WHITEPAPER

8 Tipps für Ihre API-Sicherheit

Kritische Faktoren für zuverlässige API-Sicherheit

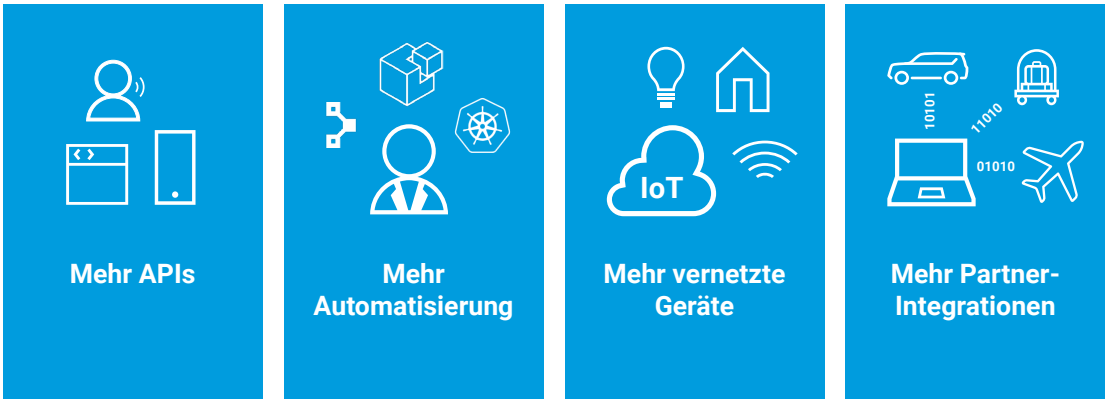
Was ist so kompliziert am API-Schutz?

Die API-Sicherheit steht bei vielen IT-Führungskräften ganz oben auf der Prioritätenliste – und das aus gutem Grund. Bedenken Sie Folgendes:

„Die explosionsartige Verbreitung von APIs bietet eine attraktive Angriffsfläche für Cyberkriminelle, und die API-Sicherheit stellt führende Sicherheitsexperten vor immer mehr Herausforderungen.“

– The Eight Components Of API Security, Forrester Research, Inc., 28. September 2023

Faktoren des API-Risikowachstums



Als Reaktion auf diese Risiken müssen Unternehmen Folgendes verstehen, bevor sie mit der Implementierung einer effektiven API-Sicherheitsstrategie beginnen:

APIs sind ein bewegliches Ziel	
Interne API-Erkennung	**Externe API-Exposition**
Bei schnellen DevOps-Prozessen werden APIs kontinuierlich erstellt und deaktiviert, was zu einem unvollständigen API-Inventar führt.	Unausgereifte API-Praktiken führen dazu, dass sensible APIs, einschließlich vieler Shadow-APIs, unbeabsichtigt externen Parteien zugänglich gemacht werden.

APIs sind anfällig für zwei verschiedene Arten von Bedrohungen	
Technische Schwachstellen	**Anwendungsfehler und Missbrauch**
Angreifer können Schwachstellen und Fehlkonfigurationen in der Software ausnutzen, einschließlich der OWASP API Security Top 10.	Missbrauch von Geschäftslogik und andere Verhaltensweisen wie aggressives Daten-Scraping können ganz unabhängig von einer technischen Schwachstelle auftreten.

Um die komplexe Herausforderung zu bewältigen, die die API-Sicherheit darstellt, ist ein durchdachter Ansatz erforderlich, der Folgendes umfasst:

Die neuesten technologischen Fortschritte nutzen

Organisatorische Hindernisse abbauen

Die gesamte API-Bedrohungslandschaft betrachten

Im Folgenden sind einige wichtige Strategien aufgeführt, die Sie bei der Entwicklung einer ausgereifteren API-Sicherheitsstrategie für Ihr Unternehmen implementieren sollten – und Stolpersteine, die Sie vermeiden sollten.

