CLOUDFLARE®

Fünf Best Practices zur Abwehr von DDoS-Angriffen

Distributed Denial-of-Service-Angriffe im Wandel: Wie man sich schützen und Schwachstellen in jeder Schicht neutralisieren kann

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

CLOUDFLARE

I. Kurzfassung

Weltweit zählen Distributed Denial-of-Service (DDoS)-Angriffe nach wie vor zu den erfolgreichsten Methoden, mit denen Cyberkriminelle Unternehmen beträchtlichen Vermögens-, Betriebs- oder Imageschaden zufügen. Diese Attacken können verschiedene Formen annehmen. Das Ziel besteht aber immer darin, die anvisierten Server, Dienste oder Netzwerke mit großen Mengen Traffic von kompromittierten Geräten oder Netzwerken außer Gefecht zu setzen.

Auf die verstärkten Abwehrmaßnahmen der Unternehmen reagieren Verbrecher im Cyberspace mit neuen Angriffsformen, die zahlreiche Anwendungen und Dienste ins Visier nehmen. Einige dieser neuartigen Offensiven richten sich gegen die Schichten 3 und 4 des Open Systems Interconnection (OSI)-Modells und verursachen Traffic-Spitzen von 1,3 TB pro Sekunde oder mehr. Hinzu kommen auf Schicht 7 basierende Angriffe auf Service Gateways und Anwendungsschichten, die langsam und mit geringer Intensität ausgeführt werden, damit sie unbemerkt bleiben.

Den Herausforderungen von DDoS-Attacken kann man nur mit einem ganzheitlichen Ansatz begegnen, der Bedrohungen in allen Schichten bekämpft. Erhöhte Sicherheit sollte aber nicht auf Kosten der Performance gehen. Lokale Lösungen können zwar durchaus einen Beitrag leisten, robuster ist aber eine skalierbare und cloudbasierte Abwehrlösung am Netzwerkrand, die größtmögliche Flexibilität bietet, mit unbegrenzten Kapazitäten aufwartet und auch die Performance berücksichtigt.

TEIL 1

Was ist ein DDoS-Angriff?

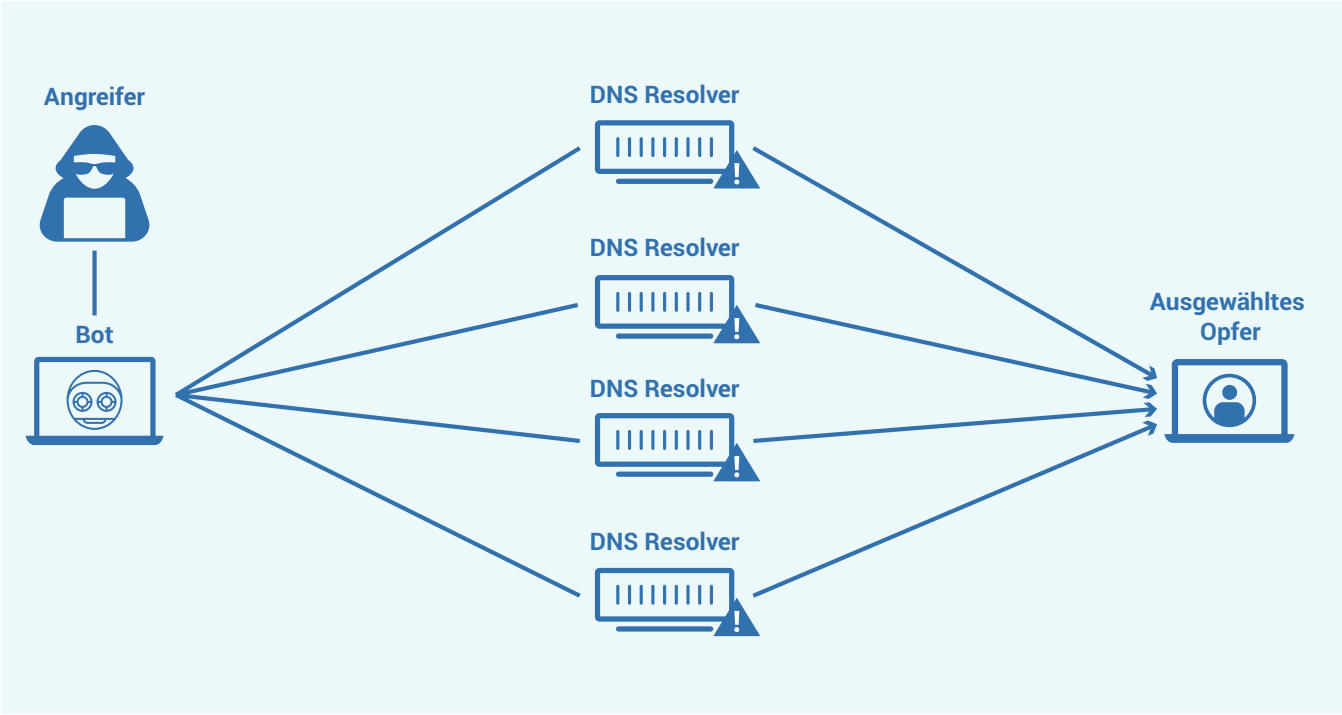
Ein Distributed Denial of Service-(DDoS)-Angriff ist ein böswilliger Versuch, mit einer großen Menge Internet-Traffic einen Server, Dienst oder ein Netzwerk zu überlasten und so den normalen Datenverkehr des Angriffsziels zu stören. Um mit solchen Attacken Erfolg zu haben, müssen die Angreifer die Kontrolle über vernetzte Computer, Router, IoT-Geräte oder andere Endpunkte erlangen, um diese als Quelle für Angriffs-Traffic einsetzen zu können. Diese an sich harmlosen Geräte werden zur Waffe, indem sie mit Malware infiziert und in ein aus der Ferne aktivierbares Botnetz eingebunden weden.

