DDoS im kontinuierlichen Wandel – wie man der Gefahr entgegentreten kann

CLOUDFLARE®

Das erste Mal, dass ein Dienst gezielt außer Gefecht gesetzt wurde, war im Jahr 1974. Damals führte ein neugieriger Schüler ein Software-Experiment durch, um einem Raum voller Anwender einen Computer-Anmeldezugriff zu verweigern. Aus diesem kleinen Experiment ist inzwischen ein regelrechtes Cybermonster geworden, das sich mit der Zeit stark weiterentwickelt hat. In den letzten zehn Jahren sind beispielsweise Auftrags-DDoS-Websites entstanden, die Profis und Laien DDoS-Angriffe als Dienstleistung bereitstellen.

Die drei Waffen von DDoS: Größe, Multi-Vektoren-Angriffe und Allgegenwart

1. GRÖSSE

Im Jahr 2016 sorgte ein von einem **Mirai-Botnet ausgeführter DDoS-Angriff** für Aufsehen: OVH, einer der größten Hosting-Dienstleister Europas, wurde durch eine gewaltige volumetrische DDoS-Attacke zum Absturz gebracht. Der Angriff, der mithilfe von 145.000 IoT-Geräten ausgeführt wurde, erreichte laut Berechnungen von OVH zum Höhepunkt eine Größe von 1 Tbps.

2018 wurde dann **GitHub** zum Opfer einer der größten jemals verzeichneten volumetrischen DDoS-Attacken mit einem Umfang von 1,35 Tbps. Zum Einsatz kam dabei ein obskurer Amplification-Angriffsvektor: das **Memcached**-Protokoll, das den UDP-Port 11211 nutzt.

Mächtige Angriffe wie dieser haben zwar durchschlagende Wirkung, doch es ist auch kostspielig, zur Bindung sämtlicher Ressourcen des Opfers große Traffic-Mengen zu generieren. Aus diesem Grund liegen inzwischen sogenannte „Burst Attacks" im Trend. Dabei handelt es sich um vergleichsweise große, aber kürzere Angriffe. Diese sorgen zwar für eine Überlastung der anvisierten Website, werden aufgrund ihrer geringen Dauer unter Umständen von automatisierten Systemen aber nicht registriert.

2. MULTI-VEKTOREN-ANGRIFFE

Die Taktik bei DDoS-Attacken besteht wie bei anderen Angriffen auf Sicherheitssysteme häufig darin, Schwachstellen in den Kommunikationsprozessen von Protokollen auszunutzen. Auf Ebene des TCP-Protokolls beispielsweise kann ein DDoS-Angriff mittels SYN- oder ACK-Flood für eine Überlastung der Server-Ressourcen sorgen. Weil zahlreiche Protokolle – darunter UDP oder ICMP – solche Achillesfersen aufweisen, steht für die Ausführung von DDoS-Angriffen ein ganzes Arsenal an Strategien zur Verfügung.

Wikipedia etwa hat im September 2019 für ungefähr neun Stunden erhebliche Einschränkungen bei den weltweiten Nutzerzugriffen auf die eigenen Websites verzeichnet. Betroffen waren nicht nur die Verfügbarkeit und Performance der Web-Anwendung in der HTTP-Server-Schicht: Auch die Rechenzentren der Online-Enzyklopädie standen auf Ebene der Netzwerkschicht im Visier der Angreifer. Die Offensive, die einen ACK- mit einem UDP-Flood-Angriff kombinierte, erreichte Erhebungen zufolge einen Umfang von mehr als 250 Gbps.

3. ALLGEGENWART

In der heutigen Zeit sind DDoS-Angriffe für Organisationen und Unternehmen trauriger Alltag. Besonders in größeren Volkswirtschaften wie den Vereinigten Staaten sind Firmen lukrative Ziele für Angreifer, die Böses im Schilde führen. Doch tatsächlich verzeichnen Unternehmen in allen Teilen der Welt und aus allen Branchen raffinierte DDoS-Attacken. Im Jahr 2019 waren in Südafrika Banken Ziel lang anhaltender DDoS-Angriffe, die von Lösegeldforderungen begleitet wurden. Inländische Telekommunikationsunternehmen wie Liquid Telecom mussten sich gegen gewaltige DDoS-Attacken von mehr als 100 Gbps zur Wehr setzen.

