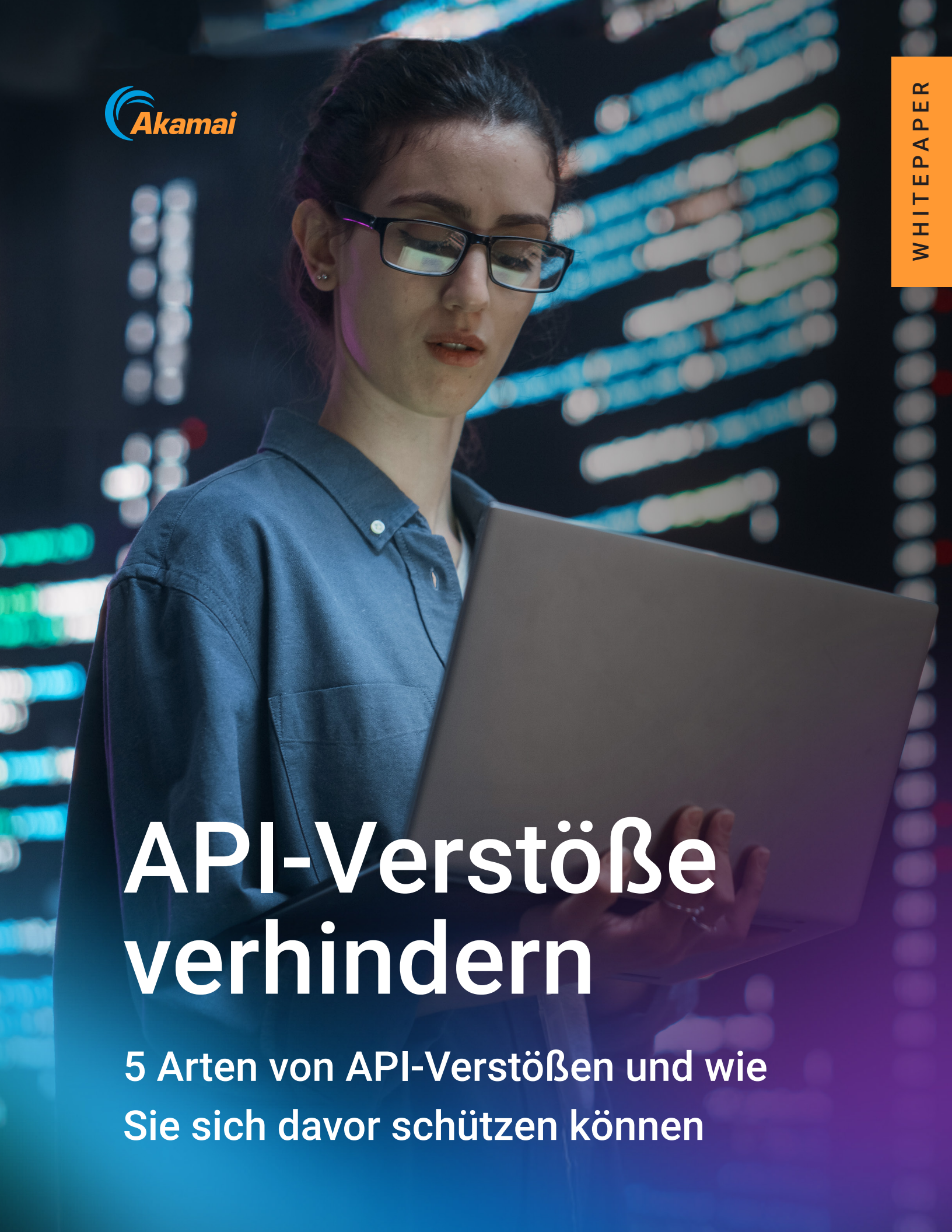


Akamai

WHITEPAPER

API-Verstöße verhindern

5 Arten von API-Verstößen und wie Sie sich davor schützen können

In diesem Bericht

Einführung

APIs verbinden Ihr Unternehmen durch den Austausch von Daten mit Partnern, Lieferanten und Kunden. Dennoch ist die API-Sicherheit in den meisten Unternehmen nach wie vor nicht umfassend. Tatsächlich sind anfällige APIs in den letzten Jahren für Unternehmen zu einer bevorzugt ausgenutzten Schwachstelle geworden, über die Angreifer auf sensible Daten zugreifen, sie an andere Bedrohungsakteure verkaufen oder sie im Internet veröffentlichen können. Im Jahr 2024 mussten globale Marken in den Bereichen Telekommunikation, Enterprise Computing und virtuelle Zusammenarbeit feststellen, dass durch API-Verstöße riesige Mengen an Kunden- und anderen sensiblen Daten veröffentlicht wurden, was zu hohen finanziellen und Reputationsschäden geführt hat.

Was ist ein API-Verstoß?

