È possibile bloccare gli attacchi DDoS in zero secondi?

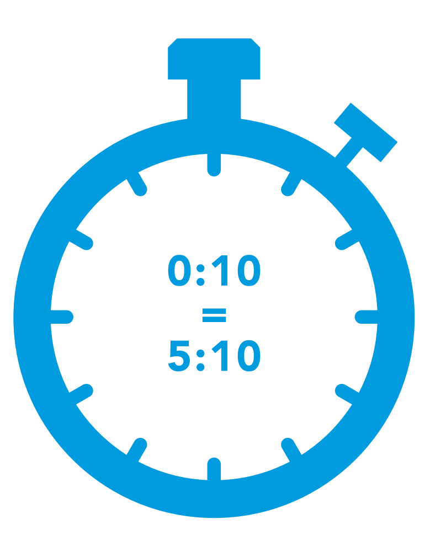
FACCIAMO CHIAREZZA SUL TTM (TIME-TO-MITIGATE)

Come risaputo, le tempistiche TTM devono essere limitate. Il TTM (Time-To-Mitigate) corrisponde al tempo che intercorre tra l'inizio di un attacco DDoS e il momento in cui le vostre risorse o applicazioni vengono protette.

Ma non tutti gli SLA (accordo sul livello di servizio) di ogni fornitore lo intendono in questo modo. Per questo è importante comprendere a fondo le tempistiche.

ATTENZIONE A QUESTI COMUNI SCENARI RELATIVI AI FORNITORI

FORNITORE A



I controlli del fornitore A devono analizzare un picco di traffico per più di 5 minuti prima di confermare un attacco DDoS.

Uno SLA con un TTM pari a 10 secondi viene avviato solo una volta confermato l'attacco.

FORNITORE B

I termini e le condizioni del fornitore B definiscono il TTM come il tempo necessario per implementare un controllo di mitigazione, ossia una risposta.

Questo SLA non garantisce di riuscire a bloccare l'attacco.

FORNITORE C

Il fornitore C si impegna a garantire l'automazione del rilevamento e della mitigazione nel suo SLA per il TTM.

Questo SLA non include tecniche di difesa manuali e personalizzate tali da bloccare attacchi sofisticati.

COMPRENSIONE DI TERMINI E CONDIZIONI

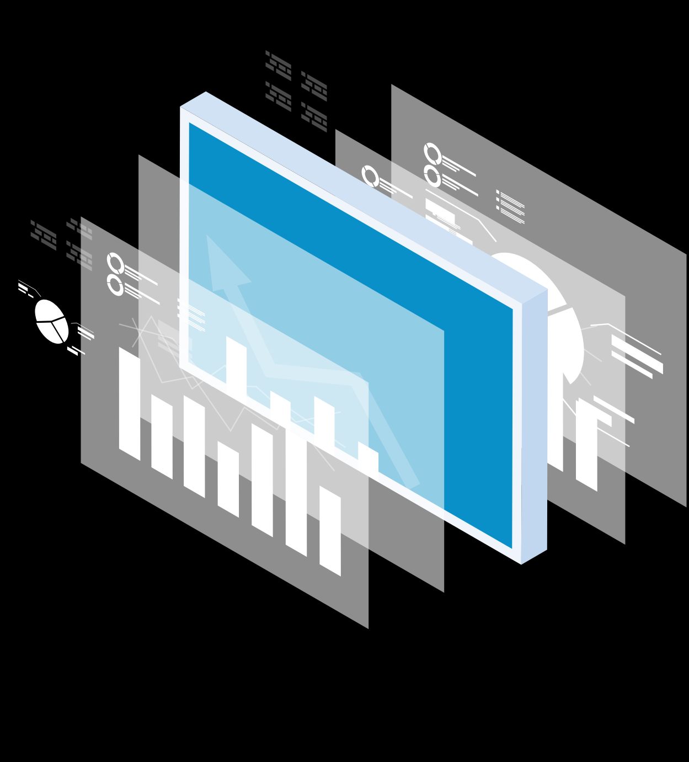
Siate **scettici** nei confronti di espressioni come:

… tempi di risposta …

Nel caso di un attacco DDoS prolungato …

… dopo il rilevamento …

TEMPISTICHE DI MITIGAZIONE DI AKAMAI



Quando **zero significa zero secondi**

I nostri controlli di mitigazione proattivi sono progettati per bloccare gli attacchi DDoS, in modo da proteggere le aziende persino prima che si accorgano di essere sotto attacco. Questa è la potenza dell'Akamai Intelligent Edge Platform.

