Abwehr von DDoS-Angriffen in Hybrid-Cloud-Umgebungen

Inhaltsverzeichnis

DDoS entwickelt sich weiter

Distributed Denial of Service (DDoS), eine der ältesten Arten von Cyberbedrohungen, entwickelt sich weiter und ist mittlerweile ein hochentwickeltes Tool für Cyberkriminelle und ideologisch motivierte Hacktivisten. Tatsächlich stellen DDoS-Angriffe nicht nur für große und kleine Unternehmen ein Sicherheitsrisiko dar, sondern auch für kritische öffentliche Infrastrukturen in Bereichen wie Gesundheitswesen, Energie- und Versorgungseinrichtungen und Bildung.

Diese Dynamik wird durch die zunehmende Nutzung von Cloud-Computing-Ressourcen durch öffentliche und private Einrichtungen zusätzlich erschwert. Wenn diese Unternehmen die Cloud mit ihren bereits vorhandenen Ressourcen vor Ort kombinieren, wird die daraus resultierende hybride Umgebung deutlich komplexer. Anwendungen, Programmierschnittstellen (APIs), Daten, Microservices und Workloads müssen nun eine fragmentierte Umgebung passieren. Die verschiedenen Architekturen dieser Umgebungen schaffen neue Schwachstellen und eine zersplitterte Angriffsfläche, die von Cyberkriminellen genutzt werden kann, um immer ausgefeiltere und verheerendere DDoS-Angriffe zu starten.

Unternehmen bemühen sich, sicherzustellen, dass ihre digitale Infrastruktur geschützt ist. Sie benötigen eine integrierte und hybride DDoS-Schutzplattform, die ihre Infrastruktur vor Ort (Private Cloud) vor kurzen, aber heftigen DDoS-Angriffen schützen kann, aber auch die Skalierbarkeit und Kapazität von Cloud-Scrubbing für große volumetrische DDoS-Angriffe nutzt.

Trends deuten darauf hin, dass DDoS-Angriffe immer stärker und immer häufiger werden. Im Februar 2023 hat Akamai den größten DDoS-Angriff abgewehrt, der jemals gegen einen Akamai Prolexic-Kunden im asiatisch-pazifischen Raum (APAC) gestartet wurde. Der Traffic erreichte Spitzenwerte von 900,1 Gigabit pro Sekunde und 158,2 Millionen Pakete pro Sekunde (Mpps). Das war nur wenige Monate nach dem bisher größten DDoS-Angriff auf einen Akamai Prolexic-Kunden in Europa, bei dem der Traffic abrupt auf 704,8 Mpps anstieg, um den Geschäftsbetrieb des Unternehmens zu unterbrechen. Darüber hinaus hat Akamai den bisher größten DDoS-Angriff überhaupt abgewehrt: ein weltweit verteilter Angriff mit 1,44 Terabit pro Sekunde (Tbit/s) und 385 Mpps, der fast zwei Stunden andauerte. Basierend auf unseren Einblicken in Traffic und Angriffsmuster hat Akamai festgestellt, dass DDoS-Angriffe im Laufe des Jahres 2023 häufiger, länger, hochgradig ausgereift (mit mehreren Vektoren) und auf horizontale Ziele ausgerichtet waren (Angriffe auf mehrere IP-Ziele im selben Angriffsereignis).

Die wachsende Bedrohung

Heute handelt es sich bei den meisten DDoS-Angriffe um Angriffe mit mehreren Vektoren, bei denen oft mehr als 10 Angriffsvektoren eingesetzt werden, um rudimentäre DDoS-Schutzsysteme und -plattformen zu überwältigen. Laut der internen Bedrohungsinformationen von Akamai hat sich die Anzahl der DDoS-Angriffe mit mehreren oder horizontalen Zielen von 2022 auf 2023 verdoppelt. Unterdessen wiesen Größe, Umfang und Dauer der volumetrischen DDoS-Angriffe im Jahr 2023 die höchsten Werte auf, die bisher jemals gemessen wurden.

Die Sicherheitsplanung für Unternehmen wird durch die Entwicklung verschiedener Taktiken erschwert, die Angreifer in Verbindung mit herkömmlichen volumetrischen Angriffen anwenden.

DDoS-Angreifer nutzen alle potenziellen Schwachstellen aus, wie z. B.:

- Websites
- Webanwendungen und andere Dienste für Unternehmen
- VPN-Konzentratoren für den Remotezugriff auf Unternehmensressourcen
- SD-WAN-Controller
- Programmier-schnittstellen (APIs)
- DNS-Server (Domain Name System) und Ursprungsserver
- Rechenzentrum und Netzwerkinfrastruktur

DNS-Infrastruktur

DDoS-Angriffe auf die DNS-Infrastruktur von Unternehmen finden immer häufiger statt, insbesondere NXDOMAIN-Angriffe (auch bekannt als Pseudo-Random-Subdomain-Angriffe, DNS-Water-Torture-Angriffe oder DNS-Überlastungsangriffe). Mehr als 60 % der DDoS-Angriffe, die 2023 von Akamai abgewehrt wurden, wiesen eine DNS-Komponente auf, wobei NXDOMAIN-Angriffe etwa die Hälfte dieser DNS-DDoS-Angriffe ausmachten. Diese Angriffe stellen ein erhebliches Risiko für das Geschäftsergebnis und den Ruf eines Unternehmens dar, denn wenn das DNS eines Unternehmens ausfällt, ist es offline.