Einfach ausgedrückt ist ein API-Verstoß jeder absichtliche Missbrauch einer API, oft um Zugriff auf sensible Daten zu erhalten. API-Verstöße können nach verschiedenen Kriterien unterteilt werden. Um Risiken zu erkennen und Verstöße im Produktionsbetrieb zu vermeiden, ist es hilfreich, die Risiken nach dem folgenden Schema in fünf Kategorien zu unterteilen:

1. **Bekannte Schwachstellen**
   - Angreifer nutzen bekannte Schwachstellen aus, die nicht gepatcht wurden.
2. **Shadow-, Rogue-, Zombie- und veraltete APIs**
   - Nicht verwaltete und vernachlässigte APIs können den Betrieb anfällig machen.
3. **Externe Risiken**
   - Zugangsdaten, Schlüssel und andere Risiken können sich außerhalb Ihrer Kontrolle befinden.
4. **Fehlkonfigurationen und Fehler der Bediener**
   - Fehlerhafte Sicherheitskonfiguration der Infrastruktur und Services können Einstiegspunkte für die Ausnutzung durch Cyberkriminelle bieten.
5. **Unentdeckte Schwachstellen und Fehler**
   - Cyberkriminelle versuchen, Fehler und Schwachstellen zu finden, die es trotz aller Bemühungen in die Produktionsumgebung geschafft haben.

In diesem E-Book wird erläutert, wo die Sicherheitsfehler bei jeder dieser fünf Arten von API-Verstößen auftreten und wie sie verhindert werden können. Außerdem soll Ihnen dieses E-Book dabei helfen, konkrete Schwachstellen in Ihrem API-Sicherheitsprogramm ausfindig zu machen, um die API-Sicherheit zu maximieren und das Risiko zu minimieren.

Art des Verstoßes: Bekannte Schwachstellen

API-Verletzungen, die bekannte (und nicht gepatchte) Schwachstellen ausnutzen, sind vielleicht die häufigsten. Wenn Cyberkriminelle an Ihre Daten gelangen wollen, überprüfen sie in einem ersten Schritt, ob Ihr Unternehmen Hintertüren offen gelassen hat.

Im Januar 2024 kompromittierte ein Angreifer ein weitverbreitetes Projektmanagementtool, indem er einen API-Endpunkt ohne Authentifizierungskontrollen ausnutzte. Nachdem sich der Angreifer Zugang zur API verschaffte, erhielt er unbefugten Zugriff auf Informationen von Millionen von Nutzern und legte Monate später über 21 GB an Daten im Internet offen – einschließlich E-Mail-Adressen und Vorstandsmitgliedschaften.

Authentifizierungs- und Autorisierungsprobleme zählen zu den häufigsten API-Problemen. Die OWASP-Top-10-Liste der API-Sicherheitsrisiken bietet Aufschluss über die 10 wichtigsten API-Schwachstellen, vor denen sich Unternehmen schützen müssen, einschließlich fehlerhafter Authentifizierung.

Neben dem Schutz von APIs vor den in den OWASP Top 10 aufgeführten Risikoarten sollten Unternehmen den API-Code vor der vollständigen Liste der häufigsten Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVEs) schützen, die vom von MITRE betriebenen US-amerikanischen National Cybersecurity Federally Funding Research and Development Center (FFRDC) erstellt wurde. Vielleicht erinnern Sie sich an die veröffentlichte Apache Log4j 2-Schwachstelle (CVE-2021-44228), die auch als „Log4Shell“ bezeichnet wurde. Aufgrund eines Fehlers in der Log4j-Bibliothek – einer beliebten Open-Source-Protokollierungsbibliothek für die Programmiersprache Java – konnten Angreifer beliebigen Code aus der Ferne ausführen, um Zugriff auf das System zu erhalten. Böswillige Akteure suchen Unternehmenssysteme routinemäßig nach bekannten Schwachstellen wie diesen ab.

In den USA führt die Cybersecurity and Infrastructure Security Agency (CISA) einen Katalog bekannter CVEs. Andere Länder führen möglicherweise ähnliche Kataloge.

Die OWASP-Top-10-Liste der API-Sicherheitsrisiken wurde 2019 erstellt und 2023 aktualisiert. Sie ist nützlich, kann allerdings nicht mit der Geschwindigkeit der Veränderung der Angriffsfläche Schritt halten. Allein im Jahr 2024 wurden mehr als 24.000 neue CVEs in den CISA-Katalog aufgenommen, davon mehr als 500 API-bezogene (Stand: Mitte August 2024).

Der vollständige Schutz Ihres Unternehmens vor bekannten Schwachstellen erfordert ein zweigleisiges Vorgehen:

1. Sicherstellung, dass Ihre Entwicklungs- und Testprozesse widerstandsfähig genug sind, um zu vermeiden, dass bekannte Schwachstellen in die Produktion gelangen.

2. Schnellstmögliche Behebung neuer Schwachstellen, nachdem sie erkannt wurden.

Viele Organisationen haben mit diesen beiden Schritten Schwierigkeiten. Darüber hinaus verwenden sie APIs und Code von Drittanbietern, die ihre eigenen Schwachstellen mit sich bringen können. 2022 entdeckte ein Forscherteam kritische API-Fehler, die mehrere Hersteller in der Automobilindustrie betrafen. Diese Schwachstellen hätten sensible Kundendaten und sogar den Standort eines Fahrzeugs preisgeben können, sodass ein Auto über ein kompromittiertes Fernmanagementsystem entsperrt, gestartet oder deaktiviert werden konnte.

