Historia de cliente de Akamai

# Un retailer del sector de bebidas de la lista Fortune 100 protege las API y los datos

Los datos de los clientes se protegen mediante la identificación de las vulnerabilidades clave de las API y la reparación de los daños causados por fraudes, abusos y robos anteriores

Las interfaces de programación de aplicaciones, o API, permiten a los retailers crear experiencias personalizadas de extremo a extremo para los clientes, al mismo tiempo que optimizan las operaciones. Cada variable que pone una bebida en manos de los consumidores (como los datos de inventario, los envíos de pedidos, los datos de localización, los pagos e incluso los programas de recompensas) se proporciona mediante las API. Las API han revolucionado la experiencia de compra al conectar el ecosistema de retailers, sus partners y sus clientes. No obstante, su proximidad constante a los datos confidenciales también las convierte en un riesgo.

Aunque los consumidores disfrutan de la nueva experiencia de retail digital, a menudo les preocupa cómo de bien está protegida su información personal, y con razón. Las API se están convirtiendo cada vez más en el vector de ataque preferido por los ciberdelincuentes. Por este motivo, una empresa de retail de la lista Fortune 100 que opera en el sector de bebidas se puso en contacto con Noname Security (ahora una empresa de Akamai) para hacer frente a las vulnerabilidades en su estrategia de seguridad de API.

## Desafíos de una presencia de API cada vez mayor

En nuestras conversaciones iniciales, la empresa expresó su preocupación por su incapacidad para lograr un buen nivel de control y seguridad de las API a escala global. Para reunir pruebas, organizó un programa de recompensa por hallar vulnerabilidades abierto al público en general, gracias al cual se identificó una vulnerabilidad enorme, por la que los nombres, las direcciones, los correos electrónicos y los números de teléfono de casi 100 millones de usuarios podrían haberse exfiltrado. Afortunadamente, se trató de un programa de recompensas y los problemas se solucionaron sin causar daños.

Retail Beverage Company

### Ubicación

Estados Unidos

### Sector

Retail, turismo y hostelería

### Solución

Akamai API Security

### Resultados clave

- Protección de más de mil millones de llamadas a API al día
- Protección de 5000 solicitudes por segundo
- Identificación y resolución de más de 200 problemas

Akamai

La empresa también tenía una visibilidad y supervisión inadecuadas de las API de producción, lo que se tradujo en la incapacidad para evaluar adecuadamente los riesgos, y sus datos de Apigee no proporcionaban detalles contextuales (por ejemplo, los tipos de datos, el comportamiento de los usuarios, las líneas de base o el análisis forense de vulnerabilidades). Debido a estas vulnerabilidades de las API, se produjeron fraudes, abusos y robos que no hicieron sino aumentar los costes operativos para el retailer.

## Refuerzo de su estrategia de seguridad de las API

La plataforma de seguridad de API de Noname (ahora parte de Akamai API Security) pudo realizar un inventario de las API del cliente y proporcionar análisis del comportamiento, detección de ataques en tiempo real y gestión de vulnerabilidades, incluidas las pruebas de desarrollo de aplicaciones específicas de API. Como resultado, el cliente fue capaz de detectar y corregir ataques a las API que los controles existentes no habían detectado. El equipo de seguridad de las aplicaciones, o AppSec, pudo aumentar la eficiencia y mejorar la priorización de los problemas de alto riesgo.

Akamai también admite hasta 50 000 API por motor sin latencia operativa. Con nuestra plataforma como base, el cliente ha desarrollado un programa de seguridad de las API global. Ahora disfruta de una visibilidad completa sobre su inventario de API con detalles relevantes en el contexto. Además, la empresa obtuvo información útil que no estaba disponible con las herramientas existentes, lo que le ha permitido reducir sus costes y garantizar la gestión eficiente de las vulnerabilidades de API y la detección de amenazas en tiempo real.


 | Publicado en agosto de 2024