TEMPO PER **rilevare un attacco** + TEMPO PER **applicare i controlli di mitigazione** + TEMPO PER **bloccare un attacco** = **Le migliori tempistiche di mitigazione**

8 PASSAGGI PER ATTUARE LA MITIGAZIONE DEGLI ATTACCHI DDOS

Akamai vanta le migliori tempistiche TTM del settore grazie ad una potente combinazione di ricercatori che si occupano di minacce, responsabili degli incidenti tecnici, architetti della sicurezza e tecnologie di difesa all'avanguardia. Il SOCC (Security Operations Command Center) di Akamai esegue queste operazioni:

1. **Rileva** un attacco tempestivamente con il monitoraggio degli attacchi DDoS always-on.
2. **Informa** il cliente tramite un runbook stabilito.
3. **Gestisce** il traffico del cliente con un sistema di instradamento facilitato always-on.
4. **Analizza** il traffico e identifica i vettori necessari per applicare la mitigazione.
5. **Regola** i controlli di mitigazione applicati per ottimizzare i falsi positivi e negativi.
6. **Identifica** i nuovi vettori di attacco.
7. **Analizza** il traffico e identifica i vettori emergenti per applicare la mitigazione in modo continuo.
8. **Ottimizza** i controlli di mitigazione applicati per neutralizzare gli attacchi in continua evoluzione.

I RISCHI DI UN RITARDO NEL TTM

Quali sono le **conseguenze** di un problema di downtime?

0:01

Dopo 1 secondo, le applicazioni o le risorse sul web non sono più disponibili.

0:10

Dopo 10 secondi, aumentano i problemi per i clienti e la produttività dei dipendenti diminuisce.

05:00

Dopo 5 minuti, si causano danni alla reputazione del brand e perdita di ricavi.

VALUTAZIONE DEL SISTEMA DI DIFESA DAGLI ATTACCHI DDOS

Con quale rapidità il vostro fornitore rileva un attacco?

In questi casi, le vostre applicazioni più importanti sono disponibili?

In questi casi, subite danni collaterali?

In questi casi, gli utenti legittimi ne risentono?

Con quale rapidità il vostro fornitore applica le contromisure di mitigazione?

Con quale rapidità il vostro fornitore inizia ad analizzare il traffico?

INFORMAZIONI SULLE MINACCE AKAMAI

Più vasti, più **complessi** e più **pericolosi**

Le dimensioni degli attacchi DDoS stanno crescendo a livelli da record. Nel 2020, abbiamo registrato un'attività di attacchi DDoS molto vasta e complessa con un numero e con combinazioni di vettori di attacco senza precedenti.

18 FEB 2018	16 GIUGNO 2020	21 GIUGNO 2020
1,3 Tbps (terabit al secondo)	**1,44 Tbps/385 Mpps** (milioni di pacchetti al secondo)	**809 Mpps** (milioni di pacchetti al secondo)
Questo attacco ha raddoppiato la portata dell'attacco precedente. Utilizzando un nuovo vettore per gli attacchi di riflessione DDoS, il traffico memcached basato su UDP.	Questo attacco ha usato nove diversi vettori e più strumenti di attacchi botnet. È durato quasi 2 ore ad una velocità costante di 1,3 Tbps.	È stato l'attacco con il maggior numero di pacchetti al secondo mai registrato sull'Akamai Intelligent Edge Platform. Ha utilizzato un gran numero di IP di origine distribuite a livello globale e mai registrate in precedenza, a indicare una botnet emergente.

Sistemi di difesa efficaci richiedono la combinazione di una piattaforma di comprovata validità, professionisti esperti e tecniche/processi ottimizzati.

Le **tempistiche di migrazione** si riferiscono alla velocità con cui il traffico dannoso viene identificato e bloccato senza influire sul traffico e sugli utenti legittimi.

In conclusione, la protezione delle applicazioni mission-critical, dell'infrastruttura e della reputazione del brand è la reale misura del successo.

RAFFORZATE SUBITO IL VOSTRO SISTEMA DI PROTEZIONE DAGLI ATTACCHI DDOS

Scoprite come Akamai può aiutarvi ad effettuare una mitigazione immediata.

Ulteriori informazioni

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. La piattaforma edge intelligente di Akamai permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24/7/365. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations.

Data di pubblicazione: 11/20