Akamai

WHITEPAPER

Die 10 wichtigsten Funktionen der API-Erkennung und Fehlerbehebung

Anpassen Ihrer API-Sicherheitsstrategie

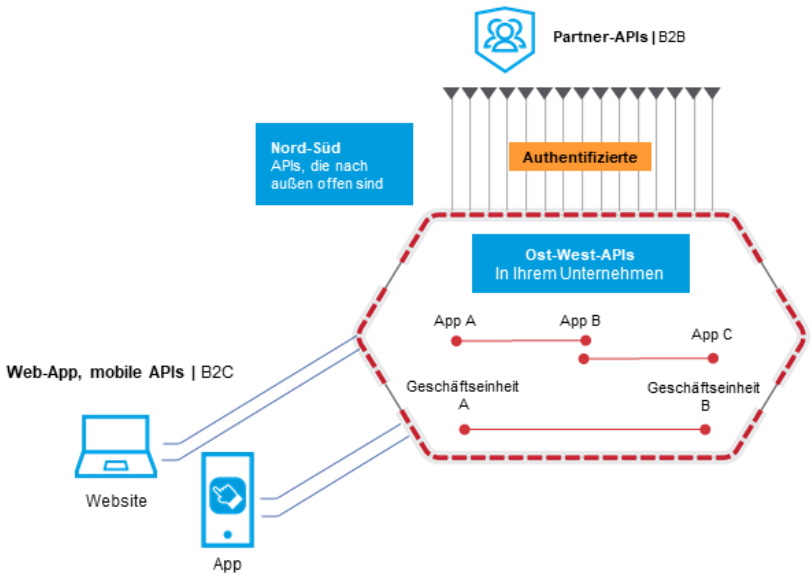
Einführung

APIs sind wichtige Bausteine auf dem Weg zu Innovationen. B2B- (Business-to-Business) und B2C-Anwendungen (Business-to-Consumer) stehen im Mittelpunkt des Wandels. Daher ist es unerlässlich, die kritische – und oftmals vertrauliche – Kommunikation zu schützen, sowohl intern zwischen Microservices als auch extern zwischen Kunden und Partnern. Den meisten Unternehmen ist inzwischen klar, dass es für den langfristigen Geschäftserfolg auf eine solide Strategie für die Anwendungssicherheit ankommt. Dabei verlassen sie sich auf Sicherheitstechnologien wie WAAP-Plattformen (Web Application and API Protection), Cloudsicherheitsfunktionen/-produkte und Tools für Sicherheitstests, um das Sicherheitsrisiko für die Anwendungen zu reduzieren. Die Angriffe haben sich laufend weiterentwickelt und zielen immer raffinierter darauf ab, die WAAPs und Ziel-APIs in Unternehmen zu umgehen. Es geht jetzt um die Frage, wie Sie Ihre API-Sicherheitsstrategie in Erwartung dieser Bedrohungen anpassen können.

Welchen Stellenwert haben die API-Erkennung und Fehlerbehebung in einer API-Sicherheitsstrategie?

In den letzten Jahren haben Unternehmen viel mehr API-Kanäle als Webanwendungsschnittstellen erstellt. Zugleich laufen über diese APIs immer mehr wichtige Geschäftsdaten und Geschäftslogik. APIs haben die Arbeitsweise von Unternehmen verändert, denn sie unterstützen mehr Anwendungsfälle, beschleunigen Veränderungen, übertragen größere Mengen an vertraulichen Daten und sind für mehr Nutzer zugänglich.

Wie sieht Ihre API-Landschaft aus?



Die meisten Sicherheitsproduktkategorien bieten eine gewisse Unterstützung für APIs, eben weil sie zunehmend verbreitet sind. APIs dagegen sind eine andere Asset-Klasse und erscheinen in einigen Compliance-Frameworks sogar als anderes Asset. Es reicht nicht, ein älteres Sicherheitsprodukt (z. B. eine WAAP-Plattform) um API-Sicherheitsfunktionen zu ergänzen, damit die neuen Probleme gelöst werden können, die durch die API-Assets erst aufgetreten sind. Sicherheitsorganisationen müssen APIs als separate Asset-Klasse behandeln und die kritischen Funktionen erkennen, die APIs umfassend schützen.

Beginnen wir mit den Grundlagen, wie sich der API-Schutz mit Blick auf die neuen Bedrohungen verändert hat. In der Vergangenheit konnten API-Bedrohungen in der Regel vermieden werden, wenn ein Unternehmen eine vollständige Übersicht seiner APIs und zuverlässigen WAAP hatte. Jetzt konzentrieren sich Angriffe auf APIs in Unternehmen und deren Partnerorganisationen darauf, den WAAP zu umgehen.

