Akamai

WHITEPAPER

Eine Strategie zum Schutz vor den OWASP Top 10 API-Sicherheitsrisiken

Wie Akamai Sie bei der Bewältigung häufiger API-Schwachstellen und -Bedrohungen unterstützen kann

OWASP Top 10 API-Sicherheitsrisiken		Kann Akamai Unterstützung bieten?
API1:2023	Fehlerhafte Autorisierung auf Objektebene	☑
API2:2023	Schwachstellen bei der Nutzerauthentifizierung	☑
API3:2023	Fehlerhafte Autorisierung auf Objekteigenschaftsebene	☑
API4:2023	Uneingeschränkter Ressourcenverbrauch	☑
API5:2023	Fehlerhafte Autorisierung auf Funktionsebene	☑
API6:2023	Unbeschränkter Zugriff auf sensible Geschäftsabläufe	☑
API7:2023	Serverseitige Fälschung von Anfragen	☑
API8:2023	Fehlerhafte Sicherheitskonfiguration	☑
API9:2023	Unsachgemäße Bestandsverwaltung	☑
API10:2023	Unsicherer Verbrauch von APIs	☑

APIs stehen im Kern der digitalen Produkte, Services und Cloud-Umgebungen des Unternehmens. Sie sind auch der Standard für die Erstellung und Verbindung von Anwendungen, da Unternehmen zunehmend auf Mikroservices-basierte Architektur für die Entwicklung von Anwendungen umsteigen. Der ständige Zugriff auf Daten und kritische Systeme macht sie sowohl zu einem Umsatztreiber als auch zu einem Betriebsrisiko.

Exponierte oder falsch konfigurierte APIs sind weit verbreitet, leicht zu missbrauchen und häufig ungeschützt. Und nur eine erfolgreich angegriffene API kann dazu führen, dass Millionen von Datensätzen gestohlen werden.

78 % der Unternehmen berichten, dass sie innerhalb eines Jahres API-Sicherheitsvorfälle erlebt haben. Daher sollte der Schutz von APIs Priorität haben. Doch die API-Angriffsfläche ist schnell zu einem beliebten Ziel geworden – viel schneller, als die meisten Unternehmen in der Lage waren, dafür ein Verständnis zu entwickeln:

API-Risiken

API-Angriffsmethoden

API-Sicherheitskontrollen und -Funktionen

Was umfasst die API-Angriffsfläche? Die kurze Antwort lautet, dass sie viel breiter ist, als viele Unternehmen annehmen. Das traditionelle Verständnis von APIs (z. B. zwischen Computern oder Drittanbieter-APIs) muss auf mobile und Webanwendungsservices als Teil einer Microservices-Architektur erweitert werden. Anders ausgedrückt: Eine Webanfrage innerhalb der Architektur ist eine API, eine in einer Reihe von Aufrufen verschiedener Microservices.

78 %

der Unternehmen berichten, dass sie innerhalb eines Jahres API-Sicherheitsvorfälle erlebt haben. Der Schutz von APIs sollte eindeutig Priorität haben.

Am 5. Juni 2023 gab das Open Worldwide Application Security Project (OWASP) die erste umfassende Aktualisierung seiner 2019 veröffentlichten Liste der Top 10 API-Sicherheitsrisiken heraus. In der aktualisierten Liste wird beschrieben, wie jeder dieser API-Aufrufe Sicherheitslücken öffnen und Datenschutzrisiken verursachen kann. Dazu gehören:

Mangelhafte Datenvalidierung

Konfigurations-fehler

Implementie-rungsfehler

Integrations-lücken zwischen Sicherheits-komponenten

Lesen Sie weiter, um mehr über die wichtigsten vom OWASP identifizierten Risiken zu erfahren und wie die API-Sicherheitslösungen von Akamai diese mindern können.

