LINK11

WEB APPLICATION API PROTECTION BUYER'S GUIDE

Wie man die richtige Sicherheitslösung für Webanwendungen auswählt

www.link11.com

Unternehmen passen ihre digitalen Infrastrukturen an das sich verändernde globale Umfeld an. Bei Investitionen in die Infrastruktur müssen sie auch die Sicherheit ihrer Webanwendungen berücksichtigen.

Da Workloads, Anwendungen, Dienste und Daten von Unternehmen zunehmend auf offenen Internetplattformen verfügbar sind, ist die Investition in eine robuste Sicherheitslösung für Webapplikationen entscheidender denn je. Der richtige Service sollte nicht nur vor den heutigen unaufhaltsamen und sich ständig weiterentwickelnden Bedrohungen schützen, sondern auch die Herausforderungen von morgen vorhersehen und sich an sie anpassen. Es ist heute wichtiger denn je, in eine Sicherheitslösung für Webapplikationen zu investieren, die einen angemessenen Schutz vor den fortschrittlichen und aggressiven Bedrohungen von heute bietet.

In diesem Leitfaden werden bewährte Verfahren zur Bewertung von Schutzoptionen für Webapplikationen und zur Auswahl einer Lösung vorgestellt, die einen ganzheitlichen Ansatz zur Sicherung Ihrer Webanwendungen bietet, sich an Ihre Geschäftsanforderungen und neu auftretende Bedrohungen anpasst.

Wichtige Kriterien, die es bei der Bewertung von Sicherheitslösungen für Webanwendungen zu berücksichtigen gilt:

1. Sicherheitsabdeckung und Umfang
2. Bot-Protection und Einblicke in den Datenverkehr
3. Effektivität und Ausgereiftheit
4. Einheitliche Lösung für alle WAAP-Säulen
5. Vereinfachung der Sicherheit durch Managed Services

1. SICHERHEITSABDECKUNG UND UMFANG DER LÖSUNG

Auf dem Markt ist eine Vielzahl von Sicherheitslösungen für Webapplikationen erhältlich, die im Allgemeinen in drei Kategorien eingeteilt werden:

· Native Tools, die von Cloud-Service-Providern (CSPs) angeboten werden
· Produkte mit einem Schwerpunkt
· Einheitliche Plattformen

1. Native tools
Die integrierten CSP-Tools sind einfach zu integrieren und zu verwenden. Sie eignen sich jedoch nicht gut für den Schutz von Webanwendungen, die auf verschiedenen Cloud-Plattformen gehostet werden, und Unternehmen können auch mit Risiken der Anbieterabhängigkeit konfrontiert sein. Sie bieten zwar einige Sicherheitsmaßnahmen, aber keinen umfassenden Schutz, da sie im Vergleich zu Services spezialisierter Sicherheitsanbieter nur über eine begrenzte Tiefe und Funktionalität verfügen.

2. Single-Focus-Produkte:
Eigenständige Sicherheitsprodukte wie Web Application Firewalls (WAFs) bieten umfassendere Funktionen als CSP-Tools, decken jedoch nur bestimmte Aspekte der Sicherheit von Webapplikationen ab. Organisationen müssen mehrere Lösungen von verschiedenen Anbietern integrieren, um die Vielzahl von Bedrohungen zu mindern, was die Komplexität, den Verwaltungsaufwand und die Interoperabilität erhöht.

3. Einheitliche Plattformen:
Viele Plattformen behaupten zwar, vollständige Sicherheit zu bieten, werden jedoch häufig als gebündelte Dienste mit zusätzlichen Kosten für wesentliche Funktionen wie Modul-Upgrades, Feeds für erweiterte Bedrohungsinformationen, zusätzliche Subdomains und SSL-Zertifikate verkauft. Unternehmen zahlen am Ende mehr als nötig, wenn sie eine vermeintlich kostengünstigere Lösung kaufen.

Für einen umfassenden Schutz in der heutigen Bedrohungslandschaft ist eine einheitliche Lösung unerlässlich.
Um sich effektiv gegen sich ständig weiterentwickelnden Cyber-Bedrohungen zu schützen, benötigen Unternehmen eine umfassende, flexible Sicherheitsplattform für Webapplikationen, die durchgängige Sicherheit bietet. Dazu gehören eine Next-Generation-WAF, Multi-Layer-DDoS-Protection, Bot-Management, API-Security, Verhinderung von Account Takeover (ATO) und weitere wichtige Abwehrmaßnahmen.