Einige Formen des API-Missbrauchs gehen beispielsweise von Kunden und Partnern aus, die ihre rechtmäßig erhaltenen API-Anmeldedaten auf unbefugte Weise nutzen. Scheinbar legitime API-Anmeldedaten oder Sicherheitstoken können 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 von herkömmlichen Sicherheitstools nicht erkannt wird.

Glücklicherweise gibt es bereits zahlreiche wichtige Funktionen, mit denen Unternehmen ihre APIs vor aktuellen Entwicklungen schützen können, insbesondere Erkennung und Fehlerbehebung. Auf den folgenden Seiten werden die wichtigsten Funktionen erläutert, die diese Plattformen effektiv auf eine sich ständig verändernde API-Bedrohungslandschaft vorbereiten.

Kritische Funktion Nr. 1
Plattformunabhängiger Schutz

API-Services werden in der Regel von verschiedenen Gruppen in einem Unternehmen implementiert, wobei häufig verschiedene Plattformen und Technologien zur Anwendung kommen. Einige APIs werden beispielsweise lokal implementiert, andere dagegen werden in der Public Cloud ausgeführt. Unter Umständen werden auch Technologien wie Reverse-Proxys, API-Gateways, WAFs (Web Application Firewall) und CDNs (Content Delivery Network) zwischengeschaltet, die die API-Transparenz noch erschweren.

Es kommt entscheidend darauf an, von allen verschiedenen 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 APIs als auch Shadow-APIs, unabhängig davon, ob sie das API-Gateway verwenden
- Erweiterte Transparenz über die North-South-APIs hinaus, einschließlich öffentlicher APIs, Partner-APIs und interner East-West-APIs

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.

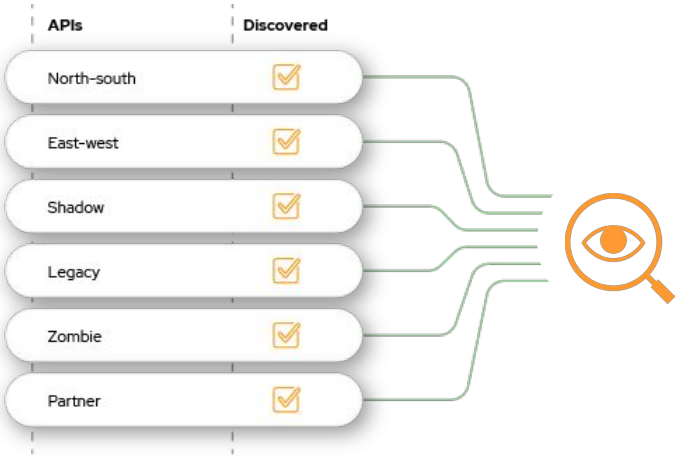
Kritische Funktion Nr. 2
Kontinuierliche API-Erkennung und Kontrolle der Sicherheitslage

Ein umfassender und kontinuierlich aktualisierter Bestandsüberblick über alle 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 aller 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
- Erkennung von Instanzen bekannter API-Sicherheitsrisiken (siehe z. B. die Top-10-Liste der OWASP)

