Akamai-Kundenreferenz

Finanzunternehmen erkennt und sichert APIs

Eine Bank schützte ihre digitalen Initiativen, indem sie versteckte APIs aufdeckte, API-Risiken bewertete und minimierte und regulatorische Anforderungen erfüllte.

Mehr Transparenz erzielt

Verbesserung der Sicherheit

Gesicherte digitale Initiativen

Die Finanzdienstleistungsbranche setzt zunehmend auf die digitale Transformation, um in einem sich ständig weiterentwickelnden Markt wettbewerbsfähig zu bleiben. Durch die Nutzung digitaler Möglichkeiten wie künstlicher Intelligenz und Big-Data-Analysen können Finanzinstitute innovative Produkte anbieten, Kosten senken und ihren Kunden individuellere und effizientere Dienstleistungen bieten.

Gleichzeitig bringt die digitale Transformation ein erhöhtes Risiko für Cyberangriffe mit sich. Um dieses wachsende Problem zu bekämpfen, ist Cybersicherheit heute ein wesentlicher Bestandteil jeder Strategie zur digitalen Transformation. Finanzdienstleistungsunternehmen müssen sicherstellen, dass ihre Systeme sicher und widerstandsfähig sind, um die Daten und Vermögenswerte ihrer Kunden vor böswilligen Akteuren zu schützen.

Eine der führenden Geschäftsbanken Asiens wandte sich schnell an Noname Security (jetzt ein Akamai-Unternehmen), um ihre API-Sicherheitslage zu verbessern. API-Sicherheitsverletzungen haben alarmierende Ausmaße erreicht. Tech Wire Asia wies darauf hin, dass „heute bis zu 1 von 13 Cybervorfällen auf API-Unsicherheit zurückzuführen ist“. Außerdem wurde betont, dass „API-Schwachstellen Unternehmen jährlich bis zu 75 Milliarden US-Dollar kosten“.

Da unser Kunde über Vermögenswerte von insgesamt mehr als 700 Milliarden US-Dollar, über 5.000 Firmenkunden und einen weltweit renommierten Ruf im Bereich der Vermögensverwaltung verfügt, war es unerlässlich, alle API-Schwachstellen so schnell wie möglich zu beheben.

Financial Services

Standort

Asien

Branche

Finanzdienstleistungen

Lösung

Akamai API Security

Akamai

Notwendigkeit einer besseren Sichtbarkeit von APIs und ihrer Risiken

Das Unternehmen hatte bereits eine API-Verwaltungsplattform für die Authentifizierung und die Kontrolle des Datenverkehrs eingeführt, aber es gab Zweifel an ihrer Eignung, API-Missbrauch und Cyberangriffe zu verhindern. API-Gateways bieten zwar dringend benötigte grundlegende API-Sicherheitskontrollen, reichen aber leider nicht aus, um Organisationen angemessen vor API-spezifischen Bedrohungen zu schützen.

Beispielsweise erscheint die Broken Object Level Authorization, oft als BOLA bezeichnet, als normaler API-Traffic zu Gateways. Dieser fehlende Kontextbezug zwischen API-Anfragen und -Antworten ermöglicht es BOLA-Angriffen, unentdeckt zu bleiben und auf kritische Backend-Dienste zuzugreifen. Dieser Fehler kann nicht nur dazu führen, dass die Unternehmen anfällig für BOLA-Exploits werden, sondern auch anderen Angriffen und dem Missbrauch der Geschäftslogik Tür und Tor öffnen.

Eine weitere Einschränkung der Sichtbarkeit betrifft die Pflege eines genauen API-Bestands. Wie die meisten großen Organisationen hatte auch die Bank mit unbekannten APIs in ihrer Umgebung zu kämpfen. Die Realität ist: Unternehmen verwalten Tausende von APIs, von denen viele nicht über einen Proxy, wie z. B. ein API-Gateway, weitergeleitet werden. Diese werden als Rogue-APIs oder Zombie-APIs bezeichnet. Diese APIs wurden wahrscheinlich von ehemaligen Mitarbeitern bereitgestellt oder bevor das Unternehmen die API-Sicherheit ernst genommen hatte. Unabhängig davon, aus welchem Grund sie existieren, konnte das API-Gateway der Bank sie nicht sehen, sodass die Anzahl der APIs leicht falsch eingeschätzt wurde.

Steigende Anforderungen an die API-Sicherheit

Das Unternehmen setzte die komplette Noname API Security Platform (jetzt Teil von Akamai API Security) ein, einschließlich Lösungen für die Verwaltung der Sicherheitslage von APIs, den Laufzeitschutz und das Testen in der gesamten Umgebung. Die Sicherheitslage des Kunden hat sich exponentiell verbessert, da er nun in der Lage ist, Schwachstellen für einen der undurchsichtigsten Bedrohungsvektoren der Welt zu erkennen und zu beheben.

Jetzt können unbekannte APIs innerhalb der Plattform entdeckt und offengelegt werden, was eine vollständige Transparenz und Risikominderung ermöglicht. Das Unternehmen hat die Ausbreitung seiner API drastisch reduziert und die Compliance verbessert, da Akamai API Security sensible Daten klassifiziert, um Vorschriften wie die DSGVO, HIPAA und andere zu erfüllen.

Die Bank ist nun außerdem in der Lage, Angriffe in Echtzeit zu stoppen und Kundendaten zu schützen. Die Laufzeitschutzlösung erkennt und priorisiert potenzielle Bedrohungen auf intelligente Weise und überwacht dabei kontinuierlich die API-Aktivität. Durch die Integration mit Web Application Firewalls, API-Gateways, Sicherheitsinformations- und Ereignismanagement, IT-Servicemanagement und anderen Workflow-Tools ermöglicht unsere Plattform die manuelle, teilautomatische oder automatische Behebung von Bedrohungen.

Resultat

APIs haben sich schnell zu einem bevorzugten Angriffsvektor für Hacker entwickelt, und die Angriffe lassen nicht nach. Zum Beispiel verzeichneten wir im Jahr 2022 „einen Anstieg der Angriffe auf den Finanzdienstleistungssektor um 257 Prozent im Vergleich zum Vorjahr“. Das Finanzdienstleistungsunternehmen wird dank Akamai API Security gut gerüstet sein, um nicht in die Statistik einzugehen und sich gegen diesen Trend zu behaupten. Insbesondere werden die Sicherheitsteams der Kunden ein besseres Verständnis dafür haben, welche Gefahren von APIs ausgehen, und in der Lage sein, noch sicherere Systeme zu entwickeln.

| Veröffentlicht: August 2024