Akamai

WHITEPAPER

Von WAF zu WAAP: Der Akamai-Ansatz für umfassende Anwendungs- und API-Sicherheit

Inhalt

Einführung **04**

Traditionelle Definition einer WAF **05**

Herausforderungen bei einer herkömmlichen WAF **06**

Designprinzipien – von WAF zu WAAP **07**

Der WAAP-Ansatz von Akamai **10**
- Mehr als bloße Regelsätze 10
- Modernisierung der DDoS-Abwehr auf Anwendungsebene über Ratenbegrenzung hinaus 10
- Eine einzige Lösung für umfassenden Schutz 11

Die Adaptive Security Engine **12**
- Adaptive Bedrohungserkennung 13
- Automatische Updates 13
- Test-Framework zur Gewährleistung der Genauigkeit 14
- Automatische Selbstoptimierung 15
- Flexible Konfiguration und Automatisierung 15
  - Überprüfung in der realen Welt 16
  - Integration modernisierter Schutzmechanismen 16

Anwendungssicherheit und DDoS-Abwehr **18**
- Behavioral DDoS Engine: So funktioniert sie 19
- Genauigkeit der Anwendungssicherheit 21
- Client-Reputationsbewertung 22

Malware-Schutz **23**

Analyse der Anwendungssicherheit **24**

API-Erkennung und -Profilerstellung **25**

Bot-Transparenz und -Abwehr **27**
Bot-Transparenz und -Abwehr in App & API Protector 27
Wichtige Bot-Funktionen 28

Mehr als eine WAF: Vorteile der Akamai-Lösung **29**

Threat Intelligence und Bedrohungserkennung **30**
Threat Intelligence der Akamai-Plattform 30
Bedrohungsforschung und Vorfallreaktion 31
Bedrohungsforschung 31
Vorfallreaktion 31
Schnelle Erkennung von Bedrohungen 31
CVE-Schutz 32

Global verteilte Edge-Plattform **33**
Zuverlässigkeit und Resilienz 33
Weltweite Skalierung 35
Performance 35
Mehr Schutz dank Edge-Plattform 36
Verwaltete Angriffsabwehr 37
Security Operations Command Center (SOCC) 37

Fazit **38**

Einführung

Angriffsflächen werden immer größer und vielfältiger, betriebliche Effizienzprobleme und Kosten nehmen zu und Bedrohungen werden immer komplexer und schwerer aufzuspüren. Um all das in den Griff zu bekommen, brauchen Sicherheitsteams Transparenz, die über herkömmliche Web Application Firewalls (WAFs) hinausgeht. Insbesondere brauchen sie stärker automatisierte Tools, um die Effizienz zu steigern, und tiefgreifendere Schutzmechanismen im Ökosystem ihrer Webanwendungen und APIs (Application Programming Interfaces). Die modernere Bezeichnung für diese Art von Schutz lautet „Web Application and API Protection" (WAAP), also „Schutz von Webanwendungen und APIs". Anspruchsvolle Unternehmen räumen der Sicherheit ihres Geschäfts und ihrer Kunden hohe Priorität ein und verlangen entsprechend, dass ihre gesamten digitale Umgebung umfassend vor verschiedenen Bedrohungen geschützt wird. Neben dem Schutz von Anwendungen vor bekannten, unbekannten und Zero-Day-Angriffen geht es hierbei um die folgenden Schutzmaßnahmen:

- Adaptive Bedrohungserkennung
- Automatische Aktualisierung von Richtlinien
- Leistungsstarke DDoS-Abwehr
- API-Erkennung und -Sicherheit
- Bot-Transparenz und -Abwehr
- Einfache Integration für Entwicklungslebenszyklen

In diesem Whitepaper behandeln wir die traditionelle WAF-Technologie, die Umstellung von WAF auf WAAP und die anhaltende Nachfrage auf dem Markt, die zu einer Weiterentwicklung von WAAP-Lösungen führt. Als etablierter Marktführer im Sicherheitsbereich legt Akamai seinen Schwerpunkt auf innovative Sicherheitstechnologien, die Endnutzer in ihrem digitalen Leben unterstützen und schützen.

Traditionelle Definition einer WAF

Eine herkömmliche WAF befindet sich mitten im Traffic zwischen Endnutzern und einer Webanwendung. Die WAF prüft den unverschlüsselten oder verschlüsselten HTTP-Traffic, der sie durchläuft, auf Angriffe, die in einer Liste von Regeln definiert sind.

Die meisten WAFs identifizieren anhand einer vordefinierten Liste von Regeln schädliche HTTP-Anfragen, die im legitimem HTTP-Traffic versteckt sind, und bieten so Schutz vor Tausenden bekannten potenziellen Exploits. Darüber hinaus entwickeln sich immer neue Angriffsvektoren oder zusätzliche Permutationen vorhandener Angriffsvektoren, die von Cyberkriminellen ausgenutzt werden. Hier müssen die Regeln einer herkömmlichen WAF ständig aktualisiert und auf die legitimen Traffic-Merkmale abgestimmt werden, die sich je nach Anwendung unterscheiden und sich im Laufe der Zeit verändern.

Da Endnutzer mehr Schutz und Performance verlangten, wurde der Umfang von WAFs auf angrenzende Sicherheitstechnologien und -services wie DDoS-Abwehr (Distributed Denial of Service), API-Sicherheit und Bot-Abwehrfunktionen ausgeweitet. Diese kontinuierliche Weiterentwicklung erfordert eine neue Definition und neue Terminologie.

Herausforderungen bei herkömmlichen WAFs

Häufig erfüllen WAFs nicht die anfänglichen Erwartungen, die Unternehmen in Bezug auf Effektivität, einfache Verwaltung und Auswirkungen auf geschützte Anwendungen und APIs haben. Aufgrund von Problemen mit der Web-Performance – die schnell entstehen, wenn Milliarden von Web- und API-Anfragen auf schädlichen Code geprüft werden –, verursachen WAFs oft innerbetriebliche Effizienz- und Performanceprobleme und behindern die Bereitstellung aufgrund von Sicherheitsprotokollen.

Einige der größten Herausforderungen beim Einsatz herkömmlicher WAFs ergeben sich aus den folgenden Faktoren:

- Ungenaue Erkennung und eine hohe Zahl von False Positives (oder Fehlalarmen) haben eine Abstumpfung gegenüber Warnungen und zusätzliche Risiken zur Folge.
- WAFs sind auf manuelle Überprüfung, Optimierung und Wartung angewiesen.
- Das Fehlen detaillierter Kontrollen führt zu ineffektiven Blockierrichtlinien, die Nutzererlebnis und Geschäftsprozesse stören.
- Veraltete Threat Intelligence erhöht das mit Schwachstellen verbundene Risiko.
- Performance und Abdeckung werden aufgrund von Einschränkungen und mangelnder Flexibilität beeinträchtigt.
- WAFs sind zu begrenzt, um die digitale Expansion zu schützen.

Herkömmliche WAFs sind ein leistungsstarkes Sicherheitstool. Sie können Unternehmen jedoch oft operativen Problemen und hohen Risiken aussetzen, auf die wir in diesem Whitepaper eingehen.

Unternehmen, die ihre WAF-Technologie mit einer WAAP-Lösung aktualisieren möchten, müssen sicherstellen, dass diese Lösung sowohl einen geschäftlichen Nutzen als auch zuverlässige Sicherheit bietet. Die Umstellung von WAF auf WAAP kombiniert diese Sicherheit mit Funktionalität, Effizienz und Nutzerfreundlichkeit, um sämtliche Anforderungen von Unternehmen zu erfüllen – sowohl in Sicherheitsteams als auch für andere Mitarbeiter.

Designprinzipien – von WAF zu WAAP

Da sich klassische WAF-Produkte auf die Erstellung von Endnutzerregeln konzentrieren, kann jeder Anbieter relativ einfach eine WAF-Lösung erstellen und auf den Markt bringen. Das zeigt auch die Verbreitung kommerzieller Angebote, die auf dem Open-Source-basierten Open Worldwide Application Security Project ModSecurity Core Rule Set (OWASP CRS) basieren.

Für einen Anbieter ist es jedoch schwierig, eine umfassende WAAP-Lösung zu entwickeln, die folgende Möglichkeiten bietet:

- Inline-Bereitstellung zum Schutz von Anwendungen und APIs, wenn neue Schwachstellen auftreten
- Einbeziehen moderner Praktiken der App-Entwicklung
- Bereitstellen starker Funktionen für DDoS-Verteidigung, Bot-Abwehr, API-Schutz und clientseitigen Schutz von Webanwendungen

Als wir bei Akamai unsere WAAP-Lösung konzipiert haben, war für uns klar, dass sie besser werden sollte als nur „gut genug“. App & API Protector wurde entwickelt, um Sicherheitsrisiken zu begegnen und dabei sicherzustellen, dass sich unsere Kundenunternehmen auf wichtige Geschäftsziele konzentrieren können. Unser Design basierte auf der Überzeugung, dass eine ideale WAAP-Lösung Folgendes bieten sollte:

Effektive Sicherheit
Jeder Aspekt des Geschäfts ist auf Anwendungen angewiesen. Deshalb besteht das wesentliche Ziel von Sicherheitsteams in Unternehmen darin, diese Anwendungen vor Angriffen zu schützen. Hierbei stehen Sicherheitsteams vor der Herausforderung, eine WAAP-Lösung zu finden, die branchenführende Erkennungsfunktionen bietet. Das ideale Sicherheitstool priorisiert die Erkennungseffizienz, da dies der wichtigste Aspekt einer WAAP-Lösung ist. Das Tool sollte außerdem eine hervorragende Erfolgsbilanz in Bezug auf Zero-Day-, Exploit- und CVE-Abwehr (Common Vulnerabilities and Exposures) vorweisen und eine starke Verfügbarkeit gewährleisten können.

