Kaufberater API-Sicherheit

Steigende Anforderungen an die API-Sicherheit

Da Unternehmen zunehmend cloudzentriert und digital arbeiten, wachsen Umfang und Skalierbarkeit ihrer APIs, was ihren Wert erhöht. APIs heute:

- Sie arbeiten im Zentrum von Anwendungen und Services, die Ihren Kunden und Partnern dienen, dazu zählen auch die neuesten KI-Innovationen
- Sind in Cloudumgebungen integriert, die von den Services, die Ihre Entwickler verwenden, bis hin zu den Workloads, die Ihre Techniker handhaben, reichen
- Stellen selbst Einnahmequellen dar, die Sie dabei unterstützen, Ihr Unternehmen zu erweitern und ein Entwickler-Ökosystem aufzubauen

Wenn Sie jedoch zu den 78 % der IT- und Sicherheitsexperten gehören, die API-Sicherheitsvorfälle miterlebt haben,[1] haben Sie selbst gesehen, dass APIs auch ein wachsendes Risiko darstellen. Exponierte oder falsch konfigurierte APIs sind weit verbreitet, ungeschützt und leicht zu kompromittieren. Viele Unternehmen wissen oft nicht einmal von vielen Ihrer APIs, sodass diese nicht verwaltet werden. Diese inaktiven oder Zombie-APIs sind wichtige Angriffsvektoren.

Es steht viel auf dem Spiel. Angriffe auf Ihre APIs können den Umsatz, die Ausfallsicherheit und die Einhaltung gesetzlicher Vorschriften im Unternehmen gefährden. Die meisten Unternehmen verfügen noch nicht über die richtigen Kontrollen und Funktionen, um API-Angriffe zu verhindern. Viele verfügen über API-Tools, wie API-Gateways und Web Application Firewalls. Obwohl diese Tools einen gewissen Schutz bieten können, sind sie nicht so konzipiert, dass sie Transparenz und Echtzeitsicherheit liefern sowie kontinuierliche Tests durchführen, um Schutz vor modernen API-Angriffen zu bieten.

1. Akamai Technologies, “API Security Disconnect Report,” 2023

Was ist also nötig, um Ihre API-Umgebung vollständig zu schützen? Obwohl in den letzten Jahren eine Vielzahl von API-Sicherheitsprodukten entwickelt wurde, kann es schwierig sein, sich angesichts des wachsenden Angebots an Anbietern und Funktionen zu orientieren.

Die heutigen Bedrohungen erfordern eine umfassende API-Sicherheitslösung, die vier kritische Bereiche umfasst: API-Erkennung, Sicherheitsmanagement, Erkennung und Behebung von Bedrohungen sowie Sicherheitstests. In diesem Kaufberater beschreiben wir die wichtigsten Funktionen, die eine umfassende API-Sicherheitslösung benötigt. Wir definieren die Funktionen und Sicherheitskontrollen, die Sie für die Entwicklung und den Betrieb sicherer APIs benötigen, und die gleichzeitig alle APIs in Ihrem Ökosystem finden und schützen.

Die wichtigsten Funktionen für umfassende API-Sicherheit

Um die erforderlichen API-Sicherheitsfunktionen zu ermitteln, ist es wichtig, die Art der Herausforderungen zu verstehen, mit denen Sie konfrontiert sind.

APIs sind oft über mehrere Umgebungen – von On-Prem bis zur Hybrid-Cloud – verteilt. Zur Komplexität Ihres API-Ökosystems trägt außerdem noch bei, dass es sich wahrscheinlich weit über Ihre eigene Netzwerk- und Cloudpräsenz hinaus erstreckt. Denken Sie an die unzähligen Verbindungen, die Ihre APIs mit Apps, Services und Systemen von Drittanbietern – deren Priorität möglicherweise nicht die API-Sicherheit ist – hergestellt haben.

Darüber hinaus ist es schwierig, Echtzeitinformationen über folgende Aspekte zu erhalten:

- Wohin Ihre APIs geleitet werden
- Wie sie konfiguriert sind
- Welche sensiblen Daten sie verschicken
- Welche Risiken sie bergen

Da Unternehmen schnell neue Anwendungen und APIs entwickeln und einführen, wächst die Angriffsfläche exponentiell. Möglicherweise gibt es in Ihrem Unternehmen eine Vielzahl von veralteten APIs, die vor Jahren – bevor die API-Sicherheit zu einer kritischen Notwendigkeit wurde – erstellt und produziert wurden.

