Rezepte und Zutaten für Cybersicherheit:

Das ultimative Kochbuch für Layer-7-DDoS-Ausfallsicherheit erstellen

Inhaltsverzeichnis

Einführung

Das richtige Verteidigungsrezept gegen die heutigen DDoS-Angriffe (Distributed Denial of Service) zusammenzustellen, kann selbst für die versiertesten Sicherheitsexperten eine Herausforderung sein. Dies gilt insbesondere für Layer-7-DDoS-Angriffe, die zusätzliche Komplikationen mit sich bringen. Als nützlich erweist sich hier eine Sammlung von Schritt-für-Schritt-Anleitungen mit unterschiedlichen Ansätzen für die verschiedenen Bedrohungen – ein Kochbuch für Layer-7-DDoS-Resilienz sozusagen.

Cyberkriminelle bereiten DDoS-Angriffe unterschiedlich vor. Angriffe auf Layer 3 und 4 sind eher von ihrer Stärke bestimmt. Wer hat die bessere Netzwerkkapazität – der Angreifer oder die Verteidigung? Layer-7-Angriffe haben es dagegen auf die Anwendungsebene des OSI-Modells (Open Systems Interconnection) abgesehen, die für die direkte Interaktion mit Softwareanwendungen zuständig ist. Sie verfolgen das Ziel, einen Webserver, eine Datenbank oder eine Anwendung zu überfordern, indem sie Kapazität, Speicherzuweisungen oder Systemschwächen bei der Anfragenverarbeitung ausnutzen.

Layer-7-DDoS-Angriffe stellen daher die Abwehrseite vor besondere Herausforderungen, denn solche Anfragen erscheinen oft als legitimer Traffic. Daher ist es schwierig, schädliche Anfragen ohne Beeinträchtigungen für legitime Nutzer herauszufiltern. Darüber hinaus ist es für Angreifer aufgrund der Verfügbarkeit von Automatisierungs- und Cloudressourcen einfacher denn je, diese Angriffe schnell und in großem Maßstab zu starten.

In diesem Whitepaper stellen wir ausführlich eine Reihe von Rezepten vor, mit denen Sie die Herausforderungen bei der Abwehr von Layer-7-DDoS-Angriffen meistern können. Dazu behandeln wir die von Angreifern verwendeten Tools und Techniken, geeignete Erkennungs- und Abwehrtaktiken sowie Vorschläge für Analyse und Wiederherstellung nach dem Ereignis.

Aufgrund unserer Erfahrung in den Bereichen Inhaltsbereitstellung und Cybersicherheit und dank einer verteilten Cloud-Plattform mit mehr als 4.200 Präsenzpunkten weltweit haben wir bei Akamai eine einzigartige Perspektive auf die heutigen DDoS-Angriffe. Da DDoS-Angriffe auf Anwendungsebene immer komplexer und vielseitiger werden, ist es wichtig, über diese Perspektive und eine kluge Verteidigungsstrategie zu verfügen. Genau darum soll es hier gehen.

Ganz gleich, ob Sie ein Sicherheitsexperte an vorderster Front sind, der Hilfe im Umgang mit einer bestimmten Bedrohung oder Schwachstelle sucht, oder ein CISO, der seine Sicherheitslage verbessern möchte: Dieses Kochbuch liefert das Erfolgsrezept.

Häufige Ziele von Layer-7-DDoS-Angriffen und Beispiele für derartige Attacken

Layer-7-DDoS-Angriffe zielen auf die oberste Schicht des OSI-Modells: die Anwendungsebene. Diese Angriffe sollen die Ressourcen eines Ziels überfordern, indem sie die Art und Weise ausnutzen, wie Webanwendungen Anfragen verarbeiten. Häufige Ziele von Layer-7-DDoS-Angriffen sind:

Webserver: Angreifer nehmen Webserver ins Visier, um die Bereitstellung von Inhalten an legitime Nutzer zu unterbrechen. Dies kann dazu führen, dass Websites langsam geladen werden oder gar nicht mehr aufgerufen werden können.

Webanwendungen: Anwendungen, die auf Datenbanken oder Backend-Services angewiesen sind, sind anfällig für Layer-7-DDoS-Angriffe, denn Angreifer können Schwachstellen ausnutzen, die Anwendungen bei der Analyse von Abfragen, der Verarbeitung von Anfragen oder der Verwaltung von Sitzungen aufweisen.

Programmierschnittstellen (APIs): APIs sind ein wichtiger Bestandteil moderner Web-Dienste und mobiler Anwendungen. Angreifer nehmen APIs ins Visier, um die Interaktion zwischen verschiedenen Softwarediensten zu unterbrechen. Das wirkt sich auf die Funktionalität von Anwendungen aus, die auf diese APIs angewiesen sind.

DNS-Services: Obwohl DNS-Angriffe auch auf anderen Ebenen möglich sind, können Layer-7-Angriffe dazu führen, dass der DNS-Dienst mit bösartigen Anfragen überflutet wird. Die Angreifer wollen so die Auflösung von Domainnamen unterbrechen, was zu umfangreichen Zugangsproblemen führen kann. Die zunehmende Einführung von DNS über HTTP/TLS könnte zu einer Zunahme solcher Angriffe führen.

E-Mail-Server: Angriffe auf E-Mail-Server können die Kommunikation unterbrechen und sowohl den eingehenden als auch ausgehenden E-Mail-Verkehr beeinträchtigen.

Zahlungs-Gateways und Finanzdienstleistungen: Dies sind lukrative Ziele für Angreifer, die Transaktionen unterbrechen und in Finanzoperationen Chaos stiften wollen.

In den SOTI-Berichten (State of the Internet Reports) und Sicherheitsinformationen von Akamai untersuchen wir routinemäßig die sich entwickelnde Bedrohungslandschaft in Bezug auf Layer-7-DDoS-Angriffe. Dabei zeigen wir auch die vielfältigen Angriffsvektoren und die am stärksten gefährdeten Branchen auf.

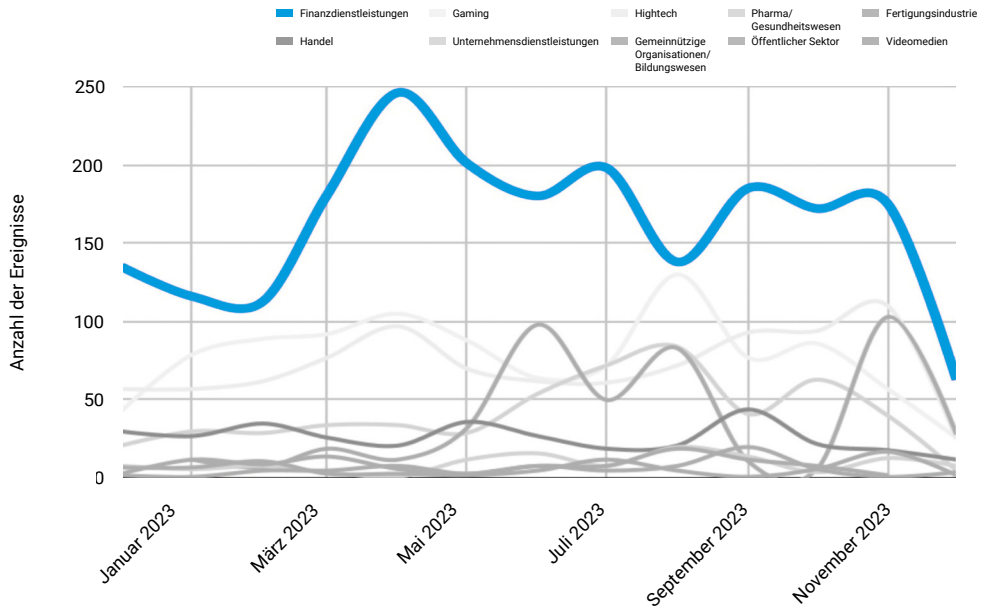
Angriffsvektoren

- Angriffe auf Webanwendungen und APIs: Die Angreifer nehmen in der Regel Website-Einstiegspunkte ins Visier, einschließlich API-Endpunkte, die aufgrund ihres Inhalts oder ihrer Konfiguration normalerweise nicht zwischengespeichert werden. Zu den allgemein bekannten Zielpfaden gehören „/“, „/home“, „/en-US“, „/pricing/“ usw.
- Verbreitet sind Angriffsvektoren wie die folgenden:
  • HTT-GET-/POST-Floods auf Homepages
  • HTTPS-GET-Flood auf randomisierten Pfaden und Abfragezeichenfolgen
  • Slow-Read-Angriffe
  • Flood-Angriff beim Hochladen großer Dateien

Hinzu kommt: Die Zahl der Unternehmen, die einem DDoS-Angriff ausgesetzt sind, steigt schon seit Längerem von Jahr zu Jahr. Was sich jetzt aber geändert hat, ist das „Wie“. Zuerst haben sich Typ und Umfang der angegriffenen Eigenschaften geändert. Statt 10 Angriffe auf dieselben oder ähnliche Endpunkte kann es jetzt 100 auf verschiedene IPs im Netzwerkbereich gerichtete Angriffe geben. Diese Angriffe zielen nicht nur auf Layer 3, sondern gleichzeitig auch auf Layer 7 ab.

Betroffene Branchen

Die Anzahl der DDoS-Angriffe (Distributed Denial of Service) gegen die Finanzdienstleistungs-, Glücksspiel- und Fertigungsbranchen nahm 2023 zu. Das gilt insbesondere für die EMEA-Region, wo die Zahl höher war als in allen anderen Regionen zusammen.