„Böswillige Akteure loten permanent neue Wege und Taktiken zur Durchführung weiterentwickelter DDoS-Angriffe aus."

DDoS-Angreifer werden immer gieriger

Anfang 2020 haben sich DDoS-Angriffe rasch ausgebreitet. Das Massively Multiplayer Online (MMO)-Spiel EVE Online wurde durch eine DDoS-Attacke mehrere Tage lahmgelegt. Die Online-Foren des Anbieters wurden von entnervten Spielern überrannt, die ihre Konten kündigen wollten oder Entschädigungen verlangten, weil sie sich tagelang nicht einloggen konnten. Bei MMO-Spielen ist schon eine geringfügig verlängerte Reaktionszeit für die Anwender äußerst frustrierend, von einer mehrere Tage dauernden Unterbrechung ganz zu schweigen.

Kriminelle sind ständig auf der Suche nach neuen Mitteln und Wegen zur Weiterentwicklung von DDoS-Angriffen. Gerade suchen zum Beispiel Hacker das Internet nach NSC Linear eMerge E3-Geräten mit der Sicherheitslücke CVE-2019-7256 ab. Diese Schwachstelle erlaubt es ihnen, die Kontrolle über Geräte zu übernehmen, Schadsoftware herunterzuladen und zu installieren und anschließend DDoS-Angriffe auf andere Ziele auszuführen. Solche Geräte werden normalerweise in Unternehmen, Fabriken und vergleichbaren Infrastrukturen für die Zugangskontrolle von Angestellten und Besuchern eingesetzt.

Die DDoS-Bedrohung in der Cloud bezwingen

Traditionell wurden für die DDoS-Abwehr lokale Hardware Appliances eingesetzt. Dieser Ansatz ist inzwischen jedoch überholt, weil die Angriffe heute größer, komplexer und global ausgerichtet sind. Dem Ausmaß, der Geschwindigkeit und dem Verteilungsgrad solcher Angriffe sind lokale DDoS-Lösungen schlicht nicht gewachsen.

Cloudbasierte Lösungen nutzen hingegen ein verteiltes System. Dadurch sind sie in der Lage, rund um den Globus einen ständig aktiven Schutz vor DDoS-Angriffen zu bieten. Bei der Auswahl einer cloudbasierten Lösung zur Abwehr von DDoS-Angriffen sind folgende Aspekte ausschlaggebend:

VERTEILTE ARCHITEKTUR

Um der globalen Dimension von DDoS-Angriffen gerecht werden zu können, benötigen Schutzlösungen eine global verteilte Architektur. Auf diese Weise sind sie in der Lage, die Attacken in größtmöglicher Nähe zu ihrem Ursprung abzuwehren. Klassischerweise setzen cloudbasierte DDoS-Lösungen auf Scrubbing-Zentren. Doch wegen der zunehmenden Größe von DDoS-Angriffen hat dieser Ansatz inzwischen ausgesorgt, weil dadurch ein Nadelöhr geschaffen wird. Traditionell investieren Anbieter von DDoS-Lösungen in eine kleine Zahl solcher Zentren, zu denen große DDoS-Angriffe umgeleitet werden müssen, weil sie nicht über ein echtes verteiltes System verfügen.

Mehr über die Schwächen der Scrubbing-Zentren-Strategie erfahren Sie in dem informativen Blogbeitrag „**No scrubs**“ (in englischer Sprache).

Die moderne Lösung von Cloudflare zur Bekämpfung von DDoS-Angriffen läuft als Dienst auf sämtlichen Servern in allen Rechenzentren der 200 Städte unseres globalen Netzwerks. Das macht sie zu einem echten verteilten System. Wenn irgendwo auf der Welt ein DDoS-Angriff gestartet wird, übernimmt das nächstgelegene Rechenzentrum von Cloudflare die Verteidigung. Dadurch kann die Attacke schneller abgewehrt und die Verfügbarkeit der Infrastruktur des Kunden erhöht werden.