Das Problem besteht darin, dass selbst bei Unternehmen, die behaupten, über ein vollständiges Inventar ihrer APIs zu verfügen, eine gravierende Diskrepanz auftritt:

Nur **4 von 10** wissen, welche APIs bei einem Aufruf vertrauliche Daten zurückgeben

API1:2023 – Fehlerhafte Autorisierung auf Objektebene

Sicherheitslücken durch fehlerhafte Autorisierung auf Objektebene (Broken Object Level Authorization – BOLA) entstehen, wenn die Autorisierung eines Clients nicht ordnungsgemäß für den Zugriff auf spezifische Objekt-IDs validiert wird. Über diese Schwachstelle können sich Angreifer direkten Zugriff auf Ressourcen verschaffen, indem sie den erwarteten Anwendungs-Workflow umgehen und unbefugten Zugang zu sensible Daten erhalten. Unternehmen können dieses Risiko verringern, indem sie die alleinige Abhängigkeit von Objekt-IDs vermeiden, die Kunden in ihren Anfragen übermitteln. Stattdessen können Unternehmen nicht zu erratende zufällige IDs für Objekte verwenden, um eine zuverlässige Validierung für jedes Objekt zu gewährleisten. Gegebenenfalls kann die Maskierung der tatsächlichen ID von Objekten eine zusätzliche Sicherheitsebene bieten.

Wie Akamai Sie unterstützen kann

Die hochsensiblen Überwachungssysteme von Akamai verfolgen Bedrohungen und generieren Warnungen bei versuchten BOLA-Exploits, um sofortige Aufmerksamkeit und Maßnahmen zu gewährleisten.

Akamai verringert Risiken durch die folgenden Maßnahmen:

- Ermitteln von BOLA-Angriffsversuchen
- Klassifizierung von API-Endpunkten, die für BOLA-Exploits anfällig sind, basierend auf empfangenen Eingaben (z. B. auflistbare Parameter) sowie den Beziehungen zwischen API-Objekten und -Eigenschaften
- Generieren von Warnungen bei versuchten oder erfolgreichen BOLA-Angriffen

API2:2023 – Fehlerhafte Authentifizierung

Fehlerhafte Authentifizierung bezieht sich auf weitreichende Sicherheitslücken im Authentifizierungsprozess, durch die das System Angreifern ausgesetzt ist. Diese können entsprechende Schwachstellen ausnutzen und den API-Objektschutz gefährden. In der Regel manipulieren Angreifer, die Schwachstellen in Verbindung mit fehlerhafter Authentifizierung nutzen, Lücken im System, wie z. B. schwache Passwörter oder Sitzungswiedergabe. Zum Schutz vor Schwachstellen bei der Authentifizierung können Unternehmen zuverlässige Authentifizierungs- und Mechanismen zur Verwaltung von Geheimnissen einrichten, wie z. B. starke Passwort-Richtlinien, Schlüsselrotation, starke Tokensignaturen und Verschlüsselungsschlüssel. Die unternehmensweite Umsetzung dieser strikten Richtlinien kann das Risiko erheblich reduzieren.

Wie Akamai Sie unterstützen kann

Akamai unterstützt die API-Sicherheit durch Identifizierung und Korrektur anfälliger Authentifizierungspunkte, Abwehr automatisierter Angriffe und proaktive Benachrichtigung bei Angriffsversuchen.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Identifizieren von API-Endpunkten, die keine Authentifizierung erfordern oder die Best Practices für die Authentifizierung nicht befolgen, z. B. schwache Tokensignaturen oder Verschlüsselungsschlüssel und das Akzeptieren abgelaufener Authentifizierungstoken
- Schutz vor automatisierten Wörterbuch- oder Credential-Stuffing-Angriffen durch unsere Bot-Management-Funktionen
- Abwicklung der Autorisierung von JSON-Web-Token mithilfe starker Tokensignaturen über unsere API-Gateway-Funktionen
- Generieren von Warnungen bei BUA-Angriffsversuchen

API3:2023 – Fehlerhafte Autorisierung auf Objekteigenschaftsebene

Fehlerhafte Autorisierung auf Objekteigenschaftsebene (Broken Object Property Level Authorization – BOPLA) ist ein Sicherheitsfehler, bei dem ein API-Endpunkt mehr Dateneigenschaften offenlegen kann, als für seine Funktion erforderlich ist, und so das Prinzip der geringstmöglichen Berechtigungen vernachlässigt wird.

