DDoS-Schutz mit Cloudflare

Die Evolution moderner DDoS-Angriffe

2016
1 Tbit/s
IoT-Botnet Schicht 7 – Angriff

Größter Angriff auf Schicht 7 mit Mirai-IoT-Botnet. Angriff sowohl volumetrisch als auch über Serverressourcen.

2014
400 Gbit/s
NTP-Verstärkung – Angriff

Angreifer nutzt 4.529 NTP-Server zur Verstärkung eines Angriffs von einem Quellserver mit gerade einmal 87 Mbit/s

2013
120 Gbit/s
Schicht 3/4 – DDoS-Angriff

Spamhaus-Angriff als zu dieser Zeit größter Angriff mit dem Titel „Angriff, der fast das Internet kaputtmachte“.

DDoS-Angriffe (Distributed Denial of Service – verteilte Dienstblockade) treten vermehrt auf und stellen mittlerweile eine komplexe und überwältigende Sicherheitsherausforderung für Organisationen dar. DDoS-Angriffe sind nichts Neues, doch die Methoden und Ressourcen zum Durchführen und Vertuschen solcher Angriffe haben sich dramatisch entwickelt. Ein Meilenstein bei der Evolution der DDoS-Angriffe war die Bildung des Mirai-Botnets, das aus über 300.000 gehackten IoT-Geräten bestand. Mit diesen wurde der bisher größte bekannte DDoS-Angriff durchgeführt. Seine Spitzenbelastung während des Angriffs lag bei einem Durchsatz von über 1 Tbit/s. Angriffe von diesem Ausmaß werden zum neuen Standard.

DDoS-Angriffe finden oft nicht nur einmal statt und auf die Opfer wird mehrmals pro Jahr abgezielt. Nach der Erfahrung von Cloudflare können sowohl kleine als auch große Organisationen diesen Angriffen zum Opfer fallen. Zwar gibt es in vielen Rechtssystemen Gesetze gegen DDoS-Angriffe, dennoch existieren Anbieter für DDoS-as-a-Service mit Abonnements schon ab 5 oder 10 US-Dollar/Monat.

Umsatzverlust ist nur eines der Risiken, die solche Angriffe für Ihre Website oder Ihr Unternehmen mit sich bringen. Selbst die Amazon-Website (99 Milliarden US-Dollar Umsatz 2015) ist in der Vergangenheit mehrmals aus unbekannten Gründen ausgefallen. 2013 ist Amazon.com zum Beispiel für geschätzte 15–45 Minuten ausgefallen, was das Unternehmen 1,8–5,3 Millionen US-Dollar an Abschlüssen kostete (berechnet auf Basis des durchschnittlichen Verkaufsumsatzes des Unternehmens von 117.882 US-Dollar pro Minute). Außerdem bringt ein fehlender Zugang weitere, weniger messbare Nachteile mit sich wie Markendegradierung und verminderte Kundenzufriedenheit.

Skalierbare und präzise DDoS-Lösung

Ein globales Anycast™-Netzwerk von Cloudflare mit 10 Tbit/s ist 10 x größer als der größte verzeichnete DDoS-Angriff. So halten alle Internetassets auf dem Netzwerk von Cloudflare massiven modernen DDoS-Angriffen stand. Der DDoS-Schutz von Cloudflare für die Schichten 3, 4 und 7 ist als Service am Netzwerkrand verfügbar, entspricht der Größe moderner Bedrohungen und kann zur Minderung von DDoS-Angriffen aller Arten und Größen verwendet werden. Durch die Ratenbegrenzung wird der DDoS-Schutz von Cloudflare erweitert, indem eine präzise Minderung der fortschrittlichsten Angriffe auf die Anwendungsschicht ermöglicht wird.

SCHUTZ GEGEN DDOS-ANGRIFFE AUF SCHICHTEN 3 UND 4

Bei DDoS-Angriffen auf die Schichten 3 und 4 handelt es sich für gewöhnlich um volumetrische Angriffe wie DDoS-Verstärkung, DDoS-Flood und DDOS-SYN-Flood. Solche Angriffe können ein herkömmliches Unicast-basiertes Netzwerk überwältigen. Das Anycast-basierte Netzwerk von Cloudflare hingegen vergrößert automatisch die Oberfläche durch eine Verteilung des Verkehrs während des Angriffs auf über 102 Cloudflare-Rechenzentren und ein vielfältiges Set an Querverbindungen mit hoher Bandbreite zu anderen Netzwerken. So wird die Belastung während des Angriffs regelrecht geschluckt.