So werden sie verhindert

Eine bekannte Methode, Ihr Unternehmen vor API-Verstößen aufgrund bekannter Schwachstellen zu schützen, besteht darin, Software und Systeme sofort zu aktualisieren, sobald Sicherheitspatches veröffentlicht werden. Außerdem müssen Sie sicherstellen, dass Ihre Entwicklungs- und Testprozesse umfassend und basierend auf Best Practices für die API-Sicherheit ablaufen. Dies umfasst:

- **Schutz Ihrer Softwarelieferkette:** Stellen Sie sicher, dass Bibliotheken, Open-Source-Software (OSS) und anderer Code von Drittanbietern, die Sie verwenden, sicher sind.

- **Shift-Left-Ansatz für die Sicherheit:** Verschieben Sie Aufgaben im Zusammenhang mit API-Sicherheit und Softwaretests hin zu einem früheren Zeitpunkt im Entwicklungsprozess. Dies kann Ihnen helfen, Schwachstellen wie Programmierfehler und Fehlkonfigurationen aufzudecken, die von Entwicklerteams unter dem Druck der schnellen Veröffentlichung von Software oder Updates gemacht wurden.

- **Kontrolle der API-Sicherheitslage:** Hierbei wird die API-Erkennung mit der Identifizierung sensibler Daten und der Erkennung von Schwachstellen kombiniert, um sicherzustellen, dass sich die Abhilfemaßnahmen auf die kritischsten APIs konzentrieren.

Wie Akamai API Security Ihnen hilft

Mit Akamai API Security können Ihre Teams bekannte Schwachstellen bei jedem neuen Build reduzieren, ohne dabei auf Geschwindigkeit zu verzichten. API Security ist eine speziell entwickelte Lösung für API-Sicherheitstests, die API-spezifische Schwachstellen umfassend abdeckt. Aktives Testen hilft, API-Sicherheitstests fest in jede Entwicklungsphase zu integrieren.

- **Suchen und testen Sie jede API** anhand der Geschäftslogik der Anwendung.
- Nutzen Sie einen **Shift-Left**-Ansatz mit Integrationen in den gesamten Lebenszyklus der Softwareentwicklung. Teams erhalten während des gesamten CI/CD-Prozesses zustands- und umgebungsübergreifend dynamische Einblicke in APIs.
- **Bieten Sie Entwicklern** erstklassige Nutzerfreundlichkeit wie etwa einfache Einrichtung und Automatisierung, integrierte Testergebnisse und kontextbezogene Anleitungen zur Behebung erkannter Probleme.

Darüber hinaus bietet das Management der Sicherheitslage von API Security einen umfassenden Überblick über den Traffic, den Code und die Konfigurationen, um Ihre API-Sicherheitslage zu beurteilen. API Security untersucht die größtmögliche Anzahl von Quellen, um Schwachstellen zu erkennen, darunter Protokolldateien, Verlaufstraffic, Konfigurationsdateien und vieles mehr. Außerdem werden alle Schwachstellen in der Liste der OWASP-Top-10-API-Sicherheitsrisiken erkannt (weitere Informationen zur Kontrolle der Sicherheitslage finden Sie im Abschnitt „Fehlkonfigurationen und Fehler der Bediener“).

Art des Verstoßes: Shadow-, Rogue-, Zombie- und veraltete APIs

Man kann nicht schützen, was man nicht sehen kann. In vielen Unternehmen wird ein großer Teil der APIs nicht verwaltet, wodurch Shadow-, Rogue-, Zombie- und veraltete APIs (siehe Seitenleiste auf der nächsten Seite) zu Zielen werden, die in Ihrem API-Bestand nicht gesehen oder nicht berücksichtigt werden. Darüber hinaus suchen Angreifer oft nach API-Varianten, die sie ausnutzen können, indem sie sich die exponierten APIs eines Unternehmens ansehen und dann mittels Fuzzing oder Ändern von Werten alte Versionen finden.

Dies ist einem großen australischen Telekommunikationsunternehmen passiert, das versehentlich mehr als 11,2 Millionen Kundendatensätze offenlegte, darunter Namen, Adressen, Geburtsdaten und einige amtliche Ausweisnummern. Der Angriff nutzte eine API für Tests, die irgendwie für das offene Internet zugänglich geworden war. Da diese Rogue-API keine Authentifizierungskontrollen enthielt, konnte ein Angreifer Millionen von Datensätzen anfordern und empfangen.

Die meisten Unternehmen arbeiten mit vielen alten und neuen APIs. Leider ist es allzu häufig der Fall, dass daneben auch Rogue-, Zombie- und Shadow-APIs existieren, die das Unternehmen einer Reihe von Cybersicherheitsrisiken und betrieblichen Problemen aussetzen.