Dieser Fehler kann Angreifern unbeabsichtigt einen übermäßigen Zugriff auf Daten ermöglichen, die dann verwendet werden können, um weitere Schwachstellen aufzudecken oder nach sensiblen Daten zu schürfen. Dies schließt Szenarien ein, in denen Eigenschaften, die ausschließlich dem Zugriff auf Administratorebene vorbehalten sind, von unbefugten Nutzern manipuliert werden können, was die Systemintegrität weiter beeinträchtigt. Um die Sicherheit zu gewährleisten und Angreifer daran zu hindern, unnötig viele Informationen zu erhalten oder Informationen zu manipulieren, ist es wichtig, geeignete Zugriffsebenen und Datenzugänge bereitzustellen, um potenzielle Angreifer daran zu hindern, Sicherheitslücken auszunutzen.

Wie Akamai Sie unterstützen kann

Mithilfe der umfassenden Taktiken von Akamai können Unternehmen BOPLA-Risiken mindern, indem sie API-Endpunkte und ihre zugehörigen Eigenschaften identifizieren und katalogisieren.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- ✓ Identifizieren und Kennzeichnen aller Endpunkte und der API-Eigenschaften, die diese Endpunkte offenlegen, wie z. B. personenbezogene Daten (PII)
- ✓ Identifizieren von nicht dokumentierten oder Shadow-API-Endpunkten, -Objekten und -Eigenschaften sowie ungewöhnlichen Eigenschaften
- ✓ Anwendung von Sicherheitsrichtlinien auf akzeptable und definierte Parameter und Eigenschaften, um die Datenbereinigung sicherzustellen
- ✓ Anwendung von Sicherheitsrichtlinien basierend auf der vollständigen API/Swagger-Spezifikation, wobei lediglich genau definierte API-Endpunkte und Methoden für den Zugriff auf API-Objekte und -Eigenschaften zugelassen sind
- ✓ Generieren von Warnungen zu versuchten BOPLA-Angriffen

API4:2023 – Uneingeschränkte Ressourcennutzung

Uneingeschränkte Ressourcennutzung (manchmal auch als „API-Ressourcenerschöpfung“ bezeichnet) ist eine Art von Sicherheitslücke, bei der APIs die Zahl der Anfragen oder das Datenvolumen, das sie innerhalb eines bestimmten Zeitraums bereitstellen, nicht beschränken. Diese Schwachstelle können Angreifer für DoS-Angriffe (Denial-of-Service) nutzen, die das System für legitime Nutzer unverfügbar machen können. Solche Angriffe können schwerwiegende geschäftliche Auswirkungen haben und je nach Dauer und Umfang des Ausfalls zu eingeschränkter Serviceverfügbarkeit, Unzufriedenheit der Kunden und potenziellen Umsatzeinbußen führen. Zur Vermeidung von Serviceverlusten ist es sehr wichtig, Maßnahmen zu ergreifen, die die Zahl der API-Anfragen und den Umfang der zurückgegebenen Daten begrenzen.

Wie Akamai Sie unterstützen kann

Akamai schützt Ihre APIs vor Bedrohungen durch uneingeschränkter Ressourcennutzung durch die folgenden Maßnahmen:

- Identifizierung gefährdeter Endpunkte und Bereitstellung von Echtzeitwarnungen bei versuchten volumetrischen Angriffen
- Überprüfung von übermäßigen Fehlern, Anmeldeversuchen oder atypischem Verhalten, die auf Risikofaktoren hindeuten.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Identifizierung von API-Endpunkten, die nicht über Ratenbeschränkung verfügen oder durch große volumetrische Wörterbücher oder Credential Stuffing angegriffen werden
- Initiierung von Workflows, um volumetrische Angriffe zu verlangsamen oder zu blockieren
- Generieren von Warnungen bei versuchten volumetrischen Angriffen