Genauigkeit
Sicherheitsteams müssen die richtige Balance zwischen Risikominderung und agiler Geschäftsentwicklung finden. Ideale Lösungen verfügen über Mechanismen zur Selbstoptimierung, die dazu beitragen, False Positives zu reduzieren, ohne dabei Nutzererlebnis und Geschäftsprozesse zu beeinträchtigen.

Moderne Schutzmaßnahmen

Unternehmen müssen Schutzmechanismen immer wieder (und häufig manuell) auf die neuesten Regeln aktualisieren, um neue Schwachstellen zu beheben, sobald sie entdeckt werden. Dazu benötigen sie zwei zentrale Fähigkeiten: Zugriff auf die neuesten Informationen zu sämtlichen Angriffsvektoren sowie qualifizierte Sicherheitsressourcen, mit denen die Verteidigungsstrategie an veränderliche Angriffe angepasst werden kann. Eine ideale Lösung muss in der Threat-Intelligence-Community als führend anerkannt sein und Funktionen bereitstellen, die den Sicherheitsbetrieb in der gesamten Umgebung vereinfachen.

Anpassungsfähigkeit

Die Bedrohungslandschaft entwickelt sich rasant weiter. Da bald auch KI-gestützte Angriffe möglich sind, müssen Sicherheitsteams mit ihren Maßnahmen effizienter sein als je zuvor. WAAP-Lösungen sollten über eine Kombination aus fortschrittlicher Automatisierung, maschinellem Lernen und umfassender globaler Threat Intelligence verfügen. So können sie Updates automatisch ausführen und Vorschläge für individuelle Regeländerungen bereitstellen, die mit einem Klick implementiert werden können.

Transparenz

Herkömmliche WAF-Lösungen liefern in der Regel einen endlosen Strom von Warnungen, die Sicherheitsexperten einzeln analysieren müssen, was die internen Ressourcen stark belastet. Eine effektivere WAAP-Lösung bietet Transparenz über mehrere Lösungen hinweg sowie proaktiven Kontext rund um Angriffe, indem sie Teams darüber benachrichtigt, wann, wo und wie sich diese Angriffe ereignet haben. So lässt sich die Ressourcenbelastung verringern.

Skalierbarkeit

Eine Lösung ohne die nötige Skalierbarkeit für den eingehenden Traffic kann leicht zu einem Engpass werden, der die Weblatenz erhöht und hohen Belastungen nicht standhalten kann. Bei einem effektiven Ansatz sollte sich die Skalierung automatisch und nahtlos an Traffic-Anforderungen und Angriffe anpassen, damit ein dauerhafter Schutz gewährleistet ist, ohne die Performance zu beeinträchtigen.

Zusammenarbeit
Eine effektive Sicherheitslösung muss sich in den aktuellen Stack integrieren lassen, muss programmierbar und nutzerfreundlich sein und muss reibungslos funktionieren. Eine ideale Lösung baut eine Brücke zwischen Sicherheits- und Entwicklungsteams.

Support
Bei anspruchsvollen Sicherheitsvorfällen sind interne Teams oft mit den Fähigkeiten und Ressourcen überfordert, die für eine zeitnahe Lösung erforderlich sind. Eine ideale Lösung umfasst regelmäßige Managed-Service-Optionen sowie On-Demand-Serviceoptionen, die Expertise und Abhilfe für gängige Szenarien wie aktive Angriffe, Serviceprobleme, Mitarbeiterfluktuation, interne Kompetenzlücken und vieles mehr bereitstellen.

Lassen Sie uns anhand dieser Designprinzipien untersuchen, wie wir bei Akamai die Entwicklung unserer führenden WAAP-Lösung App & API Protector angehen, angefangen bei der Kerntechnologie. Unsere Lösung kombiniert viele Sicherheitsprodukte in einem, um Herausforderungen in verschiedenen Bereichen ganzheitlich zu bewältigen: Schutz von Anwendungen, Abwehr volumetrischer DDoS-Angriffe, Schutz des API-Bestands sowie Kontrolle des Bot-Traffics.

Der WAAP-Ansatz von Akamai

Mehr als bloße Regelsätze

Während sich der Markt von traditionellen WAF-Designprinzipien hin zu modernen und effektiven WAAP-Sicherheitslösungen verlagerte, blieb der Fokus auf eine effektive Erkennungs- und Abwehrtechnologie gerichtet.

Akamai führte seine WAF 2009 als weltweit erste Edge-basierte WAF ein. Damals stellten Sicherheitsanbieter WAFs auf Basis statischer Regelsätze als Grundlage für die Erkennung bereit. Akamai hob sich mit seinem Angebot ab, indem es eine eigene regelbasierte Engine namens Kona Rule Set (KRS) entwickelte. Sie verwendete eine kleine Anzahl flexibler Regeln (statt statischer Regeln) in Verbindung mit einem Anomalie-Bewertungsmodell, um die Genauigkeit und Analysierbarkeit von Angriffen zu verbessern.

2017 führte Akamai dann automatisierte Angriffsgruppen ein. Damit entfiel für Unternehmen die Notwendigkeit, Regeln fortwährend mit Akamai-verwalteten Schutzmechanismen zu konfigurieren und zu aktualisieren. Automatisierte Angriffsgruppen waren ein revolutionärer Ansatz, der schnell in Tausenden von WAF-Richtlinien aktiver Akamai-Kunden umgesetzt wurde, die allesamt von den Vorteilen profitieren wollten.

Akamai entwickelte seinen Ansatz für Anwendungssicherheit noch weiter und priorisierte dabei den kombinierten Anwendungs- und API-Schutz einschließlich Bot-Abwehrfunktionen. 2021 wurde dann App & API Protector eingeführt – diese WAAP-Lösung sollte die Kona Site Defender WAF für große Unternehmen und wachsende globale Firmen ersetzen. Durch die Integration der KRS-Technologie in die Adaptive Security Engine änderte App & API Protector dieArt und Weise, wie Akamai Sicherheitsabläufe konzipierte.

Modernisierung der DDoS-Abwehr auf Anwendungsebene über Ratenbegrenzung hinaus

Bei der Abwehr von DDoS ist die Ratenbegrenzung ein bewährtes und effektives Mittel. Doch die Ausbreitung ausgeklügelter Layer-7-DDoS-Angriffe und Multi-Vektor-Attacken sowie die Ausnutzung von APIs haben dazu geführt, dass herkömmliche DDoS-Abwehrsysteme kaum Schritt halten können. Statische Abwehrmaßnahmen, die auf festen Schwellenwerten und vordefinierten Signaturen basieren, sind reaktiv und anfällig für Fehlalarme, insbesondere da Angreifer zunehmend schädlichen Traffic mit legitimen Anfragen kombinieren. Deshalb änderte Akamai den Ansatz zur DDoS-Abwehr und führte Innovationen wie URL-Schutz und die Behavioral DDoS Engine ein.

Die Behavioral DDoS Engine ist eine hochmoderne Ergänzung zu Akamai App & API Protector und eine der zentralen Technologien der Adaptive Security Engine. Zusammen bieten diese Engines beispiellosen Schutz vor modernen Bedrohungen und machen Akamai zu einem führenden WAAP-Anbieter. Dieser Doppel-Engine-Ansatz zeichnet Akamai aus, denn er bietet automatisierte Updates, Selbstoptimierungsfunktionen und kontextbezogene Erkennung, was Nutzer von manuellen Aufgaben entlastet.

Eine einzige Lösung für umfassenden Schutz

Auch heute sorgen ständige Veränderungen dafür, dass Anwendungssicherheit immer wieder neu definiert werden muss. Grund hierfür sind moderne Entwicklungspraktiken durch serverloses Edge-Computing, Microservices-basierte Architekturen, Single-Page-Anwendungen und SaaS-/IaaS-/PaaS-/FaaS-Ansätze, die allesamt die Anwendungssicherheit prägen.

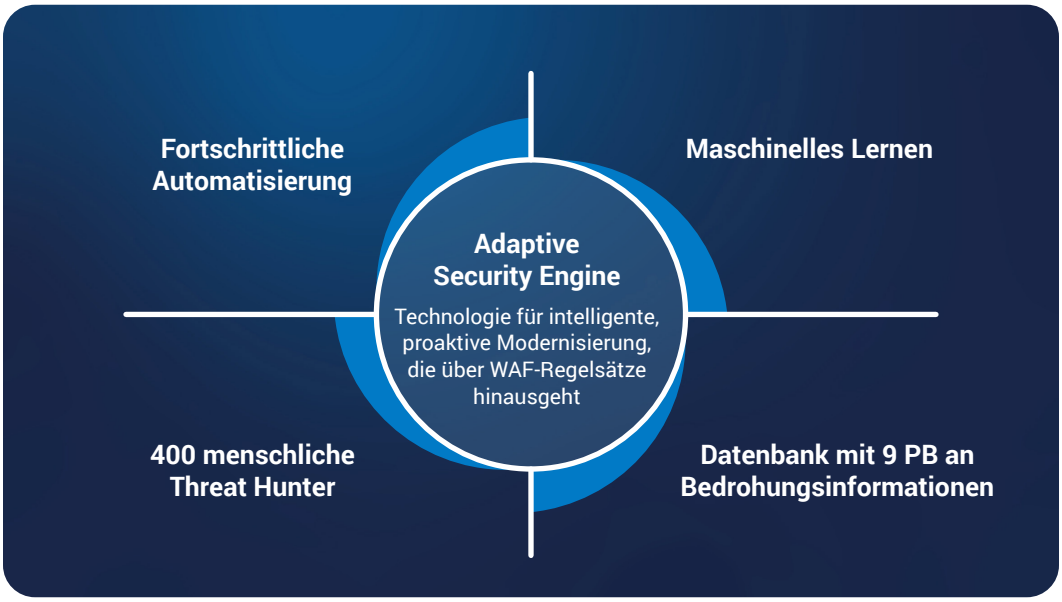
Um moderne Anwendungen und APIs in komplexen IT-Umgebungen zu schützen, hat Akamai seine Anwendungssicherheit umgestaltet, und zwar mit einem anpassungsfähigeren, flexibleren und ganzheitlicheren Ansatz. Akamai migrierte seine WAAP-Lösung von Web Application Protector und Kona Site Defender zu App & API Protector und integrierte weitere Sicherheitsfunktionen und Toolsets.