Mehr Transparenz

Nie wieder den API-Bestand aus den Augen verlieren

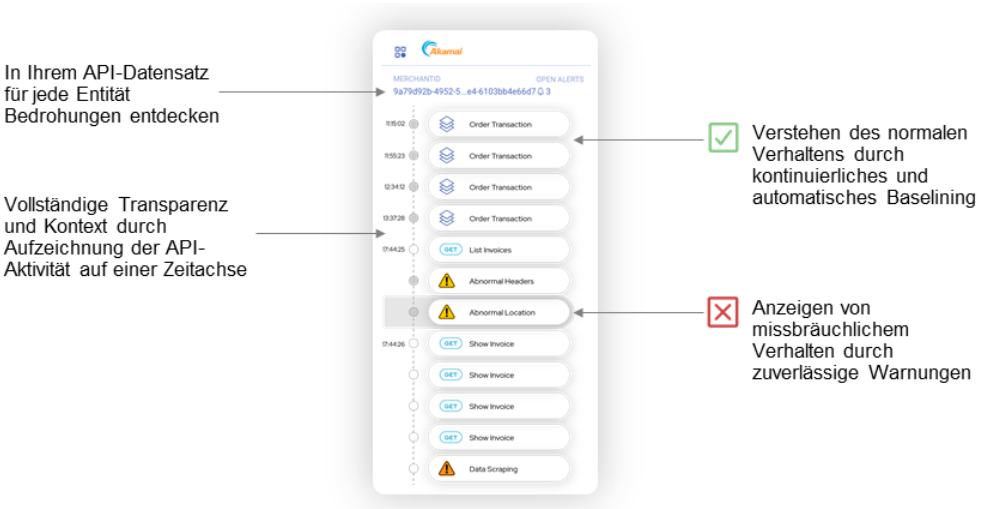


Kritische Funktion Nr. 3
Visualisierung des API-Verhaltens

Die Fähigkeit zur Darstellung und Visualisierung des tatsächlichen (API-Aufrufe) gehört zu den grundlegenden Funktionen einer API-Sicherheitsplattform. Darüber hinaus ist diese Fähigkeit erforderlich, damit wichtige Stakeholder aus Sicherheits-, Entwicklungs- und Betriebsteams 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.
- **Bedrohungssuche:** Historische Daten sollten mindestens eine rollierende 30-Tage-Ansicht umfassen, einschließlich der Möglichkeit, alle API-Aktivitäten zu sehen und Zeiträume und Aufrufe, die über bestimmte Warnungen hinausgehen, abzufragen. Diese Funktion unterstützt auch die Einhaltung von Vorschriften.
- **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 Tokenisierung muss durchgeführt werden, damit die Reichhaltigkeit der Daten erhalten bleibt, ohne vertrauliche Daten zu speichern.
- **Visualisierung per Zeitachse:** Die Nutzer sollten eine Ansicht erhalten, in der sie mühelos vorwärts und rückwärts durch Aktivitätsabfolgen blättern können.

Bedrohungen mithilfe von Verhaltensanalysen erkennen



Kritische Funktion Nr. 4
Verfolgung mehrerer Nutzerentitäten

Die Entität und die Fähigkeit, die zugehörigen API-Aktivitäten einzusehen, liefern den Kontext für jede normale Verwendung und jeden Missbrauch. Daher muss Ihre API-Schutzplattform jede Entität einzeln verfolgen können. Dieser Kontext ist wichtig, denn Aktivitäten, die für eine bestimmte Nutzerkategorie normal sind, können bei einem anderen Nutzer ein Warnzeichen für Missbrauch sein. Die Möglichkeit, die Aktivitäten der einzelnen Entitäten auf einer Zeitachse einzusehen, sorgt für die unerlässliche Transparenz und den Kontext. Zum Beispiel:

API-Aktivität	Teilnehmer	Entitäten	Geschäftsprozessentitäten
Beispiele	Interne Nutzer, B2B-Partner, externe Nutzer	IP-Adresse, API-Token, Händler-ID, Sitzungs-ID, Mandanten-ID	Zahlungs-ID, Rechnungs-ID

Kritische Funktion Nr. 5
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).

Während 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 Funktion Nr. 6
Verhaltensanalyse und -erkennung

Die Erkennung komplexer API-Bedrohungen ist nicht möglich, wenn nur einzelne API-Aufrufe oder gar einzelne Sitzungen analysiert werden. Bei der API-Erkennung und Fehlerbehebung kommt es darauf an, den Verhaltenskontext nachzuvollziehen und aus diesem Kontext zu lernen. Um erkennen zu können, ob das Verhalten einer API anormal ist (also ob diese API eventuell kompromittiert wurde), muss die API-Nutzung über längere Zeiträume analysiert werden. Die Verhaltensanalyse ermittelt Basiswerte für das normale Nutzerverhalten und überwacht dieses Verhalten kontinuierlich auf Anomalien.

Angesichts der Speicher- und Computing-Ressourcen, die für eine solche Analyse der API-Aktivität eines typischen Unternehmens erforderlich sind, ist die Bereitstellung als skalierbare lokale API-Sicherheitstools unpraktikabel. EDR- und XDR-Lösungen haben dabei die Vorreiterrolle übernommen und gezeigt, dass eine auf SaaS-basierte Architektur (Software as a Service) für aussagekräftige Verhaltensanalysen erforderlich ist. Durch die Leistungsfähigkeit und Skalierbarkeit der Cloud lassen sich Daten über einen längeren Zeitraum speichern. Gleichzeitig werden damit Analysen möglich, die das normale Nutzerverhalten über einen bestimmten Zeitraum ermitteln und anhand dieser Daten die Nadel im Heuhaufen erkennen können – also einen Missbrauch. Ein SaaS-Ansatz hat weitere Vorteile, z. B. die schnellere und einfachere Implementierung sowie eine bessere Skalierbarkeit und Flexibilität, wenn Ihre API-Nutzung zunimmt.