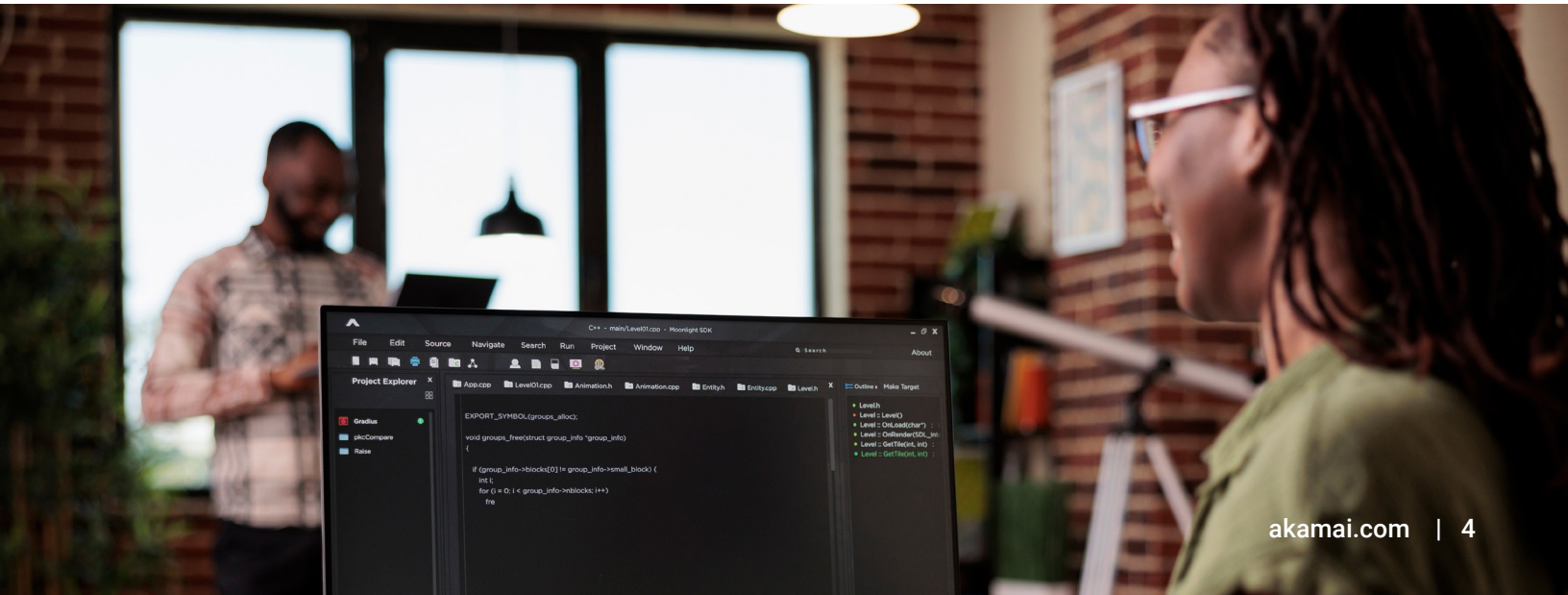
8 Tipps für effektive API-Sicherheit

1 Empfohlen: Vollständige API-Transparenz

Man kann es nicht oft genug sagen: APIs, von denen Sie nichts wissen, können Sie auch nicht schützen. Je länger eine API nicht identifiziert und überwacht wird, desto wahrscheinlicher ist es, dass sie zum Ziel eines Angriffs wird. Die beste Möglichkeit, vollständige Transparenz zu erreichen, besteht darin, sicherzustellen, dass Ihre API-Sicherheitsplattform Informationen aus einer möglichst breiten Palette an Datenquellen sammeln kann, darunter API-Gateways, Netzwerkgeräte, Orchestrierungstools für Mikroservices, Cloudanbieter und vieles mehr. Ihre API-Sicherheitslösung sollte insbesondere folgende Funktionen erfüllen können:

Zeit	Ort
• Kontinuierliche API-Erkennung • Überwachung individueller API-Aufrufe • Aufzeichnung kurzfristiger Sitzungsaktivitäten • Analyse des API-Verhaltens über längere Zeiträume hinweg	• API-Erkennung im gesamten Unternehmen • Erkennung veralteter APIs • Erkennung von Shadow-APIs

Vollständige API-Transparenz hilft Ihnen, API-Datendiebstahl zu vermeiden, insbesondere weil Angreifer seit Neuestem Ihre Angriffe langsam und über einen längeren Zeitraum hinweg durchführen, um Daten von APIs zu sammeln. Um diese neue Art von Angriffen zu verhindern, müssen Sie zuallererst wissen, wo sich all Ihre APIs befinden.



