Akamai

WHITEPAPER

Angriffsvektoren, die Ihr Kundenvertrauen bedrohen

Sicherheit und Markenvertrauen waren noch nie so stark voneinander abhängig wie heute. Da Anwendungen und APIs immer wichtiger für den Auftritt globaler Marken werden – und weil Cyberangriffe weltweit zunehmen –, ist der Schutz digitaler Anwendungen ohne Beeinträchtigung des Kundenerlebnisses mittlerweile Aufgabe für Sicherheitsteams auf der ganzen Welt geworden.

Starke Kundenerlebnisse schaffen Vertrauen in die Marke, was sich messbar auf die Unternehmensperformance auswirkt. Von der Websiteperformance bis hin zum Datenschutz und allem, was dazwischen liegt, beeinflussen die Sicherheitsentscheidungen, die Unternehmen treffen, das Kundenerlebnis jedoch häufig auf negative Weise. Umständliche Kontrollen, die das Unternehmen schützen, können beim Kunden Reibungspunkte erzeugen, die zu Vertrauensverlust und letztendlich zu Umsatzverlusten führen.

Sicherheitsentscheidungen wirken sich auch auf Wachstum und Innovation aus. Während Unternehmen ihre digitale Expansion fortsetzen und Daten und Anwendungen in die Cloud migrieren, konzentrieren sich unzählige Bedrohungsakteure auf Angriffsvektoren, die sich durch diese Verschiebungen ergeben. Aktuelle Sicherheitslösungen müssen darauf ausgerichtet sein, den wechselnden Taktiken und ausgeklügelten Multi-Vektor-Angriffen (Ausführung verschiedener Arten von Angriffen gleichzeitig oder in schneller Folge) von Cyberkriminellen stets einen Schritt voraus zu sein. Um dieses Ziel zu erreichen, sollten Sie Lösungen auswählen, die Ihr Unternehmen und das Vertrauen Ihrer Kunden in Ihre Marke schützen.

Welche Angriffsvektoren sollten auf Ihrer Liste ganz oben stehen?

Das neueste große Ziel: APIs

Anwendungen steuern nahezu jeden Aspekt Ihres Unternehmens, und APIs (Application Programming Interfaces), die Softwarekomponenten verbinden und die Kommunikation zwischen verschiedenen Anwendungen ermöglichen, sind zu einem neuen bevorzugten Ziel für Bedrohungsakteure geworden. Warum? Weil nur allzu oft Anwendungen und Geschäftsprozesse, die APIs beinhalten, schneller initiiert und bereitgestellt werden, als Sicherheitsteams sie bewerten können, was zu Fehlkonfigurationen und Schwachstellen führt. Diese Schwachstellen sind genau das, wonach Cyberkriminelle suchen. Durch den Missbrauch von Geschäftslogik ermöglichen erfolgreiche API-Angriffe ihnen Zugriff auf Ihre Umgebung, wo sie Daten stehlen und sogar zusätzliche Angriffe starten können. Und sie zielen nicht nur auf APIs ab, die Ihre Web Application Firewall durchlaufen. Selbst wenn APIs von Ihrer WAF authentifiziert werden, können sie immer noch anfällig für Angriffe sein. Das bedeutet, dass Angreifer nun regelmäßig Zielsysteme erkunden, um bestimmte APIs zu identifizieren, die ausgenutzt werden können.

Es ist wichtig, daran zu denken, dass jede API potenziell angegriffen werden kann. In Branchen wie dem Gesundheitswesen hat beispielsweise die Interoperabilität von IoT-Geräten APIs zu einem wichtigen Ziel für Kriminelle gemacht, die personenbezogene Daten stehlen oder Ransomware-Angriffe starten wollen. Der Schutz von APIs beginnt damit, einen Überblick über jede API zu erhalten, die mit Ihrem Unternehmen verknüpft ist, auch bekannt als Ihr API-Bestand.

Akamai API Security hilft Ihnen bei der Inventarisierung Ihres Bestands und bietet dann Einblick in das historische Verhalten jeder API, sodass Sie erkennen können, wie normales oder missbräuchliches API-Verhalten aussieht. Mit diesem Wissen können Sie nach aktiven Bedrohungen Ausschau halten, um Missbrauch schnell zu stoppen – bevor die Cyberkriminellen ihre Ziele erreichen.

