Akamai

WHITEPAPER

11 DDoS-Mythen, die sich hartnäckig halten

DDoS-Angriffe (Distributed Denial of Service) haben in den letzten Jahren in Bezug auf Größe, Umfang, Verteilung und Komplexität drastisch zugenommen. Das zeigen einige rekordverdächtige Angriffe. Leider halten viele Unternehmen immer noch an veralteten Vorstellungen darüber fest, wie sie diese Angriffe abwehren können. Sie gehen beispielsweise davon aus, dass ihre Abwehrmechanismen ausreichend sind – oder schlimmer noch, dass sie wahrscheinlich nicht ins Visier geraten werden. Die Wahrheit ist: Die Opfer dieser Angriffe kommen aus allen wichtigen Branchen, von Finanzdienstleistungen über E-Commerce bis hin zu Gaming. Tatsächlich sind Angriffe auf kritische öffentliche Infrastruktur, darunter Gesundheitswesen, Energie- und Versorgungseinrichtungen, Bildung und Verkehr, besonders besorgniserregend. 2023 schützte Akamai einen Kunden in der Region Asien-Pazifik vor einem massiven Angriff mit 900 Gbit/s (Gigabit pro Sekunde). Später im selben Jahr verhinderte Akamai einen Angriff mit 634 Gbit/s und 55 Millionen Paketen pro Sekunde (Mpps), der eine komplexe Mischung aus Angriffsvektoren enthielt. Es war einer der größten Angriffe, die jemals gegen einen US-Finanzdienstleister gerichtet wurden. Darüber hinaus hat Akamai den bisher größten DDoS-Angriff überhaupt abgewehrt: ein weltweit verteilter Angriff mit 1,44 Tbit/s und 385 Mpps, der fast zwei Stunden andauerte. Diese Ereignisse machen deutlich, dass Cyberkriminelle weiterhin wichtige Säulen der Wirtschaft ins Visier nehmen.

Der Umfang dieser Angriffe könnte einige kleinere Unternehmen zu der Annahme verleiten, dass ihr Risiko, Opfer eines DDoS-Angriffs zu werden, eher gering ist. In Wirklichkeit sind aber geschäftskritische Dienste und Anwendungen in jeder Branche leichte Ziele. Angesichts der Zunahme politisch und ideologisch motivierter Hacktivisten und der relativ niedrigen Kosten für DDoS as a Service, die von Cyberkriminellen wie Killnet und Anonym Sudan angeboten wird, ist mittlerweile fast jeder ein potenzielles Ziel. Aber es ist nicht nur der erste Angriff, über den sich Unternehmen Sorgen machen müssen. DDoS-Angriffe werden zunehmend als Ablenkungsmanöver eingesetzt, um Netzwerk- und Sicherheitsressourcen zu binden, während Angreifer gleichzeitig Ransomware-DDoS-Angriffe (RDDoS) oder andere schädliche Exploits wie dreifache Erpressungskampagnen durchführen. Darüber hinaus stellt auch die zunehmende und alarmierende Einführung von Tools für künstliche Intelligenz zur Orchestrierung hochentwickelter und verteilter DDoS-Angriffe eine erhebliche Herausforderung für die Verteidigung von Unternehmen und öffentlichen Einrichtungen dar, die eine durchgängige Verfügbarkeit und Performance gewährleisten müssen.

Während die Bedrohungen immer komplexer werden und sich fast täglich weiterentwickeln, gibt es leider immer noch viele Mythen über DDoS-Schutz – und einige davon werden sogar von Sicherheitsanbietern befeuert. DDoS-Schutz muss ein zentraler Grundsatz jeder Sicherheitsstrategie sein. Daher ist es für Ihre DDoS-Abwehr von entscheidender Bedeutung, dass Sie wissen, welche Gefahr von diesen Mythen ausgeht.

MYTHOS 1

Die Gesamtkapazität gibt den vollen Umfang der verfügbaren Abwehrressourcen an.

Obwohl die Gesamtkapazität wichtig ist, kann eine einfache Zahl für die Netzwerkkapazität irreführend sein, da sie wichtige Details auslässt. Unternehmen, die Lösungen für DDoS-Schutztechnologien bewerten, müssen sich folgende Fragen stellen:

- Wie hoch ist die Netzwerkkapazität, die für Angriffstraffic freigehalten wird?
- Wie viele Ressourcen des Abwehrsystems sind **speziell dafür vorgesehen,** Angriffe aufzuhalten?
- Wie viele der Netzwerk- und Systemressourcen stehen zur Verfügung, um allen Kundenursprüngen auf dieser Plattform und auf diesem Tenant bereinigten Traffic bereitzustellen?

Diese Fragen sind von entscheidender Bedeutung, denn wenn die gesamte Netzwerkkapazität auch andere Anforderungen wie die Bereitstellung von Inhalten umfasst, könnte die tatsächliche DDoS-Abwehrkapazität nur einen Bruchteil dessen ausmachen, was der Anbieter angibt.

