FORTINET

Protezione avanzata per applicazioni web su AWS

I firewall per applicazioni web offrono una sicurezza facile da gestire e con un ottimo rapporto qualità/prezzo

Sommario

Panoramica preliminare

Le aziende stanno facendo sempre più migrare le proprie applicazioni business-critical dall'infrastruttura on-premises al cloud, il che ne aumenta l'esposizione ad attacchi mirati noti e ignoti. Ogni nuova applicazione distribuita nel cloud amplia il numero di possibili punti di ingresso e, dunque, la superficie di attacco. Ad aggravare la situazione, il volume e la virulenza delle minacce continuano a crescere, esercitando una pressione senza precedenti sulle organizzazioni che si sentono indotte ad attuare e gestire più soluzioni di sicurezza.

Le aziende che scelgono Amazon Web Services (AWS) per ospitare le proprie applicazioni spesso ritengono erroneamente di non doversi preoccupare della sicurezza. Devono invece rendersi conto del fatto che AWS garantisce la sicurezza dell'infrastruttura, mentre è responsabilità del cliente garantire la sicurezza dell'applicazione e dei dati. Inoltre, la semplice riconversione degli strumenti di sicurezza esistenti on-premises non affronta le sfide dell'attuale ambiente delle minacce.

Le organizzazioni hanno piuttosto bisogno di soluzioni di sicurezza progettate specificamente per le applicazioni che si interfacciano con Internet, in particolare i firewall per le applicazioni web (WAF). I WAF proteggono da attacchi esterni e interni, monitorano e controllano l'accesso alle applicazioni web e raccolgono informazioni a fini di compliance e analisi. Per la massima flessibilità dell'architettura, i fornitori di alto livello offrono WAF in fattori di forma fisici, virtuali e cloud-native.

83%

percentuale del carico di lavoro delle aziende che sarà in cloud entro il 2020.[1]

Le sfide della sicurezza nel cloud

Quando le organizzazioni distribuiscono applicazioni web nel cloud, il loro profilo di rischio cambia. Da un lato, il cloud pubblico non ha un perimetro di sicurezza, quindi ogni nuova applicazione aumenta il numero di possibili punti di ingresso e, dunque, la superficie di attacco. Ad aggravare la situazione, il volume e la velocità delle minacce continuano a crescere. Ad esempio, gli exploit unici sono aumentati del 5% nell'ultimo trimestre del 2018, e i dati mostrano che i criminali stanno diventando più intelligenti ed efficienti sferrando attacchi codificati e mirati più sofisticati.[2]

Molte organizzazioni adottano il modello DevOps per consentire alla loro attività di muoversi velocemente. Nel farlo, spesso i team DevOps si assumono la responsabilità di rendere sicure le applicazioni che si interfacciano con Internet utilizzando i WAF. Tuttavia, il personale DevOps di solito non ha né il tempo né le competenze in materia di sicurezza per farsi carico della configurazione e della gestione dei WAF senza incidere negativamente sulle attività che generano ricavi, come ad esempio la continua creazione di nuove funzionalità. Il problema potrebbe essere risolto assumendo un altro tecnico responsabile della sicurezza, ma la carenza di talenti rende questa soluzione difficile da attuare: secondo un'importante organizzazione di categoria, i posti non ricoperti nel settore della sicurezza informatica saranno ben 1,8 milioni entro il 2022, un aumento del 20% rispetto al 2015.[3]

Nel valutare le soluzioni WAF disponibili in commercio, le aziende devono tenere conto di tutti gli elementi appena discussi. Per semplificare il processo, molti decisori iniziano a sviluppare una serie di requisiti organizzativi per la facilità di utilizzo, la protezione avanzata dalle minacce e il costo totale di proprietà (TCO).

Le applicazioni web costituiscono il principale vettore di attacco per una violazione dei dati.[4]

Requisito 1: facile da distribuire e gestire

La configurazione del firewall costituisce uno dei più importanti fattori di successo per la sicurezza delle applicazioni web. Per evitare errori di configurazione e ridurre al minimo il dispendio di tempo per gli sviluppatori, i team DevOps devono valutare i WAF in base alla facilità di distribuzione, alle policy di sicurezza personalizzabili e all'accuratezza.

Facilità di utilizzo

Vista la crescente carenza di competenze in materia di sicurezza informatica, le soluzioni di sicurezza devono ridurre al minimo il livello di competenze necessario per l'installazione e la gestione. Per raggiungere tale obiettivo, le aziende devono scegliere WAF facili da distribuire, configurare e gestire. Le caratteristiche fondamentali che contribuiscono alla facilità di utilizzo includono procedure guidate di configurazione, regole predefinite e dashboard intuitive.