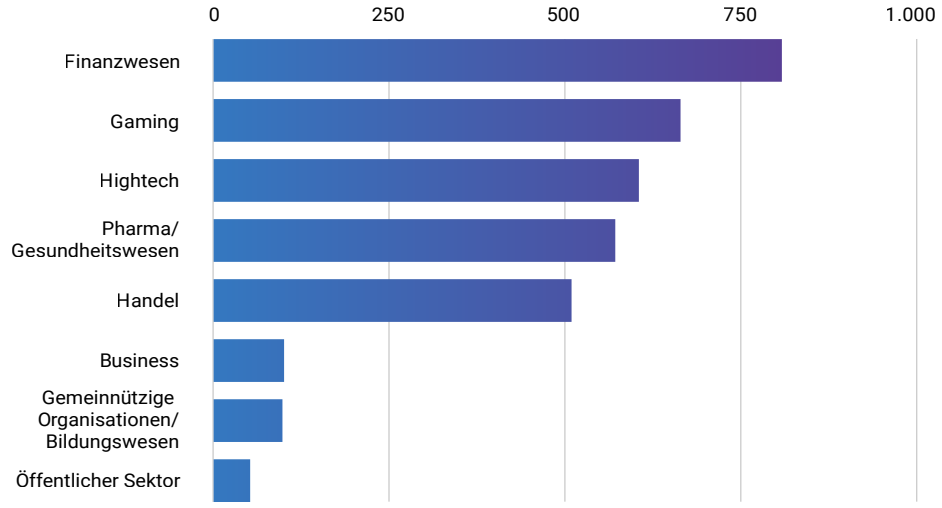


DDoS: Here to Stay, März 2024

Vor allem Finanzdienstleister sind immer häufiger Opfer von Layer-7-DDoS-Angriffen geworden. Seit 2021 beobachtet Akamai einen deutlichen Anstieg der DDoS-Angriffe auf Finanzdienstleister. Mehr als ein Drittel (35 %) der Angriffe in allen Branchen richtete sich im Jahr 2023 gegen Finanzdienstleister, womit der Sektor ein noch begehrteres Ziel war als die Gaming-Branche. Die Analyse von Akamai zeigt, dass sich 63 % aller DDoS-Angriffe weltweit im Bankensektor ereigneten. Fast drei Viertel (72 %) der Angriffe in EMEA und 91 % der Attacken in APAC waren gegen Banken gerichtet. In Nord- und Südamerika verteilten sich die DDoS-Angriffe dagegen gleichmäßiger auf Banken, Versicherungen und andere Finanzdienstleister.

Nord-/Südamerika: 28 % der DDoS-Angriffe ereigneten sich in der Finanzdienstleistungsbranche

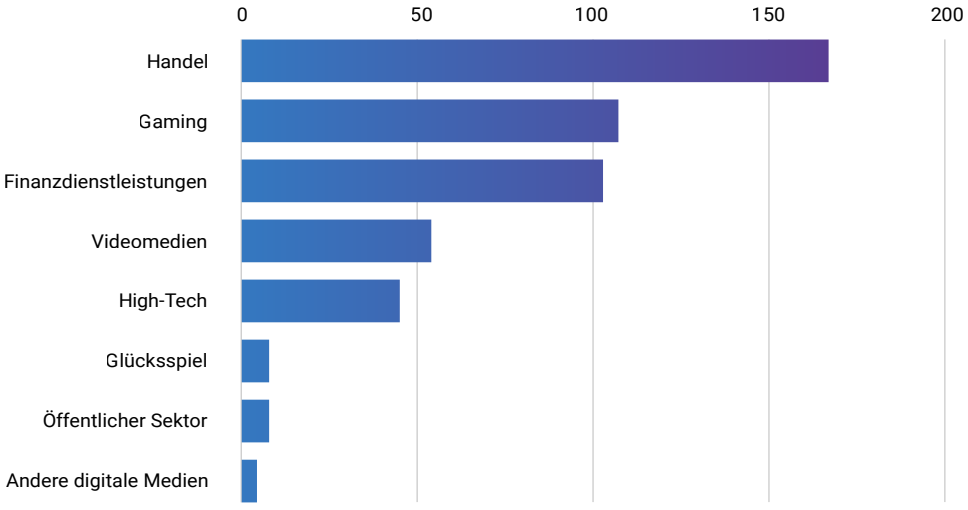
Juni bis Dezember 2023



DDoS: Here to Stay, März 2024

APAC: 11 % der DDoS-Angriffe ereigneten sich in der Finanzdienstleistungsbranche

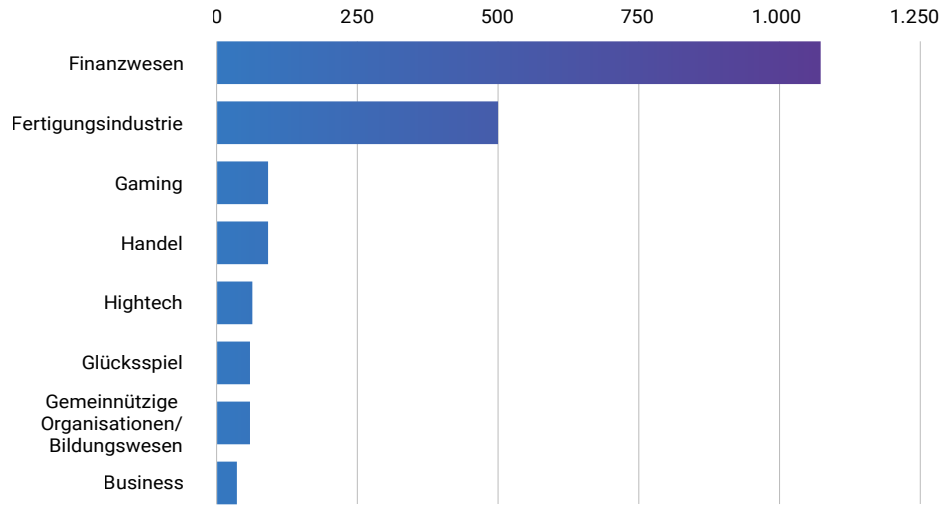
Juni bis Dezember 2023



DDoS: Here to Stay, März 2024

EMEA: 66 % der DDoS-Angriffe ereigneten sich in der Finanzdienstleistungsbranche

Juni bis Dezember 2023



DDoS: Here to Stay, März 2024

Ein aktuelles Beispiel ist der ausgeklügelte Layer-7-DDoS-Angriff auf einen Akamai-Kunden aus dem Finanzdienstleistungsbereich. In diesem Fall starteten Cyberkriminelle mithilfe von Automatisierung einen stark verteilten Angriff. Die Angreifer nutzten HTTP-GET-Flood und nahmen hauptsächlich nicht zwischenspeicherfähige URLs ins Visier (wie zum Beispiel Homepage- und Login-Endpunkte). Mithilfe verschiedener proaktiver Kontrollen wurde dieser Angriff erfolgreich und ohne Auswirkungen auf den Kundenursprung abgewehrt. Diese Heatmap der Angriffsquelle unterstreicht die zunehmende Nutzung von Cloud-Dienst-Anbietern, Tor-Exit-Knoten und anonymen oder offenen Proxyknoten:

DDoS-Angriffe durch Autonomous System

Visualisierung eines gegen ein Finanzinstitut gerichteten Angriffs auf Anwendungsebene, der im 1. Quartal 2024 in mehr als 100 Ländern stattfand und mit Unterstützung von Akamai abgewehrt werden konnte

DDoS-Angreifer können eine weit verteilte Angriffsinfrastruktur aufbauen und koordinieren, indem sie dynamische IP-Adressen in ausgedehnten Netzwerken nutzen, die sich über zahlreiche Länder und Regionen weltweit erstrecken.

Von Angreifern verwendete Tools und Techniken

Leider entwickeln sich DDoS-Angreifer und ihre Methoden ständig weiter. Sie finden immer wieder Wege, um mit ihren Aktionen Geld zu verdienen. Dazu passen sie ihre Techniken an, nutzen neue Tools und suchen sich neue Methoden. Es gibt eine Reihe von Faktoren, die diese Entwicklung deutlich machen.

Automatisierung: Angreifer verwenden automatisierte Skripte und Bots, um legitimes Nutzerverhalten nachzuahmen, was die Erkennung erheblich erschwert. Darüber hinaus nutzen Angreifer nun Algorithmen für maschinelles Lernen, die sich anpassen und herkömmliche Erkennungssysteme umgehen.

Multi-Vektor-Angriffe: Cyberkriminelle setzen zunehmend Multi-Vektor-Strategien ein. Sie kombinieren verschiedene Angriffstypen (wie GET- und POST-Flood) und DNS-Ziele (wie Verstärkungs- und Fragmentangriffe) mit anderen Kombinationen, um Netzwerk- und Anwendungsressourcen zu überfordern.

APIs als Angriffsziel: Da Unternehmen für ihre Anwendungen zunehmend auf APIs angewiesen sind, eröffnen sich für Angreifer neue Möglichkeiten, da sie API-Schwachstellen für DDoS-Angriffe ausnutzen können. Diese Angriffe zielen darauf ab, Serverressourcen zu erschöpfen, indem Tausende von Verbindungen gleichzeitig angefordert werden, oder logische Fehler auszunutzen, die zu Unterbrechungen im Service führen.

Ausnutzung von IoT-Geräten: Schlecht gesicherte IoT-Geräte breiten sich aus und stellen eine riesige Armee für Botnets dar. Diese Geräte werden häufig gekapert und für massive DDoS-Angriffe verwendet, die ihre Netzwerkkonnektivität und Rechenleistung ausnutzen.

Zunehmende Raffinesse

Durch diese neuen Tools und Techniken ist die Komplexität und Häufigkeit von DDoS-Angriffen gestiegen, und Angreifer wenden raffinierte Methoden an, um herkömmliche Abwehrmaßnahmen zu umgehen. Dies sind einige der auffälligsten Trends:

Verschlüsselung: Eine deutliche Verlagerung auf HTTPS-basierte DDoS-Angriffe hat die Abwehr schwieriger gemacht. Diese Angriffe, die verschlüsselt sind, tarnen sich als legitimer Traffic. Dadurch sind sie schwieriger zu erkennen und herauszufiltern, da herkömmliche DDoS-Schutzmaßnahmen bei der Entschlüsselung von SSL/TLS-Traffic auf Anwendungsebene Beschränkungen haben.

Botnets und Proxys: Angesichts der beträchtlichen Zunahme von DDoS-Botnets und der Verbreitung anonymer Proxys durch Angreifer werden Anfragen von einer Vielzahl von IP-Adressen gesendet (in der Regel mehr als 10.000 IP-Adressen pro Angriff). Angreifer nutzen diese Strategie, um Abwehrmaßnahmen zu umgehen, die Anfragen von einer einzelnen IP zählen. Die Verbreitung von Cloudhosting-Plattformen und die Einführung cloudbasierter Dienste erleichtern die Durchführung dieser hochintensiven und stark verteilten Angriffe.

