Fünf Fragen zu Ihrem DDoS-Abwehrdienstleister

Die Häufigkeit und Komplexität von DDoS-Angriffen nimmt zu. Wenn Sie Ihre Netzwerke und Nutzer schützen wollen, müssen Sie sich für den richtigen DDoS-Abwehrdienst entscheiden. Aber nicht alle Anbieter sind gleich. Treffen Sie die falsche Wahl, kann Ihnen das unerwartetes Kopfzerbrechen, Performance-Probleme und Ausfälle bescheren.

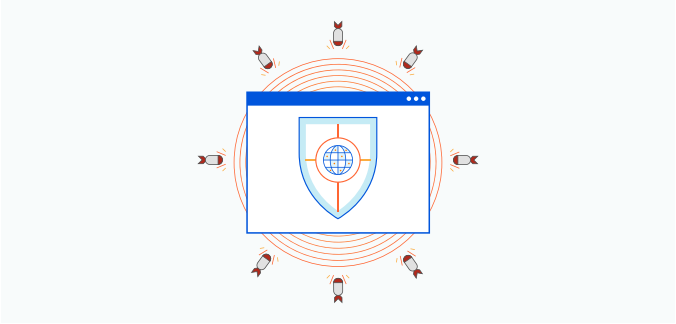
Die folgenden fünf Fragen sollten Sie sich bei der Beurteilung von DDoS-Abwehrdiensten stellen:

1. Ist der Dienst cloudnativ?

Ein effektiver DDoS-Abwehrdienst muss cloudnativ sein – es sollte sich nicht um On Premise-Technologie handeln, die virtualisiert wurde und in Cloud-Rechenzentren gehostet wird. Worin besteht der Unterschied? Cloudnative Abwehrdienste können skaliert werden und lassen sich so den Anforderungen Ihres Unternehmens reibungslos anpassen. Sie verursachen keine künstlichen Engpässe bei der Performance, wohingegen die Verwaltung virtueller und in der Cloud gehosteter Anwendungen immer noch genau so kompliziert ist wie bei lokaler Hardware.

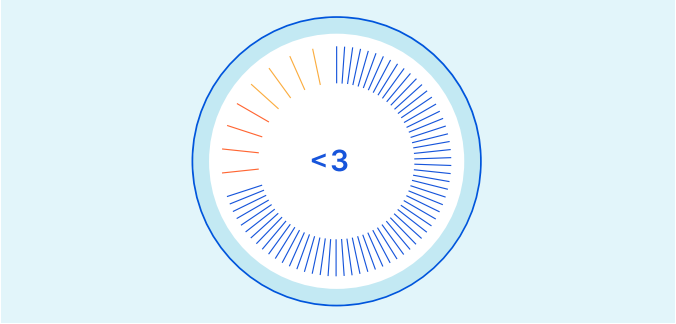
2. Wie viel Netzwerkkapazität bietet der Provider?

Groß angelegte DDoS-Angriffe (wie die 2,3 Tbit/s-Attacke gegen einen AWS-Kunden im Jahr 2020) überfordern durch ihren Traffic Service-Provider mit unzureichender Netzwerkkapazität. Für diese Größenordnungen benötigen Sie einen Anbieter, der über genügend Netzwerkkapazität verfügt, um Angriffe ohne Ausfallzeiten oder Performance-Einbußen abzuwehren.



3. Wie schnell kann der Dienst DDoS-Angriffe erkennen und darauf reagieren?

Im Fall eines Angriffs ist eine kurze Abwehrzeit (also die Zeit, die benötigt wird, um Angriffe zu erkennen und zu bekämpfen) entscheidend. Überschreitet die Ausfallzeit ein paar Sekunden, kann dies unwiderruflichen Schaden anrichten: sowohl im Hinblick auf die Erfahrung der Kunden, als auch was den Ruf Ihrer Marke und Ihre Umsätze angeht.



4. Ist der Dienst in jedem Rechenzentrum verfügbar?

Wenn die DDoS-Bereinigungsfunktionen nicht in jedem Rechenzentrum verfügbar sind, muss Ihr Traffic einen Umweg über spezielle „Scrubbing-Zentren“ nehmen. Das führt oft zu zusätzlicher Latenz und beeinträchtigt die Performance der Anwendung. Wählen Sie daher einen Provider, der in jedem Rechenzentrum Abwehrdienste anbietet und so dafür sorgen kann, dass Ihr Traffic der optimalen Route folgt.

5. Handelt es sich um einen automatisierten Dienst?

Ein solider DDoS-Abwehrdienst sollte Automatisierung und Self Service über ein Dashboard oder eine API ermöglichen, damit Sie Ihren Bedrohungsschutz schnell aktivieren und verwalten können. Suchen Sie nach einem Anbieter, der gut erreichbar ist, schnell reagiert und Bedrohungen proaktiv aufspürt und bekämpft, ohne bei Ihren Diensten zusätzliche Ausfallzeiten zu verursachen.

Cloudflare Magic Transit schützt ganze IP-Subnetze vor DDoS-Angriffen und beschleunigt gleichzeitig den Netzwerk-Traffic. Das globale Netzwerk von Cloudflare mit Rechenzentren an mehr als 200 Standorten blockiert durchschnittlich 70 Milliarden Bedrohungen am Tag und hat bereits einige der größten DDoS-Angriffe der Geschichte bewältigt.

Testen Sie Magic Transit und fordern Sie noch heute eine kostenlose Demo an.