Die Kapazität zur Abwehr von DDoS-Angriffen ist auch nicht nur auf Technologie beschränkt. Gibt es zusätzlich spezielles Personal für Eskalation, Vorfallsreaktion und Feinabstimmung der Abwehr, wenn die Technik einmal ausfällt oder nicht wie vorgesehen funktioniert? Um umfassenden Schutz und leistungsstärkste Abwehr gewährleisten zu können, sollten Automatisierung und maschinelle Intelligenz mit menschlichem Fachwissen kombiniert werden.

Tipp

Informieren Sie sich gründlich über die Unterschiede zwischen der gesamten Netzwerkkapazität und Plattformstabilität eines Anbieters sowie über die zur Abwehr von Angriffen verfügbare Kapazität und die Bereitstellung von bereinigtem Traffic. Sie sollten als einzigartige Segmente betrachtet werden. Kapazitäten sollten beispielsweise zweckgebunden sein, z. B. für das Netzwerk-Routing von Angriffstraffic, das Stoppen oder Abwehren von Angriffstraffic und die Bereitstellung von sauberem Traffic zurück an das Rechenzentrum.

MYTHOS 2

DDoS-Schutz durch Internetdienstanbieter und/ oder Cloud-Dienst-Anbieter ist ausreichend.

Leider sind viele Unternehmen immer noch der Meinung, dass der von ihrem Internetdienstanbieter (ISP) angebotene Schutz ausreichend ist. Die Wahrheit ist: ISPs bieten in der Regel nur neu umgerüsteten, handelsüblichen DDoS-Schutz von der Stange mit begrenzter Bandbreite. Die Hardware wird nicht nur von Ihrer Infrastruktur genutzt, sondern auch von der des Anbieters, was zu begrenzter Kapazität und eingeschränkten CPU-Zyklen führt. DDoS-Angriffe sind allerdings mittlerweile so umfangreich, dass sie beide Infrastrukturen überlasten können. Die ISPs werden Ihren Traffic dann über eine Null-Route (oder in ein Blackhole) leiten, um Kollateralschäden an anderen Produktionsressourcen zu vermeiden. Wenn der gesamte Traffic in ein Blackhole umgeleitet wird, verlieren Unternehmen legitimen Traffic und Services von Endnutzern und das Unternehmen ist praktisch offline, was den Angriff zu einem Erfolg werden lässt.

Darüber hinaus erlauben Cloud-Dienst-Anbieter (CSPs) ihren Kunden zwar oft, ihre eigenen Kontrollen festzulegen und weiterhin selbst über ihre Sicherheitslage in der Cloud-Umgebung des CSP zu bestimmen, doch die meisten CSPs selbst lehnen in der Regel jegliche Verantwortung ab und stellen Kunden am Ende sogar den unrechtmäßigen DDoS-Traffic in Rechnung. Angesichts des Umfangs und der Größe moderner DDoS-Angriffe kann dies zu erheblichen Mehrkosten für die Opfer führen.

Tipp

Prüfen Sie die DDoS-Schutzklauseln Ihres ISP oder CSP genau und verhandeln Sie sie bei Bedarf neu. Bringen Sie außerdem in Erfahrung, ob Ihr ISP vor Ort leistungsstarke DDoS-Schutzhardware mit Cloud-Backup verwendet, damit kleine, aber schnelle DDoS-Angriffe lokal abgewehrt werden, während große volumetrische Angriffe durch einen Cloud-DDoS-Schutzdienst ordnungsgemäß abgewehrt werden können.

MYTHOS 3

Alle Abwehrzeit-SLAs sind gleich.

Manchmal können Zahlen irreführend sein. Die Abwehrzeit (Time To Mitigate, TTM) ist eine Zahl, die häufig von Sicherheitsanbietern vermarktet wird. Sie gibt im Idealfall an, wie schnell schädlicher DDoS-Traffic aufgehalten oder blockiert werden kann, ohne dass legitimer Traffic und Nutzer beeinträchtigt werden. Hier bleibt allerdings viel Raum für Interpretation offen. Ein Anbieter könnte beispielsweise einen Traffic-Anstieg nicht als DDoS-Angriff einstufen, wenn er nicht mindestens fünf Minuten dauert. Der SLA-Timer startet also möglicherweise erst, wenn Sie bereits angegriffen werden. Bei einer durchschnittlichen Angriffsdauer von weniger als fünf Minuten wird deutlich, wie problematisch dies ist: Es bedeutet, dass die Abwehr statt der beworbenen zehn Sekunden in Wirklichkeit mehr als fünf Minuten in Anspruch nehmen könnte.

Andere Anbieter definieren die Abwehrzeit als die Zeit, bis eine Abwehrregel eingesetzt werden kann. Dies spiegelt nicht wider, ob der Angriff gestoppt wurde oder wie gut oder konsequent diese Kontrolle aktiviert wurde. Letztendlich geht es Ihnen darum, internetbasierte Ressourcen zu sichern und wieder einsatzbereit zu machen, und zwar **mit den geringsten Auswirkungen auf legitime Nutzer oder Dienste**. Lesen Sie sich das Kleingedruckte im SLA Ihres Anbieters sorgfältig durch.

