Der Leitfaden zum API-Sicherheitsmanagement

Inhaltsverzeichnis

Warum API-Sicherheit unerlässlich geworden ist

APIs ermöglichen Entwicklungsteams in Unternehmen, effizient zu arbeiten – in einem Beruf, in dem es auf Geschwindigkeit ankommt. APIs sind zwar entwicklungsfreundlich und entscheidend für die Interoperabilität von Software und Datenbeständen, doch die API-Sicherheit hat mit der Geschwindigkeit der Innovation nicht Schritt gehalten.

84 % der Unternehmen haben in den letzten 12 Monaten einen API-Sicherheitsvorfall erlebt – 2023 waren es noch 78 %.[1] Dies liegt teilweise daran, dass APIs auch Angreifenden Effizienz bieten. Viele APIs werden mit Fehlkonfigurationen, Codierungsfehlern und fehlenden Authentifizierungskontrollen erstellt. Daher kann ein API-Angriff sehr einfach durchzuführen und eine direkte Möglichkeit zum Diebstahl von Daten sein.

Und nur 27 % der Unternehmen mit vollständigen API-Bestandsaufnahmen wissen, welche APIs sensible Daten, sei es der Kundschaft oder zu geistigem Eigentum, zurückgeben – 2023 waren es noch 40 %.[2] Angesichts der zunehmenden Angriffe und geringeren Einblicke benötigen Unternehmen eine Möglichkeit, ihre API-Sicherheit zu bewerten und zu verbessern.

1, 2. Akamai, API-Sicherheitsstudie 2024

Was umfassende API-Sicherheit ausmacht

Mit zunehmender Nutzung von APIs in Ihrem Unternehmen erweitert sich auch Ihre Angriffsfläche, was neue Sicherheitsherausforderungen mit sich bringt.

Beim Sichern von APIs können die herkömmlichen Tools, die Unternehmen verwenden, wie API-Gateways und Web Application Firewalls, etwas Schutz bieten. Da API-Bestände jedoch immer komplexer werden, z. B. durch eine Vielzahl von nicht verwalteten APIs, die schwer zu erkennen und zu sichern sind, muss sich etwas ändern.

APIs sollten in der Strategie für Ihre Unternehmenssicherheit eine erhebliche Rolle spielen. Und eine dedizierte API-Sicherheitslösung, die auf die heutigen API-Risiken und Angriffsmethoden zugeschnitten ist, kann die Einblicke und Funktionen bieten, die zur Umsetzung der Strategie nötig sind. Ähnlich wie bei einem gestaffelten Sicherheitskonzept ergänzen Tools sich gegenseitig, um jeden Schritt des Angriffswegs abzudecken.

Eine umfassende API-Sicherheitsplattform, die für API-Erkennung, Sicherheitsmanagement, Laufzeitschutz und Sicherheitstests entwickelt wurde, kann Sie dabei unterstützen, versteckte API-Risiken zu erkennen, API-Angriffspfade zu identifizieren und die von Ihnen aufgedeckten Bedrohungen in Echtzeit abzuwehren.

In unserem E-Book „Der Leitfaden zur API-Erkennung“ erläutern wir das erste wichtige Element der API-Sicherheit – das Auffinden Ihrer APIs. Nachdem Sie alle APIs in Ihrem Unternehmen ermittelt und inventarisiert haben, besteht der nächste Schritt darin, Ihre gesamte API-Sicherheit zu verbessern.

Besonders wichtig kann Sicherheitsmanagement für Unternehmen sein, die fremde Anwendungen erwerben und diese als eigene Produkte verwenden, vermarkten und verkaufen. So verfügt beispielsweise fast jedes neue Fahrzeug der letzten fünf Jahre über nahezu identische Telematikfunktionen. Wenn Angreifende Sicherheitslücken in den API-Endpunkten eines Fertigungsunternehmens entdecken, erhalten sie einen einfachen Eingangspunkt für Remote-Kontenübernahmen und Datenmissbrauch.

Themen dieses Leitfadens

API-Sicherheitsmanagement bietet Ihnen die Tools zur Verwaltung, Überwachung und Aufrechterhaltung der Sicherheit Ihrer APIs während des gesamten API-Lebenszyklus. Dieser Leitfaden konzentriert sich auf die wichtigsten Anforderungen beim API-Sicherheitsmanagement – einschließlich der Erkennung von Schwachstellen und des Schutzes vertraulicher Daten. Er untersucht Methoden des Sicherheitsmanagements und beleuchtet die Funktionen der Lösung Akamai API Security vor diesem Hintergrund.

