AKAMAI-LÖSUNGSÜBERBLICK

API-Sicherheit in der Gesundheitsbranche

Erfahren Sie, wie Akamai API Security Gesundheitsdienstleister dabei unterstützt, API-Bedrohungen zu erkennen und sich zu schützen.

APIs ermöglichen Gesundheitsdienstleistern die Verbesserung und Optimierung der Patientenversorgung durch einen nahtlosen Datenaustausch zwischen Systemen, Geräten und Personen. Diese Daten sind jedoch häufig vertraulich – von Patientenakten bis hin zu Versicherungspolicen – und machen APIs zu einem interessanten Ziel für Angreifer.

Sind Ihre APIs gefährdet? Sehen Sie sich die folgenden Erkenntnisse aus der API-Sicherheitsstudie 2024 an:

- Fast 85 % der Gesundheitsorganisationen hatten 2024 API-Sicherheitsvorfälle zu verzeichnen, ein Anstieg gegenüber 79 % im Jahr 2023.
- Nur 24 % der Unternehmen mit vollständigen API-Bestandsaufnahmen wissen, welche ihrer APIs sensible Daten austauschen – 2023 waren es noch 40 %.

IT- und Sicherheitsexperten in mehreren Branchen berichten, dass sie durchschnittlich mehr als 943.000 US-Dollar für die Bearbeitung und Behebung von API-Sicherheitsvorfällen ausgeben.

APIs ermöglichen einen nahtlosen Datenaustausch, wodurch Einrichtungen im Gesundheitswesen von einer besseren Interoperabilität und Effizienz profitieren können. APIs vergrößern jedoch auch die Angriffsfläche: Da sie sich über Anwendungen, Cloudumgebungen und KI-Modelle hinweg ausbreiten, steigt auch das Risiko für APIs. Einrichtungen im Gesundheitswesen implementieren versehentlich APIs, die falsch konfiguriert, unzureichend getestet und ohne Zugriffskontrolle erstellt wurden, sodass Angreifer leichter Daten stehlen und den Betrieb unterbrechen können.

Akamai API Security hilft Anbietern dabei, herauszufinden, wie viele APIs sie haben und welche Arten von Daten diese APIs durchlaufen. Anbieter erhalten die Möglichkeit, diese Daten jederzeit zu schützen. Leider betrachten viele medizinische Fachkräfte APIs als Teil der herkömmlichen Anwendungssicherheit. Doch AppSec- und DevOps-Mitarbeiter müssen über die einzigartigen Sicherheitsaspekte von APIs gesondert nachdenken. Als grundlegende Technologie für die moderne Gesundheitsversorgung bergen APIs neue Risiken, auf die man mit älteren Tools nicht reagieren kann.

Um ein zuverlässiges API-Governance- und Sicherheitsprogramm aufzubauen, müssen Unternehmen mit dem richtigen API-Sicherheitsanbieter zusammenarbeiten. Im Gesundheitswesen stellen unüberwachte Datenflüsse erhebliche Risiken dar, doch viele Organisationen verfügen immer noch nicht über eine umfassende Inventarliste ihrer APIs. Akamai API Security hilft Institutionen dabei, einen vollständigen Einblick in ihre API-Landschaft zu erhalten, indem alle aktiven APIs identifiziert und die von ihnen verwendeten Datentypen analysiert. Auf dieser Grundlage ermöglicht unsere Lösung kontinuierlichen Schutz durch Asset-Management, Analyse sensibler Daten, Erkennung von Anomalien, API-Sicherheitstests, CI/CD-Integration sowie manuelle und automatisierte Behebungsmaßnahmen, die sich nahtlos in Workflows von Drittanbietern integrieren lassen.

Herausforderungen

APIs vergrößern die Angriffsfläche

Bei fast 85 % der Gesundheitsorganisationen kam es 2024 zu API-Sicherheitsvorfällen

Wie Akamai API Security auf API-Bedrohungen reagiert

Die Lösung von Akamai wurde speziell entwickelt, um Einrichtungen im Gesundheitswesen beim Schutz ihrer API-Umgebung zu unterstützen.

Umfassende API-Erkennung

Identifizieren und inventarisieren Sie APIs in Ihrer Umgebung, einschließlich RESTful, GraphQL, SOAP, XML-RPC und gRPC. Spüren Sie nicht verwaltete oder veraltete APIs auf, die nicht von Ihrem API-Gateway abgedeckt werden, und erhalten Sie Einblick in deren Attribute und Metadaten.

API-Verhalten verstehen und Bedrohungen erkennen

Nutzen Sie KI-gestützte Analysen, um Sicherheitsrisiken wie Datenlecks, unbefugten Zugriff, Fehlkonfigurationen und verdächtige Aktivitäten automatisch zu identifizieren. Seien Sie potenziellen Bedrohungen dank kontinuierlicher Überwachung und Erkennung von Anomalien einen Schritt voraus.

APIs schützen und Sicherheitslücken beheben

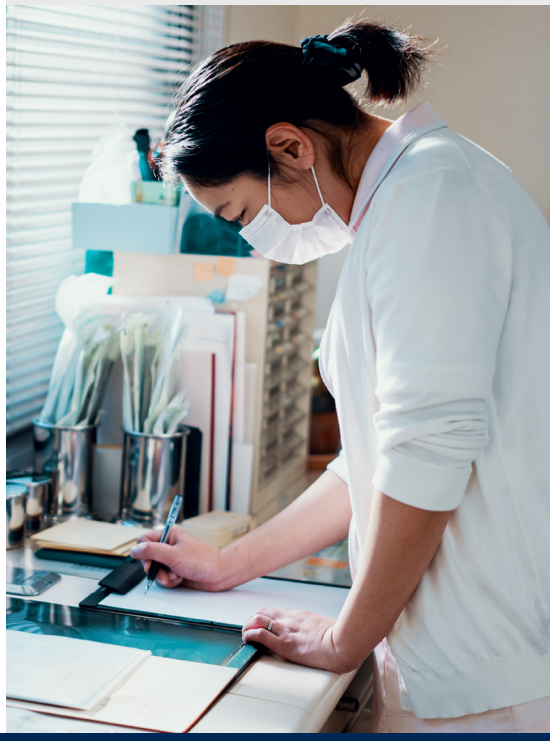
Wehren Sie Angriffe in Echtzeit ab, beheben Sie falsche Sicherheitskonfigurationen und aktualisieren Sie Firewall-Regeln automatisch, um schädlichen Traffic zu unterbinden. Integrieren Sie die Lösung nahtlos in bestehende Sicherheitsökosysteme wie WAFs, Ticketsysteme und SIEM-Plattformen, um Ihre Reaktionsmöglichkeiten zu verbessern.

Testen Sie proaktiv APIs vor der Bereitstellung

Vergewissern Sie sich, dass APIs im Rahmen des Entwicklungslebenszyklus gründlich getestet werden, um Fehler in der Geschäftslogik, Fehlkonfigurationen und andere Schwachstellen aufzudecken, bevor sie in die Produktion gehen. Durch die frühzeitige Integration von Sicherheitstests können Unternehmen Risiken proaktiv angehen und ihre API-Verteidigung stärken.

Akamai API Security

Von der API-Erkennung und Risikoanalyse bis hin zu API-Tests und Compliance



Weitere Informationen finden Sie auf unserer Seite zu API Security oder beim Vertriebsteam von Akamai.