Die mangelnde Transparenz führt zu beunruhigenden Tatsachen: Nur 4 von 10 Sicherheitsexperten mit vollständigen API-Beständen wissen, welche ihrer APIs vertrauliche Daten zurücksenden, wenn sie aufgerufen werden. Viele dieser API-Aufrufe stammen von Cyberkriminellen, die nach Schwachstellen suchen. Sobald sie eine Lücke erkennen, folgen oft unerbittliche Angriffe.

Wenn Sie Sicherheitsanbieter überprüfen, die Ihrer Meinung nach Ihre API vollständig sichern können, ist es wichtig, dass sie über produktionsbegleitende Kontrollen und Funktionen in vier kritischen Bereichen verfügen.

Im Anschluss finden Sie mehrere Checklisten für Käufer, mit denen Sie die Funktionen von Anbietern überprüfen können.

01

API-Erkennung

Es ist nicht ungewöhnlich, APIs zu haben, von denen niemand weiß. Doch ohne eine genaue Bestandsaufnahme ist Ihr Unternehmen einer Reihe von Risiken ausgesetzt. Um eine effektive Bestandsaufnahme Ihrer APIs zu ermöglichen, müssen Sie zu Folgendem in der Lage sein:

- ☑ Ihre APIs zu finden und in Bestand aufnehmen, unabhängig von Konfiguration oder Typ
- ☑ inaktive, veraltete und Zombie-APIs zu entdecken
- ☑ vergessene, ungenutzte oder anderweitig unbekannte Schatten-Domains zu erkennen
- ☑ blinde Flecken zu beseitigen und potenzielle Angriffspfade zu ermitteln

02

API-Sicherheitsmanagement

Einfache API-Fehlkonfigurationen können Angreifern die Türen öffnen. Wenn sie erst einmal in Ihr Unternehmen eingedrungen sind, können sie schnell auf vertraulichen Daten zugreifen und diese stehlen. Um zu verstehen, wie Ihre APIs konfiguriert sind, müssen Sie zu Folgendem in der Lage sein:

- ☑ die Infrastruktur automatisch zu scannen und Fehlkonfigurationen sowie versteckte Risiken aufzudecken
- ☑ nutzerdefinierte Workflows zu erstellen und wichtige Stakeholder über Schwachstellen zu informieren
- ☑ zu ermitteln, welche APIs und internen Nutzer auf sensible Daten zugreifen können
- ☑ erkannten Problemen einen Schweregrad zuzuweisen und so Abhilfemaßnahmen zu priorisieren

03

Erkennung und Behebung von API-Bedrohungen

Bis zu einem gewissen Punkt sind API-Angriffe unvermeidlich. Um Bedrohungen effektiv erkennen und beheben zu können, müssen Sie zu Folgendem in der Lage sein:

- ☑ Daten auf Manipulation und Datenlecks, Richtlinienverstöße, verdächtiges Verhalten und API-Angriffe zu überwachen
- ☑ API-Traffic aus allen Quellen zu analysieren und in vorhandene Workflows (Ticketing, Sicherheitsinformationen und Ereignisverwaltung usw.) zu integrieren, um Sicherheitsteams zu warnen
- ☑ Angriffe und Missbrauch in Echtzeit mit teil- oder vollautomatischen Abhilfemaßnahmen zu verhindern

04

API-Sicherheitstests

Geschwindigkeit ist bei jeder Anwendung, die Ihre Entwickler erstellen, von entscheidender Bedeutung. Doch durch diesen Umstand können Schwachstellen oder Konstruktionsfehler leichter unentdeckt bleiben. Um Ihre APIs ordnungsgemäß zu testen, müssen Sie zu Folgendem in der Lage sein:

- ☑ eine Vielzahl automatisierter Tests durchzuführen, die schädlichen Traffic simulieren und der zugrunde liegenden API-Geschäftslogik folgen
- ☑ Schwachstellen zu entdecken, bevor APIs in die Produktion gelangen, um das Risiko eines erfolgreichen Angriffs zu verringern
- ☑ Ihre API-Spezifikationen anhand etablierter Governance-Richtlinien und -Regeln zu überprüfen
- ☑ API-fokussierte Sicherheitstests nach Bedarf oder im Rahmen einer CI/CD-Pipeline auszuführen

