Akamai

WHITE PAPER

Die 11 wichtigsten Funktionen der API-Erkennung und -Fehlerbehebung

Weiterentwicklung Ihrer API-Sicherheitsstrategie

Einführung

APIs spielen bei jeder Anwendung, die Ihr Unternehmen für Kunden erstellt, intern verwendet oder Anbietern und Lieferanten zur Verfügung stellt, eine entscheidende Rolle. Die Aufgabe von APIs: Austausch von Informationen (oft sensible Daten) zwischen Technologien. Wo APIs sich befinden: Nicht nur in Ihren Anwendungen, sondern auch in Ihren Cloudmigrationen, generativen KI-Tools und der digitalen Lieferkette.

Die Herausforderung besteht darin, dass APIs auch in der Angriffsoberfläche Ihres Unternehmens einen wichtigen Platz einnehmen.

Da Unternehmen nach schnellen Innovationen streben, werden APIs oft überstürzt entwickelt, unzureichend getestet und gelangen trotz Fehlkonfigurationen und fehlende Sicherheitskontrollen in die Produktion. Darüber hinaus haben sich diese APIs so stark ausgebreitet, dass Sicherheitsteams in einen Großteil ihrer API-Bestände keinen Einblick haben. Und ohne angemessenen Einblick kann Unternehmen Folgendes passieren:

1. Sie können keine APIs erkennen, die nicht verwaltet werden, vergessen wurden und unkontrolliert vertraulichen Daten, dem Internet und Angreifern gegenüber exponiert sind
2. Sie können daraufhin andererseits keine API-Risiken erkennen. So wissen zum Beispiel nur 27 % der Unternehmen mit vollständigen API-Bestandsaufnahmen, welche ihrer APIs sensible Daten zurückgeben – 2023 waren es noch 40 %
3. Sie weisen letztendlich eine Angriffsfläche voller API-zentrierter Schwachstellen auf, die Angreifer häufig – und leicht – ausnutzen

Bis vor Kurzem hat es Unternehmen genügt, sich auf eine Reihe häufig verwendeter Tools für die Verwaltung von APIs und einen grundlegenden Schutz zu verlassen. Doch angesichts der Tatsache, dass 84 % der Unternehmen in den letzten 12 Monaten einen API-Sicherheitsvorfall erlebt haben – 2023 waren es noch 78 % –, muss sich das ändern.

Da API-Angriffe immer häufiger geschehen und immer ausgefeilter werden, ist es Zeit, Tools wie API-Gateways, Web Application Firewalls (WAFs) und WAAP-Plattformen (Web Application and API Protection) um weitere Schutzebenen zu erweitern.

Diese neuen Ebenen sollten einen besseren Einblick in alle APIs in Ihrer Umgebung und deren Risiken bieten. Das umfasst auch den großen Anteil der nicht verwalteten APIs, wie z. B.:

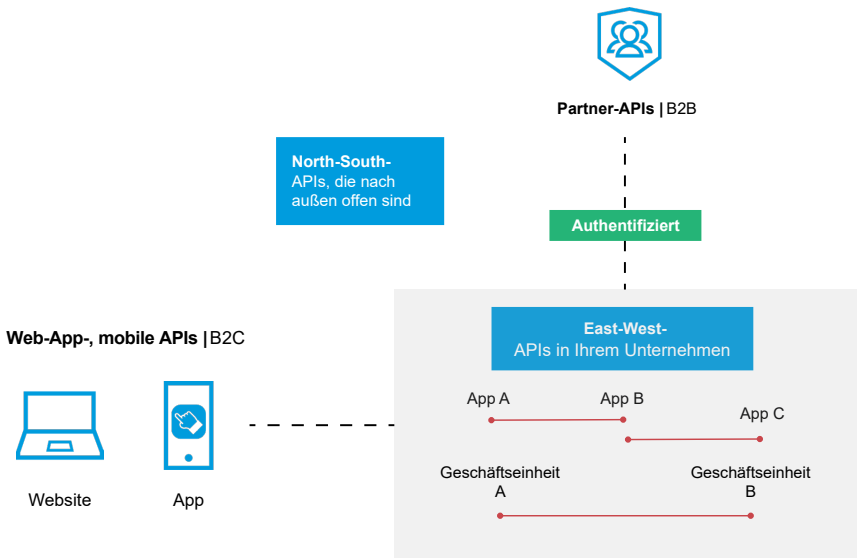
- Zombie-APIs, die deaktiviert werden sollten, aber aktiv bleiben
- Shadow-APIs, die nicht dokumentiert sind und entweder entfernt oder in formelle Governance-Prozesse integriert werden sollten

