Historia de cliente de Akamai

Un importante banco de EE. UU. protege el tráfico de API y obtiene visibilidad

Mantiene un estricto cumplimiento normativo con una visibilidad sin precedentes sobre su superficie de ataque de API

El sector bancario ha experimentado una importante transformación en los últimos años, impulsada por la adopción de interfaces de programación de aplicaciones (API). Esta proliferación de API ha permitido a los bancos aprovechar nuevas oportunidades, mejorar las experiencias de los clientes e impulsar el crecimiento empresarial.

Las API han desempeñado un papel crucial a la hora de permitir una integración perfecta entre los diferentes sistemas y aplicaciones dentro del ecosistema bancario. Al exponer sus servicios y datos a través de API, los bancos ahora pueden colaborar con desarrolladores externos, startups de tecnología financiera y otras instituciones financieras para crear soluciones innovadoras y ampliar sus ofertas. Sin embargo, a pesar de estas claras ventajas, la exposición de las API no está exenta de riesgos.

Los riesgos de seguridad de las API pueden plantear amenazas importantes a la confidencialidad, la integridad y la disponibilidad de una API. Estos riesgos incluyen el acceso no autorizado, los ataques de inyección, los ataques de denegación de servicio, la transmisión de datos insegura, la autorización insuficiente y la derivación de privilegios, la falta de validación de entrada, el almacenamiento inseguro de credenciales y el registro y la supervisión inadecuados. Para hacer frente a estos riesgos, este líder en servicios bancarios se puso en contacto con Noname Security (ahora una empresa de Akamai).

Mantenimiento del cumplimiento

En el sector de los servicios financieros, el cumplimiento de las normativas es de suma importancia para garantizar prácticas justas y transparentes, proteger a los consumidores y mantener la integridad del sistema financiero. Las normativas Conozca a su cliente (KYC) y Lucha contra el blanqueo de capitales (AML) exigen que las

Banking Leader

Ubicación

Estados Unidos

Sector

Servicios financieros

Solución

Akamai API Security

Resultados clave

- Refuerzo del cumplimiento normativo
- Integración con el entorno de producción F5
- Provisión de una identificación continua de API

Akamai

instituciones financieras verifiquen la identidad de sus clientes, evalúen los posibles riesgos asociados con el blanqueo de capitales y la financiación del terrorismo, e informen de actividades sospechosas.

Otras normativas son las Normas de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS), que es un conjunto de normas de seguridad establecidas por las principales compañías emisoras de tarjetas de crédito para proteger los datos de los titulares de tarjetas. Estas normativas son solo la punta del iceberg en lo que respecta a normativas financieras. Por este motivo, saber qué datos atraviesan sus API era crucial para el líder en servicios financieros.

La empresa necesitaba comprender, gestionar y mitigar los riesgos mejorando la visibilidad general sobre su ecosistema de API, con especial hincapié en la detección de API, la clasificación de datos, la vulnerabilidad y la detección de anomalías. También priorizó la integración con su entorno de producción F5.

Descubrimiento de su presencia de API

La plataforma de seguridad de API de Noname (ahora parte de Akamai API Security) proporcionó visibilidad sobre el tráfico de API transmitido hacia y desde la red del cliente, así como dentro de ella. El motor de Akamai API Security analizó el tráfico y descubrió todas las API de este banco líder en servicios financieros. El análisis del tráfico en tiempo real identificó nuevas API y cambios en las API existentes, y los datos se registraron y actualizaron en el panel del cliente.

Dado que la plataforma no depende de agentes ni sidecars (y gracias a su integración con la infraestructura de nube), detecta todas las API, independientemente de si están registradas con una puerta de enlace de API. Se descubrieron API internas y externas, API heredadas (anteriores a la puerta de enlace de API) y API ocultas o no autorizadas (que no se enrutan a través de una puerta de enlace), lo que proporcionó al cliente una visibilidad sin precedentes sobre la superficie de ataque de API.

Mirando hacia el futuro

El líder en servicios bancarios utiliza un conjunto de criterios para evaluar el éxito de su seguridad de API. Uno de ellos, para el que Akamai proporciona asistencia, es la clasificación rápida. Un objetivo clave es determinar cómo analizar la gravedad de cada hallazgo, lo que permitiría al centro de operaciones de seguridad (SOC) evaluar, clasificar y responder rápidamente a una alerta.

 | Publicado en agosto de 2024