DDoS-Angriffe durch Autonomous System

Visualisierung eines aktuellen DDoS-Angriffs auf Anwendungsebene – 650.000 Transaktionen pro Sekunde (TPS), 20 Gbit/s, mehr als 9 Milliarden Anfragen – gegen einen Akamai-Kunden aus der Finanzdienstleistungsbranche

DDoS-Angreifer sind in der Lage, eine extrem verteilte Angriffsinfrastruktur zu erstellen und zu koordinieren, hauptsächlich über Cloud-Anbieter.

Eine neuere Methode von Verteidigern ist die Verfolgung von Anfragen pro TLS-Fingerabdruck, der aus mehreren TLS-Layer-Signalen wie Verschlüsselungstypen und deren Reihenfolge besteht. Obwohl dieser Ansatz anfällig für False Positives ist, kann er bei korrekter Anwendung eine effektivere Abwehr bieten, wenn ein Angreifer von verschiedenen Computern und IPs aus operiert, da dieselbe Software auf den kompromittierten Geräten installiert ist. Diese Geräte weisen ähnliche Umgebungseigenschaften auf, darunter die gemeinsam genutzte TLS-Bibliothek.

Beschaffung der Zutaten

Während sich die auf dem Markt verfügbaren Tools häufig ändern, deutet die Entwicklung der Angriffstechniken auf einen Trend hin zu ausgefeilteren und weniger erkennbaren Methoden. Dazu gehören:

- **Kompromittierte IoT-Geräte:** Angreifer nutzen weiterhin kompromittierte IoT-Geräte in Botnets zum Starten groß angelegter DDoS-Angriffe, was die fortbestehende Anfälligkeit dieser Geräte unterstreicht.

- **DDoS-Dienste mit Mietoption:** Die Verfügbarkeit von DDoS-Diensten mit Mietoption hat die Einstiegsbarriere für Angreifer gesenkt, sodass Personen ohne umfangreiches technisches Wissen Angriffe in erheblichem Umfang durchführen können.
- **Ausweichtechniken:** Fortgeschrittene Ausweichtechniken wie randomisierte Header-Parameter und dynamische Anfrageargumente sind keine Seltenheit mehr. Diese Techniken sind eine Herausforderung für herkömmliche Erkennungs- und Abwehransätze, da der schädliche Traffic nur schwer von legitimen Anfragen unterschieden werden kann.

Bei solchen Angriffen ausgenutzte Schwachstellen

Die Schwachstellen, die Angreifer bei Layer-7-DDoS-Angriffen ausnutzen, hängen häufig mit der Art und Weise zusammen, wie Webanwendungen Nutzereingaben verarbeiten und Daten verwalten. Um das mit diesen Schwachstellen verbundene Risiko zu minimieren, ist es wichtig, Sicherheitsmaßnahmen zu kombinieren.

Eine der größten Sicherheitslücken, die Angreifer in den letzten Jahren bei DDoS-Angriffen auf Anwendungsebene ausgenutzt haben, war der HTTP/2-Rapid-Reset-Fehler, der Ende 2023 vielfach veröffentlicht wurde. Solche Angriffe nutzten einen Fehler im HTTP/2-Protokoll aus, das für den Betrieb des Internets und aller Websites von grundlegender Bedeutung ist. Die Ausnutzung dieser Schwachstelle führte zu einem Anstieg des HTTP-DDoS-Angriffstraffics um 65 % in einem Quartal im Vergleich zum vorherigen. Dies unterstreicht den Schweregrad und die Auswirkungen der Angriffe, die diese Schwachstelle ausnutzen.

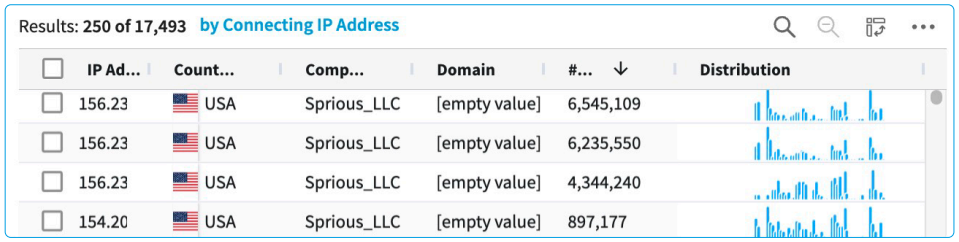
Diese spezielle Schwachstelle ermöglichte es Angreifern, durch die Nutzung von Cloud-Computing-Plattformen und die Ausnutzung von HTTP/2 effektiver vorzugehen und hypervolumetrische DDoS-Angriffe mit relativ kleinen Botnets durchzuführen. Zu den am stärksten von diesen Angriffen betroffenen Branchen gehörten Gaming, IT, Kryptowährungen, Computersoftware und Telekommunikation. Die Hauptursprungsländer für diese Attacken waren die USA, China, Brasilien, Deutschland und Indonesien.

In der Folge deckte eine branchenweit koordinierte Initiative die Schwachstelle HTTP/2-Rapid Reset (CVE-2023-44487) auf und machte auf DDoS-Angriffe aufmerksam, die sich diesen Fehler zunutze machten. Die Ausnutzungsversuche richteten sich gegen verschiedene Provider, darunter führende Cloud- und CDN-Dienstanbieter.

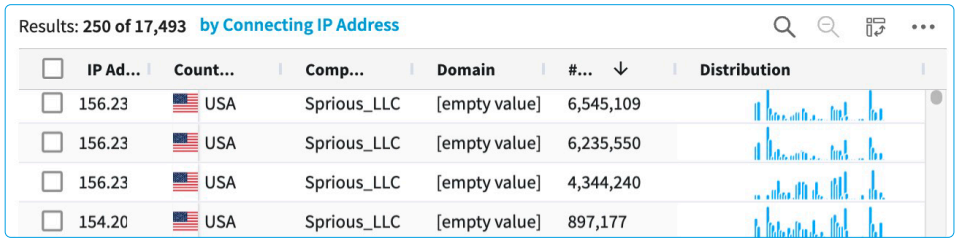
Reale Beispiele: Einsatz von Automatisierung bei einem DDoS-Angriff

Angreifer verwenden oft mehrere DDoS-Tools, um dieselben DDoS-Angriffe auszuführen. Dabei nutzen sie jeweils mehrere Techniken in Kombination, um Sicherheitsprodukte zu umgehen oder zumindest weniger effizient zu machen. Ein solches Beispiel für einen Angriff wird weiter unten im Zusammenhang mit Akamai Web Security Analytics beschrieben.

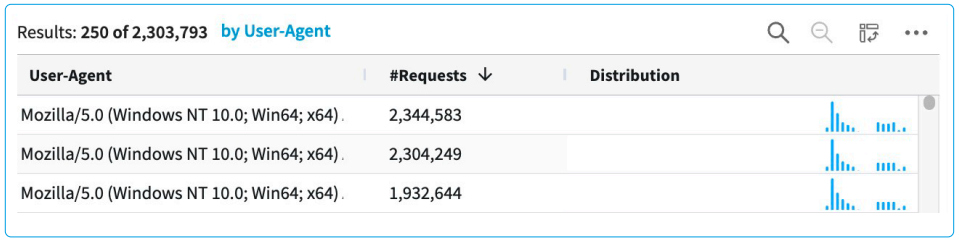
- Angriff von mehr als 17.000 IP-Adressen



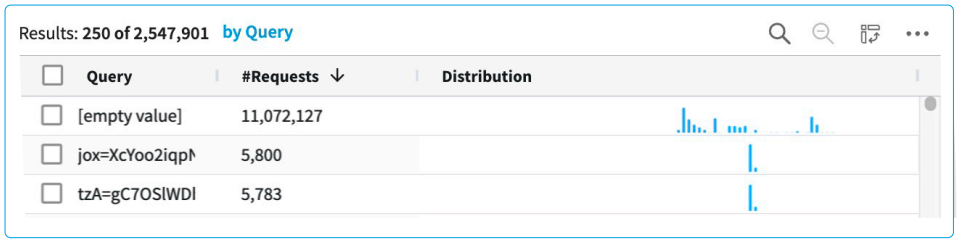
- Angriffsquellen aus mehr als 400 Netzwerken



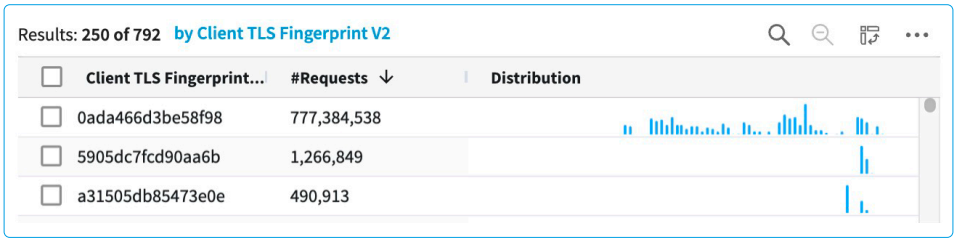
- 2.303.793 eindeutige User Agents



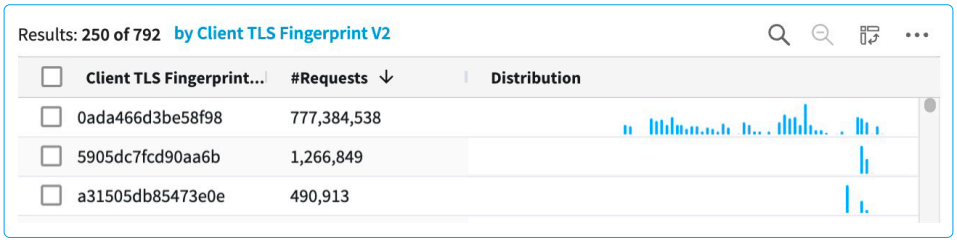
- 2.547.901 eindeutige und zufällige Abfragezeichenfolgen



- HTTP-Header-Rotation (z. B. Accept-Language, Referer)



- Rotation der TLS-Einstellungen



Die Abwehr derart ausgeklügelter Angriffe erfordert eine mehrschichtige Schutzstrategie. Hilfreich sein kann die Verwendung von proaktiven und reaktiven Kontrollen, wie zum Beispiel einer erweiterten Kombination von Anfrageübereinstimmungen und Merkmalen des Quell-Traffics bei der Ratenbegrenzung oder Kontrollen der Reputation von Quellen.