Tipp

Lesen Sie den Abschnitt zur Abwehrzeit in einem SLA gründlich durch. Sie sollte dieser Gleichung entsprechen: Die Zeit, die wirklich zählt = Zeit zur Erkennung des Angriffs + Zeit für die Anwendung von Abwehrmechanismen + Zeit zum Blockieren/Stoppen des Angriffs + Qualität/Konsistenz der Abwehr. Wählen Sie einen Anbieter aus, der ein **SLA mit tatsächlich null Sekunden** für die Abwehr von DDoS-Angriffen bietet, ohne Auswirkungen auf legitime Nutzer.

MYTHOS 4

Null-Routing/Blackholing und Ratenbegrenzungen sind akzeptable Abwehrmaßnahmen.

Null-Routing (oder Blackholing) ist eine gängige und eher primitive Abwehrreaktion einiger Anbieter von DDoS-Schutzmechanismen. Wenn ein Asset angegriffen wird und diese Angriffskapazität andere Kunden oder Dienste gefährdet, könnte der Anbieter versuchen, Kollateralschäden zu verhindern, indem er den Traffic dieser Ressource in ein virtuelles schwarzes Loch (Blackhole) leitet. Hilft Ihnen das wirklich? Aus Sicht des Angreifers ist Blackholing ein Erfolg – das angegriffene Asset ist offline. Je nach Infrastruktur des Anbieters könnten dabei jedoch auch andere Kunden offline gehen oder deren Performance könnte beeinträchtigt werden.

Eine weitere primitive DDoS-Abwehrmaßnahme, die von vielen Sicherheitsanbietern angeboten wird, besteht darin, als Gegenmaßnahme in gemeinsam genutzten Umgebungen Ratenbegrenzungen für den Kundentraffic festzulegen. Aber 20 % bis 40 % des legitimen Traffics zu verlieren, um den Eindruck zu erwecken, dass das Asset oder der Service immer noch verfügbar ist, ist für den angegriffenen Kunden kein annehmbares Ergebnis. Ratenbegrenzung ist als sekundäre oder tertiäre Gegenmaßnahme bei DDoS-Angriffen auf den Layern 3, 4 und 5 wirksam. Bei Layer-7-DDoS-Angriffen kann die Ratenbegrenzung als erste Kontrolle effektiver sein, aber Sie sollten sich immer zuerst auf die Signaturabwehr verlassen. Sie verdienen es, 100 % Ihrer digitalen Infrastruktur effektiv vor DDoS-Angriffen zu schützen, unabhängig davon, welche Layer des OSI-Modells (Open Systems Interconnection) betroffen sind – und nicht nur 60 % oder noch weniger.

Tipp

Fragen Sie Ihren Anbieter, wie oft Blackholing und Ratenbegrenzungen in ruhigen Zeiten und während eines Angriffs jeweils zum Einsatz kommen. Finden Sie heraus, wann (unter welchen Bedingungen) ein Anbieter Traffic in ein Blackhole leitet und welche Kriterien Sie erfüllen müssen, um Ihre Dienste wiederherzustellen.

