10 Mythen bei der Auswahl einer Web Application Firewall

Der zuverlässige Schutz Ihrer Webanwendungen kann eine echte Herausforderung darstellen, insbesondere, wenn Sie nicht über spezielles Sicherheitspersonal oder entsprechende Schulungen verfügen. Eine Web Application Firewall (WAF) hält Bedrohungen in Schach und sorgt gleichzeitig für die Aufrechterhaltung der Anwendungsperformance. Doch bei so vielen Lösungen fällt die Auswahl schwer. Lassen Sie uns einige WAF-Mythen aufklären. So können Sie besser beurteilen, was wirklich zählt – das bedeutet weniger Angst vor Angriffen und mehr Energie für das Wachstum Ihres Unternehmens.

MYTHOS 1: Die Handhabung einer WAF ist kompliziert.

Es geht auch anders: Die WAF von Akamai vereinfacht den Schutz vor DDoS-Angriffen (Distributed Denial-of-Service) und die Sicherheit auf Anwendungsebene durch leicht zu verwaltende Regelsätze. WAF-Regeln werden automatisch aktualisiert, um Sie vor den neuesten Cyberbedrohungen zu schützen, sodass Ihre Schutzmaßnahmen stets auf dem neuesten Stand sind. Die Regeln werden gründlich getestet, um Bedrohungen abzuwehren und legitime Nutzer zu schützen – ohne böse Überraschungen. Und wenn Sie unsere Sicherheitsexpertise benötigen, bietet Akamai Support rund um die Uhr.

MYTHOS 2: Mehr Anpassungsmöglichkeiten bieten mehr Sicherheit.

Weniger ist mehr – vor allem, wenn es um die Nutzerfreundlichkeit geht. Wenn zu viele Regeln angepasst werden müssen, entsteht unnötige Komplexität, insbesondere wenn Ihr Unternehmen nicht über das nötige Sicherheitswissen verfügt, um sich mit den Details der Regelabhängigkeiten und -interaktionen vertraut zu machen. Die automatisierten WAF-Regelsätze von Akamai sind in acht Kategorien zusammengefasst – Sie müssen sie lediglich aktivieren. Da an weniger Stellschrauben gedreht werden muss, ist es unwahrscheinlicher, dass Anpassungen Probleme verursachen.

MYTHOS 3: Ausfälle gehören zum Geschäftsbetrieb dazu.

Ausfälle sind bei Online-Geschäften nicht länger akzeptabel. *Network World* berichtet, dass eine Stunde Ausfallzeit kleine Unternehmen bis zu 8.000 US-Dollar und mittelständische Unternehmen bis zu 74.000 US-Dollar kosten kann. Akamai bietet Skalierbarkeit und Ausfallsicherheit mit 100%iger Verfügbarkeit in über 130 Ländern und über 1.700 Netzwerke hinweg weltweit. Daher wird Akamai von den Branchen mit den höchsten Ansprüchen an Verfügbarkeit geschätzt, darunter acht der weltweit führenden FinTech-Unternehmen und 91 der führenden US-Internethändler.

MYTHOS 4: Schnellere Regelaktualisierungen ermöglichen eine schnellere Anwendungsverteidigung.

Aber nicht, wenn diese Regeln nicht angemessen geprüft werden. Wenn neue WAF-Regeln voreilig in der Produktion eingesetzt werden, können sie genau das Gegenteil bewirken. Um unsere Kunden zu schützen, testet Akamai neue Regeln in zwei Phasen: zunächst in unserem Labor mit bekanntem legitimen und schädlichen Traffic und dann auf der Plattform, um die Änderungen hinsichtlich False Positives und False Negatives bei Live-Internettraffic zu analysieren. Tauschen Sie nicht Geschwindigkeit gegen Qualität ein, indem Sie zulassen, dass Ihr Unternehmen mit neuen Regeln experimentiert.

MYTHOS 5: Eine Bedrohungsanalyse per Crowdsourcing bietet ausreichend Schutz.

Analysen, die ausschließlich auf Crowdsourcing basieren, fehlt es an Präzision, Überprüfung und Kontext für das Verhalten – und False Positives werden nicht berücksichtigt. Akamai stellt für über 6.000 der größten Onlineunternehmen mehr als 95 Exabyte an Daten über Milliarden von Geräten hinweg bereit und gewinnt so umfassende Einblicke in gewaltige Mengen legitimen und schädlichen Traffics auf der ganzen Welt sowie in verschiedensten Branchen. Durch die Beobachtung dieses Traffics verfolgen die Sicherheitsexperten von Akamai, wie sich Angriffe und legitimer Traffic entwickeln. Dieser Einblick ist für die Regelgenauigkeit in allen Branchen von Vorteil.

MYTHOS 6: Eine größere Anzahl von Regelauslösern führt zu besseren Ergebnissen.

Die Anzahl der Regelauslöser ist lediglich das Grundgerüst des Systems. Entscheidend ist, wie Auslöser miteinander zusammenhängen und bewertet werden. Dies ist ausschlaggebend für die Anzahl der Angriffe, die die WAF erkennt. Akamai verarbeitet täglich mehr als 2 Billionen Internet-Interaktionen und interagiert mit über 100 Millionen IP-Adressen, was uns umfassende Informationen und Einblicke verschafft. Die meisten Angriffe beginnen in einer bestimmten Branche, bevor sie sich auf andere ausweiten. Jede Woche werden hunderte Millionen Webangriffe auf verschiedene Branchen beobachtet. Mit der einzigartigen Perspektive von Akamai sind Sie Bedrohungen immer einen Schritt voraus und vor Cyberangriffen geschützt, noch bevor diese sich verbreiten.

MYTHOS 7: Sie müssen Ihre APIs nicht schützen.

In einer immer stärker vernetzten digitalen Welt reicht es nicht aus, nur Ihre Webseiten zu schützen. Eine angemessene API-Sicherheit verkleinert Ihre Angriffsfläche. Die WAF von Akamai kann APIs vor DDoS- und Webanwendungsangriffen schützen, indem der API-Traffic nach IP-Adresse, Standort, ungewöhnlichem Zugriff oder übermäßigen Anfragen blockiert wird. Die WAF von Akamai prüft API-Anfragen (einschließlich JSON und XML) automatisch auf schädliche Inhalte und erweitert so den umfassenden Schutz von Websites auf APIs.

MYTHOS 8: Eine WAF kann vor allen Zero-Day-Angriffen schützen.

Definitionsgemäß lässt sich ein Zero-Day-Angriff nicht vorhersehen, sodass kein Anbieter dieses Versprechen abgeben kann – aber das bedeutet nicht, dass eine WAF Ihnen in einem solchen Fall nicht helfen kann. Beispielsweise verwendet die WAF von Akamai anomaliebasierte Regeln, um Zero-Day-Angriffe zu erkennen, die Gemeinsamkeiten mit bekannten Fällen aufweisen. Die WAF von Akamai nutzt einen Anomalie-Bewertungsmechanismus und hat ohne zusätzliche Anpassungen Angriffe auf Basis von Zero-Day-Schwachstellen erkannt. Außerdem werden die WAF-Regeln von Akamai automatisch aktualisiert, sodass Sie nicht mit der sich ständig ändernden Bedrohungslandschaft Schritt halten müssen.

MYTHOS 9: Eine WAF schützt vor allen Bots.

Auch wenn eine WAF eine wichtige Sicherheitsebene gegen Bots bietet, blockiert die WAF von Akamai bekannte Bots *und* solche, die viel Traffic generieren. Kümmert man sich nicht um diese lästigen Bots, werden Ihre Systeme ausgebremst und der legitime Traffic beeinträchtigt. Mit einer WAF können Sie ganz einfach gegen Bots vorgehen, die Ressourcen verbrauchen, ohne andere Schäden zu verursachen. Wenn versiertere Bot-Betreiber ein Unternehmen ins Visier nehmen, finden sie auch einen Weg, die WAF zu überwinden. Für diese Fälle bietet Akamai spezialisierte Bot-Management-Lösungen an, die fortschrittliche Bot-Bedrohungen wie den Diebstahl von Anmeldedaten erkennen und verhindern.

MYTHOS 10: Individuelle Einzellösungen sind in ihren Spezialisierungsbereichen überlegen.

Wenn es um den Schutz vor den neuesten Cyberbedrohungen geht, sorgt der Wissenstransfer durch unsere vielfältigen Sicherheitsangebote und damit beobachteten Vorfälle für einen effektiveren automatisierten Schutz, eine bessere Erkennung von Anomalien und hochwertigere Regelsätze. Eine Sicherheitsstrategie, die spezialisierte Lösungen von mehreren Anbietern verwendet, ist oft schwieriger zu verwalten, erfordert mehr Schulungen und stellt Integrationsherausforderungen dar.

Weitere Informationen darüber, wie die WAF von Akamai Ihren Schutz auf Anwendungsebene und vor DDoS-Angriffen erleichtern kann, finden Sie unter Akamai.com/Security.

Akamai

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai hält Angriffe und Bedrohungen fern und bietet im Vergleich zu anderen Anbietern besonders nutzernahe Entscheidungen, Anwendungen und Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter **akamai.de**, im Blog **blogs.akamai.com/de** oder auf Twitter unter **@AkamaiDACH** sowie **@Akamai**. Unsere globalen Standorte finden Sie unter **akamai.de/locations**. Veröffentlicht: April 2019