EXECUTIVE BRIEF: 4 OSTACOLI ALLA SICUREZZA DEL CLOUD PUBBLICO/PRIVATO

Un'analisi delle insidie alla sicurezza per gli odierni ambienti virtuali

Abstract

La virtualizzazione e il cloud possono ridurre i costi e aumentare l'efficienza e l'agilità operativa, ma devono affrontare minacce malware sempre crescenti. L'IT deve fare uso di budget vincolati per proteggere gli ambienti cloud pubblici/privati da problemi di sicurezza comuni, tra cui:

- Cecità al traffico inter-VM
- Proliferazione delle policy
- Sprawl virtuale
- Vincoli del cloud pubblico

Iniziative aziendali che spingono per il passaggio alla virtualizzazione

Affrontando mercati in rapida evoluzione, una concorrenza agguerrita e un ambiente aziendale sempre più veloce, le organizzazioni devono proteggere le quote di mercato e crescere al tempo stesso. Oggi più che mai, la tecnologia dell'informazione gioca un ruolo centrale.

Dal punto di vista del back-end, l'IT ha il compito di tenere il passo delle innovazioni tecnologiche, modernizzare i data center e l'ambiente IT e ottimizzare i servizi IT affinché l'organizzazione sia posizionata correttamente. Questi compiti includono la progettazione, l'implementazione e la realizzazione di nuove applicazioni che rendano possibile l'attività aziendale, strumenti e servizi di produttività dell'utente, oltre ad architetture di rete quali cloud computing privato/pubblico/ibrido, *network function virtualization* (NFV) e mobilità. Altrettanto importanti sono il supporto e la protezione che l'IT deve fornire a questo dinamico ambiente di rete e alla forza lavoro mobile a budget inalterato, se non addirittura ridotto.

Dal lato del front-end, l'IT deve riuscire a garantire che la presenza, i servizi e il supporto Web dell'azienda siano online 24 ore su 24, 7 giorni su 7, ogni giorno dell'anno. Ne deriva la necessità di mantenere al sicuro tutte le proprietà Web dell'organizzazione, senza interruzioni e al massimo delle prestazioni. Lo scopo dell'IT è una difesa a costo contenuto, ma senza compromessi. A tal fine è necessaria una sicurezza dinamica in grado di prevenire gli attacchi fornendo al tempo stesso strumenti di analisi per proteggere e reagire a livello dell'intera infrastruttura fisica e virtuale dell'organizzazione. L'IT deve insistere sulla sicurezza senza compromessi, che si tratti di cloud cablato/wireless o privato/pubblico e dall'ufficio centrale ai campus remoti, alle sedi distaccate, alle filiali o agli ambienti partner.

I lati positivi e negativi della virtualizzazione

Per oltre un decennio, la virtualizzazione dei server ha trasformato la parte di calcolo dell'infrastruttura IT portandola dal mondo fisico al mondo della virtualizzazione. Oggi la virtualizzazione rimane importante, in quanto continua ad avanzare e ad arricchire i vantaggi operativi ed economici dell'intero data center, riducendo sia le spese operative che le spese di capitale, consentendo al personale di concentrarsi sulle infrastrutture critiche.

I continui progressi negli strumenti e nei servizi di virtualizzazione, come la *network function virtualization*, permettono ai reparti IT di sviluppare e posizionare in modo facile e veloce i carichi di lavoro virtualizzati ovunque all'interno della rete virtuale (VN). Inoltre, la virtualizzazione consente all'IT una maggiore programmabilità della rete e capacità di autogestione, nonché la velocità di provisioning necessaria per aumentare l'efficienza dei data center. In tal modo si consente ai team addetti alle reti e alle applicazioni di personalizzare e fornire nuovi servizi e avviare, spostare, copiare, clonare, ripristinare o eliminare istantaneamente i servizi ospitati su macchine virtuali in qualsiasi momento per soddisfare le esigenze operative specifiche dei data center. Questo aumento del livello di agilità ed elasticità operativa riduce sensibilmente il costo di fornitura dei servizi applicativi all'intera azienda.