Eine effektive Sicherheitslösung für Webanwendungen sollte Folgendes bieten:

Umfassender Schutz – Schutz vor dem gesamten Spektrum moderner Web-Bedrohungen, der eine robuste Absicherung gegen alle Angriffsvektoren gewährleistet.

Eine einheitliche WAAP-Plattform – Eine vollständig integrierte Komplettlösung, die alle Säulen von Web Application and API Protection (WAAP) abdeckt und das Sicherheitsmanagement vereinfacht.

Reduzierte Komplexität – Eine zentralisierte Plattform zur Verwaltung aller Sicherheitskontrollen, die Abläufe optimiert und den Verwaltungsaufwand minimiert.

Detaillierte Richtlinienkontrolle – Fein abgestimmte Sicherheitsrichtlinien, die eine präzise Bedrohungsabwehr ermöglichen und Fehlalarme und Fehlmeldungen reduzieren.

2. BOT-PROTECTION UND EINBLICKE IN DEN DATENVERKEHR

Bots spielen bei den meisten Webangriffen eine Rolle, und die Bedrohungsakteure entwickeln ständig neue Wege, um einer Identifizierung zu entgehen. Organisationen benötigen eine zuverlässige Methode, um feindliche Bots auf ihren Websites, in ihren Anwendungen und APIs zu erkennen und zu blockieren. Daher ist das Filtern bösartiger Bots aus eingehendem Datenverkehr ein entscheidender Bestandteil moderner Sicherheit.

Zu den traditionellen Techniken zur Eindämmung von Bot-Angriffen gehören:

- Signaturerkennung
- Ratenbegrenzung
- Blacklisting
- JavaScript-Injektion und Cookie-Handling
- CAPTCHA- und reCAPTCHA-Herausforderungen

Diese Methoden sind gegen ältere Bots wirksam. Fortgeschrittene, KI-gesteuerte Bots sind darauf ausgelegt, herkömmliche Sicherheitsmaßnahmen zu umgehen und unentdeckt zu bleiben.

Diese Bots nutzen eine Vielzahl von Umgehungstechniken, darunter:

- **Spoofing von User-Agent-Strings** und täuschenden Verhaltensweisen, um legitime menschliche Benutzer zu imitieren.
- **Ausführung langsamer Angriffe**, die von Standardtechniken zur Ratenbegrenzung unentdeckt bleiben.
- **Verwendung von Headless Browsern**, um echte Benutzerumgebungen zu simulieren, einschließlich der Handhabung von Cookies, und der Ausführung von JavaScript.
- **Automatisches Lösen von CAPTCHA-Aufgaben**, wodurch diese unwirksam werden.
- **Nachahmung von mobilen Anwendungen,** wodurch herkömmliche Sicherheitsmethoden für den mobilen Datenverkehr wirkungslos werden.

Suchen Sie nach einer Lösung, die Technologien zur Erkennung von Bots der neuesten Generation beinhaltet. Dazu gehören:

1. **Erweiterte Browser-Verifizierung** - Erkennt Headless-Umgebungen und Automatisierungstools mithilfe biometrischer Analysen, Client-Zertifizierungsmechanismen und anderer Techniken, um zu überprüfen, ob eingehende Anfragen von legitimen Quellen stammen.

2. **Interaktive und nicht interaktive Bot-Herausforderungen** - Erkennt selbst die ausgeklügeltsten Bots präzise und sorgt gleichzeitig für ein nahtloses Benutzererlebnis.

3. **Schutz vor Bedrohungen durch den mobilen Anwendungsverkehr** - Bietet Sicherheitsmaßnahmen, die speziell für den mobilen Anwendungsbereich (z. B. ein mobiles SDK) entwickelt wurden, bei dem herkömmliche browserbasierte Methoden zur Erkennung von Bedrohungen nicht anwendbar sind.

4. **Erweiterte Mechanismen zur Ratenbegrenzung** - Wertet mehrere Attribute aus, die über IP-Adressen hinausgehen, um Missbrauch zu erkennen und einzudämmen.

5. **Verhaltensanalyse** - Vergleicht die aktuelle Benutzeraktivität mit einer Baseline des legitimen Benutzerverhaltens.