Diese ungesehenen APIs können aus unterschiedlichsten Quellen stammen:

- **Kommerzielle APIs:** Einige kommerzielle Softwarepakete enthalten APIs zur Verbindung mit anderen Anwendungen und externen Datenquellen. Diese können aktiviert werden, ohne dass dies jemand bemerkt (ein Problem, das durch gründliche API-Erkennung behoben werden kann).
- **Veraltete API-Versionen:** In vielen Fällen wird die ältere Version einer API – möglicherweise mit schwacher Sicherheit oder einer bekannten Sicherheitslücke – nie entfernt. Eine alte Version muss möglicherweise eine Zeit lang neben einer neuen Version existieren, während die Software aktualisiert wird. Wenn die alte API jedoch aufgrund von Prozessfehlern nicht beendet wird, wird sie zu einer Zombie-API.
- **Abkürzungen und Prozessfehler:** Shadow-APIs entstehen, wenn die richtigen Personen nicht informiert werden. So kann es beispielsweise vorkommen, dass ein Team eines Geschäftsbereichs APIs für bestimmte Anforderungen erstellt, ohne die IT- oder Sicherheitsteams zu informieren, oder dass ein Entwickler sich nicht an den korrekten Ablauf hält.
- **Geerbte APIs:** APIs, die im Rahmen von Fusionen oder Übernahmen vererbt wurden, werden häufig übersehen und in weiterer Folge zu Shadow-APIs.
- **Reaktivierter Code:** In einigen Fällen können alte Versionen von APIs versehentlich reaktiviert werden.

So werden sie verhindert

Ein manuelles API-Audit für alle Eingaben zur Dokumentation und genauen Inventarisierung kann mehrere Stunden in Anspruch nehmen, vor allem, wenn man bedenkt, wie lange es dauert, jede gefundene API zu bewerten und zu bearbeiten. Dies ist für bereits schwer ausgelastete Sicherheitsteams keine realistische Aufgabe. Um Ihr Unternehmen vor Ausnutzung von Rogue-, Zombie- und Shadow-APIs zu schützen, benötigen Sie eine automatisierte API-Erkennung, die alle verwendeten APIs jeder Art identifizieren kann. Es ist wichtig, jede API in Ihrem Betrieb zu finden und zu inventarisieren und APIs und API-Domains zu ermitteln, die nicht von einem API-Gateway verwaltet werden.

Wie Akamai API Security Ihnen hilft

API Security nutzt eine breite Palette von Integrationsquellen, um API-Daten aufzunehmen, wie Rohtraffic, Protokollierung und vieles mehr. Anhand der aus diesen Quellen gewonnenen Daten kann API Security APIs, deren Fehlkonfigurationen, Schwachstellen und API-Missbrauch identifizieren. Unsere Erkennungstools erkennen alle Schwachstellen in den OWASP-Top-10-API-Sicherheitsrisiken.

Mit zusätzlichen Erkennungsfunktionen können Sie:

- alle APIs unabhängig von der Konfiguration oder Art erkennen und inventarisieren, einschließlich RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC und gRPC
- inaktive, veraltete und Zombie-APIs aufdecken
- vergessene, ungenutzte oder anderweitig unbekannte Shadow-Domains erkennen
- den API-Bestand verwalten und die Genauigkeit der API-Dokumentation sicherstellen

Nicht verwaltete APIs mit hohem Risiko, die Angreifer suchen

Shadow-APIs (auch „undokumentierte APIs“ genannt) existieren und arbeiten außerhalb der offiziell überwachten Kanäle eines Unternehmens. Sie werden vielleicht in guter Absicht von Entwicklern erstellt, um ihre Arbeit zu beschleunigen, oder sie sind vielleicht ein Überbleibsel aus früheren Softwareversionen.

Rogue-APIs sind nicht autorisierte oder bösartige APIs, die ein Sicherheitsrisiko für ein System oder Netzwerk darstellen.

Zombie-APIs sind alle APIs, die nach dem Ersetzen durch neue Versionen oder andere APIs trotzdem noch ausgeführt werden.

Veraltete APIs sind APIs, die aufgrund von Änderungen in den APIs nicht mehr zur Verwendung empfohlen werden. Veraltete Klassen, Methoden und Felder sind zwar noch implementiert, können aber in zukünftigen Implementierungen entfernt werden, weshalb Sie sie nicht in neuem Code verwenden sollten.

Art des Verstoßes: Externe Risiken

Schwachstellen externer APIs sind in der Regel das Ergebnis von schlechten Gepflogenheiten oder Verfahrensfehlern, wie z. B. dem Verlust von API-Schlüsseln und -Anmeldeinformationen, API-Code- und -Schemaexposition, unvollständiger Dokumentation und Repo-Schwachstellen. Die Fähigkeit zur Erkennung potenzieller Angriffsvektoren jenseits der Grenzen Ihres Betriebs ist mittlerweile unerlässlich. Im vergangenen Jahr sind eine Reihe von Sicherheitsverletzungen auf die unbeabsichtigte Offenlegung von API-Schlüsseln oder anderen Anmeldeinformationen aus externen Quellen zurückzuführen. Beispielsweise nutzten Hacker eine Phishing-Kampagne, um unbefugten Zugriff auf 130 Quellcode-Repositorys von Dropbox zu erhalten. Dadurch konnten sie auf API-Schlüssel zugreifen, die nicht ordnungsgemäß auf GitHub gespeichert wurden. Diese Art der Exposition ist so häufig geworden, dass GitHub Schritte unternommen hat, um das Offenlegen von API-Schlüsseln und anderen Secrets zu verhindern, doch andere öffentliche Repositorys können immer noch anfällig sein.