Heute bietet App & API Protector viele zusätzliche Sicherheitsverbesserungen, die alle über eine einzige Nutzeroberfläche eingesehen und kontrolliert werden können. Die WAAP-Lösung von Akamai kombiniert Folgendes:

1. Die Adaptive Security Engine
2. Anwendungssicherheit mit detaillierten Kontrollen
3. DDoS-Abwehr, einschließlich erweitertem Layer-7-DDoS-Schutz
4. API-Schutz, einschließlich Erkennung sowie Schutz personenbezogener Daten
5. Bot-Transparenz und -Abwehr
6. Eine Plattform für globale Skalierbarkeit, Threat Intelligence und Ausfallsicherheit

Die Adaptive Security Engine

Die Adaptive Security Engine bietet Schutz der nächsten Generation , indem sie maschinelles Lernen (ML), Echtzeit-Sicherheitsinformationen, Cybersicherheitsexperten und fortschrittliche Automatisierung kombiniert. Als Kerntechnologie von Akamai für Erkennung und Abwehr ermöglicht die Adaptive Security Engine einen stark automatisierten Ansatz zum Schutz ganzer Webanwendungs- und API-Bestände. Darüber hinaus ergänzt sie die Fortschritte, die Akamai bei der Umstellung von WAF auf WAAP gemacht hat, darunter verwandte Sicherheitslösungen wie Bot Manager, DDoS-Schutz, DevOps-Integrationen und vieles mehr.



Die Adaptive Security Engine von Akamai ist insofern einzigartig, als 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 daran anzupassen. Sie nutzt dieselben Plattformerkenntnisse und -informationen auch, um Fehlalarme durch Optimierungsempfehlungen zu reduzieren. Diese Selbstoptimierungsfunktion erleichtert Sicherheits- und Entwicklungsteams die Arbeit, da sie adaptiven Bedrohungsschutz durch proaktive Updates bietet.

Adaptive Bedrohungserkennung

Die Engine verwendet ein mehrdimensionales Modell zur Bewertung von Bedrohungen, das die Informationen der Plattform mit Daten/Metadaten aus der jeweiligen Anfrage kombiniert. Auf diese Daten wird eine Entscheidungslogik angewendet, um echte Angriffe genau zu identifizieren.

Adaptive Erkennungsfunktionen sind besonders bei der Identifizierung hochgradig gezielter und gut getarnter Angriffe effektiv, da raffinierte Angreifer hier mehr Zeit und Mühe in ihre Strategie investieren. Während Angreifer nach Schwachstellen und Fehlkonfigurationen suchen, sammelt und korreliert die Adaptive Security Engine Nachweise zu ihrer Taktik, um die historischen Fingerabdrücke der Angreifer besser identifizierbar zu machen.

Neben der tatsächlichen Payload und ihrer Position innerhalb der Anfrage bewertet sie für jeden Client unter anderem die folgenden weiteren Angriffsdimensionen:

- Verlauf von Ausspähungen und/oder Angriffen (z. B. Häufigkeit, Ausmaß, Schweregrad)
- Jegliche Anzeichen böswilliger Automatisierung und schädlicher Angriffstools
- Korrelation mit bekannten Quellen für Angriffstraffic

Darüber hinaus wird die Adaptive Security Engine durch zwei eigens entwickelte Technologien erweitert: Smart Detect, das die Eingabe in einen Fingerabdruck umwandelt, um eine äußerst genaue Erkennung zu ermöglichen, und Smart Sniff, das den richtigen Inhaltstyp für den Anfragetext erkennt, um die Manipulation von Inhalten und die Umgehung von Schutzmaßnahmen zu verhindern. Die Bedrohungsforscher von Akamai nutzen die umfassende Infrastruktur und die Systeme von Akamai, um passiv neue Informationen im gesamten Produktionstraffic zu erkennen, und analysieren diese Ergebnisse anschließend mithilfe von ML-Modellen.

Automatische Updates

Viele Unternehmen verfügen jedoch nicht über ausreichende Ressourcen oder die nötige Sicherheitsexpertise, um die Entwicklung der Bedrohungslandschaft nachzuverfolgen, Konfigurationen zu aktualisieren und wiederholte Tests für ihren Webtraffic durchzuführen, um Richtlinien zu optimieren. Als Reaktion darauf aktualisiert Akamai die Adaptive Security Engine kontinuierlich mithilfe eines automatischen KI-/ML-basierten Test-Frameworks, um immer neuen Bedrohungen Rechnung zu tragen und gleichzeitig eine hohe Genauigkeit zu gewährleisten. Diese Updates haben Unternehmen schon oft vor Zero-Day-Angriffen geschützt, bevor diese überhaupt angekündigt wurden.

Test-Framework zur Gewährleistung der Genauigkeit

Das Testen einer WAAP-Lösung basiert auf einer einfachen Prämisse: Man testet verschiedene Angriffsvektoren und stoppt Webangriffe. Folgende Faktoren müssen jedoch berücksichtigt werden:

- Reale Umgebungen sind deutlich komplexer als Testumgebungen und verursachen so False Positives und False Negatives.
- Die Entwicklung eines Test-Frameworks, das ein hohes Maß an Genauigkeit bietet, erfordert zusätzliche Überprüfungen. Angriffserkennung allein reicht nicht aus – sie muss so erfolgen, dass keine False Positives oder False Negatives ausgelöst werden.
- Tests erfordern echten Web-Traffic – sowohl legitimen als auch Angriffstraffic.

Updates der Adaptive Security Engine bestehen aus mehreren Stufen, damit gewährleistet ist, dass legitimer Traffic nicht beeinträchtigt wird:

- Alle Erkennungen werden im Labor mit synthetischem Traffic getestet. So wird sichergestellt, dass sie Angriffe richtig erfassen und keine False Positives verursachen.
- Updates werden dann am Live-Produktionstraffic getestet, um zu gewährleisten, dass die Stichprobe dem aktuellen Plattformtraffic entspricht. Bei diesem Prozess wird das Update im Schattenmodus auf echten Kundentraffic angewendet. Die Ausführung im Schattenmodus gewährleistet, dass es keine Auswirkungen auf den Kundentraffic gibt, aber dennoch eine genaue Testerkennung gegeben ist.
- Sobald ein Update Phase 2 durchlaufen hat, identifiziert ML Muster oder Auslöser, die bei der menschlichen Analyse möglicherweise nicht berücksichtigt wurden. Anschließend überprüft das Threat Research Team die Ergebnisse manuell.
- Nur wenn diese Prüfungen in jeder Phase bestanden werden, kann eine Änderung in die nächste Phase übergehen und in einem größeren Segment des Netzwerks bereitgestellt werden. Nach einer 100-prozentigen Bereitstellung werden durch die Selbstoptimierungsfunktionen alle verbleibenden False Positives beseitigt, die durch spezifische Trafficmuster der Kunden entstehen.

Automatische Selbstoptimierung

Die automatische Selbstoptimierung verringert die manuelle Optimierungsarbeit, die zu veralteten Richtlinien und menschlichen Fehlern führen kann. Es sind fast keine manuellen Eingriffe erforderlich. Die Adaptive Security Engine wendet ML, statistische Modelle und Heuristiken auf alle Auslöser und Sicherheitsrichtlinien an, um genau zwischen echten Angriffen und fälschlich als Angriff identifiziertem Endnutzer-Traffic zu unterscheiden. Es handelt sich dabei nicht um eine allgemeine, plattformweite Prüfung, die nur während des Onboardings angewendet wird, sondern vielmehr um einen kontinuierlichen Optimierungsprozess, der rund um die Uhr ohne Konfiguration oder Eingriff durch Endnutzer durchgeführt wird.

Die Selbstoptimierung erfolgt reibungslos und ist einfach. In der Nutzeroberfläche können Sicherheitsadministratoren Empfehlungen mit nur einem Klick überprüfen und akzeptieren und können mithilfe von AppSec-APIs, Command-Line Interface (CLI) oder Terraform Automatisierungen vornehmen. Im Interesse erhöhter Transparenz wird ein vorgefilterter Link zu Web Security Analytics bereitgestellt, über den alle als False Positives eingestufte Anfragen angezeigt werden können. Außerdem wird bei jeder Optimierungsempfehlung eine Begründung angeführt.