MYTHOS 5

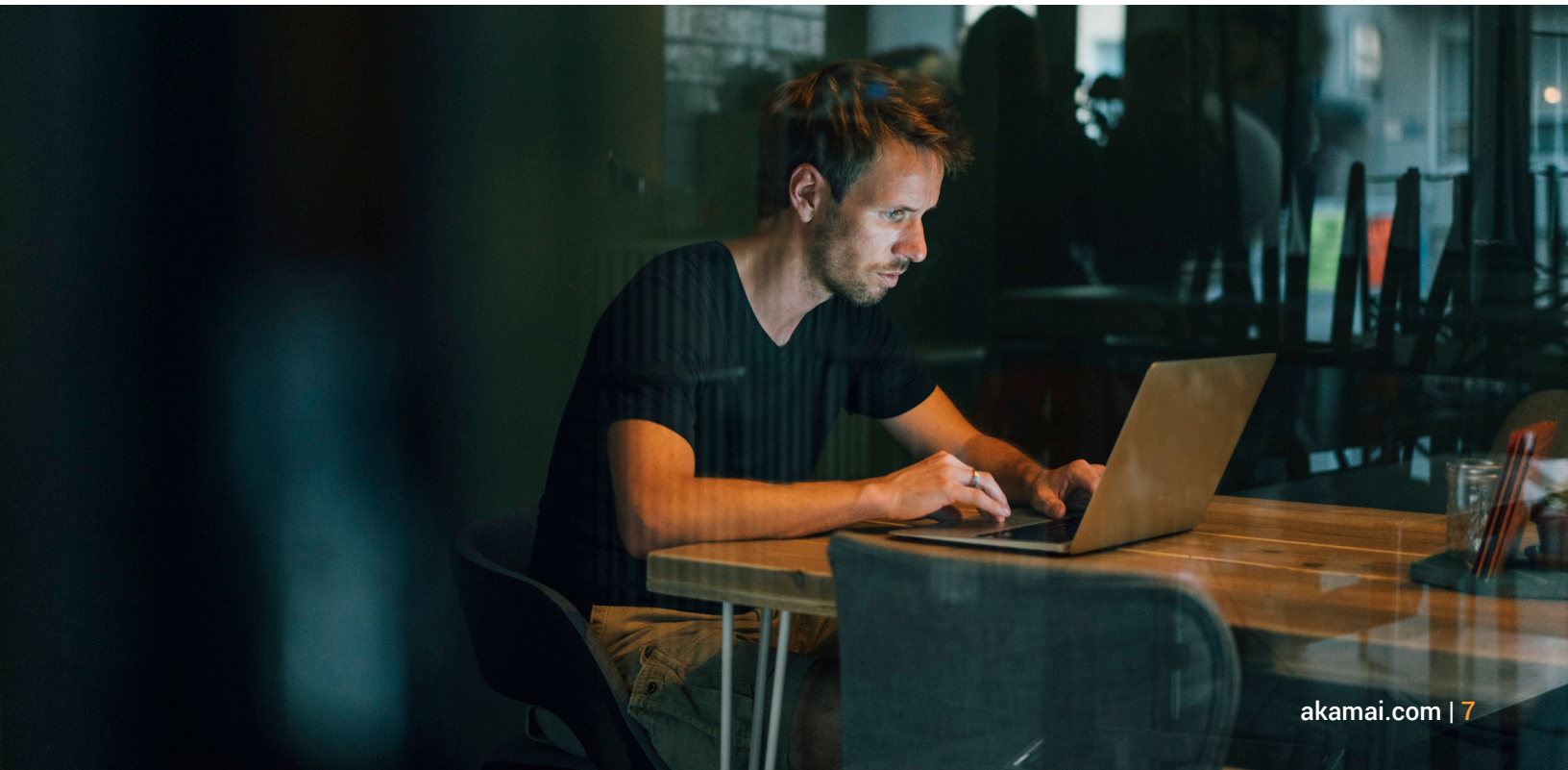
Es spielt keine Rolle, mit wem man sich eine Cloudplattform teilt.

Jedes Unternehmen benötigt Sicherheit. Auch kontroverse Geschäftszweige, die häufig Angriffen ausgesetzt sind, z. B. Graumärkte wie Websites, die Glücksspiel oder nicht jugendfreie Inhalte hosten, müssen ihre DDoS-Sicherheit verteidigen. Selbst Unternehmen, die kriminelle Aktivitäten und Terrorangriffe unterstützen, haben Cybersicherheit von legitimen Cloudanbietern erworben.

Sie glauben jetzt vielleicht, dass diese Websites Sie nicht weiter betreffen. Wenn Ihr Unternehmen jedoch eine Cloudplattform mit einem illegalen oder häufig angegriffenen Unternehmen teilt, ist das Risiko von Kollateralschäden hoch. Die Ressourcen des Anbieters sind möglicherweise anderweitig im Einsatz oder überlastet und können Ihr Unternehmen nicht mehr schützen.

Tipp

Lesen Sie die Nutzungsrichtlinie von Cloudsicherheitsanbietern sorgfältig durch, um sicherzugehen, dass Sie keine Sicherheitsplattform-Ressourcen mit Risikozielen teilen. Lesen Sie auch die Tipps zu Mythos 1 und 2 bezüglich Kapazität und Funktionalität noch einmal durch.



MYTHOS 6

Eine Web Application Firewall ist für den DDoS-Schutz ausreichend.

Web Application Firewalls (WAFs), die häufig Bestandteil einer größeren Gruppe von Lösungen für Webanwendungs- und API-Schutz (WAAP) sind, bieten effektiven DDoS-Schutz bei Angriffen auf Anwendungsebene (Layer 7). Obwohl sie auch einen grundlegenden Schutz auf Netzwerkebene (Layer 3) oder Transportebene (Layer 4) bieten, reicht dieser nicht aus, um alle IPs, Ports und Protokolle umfassend abzudecken.

DDoS-Angriffe gibt es in verschiedenen Varianten und Formaten. Sie können auf Infrastrukturebenen (Layer 3 und 4), HTTP(s)-Anwendungsebene (Layer 7) und DNS-Infrastruktur abzielen. Darüber hinaus starten Angreifer häufig dynamisch wechselnde Angriffe, die beispielsweise mit DNS beginnen und sich anschließend auf andere Ebenen oder Protokolle ausdehnen können. Echter DDoS-Schutz basiert auf einer tiefgreifenden Verteidigungsstrategie, die eine Plattform aus zuverlässigen Lösungen mit spezifischen Stärken und Funktionen zum Schutz von Layer 3, 4 und 7 sowie DNS nutzt. Eine Einzellösung allein reicht nicht immer aus, um alle Bereiche abzudecken, sondern kann Ihr Unternehmen anfällig für Angriffe machen. Außerdem besteht ein höheres Risiko, dass legitimer Traffic oder legitime Services zu sehr beschränkt werden.