In einem anderen, viel beachteten Beispiel für externe Risiken entdeckten Forscher mehr als 3.000 mobile Anwendungen, die Twitter-API-Schlüssel öffentlich zugänglich machten. Diese Art von Fehler tritt überraschend häufig auf, da Entwickler API-Schlüssel während der Entwicklung aus Gründen der Bequemlichkeit oft in den Anwendungscode einbetten. Wenn diese eingebetteten Schlüssel nicht vor einer öffentlichen Veröffentlichung entfernt werden, wird dies zu einer potenziellen Quelle für die Offenlegung von Schlüsseln.

So werden sie verhindert

Die Reduzierung oder Beseitigung dieser Arten von externen Risiken erfordert ein zweigleisiges Vorgehen:

- Straffung der Verfahren zur Identifizierung und Eliminierung von Risikoquellen wie offengelegte Schlüssel und Anmeldeinformationen, unsachgemäße Verwendung von Repositorys usw.
- Regelmäßige Überprüfung der Angriffsfläche nach außen, um Schwachstellen zu erkennen und zu beheben.

Um sich gegen ein möglichst breites Spektrum von API-Bedrohungen zu schützen, benötigen Sie sowohl eine Inside-out-Erkennung (wie im Abschnitt „Verstöße durch Rogue-APIs“ beschrieben) als auch eine Outside-in-Erkennung, die Schwachstellen identifizieren und Ihre externe Angriffsfläche reduzieren kann.

