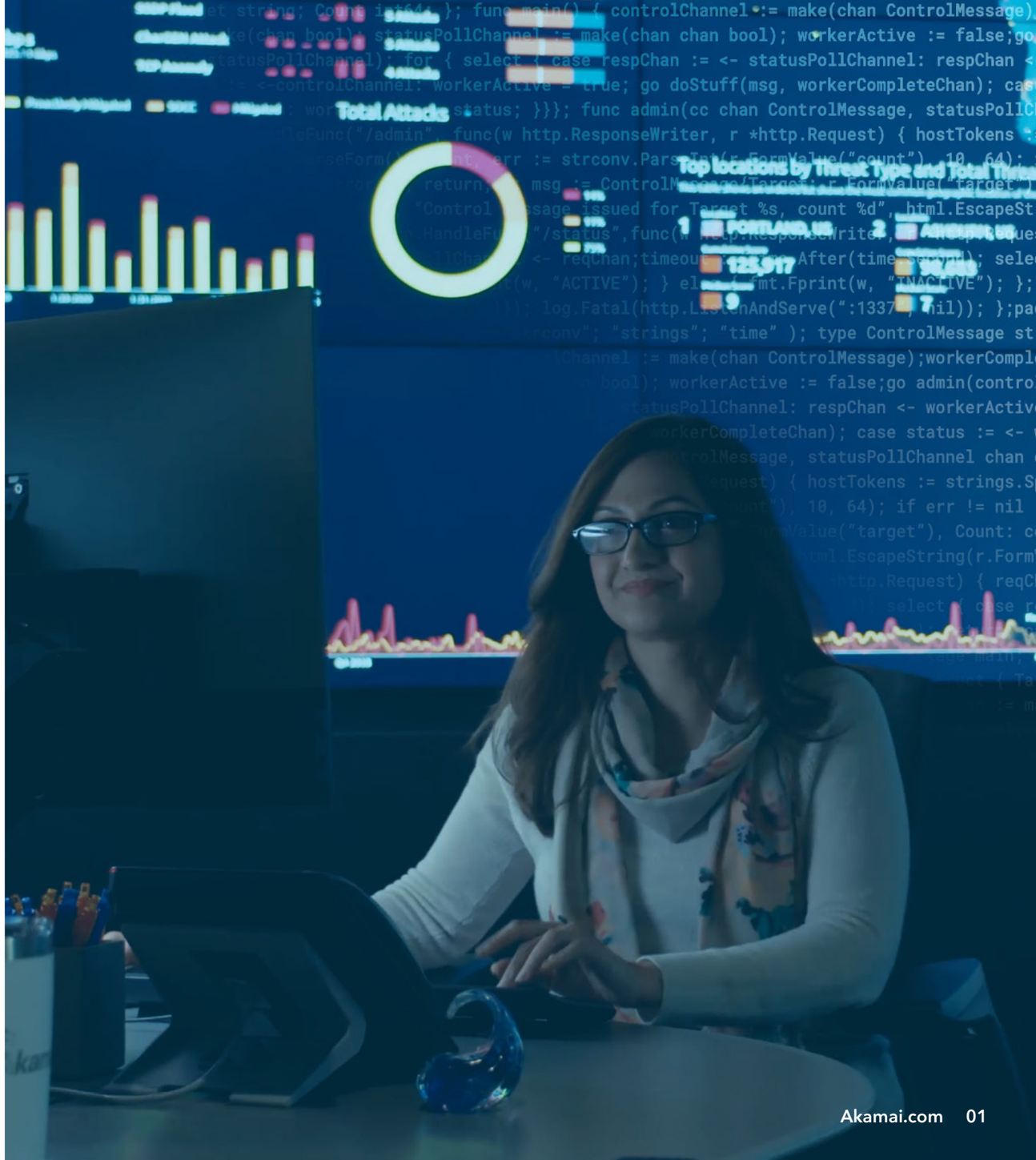
Abwehr von DDoS-Angriffen in Hybrid-Cloud-Umgebungen