Besonders ausgeklügelt und einfach bereitzustellen: Schädliche Bots

Bots sind ständig auf Ihrer Website unterwegs. In der Tat sind alle Ihre Suchmaschinenoptimierungen darauf ausgerichtet, die Gunst der Bots zu gewinnen. Doch zwischen den guten Bots können sich auch schädliche Bots verstecken, die eine Reihe von Cyberangriffen durchführen. Schädliche Bots sind vielleicht am besten dafür bekannt, begrenzte Bestände zu monopolisieren – wie den Kauf von Sportschuhen in limitierter Auflage oder riesige Mengen an Konzertkarten oder Hotelreservierungen. Bots verwenden jedoch eine ganz ähnliche Methode, wenn sie Ihr Unternehmen mit einer riesigen Menge an Anfragen in einem Distributed-Denial-of-Service-Angriff (DDoS-Angriff) überlasten, der darauf ausgelegt ist, die Verfügbarkeit Ihres Unternehmens zu stören.

Was viele nicht wissen, ist, dass DDoS zu einer relativ einfachen und kostengünstigen Angriffsform geworden ist, die von einer neuen Angreifergruppe genutzt wird, um milliardenschwere Unternehmen und kritische öffentliche Infrastruktur wie Schulen, Krankenhäuser, Flughäfen und Versorgungsunternehmen lahmzulegen. Diese Angriffe führen zu massiven Serviceunterbrechungen, die bei den Opfern enorme Umsatzeinbußen zur Folge haben können. In einer deutlichen Abkehr von den traditionellen Angreifern der Vergangenheit werden diese Angriffe aktuell fast immer von erfahrenen Akteuren aus Nationalstaaten, politischen Hacktivisten und professionellen Cyberkriminellen mit Hilfe von Botnets durchgeführt – große Netzwerke von verbundenen Geräten (oft Endnutzergeräte oder einfache IoT-Geräte), welche von Bots infiziert und gesteuert werden.

Bots kommen auch bei Credential-Stuffing-Angriffen zum Einsatz, die zu Kontoübernahmen führen. Beim Credential Stuffing nutzt ein Angreifer eine Liste von Nutzernamen und Passwörtern, die bei einer großen Datenschutzverletzung gewonnen wurden, und versucht, sich mit diesen bei anderen Institutionen anzumelden. Bots werden eingesetzt, um Millionen von Versuchen zur Kontoübernahme durchzuführen, und da viele Nutzer dazu neigen, Nutzernamen und Passwörter wiederzuverwenden, wird ein kleiner Bruchteil davon erfolgreich sein. Sobald der Angreifer Zugriff auf ein Konto erhält, wird der Angriff zu einer Kontoübernahme.

Credential Stuffing ist nur eine von vielen Methoden, mit denen Cyberkriminelle legitime Konten übernehmen. Sobald sie die Kontrolle über ein Konto erlangt haben, können sie Treuepunkte auszahlen lassen und digitale Assets übertragen, Guthaben von Geschenkkarten verwenden und betrügerische Käufe mithilfe gespeicherter Kreditkarteninformationen tätigen. Sie könnten sogar das gesamte Konto an einen anderen Bedrohungsakteur verkaufen. Sollte dies Ihren Kunden widerfahren, ist das Vertrauen in Ihr Unternehmen fast immer unwiderruflich verloren. Doch selbst erfolglose Credential-Stuffing-Angriffe können Ihrer Marke schaden, da der Bottraffic, der Ihre Website während dieser Versuche überschwemmt, die Ressourcenverfügbarkeit und die Reaktionszeiten erheblich reduzieren kann. Dies führt zu frustrierenden Erlebnissen für Ihre Kunden und Websitebesucher.

Scraper Bots werden sowohl für gute als auch für schädliche Zwecke eingesetzt. Weniger offensichtlich ist jedoch, dass ihre Präsenz die Performance der Website verschlechtern und die Kennzahlen verfälschen kann, die Unternehmen benötigen, um wichtige Entscheidungen zu treffen. Das wirkt sich potenziell schädlicher auf Ihre Marke aus als die Daten, die diese Bots von Ihrer Website abschöpfen.