Warum Sicherheits-management?

Mit API-Sicherheitsmanagement geben Sie Ihr Bestes zum Schutz Ihrer APIs. Sie verstehen das Risiko erkannter APIs besser, indem Sie herausfinden, welche Arten von Daten durchfließen, ob Schwachstellen oder Fehlkonfigurationen vorhanden sind, ob APIs ordnungsgemäß authentifiziert sind und vieles mehr. Wer API-Schwachstellen identifiziert und schnell behebt, kann Korrekturmaßnahmen ergreifen, bevor es zu einem Angriff kommt.

Ein umfassendes Sicherheitsmanagement bietet Einblick in alle Aktivitäten rund um APIs, sodass Sie Sicherheitsrichtlinien durchsetzen, die Einhaltung von Vorschriften gewährleisten und Änderungen an Ihrem API-Ökosystem prüfen können. Es schützt und sichert Ihre APIs vor bösartigen Angriffen, Nutzung durch

Nur 27 % der Unternehmen mit vollständigen API-Bestandsaufnahmen wissen, welche ihrer APIs sensible Daten zurückgeben – 2023 waren es noch 40 %.[3]

3. Akamai, API-Sicherheitsstudie 2024

Unbefugte und Datenschutzverletzungen, die jeweils zu erheblichen Rufschäden, Geschäftsverlusten und regulatorischen Strafen führen können.

Durch die Implementierung von Best Practices für Sicherheitsmanagement wird die API-Angriffsfläche minimiert und ein Großteil Ihres API-Risikos reduziert. Gründliche Bestandsaufnahmen der APIs und sensiblen Datenspeicher Ihres Unternehmens sind für ein gutes Sicherheitsmanagement von entscheidender Bedeutung. Nachstehend gehen wir weitere Elemente des API-Sicherheitsmanagements ein: Erkennung von Schwachstellen, API-Überwachung und Problembehebung.

- ## Erkennung von Schwachstellen

  Analyse: Überprüfen Sie den Quellcode auf häufige Schwachstellen, machen Sie sich damit vertraut, wie eine API mit externen Systemen interagiert, und bewerten Sie die Autorisierungs- und Authentifizierungsfunktionen.

  Beobachtung: Überprüfen Sie den Traffic zu und von einer API, um Fehlkonfigurationen zu identifizieren, Schwachstellen zu erkennen und ein Verständnis der API-Baseline zu entwickeln.

Sicherheitsmanagement ist nur ein Teil eines umfassenden API-Sicherheitsprogramms. Außerdem ist es wichtig, umfassende Vorproduktionstests zu nutzen. So kann verhindert werden, dass Schwachstellen jemals in die Produktion gelangen.

- ## API-Überwachung

  Identifizieren und überwachen Sie API-Aufrufe in der Produktion, verfolgen Sie API-Anfragen nach, erkennen Sie Abweichungen von der Baseline-Nutzung und erstellen Sie Warnungen, wenn die API-Nutzung vordefinierte Schwellenwerte überschreitet.

- ## Problembehebung

  Beheben Sie identifizierte Schwachstellen oder Sicherheitslücken, um eine API durch Codeänderungen, Feinabstimmung von Sicherheitseinstellungen oder Patching von API-Fehlern sicherer und konformer zu machen. Ein gutes Sicherheitsmanagement ermöglicht die Behebung einer Schwachstelle, bevor diese ausgenutzt werden kann.

Funktionen zum Sicherheitsmanagement, auf die Sie nicht verzichten sollten

Möglicherweise wissen Sie bereits – oder vermuten stark –, dass Ihre API-Sicherheitslage nicht so stark ist, wie sie sein könnte. Im Folgenden sind einige wichtige Funktionen aufgeführt, die Ihre Sicherheitsmanagement-Tools enthalten müssen.