E-BOOK

Abwehr von DDoS-Angriffen in Hybrid-Cloud-Umgebungen

Bei Distributed Denial of Service- (DDoS) Angriffen handelt es sich um eine der ältesten Arten von Cyberbedrohungen, die immer noch eingesetzt werden und massive Störungen verursachen. Sie stellen ein Sicherheitsrisiko für praktisch alle Arten von Unternehmen dar, unabhängig von der Größe. Die IDC geht davon aus, dass DDoS-Angriffe bis 2023 jährlich um durchschnittlich 18 % zunehmen werden. Dies macht deutlich, dass Unternehmen ihre Investitionen in zuverlässige Abwehrmechanismen steigern müssen. Manche Unternehmen glauben, dass sie kein Ziel für DDoS-Angreifer darstellen. Doch da Organisationen immer mehr von funktionierenden Internetverbindungen abhängig sind, um geschäftskritische Services und Anwendungen zu betreiben, sind sie anfällig für Ausfallzeiten und Performanceeinbußen, wenn die Infrastruktur nicht geschützt ist.



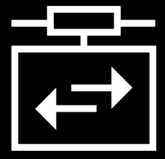
Eine **dynamische** Bedrohung

Die Menge der DDoS-Angriffe verdoppelt sich alle zwei Jahre, und die Komplexität – d. h., die Anzahl und die Kombinationen von Angriffsvektoren – nimmt in bisher ungekanntem Maße zu. Da die Verfügbarkeit von Anwendungen und Netzwerken für die Geschäftskontinuität von entscheidender Bedeutung ist, führen Cyberkriminelle volumetrische DDoS-Angriffe durch, die auf die Protokoll- und Anwendungsebene abzielen. Sie nutzen jede potenzielle Schwachstelle aus, um internetbasierte Ressourcen und Assets für die Endnutzer unzugänglich zu machen.

DDoS-ANGREIFER NUTZEN ALLE POTENZIELLEN SCHWACHSTELLEN AUS, Z. B.:

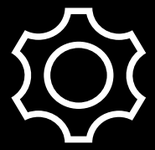
Websites

Webanwendungen und andere Unternehmensservices



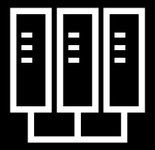
VPN-Konzentratoren für den Remotezugriff auf Unternehmensressourcen

SD-WAN-Controller



Programmierschnittstellen (APIs)

DNS-Server (Domain Name System) und Ursprungsserver



Rechenzentrums- und Netzwerkinfrastruktur

Beim Ausspähen der Umgebungen, Anwendungen und IP-Bereiche ihrer Opfer ermitteln die Angreifer, mit welchen DDoS-Vektoren sie den größtmöglichen Schaden bei internetbasierten Services und Ursprungshost-Infrastrukturen verursachen können.
Die Eintrittsbarriere ist für diese Cyberkriminellen sehr niedrig, und es stehen ihnen zahlreiche Angriffstechniken und Tools (z. B. Booter, DDoS-for-hire) zur Verfügung, mit denen sie Sicherheitslücken und Schwachstellen im Schutzsystem des Unternehmens erkennen.

> Die Beweggründe von Cyberkriminellen sind unterschiedlich und können Erpressung oder Finanzmanipulation umfassen. Die Erpressungskampagnen, die Akamai beobachtet, betreffen nicht nur den Finanzsektor, sondern haben zunehmend auch Unternehmensservices, den Glücksspielsektor, die Reisebranche und das Gastgewerbe sowie Hightech-, Logistik- und Einzelhandelsunternehmen zum Ziel.

– Roger Barranco, Vice President of Global Security Operations, Akamai

Das Schadenpotenzial von DDoS-Angriffen wird angesichts des Trends bei Unternehmen, Remotezugriffsfunktionen zu skalieren und abzusichern, um die Produktivität ihrer Mitarbeiter zu gewährleisten und den normalen Geschäftsbetrieb aufrechtzuerhalten, immer deutlicher.