Cyberkriminelle rüsten auf: Imitation von TLS-Signalen

Aktuellen Beobachtungen zufolge verwenden Cyberkriminelle häufiger TLS-Signale in ihren DDoS-Tools, um Erkennungen zu umgehen. Dabei lassen sie solche Verbindungen so aussehen, als kämen sie von legitimen Chrome-Browsern. Anstatt eine ressourcenintensive Headless-Version von Chrome zu nutzen, die den Angriff verlangsamen könnte, verwenden die Angreifer möglicherweise eine modifizierte Version der TLS-Bibliothek, mit der sie TLS-Signale eines beliebigen echten Browsers einstellen und imitieren können. Es gibt Tools zur Replikation von TLS-Fingerabdrücken, doch sie kommen in DDoS-Angriffstools normalerweise nicht vor. Der Einsatz dieser Art von Angriffen deutet darauf hin, dass die technischen Fähigkeiten der Angreifer zunehmen und dass sie die Verteidigungsstrategien genau kennen. Daher müssen für Abwehrmaßnahmen gegen Layer-7-DDoS-Angriffe die neusten Angriffstrends regelmäßig erforscht werden. Es sieht auch so aus, als würden die DDoS-Tools, die TLS-Spoofing enthalten, immer häufiger eingesetzt werden.

Überblick behalten: Risiken bewerten und Schwachstellen identifizieren

Sie können Ihre Abwehrstrategie gegen Layer-7-DDoS erheblich verbessern, indem Sie Ihre kritischen Assets identifizieren und ermitteln, wo diese für einen DDoS-Angriff anfällig sein könnten. Diese Risikobewertung hilft bei der Priorisierung der zu schützenden Ressourcen anhand ihrer Wichtigkeit und Anfälligkeit. Wenn Unternehmen potenzielle Angriffsvektoren und ihre Auswirkungen kennen, können sie spezifische Gegenmaßnahmen wie Ratenbegrenzung, Web Application Firewalls und Verhaltensanalysen implementieren, um Risiken effizient zu mindern. Darüber hinaus ermöglicht eine kontinuierliche Risikobewertung eine Verteidigungsstrategie, die sich als Reaktion auf neue Bedrohungen und sich ändernde Geschäftsanforderungen weiterentwickelt.

Verschiedene Branchen und Unternehmen werden bei der Bewertung von DDoS-Risiken auf Anwendungsebene möglicherweise unterschiedlich vorgehen. Zum Beispiel:

> **E-Commerce:** Vor einer großen Verkaufsveranstaltung kann sich im Rahmen einer Risikobewertung der Bezahlvorgang unter Umständen als eine kritische Schwachstelle herausstellen. Abwehrmaßnahmen können unter anderem die Implementierung einer Web Application Firewall (WAF) und die Ratenbegrenzung zum Schutz des Dienstes umfassen.
>
> **Finanzdienstleistungen:** Bei einer Banking-Anwendung kann die Risikobewertung ergeben, dass die Anmeldeseite ein Hauptziel für DDoS-Angriffe ist. Die Bank könnte dann mit einer Kombination aus maßgeschneiderten Endpunkt-Ratenbegrenzungen und Verhaltenserkennung zwischen legitimen Nutzern und Angriffstraffic unterscheiden.

Nur wenn spezielle Schwachstellen bekannt sind, können gezielte Abwehrmaßnahmen ergriffen und kritische Services während eines Angriffs verbessert werden.

Zu viele Köche verderben den Brei: Rollen und Verantwortlichkeiten

Die Festlegung klarer Rollen und Verantwortlichkeiten ist ein entscheidender Schritt für eine effektive Layer-7-DDoS-Strategie. Nur so werden bestmögliche Voraussetzungen für eine koordinierte und effiziente Reaktion im Falle eines Angriffs geschaffen. Ohne eine klare Rollenverteilung droht Chaos bei den Abwehrmaßnahmen, da sich Aufgabenbereiche überschneiden und Lücken in der Verteidigungslinie auftun können. Anhand definierter Verantwortlichkeiten weiß jedes Teammitglied genau, was seine Aufgabe ist – von der Überwachung des Traffics und der Identifizierung von Anomalien bis hin zur Umsetzung von Abwehrstrategien und der Kommunikation mit den Stakeholdern. Diese Koordination trägt dazu bei, die Auswirkungen von Angriffen zu minimieren, die Serviceverfügbarkeit aufrechtzuerhalten und kritische Assets zu schützen.

Wenn zu viele Entscheidungsträger keine klare Rollen haben, kann dies zu verzögerten Reaktionen bei einem DDoS-Angriff führen. Legen beispielsweise das Team für den Netzwerkbetrieb und das Team für Cybersicherheit unabhängig voneinander unterschiedliche Ansätze zur Risikominderung unkoordiniert fest, könnten sie versehentlich die Bemühungen der jeweils anderen neutralisieren oder kritische Schwachstellen übersehen. Zur richtigen Strategie gehören definierte Rollen, wie zum Beispiel eine verantwortliche Person für Vorfallsreaktion, ein Koordinator für die Kommunikation und ein technisches Reaktionsteam. Durch eine solche Festlegung lassen sich schnelle, einheitliche Maßnahmen sicherstellen, Ausfallzeiten minimieren und Analysen nach Vorfällen optimieren.

Das darf in Ihrer Küche nicht fehlen

Die Erkennung und Abwehr eines Angriffs auf Anwendungsebene kann eine Herausforderung darstellen, da es so schwierig ist, zwischen legitimem und schädlichem Traffic zu unterscheiden. Als Reaktion auf die sich entwickelnden Bedrohungen empfehlen wir einen vielseitigen Verteidigungsansatz:

- **Immer verfügbar oder nach Bedarf:** Stellen Sie sicher, dass die DDoS-Sicherheitskontrollen immer aktiv sind, und aktualisieren Sie Vorfallsreaktionspläne, um sich schnell auf neue Bedrohungen einstellen zu können.
- **Aufbau einer ausfallsicheren und zuverlässigen Architektur:** Antizipieren Sie einen Single Point of Failure, denn Angreifer werden wahrscheinlich mehrere Dienste angreifen, darunter DNS, Webanwendungen, APIs sowie Rechenzentrum und Netzwerkinfrastruktur. Die richtige Architektur ist entscheidend für den Schutz vor Layer-7-DDoS-Angriffen. Diese Überlegungen zur Architektur können die Wahl eines Edge- oder CDN-basierten DDoS-Schutzes umfassen, der immer aktiviert ist. Überschätzen Sie nicht die Zuverlässigkeit Ihrer Systeme. Das Ausmaß der heutigen DDoS-Angriffe kann die meisten Infrastrukturen leicht überfordern.
- **Bewerten Sie die SLAs Ihres Anbieters** und gleichen Sie sie mit Ihrer Strategie ab.
- **Überprüfen Sie die Bereitschaft Ihres Anbieters:** Wählen Sie einen Anbieter, der regelmäßig eine Überprüfung seiner kritischen Netzwerkkomponenten nachweist und verschiedene DDoS-Schutzmechanismen bewertet, um Einblicke in deren Effektivität gegenüber aktuellen Angriffsmethoden zu erhalten.
- **Überprüfen Sie Ihr Playbook zur Abwehr von DDoS-Angriffen:** Holen Sie Ihre Mitarbeiter aus den Bereichen IT, Operations, Sicherheit und Kundenkommunikation an einen Tisch, um im Falle eines Angriffs besser vorbereitet zu sein.
- **DDoS-Schutz im Notfall:** Halten Sie einen Plan bereit, um im Krisenfall einen Anbieter von DDoS-Abwehrlösungen ins Boot zu holen. Wenn Sie einen Anbieter für DDoS-Schutz haben, rufen Sie dessen DDoS-Support-Hotline an.

Rezepte für Erkennung und Abwehr

Effektiver DDoS-Schutz auf Ebene 7 erfordert mehrere Erkennungs- und Abwehrstrategien. Es gibt mehrere anwendbare Methoden, die jeweils ihre Vorteile und Besonderheiten haben.

Verhaltens- und anomaliebasierte Erkennung

Vorteile: Dieser auf maschinellem Lernen und statistischen Analysen basierende Ansatz ermöglicht Ihnen, die normalen Trafficmuster zu verstehen und Abweichungen zu identifizieren, die auf einen DDoS-Angriff hinweisen könnten. Er ist äußerst effektiv bei der Abwehr komplexer, bisher unbekannter Angriffe.

Überlegungen: Für eine effektive Erkennung ist eine Lernphase erforderlich. Es kann bis zu mehreren Wochen dauern, um eine Ausgangsbasis für „normalen" Traffic zu bestimmen. In dieser Zeit ist die Erkennung möglicherweise nicht so effektiv. Das Modell kann falsch positive Ergebnisse zurückgeben, wenn es nicht präzise trainiert wird.

Raten- und durchsatzbasierte Erkennung

Vorteile: Diese einfach zu implementierende Methode überwacht die Rate und das Volumen von Anfragen und löst Warnungen oder Abwehrprozesse aus, wenn der Traffic vordefinierte Schwellenwerte überschreitet. Sie ist effektiv, wenn es um die schnelle Erkennung großangelegter volumetrischer Angriffe geht.

Überlegungen: Legitime Traffic-Spitzen, zum Beispiel bei Werbeveranstaltungen, können mit DDoS-Angriffen verwechselt werden. Die Methode erkennt möglicherweise keine kleineren Slow-Rate-Angriffe, die unter dem Radar bleiben.

Signaturbasierte Erkennung

Vorteile: Durch den Abgleich des Traffics mit einer Datenbank bekannter Angriffsmuster kann diese Methode erkannte Bedrohungen schnell identifizieren und blockieren. Sie ist sehr effektiv bei der Abwehr gängiger und bereits identifizierter Angriffsvektoren.

Überlegungen: Die Methode kann keine neuen oder modifizierten Angriffe erkennen, die nicht mit vorhandenen Signaturen übereinstimmen. Für eine durchgängige Effektivität sind regelmäßige Aktualisierungen erforderlich.

Challenge-Response-Tests

Vorteile: Dieser Ansatz prüft mithilfe bestimmter Challenges, ob eingehender Traffic von Menschen oder Bots generiert wird. CAPTCHA oder JavaScript-Berechnungen können Bots und automatisierte Angriffstools effektiv abwehren.

Überlegungen: Die Herausforderungen können das Nutzererlebnis beeinträchtigen, wenn sie aggressiv implementiert werden. Ausgefeiltere Bots können möglicherweise einige Challenge-Response-Tests bestehen, sodass regelmäßige Updates Ihrer Challenge-Mechanismen erforderlich sind.