Wenn die IP-Adresse eines anvisierten Servers oder Netzwerks ermittelt wurde, senden alle Bots gleichzeitig Anfragen an dieses Ziel, um eine Überlastung zu verursachen. Das hat zur Folge, dass der jeweilige Dienst für den normalen Datenverkehr nicht mehr zur Verfügung steht. Da alle Bot-Aktivitäten von legitimen Geräten ausgehen, lässt sich Angriffs-Traffic oft nur sehr schwer von regulärem Datenverkehr unterscheiden.

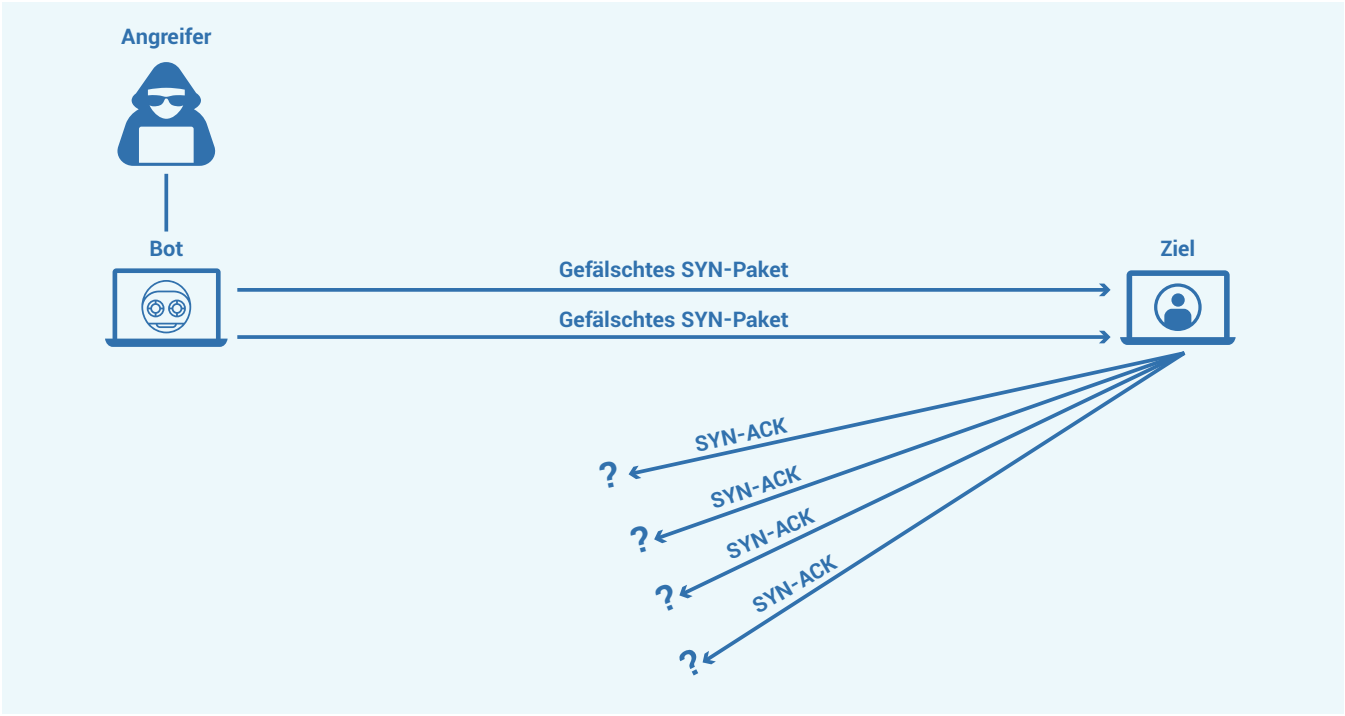
Verschiedene Formen von DDoS-Angriffen

DDoS-Angriffe können sich gegen jede der sieben Schichten innerhalb des OSI-Modells für Netzwerkverbindungen richten. Alle Attacken dieser Art haben gemein, dass ihre Ziele mit bösartigem Traffic überlastet werden sollen. Sie lassen sich jedoch in drei Kategorien unterteilen.