Unternehmen benötigen außerdem tiefergehendere Funktionen zur Erkennung und Bekämpfung von API-Missbrauch und -Angriffen (einschließlich aller Bedrohungen, die in den OWASP-Top-10-API-Sicherheitsrisiken beschrieben sind). Und um Schwachstellen während des gesamten Lebenszyklus einer API zu finden und zu beheben, sollten Unternehmen strenge Echtzeit-Sicherheitstests für APIs durchführen, und zwar von den frühen Entwicklungsphasen bis zur Produktion.

Bedeutet das, dass für jedes auftretende Problem ein neues Tool benötigt wird? Nein. Es ist eher so, dass Unternehmen sicherstellen, dass ihr „Orchester" über die wichtigsten Instrumente verfügt, und diese zur richtigen Zeit die richtigen Töne spielen – und zwar in präziser Abstimmung mit den Kollegen.

Wenn Sie darüber nachdenken, wie Sie Ihren API-Schutz um eine neue Ebenen erweitern können, sollten Sie den Defense-in-Depth-Ansatz, den Sicherheitsteams auf andere Bedrohungen anwenden, in Erwägung ziehen. Sie könnten zum Beispiel ein Netz aus Kontrollen bereitstellen, um die Auswirkungen eines Ransomware-Angriffs zu erkennen, zu verhindern und abzumildern. So sollten Unternehmen Ihre APIs betrachten.

In diesem Whitepaper stellen wir 11 kritische Funktionen vor, die Sie in Ihre API-Sicherheitsstrategie einbetten können. Dabei konzentrieren wir uns auf die Erkennung von API-Bedrohungen und die entsprechende Reaktion.



Kontext ist entscheidend

Welchen Stellenwert haben die API-Bedrohungserkennung und -Fehlerbehebung in Ihrer API-Sicherheitsstrategie?

Wie Sie wahrscheinlich selbst festgestellt haben, haben APIs die Arbeitsweise von Unternehmen verändert, denn sie ermöglichen mehr Anwendungsfälle, beschleunigen Veränderungen, übertragen mehr vertrauliche Daten und stehen mehr Nutzern zur Verfügung. Es überrascht also nicht, dass Unternehmen viel mehr API-Kanäle als Webanwendungsschnittstellen erstellt haben. Und das Risiko steigt weiter, denn in diese sich steigernde Zahl von APIs, sind wachsende Mengen an zentralen Geschäftsdaten und Geschäftslogik eingebettet.

Angesichts der Ausbreitung von APIs in den unzähligen Technologien, die Sicherheitsteams bereits schützen (d. h. Anwendungen), unterstützen die meisten Kategorien von Sicherheitsprodukten APIs in irgendeiner Form. APIs und Anwendungen sind jedoch nicht identisch; in einigen Compliance-Frameworks handelt es sich dabei sogar unterschiedliche Assets. Es reicht nicht aus, zum Beispiel ein vorhandenes Produkt für Anwendungssicherheit durch einige API-Funktionen zu erweitern. APIs verdienen mehr Aufmerksamkeit, als sie in den meisten Unternehmen normalerweise erhalten. Die Sicherheitsteams von heute sollten APIs als separate Asset-Klasse mit spezifischen Risikoattributen betrachten und nach kritischen Funktionen suchen, um jede API in großem Maßstab sehen und schützen zu können.

Wenn ein Unternehmen in der Vergangenheit über eine API-Bestandsaufnahme und einige grundlegende Tools für API-Management und -Schutz verfügte, hatte es gute Chancen, eine Reihe von gängigen API-Angriffen zu verhindern. Leider sind die Angreifer heutzutage – genau wie die Unternehmen – innovativ und wollen sich kontinuierlich verbessern.