- **Klassifizierung sensibler Daten**
  Eine API, die Wetterdaten aus öffentlichen Quellen liefert, ist viel weniger besorgniserregend als eine API, die Kreditkarteninformationen übermittelt. API-Tools für Sicherheitsmanagement sollten in der Lage sein, schnell zu erkennen, wie viele APIs auf Kreditkartendaten, Telefonnummern, Sozialversicherungsnummern und andere sensible Daten zugreifen können und wie viele Nutzende über Ihre APIs auf sensible Daten zugegriffen haben.
- **Konfigurationsprüfung**
  Viele erfolgreiche Cyberangriffe sind das Ergebnis einfacher Fehlkonfigurationen von Netzwerken, API-Gateways oder Firewalls, die API-Traffic vermitteln und schützen. Für ein starkes Sicherheitsmanagement ist es erforderlich, Infrastruktur- und Softwarekonfigurationen, einschließlich Protokolldateien und Konfigurationsdateien, regelmäßig scannen zu können. Regelmäßiges Scannen trägt dazu bei, Fehlkonfigurationen und Schwachstellen aufzudecken und Risiken zu erkennen, die durch Konfigurationsabweichungen entstehen.
- **Konfidenzwert zur Einordnung von Angreifenden**
  Suchen Sie nach einer Engine zur Einordnung von Angreifenden nach Konfidenzwert. Diese sollte Algorithmen für maschinelles Lernen einsetzen, die zur Auswertung externer und interner Signale, einschließlich API-Verhalten, Netzwerktrafficmustern,

Standortdaten und Bedrohungsfeeds, entwickelt wurden. Anhand des ermittelten Konfidenzwerts können Sie einordnen, ob ein erkannter Laufzeitvorfall das Ergebnis schädlicher Aktivitäten ist. Diese einzigartige Funktion ermöglicht der Kundschaft, kritische Bedrohungen schnell einzudämmen und für Angriffe mit hoher Wahrscheinlichkeit automatische Abhilfemaßnahmen und Benachrichtigungsflüsse zu erstellen.

- **Selbst definierte Workflows**
  Neben einem anpassbaren Schweregrad müssen Sie Workflows erstellen können, um sofort Maßnahmen zu ergreifen, wenn Schwachstellen erkannt werden. Selbst definierte Workflows können von der Erstellung von Supporttickets über die Benachrichtigung wichtiger Interessengruppen bis hin zur Aktualisierung von Netzwerkkonfigurationen reichen.

- **Automatisch generierte Dokumentation**
  Die API-Dokumentation informiert Verbrauchende über den Zweck und die Verwendung einer API. Sichere APIs müssen anhand von Spezifikationen auf Konformität geprüft und genau dokumentiert werden. Eine mangelhafte oder nicht vorhandene Dokumentation erschwert Sicherheitstests und erhöht das Risiko, dass eine API mit einer unerkannten Schwachstelle in die Produktion gelangt.

Ein Outsourcing der API-Entwicklung verschärft dieses Problem häufig noch. Unabhängig von der Ursache des Problems sind veraltete, unvollständige oder nicht vorhandene Dokumentationen inakzeptabel, wenn Ihr API-Sicherheitsprogramm Erfolge erzielen soll.

Die OpenAPI-Spezifikation (früher als „Swagger“ bezeichnet) definiert die Beschreibungen von Standardschnittstellen. Sicherheitsmanagement-Tools sollten imstande sein, automatisch eine vollständige OpenAPI-Dokumentation basierend auf dem aktuellen und zukünftigen Zustand der API zu generieren. So kann sichergestellt werden, dass alle APIs ordnungsgemäß dokumentiert sind und die Dokumentation auf dem neuesten Stand ist.

Führendes Versicherungsunternehmen verbessert die API-Sicherheitslage mit Akamai

Da Verbrauchende sich von physischen Medien ab- und den digitalen zuwenden, müssen Finanzdienstleistungsunternehmen schneller Innovationen entwickeln. Wie viele andere Unternehmen in der Branche sah sich Aflac, der führende Anbieter von Zusatzkrankenversicherungen in den USA, mit wachsenden API-Sicherheitsherausforderungen konfrontiert.

Aflac fand seine Lösung in der Noname API Security Platform (jetzt Teil von Akamai API Security). Mit dem Modul für Sicherheitsmanagement kann das Team identifizieren, welche Datentypen die APIs des Unternehmens durchlaufen. So bietet es Einblicke dazu, welche APIs auf sensible Daten zugreifen, und erkennt Anomalien beim Datenzugriff.