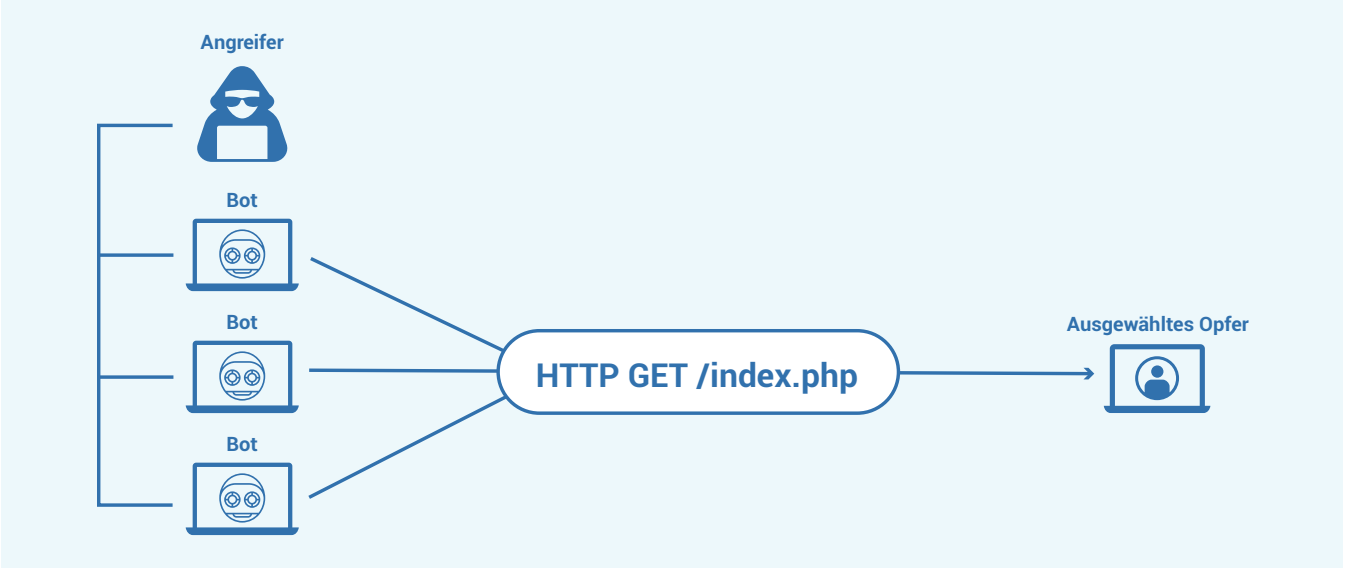
VOLUMETRISCHE ANGRIFFE: Hier wird das Netzwerk ins Visier genommen, die Web-Performance verringert und der Zugang für legitime Nutzer erschwert, um zwischen der Website und dem Rest des Internet einen Datenstau zu erzeugen. Häufig werden zu diesem Zweck Verfahren wie DNS Amplification eingesetzt. Damit lassen sich enorme Traffic-Spitzen erzeugen, die in Bits pro Sekunde (Bps) gemessen werden.



PROTOKOLLANGRIFFE: Das Ziel besteht in diesem Fall darin, Schwachstellen in den Schichten 3 (Netzwerk) und 4 (Transport) des OSI-Modells auszunutzen und die verfügbaren Kapazitäten von Webservern und ihren Zwischenressourcen – einschließlich Firewalls und Load Balancer – vollständig auszuschöpfen. Dazu können SYN Flood-, Ping of Death-, Smurf- und IP-Fragmentierungs-Angriffe eingesetzt werden, deren Intensität jeweils in Paketen pro Sekunde (Pps) gemessen wird.