DDoS-Schutzfunktionen

- Schichten 3, 4 und 7 – DDoS-Schutz
- DNS-Angriffsschutz
- Mikrobedrohungsschutz durch Ratenbegrenzung
- Vorausschauende Sicherheit mit IP-Reputationsdatenbank

„Da wir uns nun keine Sorgen mehr um DDoS-Angriffe auf unsere API- und Gateway-Server machen müssen, können wir uns auf die Optimierung unseres Produkts konzentrieren."

– Jake Heinz,
Software Engineer bei Discord

Das Cloudflare-Netzwerk

- Globales Anycast™-Netzwerk aus über 102 Rechenzentren
- Durchsatz von 10 Tbit/s gegen volumetrische Angriffe
- 6 Millionen Internetobjekte
- Bandbreiten-Flatrate

„Wir verwenden Cloudflare aufgrund der exzellenten Sicherheitsfunktionen, des Hochleistungs-CDNs und der äußerst praktischen Bündelung der Lösungen. So ist die Verwaltung ein Kinderspiel und wir können uns auf unser Kerngeschäft konzentrieren."

– Amanda Kleha,
GM der Zendesk Online-Geschäftseinheit

SCHUTZ GEGEN DDOS-ANGRIFFE AUF ANWENDUNGSSCHWACHSTELLEN IN SCHICHT 7

Herkömmliche Angriffe auf Schicht 7 sind unter anderem SQL-Einschleusung und Cross-Site-Scripting (XSS). Dadurch erhalten Angreifer unter Umständen Zugriff auf Kunden- sowie andere Anwendungsdaten und können diese manipulieren. Cloudflare verhindert diese Bedrohungen durch die Web Application Firewall (WAF). Die WAF blockiert Bedrohungen aus dem OWASP Top 10-Regelsatz, den Anwendungsregelsätzen von Cloudflare sowie aus benutzerdefinierten, von der Community oder Kunden erstellten Regeln automatisch. Cloudflare schützt Kunden vor großen Zero-Day-Schwachstellen, inklusive der Shellshock-Schwachstelle und dem Heartbleed-Bug.

RATENBEGRENZUNG

Die aktivierte Ratenbegrenzung von Cloudflare ermöglicht eine Verkehrsmikrosteuerung, die den DDoS-Schutz sowie die WAF-Services von Cloudflare erweitert. Sie schützt vor Denial-of-Service-Angriffen, Brute-Force-Passwort-Angriffen und anderen missbräuchlichen Verhaltensweisen, die auf die Anwendungsschicht abzielen.
Sie können Anforderungsschwellenwerte konfigurieren, benutzerdefinierte Reaktionen wie Minderungsaktionen (Aufgaben oder CAPTCHAs) oder Reaktionscodes definieren und analytische Einblicke in Endpunkte Ihrer Website, Anwendung oder API gewinnen.

Vorausschauende Sicherheit

Cloudflare bietet eine automatische Lernplattform, mit der der Netzwerkverkehr in Echtzeit analysiert wird. So werden anomale und schädliche Anforderungen erkannt. Wird ein Angriff einmal erkannt, blockt Cloudflare diese Angriffsart ab diesem Zeitpunkt automatisch sowohl für die bestimmte Website als auch die gesamte Community.
Das Cloudflare-Netzwerk und die Community wachsen stetig und so wird es immer schwieriger, effektive DDoS-Angriffe auf Cloudflare-Benutzer durchzuführen.

Bandbreiten-Flatrate

Cloudflare bietet unbegrenzten Enterprise-DDoS-Schutz zu einer monatlichen Flatrate. Wir sind der Meinung, dass Kunden nicht für einen Anstieg des Netzwerkverkehrs während eines DDoS-Angriffs bestraft werden dürfen. Mit dem DDoS-Schutz von Cloudflare können Sie sicher sein, dass Ihre Website online bleibt und Ihre monatliche Abrechnung nicht schwankt.

Cloudflare-Registrierung

Registrieren Sie sich bei Cloudflare und aktivieren Sie die Ratenbegrenzung zum Schutz Ihrer Website, Anwendung oder API vor DDoS-Angriffen. Gleichzeitig reduzieren Sie so die Latenz und können sicher sein, stets aktuelle Web-Technologien zu verwenden. Die Registrierung dauert in der Regel weniger als 5 Minuten. Die Tarife von „Kostenlos" bis „Enterprise" finden Sie unter www.cloudflare.com.