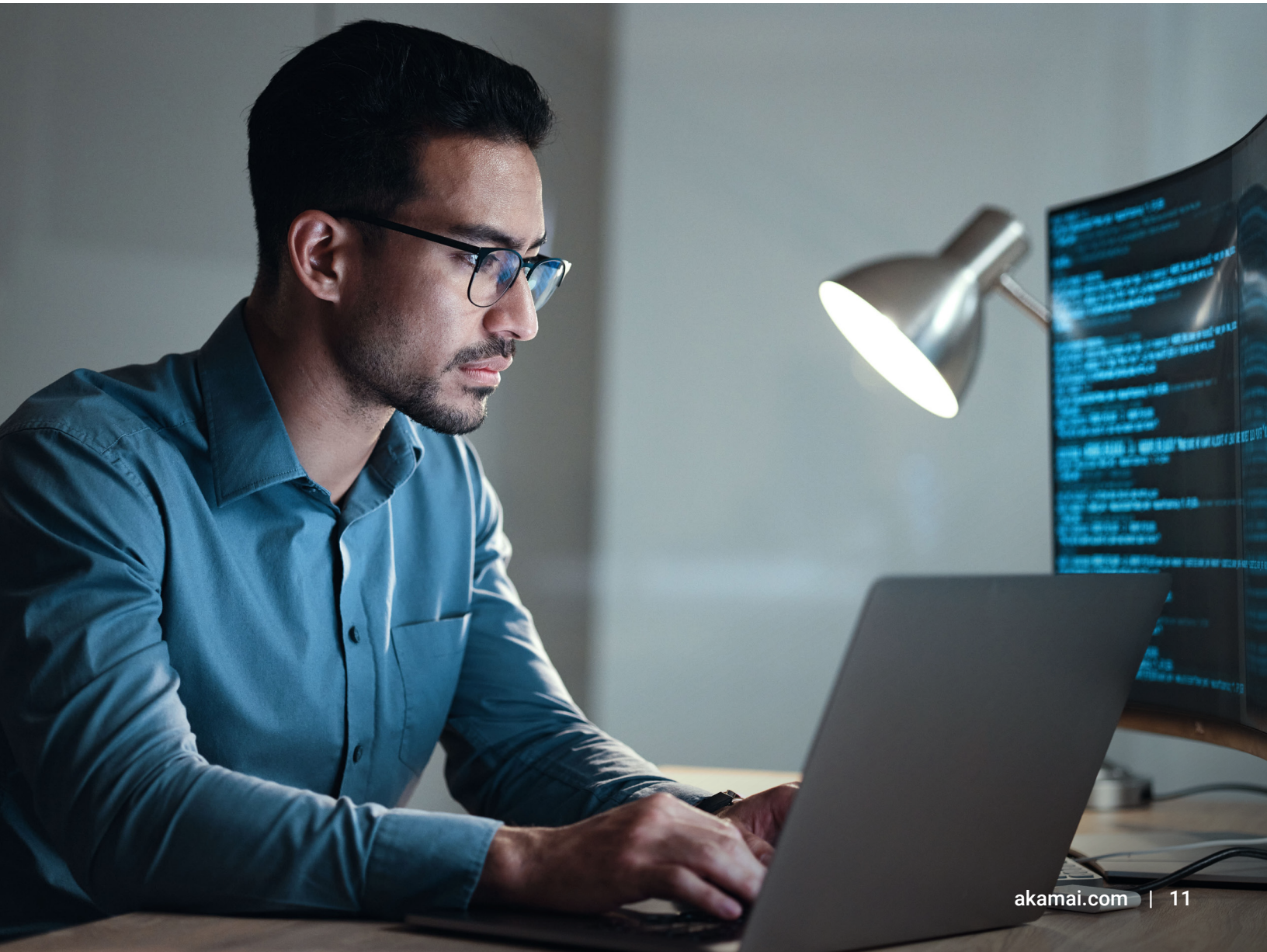
Wie Akamai API Security Ihnen hilft

API Security hilft Ihnen, Angreifern einen Schritt voraus zu sein, indem die Untersuchungstechniken simuliert werden, die Hacker verwenden, sodass Sie Probleme schnell finden und beheben können. Mit der Outside-in-Erkennung scannt API Security automatisch Ihre externe Angriffsfläche in regelmäßigen Abständen, um Schwachstellen zu finden, bevor Angreifer dies tun:

- **Öffentlich zugängliche Schwachstellen finden:** Finden und beheben Sie schnell kritische Probleme wie die Preisgabe von API-Schlüsseln und Anmeldeinformationen, die Offenlegung von Code, Fehlkonfigurationen, Schwachstellen in Repositorys und vieles mehr.
- **Mit Ihrem Unternehmen verbundene Domains und Subdomains entdecken:** Nutzen Sie Daten aus verschiedenen Quellen, einschließlich Internetregistrierstellen, Zertifikatsregistrierstellen und offener Quellen.
- **Einsatz echter Angriffsmethoden:** Simulieren Sie einen Angreifer, der von außen Informationen sammelt, indem er begrenzte Abfragen an Unternehmensdomains oder Subdomains sendet.

Art des Verstoßes: Fehlkonfigurationen und Fehler der Bediener

Viele Cyberangreifer verschaffen sich Zugang, indem sie die Fehlkonfiguration der Server, Netzwerke, API-Gateways und Firewalls ausnutzen, die den API-Traffic vermitteln und schützen. Eine Studie von IBM Security X-Force ergab, dass zwei Drittel der Cloud-Sicherheitsverstöße auf falsch konfigurierte APIs zurückzuführen sind. Falsche Sicherheitskonfigurationen können durch unsichere Standardkonfigurationen, Cloud-Speicher ohne Zugriffskontrolle (überraschend häufig) und unvollständige oder Ad-hoc-Konfigurationen verursacht werden. Mit zunehmender digitaler Präsenz kann Ihr Betrieb auf weitere Standorte ausgedehnt werden, darunter mehrere öffentliche Cloud-Verfügbarkeitszonen oder öffentliche Clouds wie AWS, Microsoft Azure und Google Cloud. Diese Umgebungen arbeiten oft mit unterschiedlichen Sicherheitskontrollen, was es komplex und schwierig macht, sicherzustellen, dass die Sicherheit überall korrekt konfiguriert ist.



So werden sie verhindert

Eine der besten Möglichkeiten zum Schutz vor Fehlkonfigurationen auf Infrastrukturseite besteht darin, die manuelle Konfiguration von Servern, Netzwerkgeräten, Gateways und Firewalls so weit wie möglich zu vermeiden. Wenn die Admin-Teams Ihres Unternehmens die Sicherheitskontrollen für Infrastruktur und Anwendungen routinemäßig manuell konfigurieren oder regelmäßig „anpassen“, steigt die Wahrscheinlichkeit, dass Sicherheitslücken in der Konfiguration auftreten.

Wenn es um Sicherheit geht, ist Automatisierung Ihr bester Freund. Einige Unternehmen nutzen das Konzept einer unveränderlichen Infrastruktur, um manuelle Fehler zu vermeiden.

Selbst wenn Sie alles in Ihrer Macht Stehende getan haben, um sicherzustellen, dass Ihre Infrastruktur, Ihre Services und APIs sicher sind, benötigen Sie dennoch ein API-Sicherheitsmanagement. Die Kontrolle der Sicherheitslage bietet Ihnen die Tools zur Verwaltung, Überwachung und Aufrechterhaltung der Sicherheit Ihrer APIs während des gesamten API-Lebenszyklus.

Wie API Security Ihnen hilft

Das Modul von API Security zur Kontrolle der Sicherheitslage analysiert API-Aufrufe und die Infrastruktur, um Fehlkonfigurationen zu identifizieren. Bei diesen Fehlkonfigurationen handelt es sich in der Regel um Amazon S3-Bucket-Probleme, vertrauliche Daten auf nicht authentifizierten APIs und verschiedene Fehlkonfigurationen auf Basis von Kubernetes-Zugriff.