Tuttavia, nonostante questi numerosi vantaggi, l'altra faccia della tecnologia di virtualizzazione è costituita dalle numerose implicazioni sulla sicurezza e dalle problematiche che l'IT deve affrontare (vedere la Tabella 2, in basso). La virtualizzazione, per sua natura, aggiunge molti livelli di infrastruttura e complessità operativa. Aspetti come l'uso condiviso di archiviazione, dispositivi di routing, segmenti di rete e canali di comunicazione si sono dimostrati vulnerabili agli attacchi informatici, come attacchi alle risorse condivise, attacchi *cross-VM*, attacchi *side-channel* e comuni vulnerabilità delle applicazioni e dei protocolli di rete. Queste minacce raggiungono tutte le parti del framework virtuale, inclusi l'hypervisor o il *virtual machine monitor* (VMM), le macchine virtuali (VM, *virtual machine*), i sistemi operativi (SO) delle VM, le applicazioni in esecuzione su tali sistemi operativi e i componenti di rete virtuali dell'ambiente virtualizzato. Una protezione non adeguata dell'intero ambiente virtuale potrebbe comportare danni incommensurabili per un'organizzazione.

Tabella 2 Relazioni tra vulnerabilità e minacce negli ambienti di virtualizzazione della rete

Categorie di minacce		Vulnerabilità	Minacce
Divulgazione	Fuga di informazioni	Mancata protezione della tabella ARP	Poisoning della tabella ARP
		Posizionamento di regole del firewall all'interno dei nodi virtuali	Sovversione delle regole del firewall
	Intercettazione delle informazioni	Mancata protezione della tabella ARP	Poisoning della tabella ARP
		Trasmissione di dati in pattern prevedibili	Attacchi di analisi del traffico
		Gestione incontrollata di richieste multiple e sequenziali di reti virtuali da una singola entità	Inferenza e divulgazione di informazioni topologiche sensibili
		Scambio non protetto di informazioni di routing tra router virtuali	Divulgazione di informazioni di routing sensibili
	Sfruttamento dell'introspezione	Introspezione incontrollata	Furto di dati
Inganno	Furto d'identità	Gestione impropria delle identità:	
		- nell'ambito di singole reti	Iniezione di messaggi maligni con fonti contraffatte
		- fra reti federate	Escalation dei privilegi
		- durante le procedure di migrazione	Abuso della rimozione e della riaggiunta dei nodi per ottenere nuove identità (pulite)
	Perdita di voci di registro	Operazioni di rollback incontrollate	Perdita di voci di registro
	Riproduzione degli attacchi	Mancanza di identificatori univoci dei messaggi	Riproduzione degli attacchi
Disruption	Sovraccarico di risorse fisiche	Allocazione incontrollata delle risorse	Degrado delle prestazioni
			Consumo abusivo di risorse
		Gestione incontrollata di richieste di rete virtuali	Esaurimento delle risorse in parti specifiche dell'infrastruttura
		Mancanza di strategie di recupero proattivo o reattivo	Attacchi Denial of Service
	Guasto di risorse fisiche	Mancanza di strategie di recupero proattivo o reattivo	Guasto di router/reti virtuali
		Riallocazione incontrollata delle risorse dopo i guasti	Sovraccarico di router virtuali rimanenti dopo i guasti
Usurpazione	Furto d'identità	Gestione impropria delle identità e privilegi associati	Escalation dei privilegi
	Sfruttamento della vulnerabilità del software	Escalation di privilegi nei monitor di macchine virtuali	Controllo non autorizzato dei router fisici

Fonte: «Virtual network security: threats, countermeasures, and challenges», Journal of Internet Services and Applications, dicembre 2015

Tali danni possono comprendere:

- Presa di controllo non autorizzata di sistemi virtuali per eseguire azioni dannose
- Accesso non autorizzato a risorse di dati protette
- Furto di informazioni
- Interruzione del servizio o degrado dell'ecosistema virtuale in parte o per intero

La virtualizzazione è attualmente un campo attivo di ricerca delle vulnerabilità e delle minacce in ambito accademico, del *bug bounty*, dell'hacking etico e delle comunità di criminalità informatica organizzata. Nuove minacce vengono scoperte regolarmente. VENOM, CVE-2015-3456, è uno di questi exploit che interessa piattaforme di virtualizzazione popolari come Xen e KVM.