- Cyberkriminelle entwickeln ihre Taktiken konsequent weiter, um die Tools zu umgehen, von denen bekannt ist, dass die meisten Unternehmen sich beim Schutz Ihrer APIs darauf verlassen.
- Wie die meisten Unternehmen KI nutzen, erweitern auch Angreifer ihre begrenzten menschlichen Fähigkeiten mit Hilfe von generativen KI-Funktionen, die ihnen rund um die Uhr zur Verfügung stehen.
- Angreifer suchen immer häufiger nach Schwachpunkten in der über APIs verbundenen digitalen Lieferkette eines Unternehmens, wie z. B. dessen B2B-Partnern, für die der API-Schutz möglicherweise keine Priorität darstellt.

Einige Formen des API-Missbrauchs gehen beispielsweise von Kunden und Partnern aus, die ihre rechtmäßig erhaltenen API-Anmeldedaten auf unbefugte Weise nutzen. So können scheinbar legitime API-Anmeldedaten oder Sicherheitstoken auch gestohlen sein. Verborgene Schwachstellen in API-Client-Implementierungen eröffnen einen weiteren Angriffsvektor, über den die Angreifer die APIs auf eine Weise missbrauchen können, die herkömmliche Sicherheitstools nicht erkennen können.

Glücklicherweise gibt es bereits zahlreiche wichtige Funktionen, mit denen Unternehmen ihre APIs vor sich schnell entwickelnden Angriffsmethoden können. Lesen Sie weiter, um mehr über die 11 Hauptfunktionen zu erfahren, mit denen Ihr Team beginnen kann, Maßnahmen zu ergreifen, um Ihre APIs und die Daten, die sie austauschen, vor Angriffen zu schützen.

Kritische Fähigkeit Nr. 1

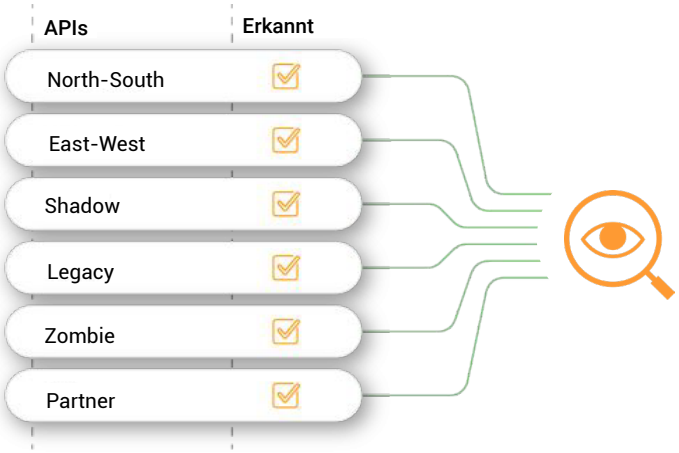
Kontinuierliche API-Erkennung und Kontrolle der Sicherheitslage

Ein umfassender und kontinuierlich aktualisierter Bestandsüberblick über APIs, die im Unternehmen verwendet werden, ist die Grundlage jeder API-Sicherheitsstrategie. Der einfache Grund: Ein Unternehmen kann nicht etwas schützen, von dem es nicht einmal weiß, dass es sich in seiner Umgebung befindet. Viele API-Sicherheitsprodukte geben an, eine gewisse API-Erkennung durchzuführen, sind jedoch auf den On-Demand- oder Tagesbetrieb beschränkt. Die API-Erkennungsfunktionen Ihrer Plattform müssen in jedem Fall Folgendes umfassen:

- Automatisierte und kontinuierliche Erkennung von APIs rund um die Uhr, insbesondere Erkennung von APIs, die nur einmal verwendet werden (On-Demand- oder tägliche Erkennung reicht nicht aus)
- Erkennung von APIs über verschiedene Technologien und Infrastrukturen hinweg
- Erkennung neu bereitgestellter APIs und Vergleich mit gut dokumentierten APIs zur Identifizierung von Shadow-APIs
- Risikobeurteilung für jeden API-Service und Endpunkt – dies hilft sowohl dem Sicherheits- als auch dem Entwicklungsteam, Klarheit zu schaffen und APIs mit den größten potenziellen Auswirkungen bei einer Kompromittierung zu priorisieren
- Erkennung von Instanzen bekannter API-Sicherheitsrisiken (siehe z. B. OWASP-Top-10 der API-Sicherheitsrisiken)

