Akamai-Kundenreferenz

Sport- und Medienunternehmen deckt versteckte API-Risiken auf

Aufbau eines vollständigen API-Bestands und Aufdecken von Fehlkonfigurationen, die API-Angriffe verhindern

Genaues Inventar erstellt

Fehlende Kontrollen aufgedeckt

SQL-Injection erkannt

Digitale Plattformen und Anwendungen revolutionieren die Sport- und Medienbranche durch die Leistungsfähigkeit von APIs. Diese technologischen Fortschritte verändern die Art und Weise, wie Live-Veranstaltungen organisiert, beworben und erlebt werden, und schaffen neue Möglichkeiten für Künstler, Veranstalter und Publikum gleichermaßen.

APIs können Veranstaltungsinformationen, Updates und Ticketlinks nahtlos über verschiedene Social-Media-Kanäle teilen, wodurch die Sichtbarkeit erhöht und der Ticketverkauf angekurbelt wird. Darüber hinaus verändern APIs das On-Site-Erlebnis bei Live-Events. Die Integration mit mobilen Anwendungen und tragbaren Geräten ermöglicht interaktive Funktionen wie personalisierte Zeitpläne, interaktive Karten und Echtzeit-Benachrichtigungen.

Es ist jedoch wichtig zu beachten, dass die sensible Natur der Daten und Transaktionen im Sport- und Mediensektor es zwingend erforderlich macht, der API-Sicherheit Priorität einzuräumen. API-Sicherheitskontrollen spielen eine entscheidende Rolle bei der Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten. Aus diesem Grund hat diese weltbekannte Sport- und Medienorganisation Noname Security (jetzt ein Akamai-Unternehmen) beauftragt

Implementierung der API-Sicherheit

Der Kunde war sich der Notwendigkeit der API-Sicherheit bewusst, war sich aber nicht genau sicher, wo er anfangen sollte und welche Bereiche priorisiert werden sollten. In der Vergangenheit lag das Hauptaugenmerk in erster Linie auf der Anwendungssicherheit. Das Unternehmen war der Meinung, dass die vorhandenen Tools, wie API-Gateways und Web Application Firewalls, für den Schutz von APIs ausreichen würden. Solche Tools können zwar einen gewissen

Sports and Media Company

Standort

USA

Branche

Medien- und Unterhaltungsbranche

Lösung

Akamai API Security

Akamai

Basisschutz bieten, sind jedoch nicht dafür ausgelegt, das Maß an Sichtbarkeit, Echtzeitsicherheit und kontinuierlichen Tests zu bieten, das spezialisierte API-Sicherheitslösungen bieten können. Ein Großteil dieser Schutzmaßnahmen konnte mit der aktuellen Infrastruktur nicht umgesetzt werden. Zwei der wichtigsten Aspekte der API-Sicherheit sind beispielsweise die Authentifizierung und Autorisierung. Durch geeignete Authentifizierungsmechanismen wird sichergestellt, dass nur autorisierte Nutzer oder Systeme auf die APIs zugreifen können.

Aufdeckung von Schwachstellen

Das API-Sicherheitsteam von Akamai nutzte die Module „Posture Management“ und „Runtime Protection“, um die aktuelle API-Sicherheitslage des Kunden zu verstehen. Sobald wir eine genaue Bestandsaufnahme der APIs in der Umgebung des Kunden hatten, konnten wir vorhandene Sicherheitslücken und Fehlkonfigurationen aufdecken.

Die erste Erkenntnis war, dass der Kunde Opfer einer Structured Query Language Injection (SQLi) war. Ein SQLi ist eine Art Sicherheitslücke, die auftritt, wenn ein Angreifer die Eingabeparameter einer API-Anforderung manipulieren kann, um nicht autorisierte SQL-Befehle auszuführen. Die Folgen eines erfolgreichen SQLi-Angriffs können schwerwiegend sein. Angreifer können unautorisierten Zugriff auf sensible Daten erhalten, Daten ändern oder löschen oder sogar willkürliche Befehle auf dem zugrunde liegenden Datenbankserver ausführen.

Die zweite Entdeckung war, dass dem Kunden die Authentifizierung fehlte. Ohne ordnungsgemäße Authentifizierung kann jeder auf API-Endpunkte zugreifen und möglicherweise vertrauliche Daten abrufen oder ändern. Daten können geändert oder gelöscht werden, was zu Problemen bei der Datenintegrität und zum potenziellen Verlust wichtiger Informationen führt. Dies kann zu Datenschutzverletzungen, unbefugter Offenlegung von Informationen oder sogar zur vollständigen Kompromittierung des Systems führen.

Ausblick

Da der Kunde nun seine APIs in der Produktion fest im Griff hat, hat er untersucht, wie Schwachstellen vor der Produktion behoben werden können. Um Unternehmen bei der Erkennung und Behebung dieser Schwachstellen zu unterstützen, umfasst Akamai API Security Active Testing, eine speziell entwickelte Lösung für API-Sicherheitstests, die die einzigartige Geschäftslogik eines Unternehmens verstehen und eine umfassende Abdeckung seiner API-spezifischen Schwachstellen bieten kann. Aktive Tests helfen Organisation beim Shift-Left-Ansatz und dabei, API-Sicherheitstests in jeder Entwicklungsphase zu etablieren.

 | Veröffentlicht 09/24