Das Modul zur Kontrolle der Sicherheitslage bietet eine umfassende Ansicht von Traffic, Code und Konfigurationen sowie einen Überblick über die gesamte Angriffsfläche von APIs und Webanwendungen, einschließlich aller Arten von sensiblen Daten, die durch Ihre APIs übertragen werden, wie z. B. personenbezogene Daten. Außerdem können Sie damit feststellen, dass Ihr API-Management-Tool starke Protokolle und Chiffren verwendet, um eine schwache Verschlüsselung zu vermeiden, die diese sensiblen Daten preisgeben könnte. Darüber hinaus sollten APIs keine abgelaufenen JSON-Webtokens akzeptieren, da dies unbefugten Zugriff ermöglichen und die Sicherheitsrisiken erhöhen würde. Das Modul hilft auch, Fehlkonfigurationen zu verhindern, etwa Load Balancer von Anwendungen, die auf unsicheren Ports ohne Weiterleitung horchen. All diese Maßnahmen stärken gemeinsam die Sicherheitslage von APIs und sorgen so für einen stärkeren Schutz vor potenziellen Bedrohungen.

Art des Verstoßes: Unentdeckte Schwachstellen

Wie bei den meisten Arten von Verstößen suchen Cyberkriminelle Ihre Infrastruktur routinemäßig nach CVEs, den OWASP Top 10 der API-Sicherheit und anderen häufig auftretenden Fehlkonfigurationen sowie Rogue-, Zombie- und Shadow-APIs ab. Sie untersuchen auch Ihre exponierten APIs auf neue Schwachstellen, die sie in Bibliotheken, Open-Source-Code und anderen Arten von öffentlichem Code ausnutzen können, sowie auf Codierungsfehler, Bugs und Fehlkonfigurationen in Ihrem API-Bestand. Diese Sicherheitsanfälligkeiten ermöglichen Cyberkriminellen, API-Aufrufe zu manipulieren und zufällige Zeichenfolgen in Anforderungen einzufügen. Infolgedessen entwickeln sich die von Cyberkriminellen verwendeten Techniken ständig weiter.

So werden sie verhindert

Ein wichtiger Teil der Vorbeugung besteht darin, sicherzustellen, dass Ihr Code möglichst frei von Fehlern und Schwachstellen ist (siehe Abschnitt „Bekannte Schwachstellen“). Sie sollten aber dennoch davon ausgehen, dass Cyberkriminelle Bugs finden oder Zugriff auf Schlüssel oder Zugangsdaten erhalten, mit denen sie APIs ausnutzen können.

Der API-Laufzeitschutz ist darauf ausgelegt, Hacker zu erkennen, die eine bekannte oder unbekannte Sicherheitslücke ausnutzen. Dies ist die einzige Möglichkeit, Ihre API-Umgebung vor bisher nicht identifizierten Fehlern und Fehlkonfigurationen zu schützen, die in die Produktionsumgebung gelangen, und es ist der beste Schutz vor kompromittierten Zugangsdaten und Schlüsseln.

Der Laufzeitschutz erkennt ungewöhnliche Muster und Anomalien bei der API-Nutzung und beim Datenzugriff, sodass fortlaufende Angriffe, die sonst übersehen werden könnten, erkannt und behoben werden können, bevor Tausende oder Millionen von Datensätzen extrahiert werden.

Der API-Laufzeitschutz hilft Ihnen, schädliche API-Anfragen zu identifizieren und zu blockieren, darunter:

- Angriffe, die große Mengen vertraulicher Daten von einer API abrufen
- BOLA-Angriffe (Broken Object Level Authorization; Angriffe durch fehlerhafte Autorisierung auf Objektebene)

Eine API-Laufzeitschutzlösung kann Folgendes erkennen:

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

Darüber hinaus protokolliert der Laufzeitschutz den API-Traffic, überwacht den Zugriff auf sensible Daten, erkennt Bedrohungen und blockiert oder behebt Angriffsvektoren.