Angriffe auf Anwendungsebene

DDoS-Angriffe auf Anwendungsebene (Layer 7) sind ausgefeilter geworden, da Angreifer ihre Taktiken weiterentwickeln, um scheinbar harmlose Logik und Workflows auszunutzen. Eine 2023 entdeckte HTTP/2-Schwachstelle führte zum größten aufgezeichneten Layer 7-DDoS-Angriff aller Zeiten.

DDoS-as-a-Service

Organisierte Gruppen von Cyberkriminellen wie Anonymous Sudan und Killnet bieten DDoS-as-a-Service an. In diesem Szenario bieten Gruppen ihre Dienste, in der Regel ein Botnet, gegen eine Gebühr an und führen Angriffe im Namen eines Kunden aus. Diese DDoS-for-Hire-Services können für motivierte Gruppen äußerst profitabel sein.

Ransomware + DDoS = RDDoS

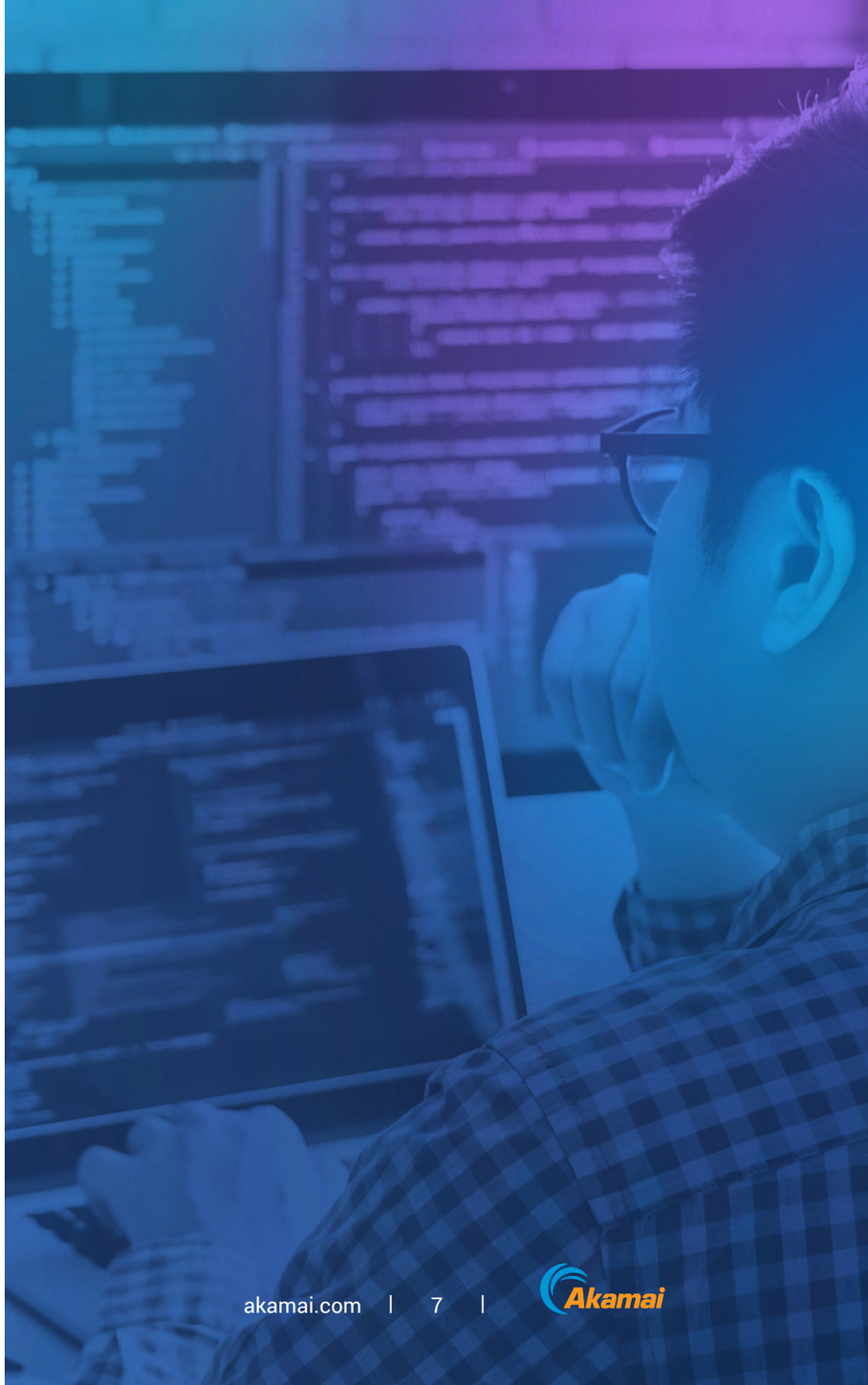
Die Verfügbarkeit von Taktiken wie DDoS-as-a-Service erleichtert Angreifern auch die Nutzung von DDoS-Angriffen als Vorwand, um Sicherheitsteams abzulenken. Währenddessen starten sie parallel einen Ransomware-Angriff oder einen dreifachen Erpressungsangriff. Diese werden als Ransom-DDoS-Angriffe (RDDoS) bezeichnet.