Policy personalizzabili

Una volta che le aziende hanno reso operativo il WAF, DevOps e gli esperti di sicurezza devono poter mettere a punto facilmente le regole del firewall in modo da ridurre i costi operativi della gestione della sicurezza e adattarsi ai cambiamenti che intervengono nel panorama della sicurezza.

Accuratezza

I falsi positivi sottraggono al personale tempo prezioso e, se troppo numerosi, possono mascherare minacce reali. Per rispondere alle principali esigenze dell'attività, le soluzioni WAF devono integrare formule di apprendimento automatico (ML) al fine di migliorare la loro capacità di identificare con accuratezza le minacce in arrivo con la minima supervisione umana.

Nel 2018, le configurazioni errate sono state la causa del 70% delle violazioni dei dati in cloud, un aumento del 424% rispetto all'anno precedente.[5]

Requisito 2: protezione avanzata dalle minacce

Il panorama delle minacce continua ad ampliarsi e diversificarsi. Ad esempio, un recente sondaggio ha rilevato che i ricercatori scoprono almeno una nuova minaccia zero-day ogni settimana.[6] Nel valutare le capacità di protezione delle potenziali soluzioni, tra i criteri fondamentali vanno considerati l'efficacia, la protezione delle API e gli aggiornamenti di sicurezza.

Efficacia della sicurezza

La Top 10 Top 10 dell'Open Web Application Security Project (OWASP) rappresenta un ampio consenso sulle minacce più critiche alla sicurezza delle applicazioni web. Le organizzazioni che desiderano proteggere efficacemente le applicazioni web devono scegliere soluzioni che difendano da tutti i rischi riportati in tale elenco e dagli exploit ignoti e zero-day (figura 1).[7]

Top 10 dell'OWASP—2017
A1: 2017-Injection
A2: 2017-Violazione dell'autenticazione
A3: 2017-Esposizione a dati sensibili
A4: 2017-Entità esterne XML (XXE)
A5: 2017-Violazione del controllo degli accessi
A6: 2017-Errata configurazione della sicurezza
A7: 2017-Cross-Site Scripting (XSS)
A8: 2017-Deserializzazione non sicura
A9: 2017-Uso di componenti con vulnerabilità note
A10: 2017-Logging e monitoraggio insufficienti

Figura 1. Top 10 dell'OWASP: rischi per la sicurezza delle applicazioni web.

Protezione delle API

Le API non protette creano gravi vulnerabilità a livello di sicurezza che consentono agli aggressori di estrarre dati e sferrare attacchi DDoS (Distributed Denial-of-Service). In questo caso, la sicurezza completa delle applicazioni richiede regole di sicurezza speciali per proteggere le API dai malintenzionati.

Aggiornamenti di sicurezza

Oltre alle capacità di protezione avanzate prima illustrate, le soluzioni devono includere un abbonamento a un servizio di ricerca delle minacce per essere sempre aggiornate sulle tendenze degli attacchi per quanto concerne signature, IP reputation, antivirus e sandboxing.

In un recente sondaggio, il 48% dei dirigenti afferma che le minacce di attacchi DDoS siano aumentate di anno in anno.[8]

Requisito 3: basso costo totale di proprietà

Tra le alternative di distribuzione, WAF-as-a-Service (WaaS) rappresenta la soluzione più economica per molte aziende. In questo modello, il fornitore di cloud mette a disposizione i componenti hardware e software, ovviando praticamente alla necessità di investimenti in conto capitale (CapEx) ed eliminando i costi di esercizio (OpEx) associati alla manutenzione della piattaforma.

L'infrastruttura globale AWS comprende 16 regioni AWS, entità geografiche fisicamente isolate l'una dall'altra. Le organizzazioni possono avvalersi di questa infrastruttura globale scegliendo un WaaS ospitato nella stessa regione AWS in cui si trovano le applicazioni protette, strategia che riduce notevolmente la latenza e i costi di trasferimento dati: l'azienda paga solo il traffico dati verso il WaaS, mentre il fornitore del WaaS gestisce i costi in uscita.

