así como las amenazas más inminentes a las que se enfrentaban.

Descubrimos que el cliente necesitaba una defensa más sólida contra las principales vulnerabilidades de seguridad para proteger sus API frente a futuros ataques. Gracias a Akamai API Security, actualmente el cliente puede detectar anomalías de comportamiento sospechosas y activar protocolos de respuesta a incidentes en tiempo real. De esta forma, una organización no depende de registros de acceso ni de informes tardíos para obtener información para su proceso de corrección. Una vez que se detectan comportamientos sospechosos con Akamai API Security, se notifican a la puerta de enlace de API del cliente, al sistema de gestión de información y eventos de seguridad (SIEM) y a otros motores de seguridad de la información para que todo el equipo de seguridad esté al tanto. El cliente puede elegir que su personal mitigue las amenazas de forma manual, semiautomática o totalmente automática, en función del caso de uso y la gravedad de la vulnerabilidad.

| Publicado en septiembre de 2024