Die Folgen eines DDoS-Angriffs

Bei volumetrischen und protokollbasierten DDoS-Angriffen auf die Netzwerkebene (Layer 3) und die Transportebene (Layer 4) versuchen Angreifer, den Webtraffic zum Erliegen zu bringen, die Server zu überlasten und die Kapazität der Tabelle für die Zustandserfassung zu erschöpfen, um den Zugang zu Netzwerken und Services zu blockieren. Bei Layer-7-Angriffen zielen Angreifer darauf ab, die Webperformance und das Nutzererlebnis durch Vektoren wie Low-and-Slow-Angriffe und HTTP-Floods zu unterbrechen, um Ausfallzeiten zu erzeugen, die sich auf das Geschäftsergebnis auswirken. DDoS-Angriffe auf DNS können etwas komplexer sein – je nach Art des Angriffs können sie sich auf verschiedene Ebenen des Netzwerks eines Unternehmens auswirken. Beispielsweise können DNS-DDoS-Angriffe mit Reflexions- und Verstärkungstechniken Traffic auf Layer 3 und 4 des Unternehmensnetzwerks erzeugen, während bei DDoS-Angriffen mit NXDOMAIN- oder DNS-Flood-Technik häufig die Anwendungsebene eines Netzwerks betroffen ist.

Die Ausfälle wirken sich jedoch nicht nur auf die Kosten der anvisierten Services und nicht verfügbaren Anwendungen aus. Laut Ponemon Institute belaufen sich die durchschnittlichen Kosten eines DDoS-Angriffs für ein Unternehmen auf 1,7 Millionen US-Dollar, bedingt durch einen Mehrbedarf an technischem Support, höheren Ressourcenaufwand für die Reaktion auf Vorfälle, interne Eskalationen, Rechtskosten, Betriebsstörungen und weniger produktive Mitarbeiter. Darüber hinaus hat das Offline-Gehen für verbraucherorientierte Unternehmen wie Finanzdienstleister, Gaming- und Medienunternehmen sowie E-Commerce-Unternehmen nicht nur finanzielle Schäden zur Folge, sondern vor allem auch irreparable Reputationsschäden.

Es steht viel auf dem Spiel, und mit der zunehmenden Migration zu Hybrid-Cloud-Infrastrukturen wird das Risiko immer größer.

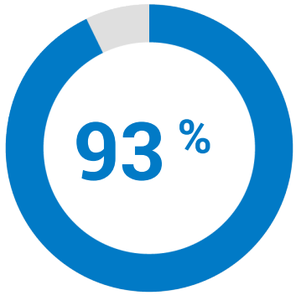


Hybrid- und Multicloud-Umgebungen erschweren weiterhin die Sicherheit

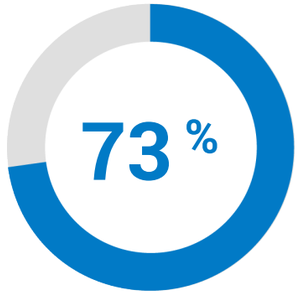
Da Unternehmen einige Workloads in Rechenzentren vor Ort oder Private Clouds verwalten und andere Anwendungen in Public Cloud-gehostete Umgebungen verlagern, ist es mit diesem Ansatz der hybriden Infrastruktur noch schwieriger, robuste Sicherheit zu gewährleisten. Ebenso verfügen Unternehmen häufig über eine hybride DNS-Infrastruktur, in der einige ihrer autoritativen DNS-Zonen in der Cloud verwaltet werden, während die verbleibenden Zonen von lokalen Nameservern und globalen Server Load Balancern (GSLBs) verwaltet werden. Es gibt Gründe, warum Unternehmen möglicherweise weiterhin eine lokale DNS-Infrastruktur unterhalten. Beispielsweise haben sie eventuell bereits beträchtliche Investitionen in die Einrichtung einer lokalen Infrastruktur getätigt, um Compliance-Anforderungen zu erfüllen. Die Migration sämtlicher DNS in die Cloud ist äußerst komplex und sprengt daher unter Umständen den finanziellen Rahmen.

Cyberkriminelle sind sich der Schwachstellen bewusst, die sich aus einer derart fragmentierten Umgebung ergeben. Sie sind bestrebt, die Schwächen in der Sicherheitsarchitektur und -strategie eines Unternehmens auszunutzen, die durch inkonsistente Sicherheitsrichtlinien und -anforderungen entstehen. Sie versuchen, die Schwierigkeiten bei der Fehlerbehebung in einer heterogenen und fragmentierten cloudbasierten Infrastruktur zu nutzen.