2 Vermeiden: Angst vor der Cloud

Web Application Firewalls (WAFs) verwenden signaturbasierte Techniken, um zu verhindern, dass nicht autorisierte APIs in Ihr Unternehmen gelangen. Da sich API-Angriffe jedoch kontinuierlich weiterentwickelt haben, benötigen Sie eine zusätzliche Schicht, um Ihre APIs mithilfe von Verhaltensanalysen vollständig vor allen möglichen Risiken zu schützen. Es ist entscheidend, nicht nur Ihre extern zugänglichen APIs zu überwachen, sondern auch die, die sich innerhalb Ihres Unternehmens befinden.

Um Verhaltensanalysen effektiv nutzen zu können, muss der API-Traffic in der Cloud analysiert werden. Sicherheitsteams zögern oft, vertrauliche Informationen über die Aktivitäten ihres Unternehmens in die Cloud zu senden. Ohne die Skalierbarkeit und Flexibilität der Cloud ist es jedoch schwierig, die schiere Menge an API-Daten, die die meisten Unternehmen generieren, einer echten Verhaltensanalyse mit erweiterten Erkennungs- und Antworttechniken zu unterziehen.

Da Sicherheitsteams mit ihren begrenzten Ressourcen meist bereits am Limit sind, stellen lange und komplexe Produktbereitstellungen ein großes Hindernis für den Fortschritt dar. Angesichts des wachsenden Risikos, das durch die breitere API-Nutzung entsteht, können es sich Sicherheitsteams nicht leisten, noch weiter zurückzufallen. Daher ist es wichtig, den Schritt in die Cloud als Teil Ihrer API-Sicherheitsstrategie zu wagen.

3 Empfohlen: Geschäftskontext als zentraler Bestandteil Ihrer Strategie

Die Erkennung von APIs und die Identifizierung von Sicherheitsrisiken sind erst der Anfang auf dem Weg zu einer reduzierten API-Angriffsfläche. Stellen Sie sich die folgenden drei Fragen:

1. Woher können Sie wissen, ob die API-Anmeldedaten eines bestimmten Partners kompromittiert wurden?

2. Woher können Sie wissen, ob Unternehmensspionage in Form von Daten-Scraping auf einer API stattfindet?

3. Woher können Sie wissen, ob Ihre Rechnungs-API von einem Nutzer missbraucht wird, der Rechnungsnummern auflistet, um Kontodaten zu stehlen?

Im ersten Szenario scheint die Aktivität von einem legitimen Nutzer zu stammen. Daher können schädliche Absichten nur erkannt werden, weil sich die betreffende API anders als erwartet verhält. Das zweite und dritte Szenario sind auch Beispiele für nicht zulässiges Verhalten, das legitime API-Zugriffsmodelle ausnutzt. In diesen Fällen ist es unerlässlich, neben dem technischen Geschehen auch den Geschäftskontext im Blick zu behalten.

4 Vermeiden: Daten als Einbahnstraße

Eine der grundlegenden Funktionen eines effektiven API-Sicherheitsansatzes ist die Möglichkeit, Warnungen und Ereignisse an bevorzugte Sicherheitsüberwachungs- und IT-Workflow-Tools zu senden. Ein häufiger Fehler von Sicherheitsanbietern – und den Teams, die die Warnungen implementieren – besteht darin, Sicherheitswarnungen und automatisierte Antworten als einseitigen Kommunikationsfluss zu betrachten.

Genau wie viele legitime Geschäftsprozesse können Angriffe über einen langen Zeitraum hinweg stattfinden. Um effektiv zu sein, müssen Verhaltensanalysen für die API-Nutzung über einen Zeitraum von mindestens 30 Tagen durchgeführt werden. Dies liefert ein vollständigeres und genaueres Bild des erwarteten Verhaltens als Ausgangsbasis. So können auch Angriffe erkannt werden, die langsam über mehrere Tage oder Wochen hinweg ausgeführt werden – und über mehrere API-Sitzungen hinweg. Denken Sie etwa an einen Daten-Scraping-Angriff, der über einen längeren Zeitraum hinweg durchgeführt wird und die definierte Rate nicht übersteigt: Ein solches Verhalten kann nur entdeckt werden, wenn das Verhalten im Verlauf mit allen Änderungen verglichen wird.

