WEBANWENDUNGS- UND API-SCHUTZFUNKTIONEN:

Eine Checkliste für Finanzunternehmen

Programmierschnittstellen (APIs) haben ein enormes Potenzial und die Fähigkeit, Verbindungen zwischen verschiedenen Geräten, Anwendungen und Daten zu unterstützen. Sie sind die Technologie, auf die sich immer mehr interne und externe Bankstrategien und -aktivitäten stützen. Sie verheißen mehr Offenheit für mehr Wettbewerb zum Vorteil der Kunden. Dennoch hat das rasante Wachstum von APIs im Finanzdienstleistungssektor die Angriffsfläche vergrößert und neue Sicherheitsrisiken mit sich gebracht.

Mit einer Sicherheitslösung für Webanwendungen und APIs bei der Planung, Implementierung oder Optimierung Ihrer Informationssicherheitsstrategie kann Ihr Unternehmen besondere Risiken erkennen, Sicherheitslücken schließen und Bedrohungen identifizieren. Um wettbewerbsfähig zu bleiben, benötigen Finanzinstitute eine WAAP-Lösung (Web Application and API Protection), die kontinuierliche Transparenz mit umfassenden Erkenntnissen bietet und die anspruchsvollsten Angriffe erkennen und stoppen kann.

Diese Checklisten können zur Bewertung der Anbieterfunktionen oder als Anforderungsliste zur Implementierung einer effektiven WAAP-Lösung verwendet werden.

01. ANFORDERUNGEN AN DIE PLATTFORM

02. ADAPTIVER WEBANWENDUNGS- UND DDoS-SCHUTZ

03. API-TRANSPARENZ, -SCHUTZ UND -KONTROLLE

04. FLEXIBLE VERWALTUNG

01 ANFORDERUNGEN AN DIE PLATTFORM

- Skalierbarkeit, um den Anforderungen des Traffics gerecht zu werden und kontinuierlichen Schutz ohne Performance-Einbußen zu bieten
- Architektur, die die Herausforderungen geografisch verteilter Anwendungen bewältigen kann
- Audit-Protokollfunktionen zur Sicherstellung der ordnungsgemäßen Nutzung
- Schutz von Website-Ursprüngen vor Ort sowie in privaten oder Public Clouds (einschließlich Multi-Cloud- oder Hybrid-Cloud-Umgebungen)
- DDoS-Abwehr (Distributed Denial of Service) auf Netzwerkebene [L3/4] mit einem Service-Level Agreement von null Sekunden
- Transparenz hinsichtlich der Angreifer, der Häufigkeit von Angriffen und der Schwere von Angriffen durch Crowdsourcing-Angriffsinformationen auf der gesamten Plattform
- Reverse-Proxy mit Webtraffic über die Ports 80 und 443
- Schutz der Netzwerkprivatsphäre durch SSL/TLS-Verschlüsselung
- Ist laut einem unparteiischen Drittanbieter seit mindestens 5 Jahren ein Marktführer in der Lösungskategorie
- Automatische Erkennung und Warnung, wann und wo personenbezogene Daten (PII) weitergegeben werden, um Datenlecks zu verhindern

Finanzinstitute sind dafür verantwortlich, vertrauliche Kunden- und Finanzdaten vor sich schnell entwickelnden Sicherheitsbedrohungen zu schützen. Um reagieren zu können, sollte Ihre Sicherheitslösung für Webanwendungen flexibel, skalierbar und einfach zu verwalten sein.

ADAPTIVER WEBANWENDUNGS- UND DDoS-SCHUTZ 02

Die Sicherheit der Webanwendungen muss über die herkömmliche signaturbasierte Erkennung hinausgehen und auf fortschrittlichere Formen eines adaptiven Webanwendungs- und DDoS-Schutzes zurückgreifen, um die genauesten und zuverlässigsten Sicherheitsergebnisse zu erzielen.

- Erkennung über signaturbasierte Angriffe hinaus mit Anomaliebewertung und risikobasierter Bewertung
- Vollständig verwaltete WAF-Regeln, um die Notwendigkeit kontinuierlicher Konfiguration und von Updates zu reduzieren
- Bewertung der Kundenreputation und Informationen für individuelle oder freigegebene IP-Adressen
- Maschinelles Lernen, Data Mining und heuristikgesteuerte Erkennungsfunktionen zur Identifizierung sich schnell entwickelnder Bedrohungen
- Automatische Updates der WAF-Regeln (Web Application Firewall) mit kontinuierlichen Bedrohungsinformationen von Sicherheitsexperten in Echtzeit
- Möglichkeit, neue oder aktualisierte WAF-Regeln mit Live-Traffic vor der Implementierung in der Produktion zu testen
- Schutz gegen (mindestens) SQL Injection, XSS, File Inclusion, Command Injection, SSRF, SSI und XXE
- Vollständig anpassbare vordefinierte Regeln, um spezifische Kundenanforderungen zu erfüllen
- Schutz vor volumetrischen DoS-Angriffen auf Anwendungsebene [L7], die darauf ausgelegt sind, Webserver mit rekursiven Anwendungsaktivitäten zu überlasten
- Nutzerdefinierte Regeln zum schnellen Schutz vor bestimmten Trafficmustern (virtuelles Patching)
- Anfrageratenbegrenzungen zum Schutz gegen automatisierten oder übermäßigen Bot-Traffic
- Schutz vor Direct-to-Origin-Angriffen
- IP-/Geo-Kontrollen über mehrere Netzwerklisten, um Traffic von bestimmten IPs, Subnetzen oder geografischen Regionen zu blockieren oder zuzulassen
- Schutz vor automatisierten Clients, wie z. B. Schwachstellen-Scans und Webangriffs-Tools