Hybride Ansätze

Die Kombination mehrerer Erkennungs- und Abwehrstrategien kann einen umfassenderen Schutz bieten. Beispielsweise ermöglicht die Verwendung von anomaliebasierter Erkennung zur Kennzeichnung potenzieller Angriffe, ergänzt durch raten- und signaturbasierte Methoden für eine breitere Abdeckung, leistungsstärkere Verteidigungsmechanismen. Challenge-Response-Tests können ausgeklügelte Bots besser aus legitimen Nutzern herausfiltern.

Konventionelle Methoden

IP- und geografische Filterung: Durch das Blockieren oder Einschränken des Traffics aus bestimmten IP/CIDR-Bereichen und geografischen Regionen, die für Ihr Unternehmen nicht relevant sind, können Sie das Risiko von Angriffen aus diesen Bereichen verringern. Diese Methode kann zwar nützlich sein, wenn die Herkunft geschäftlicher Nutzer bekannt und begrenzt ist, sie bringt jedoch häufig Herausforderungen bei der laufenden Pflege und Aktualisierung der Liste zulässiger Quellen mit sich. Erfahrene Hacker können auch Proxys nutzen, um Geoblocking zu umgehen. Dennoch ist dies nach wie vor eine beliebte Wahl und eine erste Verteidigungsstrategie gegen Layer-7-DDoS-Angriffe.

Protokollanalyse auf der Anwendungsebene: Diese Methode kann Layer-7-DDoS-Angriffe abwehren, indem sie die Daten in Protokollen auf Anwendungsebene überprüft, um Anomalien oder schädliche Muster zu erkennen und proaktive Abwehrmechanismen zu ermöglichen. Sie kann ausgeklügelte DDoS-Angriffe verhindern, die konventionelle Sicherheitsmaßnahmen umgehen. Nachteilig ist jedoch der potenziell hohe Ressourcenverbrauch für die Deep Packet Inspection und eine höhere Wahrscheinlichkeit von False-Positives, wodurch unbeabsichtigt legitimer Traffic blockiert werden könnte.

Ein passendes und ausgewogenes Rezept für eine mehrschichtige DDoS-Verteidigungsstrategie finden

Die Entwicklung einer mehrschichtigen DDoS-Verteidigungsstrategie erfordert einen nuancierten Ansatz, der auf das spezifische Risikoprofil eines Unternehmens und die sich entwickelnde Cyberbedrohungslandschaft zugeschnitten ist. Im Kern erfordert diese Strategie eine erste Bewertung, um kritische Assets und wahrscheinliche Angriffsvektoren zu identifizieren, gefolgt von der Implementierung grundlegender Schutzmaßnahmen wie Ratenbegrenzung und Firewalls. Weitere Schritte erfordern eine Mischung aus anomaliebasierter Erkennung für neue Bedrohungen, signaturbasierter Erkennung für bekannte Angriffe und Challenge-Response-Mechanismen zum Filtern von Bots.

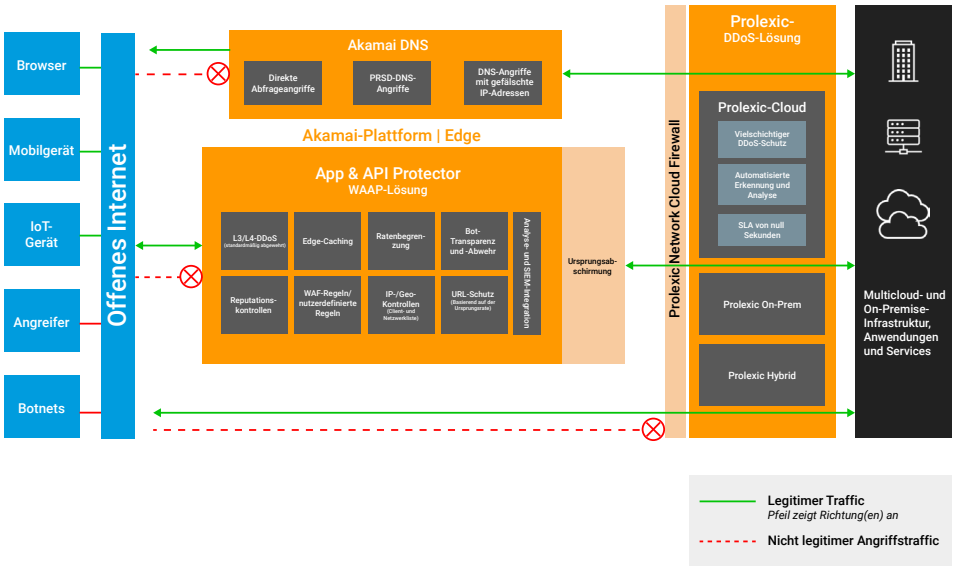
Durch die Integration adaptiver Bedrohungsinformationen wie Algorithmen, die TLS-Fingerabdruckmuster bekannter und neu entstehender DDoS-Angriffsquellen ermitteln, kann das Sicherheitssystem seine Abwehr automatisch anpassen, um den Traffic zu blockieren oder zu hinterfragen, der diesen Fingerabdruck ausweist. So lässt sich der Angriff effektiv abwehren. Ein umfassender Vorfallsreaktions- und Wiederherstellungsplan ist entscheidend, um Schäden zu minimieren und das Vertrauen während und nach einem Angriff aufrechtzuerhalten. Durch kontinuierliches Lernen und Anpassungen basierend auf vergangenen Angriffen und neuen Trends wird die Verteidigungsstrategie effektiv und widerstandsfähig.

Ein Finanzinstitut, das ausgeklügelten DDoS-Angriffen mit mehreren Vektoren ausgesetzt ist, bietet ein gutes Beispiel dafür, wie wichtig eine ausgewogene, mehrschichtige Verteidigungsstrategie ist. Die Auswirkungen, die Ausfallzeiten auf den Betrieb und das Vertrauen der Kunden haben können, machen solche Unternehmen zu bevorzugten Zielen.

Wenn sie ihre kritischen Ressourcen vor Unterbrechungen schützen und gleichzeitig die Kontinuität des Dienstes für ihre Kunden gewährleisten wollen, haben sie folgende Möglichkeiten: Sie können eine Kombination aus Erkennungs- und Abwehrmethoden wie der Erkennung von Traffic-Anomalien integrieren, konventionelle Methoden wie Ratenbegrenzung, IP/Geo-Filterung, IP-Reputation und Echtzeit-Bedrohungsinformationen nutzen und außerdem einen zuverlässigen Vorfallsreaktionsplan implementieren. Dieser umfassende Ansatz veranschaulicht beispielhaft, wie Unternehmen sich vor vielschichtigen DDoS-Angriffen schützen können, wie wir sie in der digitalen Landschaft von heute erleben.

Vorbereitung: Tiefgreifende Verteidigungsstrategie mit Edge-Architektur von Akamai

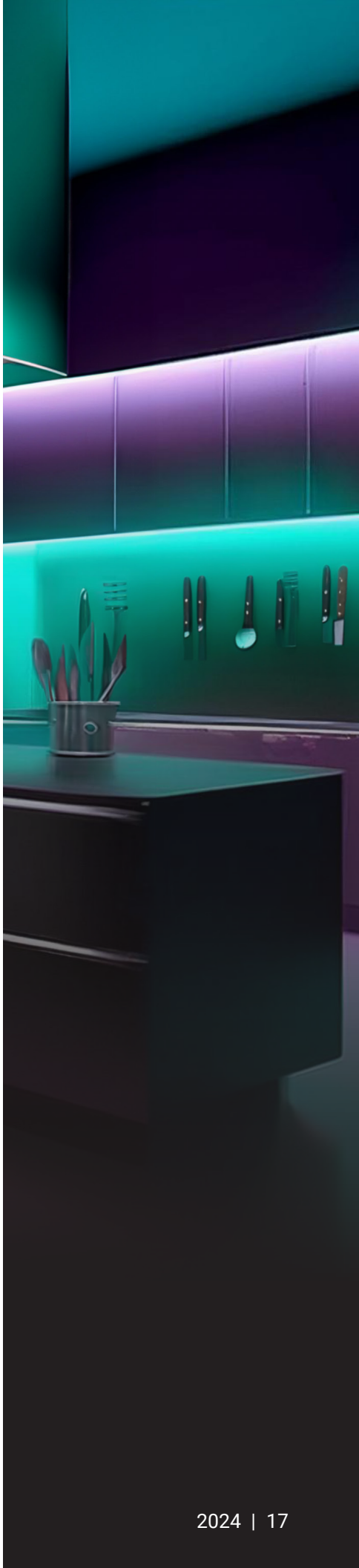
Der Ansatz von Akamai für den DDoS-Schutz auf Anwendungsebene ist mehrschichtig, umfassend und anpassungsfähig. Damit ist er geeignet, Websites, Anwendungen und APIs auch vor sehr komplexen Angriffen zu schützen. Unser App & API Protector nutzt mehrere Schlüsselfunktionen, die umfassenden Schutz bieten. Dazu werden eine Web Application Firewall, Bot-Transparenz und -Abwehr, API-Sicherheit und Layer-7-DDoS-Schutz in einem einzigen Produkt für weitreichenden Schutz kombiniert.



Referenzarchitektur für ganzheitlichen DDoS-Schutz mit den Lösungen Edge DNS, App & API Protector und Prolexic

Die DDoS-Schutzstrategie von Akamai basiert auf einer Edge-Schutz-Architektur, die den Traffic über die stark verteilte Plattform von Akamai weiterleitet, auf der jede Anfrage in Echtzeit überprüft wird. Dieses Setup schützt vor DDoS-, Web-App- und API-Angriffen sowie bösartigen Bots direkt an der Edge und verhindert, dass diese Anwendungen oder die Infrastruktur erreichen. Dadurch verbessert sich die Geschäftskontinuität. Eine schnelle, hochsichere und stets verfügbare Architektur, die den Angriffen entsprechend skalierbar ist, wird aufrechterhalten.

Die leistungsstarke Suite von Tools und Komponenten von Akamai bietet sowohl proaktive als auch reaktive Kontrollen, die jeweils einem bestimmten Zweck in der Gesamtstrategie für die Verteidigung dienen.