Mehr Transparenz

Nie wieder den API-Bestand aus den Augen verlieren



Kritische Fähigkeit Nr. 2
Visualisierung des API-Verhaltens

Die Fähigkeit zur Visualisierung des tatsächlichen API-Verhaltens (API-Aufrufe) ist für eine API-Sicherheitsplattform eine Grundvoraussetzung. Darüber hinaus ist diese Fähigkeit erforderlich, damit wichtige Stakeholder aus Sicherheit, Entwicklung und Betrieb sehen und verstehen können, wie APIs verwendet oder missbraucht werden. Dann können die Teams miteinander kommunizieren und Fälle untersuchen. Achten Sie insbesondere auf diese Visualisierungsfunktionen:

- **Untersuchung:** Jede Warnung sollte die Möglichkeit bieten, die ursprüngliche API-Aktivität aufzurufen, um so den speziellen Auslöser der Warnung zu identifizieren.
- **Datenintegrität und -anreicherung:** Bei jedem API-Aufruf sollte erkennbar sein, wer der Nutzer ist, welchen Vorgang er verwendet hat, welche Datensätze er aufgerufen oder bearbeitet hat, welche Header und Parameter verwendet wurden usw.
- **Datenschutz:** Datenintegrität ist wichtig, doch vertrauliche Daten können nicht als ruhende Daten gespeichert werden. Eine Lösung sollte den Traffic analysieren und nur relevante Metadaten senden, um Dashboards zu aktualisieren.

Kritische Fähigkeit Nr. 3

API-Missbrauchsversuche durch Kontext von Nutzerentitäten offenlegen

Sicherheitsteams müssen in der Lage sein, schädliche Aktivitäten im Bezug auf Entitäten wie IP-Adressen und Geschäftsprozesseinheiten wie Zahlungs-IDs zu verfolgen. Diese Fähigkeit kann in Kombination mit Funktionen zur Korrelation von Angriffen von verschiedenen IPs sehr wertvoll sein, beispielsweise in Fällen, in denen andere relevante Kennungen einen Kontext zum API-Missbrauch bieten können.

Angenommen, ein unbekannter Nutzer ruft die API eines Einzelhandelsunternehmens mit der ID / api/getpaymentID/50 auf. In diesem Szenario weiß das Sicherheitsteam des Einzelhandelsunternehmens, dass jeder andere Nutzer auf der Plattform des Unternehmens an eine Art von Zahlungs-ID gebunden ist. Wenn ein Sicherheitsanalyst das plötzlich bemerkt, dass der unbekannte Nutzer wiederholt Aufrufe durchführt, wobei die ID-Nummer jedes Mal leicht angepasst wird (/api/getPaymentID/51 … 52 … 53 … 54), ist dies ein wichtiger Indikator für einen versuchten API-Missbrauch.

Echtzeiteinblicke in atypisches Nutzerverhalten können dem Unterschied zwischen einem vereitelten Versuch einer Sicherheitsverletzung und einem erfolgreichen API-Angriff ausmachen.

943.162 $

Die durchschnittlichen Kosten für die Behebung von API-Sicherheitsvorfällen laut US-amerikanischen CISOs, CIOs und CTOs, die in den letzten 12 Monaten solche Ereignisse gemeldet haben.

Mehr über die Ansichten und Erfahrungen Ihrer Kollegen erfahren Sie in der API-Sicherheitsstudie 2024.

Kritische Fähigkeit Nr. 4
Verhaltensanalyse und -erkennung

Obwohl die Analyse einzelner API-Aufrufe von Nutzerentitäten – oder sogar einzelner Sitzungen – Sicherheitsteams unterstützen kann, ist es wichtig, eine umfassende API-Bedrohungserkennung zu haben, die das Gesamtbild überwacht. Suchen Sie nach Möglichkeiten, um ein besseres Verständnis von Verhaltensmustern und Anomalien in der gesamten API-Umgebung zu erlangen. Um festzustellen, ob eine API sich nicht normal verhält, – was darauf hinweist, dass sie kompromittiert ist –, sollte die API-Nutzung über längere Zeit und mit einer Kontextgrundlage, die durch eine gründliche Verhaltensüberwachung über lange Zeit erstellt wurde, analysiert werden. Dadurch erhalten Sicherheitsteams eine zuverlässige Grundlage, während sie das Verhalten kontinuierlich überwachen, um Anomalien zu erkennen.

