Der Leitfaden zum API-Laufzeitschutz

Inhaltsverzeichnis

Einführung

Warum API-Sicherheit unerlässlich ist

Wenn es darum geht, Kundenbedürfnisse zu erfüllen, stehen Unternehmen unter enormem Druck, Anwendungen, Services und GenKI-Tools schnell zu entwickeln, zu produzieren und zu verbessern. Diese Eile birgt leider ein Risiko: Die APIs, die hinter den Kulissen für all diese Innovationen zum Einsatz kommen, werden oft mit Fehlkonfigurationen, Programmierfehlern und fehlenden Sicherheitskontrollen erstellt. Und wenn diese APIs die Produktionsphase erreichen, interagieren nicht nur Endnutzer mit ihnen. Auch Angreifer testen ständig, wie sie APIs kompromittieren und auf die von ihnen ausgetauschten Daten zugreifen können.

Falsch konfigurierte und kompromittierte APIs tragen zunehmend zu erheblichen Datenschutzverletzungen bei. Dennoch sind nur wenige Unternehmen in der Lage, die Tausenden API-Aufrufe innerhalb ihrer digitalen Ökosysteme im Auge zu behalten. Und noch weniger von ihnen sind vollständig vor API-Bedrohungen während der Laufzeit geschützt.

Beispielsweise fand ein Fitness-Einzelhandelsunternehmen 2021 einen Fehler in einer API für Nutzerkontodaten. Dieser Fehler ermöglichte nicht authentifizierte Anfragen nach Daten wie Alter, Geschlecht, Stadt, Gewicht und Geburtsdatum. Glücklicherweise wurde diese Schwachstelle bei einer Sicherheitsuntersuchung entdeckt und dem Unternehmen gemeldet. Doch Bugs wie dieser können auch unbemerkt bleiben und wochen- oder monatelang ausgenutzt werden.

Beim Schutz von APIs können die herkömmlichen Tools, auf die Unternehmen setzen – z. B. API-Gateways und Web Application Firewalls – grundlegenden Schutz bieten. Doch da die Anzahl und Komplexität der API-Angriffe stetig zunimmt, benötigen moderne Sicherheitsteams zusätzliche Sicherheitsebenen. Dazu braucht es eine Ausweitung der vorhandenen Kontrollen mit tiefergreifenden Einblicken in Schwachstellen, potenzielle Angriffspfade, Cyberangriffe und API-Verhalten.

Um dieses Schutzniveau zu erreichen, benötigen Unternehmen eine umfassende Lösung für API-Sicherheit, die vier Bereiche umfasst:

1. API-Erkennung
2. API-Sicherheitsmanagement
3. API-Laufzeitschutz
4. API-Sicherheitstests

Themen dieses Leitfadens

API-Laufzeitschutz ist der Schutz von APIs, während diese im normalen Betrieb Anfragen bearbeiten und verwalten. In diesem Leitfaden gehen wir auf die wichtigsten Anforderungen an den API-Laufzeitschutz ein – unter anderem die API-Überwachung als Verteidigungsmaßnahme gegen die Ausnutzung von Schwachstellen und Fehlkonfigurationen ebenso wie die Verhinderung von API-Angriffen. Wir behandeln die Grundlagen der Angriffsprävention während der Laufzeit und stellen die Laufzeitschutz-Funktionen von Akamai API Security vor.

Warum eigentlich Laufzeitschutz?