Eine Warnung ohne zusätzliche Informationen schadet meist mehr als sie nützt. Eine Warnung mit umfassendem Kontext über Ursache und Auswirkungen ist viel besser umsetzbar. Der eigentliche Vorteil besteht jedoch darin, dass der Empfänger eine kontextreiche, umsetzbare Warnung erhält und Zugriff auf einen umfassenderen Datensatz hat, um den Vorfall zu analysieren. So können Sie Ihren WAF-Schutz nutzen, um den Traffic, der eine potenzielle Bedrohung für Ihr Unternehmen darstellt, sofort zu blockieren.

5 Empfohlen: Abteilungsübergreifende Zusammenarbeit

Einige der größten Fortschritte bei der API-Sicherheit können durch die proaktive Vermeidung von Schwachstellen bereits in der Entwicklungs- und Bereitstellungsphase erzielt werden. Um dies effektiv umzusetzen, müssen Ihre Teams zusammenarbeiten.

Beginnen Sie diesen gemeinsamen Prozess, indem Sie API-Teams Einblicke in die Verwendung (und den Missbrauch) von APIs unter realen Bedingungen geben. Im Laufe der Zeit führt dies dazu, dass Sicherheitsfragen bereits früh in den API-Entwicklungs- und -Bereitstellungsprozessen berücksichtigt wird. Stellen Sie außerdem Folgendes sicher:

- Zusätzlich zu den wichtigsten Sicherheitsfunktionen Ihres Ansatzes gibt es auch nicht sicherheitsrelevante Vorteile, die API-Teams dabei unterstützen, effektiver zu arbeiten.
- Nutzer wie Entwickler, die sich nicht mit Sicherheit beschäftigen, müssen API-Inventar- und Aktivitätsinformationen einfach anzeigen und abfragen können.
- Nutzen Sie kontextbezogene Antworten wie Integrationen in Entwicklungstools, z. B. Jira, um proaktiv Tickets für Sicherheitskorrekturen zu eröffnen, die Entwickler durchführen müssen.

Wenn Sie die API-Sicherheit als Aufgabe für alle sehen und es Stakeholdern außerhalb des Sicherheitsteams leicht machen, sich einzubringen, können Mitarbeiter Ihrer Entwicklungs-, Betriebs- und Sicherheitsteams produktiv zusammenarbeiten, anstatt sich gegenseitig die Schuld für Probleme zuzuweisen.

6 Vermeiden: APIs von Drittanbietern vergessen

Ein weiteres häufiges Problem bei der API-Sicherheitsstrategie ist die Annahme, dass nur die eigenen APIs geschützt werden müssen. So wünschenswert der Gedanke auch ist, dass die von Ihnen erworbene WAF-Lösung oder das API-Gateway Ihre gesamte API-Sicherheitsstrategie standardisiert – dies ist leider nicht immer der Fall.

Nur weil eine zentralisierte API-Gateway-Strategie umgesetzt wurde, heißt das nicht, dass nicht beispielsweise Shadow-APIs Ihren API-Governance-Ansatz umgehen könnten. Wenn Ihr Unternehmen auf APIs von Drittanbietern angewiesen ist, würde Ihr Gateway diese APIs als authentifiziert ansehen, selbst wenn sie vor der Verbindung mit Ihrem Ökosystem kompromittiert wurden.

Ihre API-Schutzstrategie muss mit Ihren primären API-Technologien wie API-Gateways verknüpft sein und gleichzeitig möglichst viele Informationen aus anderen Quellen wie Netzwerkgeräten, Cloudplattformen und Orchestrierungstools für Mikroservices sammeln. Nur so entsteht ein vollständiges Bild Ihrer API-Angriffsfläche und Ihre Sicherheitsstrategie kann zukunftssicher gestaltet werden, wenn es unweigerlich zu Technologie- und Infrastrukturveränderungen kommt.

7 Vermeiden: Reaktiv bleiben

Obwohl schnelle und effektive Reaktionen auf Warnungen eine gute Sache sind, sollten Sie sich auf keinen Fall nur darauf konzentrieren, auf Warnungen zu reagieren, wenn sie auftreten. Ziehen Sie stattdessen eine proaktive Bedrohungssuche in Betracht. Wenn Ihr API-Sicherheitspartner es Ihnen ermöglicht, Datenabfragen durchzuführen, können Sie Ihre eigenen Hypothesen testen, Beziehungen verstehen und potenzielle Bedrohungen identifizieren, bevor sich daraus ein Sicherheitsvorfall ergibt. Wenn Sie beispielsweise auffälliges API-Nutzungsverhalten bei einem bestimmten Partner identifizieren, können Sie mit wenigen Klicks bei anderen Partnern oder Lieferanten nach ähnlichem Verhalten suchen.