Tipp

Stellen Sie sicher, dass Ihre DDoS-Schutzlösung nicht nur auf eine bestimmte Art von DDoS-Angriff oder Implementierungsentwurf ausgerichtet ist. Den besten Schutz bietet ein einziger Anbieter, der mehrere dedizierte DDoS-Schutzfunktionen bereitstellen kann, welche die Interoperabilität gewährleisten und von einem einheitlichen, schnell reagierenden Sicherheitsteam unterstützt werden, um Ihre Produktionsressourcen zu schützen. Komplex wird die Angelegenheit, wenn diese Assets in hybriden Netzwerken und cloudbasierten Umgebungen bereitgestellt werden. Schutzdienste müssen unabhängig vom Netzwerk- oder Bereitstellungsmodell funktionieren.

MYTHOS 7

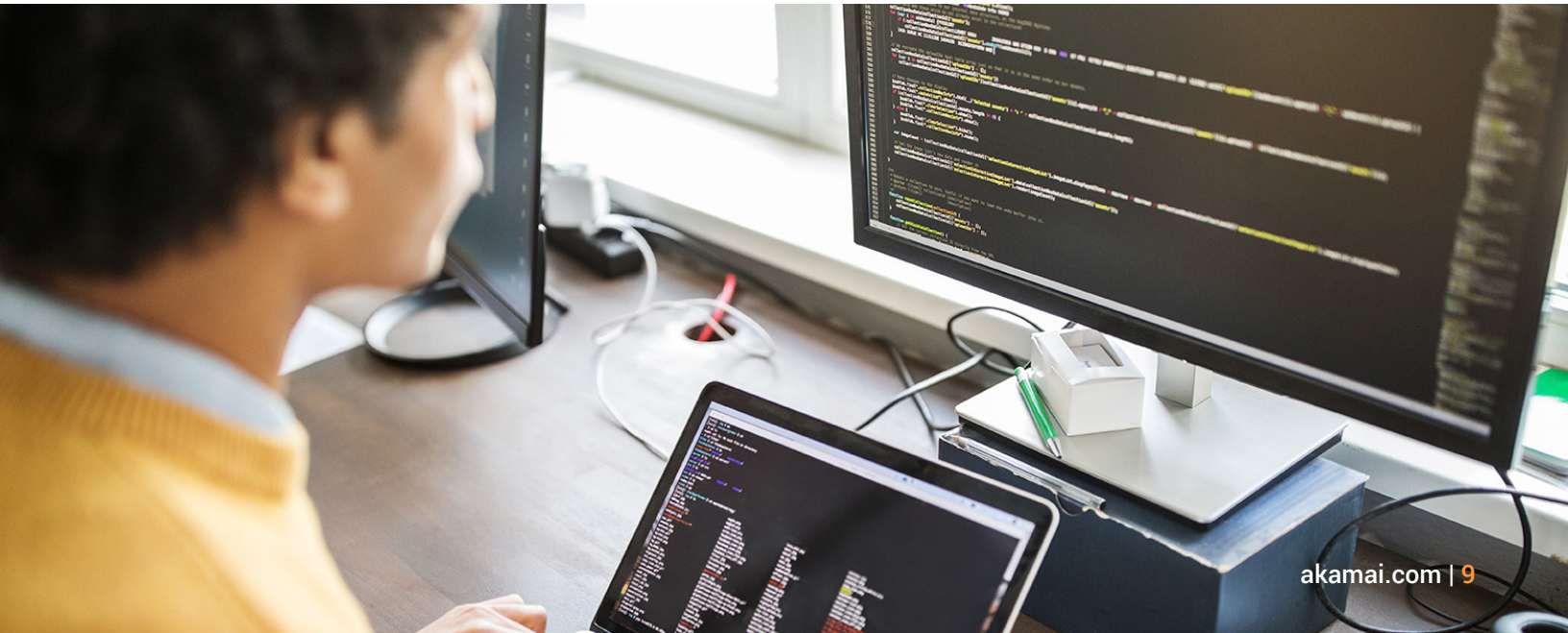
All-in-One-Sicherheitsplattform = besseres Sicherheitserlebnis

Einige Anbieter bieten eine Vielzahl von Diensten an, die auf einer einzigen Cloud-Plattform aufbauen. Dies kann die technische Komplexität bei der Bereitstellung und Integration von Sicherheitskontrollen kurzfristig reduzieren. Wenn jedoch Störungen in anderen Teilen der Umgebung auftreten, sind gleich mehrere Services, die dieselbe Backend-Infrastruktur und Netzwerke gemeinsam nutzen, anfällig für Plattformausfälle, Kollateralschäden und Probleme bei der Ausfallsicherheit. Häufig reduzieren Anbieter von integrierten Lösungen den Funktionsumfang, da der Einsatz einer einzigen Plattform Einschränkungen mit sich bringt.