Pertanto, l'IT ha motivo preoccuparsi seriamente della propria situazione di sicurezza. Molte organizzazioni temono che l'attuale sistema di difesa manchi dei controlli di sicurezza dinamici e delle funzionalità necessari per fornire un'adeguata protezione alle infrastrutture di rete virtuali su base continuativa. Ciò rende più impegnativo per l'IT garantire l'uptime operativo, la fornitura e la disponibilità dei servizi e la conformità ai requisiti normativi.

Scenario pratico

Per offrire un punto di vista più pratico è possibile analizzare uno scenario in cui l'ambiente virtuale di un'organizzazione si trova in un'architettura di sicurezza a firewall fisico. La Figura 1 (in alto a destra) descrive il canale del flusso di comunicazione dalla VM dell'applicazione alla VM del database sulla macchina host della macchina virtuale. L'applicazione potrebbe essere una Microsoft SharePoint che esegue una lettura/scrittura su un database SQL. In questo scenario, l'IT deve garantire che i servizi applicativi siano forniti in modo sicuro.

Ambiente virtuale con firewall fisico

L'IT può adottare due approcci per l'ispezione con metodi legacy già esistenti. Una possibilità consiste nell'instradare il

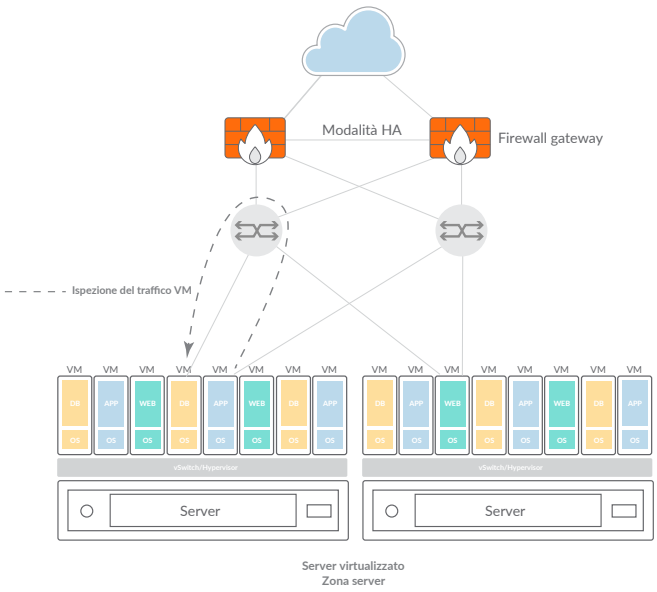

Figura 1: ambiente virtuale con firewall fisico

traffico da VM a VM attraverso lo switch virtuale (vSwitch) *northbound* fino al tessuto di commutazione esterno e quindi verso un firewall esterno che restituisce lo stesso canale *southbound*. Dirigere il traffico in questo modo richiede molti salti (*hop*) e può causare problemi come il degrado delle prestazioni, la latenza, la perdita di pacchetti e problemi di controllo della sicurezza come sopra descritto. Il secondo approccio consiste nell'utilizzare dei firewall software facendoli girare come agenti su ogni VM. Questo metodo si trova a fronteggiare problematiche simili, con basse prestazioni e aggiungendo al tempo stesso complessità gestionale a mano a mano che aumenta il volume delle macchine virtuali.

Andando ad esaminare le sfide alla sicurezza dei firewall fisici in un mondo dinamico virtualizzato, le insidie più comuni che l'IT deve affrrontare sono:

1. Cecità al traffico tra macchine virtuali
2. Proliferazione delle policy
3. Sprawl virtuale
4. Ambiente cloud pubblico

Cecità al traffico tra macchine virtuali

Quando si dispone di decine di VM in un sistema virtuale in comunicazione tra loro, un firewall perimetrale fisico potrebbe non essere in grado di vedere all'interno del traffico laterale, poiché il traffico non può mai fuoriuscire da tale server virtuale a causa degli isolamenti delle VM o delle configurazioni di routing. Dal punto di vista della sicurezza, monitorare gli eventi insoliti e le anomalie in questi scenari diventa impossibile.