La Top 10 dell'OWASP si basa essenzialmente sui dati forniti da oltre 40 società specializzate in sicurezza delle applicazioni, nonché su studi di settore compilati da oltre 500 persone. I dati riguardano le vulnerabilità raccolte da centinaia di organizzazioni e più di 100.000 applicazioni e API del mondo reale. Le voci della Top 10 sono selezionate e classificate per priorità sulla base di questi dati di prevalenza, abbinati a stime consensuali di sfruttabilità, rilevabilità e impatto.[9]

Alternative per la distribuzione di WAF

Sebbene AWS offra ai propri clienti un WAF di base con formula pay-per-usage, tale soluzione da sola non è in grado di fornire la sicurezza di livello enterprise di cui molte applicazioni business-critical hanno bisogno. DevOps e decisori responsabili della sicurezza dovrebbero invece ricercare un WAF con una gamma di alternative di distribuzione che consenta loro di soddisfare i requisiti di facilità di utilizzo, protezione avanzata dalle minacce e basso TCO.

Regole gestite per WAF AWS

Offerti da fornitori di sicurezza terzi, i pacchetti di regole gestite consentono agli utenti di stabilire in modo rapido e semplice controlli di sicurezza più robusti in aggiunta al WAF AWS. Il fornitore aggiorna automaticamente le regole man mano che emergono nuove vulnerabilità e nuovi malintenzionati, mantenendo aggiornate le policy di sicurezza.

WAF-as-a-Virtual Machine

Il WAF fornito come macchina virtuale (VM) protegge le applicazioni in esecuzione su piattaforme come VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM e Docker. I WAF VM offrono le stesse caratteristiche dei WAF hardware, ma con la flessibilità necessaria per soddisfare le esigenze degli ambienti di hosting delle applicazioni dinamici.

WAF-as-a-Service

La soluzione WaaS consente alle organizzazioni di disporre di una protezione avanzata dalle minacce in un fattore di forma che i team DevOps possono facilmente distribuire e gestire. Il fornitore del WaaS si occupa della manutenzione dell'infrastruttura di sicurezza, consentendo al personale DevOps di concentrarsi su attività ad alto valore che creano innovazione e generano ulteriori ricavi. Questa formula ha tutte le funzionalità delle versioni hardware e virtuale e offre opzioni di hosting regionale che possono ridurre latenza e costi di trasferimento.

Le organizzazioni che utilizzano modelli SaaS come, ad esempio, WAF-as-a-Service spendono per l'IT il 21% in meno sui ricavi e il 16% in meno per utente rispetto a quelle che adottano un modello applicativo on-premises.[10]

Le organizzazioni che utilizzano modelli SaaS come, ad esempio, WAF-as-a-Service spendono per l'IT il 21% in meno sui ricavi e il 16% in meno per utente rispetto a quelle che adottano un modello applicativo on-premises.[11]

Valutazione delle soluzioni WaaS: checklist

Per valutare e confrontare le soluzioni WaaS per le loro applicazioni web ospitate su AWS, i responsabili DevOps possono utilizzare la seguente checklist:

Distribuzione

- Attuata come soluzione cloud-native su AWS
- Include configurazioni predefinite
- Viene distribuita in pochi minuti utilizzando un set di policy predefinite

Gestibilità

- Si adatta rapidamente al cambiamento delle esigenze di sicurezza
- Supporta l'hosting regionale per ridurre i costi e semplificare la compliance
- Offre prezzi on-demand flessibili

Efficacia

- Protegge dalla Top 10 dell'OWASP e dagli exploit zero-day
- Consente di accedere a opzioni di configurazione avanzate
- Include regole WAF personalizzate
- Garantisce la sicurezza delle API
- Comprende l'abbonamento al servizio di ricerca delle minacce

FortiWeb Cloud WAF-as-a-Service protegge le applicazioni web ospitate in cloud pubblici dalle minacce avanzate: Top 10 dell'OWASP, minacce zero-day e altri attacchi a livello di applicazioni. Per ulteriori informazioni, visitare il sito web www.fortiweb-cloud.com.

[1] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, 7 gennaio 2018.

[2] "Quarterly Threat Landscape Report: Q4 2018," Fortinet, febbraio 2019.

[3] "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," (ISC)², 7 giugno 2017.

[4] "2019 Data Breach Investigations Report: Summary of Findings," Verizon, visitato il 2 luglio 2019.

[5] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, 6 aprile 2018.

[6] "Quarterly Threat Landscape Report: Q4 2018," Fortinet, febbraio 2019.

[7] "OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks," OWASP, visitato il 13 luglio 2019.

[8] "Q1, 2019 Cyber Threats & Trends Report," Neustar, 17 aprile 2019.

[9] "OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks," OWASP, visitato il 13 luglio 2019.

[10] "Cloud Users Enjoy Significant Savings," Computer Economics, visitato il 13 luglio 2019.

[11] Ibid.

www.fortinet.com

431437-0-0-IT

febbraio 16, 2021 11:36 AM