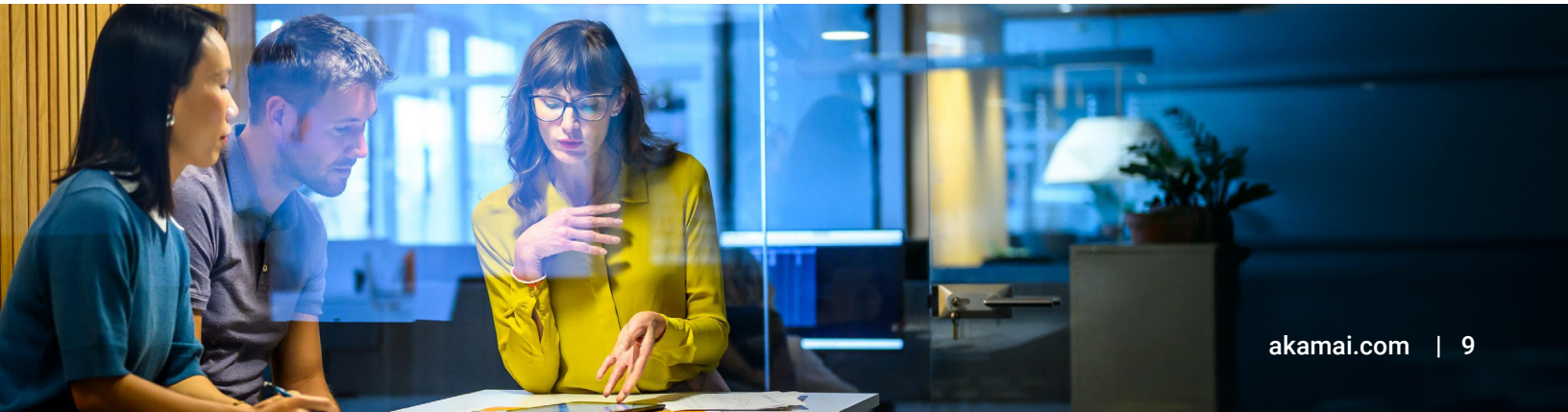
Kritische Fähigkeit Nr. 5
Erkennen der Abweichung von API-Spezifikationen

Zwischen sich verändernden Markterfordernissen und Geschäftsanforderungen unterliegen APIs einem ständigen Wandel. Aus diesem Grund veröffentlichen Unternehmen ständig neue Endpoint-Implementierungen, um dynamisch wachsende Unternehmensanforderungen zu erfüllen, Fehler zu beheben und technische Verbesserungen einzuführen. Die Aktualisierung der API-Dokumentation im Einklang mit diesen Änderungen auf Grundlage der API-Spezifikationen ist entscheidend. Dabei sollten Sie besonders darauf achten, dass der API-Traffic immer mit den API-Spezifikationen übereinstimmt.

Um APIs widerstandsfähig gegen Missbrauch und Angriffe zu machen, sollten Unternehmen nach Möglichkeiten suchen, um Abweichungen von API-Spezifikationen zu erkennen. So können sie Abweichungen oder Lücken in der API-Dokumentation erkennen, indem sie den Echtzeit-API-Traffic kontinuierlich mit den definierten Spezifikationen vergleichen.

Wenn die Funktion zur Erkennung von Abweichungen der API-Spezifikationen Unstimmigkeiten oder nicht dokumentierte Endpoints entdeckt, auf die in der Produktion zugegriffen wird, kann sie Entwickler und Sicherheitsteams benachrichtigen und ihnen folgende Möglichkeiten bieten:

- Problemen immer einen Schritt voraus zu sein, bevor sie kritisch werden
- Sicherstellen, dass APIs wie vorgesehen funktionieren
- Verbessern der Sicherheit für die Anwendungen, die diese APIs unterstützen
- Wahrung der Integrität des API-Ökosystems des Unternehmens



Kritische Fähigkeit Nr. 6
B2B- und East-West-API-Abdeckung

Der größte Wachstumsbereich bei der API-Nutzung liegt in B2B-Anwendungsfällen – sowohl intern als auch extern. Die API-Sicherheit muss B2B- und Machine-to-Machine-APIs umfassen, einschließlich North-South- (extern) und East-West-Instanzen (intern).

