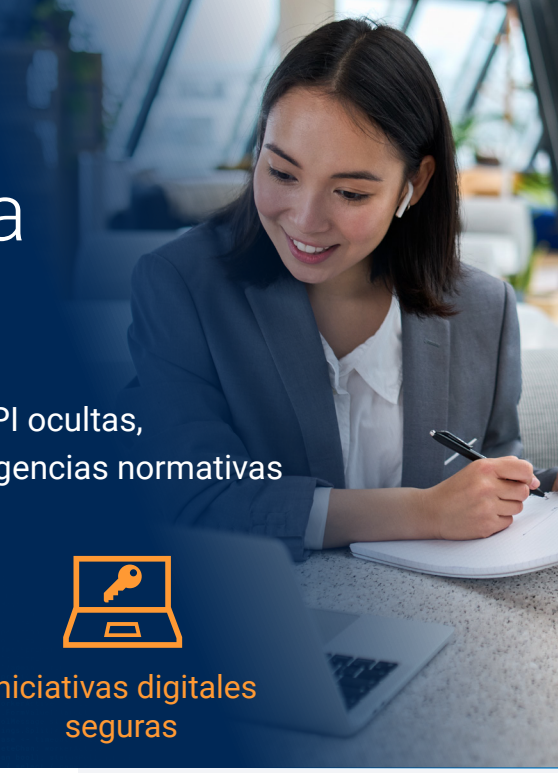
Historia de cliente de Akamai

Entidad financiera detecta y protege las API



Un banco protege sus iniciativas digitales detectando las API ocultas, evaluando y mitigando los riesgos y cumpliendo con las exigencias normativas

Visibilidad completa

Mejora del nivel de seguridad

Iniciativas digitales seguras

El sector de los servicios financieros está adoptando rápidamente la transformación digital para seguir siendo competitivo en un mercado en constante evolución. Gracias al uso de tecnologías como la inteligencia artificial y el análisis de big data, las instituciones financieras pueden ofrecer productos innovadores, reducir costes y proporcionar servicios más personalizados y eficientes a sus clientes.

No obstante, la transformación digital conlleva al mismo tiempo un mayor riesgo de ciberataques. Para combatir este problema creciente, la ciberseguridad es ahora una parte esencial de cualquier estrategia de transformación digital. Las empresas de servicios financieros deben asegurarse de que sus sistemas sean seguros y resilientes para proteger los datos y activos de sus clientes frente a los agentes maliciosos.

Uno de los principales bancos comerciales de Asia recurrió a Noname Security (ahora una empresa de Akamai) para reforzar su estrategia de seguridad de API. Las vulneraciones de seguridad de las API han alcanzado niveles alarmantes: Tech Wire Asia señala que "hoy en día, hasta 1 de cada 13 incidentes cibernéticos pueden atribuirse a la poca seguridad de las API". También recalca que "las vulnerabilidades de las API cuestan a las empresas hasta 75 000 millones de dólares al año".

Así, si consideramos que nuestro cliente tiene más de 700 000 millones de dólares en activos totales, más de 5000 clientes corporativos y una gran reputación a nivel mundial en el sector de la gestión patrimonial, era imprescindible abordar todas las vulnerabilidades de las API lo antes posible.

Financial Services

Ubicación

Asia

Sector

Servicios financieros

Solución

Akamai API Security

Akamai

Necesidad de una mayor visibilidad de las API y sus riesgos

La institución ya había implementado una plataforma de gestión de API para la autenticación y el control del tráfico, pero había dudas sobre su capacidad para evitar el abuso de las API y los ciberataques. Aunque las puertas de enlace de API proporcionan controles de seguridad de API básicos muy necesarios, lamentablemente no son suficientes para proteger adecuadamente a las organizaciones frente a las amenazas específicas de las API.

Por ejemplo, la autorización a nivel de objeto comprometida, a menudo referida como BOLA por sus siglas en inglés, aparece como tráfico normal de API en las puertas de enlace. Esta falta de contexto entre las solicitudes y las respuestas de API permite que los ataques BOLA pasen sin ser detectados y accedan a servicios de back-end esenciales. Este defecto no solo puede dejar a las organizaciones vulnerables a los ataques BOLA, sino que también puede abrir la puerta a otras amenazas y al abuso de la lógica empresarial.

Otra limitación de la visibilidad tenía que ver con la precisión del inventario de API. Al igual que la mayoría de las grandes organizaciones, el banco tenía problemas relacionados con la presencia de API desconocidas en su entorno. La realidad es la siguiente: las empresas gestionan miles de API, muchas de las cuales no se enrutan a través de un proxy, como una puerta de enlace de API. A estas API se las conoce como "no autorizadas" o "zombis", y es probable que las implementaran antiguos empleados antes de que la organización se tomara en serio la seguridad de API. En cualquier caso, la puerta de enlace de API del banco no podía verlas, por lo que era muy fácil subestimar el verdadero número de API que tenían.

Superar el reto de seguridad de API

La organización implementó la completa plataforma de seguridad de API de Noname (ahora parte de Akamai API Security) que incluía soluciones para la gestión de la situación de las API, la protección del tiempo de ejecución y la realización de pruebas en el entorno. El nivel de seguridad del cliente mejoró exponencialmente, ya que ahora es capaz de detectar y corregir vulnerabilidades para uno de los vectores de amenaza menos conocidos del mundo.

Ahora, las API desconocidas se pueden detectar y examinar en la plataforma, lo que otorga una visibilidad completa y permite mitigar los riesgos. La institución ha reducido drásticamente la proliferación de API y ha mejorado sus niveles de cumplimiento, ya que Akamai API Security clasifica los datos confidenciales para ayudar a cumplir normativas como el RGPD y la HIPAA, entre otras.

El banco también tiene ahora la capacidad de detener los ataques en tiempo real y proteger los activos de datos de los clientes. La solución de protección del tiempo de ejecución detecta y prioriza de forma inteligente las amenazas potenciales mientras supervisa continuamente la actividad de las API. Gracias a la integración con firewalls de aplicaciones web, puertas de enlace de API, herramientas de gestión de eventos e información de seguridad, sistemas de gestión de servicios de TI y otras soluciones de flujo de trabajo, nuestra plataforma permite la corrección de amenazas de forma manual, semiautomática o automática.

Resultados

Las API se han convertido rápidamente en el vector de ataque preferido de los hackers, y el número de ofensivas no parece que vaya a reducirse. Por ejemplo, en 2022 observamos "un crecimiento del 257 % en el número de ataques contra los servicios financieros respecto al año anterior". No obstante, la empresa de servicios financieros estará preparada para no convertirse en una estadística más y defenderse de esta tendencia gracias a Akamai API Security. En particular, los equipos de seguridad del cliente comprenderán mejor los peligros que presentan las API y podrán crear sistemas aún más seguros.

 | Publicado en agosto de 2024