Akamai

WHITEPAPER

Sicherheit von Webanwendungen – ganz einfach und zuverlässig

Angriffe auf Webanwendungen

Moderne Webanwendungen sind komplex geworden, insbesondere durch die zunehmende Einführung von auf Microservices basierten Architekturen. Die starke Abhängigkeit von APIs für praktisch jede Online-Interaktion trägt zu dieser Komplexität bei und bringt mögliche neue Einstiegspunkte für Hacker mit sich. Bekannte Schwachstellen im Internet bestehen weiterhin und werden von jeder neuen Entwicklergeneration wieder in Anwendungen eingeführt. Die Angreifer von heute haben reagiert und sich weiterentwickelt: Sie nutzen Bots, DDoS-for-hire (Distributed Denial of Service) und Multivektor-Attacken, um gezielt Webanwendungen, APIs und sogar clientseitige Schwachstellen anzugreifen.

Allerdings sind die meisten Webangriffe immer noch opportunistisch motiviert, das heißt, sie nehmen nicht ein bestimmtes Unternehmen ins Visier, sondern greifen dort an, wo sie Schwachstellen entdecken. Scanner nutzen automatisierte Bots, um Websites nach dem Zufallsprinzip auf Tausende mögliche Schwachstellen zu untersuchen. Sobald eine Schwachstelle gefunden wurde, können Angreifer die geheimen Bestände von Datenbanken einsehen, schädliche Dateien auf einen Webserver laden oder eine Website mit einem gewaltigen Trafficvolumen überlasten.

Welche Risiken gehen mit Webangriffen einher?

Unternehmen mit geringer Risikotoleranz benötigen ein hohes Sicherheitsniveau, um eine Vertrauenskette aufzubauen – sowohl intern (zwischen Systemen, Lieferkette, Betrieb usw.) als auch extern (bei Partnern, Kunden, Behörden usw.). Besonders wichtig ist der Schutz von APIs – von einfachen internen Strömen zwischen Teilen einer Microservice-Anwendung bis hin zu wichtigen Business-to-Business-Transaktionen –, denn APIs fungieren als digitales Bindeglied zwischen unterschiedlichen Systemen und Partner-Ökosystemen und ermöglichen so digitale und kanalübergreifende Kundenerlebnisse.

Cyberkriminelle verfügen leider über ein nahezu unbegrenztes Arsenal an Methoden für Webangriffe, die maximalen Schaden verursachen sollen. Ein erfolgreicher Hack, der zur Extraktion sensibler Daten führt, oder ein DDoS-Angriff, der den Zugriff auf Ihre Website blockiert, kann das Vertrauen zerstören. Der Schaden durch verlorene Kundentreue, Bußgelder, Gerichtsverfahren und ein angekratztes Markenimage kann erheblich sein.

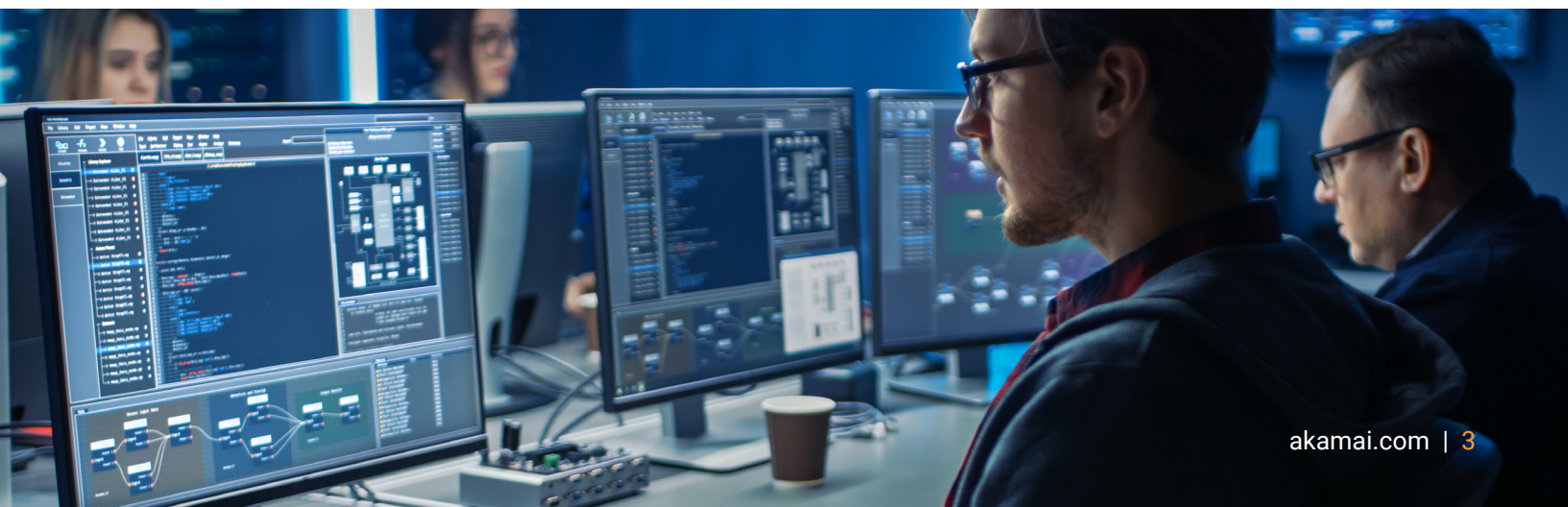
Herausforderungen bei der Sicherheit von Webanwendungen

