Können DDoS-Angriffe in null Sekunden gestoppt werden?

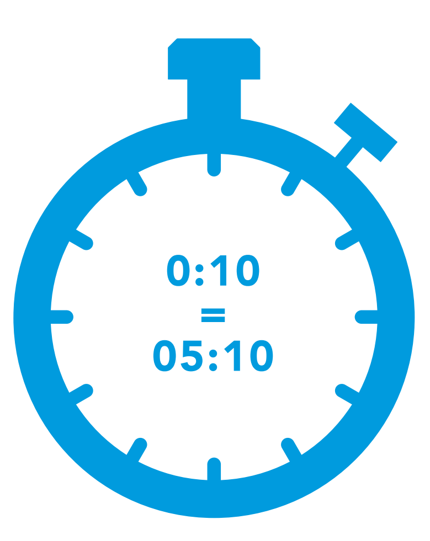
EINE KLARSTELLUNG ZUR ABWEHRZEIT

Die Abwehrzeit sollte genau definiert sein, oder nicht? Die Zeitspanne zwischen dem Beginn eines DDoS-Angriffs und dem Zeitpunkt, zu dem Ihre Assets oder Anwendungen geschützt sind.

Doch das ist nicht das, was in den Service-Level Agreements (SLAs) der einzelnen Anbieter wirklich enthalten ist. Sie müssen genau hinschauen, wann die Uhr zu laufen beginnt und wann sie angehalten wird.

VORSICHT BEI DIESEN GÄNGIGEN SZENARIEN VON ANBIETERN

ANBIETER A



Anbieter A sieht vor, dass die Schutzmechanismen einen Anstieg des Traffics über einen Zeitraum von mehr als 5 Minuten analysieren müssen, bevor ein DDoS-Angriff bestätigt wird.

Die im SLA festgelegte Abwehrzeit von 10 Sekunden beginnt erst nach Bestätigung des Angriffs.

ANBIETER B

In den AGB von Anbieter B ist die Abwehrzeit als die Bereitstellungszeit für einen Schutzmechanismus definiert – eine Reaktion.

Ein SLA, in dem die Beendigung des Angriffs verbindlich festgeschrieben ist, liegt nicht vor.

ANBIETER C

Anbieter C verpflichtet sich in seinem Abwehrzeit-SLA zur automatischen Erkennung und Abwehr.

Manuelle, individuell angepasste Verteidigungstechniken zur Abwehr ausgeklügelter Angriffe sucht man in diesem SLA vergebens.

DAS KLEINGEDRUCKTE VERSTEHEN

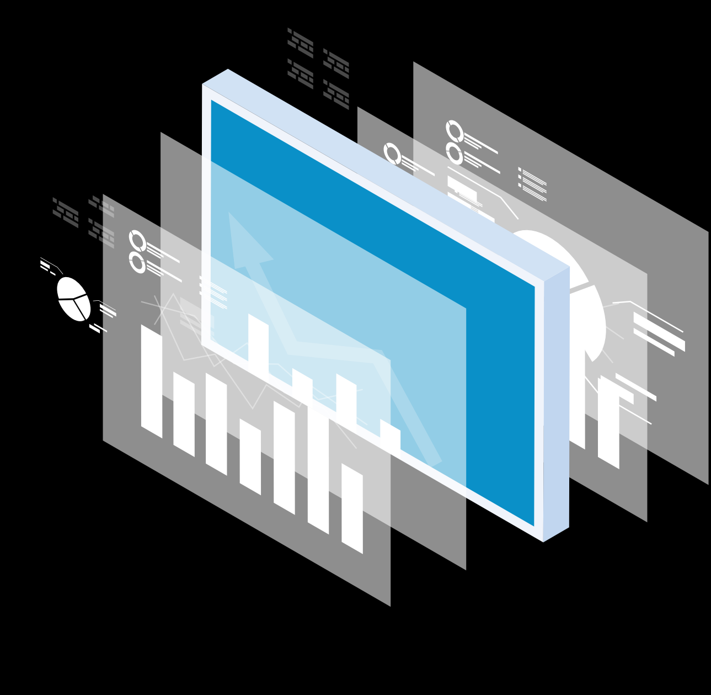
Seien Sie **skeptisch** bei Formulierungen wie:

… Reaktionszeit …

Im Falle eines anhaltenden DDoS-Angriffs …

… nach der Erkennung …

ABWEHRZEIT VON AKAMAI



Wenn **null auch wirklich null** Sekunden bedeutet

Unsere proaktiven Schutzmechanismen sind darauf ausgelegt, DDoS-Angriffe abzuwehren und Sie zu schützen, bevor Sie überhaupt bemerken, dass Sie angegriffen wurden. Das ist die Leistungsfähigkeit, über die Sie mit der Akamai Intelligent Edge Platform verfügen.