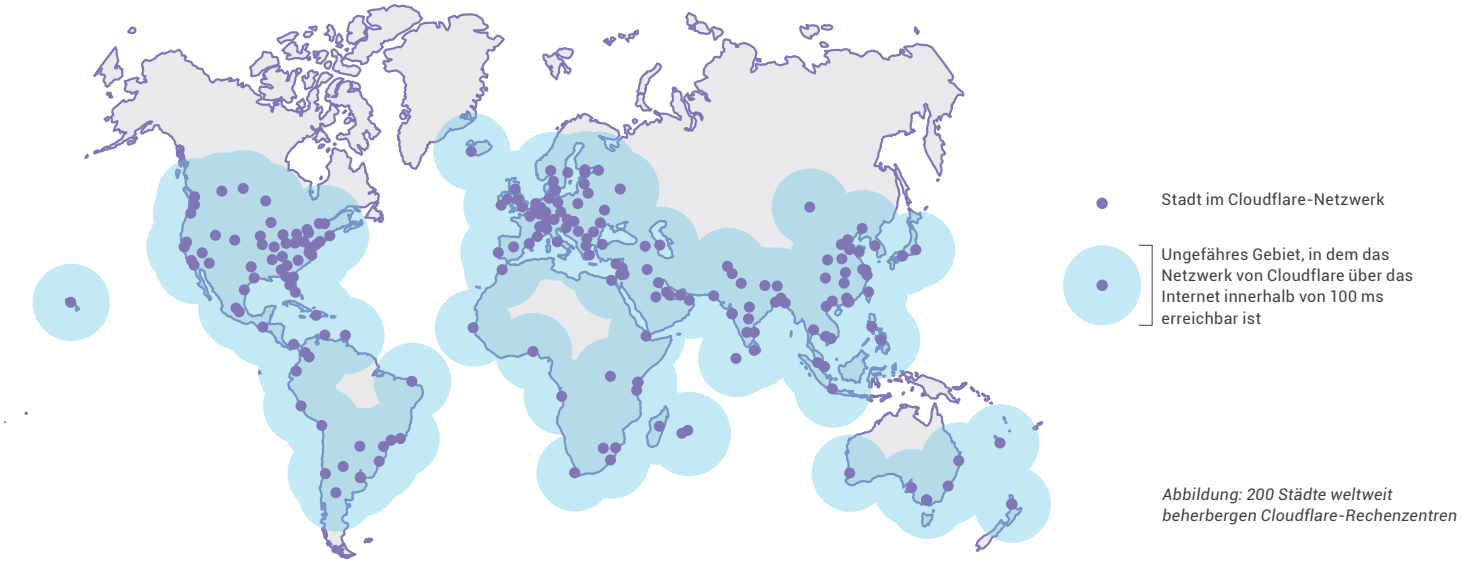


Abbildung: 200 Städte weltweit beherbergen Cloudflare-Rechenzentren

NETZWERKKAPAZITÄT

Damit eine Abwehrlösung dem Maßstab und der Größe eines DDoS-Angriffs gerecht werden kann, kommt es auf die ihr zur Verfügung stehende Netzwerkkapazität an. Das gilt insbesondere für DDoS-Attacken, die sich im Tbps-Bereich bewegen.

Das globale Anycast-Netzwerk von Cloudflare wartet mit einer Kapazität von mehr als 30 Tbps auf und ist damit selbst den mächtigsten DDoS-Angriffen gewachsen. Zudem ist Cloudflare mit mehr Internet-Knoten vernetzt als andere Anbieter auf der Welt: Das System ist mit mehr als 8.000 anderen Netzwerken rund um den Globus verbunden, darunter großen ISPs, Cloud-Diensten und Unternehmen.

RUNDUMSCHUTZ

Böswilligen Akteuren steht ein ganzes taktisches Arsenal für die Ausführung von DDoS-Angriffen in den Anwendungs- und Netzwerkschichten zur Verfügung. Cloudbasierte DDoS-Lösungen sollten in der Lage sein, Attacken umfassend in mehreren Schichten abzuwehren.

Die ausgefeile Anti-DDoS-Lösung von Cloudflare bietet einen Rundumschutz vor DDoS-Angriffen auf Layer 7. Cloudflare Spectrum und Magic Transit übernehmen die Abwehr auf Layer 3 und 4. ThousandEyes analysiert in einem **Blogbeitrag** den DDoS-Angriff auf Wikipedia. Darin wird herausgearbeitet, wie es Cloudflare gelungen ist, eine große Multi-Vektoren-Attacke schnell und umfassend zu neutralisieren.