Proaktive Kontrollen

Proaktive Kontrollen helfen, Angriffe zu verhindern, bevor sie auftreten, und konzentrieren sich auf die Stärkung der Sicherheitslage, um Sicherheitsrisiken zu minimieren. Dazu gehören:

- **IP-Kontrollen (Block-IP, CIDR-Bereiche und ASNs):** Als grundlegende Verteidigungsschicht blockieren diese Kontrollen bekannte schädliche IP-Adressen oder Bereiche, die durch Threat Intelligence identifiziert werden.
- **Geo-Kontrollen (bestimmte Regionen blockieren):** Indem Unternehmen den Traffic aus bestimmten Regionen zulassen oder einschränken, können sie das Risiko von Angriffen aus Gebieten mit hohem Risiko präventiv begrenzen.
- **Regeln für Web Application Firewalls (WAF):** Die Implementierung von Regeln gegen bekannte Schwachstellen und Angriffsvektoren – etwa DDoS-Tools wie FiberFox – bietet eine starke erste Verteidigungslinie.
- **Kontrolle der IP-Reputation:** Durch heuristische Analysen bekannter schädlicher Ressourcen gewonnene Erkenntnisse über DDoS, Web-Scraping und andere bösartige Aktivitäten ermöglichen eine präventive Blockierung oder Prüfung von verdächtigem Traffic.
- **DDoS-Erkenntnisse aus der Plattform:** Dank der Einblicke in DDoS-Angriffe aus der global verteilten Akamai Edge-Plattform kann eine proaktive Abwehrstrategie für die Bekämpfung von DDoS-Angriffen auf Anwendungsebene entwickelt werden.
- **Caching:** Durch die Optimierung von Content-Caching kann die Belastung der Ursprungsserver erheblich reduziert werden. Dadurch können die DDoS-Auswirkungen indirekt abgeschwächt werden, da Anfragen aus dem Edge-Cache bedient werden.
- **Site Shield:** Wird der Ursprung abgeschirmt, indem nur Anfragen an Ursprünge über das Edge-Netzwerk von Akamai zugelassen werden, kann sich die Serverlast weiter verringern.

Reaktive Kontrollen

Reaktive Kontrollen sind Reaktionen auf einen erkannten Angriff, die darauf abzielen, seine Auswirkungen zu mindern und die Serviceverfügbarkeit aufrechtzuerhalten.

- **Ratenbegrenzung (Ratenrichtlinien):** Diese sind entscheidend für die Abschwächung plötzlicher Traffic-Spitzen, die auf einen DDoS-Angriff hindeuten können. Die Konfiguration kann für kundenspezifische Traffic-Profile eingerichtet und angepasst werden. Ratenbegrenzung ist oft die erste Verteidigungslinie beim Schutz des Kundenursprungs vor volumetrischen und verteilten DDoS-Angriffen.
- **Slow-POST-Schutz:** Diese auf langsame HTTP-POST-Angriffe ausgerichtete Kontrolle reagiert auf ungewöhnliche Traffic-Muster, die darauf abzielen, Serverressourcen zu erschöpfen.

- **Nutzerdefinierte Regeln in der WAF:** Sie müssen in der Lage sein, Regeln schnell an Bedrohungen anzupassen und flexible und dynamische Abwehrmechanismen anzubieten.
- **Bot-Transparenz und -Abwehr:** Mit maschinellem Lernen zur Erkennung von Browser-Imitation können Sie komplexe DDoS-Angriffe erkennen und blockieren, die auf Basis von Automatisierung operieren.
- **URL-Schutz mit intelligentem Load Shedding:** Mit Kontrollen, die übermäßige Anfragen auf den Ursprung beschränken und legitime Nutzer gegenüber schädlichem Traffic priorisieren, kann bei einem DDoS-Angriff die Verfügbarkeit von Diensten aufrechterhalten bleiben.
- **DDoS-Erkenntnisse aus der Plattform:** Load Shedding ist eine Kategorie des URL-Schutzes, die DDoS-Erkenntnisse aus der global verteilten Akamai-Plattform nutzt und unseren Kunden die Möglichkeit gibt, eine proaktive Strategie zur Abwehr von DDoS-Angriffen auf Anwendungsebene zu entwickeln.

Eine ausgewogene Zutatenmischung anhand Ihres Rezepts herstellen

- **Beispiel:** Ein großer Finanzdienstleister stellt mit der WAAP-Lösung von Akamai eine umfassende Verteidigungsstrategie zusammen

Manche Unternehmen sind möglicherweise häufiger Opfer von DDoS-Angriffen. So richteten sich einer Studie von Akamai zufolge mehr als ein Drittel der DDoS-Angriffe im Jahr 2023 gegen Finanzdienstleister. Ein großer Finanzdienstleister, ein Kunde von Akamai, erlebte einen gezielten Angriff auf seiner Anmeldeseite. Das Unternehmen war in der Lage, ein bewährtes Verteidigungsrezept zu befolgen. Sie können das Gleiche tun.


Angreiferprofil: Hacktivist


Ziel: Anmelde-Endpunkt


Methode: HTTP-POST-Flood


Angriffsquellen: ca. 66.000 IP-Adressen und rund 140 Länder

Rezept

Abwehr eines HTTP-POST-Flood-Angriffs

Zutaten:

Proaktive Kontrollen:

- **IP-Kontrollen**: Verwenden Sie Bedrohungsinformationen, um IP-Adressen oder CIDR-Bereiche zu blockieren, die mit bekannten schädlichen Entitäten verbunden sind.
- **Geo-Kontrollen**: Blockieren Sie den Traffic aus Regionen, die als Heimstatt von Hacktivisten-Gruppen bekannt sind, wie zum Beispiel Regionen, die mit „Anonymous Sudan“ in Verbindung stehen.
- **Regeln für Web Application Firewalls (WAF)**: Implementieren Sie Regeln, die speziell entwickelt wurden, um bekannten DDoS-Tools und -Taktiken entgegenzuwirken, einschließlich Mustern, die typisch für HTTP-GET-Floods sind.
- **Kontrolle der IP-Reputation**: Überwachen oder blockieren Sie aktiv (und in Echtzeit) den Traffic aus Quellen mit schlechten Reputationsbewertungen.
- **DDoS-Erkenntnisse aus der Plattform**: Nutzen Sie Erkenntnisse aus den globalen DDoS-Angriffsdaten von Akamai, um neue Bedrohungsvektoren zu antizipieren und ihnen entgegenzuwirken.
- **Site Shield**: Aktivieren Sie Firewall-Zugriffskontrolllisten, um nur Traffic vom Akamai Edge-Netzwerk zuzulassen und den Rest zu blockieren.

Reaktive Kontrollen:

- **Ratenbegrenzung**: Führen Sie Ratenrichtlinien ein, um plötzliche Traffic-Spitzen zu vermeiden, und legen Sie geeignete Schwellenwerte für Anfragen pro Sekunde an die Homepage fest. Optimieren Sie Ihre Ratenbegrenzung, indem Sie (1) Zeitfenster zur Messung der Anfragegeschwindigkeit auf eine Anfrage pro Sekunde reduzieren und (2) Ratenbegrenzung basierend auf der geografischen Lage und der Reputationsbewertung sich verbindender IP-Quellen anwenden, während Sie Quellen wie die IP-Adressen und Partner des Finanzinstituts in die Zulassungsliste aufnehmen.
- **Nutzerdefinierte Regeln in der WAF**: Erstellen Sie, sobald ein Angriff erkannt wurde, maßgeschneiderte Regeln, die den spezifischen Merkmalen des Angriffs entsprechen. Die Verwendung von stichprobenartigen Traffic-Kontrollen in Ihren nutzerdefinierten Regeln sorgt dafür, dass in Traffic-Analysen die Hauptangriffsziele effizienter untersucht werden. Die Verwendung von IP/Geo-Kontrollen ermöglicht dagegen eine schnelle Abwehr.
- **Bot-Transparenz und -Abwehr**: Nutzen Sie die Möglichkeit zur Erkennung von Browser-Imitation, um Anfragen zu identifizieren und zu blockieren, die legitimes Nutzerverhalten nachahmen, aber Teil des Flood-Angriffs sind.
- **URL-Schutz**: Setzen Sie Kontrollen in Kraft, um die Raten von Anfragen speziell an die Anmelde-URL zu begrenzen und so die Bandbreite für legitime Nutzer aufrechtzuerhalten. Das Einrichten von intelligentem Load Shedding mit Kategorien wie Proxys, Tor-Exit-Knoten, einfachen Bots, IPs mit geringer Reputation usw. trägt dazu dabei, echten Nutzerverkehr gegenüber diesen wahrscheinlich schädlichen Quellen zu priorisieren.

Zubereitungsart:

Überprüfungsphase:

- **Überprüfung der Konfiguration**: Führen Sie eine gründliche Überprüfung Ihrer aktuellen Sicherheitslage durch. Konfigurieren Sie Ihre proaktiven Kontrollen auf der Grundlage Ihrer Ergebnisse, um sicherzustellen, dass alle relevanten Geo- und IP-Kontrollen ordnungsgemäß verwaltet werden.
- **Optimierung der Konfiguration**: Optimieren Sie die Konfiguration, um ungewöhnliche Traffic-Muster zu erkennen und abzuwehren, einschließlich derjenigen, die für HTTP-POST-Flood-Angriffe charakteristisch sind.

Erkennungs- und Abwehrphase:

- **Überwachung und Warnungen**: Die Edge Defense-Architektur von Akamai kann den eingehenden Traffic auf Muster überwachen, die auf einen DDoS-Angriff hinweisen könnten. Sie können Warnmeldungen für ungewöhnliche Traffic-Spitzen oder -Muster einrichten, die bekannten DDoS-Methoden wie HTTP-POST-Flood entsprechen.
- **Erkennung und Abwehr**: Verschiedene proaktive Kontrollen wie IP-Reputation, Caching und IP/Geo-Kontrollen bieten bei korrekter Einrichtung automatisch Erkennungs- und Abwehrfunktionen. Sobald ein Angriff erkannt wird, greifen Kontrollen wie Ratenbegrenzung, URL-Schutz und Erkennung von Browser-Imitation automatisch ohne Eingreifen des Nutzers.
- **Analyse und Anpassung**: Analysieren Sie kontinuierlich Angriffsmuster und passen Sie Ihre Abwehrmaßnahmen in Echtzeit an, um neuen Taktiken entgegenzuwirken. Erstellen Sie zum Beispiel passgenaue nutzerdefinierte Regeln oder Richtlinien zur Ratenbegrenzung, die auf der Analyse des aktuellen Traffics basieren.

