Die ultimative Checkliste zur WAF-Bewertung

Ein Hilfsmittel, das Sie dabei unterstützt, die richtige Lösung für Ihre Anwendungs- und API-Sicherheitsanforderungen zu finden

Vereinfachen Sie Ihre Suche nach der passenden Web Application Firewall (WAF) oder dem passenden WAAP-Anbieter (Web Application and API Protection). Verwenden Sie diese umfassende Checkliste, um WAFs und WAAP-Anbieter zu bewerten und sicherzustellen, dass die Lösung Ihren Sicherheits-, Performance-, Finanz- und Betriebsanforderungen entspricht.

Sicherheitsfunktionen

Anwendungssicherheit

- Gewährleisten Sie **Schutz gegen die OWASP Top 10-Schwachstellen**, wie etwa SQL-Injection, XSS, LFI und SSRF. Stellen Sie sicher, dass die Schutzmechanismen angepasst und automatisch bereitgestellt werden können.
- Prüfen Sie, ob Ihre Lösung den Traffic von **IPs mit schlechter Reputation** proaktiv kontrolliert und warnt, wenn eine frühere **Ausnahme missbraucht wird**.
- Bewerten Sie die **Flexibilität von Zulassungs- und Sperrlisten** – können Sie Attribute wie IP, Geo, ASN und TLS-Fingerabdrücke zuordnen, um effektive Richtlinien zu erstellen?

DDoS-Schutz

- Prüfen Sie, ob der Anbieter **mehrschichtigen DDoS-Schutz** für Anwendungen und APIs bietet, einschließlich dem Schutz vor DNS sowie Angriffen auf Layer 3, 4 und 7.
- Stellen Sie sicher, dass die Lösung eine **verhaltensbasierte DDoS-Erkennung** zum Schutz von Anwendungen bietet.
- Bestimmen Sie die Granularität der **Ratenbeschränkungskontrollen**. Werden sie automatisch oder manuell konfiguriert? Können diese Maßnahmen sowohl vor volumetrischen als auch vor Slow-Post-Angriffen schützen?
- Überprüfen Sie die Funktionen, die bei DDoS-Angriffen die **Belastung reduzieren** und die Performance verbessern.
- Informieren Sie sich über potenzielle **Zusatzkosten** durch erhöhten Traffic bei DDoS-Ereignissen.
- Setzen Sie auf **automatisierten L7-DDoS-Schutz**, um Ihrem Team Zeit und Schulungen zu sparen. Können Sie die **Schutzvorrichtungen anpassen**, damit sie Ihrem spezifischen Traffic-Profil oder Ihrer Risikotoleranz entsprechen?

Zero-Day-Exploit-Schutz

- Stellen Sie sicher, dass die WAF über einen **bestehenden Schutz vor bekannten CVEs** verfügt und sich schnell anpassen kann, um neue Zero-Day-Exploits abzuwehren. Überprüfen Sie die **Erfolgsbilanz bei der Zero-Day-Abwehr** und die Reaktionszeiten der Lösung.
- Stellen Sie fest, ob Sie als Kunde über **Schutzmechanismen gegen bestimmte CVEs** verfügen.

API-Schutz

- Stellen Sie sicher, dass die Lösung **API-Endpunkte schützt**, insbesondere vor Injection-Angriffen, DoS und Verstößen gegen Spezifikationen.
- Prüfen Sie die **API-Erkennung** – kann die Lösung neue und modifizierte APIs automatisch erkennen? Wie einfach können Sie Schutzmechanismen anwenden?
- Stellen Sie die **Erkennung von personenbezogenen Daten und entsprechende Warnungen** sicher, um vertrauliche Daten zu schützen und Datenschutzverletzungen zu verhindern.

Bot-Schutz

- Bestätigen Sie, ob die WAF durch das Verwenden eines Bot-Verzeichnisses und von Bot-Definitionen **automatisierte Bedrohungen erkennt und abwehrt**. Wie umfangreich ist das Bot-Verzeichnis? Wie oft wird es mit neuen und geänderten Bots aktualisiert?
- Bestimmen Sie, welche **Bot-Definitionen** im Tool vorhanden sind. Können Sie **eigene Bot-Definitionen erstellen**?
- Überprüfen Sie, ob die Lösung über **CAPTCHA oder einen menschlichen Verifizierungsmechanismus verfügt**, der das Nutzererlebnis nicht beeinträchtigt. Müssen Ihre Endnutzer mit CAPTCHA/der Verifizierung interagieren, bevor sie fortfahren können?