Flexible Konfiguration und Automatisierung

Wenn WAAP-Anbieter die herkömmliche Regelsatz-Technologie hinter sich lassen, werden Konfiguration und Automatisierung flexibler. Die Adaptive Security Engine bietet folgende Möglichkeiten:

- Verschiedene Arten von WAF-Updates (automatisch oder manuell) für unterschiedliche Anwendungen und die mit ihnen verbundene Risikobereitschaft
- Kontrollaktion pro Angriffsgruppe und zugehörige Regel, die zur Anpassung erforderlich sind, wenn das Anwendungs-/Trafficverhalten nicht dem Standard entspricht
- Einrichtung einfacher und komplexer Bedingungen für verschiedene Anfragemerkmale wie IP, Standort, Header, Payload usw.
- Proaktive Abwehr von Bedrohungsquellen, die bei WAF-Angriffen auf Ihre Anwendungen bzw. bei WAF-Scans dieser Anwendungen erkannt wurden (mit Penalty Box)
- Änderung des Debug-Headers
- Änderung der Prüfgröße für die Anfrage-Payload oder der Protokollierungseinstellungen für die Angriffs-Payload
- Simulation von Änderungen in der Erkennungslogik, um diese Änderungen sicher auf die Produktion zu übertragen

Überprüfung in der realen Welt

Der Evaluierungsmodus bietet Akamai-Kunden Flexibilität und Genauigkeit bei der Konfiguration spezifischer Versionen der Adaptive Security Engine. Kunden können neue Updates oder Änderungen sehen, bevor sie sich entscheiden, sie zu aktivieren, weil sie angemessen oder notwendig für die jeweilige Webanwendungsumgebung sind. Wir bei Akamai sind davon überzeugt, dass im Hinblick auf eine effektive Modernisierung der Sicherheit Tests mit Echtzeit-Traffic bessere Sicherheitsergebnisse liefern als Tests mit bisherigem Traffic. Der Evaluierungsmodus ähnelt der Anwendung einer Schattenregel: Sie können die Echtzeitergebnisse so sehen, als ob die Richtlinie durchgesetzt würde, jedoch ohne Auswirkungen auf aktuelle Endnutzer. Unternehmen können diesen manuellen Betriebsmodus bzw. Evaluierungsmodus wählen, um unerwartete Auswirkungen auf False Positives und False Negatives zu minimieren.

Integration modernisierter Schutzmechanismen

Sicherheits- und DevOps-Teams können die Sicherheit auch operationalisieren, indem sie Aufrufe an Akamai-APIs über die CLI, Akamai Terraform oder Skripte in ihre CI/CD-Automatisierungspipeline integrieren. Die flexible Konfiguration und Automatisierung sorgen dafür, dass das Entwicklungstempo niemals durch Sicherheitsabläufe beeinträchtigt wird. Diese Integrationen ermöglichen Folgendes:

- Schnelles Onboarding von Anwendungen
- Einheitliche Verwaltung von Sicherheitsrichtlinien für große Anwendungsportfolios
- Zentralisierte Durchsetzung der Sicherheit über Hybrid- und Multi-Cloud-Infrastrukturen hinweg
- Verbesserte Zusammenarbeit zwischen DevOps und Sicherheitsteams in einem GitOps-Workflow für optimale Abdeckung

Darüber hinaus können Sie mit SIEM (Security Information and Event Management) Sicherheitsereignisse erfassen, die auf der Akamai-Plattform stattfinden. Im Gegenzug bietet unsere SIEM-Integrationslösung die Möglichkeit, SIEM-Ereignisse an On-Premises- und cloudbasierte SIEM-Analysetools wie Splunk und QRadar zu übermitteln. So können Sie Sicherheitsereignisse von Akamai in vier grundlegenden Schritten in Ihre gesamte Ereignis- und Sicherheitsinfrastruktur integrieren.

Sie können Ihren Datenfeed mit folgenden Funktionen schützen und kontrollieren:

- **Ereignisfilterung**
  Verwenden Sie Sicherheitskonfigurationen und -richtlinien, damit Sie sich auf echte Bedrohungen konzentrieren können.
- **Datenaufbewahrung**
  Der Collector speichert Daten 12 Stunden lang, damit Sie verpasste Ereignisse erfassen können.
- **SIEM-Überlastungsschutz**
  In Ihrem SIEM-Connector können Sie die maximale Anzahl von Sicherheitsereignissen definieren, die in einer einzelnen Anfrage abgerufen werden. Dadurch vermeiden Sie eine Überlastung der SIEM-Anwendung.
- **Abrufintervall**
  Sie können festlegen, wie oft die SIEM-Connectors die SIEM-API aufrufen, um Daten zu Sicherheitsereignissen abzurufen.

Anwendungssicherheit und DDoS-Abwehr

Anwendungssicherheit ist ein entscheidender Aspekt moderner Cybersicherheit, denn sie sorgt dafür, dass Anwendungen gegen eine Vielzahl von Bedrohungen und Schwachstellen geschützt sind. Ihre Bedeutung liegt in mehreren Schlüsselbereichen: Sie ist entscheidend für Datenintegrität und Vertraulichkeit, da sie gewährleistet, dass vertrauliche Daten vor unbefugtem Zugriff und Manipulation geschützt sind. Anwendungssicherheit spielt auch eine wichtige Rolle für die Geschäftskontinuität, da sie Anwendungen vor Unterbrechungen durch Sicherheitsvorfälle schützt und so eine konstante Serviceverfügbarkeit gewährleistet. Darüber hinaus ist Anwendungssicherheit für das Reputationsmanagement von entscheidender Bedeutung, denn sie verhindert Sicherheitsverletzungen, die den Ruf eines Unternehmens schädigen und das Vertrauen der Kunden untergraben können. Und schließlich trägt sie dazu bei, dass Unternehmen gesetzliche Anforderungen erfüllen und so rechtliche Sanktionen und Geldstrafen vermeiden.

Die Funktion einer WAAP-Lösung besteht darin, den HTTP-Traffic zwischen Webanwendungen und dem Internet zu filtern und zu überwachen. Dieser Ansatz schützt vor gängigen webbasierten Angriffen wie XSS, SQL-Injection und DDoS.

App & API Protector ist für seinen marktführenden DDoS-Schutz bekannt. Dieser ist auf die Abwehr volumetrischer Angriffe ausgelegt, die auf eine Überlastung von Ressourcen abzielen. Die Lösung bekämpft DDoS auf folgende Weise:

- **Edge-basierte DDoS-Abwehr**
  Durch die Nutzung der global verteilten Edge-Plattform von Akamai kann App & API Protector DDoS-Angriffe sofort abwehren, bevor sie den Ursprung der Anwendung erreichen. Dieser Edge-basierte Ansatz sorgt für minimale Latenz und maximalen Schutz, ohne die Performance der Anwendung zu beeinträchtigen.

- **Ratenbegrenzung**
  App & API Protector beinhaltet eine adaptive Ratenbegrenzung zur Abwehr verteilter DDoS-Angriffe auf Anwendungsebene. Diese Kontrollen können so konfiguriert werden, dass die Rate der eingehenden Anfragen auf Grundlage verschiedener Kriterien begrenzt wird. Zu diesen Kriterien gehören unter anderem IP, Standort, IP-Reputation, verschiedene HTTP-Header und Auslösebedingungen.

- **URL-Schutz mit intelligentem Load Shedding**
  Hier wird ein anderer Ansatz zur Ratenbegrenzung verfolgt. Mit dem URL-Schutz können Sie Ihren Ursprung vor übermäßigen Anfragen schützen, basierend auf der akzeptablen Anfragerate (maximale Anfragen pro Sekunde), die von der Kapazität des Ursprungs abhängt. Er wurde speziell entwickelt, um rechenintensive URLs, API-Endpunkte usw. vor stark verteilten DDoS-Angriffen auf Anwendungsebene zu schützen.

- **Behavioral DDoS Engine**
  Die Behavioral DDoS Engine ist neu in App & API Protector und stellt ein leistungsstarkes Tool für gestaffelte Sicherheit dar. Sie bietet einen automatisierten Ansatz zur Verwaltung und Abwehr von DDoS-Ereignissen, indem mittels ML Traffic-Baselines festlegt und Abweichungen von der Norm erkennt. Die Engine versteht die dynamischen Trafficmuster und ermöglicht es Nutzern, zu definieren, wie das System auf verschiedene Anomalien reagiert, ohne explizite Schwellenwerte festzulegen. Dadurch wird der Betriebsaufwand für die Verwaltung und Optimierung des Systems verringert.

- **Automatische Updates und adaptive Selbstoptimierung**
  Mithilfe der Doppel-Engine-Strategie von Akamai (Adaptive Security Engine und Behavioral DDoS Engine) passt sich App & API Protector durch automatische Updates und ML-gesteuerte Selbstoptimierung kontinuierlich an neue Bedrohungen an. Dadurch verringert sich der erforderliche Betriebsaufwand.

Behavioral DDoS Engine: So funktioniert sie

Das Herzstück der Behavioral DDoS Engine ist ein fortschrittliches ML-Modell, das kontinuierlich und in Echtzeit den Traffic überwacht, Baselines für normales Verhalten festlegt und Abweichungen, die auf einen Angriff hinweisen, sofort erkennt. Durch die Analyse von Trafficmustern in mehreren dynamische Dimensionen wie Ursprungsland, TLS-Muster, IP- und TLS-Fingerabdrücke kann diese Engine Anomalien schnell erkennen und Maßnahmen auslösen.

Dies sind einige der wichtigsten Komponenten der Behavioral DDoS Engine:

- **Verhaltensüberwachung in Echtzeit**
  Die Engine analysiert fortlaufend den Traffic, um Baselines für normale Aktivität festzulegen, und erkennt sofort Abweichungen, die potenzielle DDoS-Angriffe signalisieren.

- **Präzision durch maschinelles Lernen**
  Mit fortschrittlichen ML-Modellen kann die Engine subtile Anomalien in den Trafficmustern erkennen. So gewährleistet sie eine präzise Abwehr, ohne legitime Nutzer zu blockieren.

- **Proaktive Abwehr**
  Durch die Nutzung der globalen Netzwerkeinblicke von Akamai (1.056 TB Traffic pro Tag) kann die Engine Angriffe vorhersagen und neutralisieren, oft bevor sie sich auf Unternehmen auswirken können.

- **Mehrdimensionale Analyse**
  Der Traffic wird über mehrere Dimensionen hinweg bewertet, darunter IP, Land und TLS-Muster. Das bietet einen zuverlässigen Schutz, der auf die Anforderungen der einzelnen Anwendungen zugeschnitten ist.