API5:2023 – Fehlerhafte Autorisierung auf Funktionsebene

Fehlerhafte Autorisierung auf Funktionsebene (Broken Function Level Authorization – BFLA) kann auftreten, wenn Zugriffskontrollmodelle für API-Endpunkte falsch implementiert sind. Falsche oder veraltete Zugriffskontrollmethoden können den unbefugten Zugriff nicht ausreichend einschränken, sodass Angreifer auf vertrauliche Informationen oder das System als Ganzes zugreifen können. Um dieses Risiko zu minimieren, können Unternehmen das Prinzip der geringsten Berechtigungen anwenden und sicherstellen, dass alle Funktionen, insbesondere administrative Funktionen, nur Nutzern mit den entsprechenden Berechtigungen zugänglich sind.

Wie Akamai Sie unterstützen kann

Durch die Verfolgung von Verhaltenszeitmustern, die Anwendung von Sicherheitsrichtlinien für sensible Funktionen, die Verwaltung von Schlüsselrotation und -widerruf und die sofortige Benachrichtigung bei verdächtigen Zugriffsversuchen kann Akamai die BFLA-Präventions- und Reaktionsstrategie von Unternehmen stärken.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Ermitteln von Verhaltenszeitmustern für den API-Endpunktzugriff durch Erfassen von Nutzern, API-Schlüsseln, Zugriffstoken, Session-IDs usw.
- Anwenden von Schlüsselrotation oder Widerruf von offengelegten Schlüsseln über Akamai API-Gateway-Funktionen
- Generieren von Warnungen bei verdächtigen Zugriffsversuchen auf administrative Funktionen

API6:2023 – Unbeschränkter Zugriff auf sensible Geschäftsabläufe

Ein unbeschränkter Zugriff auf sensible Geschäftsabläufe ist möglich, wenn eine API kritische Vorgänge wie Geschäftslogik ohne ausreichende Zugriffskontrolle offenlegt. Dies kann zu unbefugtem Zugriff und unbefugter Ausnutzung führen und erhebliche Schäden für ein Unternehmen verursachen. Die Ausnutzung umfasst in der Regel das Verständnis des Geschäftsmodells, das von der API unterstützt wird, die Identifizierung sensibler Geschäftsabläufe und die Ausnutzung von Schlupflöchern zu diesen Abläufen. Dies kann verschiedene Auswirkungen haben. Beispielsweise können legitime Nutzer daran gehindert werden, ein Produkt kaufen.

Wie Akamai Sie unterstützen kann

Sichern Sie Ihr Unternehmen mit den umfassenden API-Schutzlösungen von Akamai, die Identifizierung von sensiblen Endpunkten, Echtzeit-Exploit-Warnungen und Expertenberatung zum Schutz Ihrer wichtigsten Daten und Vorgänge bieten.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Identifizieren sensibler API-Endpunkte, wie Zahlungsflüsse oder Endpunkte, die personenbezogene Daten verarbeiten
- Generieren von Warnungen zu einer Vielzahl potenzieller Angriffe, von Datenextraktion oder Datenmanipulation bis hin zu verdächtigen Zugriffsversuchen an diesen sensiblen API-Endpunkten

API7:2023 – Serverseitig manipulierte Anfragen

Serverseitig manipulierte Anfragen (Server Side Request Forgery – SSRF) ermöglichen es einem Angreifer, die serverseitige Anwendung dazu zu veranlassen, HTTPS-Anfragen an eine beliebige Domain seiner Wahl zu senden. Bei einem typischen SSRF-Angriff verleitet der Angreifer den Server dazu, eine Anfrage an interne Ressourcen zu stellen. Dabei umgeht er Firewalls und erhält Zugriff auf interne Dienste, was zu Offenlegung von Daten oder Remoteausführung von Code führen kann. Um dieses Risiko zu minimieren, ist es entscheidend, Nutzereingaben zu validieren, zu filtern oder zu bereinigen und die ausgehenden Server-Verbindungen, zu begrenzen, damit er nur mit kritischen Services kommuniziert.