Cloudbasierte WAAP-Lösungen (Web Application and API Protection) zum Schutz von Webanwendungen und APIs wurden entwickelt, um viele Arten von Webanwendungs-, DDoS- und API-basierten Angriffen abzuwehren. Eine der größten Herausforderungen bei Firewalls ist jedoch, dass für die Anwendungssicherheit zuständige Teams Regeln ständig analysieren und anpassen müssen, wenn sich Anwendungen ändern, sich Bedrohungen weiterentwickeln und Updates verfügbar werden. Die Besetzung von Stellen mit erfahrenen Sicherheitsexperten stellt nach wie vor eine Herausforderung dar, da qualifizierte Mitarbeiter häufig alle zwei Jahre ihre Position wechseln. Dabei handelt es sich häufig um einen zeitaufwändigen manuellen Prozess, für den qualifizierte Mitarbeiter erforderlich sind und der bei den meisten Unternehmen aufgrund von Fluktuation, Lernzyklen und speziellen Architekturen zur Technologieintegration nicht skalierbar ist.

Veraltete Sicherheitsrichtlinien können zu einer Quelle großer Frustration werden, wenn ein Übermaß an Warnmeldungen die genaue Unterscheidung von False Positives und echten Angriffen drastisch erschwert. Sicherheitsteams, die nicht in der Lage sind, Regeln effektiv zu optimieren, könnten auch ihre Schutzvorkehrungen außer Betrieb nehmen und wissentlich ein erhöhtes Risiko akzeptieren, weil sie negative Auswirkungen für legitime Nutzer und Störungen des Unternehmensgeschäfts befürchten.

Warum Akamai WAAP?

Akamai App & API Protector ist eine cloudbasierte WAAP-Lösung, die Ihre Anwendungen und APIs mit weniger Aufwand vor einer Vielzahl von Bedrohungen auf Netzwerk- und Anwendungsebene umfassend schützt – auch Bot-Transparenz und -Abwehr sind in die Lösung integriert. Der Self-Service-Assistent für das Onboarding von Akamai bietet Orientierungshilfen und Einblicke für einen schnellen und einfachen Schutz Ihrer Ressourcen. Zudem ist weniger Vorwissen erforderlich. Im Rahmen unseres automatisierten Einrichtungsprozesses werden Sicherheitsauslöser analysiert. Dabei lernt das System, wie sich Anwendungen verhalten, und kann auf diese Weise Schutzmaßnahmen selbst optimieren. Dadurch werden weniger Ressourcen beansprucht. App & API Protector beseitigt viele der heutigen Firewall-Probleme, die unternehmensinterne Reibungen verursachen, den Betrieb belasten und die Bereitstellung behindern.



Automatisierte Schutzmaßnahmen, die sich vollständig von Akamai verwalten lassen, werden auf der weltweit am stärksten verteilten Plattform durchgesetzt und ermöglichen Ihnen einen praktischen Ansatz für Anwendungssicherheit und API-Schutz. Der automatische Schutz vor Webangriffen wie SQL-Injection, Cross-Site Scripting und Local File Inclusion bietet eine breite Abdeckung ohne laufende Wartung. Dank maschinellem Lernen und Heuristik können wir einzelne Richtlinien analysieren und müssen keine netzwerkweiten Prüfungen durchführen. Dadurch können wir False-Positive-Muster in Ihrem Traffic besser identifizieren und erhalten höchst relevante und nützliche Ergebnisse.