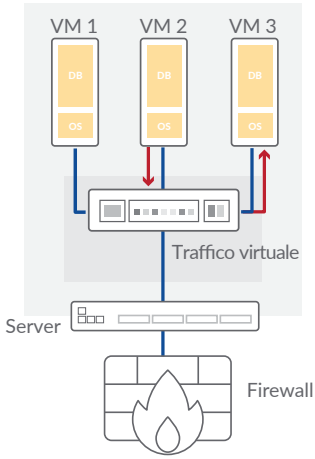

Figura 2: traffico inter-VM

Proliferazione delle policy

Quando si creano o spostano delle proprietà virtualizzate, sono necessarie numerose modifiche complesse alla configurazione della rete per indirizzare il traffico di tali VM al firewall fisico, coinvolgendo il routing e le regole NAT, le porte e i protocolli supportati dall'applicazione. Le linee guida per la gestione delle modifiche obbligano ad apportare modifiche alle policy, che devono attraversare un processo manuale e laborioso di controllo, approvazione, verifica e test del workflow, prima di procedere al roll-out in produzione. Questo processo è molto inefficiente, presenta un impatto notevole sull'operatività ed è costoso a causa del gran numero di persone coinvolte.

Inoltre, con l'accumularsi di nuove regole che si sommano alle centinaia di altre regole oscure, forse mai verificate e autorizzate prima, le policy di sicurezza diventano complicate e ingestibili. L'IT potrebbe iniziare a notare la comparsa e l'espansione di lacune nelle policy, il mancatoo rilevamento di minacce e/o un calo delle prestazioni.

Sprawl virtuale

Lo sprawl virtuale si riferisce a un problema comune in cui il numero di proprietà virtuali all'interno di un ambiente raggiunge un punto in cui diventa troppo difficile da tracciare e controllare. Quando le macchine virtuali vengono copiate, clonate o spostate (e, in molti casi, sospese e dimenticate), creano rischi per la sicurezza e lasciano l'ambiente aperto e vulnerabile, poiché le policy e i controlli di sicurezza risultano dissociati. Pertanto non è pratico avere una regola di sicurezza fissata su un indirizzo IP statico della VM, considerando che spesso gli indirizzi IP delle macchine virtuali cambiano. Si tratta di un problema diffuso che gli hacker sfruttano attivamente come vulnerabilità. Per questo motivo, un ambiente virtuale dinamico richiede controlli di sicurezza dinamici, con un processo di modifica rigorosamente regolato e verificabile per garantire che le VM siano conformi ad adeguate policy di sicurezza e di configurazione.

Ambiente cloud pubblico

Un altro caso d'uso problematico è quando i servizi applicativi di un'organizzazione si trovano su un cloud pubblico come Amazon Web Services (AWS) o Microsoft Azure. In un ambiente cloud, l'IT dell'organizzazione non può installare un dispositivo firewall fisico nel data center protetto del provider. Si tratta di strutture estremamente controllate e, anche nel caso in cui l'IT riuscisse a collocare un dispositivo fisico, non sarebbe in grado di dettare il modello di traffico, pertanto il firewall si troverebbe di fronte al traffico delle applicazioni dell'organizzazione. In questo caso, anche il firewall deve essere virtuale, quindi l'IT potrebbe utilizzare la tecnologia SDN (*Software-Defined Networking*) o configurazioni manuali per la progettazione del traffico al fine di posizionare il firewall virtualizzato tra i suoi servizi applicativi e il resto del mondo, indipendentemente dal fatto che il percorso sia interno o esterno al data center.

Conclusione

La sicurezza è un fattore chiave in qualsiasi analisi costi-benefici delle iniziative di virtualizzazione. I vantaggi in termini di risparmio ed efficienza devono essere valutati rispetto a potenziali danni dovuti a crescenti minacce e a insidie comuni. L'IT deve esplorare nuove soluzioni oltre gli approcci e le tecnologie legacy in grado di garantire efficacemente la sicurezza della virtualizzazione.

Per saperne di più: leggete il nostro brief sulle soluzioni, «Che cosa cercare in un firewall di nuova generazione» e visitate il sito www.sonicwall.com/virtual-firewall.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul potenziale utilizzo di questo materiale, contattare:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com