Akamai-Kundenreferenz

Fortune-100-Einzelhändler schützt das digitale Geschäft mit API Security

Einhaltung wichtiger Vorschriften und Verhinderung potenzieller DDoS-Angriffe und Datenlecks

Der Einzelhandel durchläuft einen bedeutenden Wandel: mit der Einführung digitaler Prozesse, die durch die Leistungsfähigkeit von APIs (Application Programming Interfaces) angetrieben werden. APIs revolutionieren die Arbeitsweise von Einzelhändlern, die Interaktion mit ihren Kunden und die Verwaltung ihrer Geschäfte.

Einzelhändler integrieren ihre Systeme über APIs in verschiedene Anwendungen und Services von Drittanbietern und ermöglichen so nahtlose Interaktionen über verschiedene Plattformen hinweg. Mit APIs können Einzelhändler beispielsweise Zahlungs-Gateways, Versandanbieter und Bestandsverwaltungssysteme in ihre E-Commerce-Plattformen integrieren. Doch wenn dieses Ökosystem skaliert wird, entstehen zahlreiche potenzielle Sicherheitslücken.

API-Sicherheit ist in der heutigen digitalen Landschaft von größter Bedeutung. Da Unternehmen zunehmend auf APIs angewiesen sind, um Systeme zu verbinden, Daten gemeinsam zu nutzen und Integrationen zu ermöglichen, wird die Sicherheit dieser Schnittstellen immer entscheidender. Aus diesem Grund wandte sich dieser Fortune-100-Händler an Noname Security (mittlerweile ein Unternehmen von Akamai), um seine API-Angriffsfläche zu sichern.

Aufdecken der API-Angriffsfläche

API-Erkennung spielt eine entscheidende Rolle bei der Kontrolle von API-Sprawl, also der unkontrollierten Verbreitung von APIs innerhalb eines Unternehmens. Da Unternehmen zunehmend APIs einsetzen, um die digitale Transformation zu ermöglichen und Innovationen voranzutreiben, ist ein systematischer Ansatz zur effektiven Erkennung und Verwaltung dieser APIs von entscheidender Bedeutung. Darüber hinaus ist es im schnell wachsenden Ökosystem des digitalen Einzelhandels ein wichtiger erster Schritt, um sicherzustellen, dass Ihre APIs geschützt sind.

Designer Merchandise Retailer

Standort

USA

Branche

Einzelhandel

Lösung

Akamai API Security

Die wichtigsten Vorteile

- Datenrisiko gemindert
- API-Angriffsfläche erkannt
- Risiko und Kosten verringert

Akamai

Dieser führende Einzelhändler hatte mit mangelnder Transparenz bei API-Inventar und -Traffic zu kämpfen. Ohne Governance über unterschiedliche Plattformen (vor Ort und Cloud) konnte die IT-Abteilung keinen skalierbaren API-SDLC-Schutz entwickeln. Das Unternehmen hat mit unserem Team eine kontinuierliche API-Asset-Erkennung bereitgestellt, um Risiken und Kosten zu reduzieren, indem Fehlkonfigurationen, Schwachstellen und Nichteinhaltung identifiziert und API-Sicherheit in den bestehenden SecOps-Workflow (z. B. Splunk) integriert wurde.

Schutz vertraulicher Daten

Im Einzelhandel gibt es mehrere Compliance-Vorschriften, die Unternehmen einhalten müssen. Diese Vorschriften zielen darauf ab, Verbraucherrechte zu schützen, faire Geschäftspraktiken zu gewährleisten und Datenschutz und -sicherheit zu wahren. Unternehmen müssen in der Lage sein, APIs mit sensiblen Daten zu überwachen und zu schützen, um wichtige Vorschriften und Branchenstandards einzuhalten und rechtliche Konsequenzen und Imageschäden zu vermeiden.

Mit dem Team von Akamai konnte der Fortune-100-Händler verhindern, dass sensible Daten offengelegt werden. Der Einzelhändler nutzte eine alte Version von Jira. Das führte zu einem Bug, der Mitarbeiternamen, Jira-Nutzernamen und E-Mail-Adressen preisgab. Öffentliche APIs stellten ebenfalls ein Sicherheitsrisiko für das Unternehmen dar.

Die Lösung „Akamai API Security“ konnte Lücken in der API-Sicherheit des Unternehmens schließen und Fehlkonfigurationen in der Umgebung beheben. Durch schlechte Architekturkonfiguration bestand beispielsweise ein höheres Risiko für DDoS-Angriffe und Datenlecks.

Pläne für die Zukunft

Der Kunde arbeitet wöchentlich aktiv mit dem Akamai-Team zusammen, um die Einführung im Unternehmen zu fördern. Darüber hinaus freut sich das Team, weitere Integrationen in die bestehenden Workflows zu erkunden. Akamai API Security identifiziert und priorisiert auf intelligente Weise potenzielle Schwachstellen, die manuell, halbautomatisch oder vollautomatisch behoben werden können – durch Integration in WAFs, API-Gateways, SIEM- und ITSM-Systeme, Workflow-Tools oder andere Services. Angesichts des schnell wachsenden Technologiepakets des Kunden gibt es außerdem eine Reihe von Integrationen, die derzeit geprüft werden.

 | Veröffentlicht: August 2024