6. **Client-Zertifizierungsmechanismen** - Verifiziert, dass eingehende Anfragen von legitimen Quellen stammen.

3. EFFEKTIVITÄT UND AUSGEREIFTHEIT

Viele Sicherheitslösungen für Webanwendungen zeigen nur blockierte Anfragen an und geben oft nur einen begrenzten Einblick in die Gründe, warum diese Anfragen abgelehnt wurden.

Während dieser Ansatz in einigen Fällen ausreichen mag, kann er bei Sicherheitsereignissen oder sogar bei normalem Datenverkehr problematisch sein, da Sie dann nur einen Teil der Vorgänge verstehen und entsprechend darauf reagieren können.

Beim Vergleich von Sicherheitslösungen für Webapplikationen wird ein wichtiger Aspekt oft übersehen: **die Transparenz des Datenverkehrs.**

Beim Vergleich von Web-Sicherheitslösungen wird ein wichtiger Aspekt oft übersehen: die Sichtbarkeit des Datenverkehrs.

In der komplexen Bedrohungslandschaft von heute ist eine vollständige Transparenz unerlässlich. Unternehmen benötigen vollen Zugriff auf jede eingehende Anfrage - egal, ob sie blockiert oder zugelassen wurde - sowie detaillierte Informationen über ihren Inhalt und Kontext.

Diese Transparenz stellt sicher, dass Sie verstehen, warum gewisse Entscheidungen getroffen wurden, Anomalien erkennen und Ihr System fein abstimmen können, um falsch-positive und falsch-negative Ergebnisse zu reduzieren. Im Laufe der Zeit erhöht dies die Präzision und Effektivität der Sicherheit Ihrer Webapplikationen.

Um vollständige Transparenz zu gewährleisten, muss eine Lösung für die Sicherheit von Webanwendungen Folgendes umfassen:

- Einsicht in den Inhalt und die Metadaten jeder HTTP/S-Anfrage.
- Klare Informationen darüber, was mit der Anfrage passiert ist und warum.
- Einfacher Zugang zu aktuellen und historischen Daten.
- Die Möglichkeit, anspruchsvolle Abfragen zu erstellen und Einblicke in historische Verkehrsmuster zu gewinnen.
- Echtzeiteinsicht in blockierte und weitergeleitete Anfragen.

4. EINHEITLICHE LÖSUNG FÜR ALLE WAAP-SÄULEN

Eine Web Application and API Protection (WAAP) kann entweder als integrierte Plattform angeboten werden, die mehrere Funktionen kombiniert, oder als individuelle, eigenständige Lösung.

Um einen umfassenden Schutz zu gewährleisten, muss eine robuste Sicherheitsstruktur die vier WAAP-Säulen umfassen:

1. **WAF (Web Application Firewall):** Schützt Webapplikationen durch Filterung und Überwachung des HTTP/S-Verkehrs.
2. **Web-DDoS-Schutz:** Schützt Webanwendungen vor Distributed Denial-of-Service (DDoS)-Angriffen.
3. **Bot-Verwaltung:** Identifiziert und entschärft bösartigen Bot-Verkehr und lässt legitime Bots passieren.
4. **API-Schutz:** Schützt APIs vor Bedrohungen wie unbefugtem Zugriff, Datendiebstahl, Injektionsangriffen, Input Fuzzing, Schwachstellen-Scans und ATO-Angriffen (Account Takeover).

Eigenständige Lösungen können bestimmte Anforderungen erfüllen, aber eine einheitliche Plattform, die alle WAAP-Säulen umfasst, bietet erhebliche Vorteile. Sie vereinfacht die Verwaltung, verringert die betriebliche Komplexität, gewährleistet eine nahtlose Integration zwischen den Komponenten und führt häufig zu einer besseren Gesamtleistung und Kosteneffizienz.

5. VEREINFACHUNG DER SICHERHEIT DURCH MANAGED SERVICES

Die Implementierung einer Sicherheitslösung für Webanwendungen ist keine einmalige Aufgabe, sondern erfordert eine kontinuierliche Verwaltung und Überwachung. Bei den Sicherheitslösungen gibt es eine ganze Reihe von Verwaltungsoptionen: von keiner, über kostenpflichtige Verwaltung und Support bis hin zu vollständig verwalteten Lösungen.