Kritische Fähigkeit Nr. 7
Aussagekräftige Warnungen mit Kontext

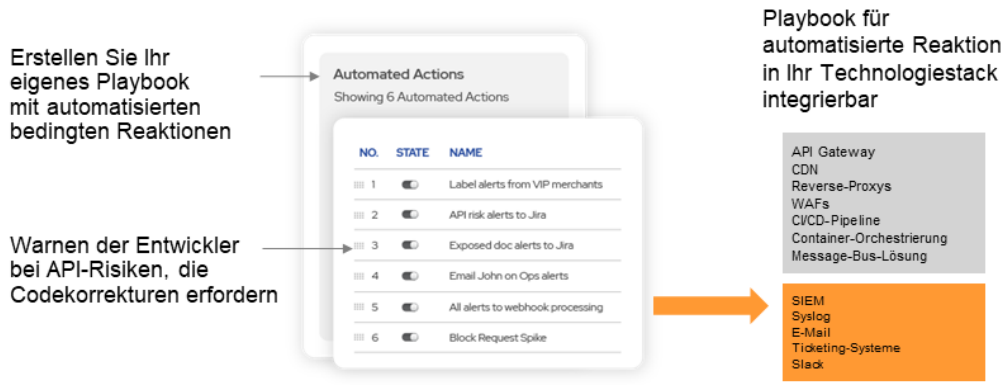
Wenn ein Unternehmen einen umfassenden Einblick in alle API-Aktivitäten und Verhaltensanalysen hat, werden Warnungen zu API-Aktivitäten wesentlich aussagekräftiger. Die Unternehmen müssen sich dann nicht mehr auf jede mögliche Angriffsmethode vorbereiten und die Abläufe bei der Sicherheitsüberwachung abstrakter gestalten. Durch die Ermittlung einer Baseline des normalen Verhaltens und die Erkennung von Anomalien lässt sich auch ein API-Missbrauch erkennen, der oft nicht anhand von Mustern oder Signaturen erkennbar ist. Die Möglichkeit, den Angriff zurückzuverfolgen und zu sehen, was vor einer Warnung geschehen ist, liefert außerdem wertvolle Einblicke in die Nutzung und den Missbrauch einer API-Umgebung.

Kritische Funktion 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, die Angriffe 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
- E-Mail-Benachrichtigungen für Sicherheits- und Geschäfts-Stakeholder
- Ticketerstellung für Entwickler
- Auslösen von Webhooks

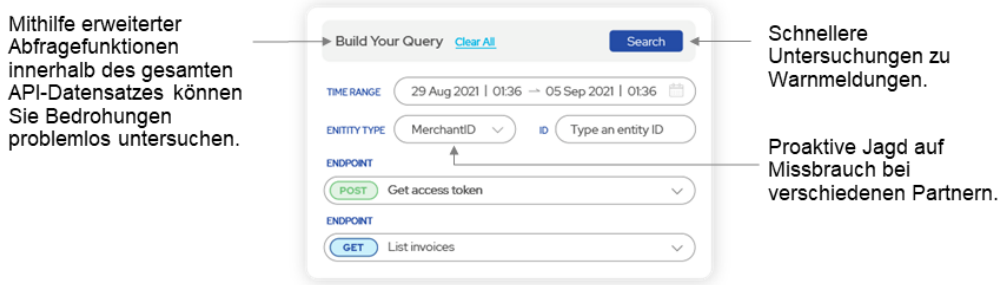
Reaktionen können an Geschäftsprozesse angepasst werden



Kritische Funktion Nr. 9
Proaktive Untersuchung und Bedrohungssuche

Viele Unternehmen können es sich nicht leisten, auf einen aktiven Sicherheitsvorfall zu warten, bevor sie handeln. Es ist effektiver, unerwünschte Situationen zu identifizieren und aktiv nach ihnen zu suchen. Eine Warnung, die einen Missbrauch einer bestimmten API erkannt hat, könnte beispielsweise über die proaktive Bedrohungssuche dazu beitragen, dasselbe Verhalten in einer anderen API zu identifizieren. Eine API-Schutzplattform sollte daher die Möglichkeit bieten, nach bestimmten Verhaltensweisen zu suchen, die über die Warnungen hinausgehen, die als Reaktion auf aktive Vorfälle generiert wurden. Diese Bedrohungssuchfunktionen müssen auf Verlaufsdaten zugreifen können, damit sie den Missbrauch aufdecken, der sich in den API-Aktivitätsdaten verbirgt. Lösungen mit Einzelanfragen, die den Daten nicht mit Kontext anreichern, können kein kohärentes Bild liefern. Bedrohungssuche und Untersuchungen basieren auf Verlaufsdaten.