03

API-TRANSPARENZ, -SCHUTZ UND -KONTROLLE

- Automatische Erkennung und Profilerstellung von unbekannten und/oder sich ändernden APIs (einschließlich API-Endpunkte, -Eigenschaften und -Definitionen)
- Automatische Prüfung von XML- und JSON-Anfragen zur Erkennung API-basierter Angriffe
- Ratensteuerung (Drosselung) für API-Endpunkte basierend auf API-Schlüsseln
- API-Netzwerklisten (Zulassungslisten/ Sperrlisten) basierend auf IP/Geografie
- API-Lebenszyklusmanagement mit Versionierung
- Nutzerdefinierte API-Inspektionsregeln zur Erfüllung spezifischer Nutzeranforderungen
- Sichere Authentifizierung und Autorisierung über JWT-Validierung (JSON Web Token)
- Möglichkeit, zulässige XML- und JSON-Objektformate vorzudefinieren, die Größe, Typ und Tiefe von API-Anfragen einschränken
- Schutz von API-Backend-Infrastrukturen vor langsamen und unauffälligen Angriffen, die Ressourcen auslasten sollen (z. B. Slow Post, Slow Get)
- Definition zulässiger API-Anfragen nach Schlüssel (Quote für jeden Schlüssel unabhängig definiert) für die volle Kontrolle über den Verbrauch
- API-Onboarding mit Standard-API-Definitionen (Swagger/OAS und RAML)

API-Schutz ist zu einem wichtigen Bestandteil der Sicherheit von Webanwendungen geworden. Sie benötigen eine WAAP-Lösung mit zuverlässigen API-Erkennungs-, Schutz- und Steuerfunktionen, um API-Schwachstellen zu reduzieren und Ihre Angriffsfläche zu verringern.

FLEXIBLE VERWALTUNG 04

- Offene APIs und CLI, um Sicherheitskonfigurationsaufgaben in CI-/CD-Prozesse zu integrieren
- Echtzeit-Dashboards, Reporting und heuristikgesteuerte Warnfunktionen
- Integration in lokale und cloudbasierte SIEM-Anwendungen (Security Information and Event Management)
- Zentrale Nutzeroberfläche (UI) für den Zugriff auf detaillierte Telemetriedaten zu Angriffen und Analysedaten zu Sicherheitsereignissen
- Vollständige Staging-Umgebung und die Möglichkeit, eine Änderungskontrolle zu implementieren
- Selbstoptimierende Sicherheitsschutzmaßnahmen, die sich automatisch an Ihren Traffic anpassen
- Vollständig verwalteter Sicherheitsservice zur Auslagerung oder Ergänzung von Sicherheitsverwaltung, Überwachung und Bedrohungsabwehr

Sie benötigen einfache und automatisierte Workflows, um Ihre Investition optimal zu nutzen und die betriebliche Effizienz zu verbessern. Ganz gleich ob Sie neue oder sich ändernde Anwendungen schützen, neue WAF-Regeln übernehmen oder den Schutz von APIs erweitern möchten: Der Prozess muss nahtlos und intuitiv sein.

Akamai bietet den weltweit führenden Finanzinstituten Webanwendungs- und API-Schutz. Unser globales Sicherheitsteam hat täglich Einblick in Millionen von Angriffen auf Webanwendungen, Milliarden von Bot-Anfragen und Billionen von API-Anfragen. Mithilfe dieser Einblicke, kombiniert mit fortschrittlichem maschinellen Lernen und Bedrohungsforschung, können wir uns ständig verbessern, neue Bedrohungen erkennen und innovative Funktionen entwickeln.

Die Sicherheitslösungen für Webanwendungen und APIs von Akamai schützen Finanzinstitute vor den fortschrittlichsten Formen von Webanwendungs-, DDoS- und API-basierten Angriffen. Bleiben Sie auf dem Laufenden über unsere neuesten Forschungsergebnisse, indem Sie unseren Security Hub besuchen.

Akamai

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Mithilfe der am meisten verteilten Computing-Plattform – von der Cloud bis zur Edge – ermöglichen wir es unseren Kunden, Anwendungen zu entwickeln und auszuführen. So bleiben die Erlebnisse nahe beim Nutzer und Bedrohungen werden ferngehalten. Möchten Sie mehr über die Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com/de und akamai.com/de/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn.