Der Leitfaden zur API-Erkennung

Inhaltsverzeichnis

Die Bedeutung der API-Erkennung

Egal, ob Sie mit der Sicherung Ihrer APIs erst beginnen oder Ihre bestehende Strategie weiter verfeinern möchten – die Suche und Inventarisierung jeder API in Ihrem Unternehmen ist ein grundlegender Schritt. Warum? Für jede Anwendung, die Ihr Unternehmen erstellt, jede Workload, die es in die Cloud migriert, und jedes Tool, das seine Mitarbeiter zur Zusammenarbeit verwenden, gibt es APIs, die im Hintergrund Daten (häufig sensible Daten) austauschen. Die Herausforderung besteht darin, dass die meisten Unternehmen – selbst diejenigen, die um den Wert eines vollständigen Bestands wissen – einen Großteil ihrer APIs nicht wirklich sehen.

Und APIs, die Sie nicht sehen, können Sie nicht sichern.

Da Unternehmen zunehmend cloudzentriert und digital arbeiten, nimmt ihre API-Umgebung an Umfang und Komplexität zu. 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 und Entwickler-Ökosystemen hergestellt haben.

Da Ihre APIs an Umfang und Komplexität zunehmen, ist es schwierig, Echtzeit-Einblicke in folgende Aspekte zu gewinnen:

- Wo in Ihren verschiedenen Geschäftseinheiten – die in vielen Fällen über jeweils eigene Entwicklerteams verfügen – sich Ihre APIs befinden
- Wie Ihre APIs konfiguriert sind, wohin sie weitergeleitet werden und ob sie über ordnungsgemäße Authentifizierungs- und Autorisierungskontrollen verfügen
- Ob Ihre APIs beim Aufruf vertrauliche Daten zurücksenden und wer Zugriff auf diese Daten erhalten kann

Und was die Sache noch schwieriger macht, ist, dass ein großer Teil der APIs, die sich im Unternehmen ansammeln, nicht verwaltet wird, nicht sichtbar ist und oft über keinen Schutz verfügt. Zu dieser Gruppe gehören veraltete, Shadow- und Zombie-APIs, die in vielen Fällen im Schutz durch häufig verwendete Tools wie API-Gateways und Web Application Firewalls (WAFs) nicht berücksichtigt werden. Diese Tools bieten zwar Vorteile und grundlegenden Schutz, doch die heutige API-Bedrohungslandschaft erfordert den höheren Grad an Transparenz, Echtzeitschutz und die kontinuierlichen Tests, die spezielle API-Sicherheitslösungen bieten.

Wenn Sie all Ihre APIs finden können, haben Sie die Grundlage für die nächsten wichtigen Schritte geschaffen. Dazu gehören u. a. die Bewertung der Risiken jeder API, das Verständnis der API-Sicherheitslage Ihres Unternehmens und die Nutzung der gewonnenen Erkenntnisse, um Angriffe durch Schutzmaßnahmen in Echtzeit zu verhindern. In diesem Whitepaper stellen wir Ihnen Folgendes vor:

- Erkenntnisse darüber, warum bestimmte APIs für Sicherheitsteams so schwer fassbar sind
- Details zu API-Erkennungsfunktionen, mit denen Sie Transparenz gewinnen und Angriffe verhindern können

Warum sind APIs so schwer zu finden?

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. Exponierte oder falsch konfigurierte APIs sind weit verbreitet, ungeschützt und für Cyberkriminelle leicht zu kompromittieren. Und es steht viel auf dem Spiel. Angriffe auf Ihre APIs können den Umsatz, die Ausfallsicherheit und die Einhaltung gesetzlicher Vorschriften im Unternehmen gefährden.

Hier sind vier Möglichkeiten, wie nicht autorisierte APIs entstehen können:

1. API-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.

2. 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 für einige Zeit gleichzeitig mit einer neuen Version existieren, während die Software aktualisiert wird. Aber die Person, die für die Deaktivierung der API verantwortlich ist, verlässt das Unternehmen, wechselt die Abteilung oder vergisst einfach, die veraltete Version außer Betrieb zu nehmen. APIs können auch offiziell außer Betrieb genommen werden, bleiben aber aufgrund von operativen Versäumnissen weiterhin in Betrieb. Beide Szenarien führen dazu, dass sogenannte Zombie-APIs entstehen.

3. Geerbte APIs

APIs, die im Rahmen von Fusionen oder Übernahmen vererbt wurden, werden häufig übersehen und in weiterer Folge zu Shadow-APIs. Inventare (sofern vorhanden) gehen durch die schwierige und komplizierte Integration von Systemen häufig verloren. Größere Unternehmen, die zahlreiche kleinere Unternehmen übernehmen, sind besonders gefährdet, da die übernommenen API-Umgebungen sich häufig unkontrolliert ausbreiten und nicht dokumentiert sind.