API-Erkennung: Die wichtigsten Funktionen im Detail

Viele Unternehmen betreiben sowohl ältere als auch neue APIs. Es ist nicht unüblich, dass nicht verwaltete APIs in der Produktion sind, von denen das Betriebs- oder das Sicherheitsteam nichts weiß, wodurch das Unternehmen einer Reihe von Cybersicherheitsrisiken und betrieblichen Schwierigkeiten ausgesetzt ist. Nicht autorisierte APIs können durch Faktoren wie Kurzbefehle, Prozessfehler und das Nichtabschalten bei Außerbetriebnahme entstehen. Auf der nächsten Seite finden Sie wichtige Beispiele, auf die Sie achten sollten.

Kommerzielle APIs

Einige kommerzielle Softwarepakete enthalten APIs zur Verbindung mit anderen Anwendungen und externen Datenquellen. Diese APIs können aktiviert werden, ohne dass es jemand bemerkt.

Fehler bei der Deaktivierung

APIs können auch offiziell außer Betrieb genommen werden, bleiben aber aufgrund von operativen Versäumnissen weiterhin in Betrieb. Diese APIs werden manchmal als „Zombie-APIs“ bezeichnet.

Veraltete API-Versionen

Manchmal wird eine ältere Version einer API nie außer Betrieb genommen. Eine alte Version muss möglicherweise für einen bestimmten Zeitraum gleichzeitig mit einer neuen Version existieren, während die Software aktualisiert wird. Aber was passiert, wenn die Person, die für die Deaktivierung der API verantwortlich ist, das Unternehmen verlässt, die Abteilung wechselt oder einfach vergisst, die veraltete Version außer Betrieb zu nehmen?

Kurzbefehle und Prozessfehler

Einige APIs werden zu nicht autorisierten APIs, wenn die richtigen Personen nicht informiert werden. Beispielsweise kann ein LOB-Team (Line of Business) APIs erstellen, um bestimmte Anforderungen zu erfüllen, ohne die IT darüber zu informieren, oder Entwickler befassen sich möglicherweise mehr mit der Ausführung der API als mit dem betrieblichen Ablauf. APIs, die im Rahmen einer Übernahme „geerbt“ wurden, werden ebenfalls häufig übersehen. Diese Art von nicht autorisierten APIs wird oft als „Shadow-APIs“ bezeichnet.

Wenn Sie mit Anbietern sprechen, fragen Sie sie, wie sie sicherstellen, dass nicht autorisierte, veraltete, Zombie- und Shadow-APIs erkannt und aufgearbeitet werden, damit sie nicht ausgenutzt werden können. Veraltete und Zombie-APIs sind oft der schwächste Punkt in der API-Sicherheit. Darum ist es wichtig, APIs, die nicht von einem API-Gateway verwaltet werden, zu erkennen, lokalisieren, in den Bestand aufzunehmen und festzustellen, ob sie behoben oder außer Betrieb genommen werden müssen.

Wichtige Funktionen zur API-Erkennung

Eine API-Sicherheitslösung sollte die folgenden Erkennungsfunktionen enthalten

API-Asset-Erkennung und detaillierte Bestandsaufnahme

Ein API-Erkennungstool muss in der Lage sein, Ihre APIs unabhängig von Konfiguration oder Art zu finden und zu identifizieren. Das umfasst auch RESTful-, GraphQL-, SOAP-, XML-RPC-, JSON-RPC- und gRPC-APIs. Außerdem sollte es ein Inventar erstellen, das automatisch aktualisiert wird, um zu verhindern, dass es veraltet, und die Möglichkeit bietet, basierend auf einem beliebigen Attribut nach APIs zu suchen, sie zu kennzeichnen, zu filtern, zuzuweisen und zu exportieren.

Inaktive, veraltete und Zombie-APIs entdecken

Veraltete und Zombie-APIs sind möglicherweise noch vor den API-Sicherheitsinitiativen Ihres Unternehmens entstanden. Diese APIs verfügen in der Regel nicht über einen Owner und arbeiten ungesehen oder ohne Sicherheitskontrollen. Es ist wichtig, dass ein API-Erkennungstool diese APIs finden kann.