Die Folgen eines DDoS-Angriffs

Bei volumetrischen und protokollbasierten Angriffen auf die Vermittlungsebene (Layer 3) und die Transportebene (Layer 4) versuchen die 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. Mit anwendungsbasierten Attacken (Layer 7) zielen die Cyberkriminellen darauf ab, die Web-Performance und das Nutzererlebnis mit Vektoren wie „Low-and-Slow"-Angriffen oder HTTP-Floods zu beeinträchtigen. So entstehen Ausfallzeiten, die sich negativ auf das Geschäftsergebnis auswirken.

Diese Ausfälle sorgen jedoch nicht nur dafür, dass die anvisierten Services und Anwendungen vorübergehend nicht verfügbar sind, sondern haben noch schwerwiegendere Auswirkungen. ***Laut Ponemon Institute belaufen sich die durchschnittlichen jährlichen Kosten eines DDoS-Angriffs für ein Unternehmen auf 1,7 Millionen US-Dollar***, bedingt durch gesteigerten Bedarf an technischem Support, höheren Ressourcenaufwand für die Reaktion auf Vorfälle, interne Eskalationen, Rechtskosten, Betriebsstörungen und verringerte Mitarbeiterproduktivität.

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

Die Cloud erschwert weiterhin eine gute **Sicherheitsstrategie**

Durch die Stilllegung herkömmlicher Rechenzentren und die Verlagerung von Anwendungen in cloudbasierte Umgebungen wird die Sicherheitsarchitektur immer komplexer. Viele Unternehmen wissen nicht, wie sie ihre internetbasierten Assets mit demselben Sicherheitsniveau wie ihre Rechenzentren gegen DDoS-Angriffe schützen können. Hinzu kommt, dass viele in der Cloud gehostete IPs außerhalb der direkten Kontrolle des Unternehmens liegen, sodass sie ohne ordnungsgemäßen Schutz besonders anfällig für DDoS-Angriffe sind.

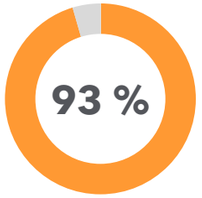
Die Cyberkriminellen sind sich der beschleunigten Migration zu Colocation-Einrichtungen und in die Public Cloud sehr wohl bewusst. Sie sind darauf aus, Schwachstellen in der Sicherheitsarchitektur und -strategie auszunutzen, die durch uneinheitliche Sicherheitsrichtlinien und -anforderungen entstehen. Zudem machen sie es sich zunutze, dass dem Unternehmen die Fehlerbehebung in einer heterogenen und fragmentierten Cloud-Hosting-Infrastruktur häufig schwer fällt.

ZUSAMMENFASSUNG:

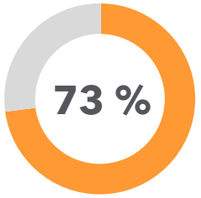
Moderne Unternehmen benötigen anpassungsfähige Verteidigungsmechanismen, um eine Vielzahl webbasierter Assets und Services unabhängig vom Standort zu schützen. Heute verfolgen mehr als 93 % der Unternehmen (mit < 1.000 Mitarbeitern) eine Multi-Cloud-Strategie. Aufgrund der komplexeren Infrastruktur können Sicherheitslücken entstehen, die sofortige Maßnahmen erforderlich machen.[1]

[1] *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*

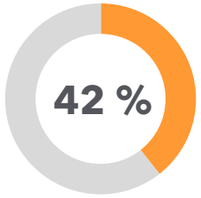
Nicht jeder Anbieter von Public-Cloud-Umgebungen übernimmt die Verantwortung für die Sicherheit. Dabei gehen Unternehmen oft von falschen Voraussetzungen aus und legen damit ihre verletzlichsten Stellen offen. So waren in einer IBM-Umfrage beispielsweise 73 % der Befragten der Ansicht, dass die Hauptverantwortung für den Schutz von Software as a Service (SaaS) bei dem Public-Cloud-Dienstanbieter (CSP) läge, und 42 % glaubten, dass hauptsächlich der CSP für den Schutz der Infrastruktur as a Service (IaaS) in der Cloud verantwortlich sei. Diese unklaren Verantwortlichkeiten bei Schutzmaßnahmen können die Sicherheit beeinträchtigen – ein Risiko, das kein Unternehmen akzeptieren sollte.



der Unternehmen verfolgen eine Multi-Cloud-Strategie.



der Befragten glauben, dass die Verantwortung für den SaaS-Schutz bei den Public-Cloud-Serviceprovidern liegt.



der Befragten sind der Meinung, dass die CSPs für den Schutz der Cloud-IaaS verantwortlich sind.