Obwohl B2C-Webanwendungen über WAAP- und WAF-Plattformen geschützt werden, sind einige äußerst heikle API-Aktivitäten, wie interne East-West-APIs oder proprietäre Anwendungsfunktionen, die Partnern über B2B-APIs zugänglich gemacht werden, selbst beim Durchlaufen des WAAP immer noch gefährdet.

Wenn ein Nutzer in einer B2B-Partner-API authentifiziert wurde, gilt er häufig als sicher, und es wird keine weitere Überwachung durchgeführt. Damit entsteht in vielen Unternehmen eine kritische Lücke in der API-Sicherheit. Um ein vollständiges Bild der API-Aktivitäten und der allgemeinen Bedrohungssituation zu erhalten, müssen Unternehmen einen Ansatz verfolgen, der für alle Anwendungsfälle effektive Transparenz, Beobachtung und Überwachung bietet.

Kritische Fähigkeit Nr. 7
Aussagekräftige Warnungen mit Kontext

Wenn ein Unternehmen einen umfassenden Einblick in seine API-Aktivitäten und Verhaltensanalysen hat, werden Warnungen zu API-Aktivitäten wesentlich aussagekräftiger. Aber wie können Sie sicherstellen, dass Sie Ihre Aufmerksamkeit und Ressourcen auf reale API-Bedrohungen konzentrieren? Eine Engine zur Einordnung von Angreifern nach Konfidenzwert verwendet fortschrittliche Algorithmen für maschinelles Lernen, die für die Auswertung externer und interner Signale – einschließlich API-Verhalten, Netzwerk-Traffic-Muster, Standortdaten, Feeds für Bedrohungsinformationen und andere kontextbezogene Faktoren – entwickelt wurden, um den Konfidenzwert zu bestimmen, der anzeigt, dass ein erkannter Laufzeitvorfall das Ergebnis eines Angriffs ist. Diese Funktion kann ein Sicherheitsteam dabei unterstützen, kritische Bedrohungen schnell ausfindig zu machen und sollte durch Funktionen ergänzt werden, die automatische Abhilfemaßnahmen und Benachrichtigungsflüsse für Angriffe mit hoher Wahrscheinlichkeit erstellen.

Kritische Fähigkeit Nr. 8
Individuelle, automatisierte Reaktionen

Herkömmliche Inline-API-Verfahren können vermutete API-Angriffe mit automatisierten Maßnahmen blockieren. Allerdings müssen die Unternehmen dazu in der Lage sein, den Angriff überhaupt zu identifizieren. Für die Verhaltensanalyse und die Anomalieerkennung für APIs sammelt sich im Laufe der Zeit ein immer größerer Geschäftskontext an. Die damit entstehende Erkennungstiefe lässt Anomalien zum Vorschein kommen. So wird eine Vielzahl von automatisierten und angepassten Reaktionen möglich, die mit hoher Genauigkeit durchgeführt werden können. Beispiele:

- Blockieren oder Drosseln des Traffics an unterstützten API-Gateways und CDN-Edge-Filtern (Netzwerk zur Inhaltsbereitstellung, Content Delivery Network)
- E-Mail-Benachrichtigungen für Sicherheits- und Geschäfts-Stakeholder
- Tickets für Entwickler erstellen
- Auslösen von Webhooks

Was können Unternehmen tun, um überlastete Sicherheitsteams dabei zu unterstützen, ihre Produktivität und Energie zu maximieren, wenn die Zahl der API-Bedrohungen wächst? Finden Sie Automatisierungsfunktionen, die Effizienz und Produktivität steigern, indem Sie die Erstellung und Verwaltung multifunktionaler Workflows vereinfachen. Die richtigen Automatisierungsfunktionen sollten eine visuelle Designer-Schnittstelle ohne Code bieten, mit der komplexe Prozesse zur Reaktion auf Ereignisse erstellt und vorfallsbezogene Daten zwischen Ihren zentralen API-Sicherheitslösungen und unzähligen Drittanbieterservices – einschließlich ServiceNow, Jira und Azure DevOps – synchronisiert werden können.