Erkennung von Shadow-Domains

Neben Shadow-APIs können auch ganze Shadow-Domains – API-Domainnamen, von denen Sie nichts wissen – vorhanden sein. API-Erkennungstools müssen in der Lage sein, vergessene, vernachlässigte oder anderweitig unbekannte Schatten-Domains, die ein Sicherheitsrisiko darstellen könnten, zu erkennen.

Automatische Scans

Scans sind unerlässlich, um blinde Flecken zu beseitigen und kritische Probleme zu erkennen. Dazu gehören:

- Offenlegen von API-Schlüsseln und -Anmeldedaten
- API-Code- und Schemaexposition
- Fehlkonfigurationen der Infrastruktur
- Schwachstellen in Dokumentation, GitHub-Repositorys, Postman-Workspaces usw.

Die Erkennung dieser und anderer Quellen ausnutzbarer Informationen kann Teams auch dabei helfen, potenzielle Angriffspfade zu verstehen, die von Cyberkriminellen ausgenutzt werden könnten.

Eingeschränkte nutzerdefinierte Entwicklung

Und schließlich sollten Sie mit dem richtigen API-Erkennungstool keine nutzerdefinierte Entwicklung für Trafficquellen benötigen. Diese Tools sollten vorgefertigte Integrationen für wichtige Infrastrukturkomponenten enthalten. Nutzerdefinierte Entwicklung ist in der Regel zeitaufwändig, und wenn sich der Ursprung der Quelle ändert, müsste eine Integration wahrscheinlich überarbeitet werden, was für überlastete IT-Sicherheitsteams nicht machbar ist.

API-Sicherheitsmanagement: Die wichtigsten Funktionen im Detail

Bedrohungen für Ihre API-Umgebung nehmen aufgrund von Trends wie dem Wechsel von der zentralisierten IT zu dezentralen LOB-Abläufen, der zunehmenden Nutzung von Cloudressourcen und dem Übergang zu Mikroservices-Architekturen schnell zu.

Eine leistungsstarke Erkennung (wie im vorherigen Abschnitt beschrieben) ist der erste Schritt zur Absicherung Ihrer API-Umgebung. Sie müssen APIs aller Arten, die derzeit verwendet werden, ermitteln und inventarisieren.

Es gibt mehrere zusätzliche Funktionen, die für die Verwaltung Ihrer Sicherheitsstrategie einschließlich all Ihrer APIs unerlässlich sind. Sie müssen in der Lage sein, zu identifizieren, welche APIs auf vertrauliche Daten zugreifen und diese übertragen, und diese APIs entsprechend klassifizieren können, da APIs, die mit Daten wie Kundeninformationen in Berührung kommen, definitiv authentifiziert werden müssen. Außerdem ist es wichtig, Schwachstellen in der Infrastruktur zu identifizieren, die APIs anfälliger machen.

Konfigurationsprüfung

Viele erfolgreiche Cyberangriffe sind das Ergebnis einfacher Fehlkonfigurationen von Netzwerken, API-Gateways oder Firewalls, die API-Traffic vermitteln und schützen.

Eine API-Sicherheitslösung sollte regelmäßig Infrastruktur- und Softwarekonfigurationen – einschließlich Protokolldateien, Verlaufstraffic, Konfigurationsdateien usw. – scannen. So können Sie Fehlkonfigurationen und Schwachstellen aufdecken und Risiken, die durch Konfigurationsabweichungen entstehen, beseitigen.

Individualisierbarer Schweregrad

Während die Lösung neue Schwachstellen in Ihrer Umgebung identifiziert, sollte sie den erkannten Problemen auch einen Schweregrad zuweisen, damit sie bei der Behebung priorisiert werden können. Schweregrade sollten an die Risikotoleranz Ihres Unternehmens, die gesetzlichen Anforderungen und internen Richtlinien angepasst werden können.

Nutzerdefinierte Workflows

Neben einem anpassbaren Schweregrad sollte das ideale Tool zur Sicherheitsverwaltung Ihnen ermöglichen, nutzerdefinierte Workflows zu erstellen, um sofort Maßnahmen zu ergreifen, wenn Sie Schwachstellen erkennen. Diese Workflows können von der Erstellung von Tickets über die Benachrichtigung wichtiger Interessengruppen bis hin zur Aktualisierung von Netzwerkkonfigurationen reichen.