Aus einem kürzlich veröffentlichten Bericht von Forrester geht hervor, dass sich die meisten Unternehmen für einen hybriden Ansatz entscheiden, der sowohl mehrere Public-Cloud-Anbieter als auch lokale Workloads umfasst. Daher empfiehlt das Analyseunternehmen eine DDoS-Abwehrtechnologie, mit der auch hybride Architekturen geschützt werden können.

Ein Cyberkrimineller braucht nur einen einzigen Treffer zu landen. Unternehmen benötigen reaktionsschnelle Abwehrmechanismen zur Verteidigung.

DDoS-Schutz ist **nicht gleich** DDoS-Schutz

Je mehr Investitionen in die Cloud-Infrastruktur getätigt werden, desto größer wird die Herausforderung der Sicherheitsteams, konsistente Kontrollen für die hybriden Umgebungen sicherzustellen. 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 die Unternehmen eine solche Zentrale nicht nur, um mehr Transparenz zu erzielen, sondern auch zur Optimierung der Berichterstellung. Auf diese Weise können die Daten zu Sicherheitsvorfällen über APIs in Korrelationssysteme eingespeist werden.

Zur Lösung dieses Problems suchen die Unternehmen Anbieter von Schutztechnologie gegen cloudbasierte DDoS-Angriffe, die ihre Hybrid-Cloud-Migrationsstrategie unterstützen und nicht behindern. Die Unternehmen benötigen skalierbare, reaktionsfähige Verteidigungsmechanismen für alle Geschäftsservices, unabhängig davon, wo sich diese befinden. 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. Viele der internetbasierten Assets sind über mehrere Clouds verteilt, was die Komplexität noch verstärkt.

Hinzu kommt, dass die lokalen DDoS-Abwehrlösungen vieler CSPs Mängel in den wichtigen Bereichen Transparenz, SLA-Compliance 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 Berichterstellung bezeichnet werden.

Darüber hinaus bieten einige CSPs kein SLA an, in dem die Reaktionszeit auf einen Angriff festgelegt ist. Stattdessen stellen sie dem betroffenen Unternehmen Serviceguthaben zur Verfügung. 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.

