Specifiche soluzioni di mitigazione ad ogni tipologia di attacco informatico

Author : Redazione

Date : 11 luglio 2018

Nel tredicesimo Worldwide Infrastructure Security Report (WISR) è stato chiesto in un sondaggio di indicare le misure di sicurezza adottate dagli intervistati contro gli attacchi DDoS. L'82% delle imprese ha indicato i firewall e il 57% di esse ha dichiarato di disporre di sistemi per il rilevamento/la prevenzione dalle intrusioni (IDS/IPS). A fronte di questi dati, soltanto il 28% delle aziende ha affermato di poter contare su sistemi IDMS (Intelligent DDoS Mitigation System).

Senza dubbio, firewall e IDS/IPS hanno motivo di comparire nell'arsenale per la sicurezza. Sono infatti la prima linea di difesa contro gli attacchi il cui scopo è, ad esempio, il furto o lo spionaggio industriale. Tuttavia, da sole, queste soluzioni non sono sufficienti per opporsi agli attacchi che prendono di mira i servizi. In realtà, sono proprio i primi target degli attacchi DDoS che tentano di compromettere l'infrastruttura di rete.

Le decisioni in materia di sicurezza sono in molti casi frutto di un approccio piuttosto semplicistico da "checklist": quali strumenti dobbiamo possedere? Solitamente le difese perimetrali come i firewall si trovano spesso in cima alla lista delle soluzioni irrinunciabili. Un approccio come questo è di frequente basato su esigenze legate alla conformità: quali sono le soluzioni imposte a livello normativo? Nella maggior parte dei casi le aziende, se sono conformi, si illudono di essere al sicuro: d'altronde, hanno spuntato tutte le caselle!

Anziché limitarsi a mettere una crocetta su un elenco di soluzioni, le aziende dovrebbero valutare a quali rischi sono sottoposte di fronte alle continue minacce DDoS. In altre parole: "Quali sono i rischi DDoS che incombono su di noi? Siamo pronti ad affrontarli?". Di seguito alcune delle potenziali risposte:

Attacchi DDoS volumetrici: Questo tipo di attacchi DDoS tenta di consumare la larghezza di banda nel target oppure tra il target e il resto di internet. Raggiunge il suo scopo di bloccare l'accesso ai servizi e la loro erogazione con l'uso di una forza schiacciante. Questi attacchi sono caratterizzati da dimensioni sempre crescenti: l'attacco da 1+ terabit sta diventando la

nuova normalità. Per difendersi da questi attacchi occorre una soluzione di mitigazione dotata di capacità assimilabili che, viste le dimensioni, è solitamente presente nel cloud.

Attacchi di tipo TCP State Exhaustion: questi attacchi tentano di consumare le tabelle di stato presenti in molti nodi dell'infrastruttura, come i bilanciatori di carico, i firewall e i server applicativi. Persino i dispositivi a elevate capacità in grado di supportare milioni di connessioni possono essere messi KO da questi attacchi.

Attacchi alle applicazioni: questi attacchi sono rivolti ad applicazioni e servizi specifici del Layer 7, noto anche come il livello applicativo. Si tratta di attacchi particolarmente insidiosi, perché possono essere estremamente efficienti: una sola macchina può sferrare un attacco capace di generare un rallentamento del traffico, caratteristica che rende questi attacchi molto difficili da rilevare e da mitigare. Per difendersi da essi occorre un qualcosa capace di distinguere il traffico dati legittimo in ingresso nella rete da minacce accuratamente celate: un compito tutt'altro che semplice visto l'aumento della velocità e dei volumi del traffico.

Attacchi stratificati, multivettore: gli attacchi DDoS si avvalgono sempre più spesso di una combinazione o di varianti di queste tre categorie di attacco in un unico attacco sferrato. Questa strategia riesce a confondere e a sviare le difese. Un attacco alla più grande banca cilena segnalato di recente ha messo fuori uso qualcosa come 9.500 server e stazioni di lavoro, già uno stravolgimento enorme in sé, successivamente rivelatosi però un semplice diversivo che ha permesso agli aggressori di raggiungere il loro vero obiettivo: sottrarre 10 milioni di dollari alla banca tramite la rete SWIFT.

Attacchi in uscita dall'interno: gli aggressori più sofisticati sovvertono l'ordine per gli specialisti della sicurezza andando a piazzare il malware nelle reti aziendali che possono essere sfruttate per lanciare attacchi a target interni ed esterni. I criminali informatici prediligono soprattutto i dispositivi IoT (Internet delle cose) per introdursi furtivamente nelle reti aziendali. Negli ultimi attacchi di grande entità, infatti, le botnet IoT l'hanno fatta da padrone.

Minacce emergenti: come se tutte le altre minacce non fossero sufficienti, il panorama delle minacce globali si arricchisce continuamente di new entry. Per riuscire a farvi fronte occorrono capacità informative sulle minacce globali.

La protezione contro tutti questi tipi di minacce è imprescindibile per una difesa solida. Qualora anche una di esse venisse ignorata, infatti, si creerebbe un'esposizione in un punto qualsiasi della "catena del rischio". Una difesa ibrida o stratificata che fonda in sé rilevazione e mitigazione su cloud e locali, allertata dalle informazioni relative alle minacce globali e gestita in modo più o meno automatico è considerata dai più una buona pratica.

Un professionista della sicurezza potrebbe valutare tutti i rischi e ciò che occorre per mitigarli e stabilire che: "Non abbiamo il budget, e non possiamo contare sulla larghezza di banda necessaria". È proprio qui che entra in gioco l'opzione del servizio DDoS gestito, che prevede l'outsourcing a un fornitore che abbia già investito nella tecnologia e possieda le competenze professionali giuste per mitigare qualsiasi tipo di attacco. In questo modo è possibile risparmiare, potenziare le risorse interne e ridurre i rischi. Oltre a mandare in pensione le

checklist per la sicurezza.

Se davvero la minaccia degli attacchi DDoS è da considerarsi un pilastro importante nell’analisi del rischio aziendale, allora un approccio pragmatico e definitivo può essere e deve essere un’eventualità da prendere in forte considerazione.

A cura di: **Ivan Straniero**, Regional Manager, Southern & Eastern Europe di NETSCOUT Arbor