API-Laufzeitschutz sichert APIs während der gesamten Produktionsphase ihres Lebenszyklus, sobald sie in Betrieb sind und zur Interaktion mit den beabsichtigten Endnutzern – und Angreifern – bereitstehen. Effektive Funktionen zum Laufzeitschutz unterstützen Unternehmen dabei, schädliche API-Anfragen schnell zu erkennen und zu beheben. So schützen sie APIs unter anderem vor folgenden Bedrohungen nach der Implementierung:

- Angreifer, die große Mengen vertraulicher Daten von einer API abrufen
- Angriffe durch Rechteausweitung unter Ausnutzung von Sicherheitslücken
- Bereitstellung nicht autorisierter APIs außerhalb der normalen Prozesse

API-Bedrohungen während der Laufzeit aufzuhalten, erfordert ein kontextuelles Verständnis der Vorgänge jeder einzelnen API – einschließlich API-Zugriff, -Nutzung und -Verhalten. Zunächst müssen Sie Ihren API-Bestand in seinem vollen Umfang kennen. In unserem Leitfaden zur API-Erkennung erläutern wir, warum eine API-Bestandsaufnahme wichtig ist. Mit einer vollständigen Liste Ihrer APIs können Sie den gesamten API-Traffic überwachen, ein grundlegendes Verständnis des „typischen“ Verhaltens jeder einzelnen APIs entwickeln und so anomales Verhalten erkennen.
Ein guter API-Laufzeitschutz erkennt:

- Datenlecks
- Verletzungen der Datenschutzrichtlinie
- Angriffe auf die API-Sicherheit
- Datenmanipulation
- Verdächtiges Verhalten

Darüber hinaus sollte Laufzeitschutz den API-Traffic protokollieren, den Zugriff auf sensible Daten überwachen, Bedrohungen erkennen und Angriffe abwehren oder beheben.

Überwachen des API-Traffics auf Angriffe

Die Beobachtung des API-Traffics ist zur Risikoerkennung unerlässlich. Wird eine Überwachungslösung ohne Verständnis Ihres API-Bestands bereitgestellt, liefert sie nur begrenzte Einblicke. Nachdem Ihre API-Umgebung inventarisiert wurde, sollte der API-Laufzeitschutz den Traffic und die API-Nutzung kontinuierlich überwachen und nach Schwachstellen und Fehlkonfigurationen suchen.

Erkennen anomalen Verhaltens

Anhand einer Baseline des normalen API-Verhaltens lassen sich alle Abweichungen ermitteln. Durch die Wiedergabe von Verlaufsdaten wird anomales Verhalten erkennbar, das auch Angriffsabsichten offenlegen kann.

Werden potenzielle Anomalien entdeckt, sollten diese im Kontext anderer Aktionen innerhalb der Anwendung oder des Netzwerks näher untersucht werden. Nehmen wir beispielsweise an, Datenanfragen haben im Allgemeinen eine bestimmte Größe. Dann sollte ein API-Aufruf, der eine größere Datenmenge als üblich anfragt, als auffällig gekennzeichnet werden. Unabhängig davon, ob es sich nun um eine schädliche Anfrage handelt oder nicht, erfordert die Anomalie eine weitere Untersuchung.

Erkennen von Datenlecks

Einige der APIs in Ihrem Bestand senden und empfangen wahrscheinlich sensible Daten. Wenn vertrauliche Informationen aufgrund einer Sicherheitslücke offengelegt werden, können Angreifer diese ausnutzen, um Berechtigungen auszuweiten oder andere unzulässige Konfigurationen der Zugriffskontrolle vorzunehmen. KI und maschinelles Lernen können bei der Echtzeitanalyse des Traffics und der Erkennung von Anomalien von entscheidender Bedeutung sein. Denn sie bieten kontextbezogene Einblicke in Datenlecks, Datenmanipulationen, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und Angriffe auf die API-Sicherheit.

Bei einem immer gängigeren Angriffstyp versuchen Cyberkriminelle, gültige API-Schlüssel abzugreifen. In einem solchen Fall bleibt Ihnen zum Schutz vor unzulässiger API-Nutzung und potenziellen Datenschutzverletzungen kaum etwas anderes übrig, als anomales Verhalten und Datenlecks effektiv ausfindig zu machen und zu unterbinden.