Akamai bietet eine Reihe von Lösungen, die speziell auf die Abwehr von Bedrohungen durch schädliche Bots ausgerichtet sind:

Akamai App & API Protector mit Malware-Schutz ist die Grundlage für den Schutz vor Diebstahl Ihrer Daten, personenbezogenen Daten und anderen Kontoinformationen sowie für die Abwehr von botgesteuerten DDoS-Angriffen, Ransomware, Malware und mehr. App & API Protector ermöglicht Ihren Kunden den ständigen Zugriff auf Ihre Webeigenschaften und stellt sicher, dass die Websiteperformance auch bei einem Angriff nicht beeinträchtigt wird.

Akamai Bot Manager erkennt den gesamten Bottraffic und wehrt schädliche Bots direkt an der Edge ab. Das Tool verwendet KI-Modelle zur Analyse des Botverhaltens und setzt Browseralgorithmen für Fingerprinting und maschinelles Lernen (ML) ein, um die Erkennung immer genauer zu gestalten, Probleme für Nutzer zu reduzieren und sie vor betrügerischen Aktivitäten zu schützen.

Akamai Content Protector verhindert, dass Scraper Ihre Webinhalte stehlen und für schädliche Zwecke verwenden können, und mindert gleichzeitig die Beeinträchtigung der Websiteperformance. Bei der ML-gesteuerten Erkennung werden potenziell schädliche Bot-Scraper-Aktivitäten nach Risiko klassifiziert, um eine angemessene Reaktion zu finden.

Eine weitere grundlegende Lösung zum Schutz Ihrer Kunden ist die Verbesserung des sicheren Kontozugriffs. Akamai Account Protector beugt menschlichem Betrug vor, der oft von Bots koordiniert wird. Vertrauenswürdigen Nutzern wird gleichzeitig ein reibungsloser, sicherer Zugriff auf Ihre Website gewährt, der dazu führt, dass sie länger angemeldet bleiben und häufig zurückkehren.

Die Kosten schädlicher Skripte: Clientseitige Bedrohungen

Ähnlich wie bei Bots können Skripte von Drittanbietern Gutes bewirken. Sie ermöglichen Funktionen, Marketingtools, Analysen und vieles mehr, um Ihr allgemeines Nutzererlebnis (UX) zu verbessern. Sie machen den Webbrowser aber auch zu einer kritischen clientseitigen Angriffsfläche.

Clientseitige Bedrohungen sollen Kunden dazu verleiten, auf schädliche Inhalte zuzugreifen. Sie nutzen Schwachstellen in Anwendungen aus, die direkt auf dem Computer des Nutzers (in der Regel Ihr Kunde), hier als Client bezeichnet, ausgeführt werden. Clientseitige Sicherheit umfasst daher die Technologien und Richtlinien, die zum Schutz von Kunden vor schädlichen Aktivitäten auf Webseiten verwendet werden.

Skriptangriffe können Unternehmen erheblichen finanziellen Schaden zufügen und das Vertrauen von Kunden, Partnern und Zahlungsabwicklern beeinträchtigen. Es überrascht nicht, dass die clientseitige Sicherheit ein zentraler Schwerpunkt der neuen Anforderungen des Payment Card Industry Data Security Standard (PCI DSS v4.0) ist. Um die Anforderungen zu erfüllen, muss jedes Unternehmen, das Zahlungskarten online verarbeitet, wissen, welche Skripte auf seiner Website ausgeführt werden, wann sie geändert werden und wann sie nicht mehr ausgeführt werden.

Die Verteidigung gegen diese Angriffe ist nicht einfach. Skripte von Drittanbietern sind zahlreich und ändern sich ständig, was ihre Überwachung extrem schwierig macht. Skriptangriffe selbst nehmen auch verschiedene Formen an, wie Web-Skimming und Formjacking. Ganze kriminelle Syndikate (am bekanntesten ist Magecart) haben sich um diese Art von Angriffstechniken organisiert, um Zahlungskartendaten und personenbezogene Daten zu stehlen.

In unserer Welt der digitalen Zahlungen, des Online-Einkaufs und der Internetrecherche ist die clientseitige Sicherheit wichtiger denn je – vor allem auf Zahlungsseiten, die persönliche und finanzielle Daten erfassen. Sie benötigen Einblick in alle Skripte, die auf Ihrer Website ausgeführt werden, die Möglichkeit, verdächtiges Verhalten zu erkennen, und Maßnahmen zur Abwehr von Angriffen. Akamai bietet eine spezielle Lösung für diese Bedrohungen:

Client-Side Protection & Compliance sichert den Datenschutz und das Vertrauen der Kunden im Browser, indem alle Nutzer vor clientseitigen Angriffen wie Web-Skimming, Formjacking und Magecart geschützt werden.