Automatisch generierte Dokumentation

Die API-Dokumentation informiert Verbraucher über den Zweck und die Verwendung einer API. Unternehmen müssen prüfen, ob sichere APIs Spezifikationen einhalten und ihre Dokumentation fehlerfrei ist. 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 ist eine veraltete, unvollständige oder nicht vorhandene Dokumentation inakzeptabel, wenn Ihr API-Sicherheitsprogramm Erfolge erzielen soll.

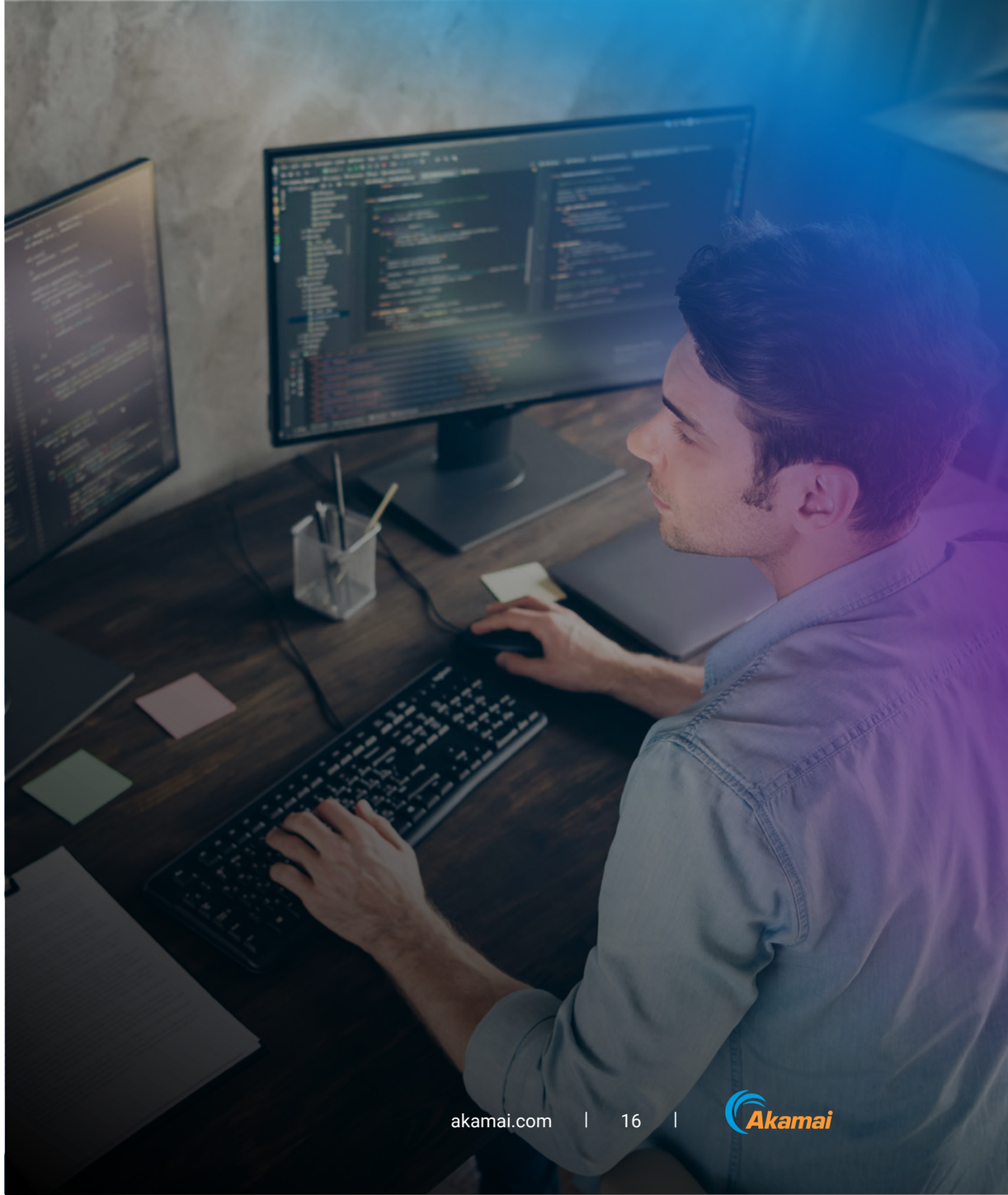
Die OpenAPI Specification definiert die Beschreibungen von Standardschnittstellen. Eine API-Sicherheitslösung sollte Folgendes bieten:

- Vergleich der API-Spezifikationen mit dem tatsächlich beobachtbaren Traffic und Erkennen von Unterschieden. So können Unternehmen sehen, welche ihrer bereitgestellten APIs außerhalb der Spezifikationen liegen und potenziell ein Risiko darstellen.
- Automatisch eine vollständige OpenAPI-Dokumentation basierend auf dem aktuellen und zukünftigen Zustand der API generieren, um sicherzustellen, dass alle APIs ordnungsgemäß dokumentiert sind und die Dokumentation auf dem neuesten Stand ist. Die Erkennung dieser und anderer Quellen ausnutzbarer Informationen kann Teams auch dabei helfen, potenzielle Angriffspfade zu verstehen, die von Cyberkriminellen ausgenutzt werden könnten.

Erkennung und Behebung von API-Bedrohungen: Die wichtigsten Funktionen im Detail

Angriffe, bei denen Cyberkriminelle versuchen, API-Schwachstellen auszunutzen, sind heute ein reales Problem. Es geht nicht mehr darum, ob Ihr Unternehmen angegriffen wird, sondern wann und wie. Es ist unerlässlich, Angriffe schnell zu erkennen und zu blockieren, bevor sie erheblichen Schaden anrichten, z. B. das Extrahieren privater Kundendaten. Selbst wenn Ihre APIs maximal abgesichert sind, benötigen Sie während der Laufzeit aktiven Schutz, um Datenlecks, Datenmanipulationen, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und API-Sicherheitsangriffe zu erkennen. Dazu gehören die Protokollierung des API-Traffics, die Überwachung des Zugriffs auf sensible Daten, die Erkennung von Bedrohungen und das Blockieren oder Beheben von Angriffsvektoren.

Auf den folgenden beiden Seiten erläutern wir die wichtigsten Funktionen, die Teil einer API-Sicherheitslösung sein sollten.



Out-of-Band-Überwachung in Echtzeit

Die API-Sicherheitsüberwachung sollte den API-Traffic nicht beeinträchtigen oder verlangsamen. Suchen Sie nach Anbietern mit einem agentenlosen Ansatz, der es Unternehmen ermöglicht, die Lösung schneller zu implementieren und mehr Traffic zu überwachen. Unter Umständen (z. B. in komplexen On-Prem-Umgebungen) sollte die Lösung jedoch flexibel genug sein, um auch Agents zu unterstützen.

Eine API-Sicherheitslösung sollte den Traffic von identifizierten Datenquellen spiegeln und im Hintergrund analysieren, wobei bei erkannten Problemen in Echtzeit Warnungen ausgegeben werden.

Erkennung von API-Anomalien und -Exploits

Die passive Datenerfassung reicht nicht aus, insbesondere da die Anzahl der APIs und das Gesamtvolumen des API-Traffics weiter ansteigen. API-Aktivitäten müssen kontinuierlich analysiert werden, um anomale Ereignisse zu erkennen und das Sicherheits- und Betriebsteam warnen zu können.

Fortschrittliche Tools umfassen KI-Funktionen und maschinelles Lernen, um Traffic in Echtzeit zu analysieren und kontextbezogene Informationen zu nutzen, um anomale Aktivitäten, die auf Datenlecks, Datenmanipulationen, Verstöße gegen Datenrichtlinien und andere API-Sicherheitsangriffe hinweisen, zu erkennen.

API-Angriffe verhindern

Sobald eine Anomalie oder ein anderes Problem erkannt und ein Alarm generiert wurde, dürfen Sie keine Zeit verlieren. Die nichtautorisierte Übertragung vertraulicher Daten über APIs oder eine andere Form von mutmaßlichem API-Missbrauch muss erkannt und blockiert werden. Eine API-Sicherheitslösung sollte Missbrauch nicht allein durch die Integration in Ihre vorhandenen Firewalls und API-Gateways verhindern, sondern auch die Problembehebung teilweise oder vollständig automatisch durchführen. Für einige Arten von Alarmen sollte eine halbautomatische Problembehebung zur Verfügung stehen. Bei bereits identifizierten, wiederkehrenden Problemen sollten Sie die Möglichkeit haben, eine vollständig automatisierte Reaktion bereitzustellen.