Kritische Fähigkeit Nr. 9
Analyse von API-Traffic

Unternehmen benötigen ständig verfügbare Funktionen zur Aufzeichnung, Visualisierung und Analyse des API-Traffics in ihren Umgebungen, für die kein Datenpool bereitgestellt werden muss. Durch die Aufzeichnung von API-Datenflüssen, die bestimmten Kriterien – einschließlich typischer und anomaler API-Aktivitäten – entsprechen, können Unternehmen in verschiedenen Anwendungsumgebungen Bedrohungen effektiver ausfindig machen und gleichzeitig das Risiko kontrollieren, das verdächtige Nutzer und ungewöhnliches API-Verhalten darstellen. Es ist wichtig, dass API-Traffic-Auditfunktionen vorhanden sind, die für einen bestimmten Anwendungsfall angepasst werden können, sodass Unternehmen den Traffic gemäß vordefinierten Filtern und Regeln erfassen und speichern können.

Kritische Fähigkeit Nr. 10
Strenge API-Tests in Echtzeit

Durch den Drang zu schnellen Innovation bringen Unternehmen APIs in die Produktion, die Schwachstellen und Designfehler aufweisen, die oft unentdeckt bleiben. Mit einem Shift-Left-Ansatz zum Testen von APIs während der Entwicklung können Unternehmen diese Probleme vermeiden. Zu den Kernfunktionen zählen:

- Durchführung automatisierter Tests, die schädlichen Traffic simulieren. Dazu gehören auch die OWASP-Top-10 der API-Sicherheitsrisiken
- API-Spezifikationen anhand etablierter Governance-Richtlinien und -Regeln überprüfen
- Testen von APIs bei Bedarf oder im Rahmen einer CI/CD-Pipeline

Kritische Fähigkeit Nr. 11
Plattformunabhängiger Schutz

API-Services werden in der Regel von verschiedenen Gruppen in einem Unternehmen implementiert, die häufig verschiedene Plattformen und Technologien anwenden. Einige APIs werden beispielsweise lokal implementiert, andere dagegen werden in der Public Cloud ausgeführt. Unternehmen verwenden oft zwischengeschaltete Technologien wie Reverse Proxies, API-Gateways, WAFs und CDNs, die einen geschäftlichen Nutzen bieten, aber mehr Komplexität in der API-Transparenz erschaffen.

Es kommt entscheidend darauf an, von allen Technologien auf die API-Aktivitätsdaten zugreifen zu können. Ein plattformunabhängiger Schutz vor API-Bedrohungen sorgt dafür, dass Ihr Unternehmen stets alle API-Aktivitäten im Blick behält, unabhängig von den Details der Implementierung oder der verwendeten Infrastruktur. So erhalten Sie die Schutzabdeckung für mehrere Elemente:

- Alle Abteilungen, übernommene Unternehmen und Umgebungen
- Sowohl genehmigte als auch Shadow-APIs, unabhängig davon, ob sie das API-Gateway verwenden oder nicht

Ein plattformunabhängiger Ansatz erweitert auch die Sichtbarkeit über North-South-APIs hinaus und bezieht auch öffentliche, Partner- und interne East-West-APIs mit ein.

Wenn Ihre API-Schutzplattform so transparent wie möglich aufgebaut ist, schützt dies Ihr Unternehmen vor Bedrohungen durch interne Mitarbeiter ebenso wie vor dem Missbrauch von APIs durch Partnerorganisationen – zusätzlich zum Schutz vor den Risiken durch externe Angreifer.

Fazit

APIs sind ein wesentlicher Bestandteil der Fähigkeit von Unternehmen, in der digitalen und cloudorientierten Wirtschaft von heute Ihren Kunden zu dienen, Umsätze zu erwirtschaften und effizient zu arbeiten. Das kontinuierliche Wachstum, die Nähe zu sensiblen Daten und das Fehlen von Sicherheitskontrollen machen APIs jedoch zu eines wesentlichen Risikofaktor.

Akamai API Security bietet alle 11 kritischen Funktionen, die in diesem Whitepaper behandelt werden, und unterstützt Unternehmen dabei, mit wichtigen Funktionen auf ihren bestehenden Ansätzen aufzubauen, wie z. B.:

- Erkennung von APIs
- Bewertung von Risiken (einschließlich der Exposition gegenüber sensiblen Daten)
- Erkennung von API-Missbrauch und -Angriffen
- Testen von APIs auf Sicherheitsrisiken und Schwachstellen

Erfahren Sie mehr über den Schutz vor den OWASP-Top-10-API-Sicherheitsrisiken.

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 unter X (ehemals Twitter) und LinkedIn. Veröffentlicht: Januar 2025.