WAF e DDoS: la partnership perfetta

Sono molte le ragioni che spingono a combinare le soluzioni DDoS e WAF. Da citare, tra le più importanti: miglior efficacia nella prevenzione degli attacchi, unico fornitore come punto di contatto ed unico portale al quale accedere per avere informazioni relative alla gestione del servizio e all'analisi degli eventi. Ma, soprattutto, vi è una motivazione logica dal punto di vista commerciale. Oggigiorno la maggior parte delle aziende ha capito quanto la protezione dagli attacchi DDoS sia fondamentale per garantire il massimo livello di "customer experience". La natura concorrenziale del business sposta gli investimenti delle aziende nel processo di trasformazione digitale e nella "customer experience". È proprio la "customer experience" (CX), secondo Gartner, il nuovo criterio su cui basare le strategie di business dell'azienda.[1]

Investire nella "customer experience" porta ad adottare una nuova strategia. Quanto è veloce il vostro sito web? Quanto investite nei processi di automazione e nelle tecnologie che basano il loro funzionamento su tecniche di apprendimento automatico? Quali sono i concorrenti più attivi nel vostro settore di mercato e che cosa state facendo per modificare il vostro contenuto digitale e renderlo più rilevante per il vostro business? Le vostre applicazioni sono diventate imprescindibili per i vostri clienti? È a questo punto che nella nuova strategia entra in gioco la "trasformazione digitale".

Nel processo di trasformazione digitale le applicazioni diventano cruciali per il successo del vostro business. La pianificazione degli investimenti, in aree quali agilità ed automazione, deve portare allo stesso livello di attenzione gli aspetti legati alla sicurezza.

Figura 1: Gartner, "Survey Analysis: The State of Customer Experience Innovation, 2015"

1 http://blogs.gartner.com/augie-ray/2016/02/13/content-isnt-king-customer-experience-is/

Sia che le applicazioni si trovino on-premise che nel cloud, è importante garantire che i diversi servizi di sicurezza adottati possano lavorare in sinergia tra loro. In questo modo è garantita la massima efficacia e quindi il massimo livello di protezione possibile. Ecco perché il mercato della sicurezza informatica si sta spostando verso una soluzione integrata di WAF e DDoS.

Quindi, se la vostra strategia ha come obiettivi agilità ed automazione, non potete prescindere da un'unica soluzione di sicurezza. La visibilità diventa estremamente importante. Da non trascurare inoltre come un'eventuale migrazione delle applicazioni dal data center al cloud, disponendo delle stesse policy di sicurezza per la protezione, rappresenti un punto chiave per questo cambiamento.

La protezione delle applicazioni web ed il WAF sono elementi strategici che permettono di rilevare e bloccare in modalità automatica gli attacchi web sconosciuti. Alcune soluzioni si basano sull'identificazione di vulnerabilità note tramite l'utilizzo di signature e, benché sia fondamentale anche la capacità di patching virtuale, la miglior efficacia si ottiene con il modello di sicurezza positivo o "whitelisting". Il modello di sicurezza positivo è in grado di identificare e mitigare gli attacchi zero-day. Se si esaminano i nuovi regolamenti come il GDPR, si comprende come una soluzione WAF possa identificare azioni quali "web scraping" o furto delle informazioni e garantire quindi la protezione dei dati personali.

Quando si rilevano attacchi applicativi che hanno come obiettivo il Web, assume grande importanza l'integrazione tra le soluzioni WAF e DDoS. La sinergia fra i diversi livelli di protezione, basata su un meccanismo di sincronizzazione, è cruciale per garantire un'elevata "customer experience", essendo in grado di bloccare botnet e ogni tipo di azione illecita. In caso di attacco verso una delle applicazioni web con tecniche di hacking quali "brute force", "application scraping" o tentativi di sfruttare le vulnerabilità note, il sistema di sincronizzazione sarà in grado di inviare tramite WAF le informazioni dell'attacco alla soluzione DDoS installata, che a sua volta proteggerà bloccando l'attacco identificato. Se si dispone di una soluzione integrata, sarà possibile avere la visibilità del quadro completo delle proprie difese. Ciò è fondamentale per garantire che le applicazioni o il WAF stesso non vengano compromessi tramite attacchi DDoS. La latenza è infatti il "killer silenzioso" delle applicazioni e di conseguenza della "customer experience".

Essendo l'automazione in grado di accelerare il processo decisionale, Radware è testimone di questa tendenza in fatto di sicurezza. I tempi richiesti per le fasi di identificazione e mitigazione degli attacchi che richiedevano decine di minuti sono oramai un ricordo passato. Come già ripetuto, l'agilità delle imprese e l'adeguata "customer experience" esigono tempi di risposta nettamente più rapidi. E Radware è in grado di garantire la "customer experience" CX tramite visibilità sui diversi livelli di sicurezza ed automazione dei processi di identificazione e mitigazione.

Scoprite di più sul Cloud Security Service, un servizio cloud in grado di proteggere le aziende dai diversi vettori di attacco e ottimizzare le prestazioni delle applicazioni.