Ein transparentes Netz aus zweckgerichteten CDN-, DNS- und DDoS-Schutzplattformen oder -lösungen, die speziell für die Bewältigung individueller technischer und sicherheitsrelevanter Herausforderungen entwickelt wurden, sorgt für eine höhere Abwehrqualität und skalierbare Performance zur Optimierung der Abwehrmechanismen.

Tipp

Denken Sie daran, dass Sie nicht dieselbe Infrastruktur teilen müssen, um eine einheitliche Sicherheit zu erreichen. Bei einem Ansatz mit verschiedenen Abwehrmechanismen werden zugrunde liegende Architekturen genutzt, die ein nahtloses Nutzererlebnis sowie eine leistungsstarke Sicherheitsabwehr ermöglichen.



MYTHOS 8

DDoS-Schutz ist bei IPv6 nicht erforderlich.

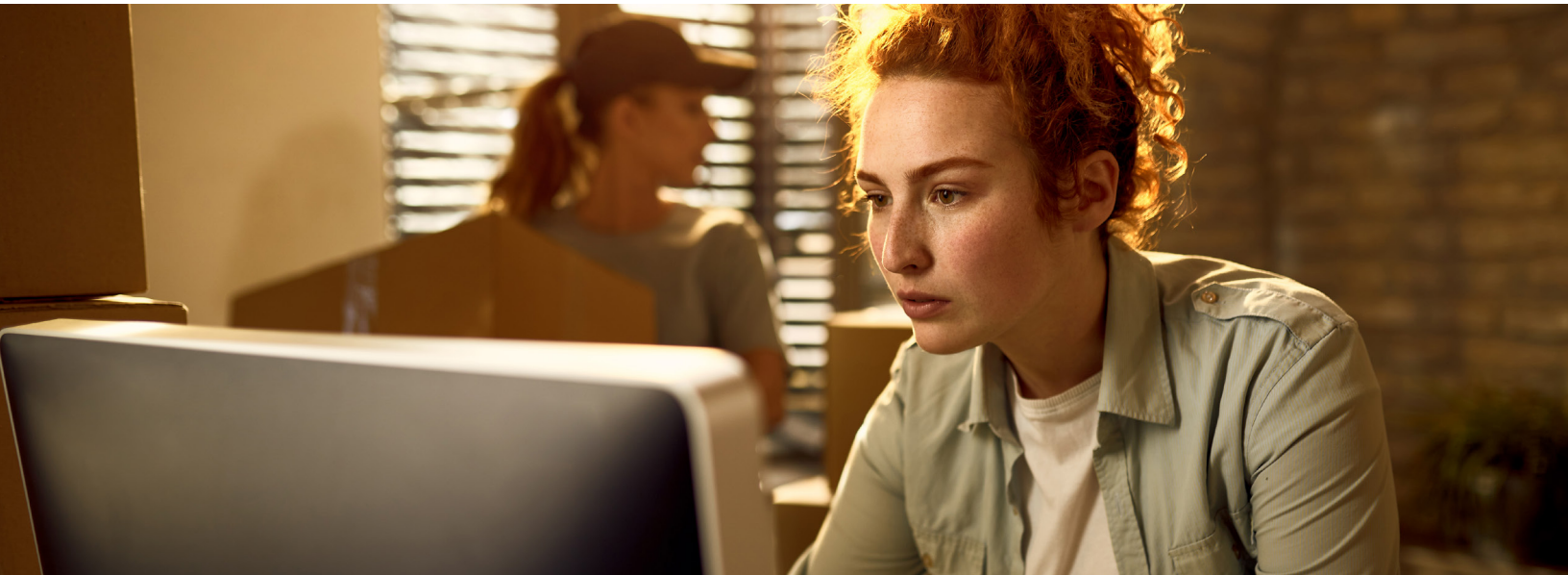
Laut Google stammen rund 45 % des Internettraffics von IPv6-kompatiblen Geräten. In Bezug auf DDoS-Angriffe bietet IPv6 einige Verbesserungen gegenüber IPv4, wie z. B. einen größeren Adressraum und integrierte Sicherheitsfunktionen wie IPsec, aber es schützt nicht grundsätzlich vor solchen Angriffen.

DDoS-Angriffe können sowohl IPv4- als auch IPv6-Netzwerke ins Visier nehmen, indem sie sie mit einem großen Trafficvolumen überlasten, Schwachstellen ausnutzen oder verschiedene Angriffsvektoren verwenden, die von der IP-Version unabhängig sind. Cyberkriminelle haben den deutlich erweiterten IP-Raum von IPv6 bereits genutzt, um noch größere volumetrische DDoS-Angriffe zu starten. In einigen Fällen haben Angreifer Traffic an zufällige Adressen in einem Netzwerk gesendet, wodurch ein Broadcast-Sturm auf der physischen Netzwerkebene verursacht wurde und Router- oder Netzwerkressourcen gebunden und erschöpft wurden.

Die derzeitige Fragmentierung zwischen IPv4 und IPv6 erhöht die Komplexität zusätzlich, da in der Regel nicht von sauberen IPv6-Umgebungen ausgegangen werden kann.