API-Sicherheitsaudits

Tools für API-Sicherheitsaudits sollten den Traffic in Echtzeit überwachen und Sie vor Angriffen und anderen schädlichen Aktionen warnen. Sie sollten folgende Mindestanforderungen erfüllen:

- Erkennen von Angriffen und schädlichen Anfragen durch kontinuierliche Überwachung
- Passives Scannen von APIs (intern wie extern) nach Fehlkonfigurationen und Sicherheitslücken, die einen Verstoß ermöglichen oder verschlimmern oder die Abwehr schwächen könnten
- Durchsetzen von Richtlinien, die bestimmen, welche Daten von APIs gesendet oder empfangen werden dürfen (und welche nicht)

Der API-Laufzeitschutz sollte auch durch ein API-Sicherheitsmanagement ergänzt werden, das Fehlkonfigurationen und bekannte Schwachstellen erkennt. Weitere Informationen erhalten Sie in unserem Leitfaden zum API-Sicherheitsmanagement.

Funktionen zum Laufzeitschutz, auf die Sie nicht verzichten sollten

Wenn Ihr Unternehmen aktiv APIs entwickelt und implementiert, muss Ihr API-Sicherheitsprogramm zuverlässigen Laufzeitschutz umfassen. Im Folgenden sind wichtige Funktionen aufgeführt, die Ihre Laufzeitschutz-Tools enthalten müssen.

Out-of-Band-Überwachung in Echtzeit

Die API-Sicherheitsüberwachung sollte den API-Traffic nicht beeinträchtigen, verlangsamen oder durch zusätzliche Latenz belasten. Sie sollte komplett separat („out of band“) laufen, ohne erforderliche Netzwerkänderungen und ohne umständliche, schwer zu installierende Agents. Laufzeitschutz-Tools sollten den Traffic von identifizierten Datenquellen spiegeln und im Hintergrund analysieren, wobei bei erkannten Problemen in Echtzeit Warnmeldungen ausgegeben werden.

Akamai läuft standardmäßig separat und agentlos. Bei Bedarf bieten wir aber auch Optionen für agentbasierte Erkennung und Inline-Abwehr.

Erkennung von API-Anomalien und -Exploits

Die passive Datenerfassung reicht nicht aus, insbesondere da die Anzahl der APIs und das Gesamtvolumen des API-Traffics weiter ansteigen. API-Aktivitäten müssen kontinuierlich analysiert werden, um anomale Ereignisse zu erkennen und das Sicherheits- und Betriebsteam warnen zu können. Modernste Plattformtools umfassen KI-Funktionen und maschinelles Lernen, um Traffic in Echtzeit zu analysieren und kontextbezogene Einblicke in Datenlecks, Datenmanipulationen, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und API-Sicherheitsangriffe zu gewinnen.

Verhinderung von API-Angriffen und Risikominderung

Sobald eine Anomalie oder ein anderes Problem erkannt und eine Warnmeldung generiert wurde, dürfen Sie keine Zeit verlieren. Die nicht autorisierte Übertragung vertraulicher Daten per API oder andere Formen mutmaßlichen API-Missbrauchs müssen erkannt und behoben werden. Laufzeitschutz sollte API-Missbrauch nicht allein durch die Integration in Ihre vorhandenen Firewalls und API-Gateways verhindern, sondern auch Optionen zur – möglichst automatisierten – Problembehebung liefern. Achten Sie auf Funktionen mit Konfidenzwerten zur Einordnung von Angreifern. Anhand dieser Werte kann Ihr Team bestimmen, ob Signale, die auf Missbrauch, Angriffe oder Verstöße hindeuten, legitim sind und einer Eskalation bedürfen.

Integrationen für die Reaktion auf Vorfälle

Im Allgemeinen sollten sich Laufzeitschutz-Tools problemlos in andere Sicherheits-, Überwachungs- und Verwaltungstools Ihres Unternehmens integrieren lassen. Wenn es beispielsweise zu einem Vorfall kommt, müssen Laufzeitschutz-Tools die erforderlichen Integrationen enthalten, um sicherzustellen, dass Maßnahmen zur Behebung den entsprechenden Teams zugewiesen werden. Wenn Fehlkonfigurationen, Verstöße gegen Datenrichtlinien oder verdächtige Verhaltensweisen erkannt werden, sollten diese an das API-Gateway, das SIEM-System und andere Informationssicherheits-Engines gemeldet werden, um das richtige Maß an Situationsbewusstsein sicherzustellen. Mit Funktionen zur Einordnung von Angreifern nach Konfidenzwert können Teams Fehlalarme herausfiltern lassen, um ihre Aufmerksamkeit den wahren API-Sicherheitsprioritäten zu widmen.