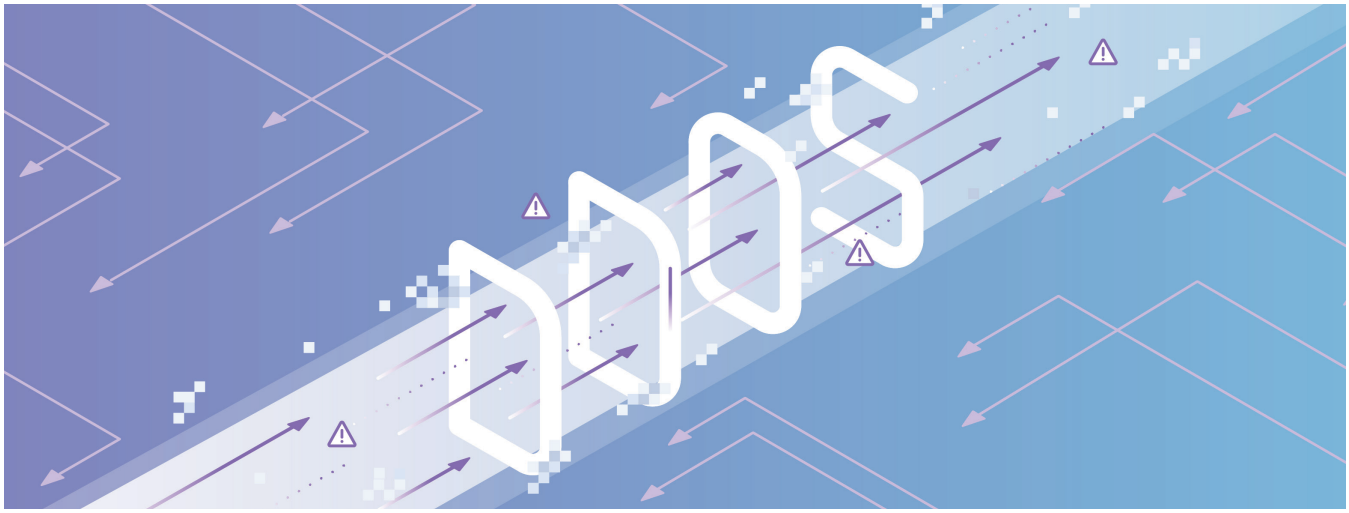
ANGRIFFE AUF DIE ANWENDUNGSSCHICHT: Bei diesen Attacken – auch als Layer-7-DDoS-Angriffe bekannt – steht die Schicht im Fokus, in der Webseiten auf dem Server erzeugt und nach HTTP- oder HTTPS-Anfragen bereitgestellt werden. Die Wirkung ist in etwa so, als würde man auf vielen Rechnern gleichzeitig im Browser die Webseite aktualisieren. Die Folge ist eine Flut an HTTP/S-Anfragen, deren Intensität in Anfragen pro Sekunde (Requests per second – Rps) angegeben wird.



Es bestehen einige Überschneidungen zwischen den einzelnen Angriffsformen. So können Protokollangriffe beispielsweise volumetrisch sein. Darüber hinaus haben Kriminelle die Möglichkeit, mit Multi-Vektor-Angriffen mehrere Schichten des Protokollstapels gleichzeitig zu attackieren oder entsprechend den von ihrem Ziel eingesetzten Gegenmaßnahmen variierende Angriffsvektoren einzusetzen. Außerdem dienen viele Multi-Vektor-Attacken nur als Ablenkungsmanöver für andere kriminelle Machenschaften wie Datendiebstahl oder -missbrauch.

Wie DDoS-Angriffe Unternehmen schaden

Ist der Internetauftritt eines Unternehmens aufgrund von DDoS-Angriffen nicht mehr erreichbar, hat das negative Auswirkungen auf Einnahmen, Kundenbetreuung und die grundlegenden Geschäftsfunktionen. Ob es den Angreifern nun darum geht, eine Website oder ein Netzwerk außer Gefecht zu setzen, Traffic zu geschäftlichen Rivalen umzuleiten, den Diebstahl von Unternehmensdaten zu verschleiern oder schlicht den größtmöglichen Imageschaden zu verursachen: Häufig werden die Nutzer die Schuld bei dem Unternehmen suchen. Im Schnitt kostet ein DDoS-Angriff einen mittelständischen Betrieb 123.000 USD und ein großes Unternehmen über 2 Mio. USD[1]. Und die Attacken reißen nicht ab. Es wird erwartet, dass die Zahl der DDoS-Angriffe rund um den Globus von 11,9 Mio. im Jahr 2020 auf über 14,5 Mio. im Jahr 2022 ansteigt[2].



TEIL 2

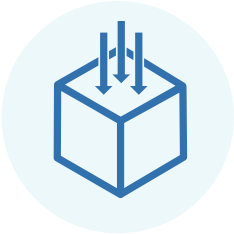
Wie sich DDoS-Angriffe wandeln und was man ihnen entgegensetzen kann

Folgende Fähigkeiten sind im Allgemeinen für einen wirksamen Schutz vor DDoS-Angriffen erforderlich:

- Unterscheidung einer hohen Nutzernachfrage von den durch einen Angriff verursachten Traffic-Spitzen
- Blockade des Botnet-Traffics, ohne reguläre Datenströme zu unterbrechen
- Aufteilung des verbleibenden Traffic in handliche Einheiten und intelligentes Routing dieser Datenpakete, um Ausfälle zu verhindern
- Kontinuierliche Analyse des Datenverkehrs, um schädliche Muster zu erkennen und auf dieser Grundlage anpassungsfähige und robuste Abwehrmechanismen zu entwickeln

Diese Aufgaben werden jedoch durch zwei sich derzeit abzeichnende Trends erschwert.