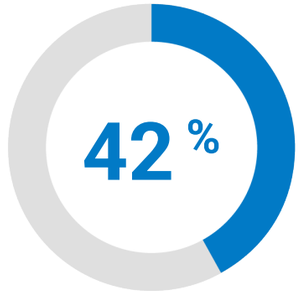
Leider übernehmen nicht alle Anbieter von Public-Cloud-Umgebungen im gleichen hohen Maße die Verantwortung für die Sicherheit. Viele Unternehmen treffen falsche Annahmen, die sie angreifbar machen. So waren in einer IBM-Umfrage 73 % der Befragten der Ansicht, dass die Hauptverantwortung für den Schutz von Software-as-a-Service (SaaS) bei dem Public-Cloud-Dienstanbieter (CSP) läge. 42 % glaubten, dass hauptsächlich der CSP für den Schutz der Infrastruktur as a Service (IaaS) in der Cloud verantwortlich sei. Dieses mangelnde Wissen über die Verantwortung für Schutzmaßnahmen kann die Sicherheit beeinträchtigen – ein Risiko, das kein Unternehmen eingehen sollte.



wenden eine Multicloud-Strategie an



glauben, dass die Verantwortung für den SaaS-Schutz bei den CSPs liegt



glauben, dass die CSPs für den Schutz der Cloud-IaaS verantwortlich sind

Unternehmen wenden sich an DDoS-Sicherheitsanbieter, die eine integrierte, hochgradig skalierbare und umfassende DDoS-Schutzplattform bieten, die ihre Anwendungen, APIs, DNS und die zugrunde liegende Infrastruktur, die all das ermöglicht, schützen kann.

DDoS-Abwehr ist nicht gleich DDoS-Abwehr

Da Unternehmen weiterhin in die Cloud-Infrastruktur investieren, stellt die Gewährleistung konsistenter Kontrollen für hybride Umgebungen eine Herausforderung für Sicherheitsteams dar. Und je mehr Anwendungen in Cloud-Infrastrukturen mit mehreren Backends bereitgestellt werden, desto schwieriger wird es, sie zu schützen. Viele Unternehmen wollen einen zentralen Kontrollpunkt für die Orchestrierung aller Verteidigungsmechanismen haben.

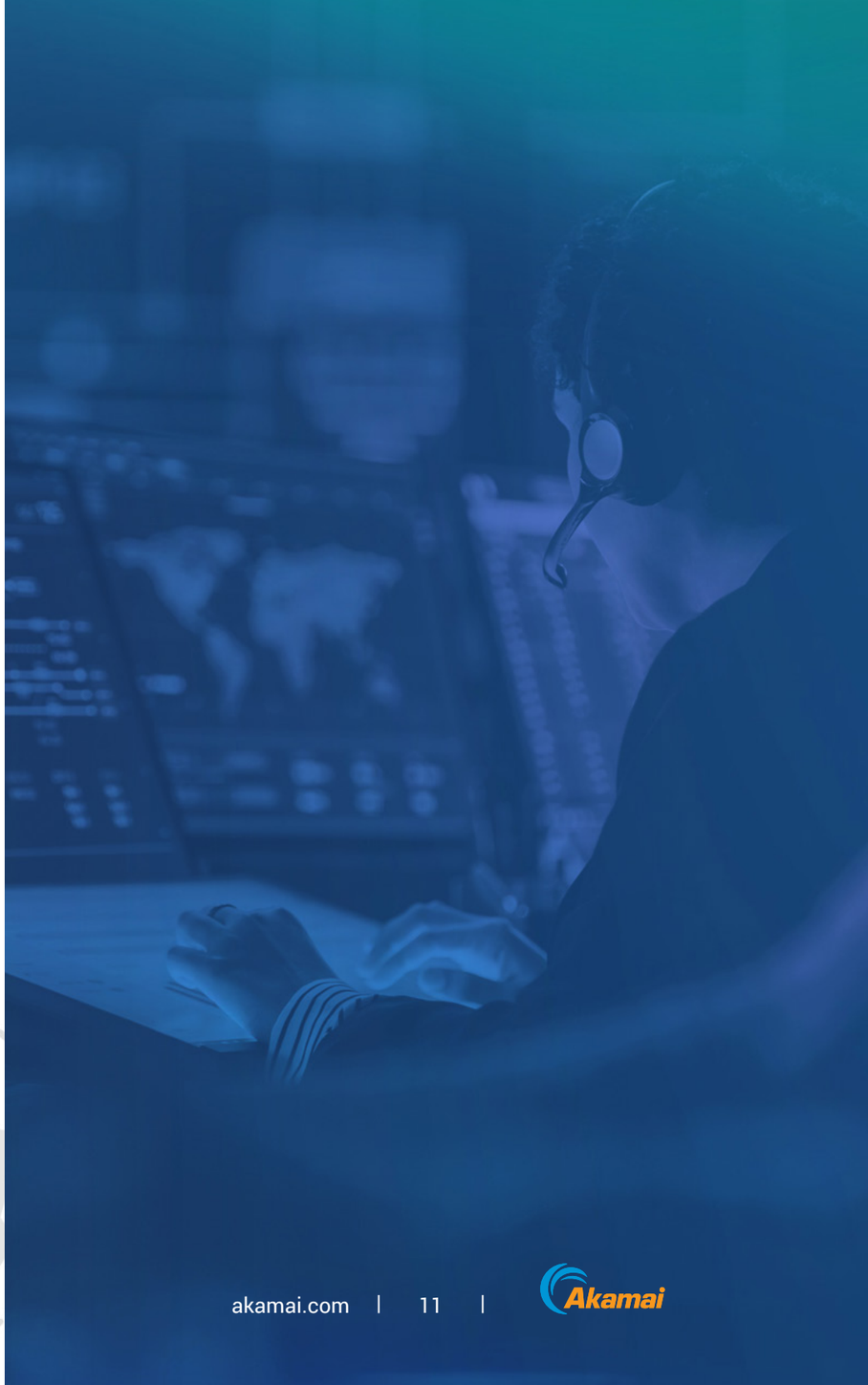
Angesichts der immer unübersichtlicheren Sicherheitstechnologien wünschen sich viele Unternehmen eine konsolidierte Ansicht ihrer Umgebung – nicht nur für eine bessere Transparenz, sondern auch für eine optimierte Berichterstellung. Auf diese Weise können die Daten zu Sicherheitsvorfällen über APIs in Korrelationssysteme eingespeist werden.