ECHTZEITINFORMATIONEN

DDoS-Lösungen sollten mit Echtzeitinformationen untermauert werden, damit sie im Kampf gegen DDoS-Angriffe nicht nur reagieren, sondern selbst aktiv werden können.

Die Abwehrlösung von Cloudflare für DDoS-Angriffe beruht auf Bedrohungsinformationen, die von einem ständig dazulernenden Netzwerk erhoben werden. Dieses schützt über 20 Mio. Internetwebsites und prüft täglich Anfragen von mehr als 1 Mrd. eindeutigen IP-Adressen. Dank dieser Erkenntnisse, auf Machine Learning basierender Modelle und des technischen Know-how eines kampferprobten Teams stellt der DDoS-Schutz von Cloudflare eine robuste Lösung für die ausgefeiltesten DDoS-Angriffe bereit.

AUTOMATISIERTER SCHUTZ

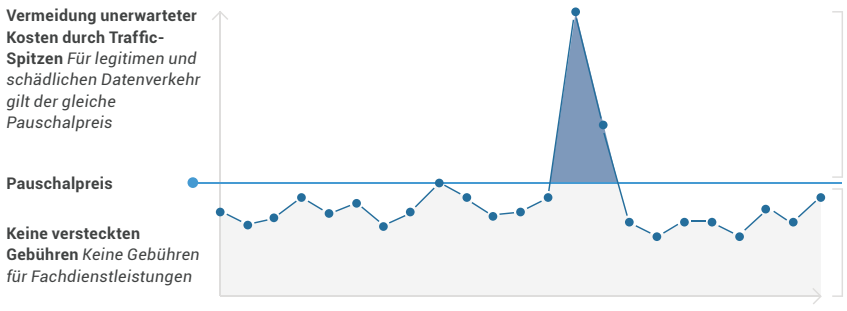
Raffinierte DDoS-Attacken erfordern eine automatisierte Abwehr, die kontinuierlich (vor Ort oder in der Cloud) den für ein Unternehmen bestimmten Traffic prüft, Echtzeitanalysen durchführt und die Bedrohung schnell bekämpft.

Die automatisierten Systeme von Cloudflare (**Gatebot** und **DosD**) analysieren laufend Fingerprints von Angriffen, Anomalien, Regeln, Blacklists und vieles mehr. Das Gatebot-System dient zur Abschirmung vor globalen volumetrischen Angriffen, während DosD auf jedem Server läuft, um lokal begrenzte Attacken zu blockieren. Um eine schnelle Gefahrenabwehr sicherzustellen, empfehlen diese automatisierten Systeme gemeinsam über 400.000 dynamische Regeln pro Sekunde.

KOSTENEFFIZIENZ

Angesichts der zunehmenden Größe und des wachsenden Ausmaßes von DDoS-Angriffen müssen sich alle Unternehmen und Organisation bewusst machen, dass sich die Investition in DDoS-Schutz auszahlt. Bei cloudbasierten Anti-DDoS-Lösungen wird für die Abrechnung häufig ein nutzungsabhängiges Modell genutzt. Cloudbasierte Angebote bieten einen höheren Schutz als lokale Lösungen, da sie sich flexibel an den Umfang einer DDoS-Attacke anpassen. Doch eine nutzungsabhängige Regelung geht oft mit einer gesalzenen Rechnung einher. Unternehmen erleiden dann zwar keine Einnahmeeinbußen durch den Ausfall ihrer Dienste, müssen aber stattdessen unter Umständen horrende Kosten für einen nutzungsabhängigen DDoS-Schutz schultern.

Cloudflare bietet einen **zeitlich unbegrenzten Rundumschutz** vor DDoS-Angriffen. Damit verliert das alte Modell des „Surge Pricing", bei dem die höhere Beanspruchung des Abwehrdiensts bei Angriffen in Rechnung gestellt wird, seine Berechtigung. Diese Praxis ist für ein Unternehmen besonders belastend, wenn es sich durch einen DDoS-Angriff ohnehin gerade in einer Notsituation befindet. Mit unserer Lösung vermeiden Sie dagegen unvorhergesehe Kosten durch Traffic-Spitzen.



Seien Sie ein Held – **schlagen Sie DDoS-Angreifer in die Flucht!**

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