Fortschrittliche Architektur für hervorragenden Schutz
Die Behavioral DDoS Engine arbeitet mit einer ausgeklügelten Architektur, die mehrere wichtige Komponenten umfasst:

- **Erkennungs-Engine**
  Verwendet dynamische Dimensionen und historische Angriffsdaten, um DDoS-Angriffe in Echtzeit zu identifizieren.
- **Abwehr-Engine**
  Nutzt Informationen aus dem Baseline-Generator sowie Bedrohungssignale, um Angriffe automatisch abzuwehren, wodurch sich der Betriebsaufwand für Sicherheitsteams verringert.
- **Reduktion unnötiger Warnungen / False Positives**
  ML-Modelle filtern irrelevante Daten heraus und stellen sicher, dass sauberer Traffic für Analyse und Abwehr verwendet wird.
- **Baseline-Generator**
  Optimiert kontinuierlich Trafficprofile durch Verarbeitung bereinigter Daten über einen Zeitraum von zwei Wochen, damit die Engine stets die neuesten Angriffsstrategien kennt.
- **Baseline-Validator**
  Mithilfe von KI bewertet diese wichtige Komponente jeden Monat Hunderte von DDoS-Angriffen, um die Lösung zu optimieren.

Dieses automatisierte Framework stellt sicher, dass sich Sicherheitsteams darauf verlassen können, dass die Engine ihre Abwehrmechanismen auch ohne manuelle Eingriffe dynamisch anpasst. Die Lösung erkennt anormale Traffic-Aktivität, wie zum Beispiel Bot-generierten Traffic oder DDoS-Versuche, und filtert sie heraus, um Anwendungen effektiv zu schützen.

Genauigkeit der Anwendungssicherheit

Wenn eine Lösung für Anwendungssicherheit (WAF oder WAAP) nicht die nötige Genauigkeit bietet, sind mehr interne Ressourcen erforderlich, um die erhöhte Anzahl täglicher Warnungen zu bewältigen. Ungenauigkeiten können eine große Anzahl von False Positives (bei denen eine Anfrage fälschlich als bösartig gemeldet wird) und False Negatives (bei denen eine Anfrage fälschlich als ungefährlich eingestuft wird) mit sich bringen. Die Folge: Es werden Sicherheitskompetenzen und kostbare Zeit für die Untersuchung und Analyse dieser Warnungen verschwendet.

Unternehmen erleben häufig eine gewisse Abstumpfung gegenüber Warnungen. Doch sie haben keine Lösung für das Problem, dass Kontrollen zu umfassend sind und Funktionen zu genau oder zu ungenau arbeiten. Das führt häufig dazu, dass Unternehmen ihre WAF offline schalten – oder schlimmer noch: die Warnungen und Versionsupdates ignorieren. So werden zwar nicht mehr so viele legitime Nutzer blockiert, jedoch sind Anwendungen und APIs auch nicht mehr so gut vor Angriffen geschützt. In vielen Unternehmen fehlt es Kontrollen zudem an Genauigkeit, sodass sie keine präzise Balance zwischen dem Zulassen von legitimem und dem Blockieren von schädlichem Traffic finden können.

Der Vorteil einer effektiven WAAP-Lösung besteht darin, dass sie mit umfassenden WAAP-Kontrollen und -Funktionen sowohl False Positives als auch False Negatives verringert, um die Präzision zu erhöhen und die Auswirkungen auf legitime Nutzer zu minimieren.

Was bedeutet „Genauigkeit“?

Der Begriff „Genauigkeit“ beschreibt die Fähigkeit einer WAF oder WAAP, Angriffe aufzuhalten, aber legitime Nutzer dabei nicht zu blockieren. Dabei werden vier Variablen berücksichtigt:

- **True Positives (TPs):** Echte Angriffe, die ordnungsgemäß als bösartig identifiziert werden
- **False Positives (FPs):** Legitime Anfragen, die fälschlicherweise als schädlich identifiziert werden
- **True Negatives (TNs):** Legitime Anfragen, die an die Anwendung weitergeleitet werden
- **False Negatives (FNs):** Echte Angriffe, die fälschlicherweise an die Anwendung weitergeleitet werden

Client-Reputationsbewertung

Client Reputation verwendet eine ausgeklügelte Risikoanalyse-Engine, um für jede IP-Adresse, die versucht, auf Ihre Website zuzugreifen, eine Reihe von Risikobewertungen zu berechnen. Es analysiert die eingehenden IP-Adressen und verwendet verschiedene Faktoren (wie die Persistenz des Angreifers, die Anzahl der angegriffenen Anwendungen, den Schweregrad und das Ausmaß des Angriffs, die Branche sowie frühere Angriffe auf Kundenanwendungen), um eine Bewertung zu ermitteln, die angibt, wie wahrscheinlich diese IP-Adresse an einem Webangriff der folgenden Art beteiligt ist:

- **DOSATCK**
  Verwendet Botnets, um DoS-Angriffe (Denial-of-Service) zu starten. Das Ziel eines DoS-Angriffs besteht darin, eine Website mit so vielen falschen Anfragen zu überfluten, dass die Website unerträglich langsam wird oder sogar abstürzt. Bei einem DDoS-Angriff (Distributed Denial-of-Service) kommen diese Anfragen von Tausenden von Orten (in der Regel mit Malware infizierte Computer oder Telefone), wodurch es unmöglich ist, den Angriff einfach durch Blockieren einer bestimmten IP-Adresse zu stoppen.

- **SCANTL**
  Scan-Tools können potenzielle Sicherheitsrisiken wie SQL-Injection, Cross-Site Request Forgery (CSRF), ungültige Umleitungen und andere Schwachstellen identifizieren. Es empfiehlt sich, ein Webscan-Tool für die eigene Website anzuwenden. Kriminelle ein Scantool auf Ihrer Website ausführen zu lassen, ist weniger empfehlenswert.

- **WEBATCK**
  Verwendet Techniken wie SQL-Injection, Remote File Inclusion oder Cross-Site Scripting, um Malware zu installieren oder Nutzerdaten zu stehlen. Ein Hacker kann all Ihre Nutzerdaten abrufen, die Sie möglicherweise in der Nutzerdatenbank gespeichert haben, einschließlich Passwörtern, Kreditkartennummern, Sozialversicherungsnummern und anderen Informationen.

- **WEBSCRP**
  Verwendet automatisierte Tools, um eine Kopie einer Webseite herunterzuladen und anschließend den gesamten Inhalt dieser Seite zu „scrapen“ (also zu kopieren). Der Inhalt kann dann für illegale oder unethische Zwecke verwendet werden.

Mit Client Reputation können Sie die gesammelte Threat Intelligence der Akamai Connected Cloud nutzen, um Ihr Unternehmen proaktiv vor verdächtigen Bedrohungsquellen schützen.

Malware-Schutz

Angreifer nutzen häufig Malware als Angriffstaktik. Für einen umfassenden Schutz von Anwendungen bietet Akamai auch eine Lösung zum Schutz vor Malware. Unternehmen jeder Größe erlauben Datei-Uploads, um intern wie extern effiziente Abläufe zu gewährleisten. Hier sind einige typische Fälle aus der Praxis:

- Lebensläufe für Bewerbungen
- Arbeitsverträge, Onboarding, E-Verify, Einrichtung von Direkteinzahlungen und vieles mehr
- Anträge, einschließlich Darlehen, Kontoeinrichtung und Kreditanträge
- Kostenvoranschläge für Versicherung oder Reparatur von Auto, Haus und mehr
- Patientenakten für Versicherungen oder die Einrichtung von Patientenkonten
- Kundenrezensionen zu Produkten oder Erfahrungsberichte, die Bilder beinhalten

Malware-Schutz innerhalb der App- und API-Sicherheit erkennt und isoliert Malware-Bedrohungen an der Edge, bevor sie das anvisierte Unternehmenssystem erreichen. Unternehmen können Zeit, Budget und Produktivität sowie interne Daten und Kundendaten schützen, indem sie sich die Vorteile des Malware-Schutzes für Apps und APIs zunutze machen:

- **Malware an der Edge erkennen und blockieren**
  Vermeiden Sie das Risiko von Scans auf Servern, auf denen sich die Malware zum Zeitpunkt des Scans bereits ausgebreitet haben könnte.
- **Komplexität vermeiden und Zeit sparen**
  Scannen Sie Dateien nur einmal, anstatt wie bei ICAP und agentbasierten Scannern den Schutz in jedem System individuell einzurichten.
- **Sicherheit auf Wachstum ausrichten**
  Durch die Wahl eines präventiven und mehrschichtigen Ansatzes können Unternehmen den Schutz an ihr Wachstum anpassen. So erhalten sie zusätzlichen Schutz an der Edge und die Option, erneut am Ursprung zu scannen.
- **Beständige Anwendungssicherheit gewährleisten**
  Unternehmen müssen den Anwendungscode weder konfigurieren noch ändern. Der Malware-Schutz wird vollständig in der Akamai Connected Cloud gehostet.

Analyse der Anwendungssicherheit

In App & API Protector ist auch das beliebteste (und am meisten verwendete) Produkt von Akamai enthalten:
Web Security Analytics. Mit dieser WAAP-Lösung können Sie auf der Akamai-Plattform die Sicherheitsvorfälle erfassen, die Ihre Webanwendungen und APIs betreffen, und sie in den bereitgestellten Analysetools visualisieren.