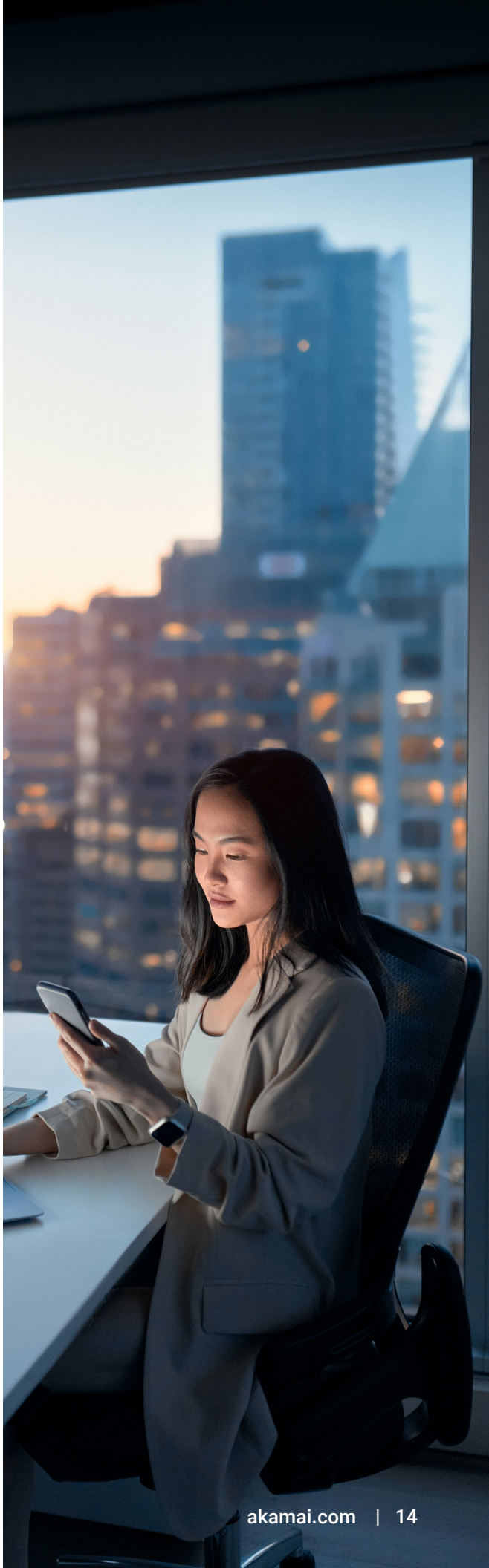
Wie API Security Ihnen hilft

Denken Sie an Laufzeitschutz als letzte Verteidigungslinie, wenn andere Präventionsmaßnahmen nicht ausreichen. Die primäre Funktion des Laufzeitschutzes besteht darin, API-Angriffe in Echtzeit zu erkennen und zu blockieren. Mithilfe von autonomem maschinellem Lernen (ML) wird der Traffic in Echtzeit analysiert und ein kontextbezogener Einblick in Datenlecks, Datenmanipulationen, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und API-Sicherheitsangriffe gewährt. API Security erkennt Anomalien und potenzielle Bedrohungen in Ihrem API-Traffic und erleichtert die Behebung von Gegenmaßnahmen anhand vorab gewählter Richtlinien für die Reaktion auf Vorfälle.

Mithilfe von ML erstellt API Security ein Verhaltensmodell für jede API. Anhand dieser Basiswerte für normales Verhalten werden dann Angriffe auf die API-Geschäftslogik erkannt. Jedes durch den Laufzeitschutz generierte Problem umfasst Schweregrad, Status, eine Zuordnung zu den OWASP Top 10 der API-Sicherheit und Angreiferdetails, sofern zutreffend. Zu den Problemen gehören auch Hinweise wie die Sitzungsdaten des Angreifers und eine Kopie der API-Anfrage und -Antwort, die bei der Untersuchung und Behebung des Problems helfen.

Der Laufzeitschutz von API Security bietet Echtzeit-Erkennung und -Prävention von API-Angriffen zusammen mit kontinuierlicher Erkennung von API-Fehlkonfigurationen sowie viele beliebte Workflow-Integrationen, die den Betrieb und Abhilfemaßnahmen vereinfachen.

Die vielleicht beste Nachricht für Ihr Team ist, dass API Security in WAFs, API-Gateways, ITSMs, SIEMs und andere Workflow-Tools integriert werden kann und so einen ganzheitlichen Schutz vor Angriffen bietet. Sie können wählen, ob Sie die Beseitigung von Bedrohungen vollständig automatisieren oder verschiedene Stufen manueller Eingriffe verlangen, um mehr Transparenz und Kontrolle zu erhalten.



5 Arten von Verstößen, 5 Präventionsgrundsätze

Da Sie nun besser verstehen, wie APIs von Cyberkriminellen genutzt werden, können Sie sich darauf konzentrieren, diese zu verhindern. Hier sind die fünf Präventionstools und strategischen Perspektiven, die Sie zusammen einsetzen müssen:

1. Shift-Left-Ansatz für API-Sicherheit

- Ein Shift-Left-Ansatz für API-Sicherheit bedeutet, dass Sie APIs in der Entwicklung ausgiebig testen, damit Sie keine Schwachstellen in Ihrer Produktionsumgebung offenlegen, wo Cyberkriminelle sie finden können.

2. Inside-out-Erkennung

- Identifizieren Sie alle APIs in Ihrem gesamten Betrieb.

3. Outside-in-Erkennung

- Erkennen und beseitigen Sie Risikoquellen – z. B. offengelegte Schlüssel und Zugangsdaten sowie unsachgemäße Verwendung von Repositorys – und überprüfen Sie regelmäßig die Angriffsfläche nach außen, um Schwachstellen zu erkennen und zu beheben.

4. Umfassendes Sicherheitsmanagement

- Geben Sie immer Ihr Bestes, wenn es um API-Sicherheit geht, und vermeiden Sie Fehlkonfigurationen und Schwachstellen.

5. Laufzeitschutz

- Erkennen Sie anomale API-Aktivitäten und schützen Sie sich vor allen möglichen Bedrohungen, einschließlich zuvor nicht identifizierter Schwachstellen und Bugs.

Demo anfordern

Überzeugen Sie sich davon, wie einfach es ist, Fehlkonfigurationen in Ihren APIs zu erkennen und zu beheben und sich vor bösartigen API-Angriffen zu schützen, indem Sie Akamai API Security in Aktion erleben. Sehen Sie selbst, warum führende Unternehmen sich für unsere API-Sicherheitslösung entscheiden.

Demo anfordern

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: 11/24.