Es gibt jedoch einige Hindernisse, die eine effektive Konfiguration und Verwaltung dieser Lösungen erschweren:

Zeit:
Das Sicherheitsmanagement ist ein zeitaufwändiger Prozess. Neben der Erstimplementierung umfasst die laufende Wartung die Aktualisierung der Lösung, die Anpassung der Regeln und die Überwachung auf Anomalien.

Komplexität:
Die Bedrohungslandschaft entwickelt sich ständig weiter. Da Cyberkriminelle über immer bessere Ressourcen verfügen, ist es für Unternehmen schwierig, mit dem Tempo der neuen Bedrohungen Schritt zu halten. Gleichzeitig bietet der heutige Cyberspace hohe finanzielle Anreize für Cyberkriminalität.

Fachwissen:
In einer Zeit immer raffinierterer Angriffe erfordert die Verwaltung einer Sicherheitslösung ein hohes Maß an Fachwissen, das stetig weiterentwickelt werden muss. Für viele Unternehmen ist es eine teure und schwierige Aufgabe, ausreichende Ressourcen dafür bereitzustellen und gleichzeitig das erforderliche Fachwissen im Haus zu halten.

Die interne Verwaltung einer Sicherheitslösung ist weder einfach noch kostengünstig - und vielleicht noch nicht einmal besonders effektiv. Um diese Probleme zu lösen, gehen viele Unternehmen zu Managed Security Solutions über.

Anstatt ein internes Team ihre Plattformen verwalten zu lassen, überlassen diese Unternehmen die Verwaltung einem spezialisierten Sicherheitsanbierter.

Dies löst alle oben genannten Probleme und hat darüber hinaus viele weitere Vorteile.

- Sicherheitsanbieter, die Managed Services anbieten, verfügen über engagierte 24/7-Supportteams, die jede noch so kleine Anfrage sofort bearbeiten und selbst größere Probleme nach nur einem Telefonanruf oder einer kurzen Mail lösen.

- Eine All-in-One-Plattform (z. B. WAF der nächsten Generation, DDoS-Schutz, Bot-Verwaltung) kann das Sicherheitsmanagement vereinfachen und durch die Konsolidierung mehrerer Dienste bei einem Anbieter Zeit und Geld sparen.

FAZIT

In der modernen Bedrohungslage ist eine robuste Sicherheit von Webanwendungen von entscheidender Bedeutung. Es gibt eine Vielzahl von Lösungen, aber nicht alle sind gleich.

Es gibt erhebliche Unterschiede in Bezug auf Effektivität, Flexibilität, Datenschutz, Transparenz, Preisgestaltung und vielem mehr. Unternehmen, die bei der Evaluierung von Lösungen die nötige Sorgfalt walten lassen, können beträchtliche Einsparungen erzielen und gleichzeitig eine stärkere und leistungsfähigere Sicherheitsstruktur aufrechterhalten.

Die Auswahl der richtigen Web Application and API Protection (WAAP) ist der Schlüssel zum Schutz der digitalen Infrastruktur vor den hochentwickelten Bedrohungen der heutigen Zeit. Eine einheitliche Plattform bietet umfassenden Schutz für alle WAAP-Säulen und vereinfacht gleichzeitig die Verwaltung, reduziert die betriebliche Komplexität und gewährleistet die Skalierbarkeit, um zukünftigen Anforderungen gerecht zu werden.

ÜBER LINK11

Link11 ist ein globaler Cloud-Sicherheitsanbieter, der Lösungen für Netzwerksicherheit, Anwendungs- und API-Schutz sowie Anwendungsperformance für eine Vielzahl von Branchen anbietet. Vom umfassenden Netzwerk-DDoS-Schutz bis hin zu einer fortschrittlichen WAAP-Lösung umfasst unsere Plattform eine Web Application Firewall (WAF), Web-DDoS-Schutz, Bot-Management (einschließlich ATO), API-Schutz und Secure CDN & DNS.

Die Link11 Cloud WAAP-Plattform bietet mehrschichtigen Schutz für wichtige Web-Assets, einschließlich Web-Anwendungen und APIs. Durch die Integration von WAF, Web DDoS Protection, Bot Management und API Protection bietet Link11 eine einheitliche Sicherheitsplattform und eine vollständig verwaltete WAAP-Lösung, alles in einem einzigen Fenster.

Demo buchen

LINK11

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | www.link11.com