Wie Akamai Sie unterstützen kann

Verbessern Sie Ihre Sicherheit mit Akamai durch Erkennung von Anomalien in vertrauenswürdigen API-Verbindungen, effektives Schlüsselmanagement und sofortige Benachrichtigungen über SSRF-Exploitversuche.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Schutz von Webanwendungen und APIs durch Anwendung entsprechender Schutzrichtlinien, die auf SSRF-Angriffe abzielen
- Anwenden von Schlüsselrotation oder Widerruf von offengelegten Schlüsseln über API-Gateway-Funktionen

API8:2023 – Fehlerhafte Sicherheitskonfiguration

Fehlerhafte Sicherheitskonfiguration bezieht sich auf die unsachgemäße Einrichtung von Sicherheitskontrollen, die ein System anfällig für Angriffe machen kann. Zu nennen sind hier unsichere Standardkonfigurationen, unvollständige oder Ad-hoc-Konfigurationen, offene Cloud-Speicher, falsch konfigurierte HTTP(S)-Header und ausführliche Fehlermeldungen, die vertrauliche Informationen enthalten. Um Risiken zu minimieren, müssen Unternehmen sicherstellen, dass sie ihre Sicherheitskontrollen für alle Aspekte ihrer Anwendungen und APIs korrekt konfiguriert haben. Dies umfasst regelmäßige Updates, gründliche Tests und kontinuierliche Überwachung, um Fehlkonfigurationen umgehend zu identifizieren und zu beheben.

Wie Akamai Sie unterstützen kann

Verbessern Sie Ihre Einblicke, indem Akamai Sie mit der Erkennung von „Shadow"-, „Rogue"- oder „Zombie"-APIs unterstützt. Darüber hinaus profitieren Sie von Best Practices für die Sicherheit, zuverlässiger HTTPS-Implementierung und sofortigen Warnungen bei fehlerhaften Sicherheitskonfigurationen.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Identifizieren von „Shadow"-API-Endpunkten, die Umgebungen auf niedriger Ebene (z. B. Test- und Staging-Umgebungen) offenlegen können
- Identifizieren und Abgleichen von API-Endpunkten, -Objekten und -Eigenschaften anhand von Best Practices und Standards der Sicherheitskonfiguration
- Anwenden von Sicherheitsrichtlinien durch Best Practices für die API-Sicherheit, wie z. B. wohlgeformte HTTPS-Anfragen und -Antworten, Konfigurieren oder Entfernen korrekter HTTP-Header sowie vollständiges Kontrollieren der CORS- (Cross Origin Resource Sharing) und Cache-Control-Header
- Anwendung einer ordnungsgemäßen HTTPS-Implementierung über SSL/TLS, einschließlich korrekter und sicherer Verschlüsselungssammlungen
- Generieren von Warnungen für Fehlkonfigurationen oder mangelnde Compliance von Best Practices und Standards für die API-Sicherheit

API9:2023 – Unsachgemäße Bestandsverwaltung

Unsachgemäßes Bestandsmanagement stellt für jedes Unternehmen, das APIs verwaltet, eine Herausforderung dar. API-Sicherheitslösungen können bekannte APIs schützen. Unbekannte und auch Shadow-APIs sind aber möglicherweise nicht gepatcht und daher anfällig für Angriffe. Mögliche Folgen sind veraltete Komponenten, ungenutzte Seiten oder APIs und die unnötige Offenlegung vertraulicher Informationen. Nicht gewartete Service-Verwaltung kann Systeme anfällig für Bedrohungen machen, und Angreifer können über unbekannte APIs, die mit derselben Datenbank verbunden sind, möglicherweise Zugriff auf sensible Daten oder sogar auf den Server erhalten. Zugriffskontrollen und regelmäßige Audits sind unerlässlich, um die sich ständig ändernden Komponenten der Services eines Unternehmens zu vermeiden.

Wie Akamai Sie unterstützen kann

Akamai überwacht den API-Traffic ständig, um versteckte API-Endpunkte und risikobehaftete APIs zu ermitteln. So haben Unternehmen die Möglichkeiten sicherer Datenspeicherung, einer erweiterten Bedrohungsanalyse und sofortiger Warnungen bei potenziellen Exploits.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Kontinuierliche Überwachung des freigegebenen API-Traffics, der durch Ihre Umgebungen fließt, einschließlich North-South-API-Endpunkten, die öffentlich zugängliche APIs und interne East-West-API-Endpunkte ansprechen
- Identifizieren von Shadow-API-Endpunkten, die Umgebungen auf niedriger Ebene (z. B. Test- und Staging-Umgebungen) oder nicht dokumentierte und/oder veraltete API-Versionen offenlegen können
- Erstellung eines aktuellen API-Inventars auf der Grundlage von Risikobewertung und Datenklassifizierung
- Generieren von Warnungen zu einer Vielzahl potenzieller Angriffe, von Datenextraktion oder Datenmanipulation bis hin zu verdächtigen Zugriffsversuchen an diesen sensiblen API-Endpunkten

API10:2023 – Unsichere Nutzung von APIs

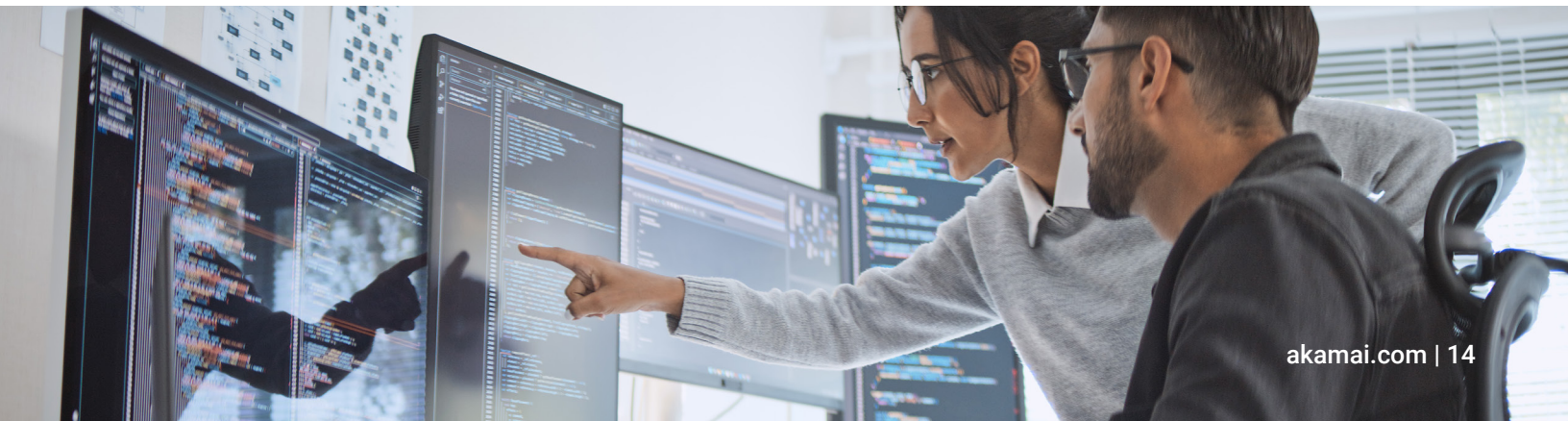
Unsichere Nutzung von APIs bezieht sich auf die Risiken, die mit der Verwendung von Drittanbieter-APIs verbunden sind, wenn keine angemessenen Sicherheitsmaßnahmen ergriffen werden. Unternehmen sind zunehmend auf Drittanbieter-APIs angewiesen, um Services und Funktionen zu erweitern. Daher werden diese APIs oft standardmäßig als vertrauenswürdig eingestuft. Dies kann zu erheblichen Sicherheitslücken führen. Wenn Unternehmen nicht die richtige Verschlüsselung, Datenvalidierung und -bereinigung implementieren und die Ressourcennutzung nicht begrenzen, setzen sie sich erheblichen Sicherheitsrisiken aus. Um diese Risiken zu mindern, können Unternehmen Verschlüsselung für alle über das Netzwerk übertragenen Daten implementieren, alle Dateneingaben validieren und bereinigen und angemessene Grenzen für die Ressourcennutzung festlegen.