4. Kommerzielle APIs

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

Was ist API-Erkennung?

Unter API-Erkennung versteht man einen Prozess und eine Reihe von Funktionen, mit denen Unternehmen APIs identifizieren, katalogisieren, verwalten und ihre API-bezogenen Risiken beurteilen können. Wenn sie ordnungsgemäß durchgeführt wird, kann API-Erkennung Unternehmen bei Folgendem unterstützen:

- die unkontrollierte Ausbreitung von APIs (die schnell wachsende Anhäufung von APIs ohne ordnungsgemäße Dokumentation oder Überwachung, auch API-Sprawl genannt) zu reduzieren und die Sicherheit zu verbessern
- ihre aktuelle API-Landschaft besser zu verstehen und fundierte Entscheidungen mit Blick auf zukünftige Entwicklungen zu treffen
- Überwachung und Kontrolle des Zugriffs auf die APIs zu erleichtern, um sicherzustellen, dass nur autorisierte Nutzer Zugriff haben

Wichtige API-Erkennungsfunktionen zur Erhöhung der Transparenz und Risikominderung

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 ein Inventar aufnehmen, unabhängig von Konfiguration oder Typ

nicht verwaltete APIs, wie z. B. veraltete und Zombie-APIs, zu **erkennen**

vergessene, ungenutzte oder anderweitig unbekannte Schatten-Domains zu **identifizieren**

Sichtbarkeitslücken zu **beseitigen** und potenzielle Angriffspfade zu ermitteln

Beachten Sie beim Evaluieren neuer Lösungen zur API-Erkennung die folgenden Funktionen – ein Erkennungstool sollte sie alle enthalten.

Erkennung aller API-Typen

Ein API-Erkennungstool muss in der Lage sein, APIs aller Konfigurationen oder Arten zu identifizieren. Das umfasst auch RESTful-, GraphQL-, SOAP-, XML-RPC-, JSON-RPC- und gRPC-APIs.

Detailliertes API-Inventar

Ein API-Erkennungstool sollte außerdem 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.

Schwer fassbare APIs erkennen

Nicht verwaltete APIs sind gegebenenfalls älter als die API-Sicherheitsinitiativen Ihres Unternehmens. Die Ursprünge der unkontrollierten Ausbreitung Ihrer APIs liegen möglicherweise bei einem Entwicklerteam, das es in Ihrem Unternehmen nicht mehr gibt. Diese APIs verfügen in der Regel nicht über einen Owner und arbeiten ungesehen oder ohne Sicherheitskontrollen. Es ist wichtig, dass ein Erkennungstool diese APIs findet.

Erkennung von Shadow-API-Domains

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

Automatische API-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.

Keine erforderlichen Integrationen

Ein API-Erkennungstool sollte in der Lage sein, Ihre API-Umgebung vollständig zu erkennen und anfällige APIs und Shadow-Domains zu finden, ohne dass spezielle Integrationen oder Softwareinstallationen erforderlich sind. Das ist wichtig, um Sichtbarkeitslücken zu vermeiden, die einfach dadurch entstehen können, dass nicht die richtigen Agents installiert sind oder das Tool nicht korrekt konfiguriert wurde.

Eingeschränkte nutzerdefinierte Entwicklung

Und schließlich sollte ein 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.

Wie Akamai Sie dabei unterstützt, alle APIs zu erkennen

Umfassende und kontinuierliche API-Erkennungsfunktionen bieten Unternehmen folgende Vorteile:

- die vollständige API-Angriffsfläche verstehen
- die Kosten Ihrer API-Bestände und Dokumentationsaktualisierungen senken
- die Einhaltung gesetzlicher Vorschriften und interner Richtlinien verbessern

Die heutigen Bedrohungen erfordern eine umfassende API-Sicherheitslösung, die vier kritische Bereiche umfasst: API-Erkennung, Sicherheitsmanagement, Erkennung und Behebung von Bedrohungen sowie Sicherheitstests. Akamai API Security bietet alle vier dieser wichtigen Module und schützt APIs während ihres gesamten Lebenszyklus von der Entwicklung bis zur Produktion. API Security wurde für Unternehmen entwickelt, die Partnern, Lieferanten und Nutzern APIs zur Verfügung stellen. Die API-Security-Lösung ermittelt APIs, versteht deren Risikopotenzial, analysiert ihr Verhalten und hält Bedrohungen fern.

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.

Informationen zu Akamai

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: Oktober 2024.