Wiederherstellung und Analyse nach dem Angriff:

- **Protokollanalyse**: Führen Sie nach dem Angriff eine detaillierte Analyse der Traffic-Protokolle durch, um die Angriffsvektoren und die Effektivität der eingesetzten Kontrollen zu ermitteln.
- **Anpassungen**: Nehmen Sie auf der Grundlage der Erkenntnisse aus der Angriffsanalyse die erforderlichen Anpassungen an den proaktiven und reaktiven Kontrollen vor.

Serviervorschläge:

- Überprüfen und aktualisieren Sie regelmäßig Ihre Verteidigungsstrategie, um sich auf neue DDoS-Taktiken einzustellen. Diese Überprüfungen können je nach konkretem Bedarf, Bedrohungslage und branchenspezifischen Best Practices von Unternehmen zu Unternehmen erheblich variieren. Ein Finanzdienstleister benötigt solche Überprüfungen möglicherweise jedes Quartal, während eine E-Commerce-Plattform halbjährliche Reviews zur Vorbereitung auf saisonale Einkaufsspitzen anvisieren könnte.
- Schulen Sie das Sicherheitsteam kontinuierlich, damit es neue DDoS-Angriffsvektoren erkennt und darauf reagieren kann.
- Führen Sie simulierte Angriffe durch, um die Wirksamkeit der eingeleiteten Maßnahmen zu testen und zu ermitteln, wie gut das Team auf echte Vorfälle vorbereitet ist.

Wiederherstellung und Analyse nach dem Angriff

Bei der Abwehr von DDoS-Angriffen auf Anwendungsebene (Layer 7) ist die Phase nach dem Angriff entscheidend, um künftige Abwehrmaßnahmen zu stärken und den Gegner zu verstehen. Hier gibt es zwei wichtige Schritte: Die Analyse des Angriffsmusters und die Verbesserung Ihrer Verteidigung auf Grundlage Ihrer Analyse. Diese Schritte sind entscheidend für die Entwicklung einer robusten Verteidigungsstrategie und die Gewährleistung der Kontinuität und Integrität von Online-Diensten.

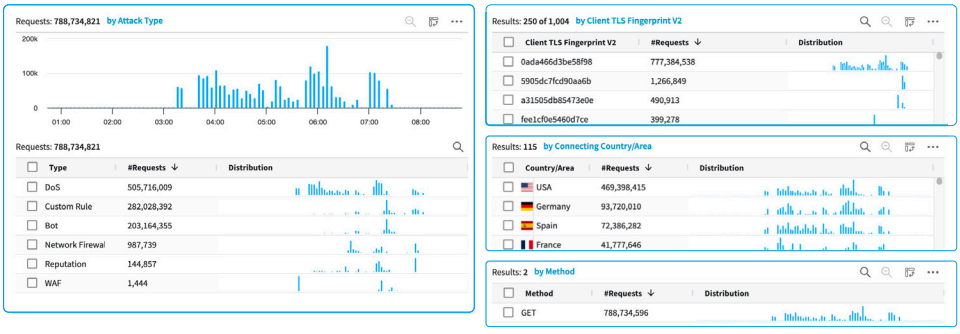
Analyse des Traffics und des Angriffsmusters

Der nächste Schritt nach der Reaktion auf einen Angriff besteht darin, den Vorfall zu analysieren, um zu verstehen, welche Strategie funktioniert hat und welche nicht. Diese Bewertung umfasst längerfristige Faktoren wie die Auswirkungen auf das Kundenvertrauen, die Datenintegrität und potenzielle finanzielle Verluste. Umfassende Sicherheitsanalyse-Systeme wie Akamai Web Security Analytics sind in dieser Phase unverzichtbare Tools, mit denen Unternehmen den Traffic und seine Auswirkungen verstehen können.

Diese Analyse beinhaltet die Untersuchung der Taktiken, Techniken und Verfahren (TTPs), die von den Angreifern verwendet werden. Hier sind einige der wichtigsten Fragen:

- Welcher Art war die Traffic-Spitze?
- Wurden bestimmte Anwendungsfunktionen ins Visier genommen?
- Hat der Angriff bekannte Schwachstellen ausgenutzt?

Akamai Web Security Analytics kann Anomalien in den Traffic-Mustern identifizieren, den geografischen Ursprung des Angriffs ermitteln und den Angriffstyp basierend auf beobachteten Verhaltensweisen klassifizieren. Das folgende Beispiel zeigt einige der Traffic-Merkmale oder -Dimensionen, die zur Untersuchung eines DDoS-Angriffs angewendet werden können.



Die gezeigten Bilder stammen aus Web Security Analytics, das eine beispiellose Transparenz und proaktive Analyse von Sicherheitsereignissen bietet

Überprüfen und Aktualisieren von Verteidigungsstrategien basierend auf Ihrer Angriffsanalyse

Die Überprüfung und Aktualisierung von Verteidigungsstrategien auf der Grundlage von Angriffsanalysen ist eine entscheidende Komponente zur Stärkung der Cybersicherheit eines Unternehmens. Durch die Untersuchung der Besonderheiten eines früheren Angriffs können Unternehmen Schwachstellen in ihren aktuellen Abwehrmechanismen erkennen und fundierte Anpassungen vornehmen. Im Folgenden finden Sie einige Beispiele, wie dieser Prozess mithilfe von Akamai Web Security Analytics angewendet werden kann.

Beispiel 1: Aktualisieren von WAF-Regeln basierend auf Angriffsmustern

Szenario: Ein Unternehmen ist einem Layer-7-DDoS-Angriff ausgesetzt, in dem die Webanwendung mit einem Trommelfeuer schädlicher, an die Homepage der Anwendung gerichteter Anfragen attackiert wird.

Überprüfen: Die Angriffsanalyse zeigt, dass die bestehenden WAF-Regeln (Web Application Firewall) mehr als 90 % des Angriffstraffics richtig erkannt und blockiert haben. Die restlichen fast 10 % drangen jedoch durch, weil es eine explizite Geo-Zulassungsliste gab, die es den Angriffsquellen dieser Region gestattete, die Anwendung zu überfordern.

Aktualisieren: Auf der Grundlage dieser Analyse hat das Unternehmen seine WAF-Konfigurationen aktualisiert, um eine nutzerdefinierte WAF-Regel zu verwenden, die den spezifischen Merkmalen des Angriffstraffics aus dieser Region entspricht. Überschreibungen können die betreffende Region weiterhin zulassen, blockieren aber die spezifischen Attribute des Angriffstraffics. Außerdem wurden die Einstellungen der Ratenbegrenzung für diese Region strenger gefasst.

Beispiel 2: Verbesserung des Ursprungsschutzes

Szenario: Der Anmeldeprozess einer Einzelhandelswebsite wird durch einen hochgradig verteilten und ausgeklügelten Layer-7-DDoS-Angriff beeinträchtigt, der automatisierte Bots nutzt.

Überprüfen: Die Analyse nach dem Angriff zeigt, dass der Angriffstraffic stark verteilt war und aus mehr als 150 Ländern und Hunderten von TLS-Fingerabdrücken kam, die wie ein legitimer Browser aussehen. Ein erheblicher Teil des Traffics stammte von Cloud-Anbietern, von denen einige in der Zulassungsliste als vertrauenswürdige Partnerquellen geführt wurden. Während der Angriff effektiv abgeschwächt wurde, ergab die Analyse, dass zusätzliche Verteidigungsmaßnahmen erforderlich waren.

Aktualisieren: Um rechenintensive URLs wie zum Beispiel Bezahlvorgänge zu schützen, implementierte dieses Unternehmen URL-Schutz. Diese Funktion wurde speziell entwickelt, um rechenintensive URLs und API-Endpunkte vor stark verteilten DDoS-Angriffen auf Anwendungsebene zu schützen. Ein Sicherheitsarchitekt ermöglichte außerdem intelligentes Load Shedding für Bots, Proxys, IP-Reputation usw. Diese Unterfunktion des URL-Schutzes kann echten Nutzertraffic priorisieren, indem Anfragen von wahrscheinlich schädlichen Quellen zuerst abgelehnt werden.

Das Unternehmen entschied außerdem, integrierte Bot-Schutzfunktionen in der WAF zu aktivieren. Diese Funktionen hatte das Unternehmen zuvor nicht angemessen berücksichtigt, da eine Bot-Lösung vor Ort existierte, die aber bei diesem mit hoher Geschwindigkeit ausgeführten Angriff nicht skalierbar war.

Beispiel 3: Implementieren von Ratenbegrenzungen für API-Endpunkte

Szenario: Ein API-Endpunkt der Anwendung eines Finanzdienstleisters wird von einer Flut betrügerischer Transaktionsanfragen überfordert. Das deutet auf einen Layer-7-DDoS-Angriff hin, der darauf abzielt, Serverressourcen zu erschöpfen.

Überprüfen: Die Analyse des Angriffsmusters zeigt, dass die Angreifer gezielt schlecht geschützte API-Endpunkte anvisierten, die nicht in der Lage waren, eine große Anzahl von Anfragen zu verarbeiten.

Aktualisieren: Als Reaktion darauf implementierte das Unternehmen eine strenge Ratenbegrenzung für alle API-Endpunkte, insbesondere diejenigen, die als anfällig identifiziert wurden. Außerdem wurde ein dediziertes API-Sicherheits-Add-on eingeführt, das erweiterte Ebenen für API-Sicherheit bietet, einschließlich API-Logikmissbrauch, Bedrohung durch Schatten-APIs und API-Schwachstellenüberwachung.

Strategische Erkenntnisse

- **Kontinuierliche Überwachung und Protokollierung:** Richten Sie zuverlässige Überwachungs- und Protokollierungssysteme ein, um Anomalien sofort zu erkennen und Schäden sowohl während als auch nach einem Angriff genau zu bewerten.
- **Schwachstellenmanagement:** Aktualisieren und patchen Sie Systeme regelmäßig, um die mit bekannten Schwachstellen verbundenen Gefahren und das Risiko der Ausnutzung zu verringern.
- **Analyse des Angriffstraffics:** Verwenden Sie geeignete Transparenztools für eine tiefgreifende Analyse der Angriffsmuster, um die Methoden und Absichten der Angreifer zu verstehen.