Web Security Analytics ist eine wichtige Komponente moderner Cybersicherheit und bietet umfassende Einblicke in den Webtraffic und in potenzielle Bedrohungen. Durch die Analyse einer Vielzahl von Datenpunkten, einschließlich Trafficmuster, Nutzerverhalten und Sicherheitsvorfällen, bietet die Lösung detaillierte Einblicke in die Sicherheitslage von Webanwendungen. Dieser proaktive Ansatz ermöglicht es Unternehmen, Bedrohungen effektiver zu erkennen und zu behandeln und Risiken zu minimieren, bevor sie erhebliche Schäden verursachen können. Web Security Analytics unterstützt nicht nur die Identifizierung schädlicher Aktivitäten wie Bot-Angriffe, SQL-Injection und Cross-Site Scripting. Es trägt auch dazu bei, Schwachstellen in Webanwendungen zu verstehen und zu beheben. Darüber hinaus unterstützt es Compliance-Bemühungen, indem es Berichte generiert, die die Einhaltung von Sicherheitsrichtlinien und gesetzlichen Anforderungen nachweisen.

API-Erkennung und -Profilerstellung

Mit APIs können Unternehmen ihren Nutzern leistungsstarke Webanwendungen und mobile Apps bereitstellen, wobei häufig Backend-Daten und -Logik offengelegt werden, um neue und innovative Angebote zu entwickeln. APIs vergrößern jedoch auch die Angriffsfläche. Unternehmen müssen wissen, welche API-Endpunkte sich in ihrer Umgebung befinden, welche Funktionen die APIs haben und wie ihre Trafficprofile aussehen. Die API-Erkennung und -Profilerstellung von Akamai ermöglicht genau das und noch mehr – automatisch und kontinuierlich.

Die Funktion für API-Erkennung macht Sicherheitsteams auf neue, häufig ungeschützte Anwendungen und APIs aufmerksam, die mit verschiedenen Geschäftsbereichen in einem Unternehmen verknüpft sind. Diese automatisierte Erkennungstechnologie ist eine neue Funktion der Akamai-WAAP-Lösung. Sie sorgt dafür, dass Entwicklungsteams, Führungskräfte und Sicherheitsteams stets aufeinander abgestimmt sind.

Die Adaptive Security Engine erkennt automatisch alle 24 Stunden APIs basierend auf einem Bewertungsmechanismus, der den Inhaltstyp der Antwort, die Pfadeigenschaften sowie Trafficmuster berücksichtigt. Die Erkennungsdaten enthalten Informationen zur beobachteten API-Spezifikation mit Details wie den folgenden:

- Hostname
- Basispfad
- Ressourcenpfad
- Parameter und ihr Datentyp
- Methoden
- Format der API

Basis- und Ressourcenpfade werden anhand eines Algorithmus bestimmt, der die Pfadtiefe, die Anzahl untergeordneter Pfade sowie die gleichgeordneten Pfade im beobachteten Traffic eines bestimmten Hostnamens mit API-Traffic berücksichtigt. Wenn innerhalb des Ressourcenpfads ein Parameter für eine bestimmte Methode beobachtet wird, wird er markiert und der Datentyp dieses Parameters wird identifiziert.

Das Trafficprofil für die API-Endpunkte enthält Informationen, die Aufschluss über den Zweck der API und die aktuelle Bedrohungsstufe geben. Einige der Datenpunkte sind:

- Gesamte Anfragen seit der ersten API-Erkennung, sowohl in den letzten 24 Stunden als auch im Zeitverlauf
- Datum, an dem die API zum ersten Mal entdeckt und zum letzten Mal gesehen wurde
- Anzahl der Anfragen über verschiedene Methoden wie GET, PUT, POST, DELETE und OPTIONS
- Anzahl der Anfragen, die 2xx-, 3xx-, 4xx- und 5xx-Antworten generieren
- End-Client-Identifizierung basierend auf User Agent
- Antwortfehler, wie der Prozentsatz des Traffics, der zu Client- und serverseitigen Fehlern führt
- Hits von bekannten Cyberkriminellen, einschließlich des Prozentsatzes des gesamten Traffics, der von bekannten Cyberkriminellen auf die Akamai-Plattform übertragen wird, aufgeteilt nach Webangreifern, Webscannern, Scrapern und DoS-Angreifern

Der Schutz von APIs kann ohne die nötige Transparenz eine große Hürde darstellen. Wie schützt ein Unternehmen das, was es nicht sehen kann? Mit Akamai können Unternehmen APIs automatisch und kontinuierlich erkennen und ein Profil erstellen, einschließlich Endpunkten, Definitionen sowie Ressourcen- und Traffic-Eigenschaften. Sobald APIs identifiziert wurden, bietet Akamai umfassenden Schutz gegen DoS, Injection von Schadcode, Missbrauch von Anmeldedaten und Verstößen gegen API-Spezifikationen schützen. Der cloud- und ursprungsunabhängige Ansatz von Akamai ermöglicht eine einfache API-Erkennung über eine gesamte Anwendungsumgebung hinweg – ohne zusätzliche Konfigurationen für den Endnutzer. Diese Transparenz ermöglicht es Entwicklern, Anwendungseigentümern und Sicherheitsteams, neuen, unbekannten oder sich ändernden APIs einen Schritt voraus zu sein und sie zu Schutzzwecken leicht zu registrieren.

Bot-Transparenz und -Abwehr

Da Bots mehr als die Hälfte des Website-Traffics ausmachen, lässt sich oft nur schwer herausfinden, welche Bots Ihrem Unternehmen dabei helfen, seine Ziele zu erreichen, und welche nur Schaden verursachen. Gute Bots sorgen für Effizienz im Unternehmen, indem sie Bewertungen, Konversationen oder Empfehlungen automatisieren. Schlechte Bots können Trafficpfade verstopfen und das Kunden- und Betriebserlebnis beeinträchtigen, was sich auf den Umsatz auswirkt. Innerhalb von App & API Protector bietet Bot-Transparenz und -Abwehr leistungsstarke Erkennung, mit der gute Bots identifiziert und durchgelassen, aber schlechte Bots blockiert werden. Das eröffnet Unternehmen folgende Möglichkeiten:

- **Bots sehen und ihre Auswirkungen verstehen**
  Die Transparenz des Bot-Traffics ist für moderne digitale Unternehmen von entscheidender Bedeutung, da Bots häufig für Vorgänge wie Suchen, die Überprüfung der Website-Performance oder die Interaktion mit Geschäftspartnern zum Einsatz kommen.
- **Operative Kontrolle verbessern**
  Das Blockieren schädlicher Bots steigert die Effizienz, reduziert Geschäfts- und Finanzrisiken und ermöglicht eine bessere Kontrolle der IT-Ausgaben.
- **Bessere, datengesteuerte Entscheidungen treffen**
  Dank detaillierter Analysen und detailliertem Reporting können Sie kreative und effektive Entscheidungen hinsichtlich Customer Journeys, Sicherheitsstruktur, Risikotoleranz und IT-Prozessen treffen.

Bot-Transparenz und -Abwehr in App & API Protector

App & API Protector bietet Bot-Erkennung und Kontrollen für Bot-Traffic, der sich nachteilig auf die Performance und Sicherheit von Webressourcen auswirken kann. Die Lösung bietet frühzeitige Einblicke und ermöglicht so eine proaktive Überwachung auf Bot-bezogene Anomalien und Bedrohungen, die sich im Laufe der Zeit entwickeln.

Mit der in App & API Protector bereitgestellten Bot-Lösung von Akamai haben Sie folgende Möglichkeiten:

- Greifen Sie auf mehr als 1.700 definierte Bots zu, die Akamai bekannt sind.
- Erhalten Sie Echtzeit-Einblicke in den Bot-Traffic.
- Erstellen Sie individuelle Bot-Definitionen.
- Lassen Sie gute Bots zu und blockieren Sie schlechte.
- Erhalten Sie Bot-Einblicke und Trendberichte.

Für Websites mit fortgeschrittenen Bot-Problemen bietet Akamai Bot Manager an, der erweiterten Bot-Schutz für gesteigerte E-Commerce- und digitale Sicherheit bereitstellt. Bot Manager bietet präzisere Aktionen für persistente, schädliche Bots, wie sie zum Beispiel für folgende Angriffe verwendet werden:

- Credential Stuffing
- Bestandsmanipulation
- Inhalts- und Preis-Scraping
- Missbrauch der Geschäftslogik

Wichtige Bot-Funktionen

Akamai erkennt den wachsenden Bedarf für Bot-Verwaltung über WAAP und hat seine Tools für Bot-Transparenz und -Abwehr entsprechend um neue Funktionen erweitert:

- **Erkennung von Browser-Imitation**
  Diese bei Kunden beliebte Funktion von Akamai Bot Manager verwendet dynamische Scoring-Modelle und ML, um Bot-Aktivitäten auf Browser-Ebene zu erkennen und ihnen entgegenzuwirken. Sie ist in App & API Protector enthalten.
- **Bedingungsabhängige Maßnahmen**
  Kunden haben nun ein besseres Verständnis der Bot-Aktivitäten auf Browser-Ebene und können mit bedingten Aktionen reagieren, um verschiedene Reaktionsstrategien gegen bösartige Bots anzuwenden.
- **Challenge-Aktionen**
  Gehen Sie Bots mit einer Reihe verschiedener Challenge-Aktionen an. Dazu gehören zum Beispiel Interstitial Challenges, bei denen der Zugang zu Inhalten blockiert werden kann, wenn die Challenge nicht gelöst wird.

Mehr als eine WAF: Vorteile der Akamai-Lösung

Der WAAP-Ansatz von Akamai hat die Lösung App & API Protector hervorgebracht. Es gibt jedoch mehr als nur ein Produkt, von dem unsere WAAP-Kunden profitieren können. Akamai Connected Cloud basiert auf der am stärksten verteilten globalen Plattform und wird von Hunderten von Bedrohungsexperten unterstützt. Sie bietet Performance, Verfügbarkeit, Informationen, Fachwissen und effektive Sicherheitsergebnisse.