Leistungsstarke Funktionen für Untersuchung und Bedrohungssuche



Kritische Funktion Nr. 10
Beobachtbarer Data Lake

Bei allen Funktionen einer zuverlässigen API-Sicherheitsstrategie ist Kontext der entscheidende Faktor für den langfristigen Schutz jeder API. Ein ausreichender Kontext für die Beobachtung von Bedrohungen, die Identifizierung potenzieller Schwachstellen und die Fehlerbehebung im Falle eines Angriffs lässt sich am besten zusammenstellen, wenn das gesamte API-Verhalten protokolliert und Buch über diese Aktivitäten geführt wird. Hierzu kann ein Data Lake mit der API-Sicherheitslösung verknüpft werden. Wählen Sie einen Data Lake, der Verlaufsdaten mit größtmöglicher Detailtiefe als Grundlage für Ihre Strategie liefert. Es kann helfen, grundlegende Anfragedaten in Modelle für maschinelles Lernen einzugeben. Mit Details wie den Anfrageparametern sind Unternehmen jedoch in der Lage, auf ihren Verlaufsdaten aufzubauen und sich damit vor zukünftigen Bedrohungen und Angriffen zu schützen.

Nr. 1: Plattformunabhängiger Schutz	Wenn Ihre API-Schutzplattform so transparent wie möglich aufgebaut ist, schützt dies Ihr Unternehmen vor Bedrohungen und Missbrauch.
Nr. 2: Kontinuierliche API-Erkennung und Kontrolle der Sicherheitslage	Ein umfassender und kontinuierlich aktualisierter Bestandsüberblick über alle APIs, die im Unternehmen verwendet werden, ist die Grundlage jeder API-Sicherheitsstrategie, denn ein Unternehmen kann nicht etwas schützen, von dem es nicht einmal weiß, dass es sich in seiner Umgebung befindet.
Nr. 3: Visualisierung des API-Verhaltens	Transparenz ist erforderlich, damit wichtige Stakeholder aus den Sicherheits-, Entwicklungs- und Betriebsabteilungen sehen und verstehen können, wie APIs verwendet oder missbraucht werden. Dann können die Teams miteinander kommunizieren und Fälle untersuchen.
Nr. 4: Verfolgung mehrerer Nutzerentitäten	Die Entität und die Fähigkeit, die zugehörigen API-Aktivitäten einzusehen, liefern den Kontext für jede normale Verwendung und jeden Missbrauch. Daher muss Ihre API-Schutzplattform jede Entität einzeln verfolgen können.
Nr. 5: B2B- und East-West-API-Abdeckung	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.
Nr. 6: Verhaltensanalyse und -erkennung	Um erkennen zu können, ob das Verhalten einer API anormal ist (also ob diese API eventuell kompromittiert wurde), muss die API-Nutzung über längere Zeiträume analysiert werden. Die Verhaltensanalyse ermittelt Basiswerte für das normale Nutzerverhalten und überwacht dieses Verhalten kontinuierlich auf Anomalien.
Nr. 7: Aussagekräftige Warnungen mit Kontext	Wenn ein Unternehmen einen umfassenden Einblick in alle API-Aktivitäten und Verhaltensanalysen hat, werden Warnungen zu API-Aktivitäten wesentlich aussagekräftiger. Die Unternehmen müssen sich dann nicht mehr auf jede mögliche Angriffsmethode vorbereiten und die Abläufe bei der Sicherheitsüberwachung abstrakter gestalten.

Nr. 8: Individuelle, automatisierte Reaktionen	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.
Nr. 9: Proaktive Untersuchung und Bedrohungssuche	Viele Unternehmen können es sich nicht leisten, auf einen aktiven Sicherheitsvorfall zu warten, bevor sie handeln. Es ist effektiver, unerwünschte Situationen zu identifizieren und aktiv nach ihnen zu suchen.
Nr. 10: Beobachtbarer Data Lake	Ein ausreichender Kontext für die Beobachtung von Bedrohungen, die Identifizierung potenzieller Schwachstellen und die Fehlerbehebung im Falle eines Angriffs lässt sich am besten zusammenstellen, wenn das gesamte API-Verhalten protokolliert und Buch über diese Aktivitäten geführt wird. Hierzu kann ein Data Lake mit Ihrer API-Sicherheitsplattform verknüpft werden.

Wenn dieser Artikel Ihnen weitergeholfen hat, sollten Sie sich nun mit der Lösung API Security von Akamai vertraut machen, damit Sie die bestmögliche API-Sicherheitsstrategie erhalten.

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. 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: 12/23.