Akamai-Kundenreferenz

Fortune-500-Modehändler: Gesicherte APIs und Einzelhandelsabläufe

Die APIs, die für bequeme und personalisierte Einzelhandelserlebnisse sorgen, wurden gesichert, während die Kundendaten vor Datenschutzverletzungen geschützt wurden.

Alle APIs erkannt

Schwachstellen identifiziert

Sicherheitslage verbessert

APIs haben eine wesentliche Rolle bei der Verlagerung des Einzelhandels von traditionellen Ladengeschäften hin zu E-Commerce-Plattformen gespielt. Hinter jeder digitalen Interaktion steht eine API, die es Einzelhändlern ermöglicht:

- verschiedene Systeme, Anwendungen und Dienste nahtlos miteinander zu verbinden
- ihre Online-Outlets mit Backend-Lagerverwaltungssystemen, Zahlungsportalen, Versanddienstleistern und Tools für das Kundenbeziehungsmanagement zu integrieren
- einen schnellen Datenaustausch zu ermöglichen, der den Online-Einzelhandel personalisiert und bequem macht

Da der Schutz dieser Daten oberste Priorität hat, spielt die API-Sicherheit eine entscheidende Rolle bei der Sicherstellung von Vertrauen, Integrität und Vertraulichkeit von Online-Geschäftsvorgängen.

Die ständige Nähe von APIs zu sensiblen Daten macht sie zu attraktiven Zielen für Cyberkriminelle, die Schwachstellen ausnutzen wollen. Eine erfolgreiche API-Verletzung kann zur Exposition von Kundendaten führen, z. B. personenbezogene Daten, Zahlungskartendaten und Kaufverlauf. Aus diesen Gründen wandte sich dieser Fortune-500-Modehändler an Noname Security (heute ein Unternehmen von Akamai), da das Unternehmen mit seiner Beziehung zu Salt Security unzufrieden war.

Fashion Retailer

Standort

USA

Branche

Einzelhandel

Lösung

Akamai API Security

Akamai

Entwicklung eines programmatischen Ansatzes für die API-Sicherheit

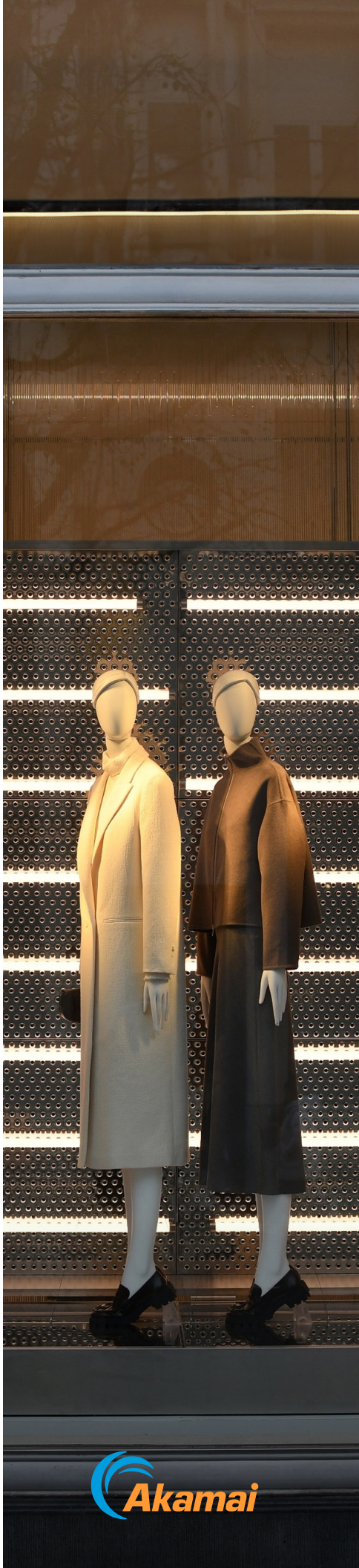
Der Fortune-500-Einzelhändler wollte einen vollständigen End-to-End-Workflow zur Minderung von API-Sicherheitsrisiken über Web Application Firewalls und API-Gateways hinaus schaffen. Dies würde eine solide API-Sicherheitsstrategie mit robusten Kontrollen für die API-Governance erfordern. Das Unternehmen konzentrierte sich zudem auf die Eindämmung von Bots, um letztlich zwischen legitimen Nutzern und bösartigen Bots unterscheiden zu können und so seine Systeme, Daten und die Nutzererfahrung zu schützen.

Angesichts der Größe des Projekts einigten sich der Einzelhändler und Akamai auf einen schrittweisen Ansatz. In Phase 1 sollten alle APIs lokalisiert, sensible Daten klassifiziert, Erkennungs- und Reaktionsmechanismen implementiert und eine Integration mit Splunk vorgenommen werden. In Phase 2 soll auf einen API-Sicherheitstestansatz mit Shift-Left umgestellt werden, um die Erstellung von sicherem Code zu beschleunigen.

Schnellere Bereitstellung verkürzte Time-to-Value

Obwohl Phase 1 eine große Herausforderung darstellte, konnte das Akamai-Team die API-Erkennungs- und Laufzeitschutzmodule von Noname während der Splunk-Integration in nur 120 Tagen bereitstellen. Die API-Erkennung spielt eine wichtige Rolle bei der Verwaltung der API-Ausbreitung. Sie umfasst die systematische Identifizierung und Katalogisierung aller APIs innerhalb eines Unternehmens. Durch die Verwaltung eines zentralisierten APIs-Repositorys können Entwickler vorhandene APIs einfach durchsuchen und erkennen, bevor sie mit neuen Entwicklungsmaßnahmen beginnen. Dies trägt dazu bei, Doppelungen zu vermeiden und die Wiederverwendung zu fördern, wodurch Zeit und Aufwand gespart werden.

Akamai verwendet automatisierte, lernbasierte Erkennung, um API-Schwachstellen zu identifizieren, einschließlich Datenlecks, Datenmanipulationen, Datenrichtlinienverletzungen, verdächtiges Verhalten und API-Sicherheitsangriffe. Der Fortune-500-Einzelhändler kann die Sicherheit und Integrität seiner APIs erheblich verbessern, vertrauliche Daten schützen und das Vertrauen von Nutzern und Partnern wahren.



 | Veröffentlicht: August 2024