Bewertungen zur Einordnung von Angriffen

Einige Lösungen auf dem Markt verwenden Algorithmen für maschinelles Lernen, die für die Auswertung externer und interner Signale, einschließlich API-Verhalten, Netzwerktrafficmustern, Standortdaten und Bedrohungsfeeds, entwickelt wurden. Mithilfe kontextbezogener Faktoren wie diesen kann eine Lösung bestimmen, mit welcher Wahrscheinlichkeit davon ausgegangen werden kann, dass ein erkannter Laufzeitvorfall das Ergebnis eines Cyberangriffs ist.

Integrationen für die Reaktion auf Vorfälle

Wenn es zu einem Vorfall kommt, muss eine API-Sicherheitslösung die erforderlichen Integrationen enthalten, um sicherzustellen, dass Maßnahmen zur Behebung den entsprechenden Teams zugewiesen werden. Wenn Fehlkonfigurationen, Verstöße gegen Datenrichtlinien oder verdächtige Verhaltensweisen erkannt werden, sollten diese an das API-Gateway, das SIEM-System und andere Informationssicherheits-Engines gemeldet werden, um das richtige Maß an Situationsbewusstsein sicherzustellen.

Im Allgemeinen sollte sich eine API-Sicherheitslösung problemlos in andere Sicherheits-, Überwachungs- und Verwaltungstools Ihres Unternehmens integrieren lassen.

API-Sicherheitstests: Die wichtigsten Funktionen im Detail

Ein Fehler, den viele Entwicklungsteams machen, ist, API-Tests zu spät zu beginnen, sodass es hier zu Engpässen kommt. Die Teams müssen einen „Shift Left“-Ansatz wählen, um sicherzustellen, dass Tests früh genug während des Entwicklungsprozesses beginnen, um sicherzustellen, dass sie umfassend sind. Effektive API-Sicherheitstests bieten erhebliche Vorteile:

- **Angriffen vorbeugen**
  - Das Entdecken von Schwachstellen, bevor APIs in die Produktion gelangen, um das Risiko eines erfolgreichen Angriffs zu verringern
- **Verbesserte Compliance**
  - Umfassende Tests helfen Ihnen dabei, Compliance sicherzustellen und Bußgelder und Rufschädigungen zu vermeiden
- **Mehr Vertrauen**
  - Strenge und effektive Tests können das Vertrauen Ihres Unternehmens in APIs stärken und sicherstellen, dass die Releases Ihrer Entwickler pünktlich erfolgen

Einige Anbieter auf dem Markt bieten Unternehmen Empfehlungen zur Behebung von Problemen in ihren Umgebungen und zur Aktivierung umfassender API-Testkonfigurationen. Empfehlungen können Maßnahmen zum Konfigurieren der richtigen Authentifizierungen oder zum Beheben von API-Abhängigkeiten enthalten. Der Vorteil: Wenn Sie Probleme mit der Geschäftslogik in Ihrer Umgebung lösen können, können Sie die Anzahl der für Tests optimierten APIs erhöhen, was zu einer größeren Testabdeckung führt.

Das gesamte Konzept des API-Sicherheitstests bleibt jedoch etwas undurchsichtig. Entwicklungsteams verstehen möglicherweise nicht vollständig, was dazugehört. „Shift Left"-API-Tests sind ein dreistufiger Prozess:

1. **Die API verstehen:** Das Verständnis des Anwendungsszenarios der API ist beim Testen hilfreich, insbesondere bei kniffligen Problemen mit der Geschäftslogik.
2. **Sicherstellen, dass eine korrekte Interaktion mit der API möglich ist:** Stellen Sie sicher, dass Sie die API wie vorgesehen verwenden können. Nur so können Sie validieren, dass Ihr Verständnis der API mit ihrer Funktionsweise übereinstimmt.
3. **Senden von Angriffstraffic an die API:** Dies kann die manuelle Bearbeitung von Anfragen an die API, das Einfügen von zufälligen, unstrukturierten Daten in Anfragen oder die Verwendung eines automatisierten Tools für die Durchführung von API-Sicherheitstests umfassen. Wie fast immer in der modernen IT ist Automatisierung oft der beste Weg, um diese Arbeit in großem Maßstab zu erledigen, ohne dabei Geschwindigkeitseinbußen hinnehmen zu müssen.