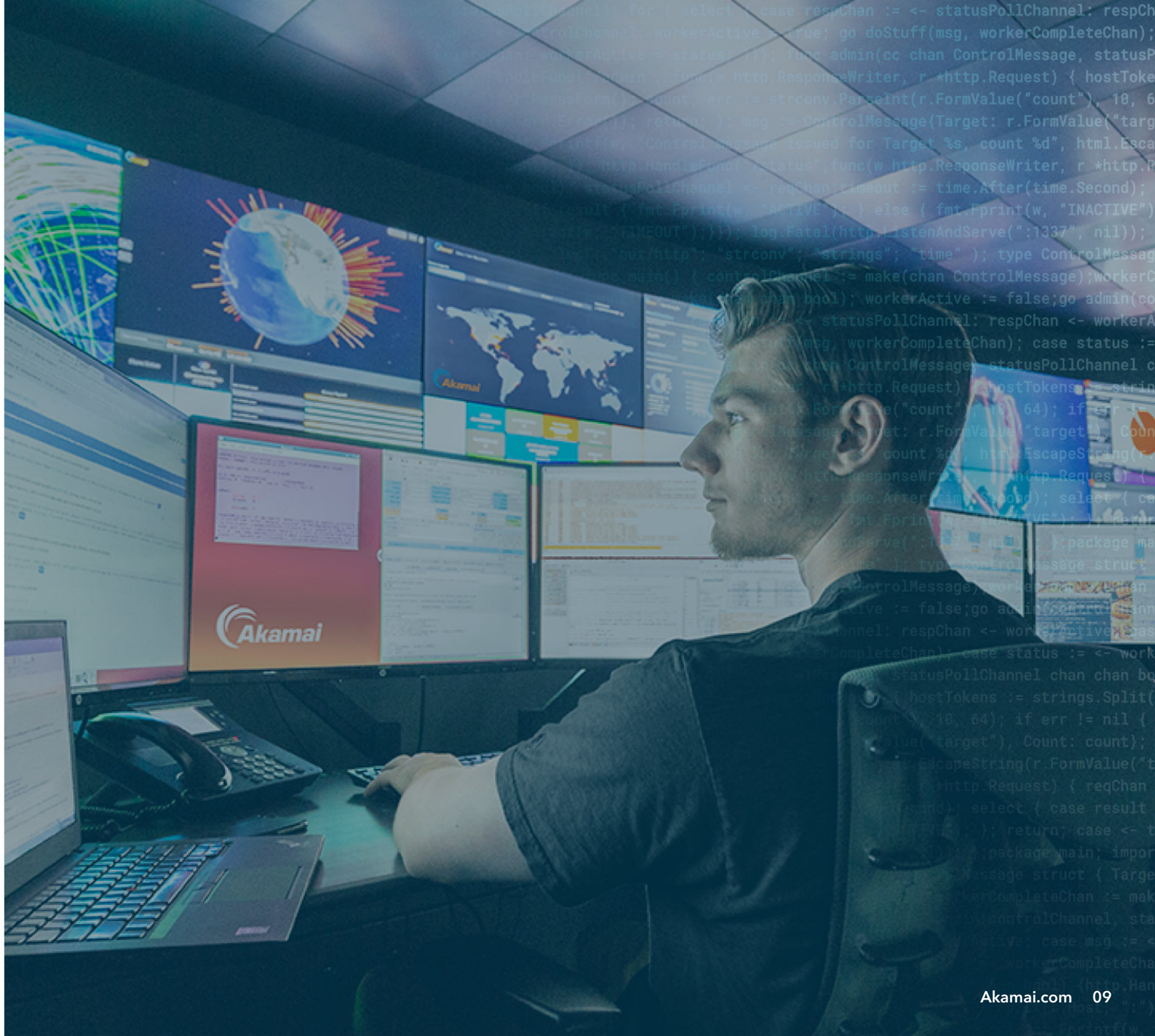
Außerdem stellen viele CSPs neben der Unterstützung vor, während und nach einem Angriff keinen On-Demand-Support in einem rund um die Uhr verfügbaren Security Operations Center zur Verfügung, wie es bei führenden Anbietern von cloudbasierten DDoS-Schutzsystemen der Standard ist. Wenn ein CSP Support anbietet, muss dafür oft ein Aufschlag gezahlt werden. Dies ist meist teurer als eine dezidierte DDoS-Abwehrlösung von einem führenden Anbieter. Bei einer vollständig verwalteten 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.