Mehr dazu können Sie in der vollständigen Aflac-Fallstudie nachlesen.

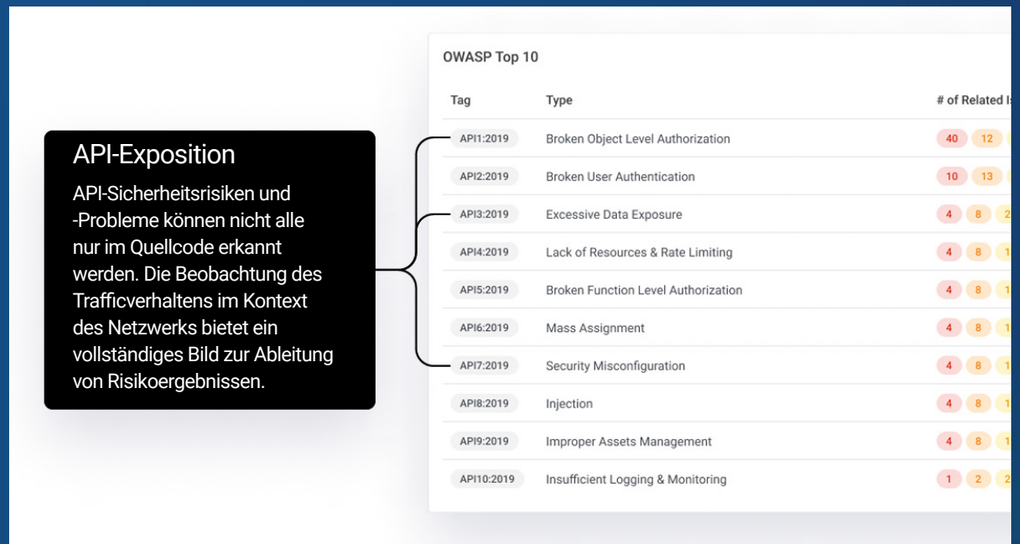
> Wir wussten, dass wir eine große API-Präsenz hatten, und wir wollten uns voll und ganz darauf verlassen können, dass wir alle APIs erkennen, dass wir vollständigen Einblick in ihren Betrieb haben und dass sie kontinuierlich auf Sicherheitsrisiken getestet werden.

– DJ Goldsworthy, VP, Security Operations and Threat Management, Aflac

Der Sicherheitsmanagement-Ansatz von Akamai

Das Modul für Sicherheitsmanagement von Akamai API Security bietet einen umfassenden Überblick über den Traffic, den Code und die Konfigurationen, um die API-Sicherheitslage Ihres Unternehmens zu beurteilen. Akamai ermittelt, wie Ihre wahre Angriffsfläche in allen APIs und Webanwendungen aussieht, und deckt alle Arten von vertraulichen Daten auf, die über Ihre APIs übertragen werden. So können Sie sensible Daten schützen.

Einfache API-Fehlkonfigurationen können Sie schutzlos gegenüber Cyberkriminellen machen. Wenn Hacker erst einmal in Ihr Unternehmen eingedrungen sind, erhalten sie schnell Zugriff auf Ihre vertraulichen Daten und können diese stehlen. Das Modul für Sicherheitsmanagement von Akamai API Security bietet folgende Hauptfunktionen:



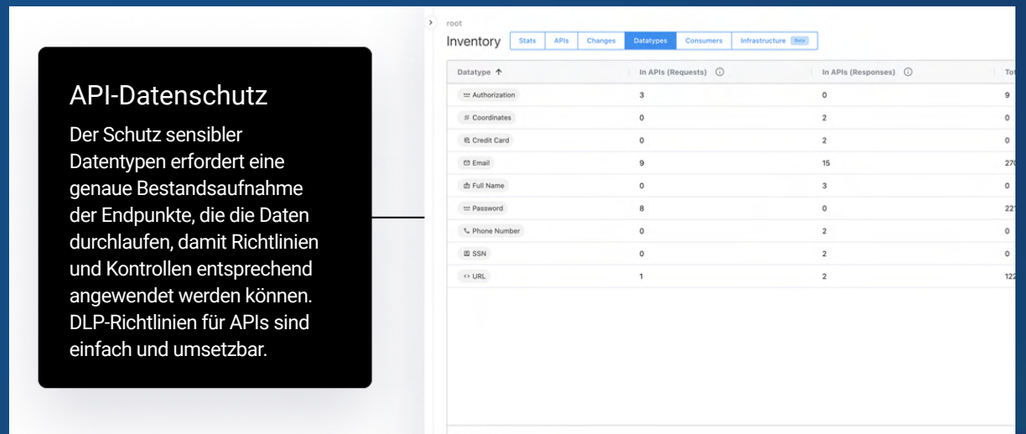
- Bandexterne Integration für kontinuierliche API-Erkennung lokal sowie in Hybrid und Public Clouds
- Eine einfache, durchsuchbare API-Bestandsaufnahme, die Details zu Schema, Netzwerkplatzierung und Datentypen enthält
- Automatisierte Erstellung von API-Dokumentation (OAS/Swagger)
- Kontextsensitive Analyse von API-Fehlkonfigurationen und Schwachstellen mit Priorisierung
- Erkennung aller Schwachstellen der Top 10 für API-Sicherheit gemäß OWASP
- Automatisierte Erkennung und Klassifizierung von vertraulichen Daten und API-Änderungen

API-Exposition

Neben der Aufdeckung von Risiken innerhalb des API-Codes ist es auch wichtig, den API-Traffic mit Blick auf das Verhalten – typisch oder atypisch – und im Kontext des Netzwerks zu beobachten.

Das Sicherheitsmanagement von Akamai API Security untersucht die größtmögliche Anzahl von Quellen, um Schwachstellen zu erkennen, darunter Protokolldateien, Verlaufstraffic, Konfigurationsdateien und vieles mehr. Die Lösung erkennt alle Schwachstellen der Top 10 für API-Sicherheit gemäß OWASP und schützt APIs vor Datenlecks, Autorisierungsproblemen, Missbrauch, illegitimer Nutzung und Datenbeschädigung.

Akamai identifiziert und priorisiert potenzielle Schwachstellen auf intelligente Weise. Schwachstellen können manuell, halbautomatisch, oder vollautomatisch durch Integration in WAFs, API-Gateways, SIEM- und ITSM-Tools, Workflow-Tools und andere Services behoben werden.



API-Datenschutz

Der Schutz sensibler Datentypen erfordert eine genaue Bestandsaufnahme der Endpunkte, die die Daten durchlaufen, damit Richtlinien und Kontrollen entsprechend angewendet werden können. DLP-Richtlinien für APIs sind einfach und umsetzbar.

Compliance nimmt mit der wachsenden Nutzung von APIs eine ganz neue Dimension ein. Als Reaktion auf die wachsende Angriffsfläche hat sich eine Reihe von Vorschriften entwickelt. Regulierte Branchen müssen APIs nun in ihre Compliancepläne einfließen lassen.

Das Modul für Sicherheitsmanagement von Akamai API Security identifiziert alle Arten von sensiblen Daten, die über Ihre APIs übertragen werden, einschließlich aller personenbezogenen Daten wie Kreditkarten, Sozialversicherungsnummern, Adressen und Versicherungsinformationen. Durch einen reduzierten Zugriff auf diese Datentypen und die Implementierung eines Datenmanagement-Frameworks können Sie sicherstellen, dass sensible Daten sich am richtigen Ort befinden und vor Bedrohungen geschützt sind.

So kann API-Sicherheitsmanagement Sie unterstützen

Jedes Mal, wenn die Kundschaft bzw. Partner- oder Lieferfirmen digital mit Ihrem Unternehmen in Kontakt treten, arbeitet eine API hinter den Kulissen, um einen schnellen Austausch von (oft sensiblen) Daten zu ermöglichen. Wenn Sie Einblicke in jede API in Ihrem Unternehmen gewinnen und deren Risikoattribute bewerten, z. B. welche APIs vertrauliche Daten zurückgeben, können Sie Ihr Unternehmen vor schnell wachsenden Angriffsvektoren schützen. API-Sicherheitsmanagement kann Sie auch bei der Einhaltung globaler Vorschriften zur Vermeidung von Datenschutzverletzungen unterstützen.

Hier erfahren Sie mehr über die Datenschutz-anforderungen, die das Anzeigen und Sichern aller APIs erforderlich machen.

Hier können Sie eine personalisierte Demo für Akamai API Security vereinbaren, in der Sie erfahren, wie wir Sie unterstützen können.

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