Threat Intelligence und Automatisierung

Threat Intelligence

- Stellen Sie sicher, dass der Anbieter **Daten aus erster Hand** für die Threat Intelligence nutzt, um Verzögerungen durch Dritte und potenzielle Datenmanipulationen zu vermeiden.
- Verifizieren Sie die Größe des **Threat-Hunting-Teams** des Anbieters und des globalen Netzwerks von Sicherheitsexperten, die neue Risiken überwachen.
- Bewerten Sie den **Umfang und die Relevanz der Daten** der Threat-Intelligence-Datenbank. Umfasst sie Daten aus Branchen, die Ihrer ähnlich sind, oder aus Unternehmen, die häufig von Cyberangriffen betroffen sind?

Automatisierung

- Überprüfen Sie, ob die WAF auf **veralteter Regelwerktechnologie** beruht. Verwendet sie fortschrittliche, zeitgemäße Technologien wie automatisierte Updates über fortschrittliche Heuristik und maschinelles Lernen?
- Stellen Sie sicher, dass Regelwerke automatisch aktualisiert werden, um **manuelle Eingriffe zu vermeiden**. Erfolgen automatische Aktualisierungen auf globaler Ebene? Welche Optionen haben Sie, um ein zuvor installiertes Update zu entfernen oder **es mit Live-Traffic zu testen**?
- Stellen Sie fest, ob die Lösung die Schutzmechanismen ohne manuelle Eingriffe an Ihre Umgebung anpasst. Kann die Lösung die Sicherheitsrichtlinien kontinuierlich auf der Grundlage des Live-Traffic-Profils Ihres Unternehmens **selbst optimieren**?
- Bewerten Sie, wie die Lösung **False Positives** reduziert. Wie findet die Lösung eine Balance zwischen dem Reduzieren von False Positives und der **Störung von legitimem Traffic**?

Transparenz und Reporting

Umfassende Transparenz

- Stellen Sie sicher, dass die WAF mit anpassbaren Dashboards und Berichten, die Umgebungen mit mehreren Lösungen abdecken, **detaillierte Transparenz im Bezug auf Bedrohungen** und Performance bietet.
- Beim Betrieb einer WAF verbringen Sicherheitsteams die meiste Zeit in der Datenkonsole. Informieren Sie sich über die **Anpassungen**, proaktive Analysefunktionen und **die Granularität der Berichte**, auf die Sie zugreifen können.
- Bewerten Sie die Fähigkeit der Lösung, zur effektiven **Überwachung von API-Traffic** und Anwendungstraffic, zum Erkennen von Missbrauch und zur Bereitstellung detaillierter Einblicke in die Ausbreitung von APIs.

Echtzeitwarnungen und proaktive Analysen

- Prüfen Sie, ob **Warnfunktionen in nahezu Echtzeit** vorhanden sind, die Ihr Team über kritische Bedrohungen informieren. Warnmeldungen sollten auf Grundlage bestimmter Kriterien wie Schweregrad, Quelle oder Angriffsart angepasst werden können, damit sie leichter verständlich sind und eine schnelle Reaktion erfolgen kann.
- Achten Sie darauf, dass die Lösung **vorab analysierte Einblicke** über den Ort, den Zeitpunkt und die Art des Angriffs liefert, um die Belastung Ihres Sicherheitsteams zu verringern. Die Lösung sollte auch **die nächsten Schritte** zur Verbesserung Ihrer Sicherheitsstrategie empfehlen.

Plattform und Architektur

Globale Reichweite

- Prüfen Sie, ob die WAF Zugriff auf eine globale Edge oder Netzwerk- und Inhaltsbereitstellungsservices bietet, um die Performance und Sicherheit zu verbessern. Informieren Sie sich über die **globale Verfügbarkeit der Lösung**, um die Abdeckung Ihrer primären Standorte und die primären Standorte Ihrer Kunden sicherzustellen.

Cloud- und Hybrid-Unterstützung

- Stellen Sie sicher, dass die Lösung **cloudunabhängig** ist und Ihre Multi-Cloud-, Hybrid- und lokalen Umgebungen unterstützt. Wenn die Lösung auf CDN basiert, stellen Sie sicher, dass sich der Schutz über die Netzwerk- und Inhaltsbereitstellung hinaus erweitern lässt, um Sicherheit auch außerhalb der Edge zu gewährleisten.