Volumetrische Angriffe werden größer



- Zwischen 2018 und 2019 ist die Zahl volumetrischer DDoS-Angriffe mit einem Umfang von mehr als 100 Gbps um 967% in die Höhe geschnellt[3]
- DDoS-Angriffe mit bis zu 1,3 TB pro Sekunde, wie zum Beispiel die Attacke, die im Jahr 2018 GitHub lahmgelegt hat, sind mittlerweile an der Tagesordnung
- Anfang 2020 wurde Berichten zufolge ein volumetrischer DDoS-Angriff in der Netzwerkschicht ausgeführt, der einen Umfang von 92 Gbit/s und 10,38 Millionen Paketen pro Sekunde (Mpps) erreicht hat[4]
- Die meisten volumetrischen DDoS-Attacken sind nach wenigen Minuten vorüber, doch manche können Stunden dauern und bis zu 73 % der Unternehmen, die Opfer einer solchen Offensive werden, verzeichnen innerhalb der nächsten 24 Stunden einen weiteren Angriff[5]

Die Komplexität der Angriffe nimmt zu

- Drei Viertel[6] aller DDoS-Angriffe setzen mehrere Vektoren ein
- Ein gegen die Schichten 3 und 4 gerichteter DNS Amplification-Angriff in Kombination mit einer HTTP/S Flooding-Attacke in Schicht 7 wäre ein Beispiel für einen Multi-Vektor-DDoS-Angriff
- Je komplexer der Angriff, desto schwieriger ist es, ihn abzuwehren. Der Angreifer versucht, so unauffällig wie möglich zu agieren, was die Unterscheidung zwischen regulärem und bösartigem Traffic zusätzlich erschwert
- Abwehrmaßnahmen zur Unterbindung oder Einschränkung des Datenverkehrs laufen ins Leere, wenn sich die Angriffsmethode daran anpasst

Wir möchten nun fünf Best Practices unter Berücksichtigung dieser Anforderungen und der sich wandelnden Trends vorstellen, denen Unternehmen im Kampf gegen DDoS-Angriffe Vorrang einräumen sollten.

TEIL 3

Best Practices zur Abwehr von DDoS-Angriffen

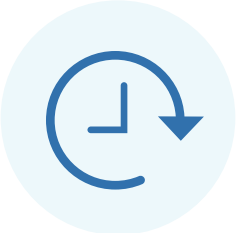
1 STIMMEN SIE IHRE TAKTIK AUF DAS AB, WAS SIE SCHÜTZEN WOLLEN

Wenn es Ihnen um den Schutz von Webservern geht, kann ein Reverse Proxy verhindern, dass Angreifer die IP-Adressen Ihrer Server ermitteln und ins Visier nehmen. So kann nur der Reverse Proxy ins Fadenkreuz geraten. Bei komplexeren Angriffen in Schicht 7 kann eine Web Application Firewall (WAF) als Reverse Proxy fungieren und angegriffene Server gegen bestimmte Arten von bösartigem Traffic abschirmen. Manche Unternehmen entscheiden sich, ihre Reverse Proxys selbst zu entwickeln oder zu installieren, doch das bringt eine hohe Beanspruchung von Software- und Personalressourcen mit sich und erfordert beträchtliche Investitionen in Hardware.

Ein Content Delivery Network (CDN) zählt zu den einfachsten und günstigsten Möglichkeiten, sich die Vorteile eines Reverse Proxy zunutze zu machen. Halten Sie Ausschau nach einem CDN mit Global Server Load Balancing, damit die Daten Ihrer Website auf mehrere Server rund um den Globus verteilt werden können. Auf diese Weise werden DDoS-Angriffe näher an ihrem Ausgangspunkt bekämpft, ohne dass die Performance dabei leidet.

Geht es um die Härtung der Netzwerkinfrastruktur, kann der Datenverkehr mithilfe des Border Gateway Protocol (BGP) zu Scrubbing-Zentren umgeleitet werden, die bösartigen Traffic herausfiltern können. Doch wenn der gesamte Traffic diese nur in begrenzter Anzahl vorhandenen speziellen Rechenzentren durchlaufen und dabei lange Wege zurücklegen muss, erhöht sich die Latenz unter Umständen erheblich.

Deshalb ist es ratsam, zur DDoS-Abwehr auf cloudbasierte Lösungen in ausreichendem Maßstab zu setzen. Bei cloudbasierten Abwehrsystemen veröffentlicht der Anbieter AS-Nummern (Automous System Numbers – ASNs), sodass der Datenverkehr ohne Umweg über den Ursprungsserver direkt zu einem Scrubbing-Zentrum geleitet wird. Weil der Traffic auf diese Weise in geringerer Entfernung zur Angriffsquelle gefiltert wird, reduziert sich die Latenz.