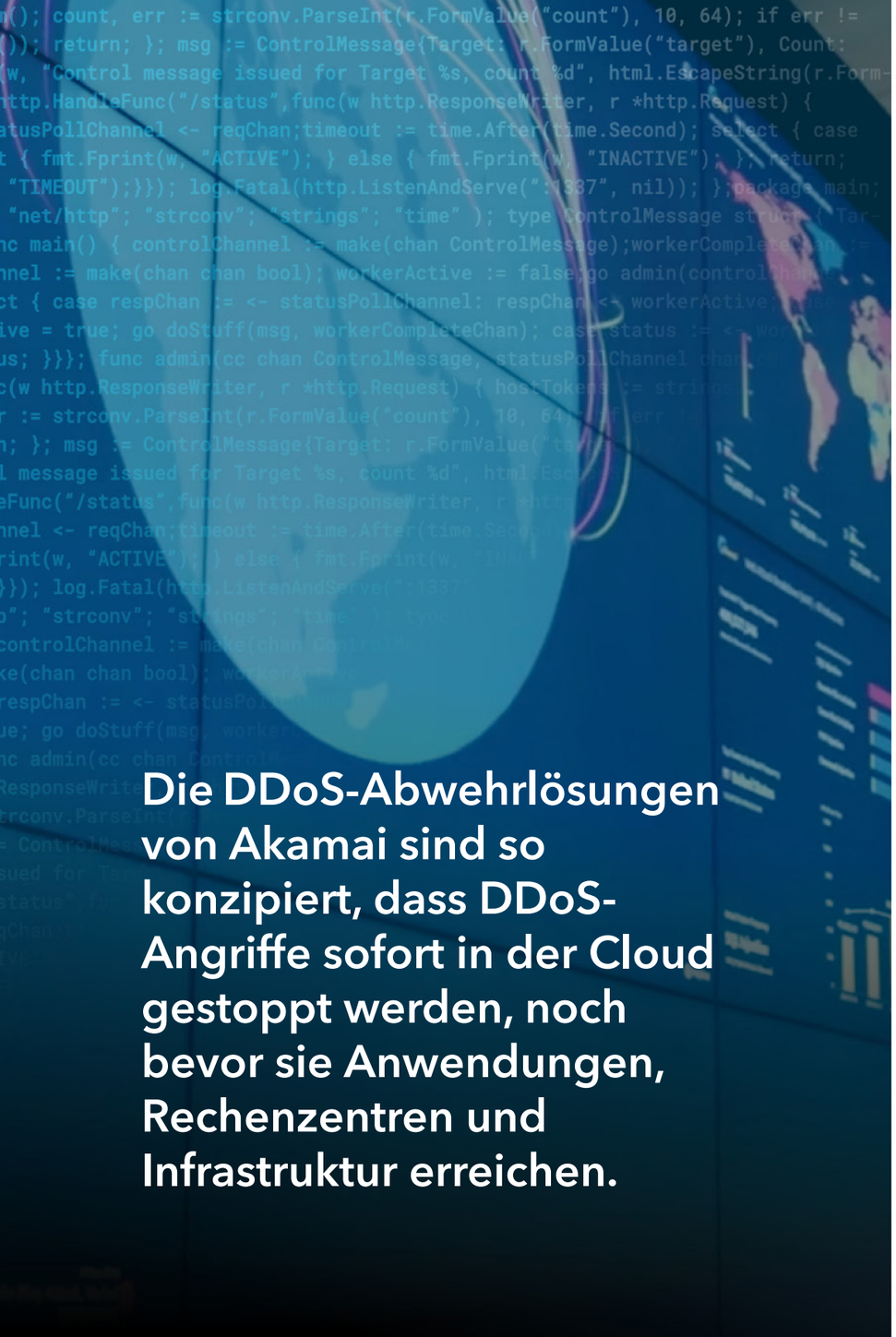
In der heutigen Bedrohungslandschaft setzen moderne Unternehmen bei der DDoS-Abwehr auf Partner, die in hybriden Umgebungen ein optimales Sicherheitserlebnis gewährleisten und gleichzeitig die Komplexität der Angriffsfläche verringern können.

Ein guter Partner für die DDoS-Abwehr sollte Ihre Cloud-Strategie nicht behindern, sondern unterstützen. Nur so lassen sich Sicherheitsrisiken verringern.

Maßgeschneiderter DDoS-Schutz von Akamai

Bei der Cloud-Strategie brauchen Unternehmen eine End-to-End-Lösung, und beim DDoS-Schutz ist ebenfalls ein End-to-End-Ansatz erforderlich. Die Schutzsysteme von Akamai folgen einem ganzheitlichen Ansatz und fungieren als die erste Verteidigungslinie bei einem Angriff. Sie bieten eine dedizierte Edge-Struktur, verteilte DNS-Services sowie Sicherheitsfunktionen für die Cloud und sind so konzipiert, dass Kollateralschäden und Ausfälle einzelner Komponenten verhindert werden. Im Gegensatz zu den Cloudsicherheitsarchitekturen anderer Anbieter, die als „Komplettlösung" vermarktet werden, bieten die speziell entwickelten DDoS-Clouds von Akamai bessere Ausfallsicherheit, dedizierte Scrubbing-Kapazität und höhere Abwehrqualität. Sie sind genau auf die individuellen Anforderungen der Webanwendungen oder internetbasierten Services abgestimmt.