Wichtige Funktionen für API-Sicherheitstests

API-Sicherheitstests sollten statische, dynamische und Penetrationstests umfassen. Eine API-Sicherheitslösung sollte Tools enthalten, die gründliche Tests vereinfachen und Testprozesse so weit wie möglich automatisieren. Achten Sie darauf, dass eine API-Sicherheitslösung folgende API-Testfunktionen umfasst:

Proaktive automatisierte API-Sicherheitstests

Automatisierte Sicherheitstests reduzieren Risiken und Kosten erheblich, da Fehlkonfigurationen, Schwachstellen und mangelnde Compliance erkannt werden, bevor eine API in die Produktion gelangt.

API-Governance

Es ist wichtig, Governance-Belange wie Rollen, Verantwortlichkeiten und Richtlinien zu bedenken. Dazu gehören die Verantwortlichkeiten der Entwickler, Sicherheitstechniker und Plattformentwickler auf Ausführungsebene sowie die Richtlinienüberwachung und Entscheidungen über Risiken. Eine API-Sicherheitslösung sollte es Ihnen ermöglichen, Ihre API-Spezifikationen anhand etablierter Governance-Richtlinien und -Regeln zu überprüfen.

Integration einer CI/CD-Pipeline und eines Code-Repository

DevSecOps ist eine Variante von DevOps, die dem Softwareentwicklungs-Workflow mehr Sicherheit verleiht. API-Sicherheit muss Teil der DevSecOps-Initiativen sein. Eine API-Sicherheitslösung sollte eine Suite von API-fokussierten Sicherheitstests bereitstellen, die nach Bedarf oder als Teil einer CI/CD-Pipeline ausgeführt werden. Die CI/CD-Integration ist entscheidend, da sie kontinuierliche, schnelle API-Sicherheitstests ermöglicht, die notwendig sind, um mit der Anwendungsentwicklung Schritt zu halten.

Alles zusammenbringen: Identifizieren und beheben Sie API-Sicherheitslücken

APIs sind ein wesentlicher Bestandteil der Fähigkeit von Unternehmen, in einer zunehmend digitalen und cloudorientierten Wirtschaft 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 in der heutigen Zeit jedoch zu einem attraktiven Ziel für Angreifer.

Die vorhandenen Tools, die viele Unternehmen zur Verwaltung von APIs, und um einen Basisschutz zu erhalten, verwenden, reduzieren das Risiko bis zu einem bestimmten Grad. Doch sie reichen nicht aus, um es mit den heutigen API-Bedrohungen aufzunehmen. Sie können nicht als einzige Schutzmaßnahme eingesetzt werden.

Stattdessen sollten Unternehmen eine umfassende API-Sicherheitslösung anstreben, die alle vier in diesem Kaufratgeber beschriebenen Komponenten umfasst: API-Erkennung, Sicherheitsmanagement, Erkennung und Behebung von Bedrohungen sowie Sicherheitstests. Sie müssen nicht auf vorhandene Tools verzichten, die sich in bestimmten Bereichen als effektiv erwiesen haben – suchen Sie einfach nach einer Lösung, die sich nahtlos in Ihre vorhandenen Tools integrieren lässt.

API-Sicherheit einzuführen, bedeutet nicht, dass Sie eine erhebliche Menge an Ressourcen zuweisen müssen. Beginnen Sie mit einer kleineren, überprüfbaren Pilotlösung, die bestimmte Lücken in Ihrem Sicherheitspaket schließt. Oder beginnen Sie Ihre API-Sicherheitsreise mit einem umfassenden Update. Jedes Unternehmen ist anders.

Da es immer häufiger zu API-fokussierte Angriffen kommt, ist die Entscheidung, Maßnahmen zu ergreifen, der wichtigste Schritt. Wir hoffen, dass Sie diesen Kaufratgeber hilfreich fanden.

Erfahren Sie mehr über API-Angriffsmethoden, häufige API-Schwachstellen und wie Sie Ihr Unternehmen schützen können.

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 auf **X** (ehemals Twitter) und **LinkedIn**. Veröffentlicht: 09/24.

Akamai