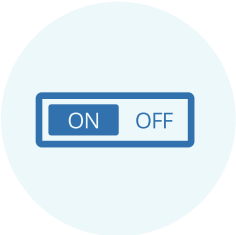


2 LEGEN SIE DEN FOKUS AUF DIE ZWEI WICHTIGSTEN METRIKEN –KAPAZITÄT UND ABWEHRZEIT

Verschaffen Sie sich einen Überblick, welche Kapazitäten Sie zur Abwehr von DDoS-Angriffen nutzen können, ohne die Funktionsfähigkeit Ihrer Website einzuschränken. Die Einrichtung lokaler Serverfarmen ist die herkömmliche Lösung für die Bewältigung von Traffic-Spitzen. Dafür muss man aber schnell tief in die Tasche greifen und früher oder später kann selbst die widerstandsfähigste Unternehmensinfrastruktur volumetrischen Angriffen, die jeden Tag mächtiger werden, nicht mehr standhalten.

Eine Durchsatzbegrenzung kann zwar eine Hilfe sein, schränkt aber die Performance ein und ist im Fall einer Überlastung der Infrastruktur auch nicht in der Lage, einen Ausfall zu verhindern. Wenn bereits eine Einschränkung der Verfügbarkeit von nur wenigen Sekunden Einnahmen und Rentabilität schmälert, sind kurze Abwehrzeiten ausschlaggebend. Wenn bei einem Ausfall eine andere Site den Datenverkehr schultern kann, verkürzt sich die Abwehrzeit. Das funktioniert allerdings nur, solange Ihre Infrastruktur der Belastung standhält.

Auch in diesem Fall arbeitet eine cloudbasierte Abwehrlösung mit unbegrenzter Kapazität zum Schutz vor DDoS-Angriffen – unabhängig von deren Ausmaß und Komplexität – erfolgreicher. Damit können Dienste am Netzwerkrand bereitgestellt werden, was größtmögliche Flexibilität im Kampf gegen sich rasant wandelnde DDoS-Attacken bietet.



3 VERGLEICHEN SIE KONTINUIERLICHEN SCHUTZ UND SCHUTZ AUF ABRUF

Auf Abruf verfügbare Abwehrdienste erlauben einen normalen Datenverkehr, bis ein möglicher DDoS-Angriff registriert wird. Der Traffic wird dann zu dem Abwehrdienst in der Cloud geleitet, gefiltert und anschließend wieder zu dem ursprünglichen Server geschickt. Sie zahlen nur im Bedarfsfall für die DDoS-Abwehr und weder entsteht weiterer Verwaltungsaufwand noch werden zusätzliche Ressourcen beansprucht. Allerdings hat diese Lösung auch Nachteile, insbesondere was die Abwehrzeit angeht. Es dauert länger, dem Angriff Einhalt zu gebieten, weil eine Analyse erst beginnt, wenn Traffic-Spitzen bestimmte Schwellenwerte erreicht haben und die Abwehrfunktion manuell aktiviert wird.

Bei der dauerhaften Abwehr wird dagegen der gesamte Datenverkehr der Website kontinuierlich geroutet und gefiltert, sodass grundsätzlich nur unbedenklicher Traffic zu den Servern des Kunden gelangt. Diese Variante ist zwar kostspieliger als ein On-Demand-Dienst, bietet dafür aber auch einen unterbrechungsfreien Schutz und kürzere Reaktionszeiten, weil die Funktion niemals manuell aktiviert werden muss. Darüber hinaus können sich Dauerdienste zu einem Pauschalpreis für Unternehmen, die inzwischen aufgrund einer wachsenden Zahl von DDoS-Attacken einem regelrechten Sperrfeuer von Angriffen ausgesetzt sind, auf längere Sicht als die günstigere Alternative erweisen.

4 SICHERHEIT SOLLTE NIE ZULASTEN DER PERFORMANCE GEHEN

DDoS-Angriffe verursachen Verzögerungen und Ausfälle, die nicht nur die Performance beeinträchtigen, sondern auch dem nachhaltigen Wachstum eines Unternehmens im Wege stehen. In der digitalen Welt erwarten moderne Verbraucher von Webseiten und Anwendungen kurze Ladezeiten und ständige Erreichbarkeit. Der durchschnittliche Nutzer bemerkt Latenz ab 30 Millisekunden. Verlängert sich die Ladezeit auch nur um eine Sekunde, kann dadurch die Konversionrate um 7 % sinken[7].

Zudem geht mit höherer Latenz eine geringere Produktivität einher. Selbst unter optimalen Bedingungen vergeudet jeder Angestellte im Schnitt eine Woche im Jahr damit, auf die Reaktion des Firmennetzwerks zu warten[8]. Den 1000 umsatzstärksten Unternehmen der USA bescheren Ausfallzeiten schon jetzt im Jahr durchschnittliche Gesamtkosten von 1,25-2,5 Mrd. USD[9]. Sich vor DDoS-Angriffen zu schützen, ohne dass dabei die Performance leidet, ist ein Balanceakt.