Die DDoS-Abwehrlösungen von Akamai sind so konzipiert, dass DDoS-Angriffe sofort in der Cloud gestoppt werden, noch bevor sie Anwendungen, Rechenzentren und Infrastruktur erreichen.

EDGE-SCHUTZ

Die Akamai Edge (Content Delivery Network, CDN) leitet und beschleunigt den Webtraffic mithilfe von HTTP- und HTTPS-Protokollen. Jeder Edge-Server von Akamai fungiert als Reverse-Proxy und leitet legitimen HTTP/S-Traffic an die Ports 80 und 443 weiter. Der gesamte sonstige Traffic wird an der Netzwerk-Edge gestoppt. Das bedeutet, dass die sofortige Abwehr aller DDoS-Angriffe auf Netzwerkebene inhärenter Bestandteil der Lösung jedes Akamai-Kunden ist. Der Schutz ist bereits in die Webbereitstellung integriert.

DNS-SCHUTZ

Die gleiche Technologie wird für den autoritativen DNS-Service „Edge DNS“ von Akamai verwendet. Der gesamte Traffic, der nicht über Port 53 läuft, wird sofort abgebrochen.
Im Gegensatz zu anderen DNS-Lösungen wurde Edge DNS von Akamai speziell für Verfügbarkeit und Ausfallsicherheit bei DDoS-Angriffen entwickelt. Daneben wurde die Performance berücksichtigt. Die Lösung umfasst Redundanzen auf mehreren Ebenen einschließlich Nameservern, Points of Presence, Netzwerken und sogar segmentierten IP-Anycast-Clouds.

SCHUTZ DURCH CLOUD-SCRUBBING

Der praxisbewährte Cloud-Scrubbing-Service Prolexic schützt ganze Rechenzentren und die internetbasierte Infrastruktur vor DDoS-Angriffen – über alle Ports und Protokolle hinweg. Indem wir sowohl legitimen als auch schädlichen Traffic über Prolexic weiterleiten, können wir sowohl positive als auch negative Sicherheitsmodelle erstellen, um DDoS-Angriffe proaktiv und unmittelbar mit hoher Genauigkeit abzuwehren. Die Experten im Security Operations Command Center (SOCC) von Akamai fungieren als Erweiterung des Notfallteams des Kunden. Dies schafft ein Gleichgewicht zwischen automatisierter Erkennung und Reaktion sowie menschlichem Eingreifen.

Warum Akamai?

Akamai verfügt über die größten und ausgereiftesten Clouds zu Abwehr von DDoS-Angriffen weltweit. Ganz gleich, ob Sie einzelne Anwendungen, ganze Rechenzentren oder autoritative DNS-Dienste schützen müssen, die Architektur von Akamai zur DDoS-Abwehr bietet besonders umfassende Kapazitäten, große Ausfallsicherheit und sehr schnelle Prozesse.

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

Akamai

Da sich die DDoS-Angriffsvektoren ständig ändern und der Umfang der Angriffe immer weiter wächst, müssen Anbieter fortlaufend in die Entwicklung und Bereitstellung von Tools und Methoden investieren, um Bedrohungen zu erkennen und die Abwehr zu orchestrieren. Akamai ist bestrebt, den Bedrohungen immer einen Schritt voraus zu sein, indem Angriffe bereits abgewehrt werden, bevor sie beginnen.

Die Strategie Ihres Unternehmens zur DDoS-Abwehr muss auch auf Ihre Cloud-Strategie abgestimmt sein. Dank der DDoS-Abwehrfunktionen der Akamai Intelligent Edge Platform können unsere Kunden den Schutz über ihre Kernsysteme hinaus auf die Cloud und die Edge ausweiten und Risiken minimieren, ohne an Flexibilität für zukünftige Entwicklungen ihrer Cloud-Strategien einzubüßen.

Fragen Sie uns, wie wir Ihr Unternehmen **schützen** können

Weitere Informationen

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter ***www.akamai.com****, im Blog* ***blogs.akamai.com*** *oder auf Twitter unter* ***@Akamai****. Unsere globalen Standorte finden Sie unter* ***www.akamai.com/locations****. Veröffentlicht: November 2020*