Wie Akamai Sie unterstützen kann

Halten Sie Ihre Systeme ständig geschützt, indem Sie mit den Überwachungs-, Warn- und Beratungsdiensten von Akamai Ihre Services überwachen und validieren, um die Sicherheit zu gewährleisten.

Akamai verringert dieses Risiko durch die folgenden Maßnahmen:

- Kontinuierliche Überwachung des gesamten gefährdeten API-Traffics, der durch Ihre Umgebungen fließt, einschließlich East-West- und ausgehenden APIs, die B2B- und/oder Drittanbieterintegrationen erleichtern
- Generieren von Warnungen zu einer Vielzahl potenzieller Angriffe, von Datenextraktion oder Datenmanipulation bis hin zu verdächtigen Zugriffsversuchen an diesen sensiblen API-Endpunkten
- Schutz von Webanwendungen und APIs durch Anwendung entsprechender Schutzrichtlinien, die auf eine Vielzahl von in Angriffsgruppen erfassten API-Angriffen abzielen



Weitere Sicherheitsrisiken laut OWASP

Die OWASP Top 10 API-Sicherheitsrisiken von 2023 waren die erste größere Aktualisierung der Liste der gemeinnützigen Organisation seit 2019. Es lohnt sich jedoch, auf die ursprüngliche Liste zurückzublicken, in der zusätzliche Sicherheitsrisiken wie Injektionsangriffe erörtert werden, die in der heutigen Landschaft immer noch relevant sind.

Akamai kann dieses Sicherheitsrisiko durch die folgenden Maßnahmen minimieren:

- Identifizieren von Injection-anfälligen Endpunkten und Injection-Versuchen durch Abgleich von Signaturen und Erkennung von Anomalien
- Anwendung von Sicherheitsrichtlinien durch JSON- und XML-Prüfung von API-Anfragen und Untersuchung auf verschiedenste Injection-Angriffe wie SQLi, XSS, CMDi, RFI und LFI
- Generieren von Warnungen zu Injection-Exploits

OWASP hat zudem weitere Top-10-Listen zu Sicherheitsrisiken veröffentlicht, wie z. B. die OWASP Top 10 Web Application Security Risks. Das Sicherheitsportfolio von Akamai kann auch zur Minimierung dieser Sicherheitsrisiken beitragen.

Wir helfen Ihnen gerne!

Unternehmen und ihre Sicherheitsanbieter müssen eng zusammenarbeiten und Menschen, Prozesse und Technologien zusammenbringen, um effektiven Schutz vor den in den OWASP Top 10 beschriebenen API-Sicherheitsrisiken zu gewährleisten.

Akamai bietet branchenführende Sicherheitslösungen, erfahrene Experten und eine Plattform, die jeden Tag Einblicke aus Millionen von Angriffen auf Webanwendungen und APIs, Milliarden von Bot-Anfragen und bis zu Billionen von API-Anfragen bereitstellt.

Die Sicherheitslösungen für Webanwendungen und APIs von Akamai schützen Ihr Unternehmen vor den fortschrittlichsten Formen von Webanwendungs-, DDoS- und API-basierten Angriffen. Darüber hinaus bietet der Akamai Managed Security Service Überwachung rund um die Uhr, Sicherheitsmanagement und Bedrohungsabwehr.

Weitere Informationen zum Sicherheitsportfolio von Akamai finden Sie auf unserer Website. Wenn Sie mehr darüber erfahren möchten, wie wir als Partner den bestmöglichen Schutz für Ihr Unternehmen bereitstellen können, wenden Sie sich noch heute an Ihren Akamai-Vertriebsmitarbeiter.

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.