Wie bereits erwähnt, versuchen viele Unternehmen, dieses Dilemma zu lösen, indem sie Datenverkehr zu in der Regel weit von der Traffic-Quelle oder dem Ursprungsserver entfernten Scrubbing-Zentren leiten. Dadurch entsteht ein Nadelöhr, das eine höhere Latenz zur Folge hat, die genauso negative Auswirkungen haben kann wie ein Angriff. Aufgrund der begrenzten Zahl an Scrubbing-Zentren ist es unrealistisch, auf diesem Weg DDoS-Angriffe abzuwehren. Darüber hinaus sollten Sie cloudbasierte Abwehrdienste in Betracht ziehen, die in jeder Weltregion in geringer Entfernung von der Angriffsquelle Bedrohungen aufspüren und bekämpfen können, weil sich dadurch die Reaktionszeit verkürzt.

5 ENTSCHEIDEN SIE SICH FÜR INTELLIGENTE LÖSUNGEN, UM DEN ANGREIFERN IMMER EINEN SCHRITT VORAUS ZU SEIN

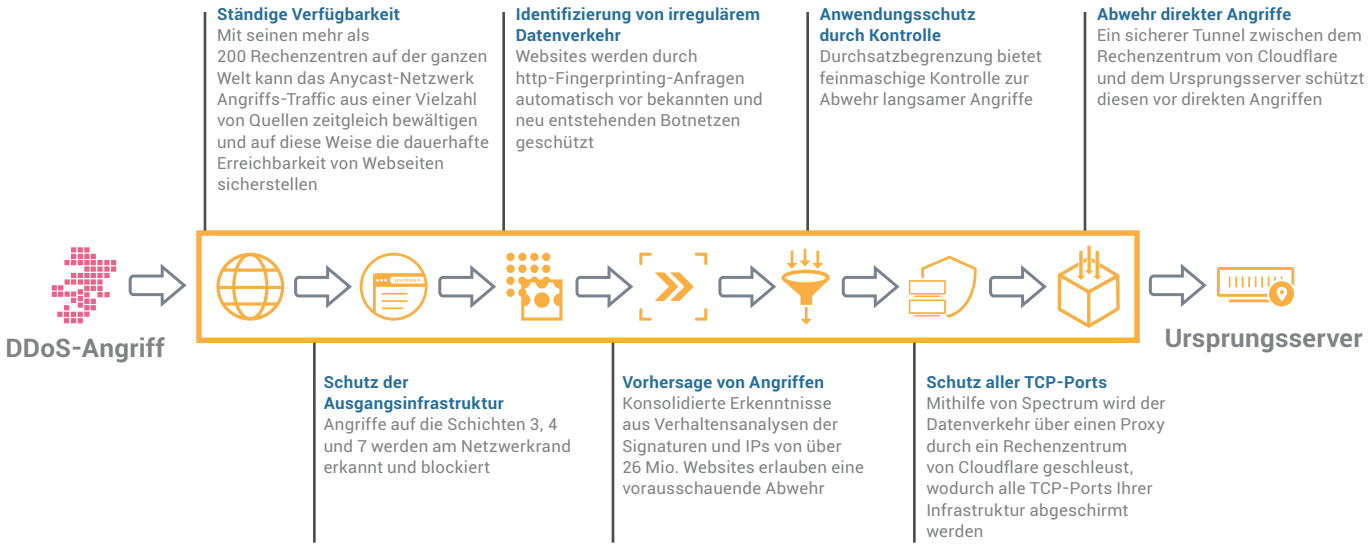
Mit einem mehrstufigen Ansatz allein kann man komplexer werdenden DDoS-Angriffen nicht Herr werden. Erforderlich ist vielmehr eine kontinuierliche Analyse des Datenverkehrs, um schädliche Muster zu erkennen und auf dieser Grundlage die für künftige Angriffe notwendigen smarten und anpassungsfähigen Abwehrmechanismen zu entwickeln.

Jeder DDoS-Angriff birgt immer auch die Chance, sich auf die nächste Attacke besser vorbereiten zu können. Bei der Bewertung cloudbasierter Abwehrlösungen sollte neben Übertragungs-, Filtergeschwindigkeit und Kapazität unbedingt auch die Art der durch seine Reichweite gewonnenen Informationen berücksichtigt werden. Je größer und robuster ein Abwehrnetzwerk ist, desto wertvollere Erkenntnisse kann es zu sich weiterentwickelnden Angriffsmustern liefern und umso besser kann es zur Vorbeugung beitragen.

Wie Cloudflare helfen kann

Der mehrstufige Sicherheitsansatz von Cloudflare fasst mehrere DDoS-Abwehrfunktionen in einem Dienst zusammen. Er verhindert durch illegitimen Datenverkehr verursachte Störungen, lässt aber unbedenklichen Traffic passieren. So bleiben Websites, Anwendungen, APIs und komplette Netzwerke einsatzbereit, in hohem Maße verfügbar und leistungsfähig.

Mit Rechenzentren in über 200 Städten und mehr als 90 Ländern sowie einer Netzwerkkapazität jenseits von 35 Tbps wehrt Cloudflare DDoS-Angriffe in der Nähe ihres Ausgangspunkts ab – in Industrieländern sind 99 % der Bevölkerung mit Internetzugang über unser Netzwerk binnen 100 Millisekunden erreichbar.



