Historia de cliente de Akamai

Un retailer de la lista Fortune 100 protege su negocio digital con API Security

Cumple con las normativas clave y cierra la puerta a posibles ataques DDoS y filtraciones de datos

El retail está experimentando una importante transformación con la adopción de procesos digitales impulsados por la potencia de las interfaces de programación de aplicaciones (API). Las API están revolucionando la forma en que los retailers operan, interactúan con los clientes y gestionan sus negocios.

Los retailers están integrando sus sistemas con diversas aplicaciones y servicios de terceros a través de API, lo que permite interacciones fluidas entre diferentes plataformas. Por ejemplo, las API permiten a los retailers integrar sus plataformas de comercio electrónico con pasarelas de pago, servicios de envío y sistemas de gestión de inventario. Sin embargo, a medida que este ecosistema se amplía, crea una abundancia de posibles vulnerabilidades de seguridad.

La seguridad de las API es primordial en el panorama digital actual. A medida que las organizaciones confían cada vez más en las API para conectar sistemas, compartir datos y habilitar integraciones, garantizar la seguridad de estas interfaces es fundamental. Por ese motivo, este retailer de la lista Fortune 100 recurrió a Noname Security (ahora una empresa de Akamai) para proteger su superficie de ataque de API.

Detección de la superficie de ataque de API

La detección de API desempeña un papel fundamental en el control de la proliferación de API, que se refiere al incremento incontrolado de API dentro de una organización. A medida que las empresas adoptan cada vez más API para posibilitar la transformación digital e impulsar la innovación, resulta esencial contar con un enfoque sistemático para detectar y gestionar de forma eficaz estas API. Además, en el creciente ecosistema de retail digital, es un primer paso fundamental para garantizar la protección de las API.

Designer Merchandise Retailer

Ubicación

Estados Unidos

Sector

Retail

Solución

Akamai API Security

Resultados clave

- Prevención de la exposición de datos
- Detección de la superficie de ataque de API
- Reducción de riesgos y costes

Akamai

Este líder del sector del retail se enfrentaba a una falta de visibilidad sobre el inventario y el tráfico de API. Sin el control de plataformas dispares (locales y en la nube), no era posible desarrollar una protección escalable del ciclo de vida de desarrollo de software (SDLC) para sus API. Así pues, la empresa se puso en contacto con nuestro equipo para solicitar una detección continua de activos de API con el fin de reducir el riesgo y los costes mediante la identificación de errores de configuración, vulnerabilidades y componentes no conformes, y para la integración con su flujo de trabajo de SecOPS existente (por ejemplo, Splunk).

Prevención de la exposición de datos confidenciales

En el sector del retail, las organizaciones deben adherirse a diversas normativas de cumplimiento. El objetivo de estas normativas es proteger los derechos de los consumidores, garantizar prácticas comerciales justas y mantener la privacidad y la seguridad de los datos. Las empresas deben ser capaces de ver y proteger las API que gestionan datos confidenciales para cumplir con las normativas clave y los estándares del sector, así como para evitar consecuencias legales y daños a la reputación.

El equipo de Akamai ayudó a prevenir la exposición pública de datos confidenciales de este retailer de la lista Fortune 100. El retailer había estado utilizando una versión antigua de Jira, lo que provocó un error que dio lugar a la exposición pública de los nombres de los empleados, los nombres de usuario de Jira y las direcciones de correo electrónico. Las API públicas también presentaban riesgos en la estrategia.

La solución Akamai API Security consiguió resolver los problemas en la estrategia de seguridad de las API de la empresa y corregir los errores de configuración en su entorno. Por ejemplo, la configuración deficiente de la arquitectura incrementaba el riesgo a través de ataques DDoS y filtración de datos.

De ahora en adelante

El cliente interactúa activamente con el equipo de Akamai semanalmente para impulsar la adopción por parte de la organización. También desea explorar nuevas integraciones con sus flujos de trabajo existentes. Akamai API Security identifica y prioriza de forma inteligente las posibles vulnerabilidades, que se pueden corregir de forma manual, semiautomática o totalmente automática a través de integraciones en WAF, puertas de enlace de API, sistemas de gestión de la información y eventos de seguridad (SIEM), ITSM, herramientas de flujo de trabajo u otros servicios. Además, debido al rápido crecimiento en la pila tecnológica del cliente, se están evaluando otras posibles integraciones.

©2024 Akamai Technologies | Asistencia | | Publicado en agosto de 2024