Threat Intelligence und Bedrohungserkennung

Die Fähigkeit, intern umfangreiche Bedrohungsinformationen zu ermitteln, ermöglicht es WAAP-Anbietern, auf immer neue Bedrohungen zu reagieren. Hierbei bestimmen Qualität, Rechtzeitigkeit und Verwertbarkeit der Informationen darüber, ob und inwieweit sie die Effektivität der Anwendungssicherheit verbessern können. Akamai analysiert kontinuierlich die über Akamai Connected Cloud verfügbaren Daten, um aktuelle Trends in der Bedrohungslandschaft, neue Angriffsvektoren und derzeit aktive Angreifer zu ermitteln. Akamai integriert diese Erkenntnisse dann auf unterschiedliche Weise in seine WAAP-Lösung.

Die Akamai Adaptive Security Engine, die weiter oben in diesem Whitepaper bereits vorgestellt wurde, kombiniert zwei Ebenen tiefgreifender Threat Intelligence zu einer leistungsstarken Engine, mit der die neuesten Schutzmechanismen für unsere Kunden automatisch verwaltet werden können. Zusätzlich zu ML und der automatisierten Regelübernahme bietet die Adaptive Security Engine Bedrohungsinformationen von der globalen Akamai-Plattform sowie ein großes Team aus spezialisierten Bedrohungsforschern.

Threat Intelligence der Akamai-Plattform

Akamai betreibt eine der größten globalen Plattformen und verfügt damit über einen geeigneten Mechanismus, um sämtlichen gegen Akamai-Kunden gerichteten Angriffstraffic rechtzeitig und auf globaler Ebene zu analysieren. Unsere Intelligence-Datenbank enthält durchschnittlich 1.056 TB Angriffsdaten pro Tag. Sie nutzt unsere Einblicke in den Webtraffic Tausender der größten, meistfrequentierten und am häufigsten angegriffenen Online-Unternehmen, um relevante und hochwertige Daten zu gewinnen, die anschließend durch das Akamai Threat Research Team analysiert werden:

- **WAAP-Auslöser**
  Bezieht Daten direkt aus den weltweiten WAAP-Bereitstellungen von Akamai und erfasst dabei echte Angriffsereignisse, von denen alle Akamai-Sicherheitskunden betroffen sind.
- **CDN-Protokolle**
  Integriert Offlineanalysen der Ereignisprotokolle aller Akamai-Kunden – auch solcher, die nicht die WAAP-Lösung von Akamai implementiert haben.

Die Intelligence-Datenbank von Akamai enthält einen der größten Datensätze der Welt (9 PB). Bei Unternehmen, für die ihre eigene Sicherheit und die Sicherheit ihrer Kunden Priorität haben, ist Akamai mit seinen Threat-Intelligence-Teams der führende WAAP-Lösungsanbieter.

Bedrohungsforschung und Vorfallreaktion

Anbieter von Bedrohungsforschung und Vorfallreaktion stellen Fachwissen und Analysen bereit, um die Abdeckung einer WAAP-Lösung zu ergänzen und auszuweiten. Akamai setzt verschiedene Teams mit unterschiedlichen Aufgaben ein, um seine WAAP-Kunden zu unterstützen und neue Angriffsvektoren zu ermitteln, die möglicherweise nach neuen Schutzmechanismen verlangen.

Bedrohungsforschung

Das Akamai Threat Research Team führt regelmäßig und über die gesamte Akamai-Kundendatenbank hinweg Analysen von Angriffstrends sowie ggf. individuelle Analysen für einzelne Kunden durch. Das Team entwickelt und implementiert Heuristiken, um verwertbare Informationen abzufragen und die Erstellung und Aktualisierung der zentralen WAF-Regellogik und der Client-Reputation zu unterstützen.

Vorfallreaktion

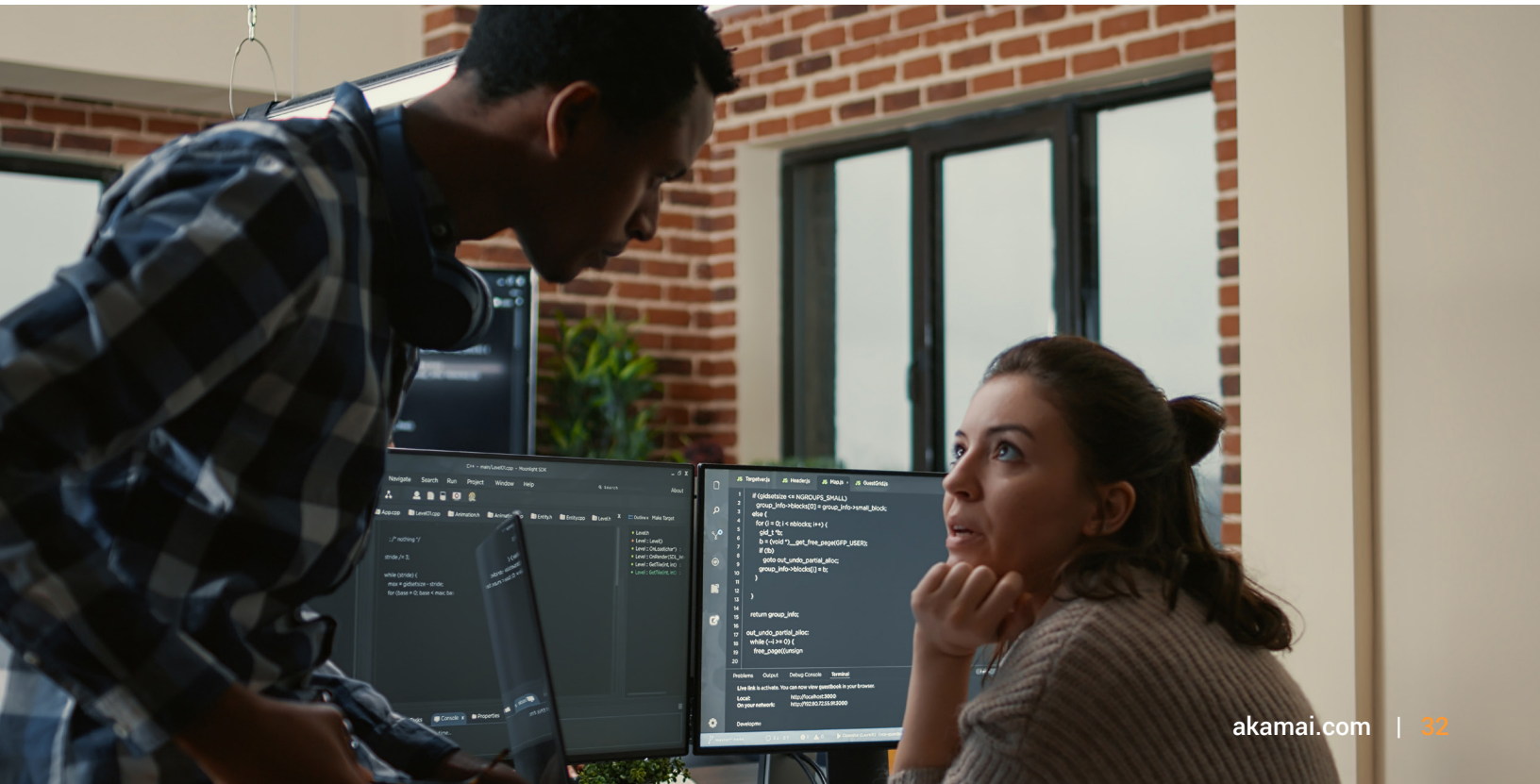
Akamai betreibt zwei Teams zur Vorfallreaktion: das Computer Security Incident Response Team (CSIRT) und das Security Intelligence Response Team (SIRT). Diese beiden Teams arbeiten gemeinsam mit dem Security Operation Center (SOC), um individuelle Analysen und Vorfallreaktionen für einzelne Kunden bereitzustellen, wenn diese angegriffen werden. Darüber hinaus überwacht das CSIRT häufig angegriffene Akamai-Kunden aus vielen verschiedenen Branchen, um Hinweise auf neue Angriffsvektoren oder -trends zu ermitteln.

Schnelle Erkennung von Bedrohungen

Unsere neuen Funktionen ermöglichen eine schnelle Bereitstellung von Schutzmechanismen gegen neue Bedrohungen und wichtige CVEs. Automatische Updates und optional von Akamai verwaltete Aktionen sorgen dafür, dass Sie Ihre Abwehrmaßnahmen flexibel steuern können.

CVE-Schutz

Das Akamai Threat Research Team überwacht kontinuierlich gängige Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVEs) und stellt sicher, dass die WAAP-Lösung entsprechend aktualisiert wird. So bleiben Kundenanwendungen geschützt und die erforderlichen Informationen sind über die CVE-Suche von Akamai verfügbar. Dieses Tool bietet detaillierte Informationen zu CVEs, einschließlich Bedrohungsstufen und Einblicken in die aktuellen Schutzmaßnahmen von Akamai. Der CVE-Schutzkatalog von Akamai bietet Ihnen Transparenz, damit Sie Sicherheitsmaßnahmen in Übereinstimmung mit den Schutzmaßnahmen von Akamai priorisieren können. Sie können die CVE-Datenbank durchsuchen, um die bestehenden Schutzmaßnahmen von Akamai gegen eine Schwachstelle zu ermitteln, die Bedrohungsstufe zu bewerten und auf CVE-Details zuzugreifen.



Global verteilte Edge-Plattform

Zuverlässigkeit und Resilienz

Premium-WAAP-Lösungen basieren auf umfangreichen, leistungsstarken Netzwerken, die selbst bei sehr großen Cyberangriffen den legitimen Traffic der Kunden nicht einschränken. Die nachweisliche Qualität, Kapazität und Reaktionsfähigkeit der globalen Plattform eines WAAP-Anbieters sind für die Funktionen seiner Lösung gleichermaßen wichtig. Wenn ein WAAP-Anbieter während eines aktiven Angriffs nicht gewährleisten kann, dass legitimer Traffic weitergeleitet wird, sollten Kunden prüfen, ob sie in eine Lösung oder lediglich in ein Tool investiert haben.