Rapyd

Rapyd, ein globales Unternehmen im Bereich Zahlungsverarbeitung und Finanztechnologie, betreibt Zahlungssysteme in über 100 Ländern. Das Unternehmen hatte keinen differenzierten Einblick in die API-Nutzung und das API-Verhalten. Daher brauchte es eine bessere Lösung zur Sicherung öffentlich zugänglicher APIs – und Hunderter interner APIs – in einem hochkomplexen, globalen System, das in der AWS-Cloud betrieben wird. Rapyd benötigte eine differenzierte Bestandsaufnahme aller APIs, Einblick in Fehlkonfigurationen und Schwachstellen sowie eine intelligente Priorisierung von Warnmeldungen, damit die Problembehebung nach einem logischeren Ansatz erfolgt.

Akamai API Security erfüllte die Anforderungen von Rapyd dank umfassenden Einblicken und Laufzeitschutz, der mit maschinellem Lernen eine Traffic-Baseline für jede API erstellt und Anomalien automatisch erkennt und behebt.

Vollständige Kundenreferenz lesen

> Jetzt können wir unser Risiko auf die wissenschaftlich fundierteste Art und Weise bewerten und haben unsere Sicherheitslage im Griff.

– Nir Rothenberg
CISO, Rapyd

Laufzeitschutz mit Akamai API Security

Als integraler Bestandteil Ihres Compliance- und Risikobewertungsprogramms sollten Sie in der Lage sein, API-Angriffe noch bei ihrer Entstehung zu erkennen und abzuwehren. Wenn andere Sicherheitskontrollen scheitern, halten Sie so Ihre letzte Verteidigungslinie aufrecht.

Das Laufzeitschutz-Modul von Akamai API Security umfasst alle im vorangehenden Abschnitt beschriebenen Funktionen. Seine primäre Funktion besteht darin, API-Angriffe in Echtzeit zu erkennen und zu blockieren. Mithilfe von automatisiertem maschinellem Lernen wird der Traffic analysiert und ein kontextbezogener Einblick in Datenlecks, Datenmanipulationen, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und Angriffe auf die API-Sicherheit gewährt. Laufzeitschutz erkennt Anomalien und potenzielle Bedrohungen in Ihrem API-Traffic und erleichtert Gegenmaßnahmen anhand vorab gewählter Richtlinien für die Reaktion auf Vorfälle.

Laufzeitschutz kann in WAFs, API-Gateways, ITSMs, SIEMs und andere Workflow-Tools integriert werden und bietet so einen ganzheitlichen Schutz vor Angriffen. Sie können wählen, ob Sie die Beseitigung von Bedrohungen vollständig automatisieren oder verschiedene Stufen manueller Eingriffe verlangen, um mehr Transparenz und Kontrolle zu erhalten. Akamai API Security ist zudem eine Lösung mit nativer Integration in die Akamai-Plattform. So können wir IPs von Angreifern direkt an der Edge aufhalten.

Erstellung von Fällen

Akamai erstellt mit maschinellem Lernen ein Modell für jede API. Diese Basile für normales Verhaltens wird dann dazu verwendet, Angriffe auf die API-Geschäftslogik zu erkennen. Das kann z. B. eine fehlerhafte Autorisierung auf Objektebene (Broken Object Level Authorization, BOLA) sein, bei der eine Person Zugriff auf Daten erlangt, auf die sie nicht zugreifen dürfte. Jedes Mal, wenn der API-Traffic vom normalen Verhalten abweicht, erstellt Akamai einen Fall.

