AKAMAI-PRODUKTBESCHREIBUNG

API Security

Mit API Security von Akamai schützen Sie Ihre APIs auf intelligente Weise vor Missbrauch der Geschäftslogik und Datendiebstahl.

API-Bedrohungen entwickeln sich weiter

APIs sind der Motor, der Ihr Unternehmen antreibt – sie verbinden es mit Partnern, Lieferanten und Kunden. Doch mit jeder weiteren API vergrößert sich Ihre Angriffsfläche, und das wissen auch die Bedrohungsakteure. API-Angriffe nehmen rasant zu und entwickeln sich schnell weiter, oft auf eine Art und Weise, die Ihr Webanwendungs- und API-Schutz nicht erkennt. Und ohne eine umfassende Bestandsaufnahme Ihrer APIs entsteht schnell ein blinder Fleck und die APIs Ihres Unternehmens sind ungeschützt.

Warum Akamai API Security?

Unsere Plattform 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. API Security ermittelt Ihre APIs, versteht deren Risikopotenzial, analysiert ihr Verhalten und hält Bedrohungen fern.

Die kritischen Funktionen von API Security

Entdeckung

Es ist nicht ungewöhnlich, APIs zu haben, von denen niemand weiß. Doch ohne eine genaue Bestandsaufnahme ist Ihr Unternehmen einer Reihe von Sicherheitsrisiken ausgesetzt. Schluss mit dem Rätselraten – wir helfen Ihnen weiter:

- Erkennen und inventarisieren Sie alle APIs unabhängig von der Konfiguration oder Art, einschließlich RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC und gRPC
- Entdecken Sie inaktive, veraltete und Zombie-APIs
- Identifizieren Sie vergessene, ungenutzte oder anderweitig unbekannte Schatten-Domains
- Beseitigen Sie blinde Flecken und ermitteln Sie potenzielle Angriffspfade

Tests

Anwendungen werden schneller als je zuvor entwickelt. Das bedeutet auch, dass Sicherheitslücken oder Entwicklungsfehler leichter unentdeckt bleiben. Mit unserer Suite an API-Sicherheitstests können Sie:

- automatisch über 150 Tests durchführen, die schädlichen Traffic simulieren, einschließlich der OWASP API Security Top 10-Bedrohungen
- Schwachstellen entdecken, bevor APIs zum Einsatz kommen, um das Risiko eines erfolgreichen Angriffs zu verringern
- Ihre API-Spezifikationen anhand etablierter Governance-Richtlinien und -Regeln überprüfen
- auf APIs fokussierte Sicherheitstests bei Bedarf oder entlang einer CI/CD-Pipeline ausführen

VORTEILE FÜR IHR UNTERNEHMEN

Entdeckung
Erhalten Sie Einblick in Ihre API-Angriffsfläche. Senken Sie die Kosten Ihrer API-Bestände und Dokumentationsaktualisierungen. Verbessern Sie die Einhaltung gesetzlicher Vorschriften und interner Richtlinien.

Tests
Senken Sie die Kosten für die Behebung von Problemen, indem Sie sie schneller erkennen. Verbessern Sie die Codequalität ohne Abstriche bei der Geschwindigkeit. Steigern Sie den Umsatz durch Beschleunigung der Markteinführung.

Erkennung
Verschaffen Sie sich wichtigen Geschäftskontext, indem Sie herausfinden, was genau passiert ist. Ermitteln Sie, worin das Problem besteht, und decken Sie die potenzielle Auswirkungen auf. Bestimmen Sie die optimalen Abhilfemaßnahmen.

Reaktion
Verringern Sie Risiken, indem Sie Angriffe sofort stoppen. Senken Sie die Kosten, indem Sie Schwachstellen beheben, bevor sie ausgenutzt werden. Reduzieren Sie Umsatzverluste durch Ausfallzeiten.

Akamai

Erkennung

Einfache API-Fehlkonfigurationen können Sie schutzlos gegenüber Cyberkriminellen machen. Wenn Hacker erst einmal in Ihr Unternehmen eingedrungen sind, können sie schnell auf Ihre vertraulichen Daten zugreifen und diese stehlen. Nutzen Sie unsere Plattform, um:

- 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

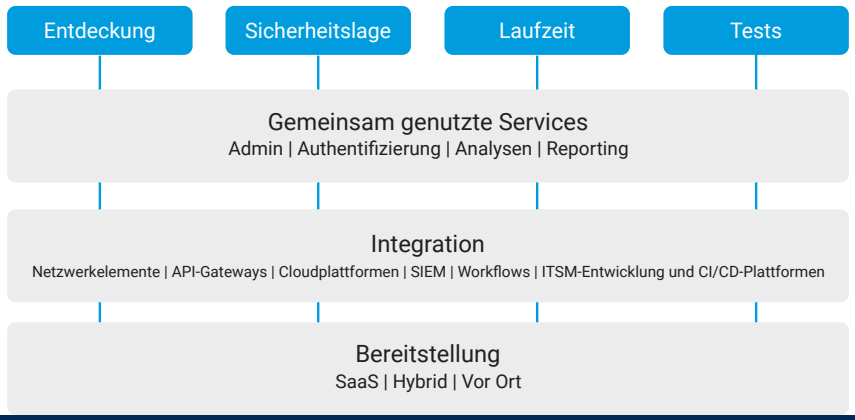
Reaktion

Die Frage ist nicht mehr, ob, sondern wann Ihr Unternehmen angegriffen wird. Das bedeutet, dass Sie Angriffe in Echtzeit erkennen und blockieren können müssen. Nutzen Sie unsere auf künstlicher Intelligenz/maschinellem Lernen basierende Anomalieerkennung, um:

- Daten auf Manipulation und Datenlecks, Richtlinienverstöße, verdächtiges Verhalten und API-Angriffe zu überwachen
- den API-Traffic ohne zusätzliche Änderungen am Netzwerk oder schwer zu installierende Agents zu analysieren
- Sicherheits-/Betriebsteams durch Integration in bestehende Workflows (Ticketing, Security Information and Event Management [SIEM] usw.) warnen zu können
- Angriffe und Missbrauch in Echtzeit mit teil- oder vollautomatischen Abhilfemaßnahmen zu verhindern

Akamai macht den Unterschied: Blockieren an der Edge

Akamai App & API Protector erkennt und wehrt API-Bedrohungen für Anwendungen und APIs ab, die über die Akamai Connected Cloud ausgeführt werden, und kann jeglichen Traffic blockieren, der von API Security erkannte potenzielle Bedrohungen enthält. Bei gemeinsamer Bereitstellung bieten die API-Schutzfunktionen von Akamai umfassende und kontinuierliche Einblicke in APIs und ermöglichen es Ihnen, API-Sicherheitsprobleme in Ihrer gesamten Anwendungsumgebung zu entdecken, zu prüfen, zu erkennen und zu beheben.



Möchten Sie erfahren, wie API Security funktioniert? Vereinbaren Sie unter akamai.com/apisecurity ein Gespräch mit unserem Team.

 | Veröffentlicht: Juni 2024