Akamai hat den Anspruch, seinen Kunden branchenführende Performance und Sicherheit zu bieten. Diese Mission können wir nur erfüllen, weil unsere Services auf einem sehr starken Fundament aufbauen: Akamai Connected Cloud. Akamai hat die weltweit am weitesten verteilte Cloudplattform mit mehr als 4.200 Edge-Standorten in über 130 Ländern entwickelt.

Zu den Kunden von Akamai gehören jeweils die Top 10 der führenden Broker, Banken, Videostreaming-Dienste und Gaming-Unternehmen. Unser Kundenstamm umfasst einen Großteil der führenden Automobilkonzerne, Gesundheitsdienstleister, Einzelhändler und Telekommunikationsanbieter, eine erhebliche Anzahl von Regierungsbehörden sowie das US-amerikanische Militär.

Diese Kunden vertrauen auf die Fähigkeit von Akamai, sie vor 40 Milliarden Bots pro Tag, 780 Millionen Anwendungsangriffen pro Tag und 1.889 DDoS-Attacken pro Quartal zu schützen, um Bedrohungen für ihren Netzwerkbetrieb abzuwehren. Akamai sorgt für optimale Sicherheit, da die Bedrohungsinformationen, die bei einem Kunden gewonnen werden, auch dem Schutz aller anderen Kunden zugute kommen. Aufgrund ihrer Größe liefert die globale Akamai-Plattform die erforderliche Datenquantität und -qualität, die Unternehmen im KI-Zeitalter für ihre Sicherheit benötigen.

Weltweite Skalierung

Für eine WAF dreht sich das Thema Skalierung nur um zwei Aspekte: die Fähigkeit, das aufkommende Trafficvolumen untersuchen zu können – sowohl zum aktuellen Zeitpunkt als auch mit zunehmender Trafficmenge –, sowie die Anzahl von WAF-Regeln, die zur Bewertung des Traffics erforderlich sind. Klassische hardwarebasierte WAF-Lösungen bieten oft nur eine unzureichende Skalierung, da sie auf die verfügbaren CPU- und Arbeitsspeicherressourcen der Appliance angewiesen sind und sich diese vielleicht sogar noch mit anderen Lösungen auf derselben Appliance teilen müssen.

Wird eine integrierte WAAP-Lösung jedoch auf der Cloudplattform von Akamai implementiert, so ist das Problem der unzureichenden Skalierung beseitigt, da zur Überprüfung des eingehenden Webtraffics die Ressourcen der weltweit verteilten Akamai-Server genutzt werden. Nutzer und Angreifer stellen über den nächstliegenden Akamai-Server Verbindungen zu geschützten Websites her. Hier wird der Traffic dann auf Angriffe untersucht und erkannte schädliche Anfragen werden blockiert. So bietet die WAAP-Lösung von Akamai an jedem Nutzerstandort weltweit nahtlose Skalierung unabhängig von der Zunahme des Trafficvolumens, das bei Ihrer Webanwendung eingeht – sowohl bei plötzlichen Trafficspitzen als auch bei langfristigem Wachstum.

Performance

Eine schlechte Performance kann die Bereitstellung einer Sicherheitslösung behindern, insbesondere bei einer WAAP-Lösung, die inline vor einer Anwendung bereitgestellt wird. Die Performance-Minderung von Websites, die für das Unternehmen wichtig sind, kann eine niedrigere Produktivität, ein schlechtes Nutzererlebnis, eine verzögerte Markteinführung und eine verringerten Umsatz nach sich ziehen.

Dank der weltweiten Skalierung der Akamai-Cloudplattform können die WAAP-Lösungen Webanwendungen schützen, ohne dabei die Performance einzuschränken. Die global verteilte WAAP untersucht den HTTP-Traffic, wenn er auf der Plattform eingeht, und teilt dabei die CPU- und Arbeitsspeicherressourcen, die für die Untersuchung des Traffics erforderlich sind, gleichmäßig auf alle Plattformserver auf. So werden Performanceprobleme als Quelle für interne Effizienz- und Bereitstellungsprobleme beseitigt.

Mehr Schutz dank Edge-Plattform

Die cloudunabhängigen Akamai-Sicherheitslösungen für Webanwendungen funktionieren nahtlos über die gesamte Plattform hinweg und wehren eine Vielzahl von anwendungs- und API-basierten Angriffen ab. Die Abbildung unten zeigt den gesamten Stack der mehrschichtigen Sicherheitsmechanismen und -kontrollen von Akamai, mit denen Bedrohungen weit vom Ursprung ferngehalten werden. Gleichzeitig verbessern sie die Performance und den Zugriff für legitime Nutzer.

Akamai App & API Protector umfasst eine breite Palette von automatisch integrierten Sicherheitsmechanismen und Kontrollen (blau dargestellt) für einen sofort einsatzbereiten, umfassenden Schutz. Für vollständigen Layer-7-Schutz werden zusätzliche Akamai-Produkte und -Services hinzugefügt.

Verwaltete Angriffsabwehr

Zusätzlich zur dauerhaften WAAP-Verwaltung bietet Akamai seinen Kunden auch einen verwalteten Service zur Angriffsabwehr an. Dieser umfasst die Überwachung der geschützten Websites rund um die Uhr sowie die gesteuerte Reaktion auf erkannte Angriffe.

Beim verwalteten Abwehrservice kommen Mitarbeiter des Akamai-SOC zum Einsatz, die wie folgt auf Sicherheitsvorfälle reagieren:

- Reaktion auf WAAP-Warnungen und Kundenanfragen sowie weiterführende Untersuchung der Probleme
- Bestimmen der entsprechenden Angriffssignaturen und Einleiten zusätzlicher Abwehrmaßnahmen
- Zusammenarbeit mit den Anwendungsteams des Kunden, um die Effektivität und Genauigkeit der eingesetzten Abwehrmaßnahmen zu messen und ggf. anzupassen
- Nach dem Vorfall: Aktualisieren der allgemeinen Vorfallreaktion mit den Anwendungsteams des Kunden
- Bereitstellung von Schaltflächen für Angriffswarnungen in der Nutzeroberfläche, über die eine Notfallsupport-Anfrage initiiert werden kann

Security Operations Command Center (SOCC)

Das SOCC von Akamai leistet seit über 10 Jahren einen Beitrag zur Abwehr von vielen der weltweit größten Angriffe und schützt Kunden in der äußerst dynamischen globalen Bedrohungslandschaft.

Die Überwachung und Abwehr eines Angriffs erfordert vier Funktionen:

- Globale Transparenz
- Proaktive Überwachung und Warnung
- Agile Angriffsabwehr
- Kontinuierlicher Beratungsservice durch ein erfahrenes Sicherheitsteam

Das SOCC von Akamai bietet diese Funktionen, da es die weltweit größte Sicherheitsinfrastruktur betreibt. Der gesamte Netzwerktraffic läuft über unsere einheitliche Sicherheitsplattform, die Informationen in Echtzeit sammelt. So hat Akamai beispielsweise Sicherheitstrends wie die derzeit starke Zunahme von SQL-Injection-Angriffen ermittelt.

All das hilft dem Sicherheitsteam von Akamai dabei, Kundenbedrohungen schnell, mit maximaler Effektivität und mit minimalen Auswirkungen abzuwehren.

Fazit

Neben DDoS-Angriffen auf Netzwerk- und Anwendungsebene gibt es heute auch neue Formen von automatisierten Bots und gezielten Angriffen über APIs und clientseitige Komponenten. Um dieser Entwicklung zu begegnen, müssen Unternehmen all ihre Webanwendungen, API-Endpunkte, Browser und sämtliche Komponenten der Infrastruktur mit einem umfassenden, gestaffelten Sicherheitskonzept schützen. Um ihre Webanwendungen zu schützen, brauchen Sicherheitsteams Lösungen, die Bedrohungen von mehreren Angriffsvektoren schnell erkennen und abwehren können. Hierzu müssen diese Lösungen den traditionellen Schutz über die Firewall hinaus auch auf verwandte Sicherheitstechnologien ausweiten, um die bestmögliche Bedrohungsabwehr zu gewährleisten.

Akamai bietet mit seinem WAAP-Ansatz ein Lösungspaket an, das in seiner Breite und Effektivität unübertroffen ist, da es alle Technologien bereitstellt, die für moderne Sicherheit erforderlich sind. Wir glauben, dass die führende Sicherheitslösung nicht allein den größten oder beliebtesten Unternehmen der Welt vorbehalten sein sollte. Unser mehrstufiges Portfolio für App- und API-Schutz macht effektive Sicherheit von Webanwendungen für jedes sicherheitsorientierte Unternehmen verfügbar.

Mit einer Sicherheitslösung, die sich fortlaufend weiterentwickelt und anpasst und aus umfassenden Angriffsinformationen Maßnahmen ableitet, unterstützt Akamai globale Unternehmen dabei, ihre Sicherheit zu modernisieren und kontinuierlich zu verbessern. Wir möchten die Sicherheitsteams Ihres Unternehmens mit Informationen, Transparenz, Automatisierung und Beratung unterstützen, damit sie interne Initiativen voranbringen und Angreifer von Ihren Systemen fernhalten können. Aus diesem Grund vertrauen die anspruchsvollsten Marken auf uns, wenn es um den Schutz ihrer Aktivitäten in der digitalen Welt geht.

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. Gemeinsam mit Ihnen können wir auf diese Weise Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X und LinkedIn. Veröffentlicht: 02/25.