Akamai-Kundenreferenz

Führende US-Bank schützt API-Traffic und steigert Transparenz

Einhaltung strenger Auflagen und beispiellose Transparenz der API-Angriffsfläche

Die Bankenbranche hat in den letzten Jahren einen bedeutenden Wandel durchlaufen, der durch die Einführung von Application Programming Interfaces (APIs) vorangetrieben wurde. Dank der Verbreitung von APIs konnten Banken neue Möglichkeiten nutzen, das Kundenerlebnis verbessern und das Geschäftswachstum fördern.

APIs spielen eine entscheidende Rolle bei der nahtlosen Integration zwischen verschiedenen Systemen und Anwendungen innerhalb des Banken-Ökosystems. Durch Offenlegung ihrer Services und Daten über APIs können Banken heute mit Drittanbietern, FinTech-Startups und anderen Finanzinstituten zusammenarbeiten, um innovative Lösungen zu entwickeln und ihr Angebot zu erweitern. Doch trotz dieser eindeutigen Vorteile ist die öffentliche Verfügbarkeit von APIs nicht ohne Risiko.

API-Sicherheitsrisiken können erhebliche Bedrohungen für die Vertraulichkeit, Integrität und Verfügbarkeit einer API darstellen. Zu diesen Risiken gehören unbefugter Zugriff, Injection-Angriffe, Denial-of-Service-Attacken, unsichere Datenübertragung, unzureichende Autorisierung und Berechtigungseskalation, fehlende Input Validation, die unsichere Speicherung von Anmeldedaten sowie unzureichende Protokollierung und Überwachung. Um diesen Risiken entgegenzuwirken, hat sich diese führende Bank an Noname Security (mittlerweile ein Unternehmen von Akamai) gewandt.

Optimale Compliance

In der Finanzdienstleistungsbranche ist die Einhaltung von Vorschriften absolut entscheidend, um faire und transparente Praktiken zu gewährleisten, Verbraucher zu schützen und die Integrität des Finanzsystems zu wahren. Laut KYC- (Know Your Customer) und AML-Vorschriften (Anti Money Laundering, Bekämpfung von

Banking Leader

Standort

USA

Branche

Finanzdienstleistungen

Lösung

Akamai API Security

Die wichtigsten Vorteile

- Compliance verbessert
- In F5-Produktions-umgebung integriert
- Kontinuierliche API-Iden-tifikation bereitgestellt

Akamai

Geldwäsche) müssen Finanzinstitute die Identität ihrer Kunden überprüfen, potenzielle Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung bewerten und verdächtige Aktivitäten melden.

Weitere Vorschriften sind der Payment Card Industry Data Security Standard (PCI DSS), eine Reihe von Sicherheitsstandards, die von großen Kreditkartenunternehmen zum Schutz der Daten von Karteninhabern festgelegt wurden. Doch diese Vorschriften sind nur die Spitze des Eisbergs, wenn es um Finanzvorschriften geht. Aus diesem Grund war es für diesen führenden Finanzdienstleister entscheidend, zu wissen, welche Daten über seine APIs übertragen werden.

Das Unternehmen musste Risiken verstehen, managen und mindern, indem es die allgemeine Transparenz seines API-Ökosystems verbesserte – mit Schwerpunkt auf API-Erkennung, Datenklassifizierung, Schwachstellen und Anomalie-Erkennung. Außerdem wurde die Integration in die F5-Produktionsumgebung priorisiert.

Ermittlung des API-Fußabdrucks

Die Noname API Security Platform (mittlerweile Teil von Akamai API Security) bot Einblick in den API-Traffic, der sowohl vom und zum Kundennetzwerk als auch innerhalb dieses Netzwerks übertragen wurde. Die Engine von Akamai API Security analysierte den Datenverkehr und entdeckte alle APIs des Finanzdienstleisters. Die Echtzeit-Datenverkehrsanalyse identifizierte neue APIs und Änderungen an bestehenden APIs. Die Daten wurden dann im Dashboard des Kunden aufgezeichnet und aktualisiert.

Da die Plattform nicht auf Agents oder Sidecars angewiesen ist und sich in die Cloud-Infrastruktur integrieren lässt, erkennt sie jede API unabhängig davon, ob die API bei einem API-Gateway registriert ist. Interne und externe APIs, ältere APIs (die vor dem API-Gateway entstanden sind) und Schatten- oder Rogue-APIs (solche, die nicht über ein Gateway geleitet werden) wurden alle entdeckt. Das bot dem Kunden einen noch nie dagewesenen Einblick in die API-Angriffsfläche.

Ausblick

Die führende Bank verwendet verschiedene Kriterien, um den Erfolg ihrer API-Sicherheit zu bewerten. Eines dieser Kriterien, für die Akamai Support bereitstellt, sind schnelle Tests. Ein wichtiges Ziel besteht darin, zu bestimmen, wie der Schweregrad jedes Ergebnisses analysiert werden kann, damit das SOC Alarme schnell bewerten, selektieren und darauf reagieren kann.

 | Veröffentlicht: August 2024