Zur Lösung dieses Problems wenden sich Unternehmen an DDoS-Sicherheitsanbieter, die eine integrierte, hochgradig skalierbare und umfassende DDoS-Schutzplattform bieten, die ihre Anwendungen, APIs, DNS und die zugrunde liegende Infrastruktur, die all das ermöglicht, schützen kann. Unternehmen benötigen skalierbare, reaktionsfähige Verteidigungsmechanismen für alle Geschäftsservices, unabhängig davon, wo sich diese befinden – vor Ort, in der Cloud oder in einer hybriden Umgebung. Diese Anforderung ergibt sich direkt aus der zunehmenden betrieblichen Komplexität, die mit der Integration, Bereitstellung und Verwaltung von DDoS-Abwehrmechanismen in der speziellen CSP-Umgebung einhergeht. Und da sich viele internetbasierte Ressourcen über mehrere Private und Public Clouds verteilen, wird die Sache schnell komplex.

Hinzu kommt, dass die lokalen DDoS-Abwehrlösungen vieler CSPs Mängel in den wichtigen Bereichen Transparenz, Service-Level Agreements (SLAs) und Reporting aufweisen, die für den Unternehmensschutz entscheidend sind.

Für die Sicherheitsteams dreht sich alles um Transparenz und verwertbare Erkenntnisse, damit sie die Reaktion auf Vorfälle optimieren und Vorsorgemaßnahmen treffen können. Die DDoS-Lösungen mancher CSPs bieten wenig bis gar keine Transparenz in Bezug auf Reporting, Einblicke und Analyse nach dem Angriff. Da ist es nicht überraschend, dass CSPs häufig als eine „Blackbox“ für Analysen und Reporting bezeichnet werden. Während einige CSPs es dem Sicherheitsteam eines Unternehmens ermöglichen, Kontrollen einzurichten und ihre Client-spezifische Umgebungen selbst zu verwalten, lehnen sie in der Regel jegliche Haftung für DDoS-Traffic ab. Sie stellen Kunden letztendlich das astronomische Volumen an schädlichem Traffic in Rechnung, das mit einem DDoS-Angriff einhergeht – unabhängig davon, ob es sich um einen Angriff auf Anwendungsebene, auf Netzwerkebene oder einen DNS-DDoS-Angriff handelt.

Darüber hinaus bieten einige CSPs und Sicherheitsanbieter kein SLA an, in dem die Abwehrreaktionszeit (TTM) klar festgelegt ist. Stattdessen stellen sie dem betroffenen Unternehmen Serviceguthaben zur Verfügung. Entscheiden ist, ob die TTM-Klausel die Zeit für die Identifizierung eines Angriffs enthält. Wenn eine Plattform mehrere Minuten oder gar Stunden benötigt, um einen DDoS-Angriff zu erkennen, bevor ihre Abwehrprotokolle greifen, könnte das betroffene Unternehmen für einen längeren Zeitraum offline bleiben. Wenn es auf jede Sekunde ankommt, müssen sich Unternehmen darauf verlassen können, dass ihr Anbieter den Servicebetrieb und die Verfügbarkeit ohne Beeinträchtigung der Performance aufrecht erhält.



Darüber hinaus ist es für Sicherheitsteams oder Käuferunternehmen gleichermaßen wichtig (wenn nicht sogar noch wichtiger) zu ermitteln, ob DDoS-Sicherheitsanbieter und CSPs **dedizierte DDoS-Verteidigungskapazitäten** anbieten oder ob die Verteidigungskapazitäten mit ihrem Netzwerk zur Inhaltsbereitstellung gemeinsam genutzt werden. Die dedizierte DDoS-Verteidigung ist wie ein SWAT-Team, das sich ausschließlich auf die Bekämpfung von DDoS-Angriffen konzentriert und keine Ressourcen oder Infrastruktur mit anderen Aspekten eines Unternehmens, wie der Inhaltsbereitstellung, gemeinsam nutzt, um so selbst bei rekordverdächtigen DDoS-Angriffen eine minimale Beeinträchtigung sicherzustellen. Unternehmen, die DDoS-Schutz prüfen, müssen sich bewusst sein, dass die Anbieter selbst manchmal DDoS-Angriffen ausgesetzt sind und sollten daher unbedingt berücksichtigen, ob der Anbieter ein SLA für Verfügbarkeit anbietet.