SCHNELLE UND AUTOMATISIERTE ABWEHR

Im Gegensatz zu herkömmlichen Lösungen, bei denen durch den Einsatz einer begrenzten Zahl an Scrubbing-Zentren Nadelöhre entstehen, hosten unsere Points of Presence weltweit Sicherheitsdienste zum Schutz vor DDoS-Angriffen unterschiedlichster Größe und Komplexität. Mit dieser Lösung sind wir unter anderem in der Lage, Datenverkehr so auf verschiedene Server zu verteilen, dass dieser von dem Netzwerk bewältigt werden kann.

BEDROHUNGSDATEN IN GLOBALEM MASSSTAB

Der DDoS-Schutz von Cloudflare beruht auf den Erkenntnissen aus unserem weltumspannenden Netzwerk, das mehr als 25 Mio. Webseiten schützt und Tag für Tag über 1 Mrd. Zugriffe von eindeutigen IP-Adressen bewältigt. Diese Informationen befähigen uns in einzigartiger Weise, die raffiniertesten Angriffe abzuwehren.

KOSTENWIRKSAMER SCHUTZ

Bei sämtlichen Optionen von Cloudflare ist ein uneingeschränkter und verbrauchsunabhängiger Schutz vor DDoS-Angriffen jeglichen Umfangs im Preis enthalten. Wir berechnen auch keine weiteren Gebühren für einen durch Angriffe verursachten sprunghaften Anstieg des Netzwerk-Traffics.

NUTZERFREUNDLICH UND LEICHT ZU VERWALTEN

Der cloudbasierte kontinuierliche Schutz von Cloudflare vor DDoS-Angriffen beruht auf einer intuitiv bedienbaren Benutzeroberfläche. Damit können Anwender mit wenigen Klicks Websites und Webapplikationen schnell und unkompliziert vor DDoS-Angriffen – unabhängig von ihrem Umfang und dem Grad ihrer Komplexität – schützen.

INTEGRIERTE SICHERHEIT UND PERFORMANCE

Unsere Schutzlösung ist darauf ausgelegt, sich nahtlos in die Web Application Firewall, das Bot Management, Magic Transit, den Load Balancer, das CDN und andere Sicherheits- und Performance-Angebote einzufügen, von diesen zu lernen und im Einklang mit ihnen zu arbeiten.

BEDARFSGERECHTE DATENANALYSE

Mit Cloudflare Analytics können Sie das integrierte Cloudflare Dashboard oder GraphQL zur Analyse von DDoS-Ereignissen einsetzen. Oder binden Sie die Cloudflare-Protokolldateien einfach in führende SIEM-Lösungen anderer Anbieter ein und gewährleisten Sie so eine nahtlose Integration in Ihre Geschäftsprozesse.

Fazit

Ein ganzheitlicher Ansatz, der sich sämtlicher Bedrohungen in allen Schichten annimmt, ist die Grundvoraussetzung für eine wirkungsvolle Strategie zur Bewältigung der mit DDoS-Angriffen einhergehenden Herausforderungen. Lokale Lösungen können zwar durchaus ihren Teil zur Sicherheit beitragen, werden allerdings unter Umständen schnell kostspielig. Robuster ist eine skalierbare und cloudbasierte Abwehrlösung, die Dienste am Netzwerkrand abdeckt, größtmögliche Flexibilität bietet, mit unbegrenzten Kapazitäten aufwartet und dabei auch die Performance berücksichtigt. Sie gewährleistet, dass das System jeder DDoS-Attacke – sei sie auch noch so mächtig oder komplex – gewachsen ist.

Endnoten

1 Kaspersky Labs, „DDoS Breach Costs Rise to Over $2M for Enterprises Finds Kaspersky Lab Report“, Kaspersky Labs, 22. Februar 2018

2 Crane, Casey, „The 15 Top DDoS Statistics You Should Know in 2020“, Cybercrime Magazine, 16. November 2019

3 DeNisco Rayome, Alison, „Major DDoS attacks increased 967% this year“, TechRepublic, 24. April 2019

4 Avital, Nadav, „2019 Global DDoS Threat Landscape Report“, Security Boulevard, 5. Februar 2020

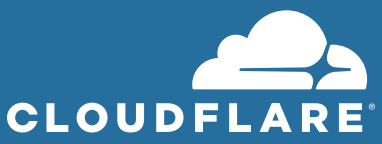
5 Cook, Sam, „DDoS attack statistics and facts for 2018-2019“, Comparitech, 20. August 2019

6 Ebd.

7 Stein, Jake, „Behind the Buzzword: The Reality of Real Time“, InformationWeek, 5. September 2019

8 Tyson, Mark, „Users Lose a Full Working Week Every Year Due to Slow Computers“, Hexus.net, Oktober 2013

9 „IDC Study - The cost of downtime“, Tech Republic, 30. September 2017



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV: 200330