Tipp

DDoS-Schutz für IPv6 erfordert ähnliche Strategien und Technologien wie für IPv4, einschließlich Netzwerküberwachung, Filterung des Traffics, Ratenbegrenzung und Einsatz spezieller DDoS-Abwehrdienste.



MYTHOS 9

Mehrere Verteidigungsebenen sind nicht nötig.

Die meisten Unternehmen glauben diesen Mythos zwar nicht wirklich, aber manchmal konstruieren sie ihre Verteidigungsstrategie so, als wäre er wahr. Wenn Sie jedoch Ihre Haustür abschließen, um Ihr Zuhause zu sichern, können Sie auch nicht Ihre Hintertür und Fenster offen lassen. Eine echte DDoS-Abwehr wird durch den Aufbau von Sicherheitsebenen erreicht, die nahtlos zusammenarbeiten, um zu verhindern, dass Angreifer ihr Ziel beim ersten Versuch erreichen.

Erstklassige DDoS-Abwehr beginnt mit einer Network Cloud Firewall, die die Last Ihrer Firewalls bis an den Rand Ihres Netzwerks verringert. Ein hybrides DDoS-Schutzmodell umfasst dann einen lokalen, auf Hardware-Appliances basierenden Schutz vor kurzen, aber heftigen DDoS-Angriffen und greift auf dedizierten cloudbasierten Schutz für große, komplexe und volumetrische DDoS-Angriffe zurück. Ihre DNS-Infrastruktur muss außerdem mit einer ähnlich mehrschichtigen Strategie geschützt werden, die die Verwendung eines Proxy-Dienstes umfasst, der Sicherheitsrichtlinien dynamisch am Rand Ihres Netzwerks implementieren und diese mit einer autoritativen DNS-Lösung entweder im primären oder sekundären Modus weiter aufteilen kann. Schließlich müssen Sie alle Ihre Anwendungen und APIs mit einer leistungsstarken WAAP-Lösung mit WAF-Funktion schützen.

Tipp

Kombinieren Sie branchenführende Technologien und Lösungen mit unterschiedlichen und dedizierten Stärken, um eine umfassende, tiefgreifende Verteidigungsstrategie zu entwickeln, die es Cyberkriminellen extrem schwer macht, mit ihren Angriffen erfolgreich zu sein.

MYTHOS 10

Jedes Security Operations Center bietet denselben Support.

Viele Anbieter werben mit SOC-Support (Security Operations Center). Aber ein rund um die Uhr verfügbares SOC ist nicht das Entscheidende. Wichtig ist der Grad an Service und Fachwissen, den Sie erwarten können, wenn Ihre Assets angegriffen werden. Zu den wichtigsten Überlegungen bei der Bewertung von Anbietern von DDoS-Abwehr gehören:

- Welche Art von Support und Analyse würden Sie vor, während und nach einem Angriff erhalten?
- Wie ist das SOC besetzt, um eine anhaltende Verteidigung zu gewährleisten?
- Ist die Person, mit der Sie im SOC Kontakt haben, der Analyst, der die Abwehr durchführt, oder ist sie nur für die Eskalation zuständig?
- Verfügt Ihr Anbieter über Sicherheitsexperten, die in Abwehr geschult sind, oder sind sie lediglich „Verkehrspolizisten“, die Traffic an handelsübliche Abwehrmechanismen weiterleiten?
- Bieten sie ein kundenspezifisches Runbook an?

Das SOC Ihres Sicherheitsanbieters sollte als Erweiterung Ihres Vorfallsreaktionsteams fungieren, um einen echten Mehrwert zu erzielen.

Tipp

Schätzen Sie die erwartete Support-Qualität ein, die Sie vom SOC des Serviceanbieters erhalten würden. Informieren Sie sich, ob der Anbieter neben der Erkennung und Abwehr von Angriffen auch Integration und Tests, Fehlerbehebung bei Vorfällen, nachträgliche Analysen (gewonnene Erkenntnisse) und Unterstützung bei der Entwicklung bietet, um Ihre Angriffsfläche zu reduzieren.