Der Schutz der Infrastruktur schützt auch das Kundenerlebnis

Das Herzstück des Kundenerlebnisses ist die zugrunde liegende digitale Infrastruktur, die Ihre gesamte Marke antreibt. DNS-Sicherheit, Zuverlässigkeit und Performance sorgen dafür, dass Ihre Kunden jederzeit auf Ihre Services zugreifen können. DNS-Systeme entsprechen im Wesentlichen Ihrer Online-Präsenz. Wenn sie ausfallen, ist auch Ihre gesamte digitale Präsenz nicht mehr erreichbar. Aus diesem Grund greifen Bedrohungsakteure ständig die DNS-Systeme ihrer Ziele mit DDoS-Angriffen an. Angesichts der Wettbewerbsbedingungen, die in allen Branchen herrschen, brauchen Sie unbedingt durchgehende DNS-Verfügbarkeit, um sicherzustellen, dass Kunden und potenzielle Kunden das Beste erleben, was Ihre Marke zu bieten hat.

Akamai bietet das ultimative Lösungsportfolio, um Ihre digitale Infrastruktur vor verschiedenen DDoS-Angriffen zu schützen:

Für die leistungsstärkste DDoS-Abwehr bietet Akamai Prolexic mehrere Schutzoptionen, darunter Scrubbing Center an mehr als 32 Standorten weltweit und eine dedizierte Verteidigungskapazität von bis zu 20 Tbit/s.

Akamai Edge DNS liefert eine umfassende, speziell entwickelte, autoritative DNS-Lösung, die die Skalierbarkeit, Sicherheit und Kapazität der Akamai Connected Cloud nutzt, um Ihre DNS-Zonen zu verwalten.

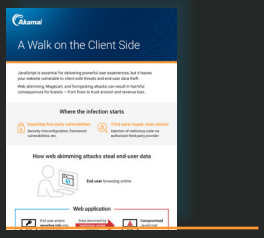
Akamai Shield NS53, eine bidirektionale DNS-Proxy-Lösung mit dynamischer Durchsetzung von Sicherheitsrichtlinien, kann zum Schutz wichtiger Komponenten Ihrer Ursprungs-DNS-Infrastruktur vor Ressourcenüberlastungsangriffen eingesetzt werden – vor Ort, in der Cloud oder hybrid.

Wir sind Ihr Partner, wenn es darum geht, das Kundenvertrauen zu sichern

Wir bei Akamai konzentrieren uns seit über 25 Jahren darauf, wie Marken auftreten. Als Pionier für Netzwerke zur Inhaltsbereitstellung haben wir bereits die Geschwindigkeitsprobleme der ersten digitalen Storefronts gelöst. Unser Netzwerk zur Inhaltsbereitstellung zählt zu den größten der Welt. In den letzten zehn Jahren haben wir die Einblicke in den Traffic, die es uns ermöglicht, genutzt, um Bedrohungen täglich zu überwachen und zu analysieren. Auf der Basis dieser Forschungsergebnisse können wir unsere Sicherheitslösungen stetig weiterentwickeln, wenn Angriffsvektoren wachsen und sich verändern. Als wichtiger Sicherheitspartner für unsere Kunden haben wir uns verpflichtet, ihre Geschäfte am Laufen zu halten und ihre Kundenerlebnisse zu schützen. Gleichzeitig geben wir ihnen das Vertrauen, mit neuen digitalen Erlebnissen zu experimentieren, die in ihrer Branche führend sind.

Nächste Schritte

Hier finden einige Ressourcen, die Ihnen helfen, den optimalen nächsten Schritt zum Schutz Ihrer Marke zu planen:



Stärken Sie die Integrität Ihrer Webseite mit clientseitigem Schutz.

Erhalten Sie kompromisslose Sicherheit für Websites, Anwendungen und APIs aus einer Hand.

Erfahren Sie mehr über die wichtigsten Überlegungen für eine Bot-Management-Strategie.

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. 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 (ehemals Twitter) und LinkedIn.
Veröffentlicht: Juni 2024.