Jeder API-Sicherheitspartner muss historische Daten in einem Data Lake speichern und Zugriff auf diese Daten gewähren, um Ermittlungen und Bedrohungssuche zu ermöglichen.

Im Idealfall sollten diese umfangreichen Abfragefunktionen auf zwei Arten zur Verfügung stehen:

1. als einfache und intuitive Web-Nutzeroberfläche

2. als eine Reihe von API-Schnittstellen zum API-Sicherheitsanbieter selbst zur Verwendung bei der Entwicklung komplexerer Workflows

8 Empfohlen: API-Sicherheit als kontinuierlicher Lebenszyklus

Der beste Weg, um API-Sicherheit direkt in Ihr Unternehmen zu integrieren, sind API-Tests. Wenn Sie dieses Tool zum API-Lebenszyklus hinzufügen, können Sie die Wahrscheinlichkeit verringern, dass eine falsch konfigurierte oder anfällige API eingeführt wird. Durch Testen und Ausbessern zu einem früheren Zeitpunkt im Entwicklungszyklus reduzieren Sie Belastungen, sparen Zeit und senken die Kosten.

Als Nächstes sollten Sicherheitsteams als Grundlage ihrer API-Schutzmaßnahmen alle APIs inventarisieren, die in ihrem Unternehmen zum Einsatz kommen. Da APIs kontinuierlich hinzugefügt und stillgelegt werden, ist es für Sicherheitsteams wichtig, ein Inventar der API-Schnittstellen in ihren sensiblen Anwendungen und Daten-Repositorys zu führen. Wenn die kontinuierliche API-Erkennung effektiv durchgeführt wird, gehören Shadow- und Zombie-APIs sowie nicht autorisierte, vergessene, verwaiste und veraltete APIs bald der Vergangenheit an.

Sicherheitsteams sollten die Transparenz haben, die sie benötigen, um eine Vielzahl neuer API-Sicherheitsbedrohungen zu erkennen und abzuwehren. Doch die Bedrohungserkennung muss auch während der Laufzeit erfolgen. Missbrauch von Geschäftslogik findet nur auf aktiven APIs statt. Der Vergleich des Laufzeitverhaltens mit normalen Nutzungsmustern hilft dabei, missbräuchliches Verhalten aufzudecken.

Und schließlich ist es wichtig, auch während der Laufzeit in der Lage zu sein, Bedrohungen zu stoppen, die Ihre APIs ausnutzen können. Das automatische Blockieren durch die WAF ist für diesen Schritt von entscheidender Bedeutung, da es für den Schutz Ihres Unternehmens auf Makroebene nicht ausreicht, einfach nur Warnungen für alles zu erhalten. Andere automatisierte Antworten können variiert und angepasst werden, wie z. B. die Senkung eines Ratenlimits für das API-Gateway, das Eröffnen eines Jira-Tickets, damit ein Entwickler die Sache untersucht, oder das Senden einer E-Mail an das Sicherheitsteam. Es kann nur dann auf jede erkannte Bedrohung angemessen reagiert werden, wenn der Kontext verstanden und die Reaktion dementsprechend angepasst werden kann.

Zusammenfassung

Empfohlen	Zu vermeiden
✓ Vollständige API-Transparenz	✗ Angst vor der Cloud
✓ Geschäftskontext als zentraler Bestandteil Ihrer Strategie	✗ Daten als Einbahnstraße
✓ Abteilungsübergreifende Zusammenarbeit	✗ APIs von Drittanbietern vergessen
✓ API-Sicherheit als kontinuierlicher Lebenszyklus	✗ Reaktiv bleiben

Verlieren Sie keine wertvolle Zeit

Sind Sie bereit, den ersten Schritt zu einem modernen, systematischen Ansatz für die API-Sicherheit zu machen?

Erfahren Sie mehr über Akamai API Security.

Der cloudbasierte Ansatz von Akamai ermöglicht einen einfachen Einstieg in nur wenigen Minuten. Innerhalb weniger Stunden erhalten Sie ein vollständiges Bild der API-Nutzung in Ihrem Unternehmen, einschließlich detaillierter Einblicke in die Beziehungen zwischen Ihrer Geschäftslogik und Ihren APIs.