
Akamai
Die Aufklärung der 5 Mythen rund um Web Application Firewalls

Für Unternehmen, die im Internet geschäftskritische Geschäfte tätigen, sollte die Web Application Firewall (WAF) die erste Verteidigungslinie sein, um schädlichen Traffic abzuwehren und gleichzeitig legitimen Traffic durchzulassen. WAF-Technologie ist seit vielen Jahren verfügbar. Doch die ursprüngliche Definition der WAF ist für ihre weiterentwickelten und modernen Anwendungen viel zu einfach. Deshalb halten viele Führungskräfte und Sicherheitsexperten weiter an veralteten Denkweisen und Mythen fest.

Diese Mythen können dazu führen, dass Unternehmen die Leistungsfähigkeit der WAF – die wahrscheinlich bereits in ihrem Stack vorhanden ist – unterschätzen und nicht voll ausschöpfen. Und das öffnet Angreifern Tür und Tor und erhöht das betriebliche Risiko. Der Bedarf an umfassender digitaler Sicherheit von WAF-Technologien wächst weiter. Um die Sicherheit zu steigern und die neuesten Schutzmethoden für WAF-Technologie zu nutzen, müssen wir uns zunächst einmal mit den häufigsten Mythen beschäftigen.

Im 3. Quartal 2023 verzeichneten wir 9,93 Milliarden Webanwendungs-angriffe

Die täglichen Angriffe im 3. Quartal 2023 erreichten ihren Höhepunkt bei rund 327 Millionen

Quelle: Bedrohungsforschung bei Akamai

Mythos 1

WAFs erfordern ständige manuelle Updates, um effektiv zu bleiben

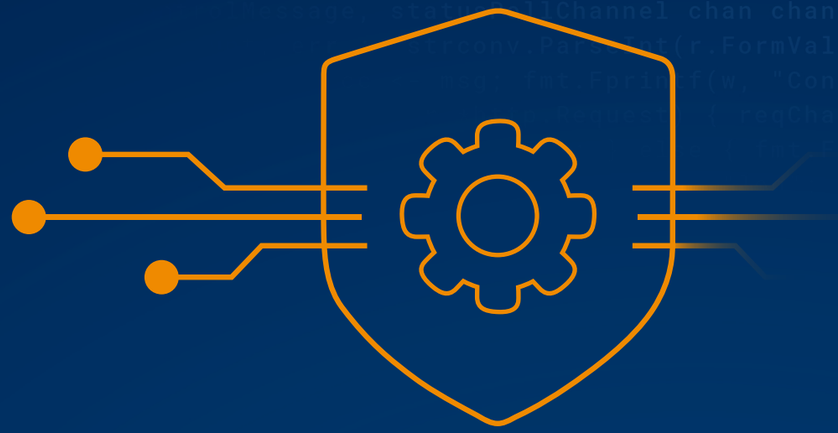
Es stimmt zwar, dass die neuesten Updates den neuesten Schutz bieten, aber es gibt einige Mythen rund um diese Aussage, die aufgeklärt werden müssen. Viele Unternehmen verfügen heute nicht über ausreichende Ressourcen oder Sicherheitskenntnisse, um WAF-Regeln kontinuierlich zu aktualisieren und anzupassen. Automatisierte und adaptive Updates bieten mehr als nur Zeitersparnis und Nutzerfreundlichkeit: Sie verringern auch das Risiko.

Als wir uns die Unternehmen angesehen haben, die sich für manuelle Updates entschieden haben, waren über 77 % bei der Aktualisierung von Regelsätzen mindestens fünf Versionen im Rückstand. Akamai spielt kontinuierlich und automatisch WAF-Updates auf. Ihr Unternehmen spart auf diese Weise Zeit, Ressourceninvestitionen und umgeht unnötige Risiken.

Mythos 2

WAFs steuern nur den Traffic

Veraltete WAFs befinden sich in der Mitte des Traffics zwischen Nutzern und Webanwendungen und prüfen den HTTP-Traffic anhand einer definierten Liste von Regeln. Die Lösung von Akamai hat sich rasant über herkömmliche WAFs hinaus entwickelt und bietet mehr Funktionen und besseren Schutz, einschließlich DDoS-Abwehr, API-Sicherheit, Bot-Abwehr, Malware-Erkennung, Erkennung sensibler Daten und Performancesteigerung. Und mit der Veröffentlichung von App & API Protector umfasst Ihre WAF-Sicherheitslösung jetzt weitere beliebte Technologien wie Site Shield, mPulse Lite, EdgeWorkers, Image & Video Manager, API Acceleration und mehr. Die WAF-Lösung von Akamai ist eine umfangreiche Technologie, die Sicherheitsexperten vollständige Transparenz und Kontrolle bietet, damit sie standortübergreifenden Schutz erreichen können.