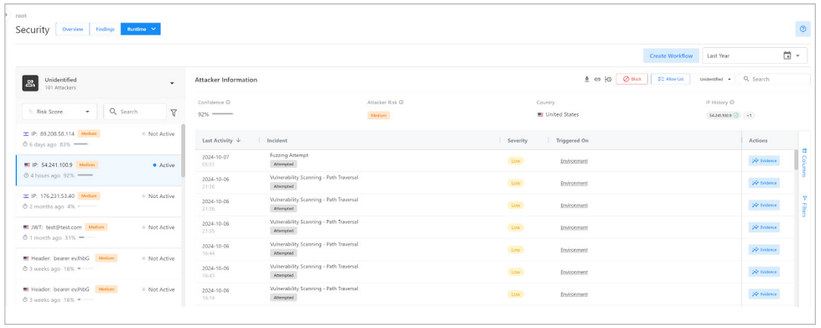
Ein Fall ähnelt einer Warnmeldung und wird immer dann erstellt, wenn anomales API-Verhalten erkannt oder eine Fehlkonfiguration gefunden wird. Wenn Fälle generiert werden, können Warnmeldungen automatisch an ein SIEM wie Splunk oder QRadar gesendet werden. Außerdem können Warnmeldungen automatisch an ein Ticketsystem wie ServiceNow oder Jira gesendet werden.

Falldetails

Jeder durch das Laufzeitschutz-Modul von Akamai API Security erstellte Fall umfasst den Schweregrad und Status, eine Zuordnung zu den OWASP Top 10 der API-Sicherheitsrisiken sowie ggf. Angreiferdetails.

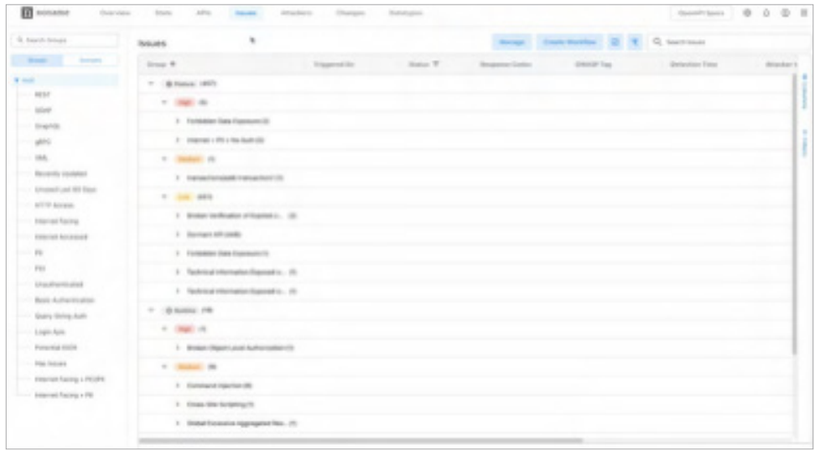
Auf den Seiten mit den Falldetails sind eine Beschreibung des Falls und seiner potenziellen Auswirkungen auf Ihr Unternehmen sowie Empfehlungen zur Problembehebung aufgeführt. Akamai API Security stellt außerdem Verlaufsprotokolle pro Angriff zur Verfügung, damit Unternehmen einsehen können, welche Handlungen die Angreifer über einen bestimmten Zeitraum vorgenommen haben, und gegen die Cyberkriminellen vorgehen können.