Analyse nach dem Angriff

Die Bewertung des Schadens und die Analyse des Angriffsmusters sind wichtige Komponenten einer robusten Layer-7-DDoS-Verteidigungsstrategie. Diese Schritte fördern nicht nur das Verständnis und helfen, die unmittelbaren Auswirkungen eines Angriffs abzumildern, sondern ermöglichen auch die kontinuierliche Verbesserung der Verteidigungsmechanismen. So wird gewährleistet, dass Sie auf künftige Bedrohungen besser vorbereitet sind.

Pflegen und Aktualisieren Ihrer Rezepte

Die Aufrechterhaltung einer starken Layer-7-DDoS-Abwehr erfordert eine ständige Überwachung der neuesten Trends und Techniken.

Angreifer kombinieren immer wieder Angriffsmuster und machen sich neue Tools und Schwachstellen zunutze. Um diesen Bedrohungen proaktiv entgegenzuwirken, müssen Unternehmen Zeit und Mühe in die Forschung, Überwachung, Bewertung von Abwehrmaßnahmen, die Automatisierung von Schutzmechanismen und die Zusammenarbeit mit der Threat-Intelligence-Community investieren.

Die Beobachtung der führenden Cybersicherheitsforen ist ein guter Anfang, aber nicht mehr. Wir schlagen einen präskriptiveren Ansatz vor:

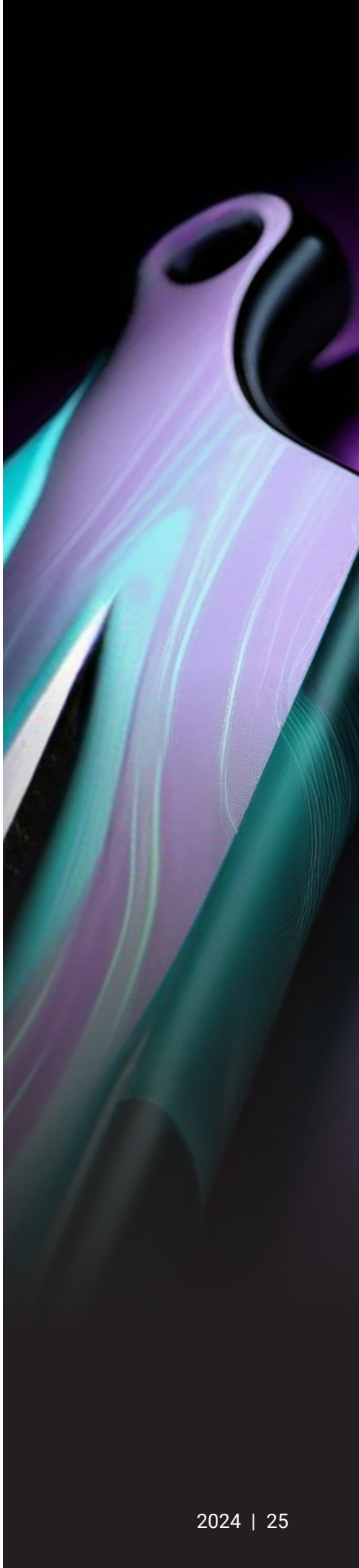
Kontinuierliche Überwachung und Bewertung: Überwachen Sie Ihre Netzwerk- und Anwendungsperformance regelmäßig, um neue Muster oder Anomalien zu erkennen, die auf neue Bedrohungen hinweisen. Nutzen Sie diese Daten, um die Effektivität Ihrer bestehenden Verteidigungsmechanismen zu bewerten und Bereiche zu identifizieren, in denen Verbesserungen oder Anpassungen erforderlich sind.

Ein Anti-DDoS-Team bilden: Benennen Sie eine verantwortliche Person oder ein Team innerhalb des Unternehmens, das die DDoS-Angriffslandschaft erforscht und überwacht und dem gesamten Unternehmen mindestens vierteljährlich mit allen wichtigen Erkenntnissen und Empfehlungen Bericht erstattet.

Mit der Threat-Intelligence-Community interagieren: Angreifer kommunizieren untereinander über die neuesten, effektivsten Methoden. Es gibt keinen Grund, warum Sie nicht mit Kollegen in anderen Unternehmen und Branchen über die besten Schutzmaßnahmen kommunizieren sollten. Bleiben Sie auf dem Laufenden, was die neuesten Bedrohungsinformationen angeht. Abonnieren Sie Sicherheitsfeeds, beteiligen Sie sich an Cybersicherheitsforen und arbeiten Sie mit Kollegen in Ihrer Branche zusammen. Mithilfe dieser Informationen können Sie neue Angriffsmethoden vorhersehen und Ihre Abwehrmechanismen entsprechend anpassen.

Auf Ihren Anbieter für Cybersicherheit verlassen: Technologieanbieter haben oft spezielle Forschungsgruppen zu Bedrohungen, und Anbieter mit einem Netzwerk zur Inhaltsbereitstellung können Erkenntnisse liefern, die anderswo nicht verfügbar sind. Nutzen Sie diese Lernmöglichkeiten, wann und wo immer Sie können. Es ist auch sinnvoll, regelmäßig die Expertise von Sicherheitsberatern einzuholen.

Eigene Verteidigungsmechanismen testen: Wer sich nicht vorbereitet, bereitet sein Scheitern vor. Oder: Übung macht den Meister. Sie können diese Binsenweisheit auslegen, wie Sie wollen, die Botschaft bleibt immer gleich: Regelmäßiges Testen und Üben zahlt sich aus.



Führen Sie regelmäßige Überprüfungen und simulierte Angriffsszenarien durch (Red-Team-Übungen), um die Widerstandsfähigkeit Ihrer Verteidigungsstrategien zu testen. Diese Übungen decken Schwächen in Ihrem aktuellen Setup auf und liefern Erkenntnisse darüber, wie Angreifer Ihr System ausnutzen könnten.

Testen Sie Ihr Netzwerk mindestens einmal im Jahr. Auch aktuelle Angriffsprofile können eine gute Referenz für einen Testfall sein, zumal dann, wenn es sich um das Beispiel eines Unternehmens aus Ihrer Branche handelt.

Erkenntnisse mit der Community teilen: Man kann es nicht oft genug wiederholen: So wie Angreifer ihre Tools und Taktiken teilen, sollten auch Unternehmen ihr Wissen über erfolgreiche Verteidigungsstrategien weitergeben.

Durch die Dokumentation von Erfolgen und Misserfolgen können Cybersicherheitsexperten praxisnahe Einblicke liefern, die die kollektive Wissensdatenbank bereichern. Die Teilnahme an Branchenforen, Mentoringangebote für Neulinge und die Teilnahme an Kooperationsprojekten sind für die Förderung eines leistungsstarken Abwehr-Ökosystems von entscheidender Bedeutung. Solche Bemühungen tragen nicht nur zur Entwicklung wirksamer Strategien und Tools bei, sondern lassen auch einen vielfältigen Erfahrungs- und Erkenntnispool entstehen, der eine Anpassung an die sich wandelnden Taktiken der Cyberkriminellen ermöglicht. Dieser Geist der Zusammenarbeit ist entscheidend, um in der Cybersicherheitslandschaft einen Schritt voraus zu sein. Insofern ist jeder Beitrag zum Aufbau einer stärkeren, widerstandsfähigeren digitalen Welt wertvoll.

Wichtige Erkenntnisse

Die DDoS-Bedrohungslandschaft ist dynamisch. Angreifer suchen ständig nach neuen Wegen, um Abwehrmaßnahmen zu umgehen. Die Pflege und Aktualisierung Ihrer Layer-7-DDoS-Schutzstrategien ist ein kontinuierlicher Prozess, der Wachsamkeit, Anpassungsfähigkeit und einen proaktiven Ansatz erfordert. Wenn Sie auf dem Laufenden bleiben, regelmäßige Tests und Überprüfungen durchführen und eine Kultur der kontinuierlichen Verbesserung fördern, können Sie einen soliden Schutz vor aktuellen und zukünftigen Bedrohungen aufrechterhalten.

Fazit

Es ist klar, dass Layer-7-DDoS-Angriffe nicht nur ausgefeilter geworden sind, sondern dank der Fortschritte bei der Automatisierung und der Koordination zwischen Angreifern auch einfacher zu starten sind. Gleichzeitig müssen Unternehmen eine größere, komplexere Landschaft verteidigen, auch wenn die Kosten für Ausfälle steigen.

Tatsächlich ist es keine leichte Aufgabe, ein Verteidigungsrezept zusammenzustellen. Keine einzelne Methode bietet ein Allheilmittel für Layer-7-DDoS-Angriffe. Wie wir gezeigt haben, bietet ein mehrgleisiger Ansatz, der verschiedene Erkennungs- und Abwehrstrategien kombiniert, die robusteste Verteidigung.

Darüber hinaus sollten Sie bei der Entscheidung für die richtigen Methoden die spezifischen Anforderungen, Traffic-Muster und das Risikoprofil der Anwendung oder des Dienstes berücksichtigen, die/der geschützt werden soll. Sie können keine Verteidigung aufbauen, wenn Sie Ihr Unternehmen, Ihren Traffic und Ihre Schwachstellen nicht kennen. Regelmäßige Aktualisierungen und Anpassungen dieser Strategien sind für die Anpassung an die sich entwickelnde DDoS-Bedrohungslandschaft unerlässlich.

Schließlich ist auch klar geworden, dass die Arbeit nicht getan ist, sobald ein Angriff vorbei ist. Analysen und Anpassungen nach dem Angriff sind für den anhaltenden Erfolg von entscheidender Bedeutung und können eine wichtige Rolle beim Wissensaustausch und bei der Karriereentwicklung spielen, wenn Sie schon einmal dabei sind.

Glücklicherweise kann Sie Akamai bei jedem Schritt unterstützen. Von App- und API-Schutz über unerreichte Einblicke in den globalen Traffic bis hin zu Expertenanalysen nach Angriffen: Viele Unternehmen nutzen die Möglichkeit, alle benötigten Tools für Layer-7-DDoS-Schutz von einem einzigen Anbieter zu beziehen.

Sehen Sie sich den Layer-7-DDoS-Schutz von Akamai in der Praxis an.
Starten Sie eine kostenlose Testversion von App & API Protector.

Akamai

Mitwirkende

Redaktion und Text

Aseem Ahmed
Barney Beal

Prüfung und fachliche Expertise

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

Marketing und Veröffentlichung

Georgina Morales Hampe
Shivangi Sahu

Akamai

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 (ehemals Twitter) und LinkedIn.
Veröffentlicht: Oktober 2024.