Mythos 3

WAFs überfluten Verteidiger mit Warnungen

Wenn Sie die Verteidigungsteams an der Front befragen, werden sie Ihnen berichten, dass sie durch die schiere Menge an Warnungen und Triggern, die sie untersuchen müssen, überlastet und überfordert sind – insbesondere durch die Warnungen, die von WAF-Abwehrsystemen ausgelöst werden. Genau aus diesem Grund hat Akamai Adaptive Security Engine entwickelt, die Kerntechnologie der WAF-Lösung von Akamai. Mit Adaptive Security Engine erhält Ihr Unternehmen modernen Schutz durch die Kombination von maschinellem Lernen, Echtzeit-Sicherheitsinformationen, fortschrittlicher Automatisierung und Erkenntnissen von mehr als 400 Bedrohungsforschern von Akamai. Adaptive Security Engine wurde zum Schutz ganzer Webanwendungen und API-Bestände entwickelt. Die Lösung ist dahin gehend einzigartig, dass sie Traffic- und Angriffsmuster für jeden Kunden erlernt, die Eigenschaften jeder Anfrage in Echtzeit analysiert und dieses Wissen nutzt, um zukünftige Bedrohungen abzufangen und sich an diese anzupassen. Dank Adaptive Security Engine können sich Verteidiger von der Flut an Warnmeldungen verabschieden, wertvolle Zeit sparen und den Aufwand für den Schutz von Anwendungen und APIs reduzieren.

Die Optimierungsempfehlungen der Adaptive Security Engine reduzieren die Anzahl von False Positives nachweislich um das

5-Fache

Mythos 4

Mehr WAF-Anpassungsmöglich-keiten bieten mehr Sicherheit

Mit zusätzlichen Regeln können auch zusätzlicher Einrichtungsaufwand, mehr Tests und weitere Analysen einhergehen. Doch weder mehr noch weniger Regeln bedeuten automatisch mehr Sicherheit. Wenn Sie einer der Sicherheitsexperten sind, die an den Grundsatz „Viel hilft viel" glauben, dann machen Sie sich keine Sorgen: Unsere WAF ermöglicht unbegrenzte nutzerdefinierte Regeln – und unsere proaktiven, adaptiven Regelaktualisierungen werden unabhängig von der Anzahl Ihrer vorhandenen Regeln bereitgestellt. Mit automatischen Updates und automatisierter Selbstoptimierung kann Ihr Team die WAF-Konfiguration in Ihrem gesamten digitalen Bestand effizient und effektiv überprüfen. Sie möchten eine neue Regel hinzufügen? Im Auswertungsmodus können Sie die Auswirkungen neuer und geänderter Regeln auf den Live-Traffic bewerten – und dabei die Echtzeiteffekte in den Kundenportal-Dashboards sehen. Dieser Teststil im Shadow-Modus stellt sicher, dass Ihre neue Regel genau den Schutz bietet, der bei der Bereitstellung erwartet wurde.

Mythos 5

WAFs stehen Entwicklern nur im Weg

Entwickler steigern den Wert, den moderne Unternehmen ihren Kunden bieten können. Wenn die Sicherheit im Weg steht, verlangsamt sich die Innovation, Veröffentlichungszyklen verzögern sich und die Wertschöpfung nimmt ab. Doch auf der anderen Seite können ungetestete Releases verheerende Sicherheitsergebnisse zur Folge haben, die den Geschäftsbetrieb zum Erliegen bringen. Wir bei Akamai sind Fürsprecher für Sicherheitsexperten und -entwickler. Wir sind davon überzeugt, dass WAF-Abwehrmechanismen – solche, die Anwendungen, APIs und vieles mehr schützen – eine DevSecOps-Kultur unterstützen können, die Geschwindigkeit, Agilität und Zusammenarbeit vorantreibt. Deshalb können all unsere WAF-Funktionen über eine offene AppSec-API oder Terraform verwaltet werden. So kann Ihr Team das Onboarding von Anwendungen und APIs sowie die Verwaltung von Sicherheitskonfigurationen automatisieren. Und wenn Sie Hilfe benötigen, bietet Akamai TechDocs moderne, interaktive und intuitive Funktionen, die speziell auf Entwickler ausgelegt sind.

So kann Akamai Abhilfe schaffen

Angesichts der Kombination aus schnell wachsender Angriffsfläche, ständig weiterentwickelten Bedrohungen und hoch motivierten Angreifern brauchen Verteidiger Transparenz, die über herkömmlichen WAF-Schutz hinausgeht. Der App & API Protector von Akamai ist eine Lösung, die viele Sicherheitstechnologien wie Web Application Firewall, Bot-Abwehr, API-Sicherheit und DDoS-Schutz vereint. Mit dem App & API Protector werden Sicherheitsmaßnahmen kontinuierlich und automatisch aktualisiert. Individuelle Richtlinienempfehlungen werden zudem mit einem einzigen Klick implementiert. Die Adaptive Security Engine, die Technologie im Kern des App & API Protector, bietet modernen Schutz durch eine Kombination von maschinellem Lernen, Sicherheitsinformationen in Echtzeit, fortschrittlicher Automatisierung und den Erkenntnissen von mehr als 400 Bedrohungsforschern.

Starten Sie einen kostenfreien Test oder erfahren Sie, wie Akamai Ihre wichtigsten webbasierten Ressourcen schützt, um Risiken und betriebliche Reibungen für Ihr Unternehmen zu reduzieren.