Außerdem stellen viele CSPs und Sicherheitsanbieter neben der Unterstützung vor, während und nach einem Angriff keinen bedarfsgesteuerten Zugriff auf ein rund um die Uhr verfügbares Security Operations Center (SOC) zur Verfügung. Ist dies doch der Fall, muss dafür oft ein Aufschlag gezahlt werden. Dies ist meist teurer als eine dezidierte hybride DDoS-Abwehrlösung von einem führenden Anbieter. Bei einer vollständig verwalteten, hybriden DDoS-Schutzlösung fungiert der Service Provider als Erweiterung des Notfallteams des Unternehmens und stellt das Fachwissen bereit, um schnell auf DDoS-Ereignisse reagieren zu können.

In der heutigen Bedrohungslandschaft setzen moderne Unternehmen bei der DDoS-Abwehr auf Partner, die in hybriden Umgebungen ein optimales Sicherheitserlebnis gewährleisten und gleichzeitig die Komplexität der Angriffsfläche verringern können. Ihr Partner für DDoS-Schutz sollte Ihre Hybrid- oder Multicloud-Strategie unterstützen und nicht behindern und auf Ihre Geschäftsziele abgestimmt sein.

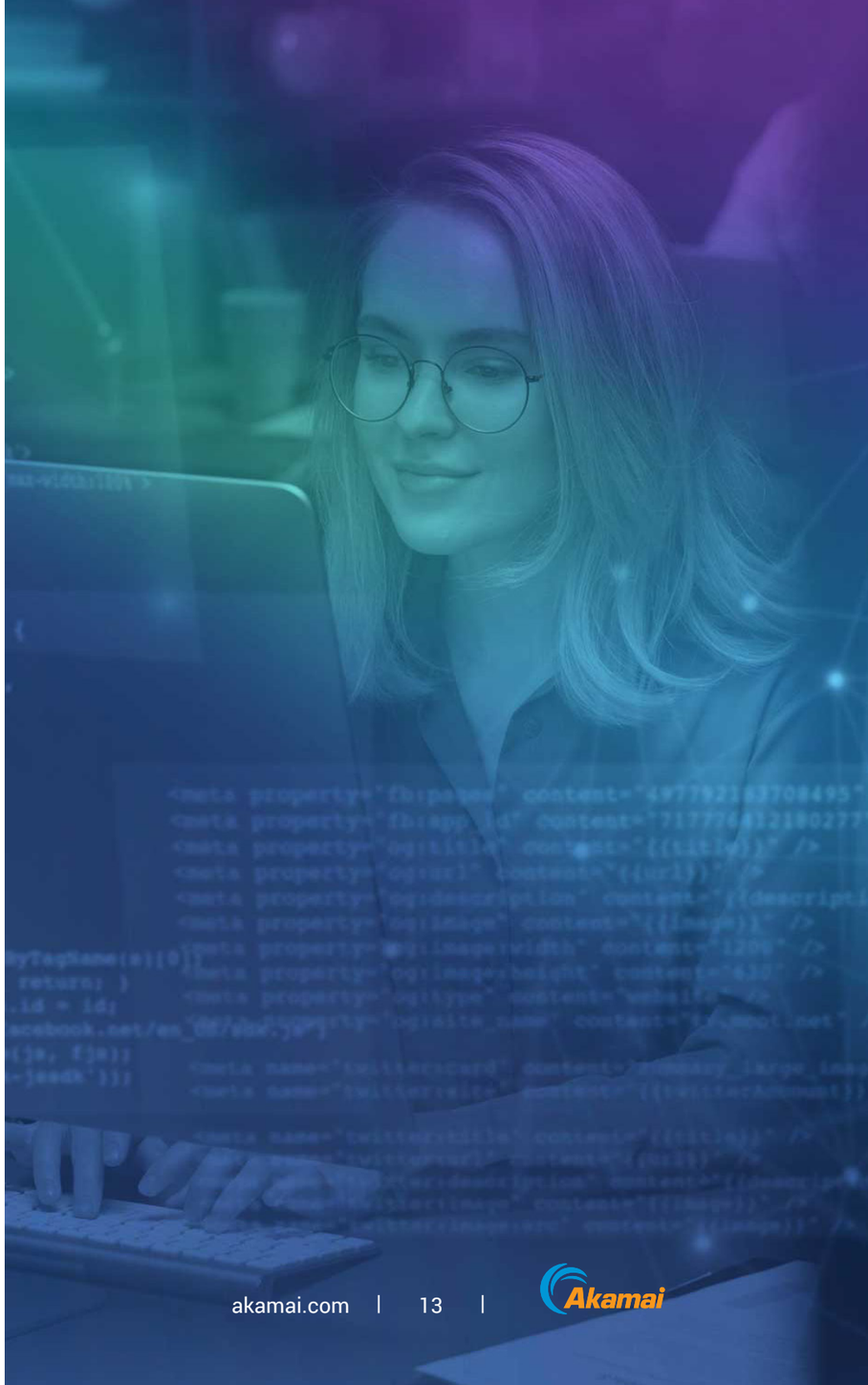
Maßgeschneiderte DDoS-Abwehr von Akamai

Unternehmen benötigen nicht nur eine End-to-End-Strategie für die digitale Infrastruktur, die hybride und Multicloud-Umgebungen umfasst, sie sollten auch einen End-to-End-Schutz gegenüber DDoS-Angriffen in Betracht ziehen. Die Schutzsysteme von Akamai folgen einem umfassenden Ansatz und fungieren als die erste Verteidigungslinie bei einem Angriff. Sie bieten eine dedizierte Edge-Struktur, verteilte DNS-Services sowie hybride Abwehrfunktionen und sind so konzipiert, dass Kollateralschäden und Ausfälle einzelner Komponenten verhindert werden. Im Gegensatz zu CSP-Architekturen, die als Komplettlösung vermarktet werden, bieten die speziell entwickelten DDoS-Lösungen von Akamai bessere Ausfallsicherheit, dedizierte DDoS-Verteidigungskapazitäten und eine höhere Abwehrqualität. Sie sind genau auf die individuellen Anforderungen der Webanwendungen oder internetbasierten Services abgestimmt. Die DDoS-Abwehr von Akamai steht Kunden nicht nur dort zur Verfügung, wo sie sie benötigen (vor Ort, in der Cloud, hybrid), sondern auch wie sie sie benötigen – immer verfügbar oder nach Bedarf. Dieser umfassende Schutz erstreckt sich auf drei Kernprodukte.

Dedizierte DDoS-Verteidigungskapazität

Verteiltes DNS

Hybride Abwehr