Beispiel: Einblicke in die Angriffshandlungen

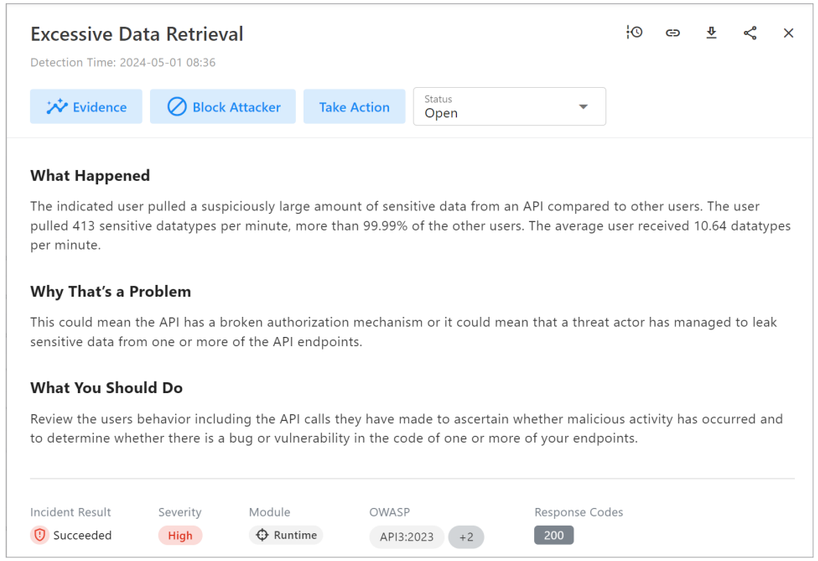


Jeder Fall enthält Nachweise. Dazu zählen die für die Fallerstellung verantwortlichen Sitzungsdetails der Angreifer sowie eine Kopie der API-Anfrage und -Antwort (sowohl Header als auch Text), um bei der schnellen Untersuchung und Lösung des Falls zu helfen. Mit intuitiven Dashboards sowie Filter-, Warn- und Berichtsfunktionen unterstützt das Laufzeitschutz-Modul von Akamai API Security Unternehmen dabei, zu ermitteln, was warum vorgefallen ist und wie dagegen vorzugehen ist.

Beispiel: Berichterstellung zu API-Fällen mit Nachweisen



Beispiel: Einblick in übermäßigen Datenabruf



Richtlinienaktionen

Mit Akamai API Security kann für jeden generierten Fall eine halbautomatische Richtlinienaktion ausgeführt werden. So können etwa ein Ticket eröffnet, Informationen an ein SIEM übertragen oder ein Webhook an ein externes System gesendet werden. Die Aktion kann auch darin bestehen, einen Angreifer abzuwehren. Welche Aktionen verfügbar sind, hängt davon ab, welche Integrationen in der Akamai-Plattform konfiguriert sind.

Die Lösung enthält zahlreiche vordefinierte Richtlinien, die sofort einsatzbereit sind, um API-Angriffe und API-Fehlkonfigurationen zu erkennen. Akamai API Security umfasst außerdem über 20 vorkonfigurierte Datentypen, mit denen Sie die Datenrichtlinien erstellen können, die Sie zur Erkennung und Ergreifung von Maßnahmen brauchen, wenn sensible Datentypen Ihre APIs durchlaufen.

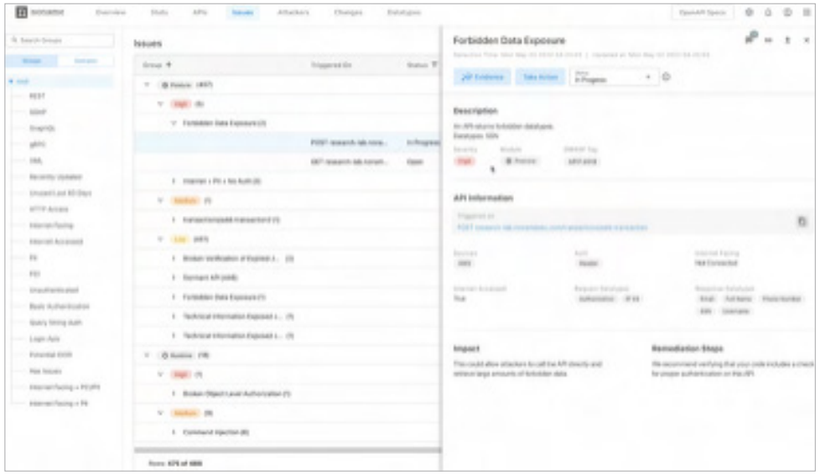
Zusammengefasst enthält das Laufzeitschutz-Modul von Akamai API Security Echtzeit-Erkennung und -Prävention von API-Angriffen zusammen mit kontinuierlicher Erkennung von API-Fehlkonfigurationen sowie viele beliebte Workflow-Integrationen, die den Betrieb und die Abhilfemaßnahmen vereinfachen.