ZEIT ZUR **Erkennung von Angriffen** + ZEIT ZUR **Anwendung von Abwehrmaßnahmen** + ZEIT ZUM **Blockieren von Angriffen** = **Branchenführende Abwehrzeit**

8 SCHRITTE ZUR DDOS-ABWEHR

Die Abwehrzeit von Akamai ist die kürzeste in der Branche. Dafür sorgt eine leistungsstarke Kombination aus Bedrohungsforschern, Ereignismanagern, Sicherheitsarchitekten und modernsten Verteidigungstechnologien. Das Security Operations Command Center (SOCC) von Akamai führt die folgenden Schritte aus:

1. **Erkennung** von Angriffen zu einem frühen Zeitpunkt dank der durchgehenden DDoS-Überwachung.
2. **Benachrichtigung** des Kunden unter Verwendung des bestehenden Runbooks.
3. **Management** des Kundentraffics mit dem ständig verfügbaren, vereinfachten Routing.
4. **Analyse** des Traffics und Identifizierung der Vektoren, um die Abwehrmaßnahmen zu starten.
5. **Nachjustieren** der angewandten Abwehrmaßnahmen, um zwischen False Positives und False Negatives zu optimieren.
6. **Identifizieren** neuer Angriffsvektoren.
7. **Analyse** des Traffics und Identifizierung neuer Vektoren für kontinuierliche Abwehrmaßnahmen.
8. **Optimierung** der laufenden Abwehrmaßnahmen zur Neutralisierung sich ändernder Angriffe.

DIE RISIKEN EINER VERZÖGERTEN ABWEHRZEIT

Welche **Folgen** haben Ausfallzeiten?

0:01

Nach 1 Sekunde sind Ihre Web-Assets oder -Anwendungen nicht mehr verfügbar.

0:10

Nach 10 Sekunden nimmt die Frustration auf Kundenseite zu und die Produktivität der Mitarbeiter verringert sich.

05:00

Schon nach 5 Minuten nimmt der Ruf Ihrer Marke Schaden und Sie verlieren Umsätze.

BEWERTEN SIE IHRE DDOS-ABSICHERUNG

Wie schnell kann Ihr Anbieter einen Angriff erkennen?

Wären Ihre kritischen Anwendungen verfügbar?

Würden Sie von Kollateralschäden betroffen sein?

Wären legitime Nutzer betroffen?

Wie schnell kann Ihr Anbieter Gegenmaßnahmen ergreifen?

Wie schnell kann Ihr Anbieter mit der Analyse des Traffics beginnen?

AKAMAI THREAT INSIGHTS

Umfangreicher, **komplexer** und **gefährlicher**

Der Umfang von DDoS-Angriffen erreicht Rekordniveau. Im Jahr 2020 haben wir eine Zunahme des Umfangs und der Komplexität der DDoS-Aktivitäten beobachtet. Die Anzahl und die Kombinationen der Angriffsvektoren sind beispiellos.

18. FEB. 2018	16. JUNI 2020	21. JUNI 2020
1,3 Tbit/s (Terabit pro Sekunde)	**1,44 Tbit/s / 385 Mpps** (Millionen Pakete pro Sekunde)	**809 Mpps** (Millionen Pakete pro Sekunde)
Dieser Angriff war doppelt so umfangreich wie der zuvor größte Angriff. Dabei wurde ein neuer DDoS-Reflection-Angriffsvektor verwendet – UDP-basierter Memcached-Traffic.	Dieser Angriff nutzte neun verschiedene Vektoren und diverse Botnet-Angriffstools. Er dauerte fast 2 Stunden an und erreichte eine Geschwindigkeit von 1,3 Tbit/s.	Dies war der größte Angriff bezüglich der Pakete pro Sekunde, der jemals auf der Akamai Intelligent Edge Platform registriert wurde. Dabei kam eine große Anzahl global verteilter und zuvor nicht erfasster Quell-IPs zum Einsatz, die auf ein neues Botnet hindeuten.

Eine wirksame Verteidigung erfordert die Kombination aus einer erprobten Plattform, erfahrenen Fachleuten und ausgefeilten Prozessen und Techniken.

Die **Abwehrzeit** sollte der Zeitraum sein, in dem schädlicher Traffic erkannt und blockiert wird, ohne den legitimen Traffic und die Nutzer zu beeinträchtigen.

Letztendlich ist der Schutz unternehmenskritischer Anwendungen, Infrastruktur und Markenreputation der eigentliche Maßstab für den Erfolg.

VERBESSERN SIE IHRE DDOS-ABWEHR NOCH HEUTE

Erfahren Sie, wie Akamai Sie dabei unterstützen kann, eine Null-Sekunden-Abwehr zu erreichen.

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