Akamai-Kundenreferenz

Fortune-100-Getränkehändler schützt APIs und Daten

Kundendaten werden geschützt, indem wichtige API-Schwachstellen identifiziert und Schäden durch früheren Betrug, Missbrauch und Diebstahl behoben werden

Mit Application Programming Interfaces (APIs) können Einzelhändler personalisierte End-to-End-Erlebnisse für Kunden schaffen und gleichzeitig den Betrieb optimieren. Jede Variable, die für die Produktion eines Getränks wichtig ist – einschließlich Bestandsdaten, Bestelleinreichungen, Standortdaten, Zahlungen und sogar Prämienprogramme –, wird von APIs bereitgestellt. APIs haben das Einkaufserlebnis revolutioniert, indem sie das Ökosystem von Einzelhändlern, ihren Partnern und ihren Kunden vernetzen. Doch die ständige Nähe zu sensiblen Daten bringt auch Risiken mit sich.

Obwohl Verbraucher das neue digitale Einkaufserlebnis genießen, sind sie oft besorgt darüber, wie gut ihre persönlichen Daten geschützt werden – und das zu Recht. APIs werden zunehmend zu einem bevorzugten Angriffsvektor von Cyberkriminellen. Aus diesem Grund wandte sich ein Fortune-100-Getränkehersteller an Noname Security (mittlerweile ein Unternehmen von Akamai), um Schwachstellen in der API-Sicherheit zu beheben.

Herausforderungen einer wachsenden API-Umgebung

In unseren ersten Gesprächen äußerte sich das Unternehmen besorgt darüber, dass es nicht in der Lage war, echte API-Governance und -Sicherheit auf globaler Ebene zu erreichen. Um Beweise zu sammeln, gab es ein öffentlich dokumentiertes Bug-Bounty-Programm in Auftrag, bei dem eine riesige Schwachstelle identifiziert wurde, über die die Namen, Adressen, E-Mail-Adressen und Telefonnummern von fast 100 Millionen Nutzern hätten gestohlen werden können. Glücklicherweise war dies ein Bug-Bounty-Programm und die Probleme wurden ohne Schaden behoben.

Retail Beverage Company

Standort

USA

Branche

Einzelhandel, Reisebranche und Gastgewerbe

Lösung

Akamai API Security

Die wichtigsten Vorteile

- Milliarden API-Aufrufe pro Tag geschützt
- 5.000 Anfragen pro Sekunde geschützt
- Über 200 Probleme identifiziert und behoben

Akamai

Das Unternehmen verfügte auch über unzureichende Transparenz und Überwachung der Produktions-API, was dazu führte, dass Risiken nicht angemessen bewertet werden konnten. Außerdem lieferten seine Apigee-Daten keine kontextbezogenen Details (z. B. Datentypen, Nutzerverhalten, Baselines, Schwachstellen-Forensik). Aufgrund dieser API-Schwachstellen kam es zu Betrug, Missbrauch und Diebstahl. Und das führte zu hohen Betriebskosten für den Einzelhändler.

Stärkung der API-Sicherheit

Die Noname API Security Platform (mittlerweile Teil von Akamai API Security) konnte eine Bestandsaufnahme der APIs des Kunden durchführen und Verhaltensanalysen, Echtzeit-Angriffserkennung und Schwachstellenmanagement bereitstellen, einschließlich API-spezifischer AppDev-Tests. Dadurch konnte der Kunde API-Angriffe erkennen und beheben, die von bestehenden Kontrollen verpasst wurden. Das Team für Anwendungssicherheit (AppSec) konnte die Effizienz steigern und Probleme mit hohem Risiko besser priorisieren.

Akamai unterstützt außerdem bis zu 50.000 APIs pro Engine ohne Betriebslatenz. Mit unserer Plattform als Kern hat der Kunde ein globales API-Sicherheitsprogramm entwickelt. Heute verfügt er über vollständige Transparenz in seinem API-Bestand, einschließlich kontextrelevanter API-Details. Darüber hinaus erhält das Unternehmen aussagekräftige Informationen, die mit den vorhandenen Tools nicht verfügbar waren. Das ermöglicht kostengünstige Funktionen für effizientes API-Schwachstellenmanagement und Bedrohungserkennung in Echtzeit.

 | Veröffentlicht: August 2024