Akamai Prolexic ist ein erstklassiger DDoS-Schutz, der auf die proaktive und positive Sicherheitsstrategie eines Unternehmens zugeschnitten ist

Eine moderne und skalierbare Architektur

Akamai Prolexic verwendet eine vollständig softwaredefinierte Architektur, die an sich ändernde Netzwerktrends in Bezug auf Edge Computing, 5G/6G und Netzwerkvirtualisierung angepasst werden kann. Mit der Umstellung auf virtualisierte Software-Umgebungen hat Prolexic alle Abhängigkeiten von spezieller Hardware eliminiert. Diese Standardisierung der Bereitstellungen sorgt dafür, dass Akamai den sich weiterentwickelnden Kundenanforderungen schneller gerecht werden, modulare Bereitstellungen zur Kapazitätserweiterung vereinfachen, die regionale Abdeckung von Verbindungen mit geringer Latenz verbessern und die Redundanz auf der Plattform reduzieren kann. Darüber hinaus beschleunigt die Architektur die fortschrittlichen Funktionen von Prolexic, aus Angriffssignaturen zu lernen, sich an neue Bedrohungsvektoren anzupassen und für Kunden proaktiv mehr Resilienz gegenüber DDoS-Angriffen zu schaffen. Die Prolexic Cloud wird von mehreren **Scrubbing-Centern in 32 globalen Metro-Umgebungen und insgesamt über 20 Tbit/s dedizierter Verteidigungskapazität unterstützt**. Um eine Vorstellung der Verteidigungskapazität von Prolexic zu vermitteln: selbst die größten bekannten DDoS-Angriffe auf Layer 3 und 4 umfassen nicht einmal 10 % der Kapazität, die Prolexic-Kunden zur Verfügung steht.

Umfassender, flexibler und zuverlässiger DDoS-Schutz

Akamai Prolexic ist als Prolexic Cloud, Prolexic On-Prem und Prolexic Hybrid erhältlich.

Prolexic Cloud ist der Branchenpionier für cloudbasierten DDoS-Schutz und bietet Kunden SLAs mit Abwehr in null Sekunden und 100%iger Plattformverfügbarkeit. Abwehrmechanismen skalieren die Kapazität zur Abwehr von Angriffen über IPv4- und IPv6-Traffic dynamisch. Den Abwehrmechanismen, die ausgebaut werden müssen, können dynamisch Rechenressourcen zugewiesen werden.

Prolexic On-Prem bietet immer verfügbaren, physischen oder logischen Inline- und Datapath-DDoS-Schutz, der sich nativ in die Edge-Router eines Kunden integrieren lässt, um mehr als 98 % der Angriffe an der Peripherie des Netzwerks zu stoppen, ohne dass der Traffic zurückgeleitet werden muss. Dies ist ideal für die meisten kleinen und schnellen Angriffe und für Unternehmen, die DDoS-Schutz mit besonders niedriger Latenz benötigen.