Die Anatomie eines API-Sicherheitsvorfalls

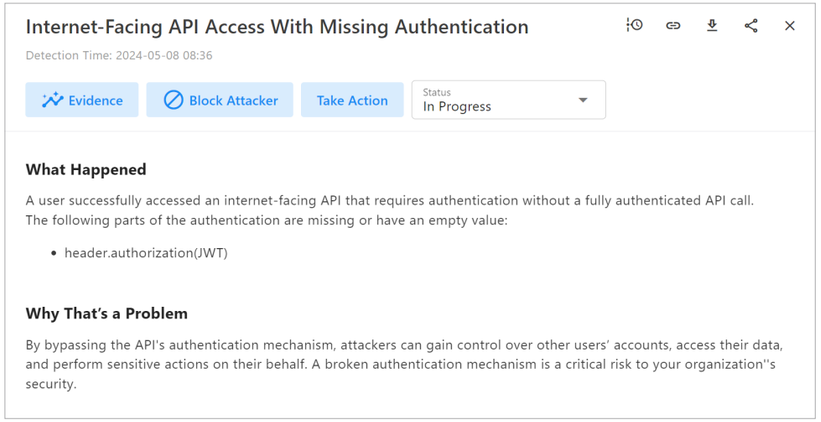
Werfen wir einmal einen Blick auf folgendes Beispiel einer Offenlegung von verbotenen Daten. Dieser Fall veranschaulicht ein Sicherheitsproblem im Inneren einer API. Die Akamai-Plattform kennt den Kontext der Datentypen und Werte, die mit jeder API verknüpft sind.

In der nachstehenden Abbildung ist zu sehen, wie verbotene Daten von einer API offengelegt werden. Die Akamai-Plattform hat erkannt, welcher Datentyp (in diesem Fall eine Sozialversicherungsnummer) übertragen wird und dass dieser zuvor als verboten gekennzeichnet wurde. Akamai erkennt auch Fehlkonfigurationen außerhalb der API, z. B. APIs, die über das Internet zugänglich, aber nicht bei einem API-Gateway registriert sind.

Beispiel: Einblicke in die Offenlegung verbotener Daten



Beispiel: Ermittlung von APIs mit fehlender Authentifizierung



Nächste Schritte zur Einrichtung eines effektiven API-Laufzeitschutzes

Jedes Mal, wenn ein Kunde, ein Partner oder ein Lieferant digital mit Ihrem Unternehmen in Kontakt tritt, arbeitet eine API hinter den Kulissen, um einen schnellen Austausch von (oft sensiblen) Daten zu ermöglichen. Durch die Implementierung wichtiger Funktionen für den API-Laufzeitschutz können Sie Ihr Unternehmen vor schnell wachsenden Angriffsvektoren schützen. Zu diesen Funktionen zählen z. B. die API-Überwachung als Verteidigungsmaßnahme gegen die Ausnutzung von Schwachstellen und Fehlkonfigurationen sowie die Verhinderung von API-Angriffen.

Erfahren Sie, wie Sie API-Sicherheitsanbieter bewerten, um sicherzustellen, dass sie kritische Laufzeitschutz-Funktionen anbieten.

Erfahren Sie, wie wir Sie unterstützen können, und vereinbaren Sie eine individuelle Demo zu Akamai API Security.

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. Gemeinsam mit Ihnen können wir auf diese Weise Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter **akamai.com** und **akamai.com/blog** oder folgen Sie Akamai Technologies auf **X** (ehemals Twitter) und **LinkedIn**.

Veröffentlicht: Dezember 2024.

Akamai