Resilienz und Failover

- Bewerten Sie die **Resilienz der Lösung** – kann automatisch ein Failover-Prozess ausgelöst werden, um bei Ausfällen oder Unterbrechungen die Schutzmechanismen aufrechtzuerhalten?
- Überprüfen Sie die **letzten Serviceunterbrechungen und Vorfallsreaktionen** des Anbieters.
- Stellen sie fest, ob die **Service Level Agreements** (SLAs) Ihren Geschäftsanforderungen entsprechen.

Support und Managed Services

Enthaltener Support und Zugriff auf Services

- Bestimmen Sie das **Maß an Support, das in der WAF-Lösung inbegriffen** oder gegen einen Aufpreis verfügbar ist.
- Prüfen Sie, ob **rund um die Uhr Vorfallsreaktion** verfügbar ist und ob Sie während Angriffen direkten Zugriff auf das Security Operations Center (SOC) haben.
- Stellen Sie sicher, dass der Anbieter **vollständig verwaltete Sicherheitsservices** anbietet, um potenzielle Lücken in Ihren internen Ressourcen, einschließlich Fachleute für den Umgang mit Angriffen, Konfiguration oder Personalfluktuation, zu schließen.

Integration und DevSecOps-Kompatibilität

APIs, CLI und Infrastrukturautomatisierung

- Prüfen Sie auf die Integration von **APIs, CLI und Terraform**, um Sicherheitsmechanismen zu automatisieren und in Ihre Entwicklungs-Workflows einzubetten. Die Unterstützung von GitOps und anderen Infrastructure-as-Code-Frameworks ist für eine konsistente Durchsetzung der Sicherheitsrichtlinien in allen Umgebungen entscheidend.

SIEM-Integration

- Stellen Sie sicher, dass die WAF **nahtlos in SIEM-Tools** wie Splunk oder QRadar integriert werden kann, um die Überwachung, Berichterstellung und Vorfallsreaktion zu verbessern.

Geschäftsergebnisse und Effizienz

Skalierbarkeit und Performance

- Stellen Sie sicher, dass die Lösung **automatisch skaliert werden kann**, um große Datenmengen ohne Performanceeinbußen zu verarbeiten. An welchem Punkt verursacht die Lösung Latenzen oder wird bei hoher Belastung anfällig?
- Stellen Sie sicher, dass ein SLA für **100 % Verfügbarkeit** besteht, und prüfen, ob die Lösung auch Maßnahmen zur Verbesserung der Performance wie Caching und die Beschleunigung von Traffic bietet, um Ihre Anwendungen zu verbessern.

Einheitliche Verwaltung

- Überprüfen Sie, ob der Anbieter eine zentrale Schnittstelle zur **Verwaltung von Sicherheitsrichtlinien in allen Umgebungen** – Cloud, lokal und hybrid – bietet. Stellen Sie sicher, dass die Lösung in Ihren aktuellen Stack integriert werden kann und sowohl dem Sicherheits- als auch dem Entwicklungsteam ein reibungsloses Nutzererlebnis bietet.

Kosteneffizienz

- Bewerten Sie die Fähigkeit der Lösung zur **Vereinheitlichung von WAF, DDoS, Bot-Management und API-Schutz** unter einem einzigen Anbieter, um die Komplexität und Verwaltungskosten zu reduzieren. Bewerten Sie das Gleichgewicht zwischen Sicherheitseffizienz und Betriebskosten, um den Gesamtwert zu ermitteln.

Vertrauen und Zuverlässigkeit des Anbieters

Service und Stabilität in der Vergangenheit

- Überprüfen Sie die **Ausfälle und Serviceunterbrechungen des Anbieters** in den letzten 5 Jahren.
- Prüfen Sie die **finanzielle Stabilität** des Unternehmens. Ist es profitabel? Wie lange ist es schon aktiv? Welche Kundengrößen und -arten bedient es?

Ruf und Bewertungen

- Suchen Sie nach verifizierten Rezensionen und Kundenbewertungen, um zu sehen, ob ähnliche Unternehmen in Ihrer Branche **dem Anbieter vertrauen**. Stimmen die Anwendungsfälle aktueller Kunden mit Ihren Anforderungen überein?
- Prüfen Sie, ob das Unternehmen für seine Anwendungs- und API-Schutzlösungen **von Branchenanalysten anerkannt wird** (z. B. Gartner und Forrester).
- Stellen Sie sicher, dass Sie nach Gesprächen mit dem Anbieter von seiner Reaktionsfähigkeit und seinem Kundensupport bei Problemen **überzeugt sind**. Fragen Sie nach, wer Sie nach dem ersten Onboarding betreut.