Prolexic Hybrid kombiniert die Leistung, Automatisierung und Performance von Prolexic On-Prem mit der branchenführenden Skalierbarkeit und Kapazität der Prolexic-Cloud, um die Kundenursprünge vor den umfangreichsten volumetrischen DDoS-Angriffen zu schützen.

Sicherheit jenseits von DDoS

Akamai Prolexic verfügt über die Prolexic Network Cloud Firewall, einer vollständig im Self-Service verwalteten und nutzerkonfigurierbaren Funktion, mit der Kunden ihre eigenen Zugriffskontrolllisten (ACLs) und die Regeln, die sie an der Peripherie ihres Netzwerks durchsetzen möchten, einfach definieren, bereitstellen und verwalten können. Es ist eine Firewall, die sich vor allen anderen Firewalls befindet. Network Cloud Firewall empfiehlt außerdem ACLs für den besten proaktiven Schutz auf Grundlage der Bedrohungsinformationen von Akamai und liefert umsetzbare Analysen von bestehenden Regeln. Als Next-Generation Firewall as a Service ermöglicht die Network Cloud Firewall Kunden Folgendes:

- Definieren proaktiver Schutzmaßnahmen, um schädlichen Traffic sofort zu blockieren
- Entlasten der lokalen Infrastruktur durch Verschieben von Regeln an die Edge
- Schnelles Reagieren auf Veränderungen im Netzwerk über eine neue Nutzeroberfläche

Akamai Edge DNS und **Akamai Shield NS53** sichern und stärken kritische DNS-Infrastrukturen

Akamai Edge DNS bietet Ihnen umfassenden Schutz vor einer Vielzahl von DNS-Angriffen auf Ihre DNS-Infrastruktur, sei es vor Ort, in der Cloud oder hybrid. Die Lösung bietet zudem ein hohes Maß an DNS-Performance, Ausfallsicherheit und Verfügbarkeit. Edge DNS basiert auf einem global verteilten Anycast-Netzwerk und kann als primärer oder sekundärer DNS-Service implementiert werden. So kann es die vorhandene DNS-Infrastruktur je nach Bedarf ersetzen oder ergänzen.

Akamai Shield NS53 ist eine bidirektionale DNS-Reverse-Proxy-Lösung, die Vor-Ort- und hybride DNS-Infrastrukturen – einschließlich GSLBs, Firewalls und Nameserver – vor DNS-Überlastungsangriffen (NXDOMAIN) schützt. Kunden können ihre eigenen dynamischen Richtlinien in Echtzeit selbst konfigurieren, anwenden, verwalten und durchsetzen. Unzulässige DNS-Abfragen und DNS-Flood-Angriffe werden direkt an der Edge des Akamai-Netzwerks verworfen, um kritische DNS-Infrastrukturen vor DNS-DDoS-Angriffen zu schützen.

Akamai App & API Protector schützt Anwendungen und APIs vor DDoS-Angriffen

App & API Protector gilt als marktführende WAAP-Lösung (Web Application and API Protection) und wehrt DDoS-Angriffe auf Netzwerkebene sofort an der Edge ab (bei Online-Präsenzen, die in Akamai Connected Cloud gehostet werden) und bietet umfassende Verteidigungsstrategien gegen DDoS-Angriffe auf Anwendungsebene.

Warum Akamai?

Akamai bietet Lösungen zur DDoS-Abwehr, die weltweit großes Vertrauen genießen. Ganz gleich, ob Sie einzelne Anwendungen, ganze Rechenzentren oder kritische DNS-Infrastrukturen schützen müssen, die Architektur von Akamai zur DDoS-Abwehr bietet besonders umfassende Kapazitäten, große Ausfallsicherheit und sehr schnelle Abwehr.

Unsere Lösungen konnten einige der weltweit größten DDoS-Angriffe abwehren. Unsere proaktiven Schutzmaßnahmen ermöglichen eine Abwehr, die tatsächlich null Sekunden in Anspruch nimmt, und ein branchenführendes SLA. Zudem können wir Schutzservices gegen DDoS-Angriffe für mehrere Clients bereitstellen und mehrere DDoS-Angriffe gleichzeitig zurückschlagen.

Da sich die DDoS-Angriffsvektoren ständig ändern und Angriffe immer größer werden, muss eine vertrauenswürdige DDoS-Plattform kontinuierlich innovative Funktionen entwickeln und bereitstellen, um Bedrohungen proaktiv zu erkennen, Abwehrstrategien zu orchestrieren und Auswirkungen zu minimieren. Akamai ist bestrebt, den Bedrohungen immer einen Schritt voraus zu sein, indem Angriffe bereits abgewehrt werden, bevor sie beginnen.

Ihre DDoS-Abwehrstrategie sollte Ihre Hybrid- und Multicloud-Strategie unterstützen. Die DDoS-Lösungen der nächsten Generation von Akamai schützen Ihre digitale Netzwerkinfrastruktur, Anwendungen und DNS vor Ort, in der Cloud oder beides, und bieten die kombinierten Vorteile von maschineller und menschlicher Intelligenz.

Mehr erfahren

©2024 Akamai Technologies | Support | | Veröffentlicht: Oktober 2024