MYTHOS 11

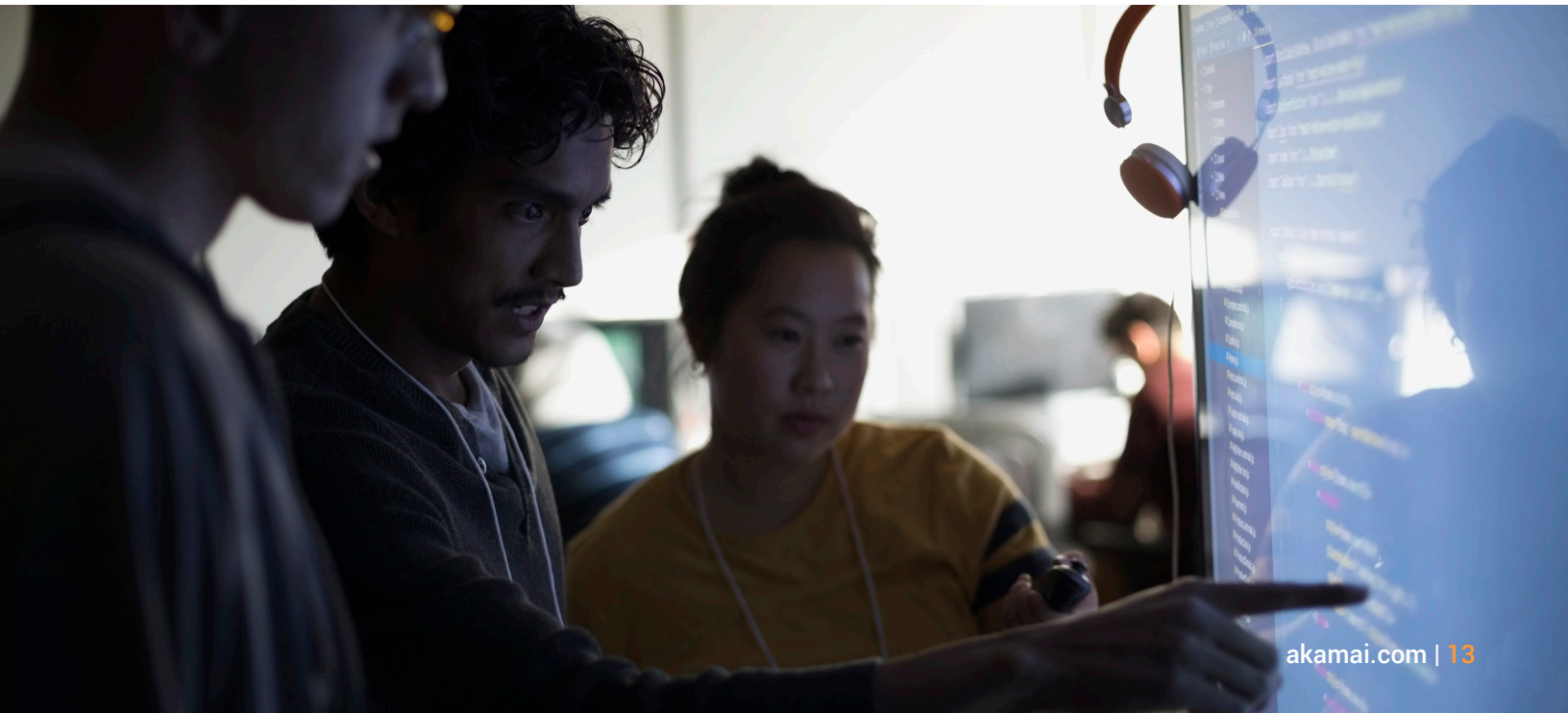
DDoS ist ein bekanntes Problem, daher reicht der günstigste Schutz aus.

Die alte Volksweisheit „Nichts im Leben ist schließlich umsonst“ trifft auch auf den DDoS-Schutz zu. Auch wenn ein niedriger Preis attraktiv erscheinen mag, gibt es oft versteckte Kosten.

Einige Anbieter locken zwar mit einem niedrigen Preis, beschränken jedoch die Anzahl oder Größe der Angriffe, die sie abwehren. Wenn Sie mit zu vielen Angriffen oder einem zu großen Angriff konfrontiert sind, werden Sie vom Anbieter aufgefordert, ein Upgrade auf eine höhere (und teurere) Servicestufe durchzuführen, bevor er den Angriff aufhält – und das, während Sie versuchen, Ihr Unternehmen wieder ans Netz zu bekommen. Erfahrene Anbieter von DDoS-Sicherheitslösungen ermöglichen es Kunden, flexibel zwischen stets verfügbarem DDoS-Schutz („Always-on“) und DDoS-Schutz nach Bedarf („On-Demand“) zu wählen und nahtlos zwischen ihnen zu wechseln, um die Betriebskosten niedrig zu halten und gleichzeitig erstklassigen Schutz zu bieten. Stellen Sie beim Vergleich von Anbietern und Preisen sicher, dass Sie die Kompromisse und deren Auswirkungen auf Ihre DDoS-Sicherheit verstehen.

Tipp

Informieren Sie sich gründlich darüber, was Sie für den Preis bekommen, der Ihnen angeboten wird.



Die DDoS-Sicherheit ist komplex und nimmt in der heutigen, sich schnell entwickelnden Bedrohungslandschaft viel Zeit und Ressourcen in Anspruch. Was gestern funktioniert hat, funktioniert heute oder morgen vielleicht nicht mehr. Der Grundpfeiler für den Erfolg Ihres Geschäfts besteht darin, mit Ihren Endnutzern, Kunden und Mitarbeitern in Verbindung zu bleiben. Hier kann man sich keine Fehler leisten, und es gibt keinen Grund, alleine klarzukommen und dabei hohe Kosten in Kauf zu nehmen. Akamai bietet die umfassendste, flexibelste und zuverlässigste DDoS-Schutzplattform und kann Sie unterstützen.

Erfahren Sie mehr über die DDoS-Sicherheitslösungen von Akamai.

Informationen zu 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: 10/24.