AKAMAI-CHECKLISTE

Checkliste für Webanwendungs- und API-Schutzfunktionen

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. Sie benötigen eine WAAP-Lösung (Web Application and API Protection), die kontinuierliche Transparenz mit umfassenden Erkenntnissen bietet und die anspruchsvollsten Angriffe erkennen und stoppen kann.

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

Kategorie 1: Anforderungen an die Plattform

Unternehmen gibt es in allen Formen und Größen und mit unterschiedlichen Anforderungen. Ihre Sicherheitslösung für Webanwendungen sollte flexibel, skalierbar und einfach zu verwalten sein.

- [ ] 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 Multicloud- 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

Kategorie 2: Adaptiver Webanwendungs- und DDoS-Schutz

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

- [ ] Erkennung über signaturbasierte Angriffe hinaus mit Anomaliebewertung und risikobasierter Bewertung
- [ ] 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 (Denial of Service) auf Anwendungsebene [L7], die darauf ausgelegt sind, Webserver mit rekursiven Anwendungsaktivitäten zu überlasten
- [ ] 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
- [ ] 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

Kategorie 3: API-Transparenz, -Schutz und -Kontrolle

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

- [ ] Automatische Erkennung und Profilerstellung von unbekannten und/oder sich ändernden APIs (einschließlich API-Endpunkte, -Eigenschaften und -Definitionen)
- [ ] Automatische Prüfung von XML- und JSON-Anforderungen zur Erkennung API-basierter Angriffe
- [ ] Nutzerdefinierte API-Inspektionsregeln zur Erfüllung spezifischer Nutzeranforderungen
- [ ] Möglichkeit, zulässige XML- und JSON-Formate 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)
- [ ] Echtzeitwarnungen, Berichte und Dashboards auf API-Ebene
- [ ] Ratensteuerung (Drosselung) für API-Endpunkte basierend auf API-Schlüsseln
- [ ] API-Netzwerklisten (Zulassungslisten/Sperrlisten) basierend auf IP/Geografie
- [ ] API-Lebenszyklusmanagement mit Versionierung
- [ ] Sichere Authentifizierung und Autorisierung über JWT-Validierung (JSON Web Token)
- [ ] 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)

Kategorie 4: Flexible Verwaltung

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.

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

Die Akamai Connected Cloud stellt jeden Tag Einblicke aus Millionen von Angriffen auf Webanwendungen, Milliarden von Bot-Anfragen und Billionen von API-Anfragen bereit. Mithilfe dieser Einblicke, kombiniert mit fortschrittlichem maschinellen Lernen und Bedrohungsforschung, können wir uns ständig verbessern, neue Bedrohungen erkennen und innovative Funktionen entwickeln.

Weitere Informationen erhalten Sie unter akamai.com oder vom Vertriebsteam von Akamai.

 | Support-Website | | Veröffentlicht: 10/23