Validieren Sie Ihre Sicherheitsmaßnahmen mit unserem CVE-Lookup-Tool, das detaillierte Informationen zu einzelnen CVEs liefert, einschließlich Bedrohungsstufen und Einblicken in die aktuellen Schutzlösungen von Akamai, und Ihnen so als Orientierungshilfe für Ihre internen Sicherheits- und Entwicklungsstrategien dient. Optimieren Sie zudem die interne Ausrichtung und verkürzen die Markteinführungszeit mit den vordefinierten SecDevOps-Integrationen von Akamai, einschließlich Akamai als Code, APIs, CLI, Terraform und Integrationen.

Adaptive Schutzfunktionen setzen neue Maßstäbe

Wie bietet Akamai App & API Protector sowohl Einfachheit als auch Genauigkeit? Zunächst ist Akamai Adaptive Security Engine, die Kerntechnologie in App & API Protector, 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. Diese Technologie vereinfacht Sicherheitsvorgänge, indem sie alle anomalen oder verdächtigen Datenpunkte berücksichtigt und jeder Anfrage eine Bedrohungsbewertung zuweist. Je höher die Bedrohungsbewertung, desto aggressiver der Schutz. Durch die dynamische Anpassung der Schutzmechanismen an das Ausmaß der erkannten Bedrohung können wir selbst gut getarnte Angriffe erkennen und gleichzeitig die Zahl der False Positives extrem niedrig halten.

Angriffe auf Anwendungen setzen in der Regel Ausspähungsaktivitäten voraus. Doch Akamai sammelt Informationen zu Methoden und Taktiken der Angreifer, wenn diese nach Schwachstellen suchen. Dadurch sind die Angreifer nicht nur schnell erkennbar, sie hinterlassen auch eine Verlaufsspur für Ihren spezifischen Traffic, falls sie wiederkommen. Je häufiger ein Angreifer es versucht, desto stärker wird Ihr Schutz.

Akamai hat Einblick in:

mehr als 780 Millionen
tägliche Angriffswarnungen für Webanwendungen

mehr als 26 Milliarden
Bot-Anfragen

mehr als 932 TB
an Daten, die täglich analysiert werden

Threat Intelligence auf Basis von Crowdsourcing

Viele der am häufigsten angegriffenen Internet-Websites gehören Kunden von Akamai, darunter neun der zehn führenden Einzelhandelsunternehmen, alle zehn führenden Banken, neun der zehn führenden Unternehmen im Gesundheitswesen und alle sechs Zweige des US-Militärs. Wir können mehr als 780 Millionen Angriffe auf Webanwendungen und 26 Milliarden Bot-Anfragen pro Tag einsehen. Hunderte von fachkundigen Bedrohungsexperten und Data Scientists untersuchen bei Akamai täglich über 932 TB neuer Daten auf Bedrohungen. In Kombination mit fortschrittlichem maschinellem Lernen, KI und menschlicher Analyse können wir mithilfe dieser globalen Einblicke sowohl besonders verbreitete als auch hochkomplexe Angriffe proaktiv und vorausschauend stoppen.

Akamai wehrt seit mehr als einem Jahrzehnt Angriffe auf Anwendungen ab und konnte Kunden und deren Infrastruktur selbst bei den größten Angriffen schützen. Wir untersuchen weiterhin neu aufkommende Bedrohungen und erstellen Bedrohungsberichte. Da sich die Angriffe weiterentwickeln und immer raffinierter werden, entwickeln auch wir unsere Lösungen weiter und passen sie an, um Cyberkriminellen immer einen Schritt voraus zu sein. Und da App & API Protector auf der Plattform von Akamai basiert, verfügt es über integrierte Performancefunktionen, die dafür sorgen, dass Ihre Websites, Anwendungen und APIs optimal funktionieren.

Überprüfen Sie Ihre Anforderungen an den Schutz von Webanwendungen und APIs und entdecken Sie die Vorteile von Akamai App & API Protector mit dieser kostenlosen Testversion.