NOTA SINTETICA

Le sfide nel settore della gestione della sicurezza delle reti

Quali sono gli ostacoli da affrontare nella gestione del rischi, della sicurezza e delle risorse

Sommario

La rapida diffusione dei firewall e degli altri servizi di sicurezza nelle reti iperdistribuite e il crescente ricorso alla mobilità nella "nuova normalità" evidenziano la necessità di una gestione unificata della sicurezza nelle aziende di qualsiasi dimensione. Questo breve documento analizza le tendenze emergenti ed esamina le sfide che si devono affrontare per quanto riguarda la gestione del rischio, la sicurezza e l'utilizzo delle risorse.

Introduzione

Il telelavoro, le reti distribuite, il passaggio al cloud e la proliferazione di applicazioni e dispositivi hanno comportato un aumento indiscriminato dei punti di esposizione. Indipendentemente dal fatto che si tratti di aziende di piccole dimensioni, imprese distribuite o fornitori di servizi di sicurezza gestiti, la necessità di proteggere le attività "sempre e dovunque" costituisce la nuova normalità.

Allo stesso tempo, le minacce sono sempre più evasive. Con un aumento annuo delle minacce non rilevate pari al 145%[1], le organizzazioni non sono in grado di capire quali minacce non siano state individuate.

Inoltre, le organizzazioni informatiche devono fare i conti con l'aumento dei costi, con budget limitati e con la carenza di personale qualificato.

L'effetto combinato di questi aspetti pone importanti sfide in termini di sicurezza delle reti in termini di contenimento dei rischi, di gestione delle attività e di utilizzo delle risorse.

Esigenze diverse

Tutte le organizzazioni devono conoscere e individuare minacce in continua evoluzione. Tutte hanno bisogno di conoscere le attività e l'uso delle reti e i rischi connessi. Tutte devono inoltre monitorare, risolvere le anomalie e le sfide operative e di sicurezza. E tutte devono attenersi a rigorose linee guida di sicurezza interne.

Le imprese di piccole dimensioni, tuttavia, possono avere risorse tecniche interne limitate. Gestire la sicurezza e ottimizzare le prestazioni può essere impossibile. Anche le imprese di dimensioni maggiori e i fornitori di servizi che dispongono di personale di sicurezza interno, possono trovarsi a dover affrontare problematiche più ampie e più impegnative, e dover modulare l'installazione e la gestione dei sistemi di sicurezza in reti distribuite complesse. Inoltre devono preoccuparsi dell'automazione della sicurezza e della gestione del cambiamento, dei rapporti di verifica e della continuità delle politiche.

Gestione del rischio

Le moderne organizzazioni sanno bene che in un determinato giorno la situazione può passare dalla normalità al caos più completo nel giro di pochi secondi. Il rischio di cadere vittima di attacchi mirati non è venuto meno per molte organizzazioni, dal momento che le notizie relative alle violazioni delle reti e all'esposizione di grandi moli di dati continuano a fare notizia.

Conoscete in che misura la vostra organizzazione è a rischio? Vi sono lacune di sicurezza nelle vostre attività interne? Che cosa sapete su chi utilizza la vostra rete e di quali risorse, siti web e applicazioni SaaS dispongono? E che decisioni prendete per prioritizzare e affrontare questi rischi?

Il traffico delle applicazioni e dei dati interessa Internet, le università remote, le filiali e anche i fornitori esterni. Le organizzazioni possono avere una visibilità e un controllo insufficienti per quanto riguarda le attività di rete non sicure, le irregolarità del traffico, l'accesso e la movimentazione anomali dei dati, i firmware non aggiornati, gli eventi di sicurezza e lo stato di salute dei sistemi.

I rischi non gestiti possono comportare qualcosa di ancora peggiore. Le violazioni rallentano l'accelerazione e la crescita delle aziende. Le attività vengono stravolte dal momento che il personale specializzato non può più concentrarsi

su quelle che sono le priorità aziendali. I funzionari sono costretti a dedicare tutto il loro tempo al controllo dei danni e alle pubbliche relazioni. L'incapacità di riconoscere i rischi di sicurezza impedisce la pianificazione della sicurezza, le decisioni politiche e le azioni decisive.

Operazioni di sicurezza

Anche gli stessi firewall sono punti di esposizione. Una ricerca di Gartner[2] indica che il 99% delle violazioni dei firewall è imputabile ad una errata configurazione degli stessi. Quando le regole del firewall vengono definite, copiate e modificate, possono risultare in contraddizione tra loro con conseguenze impreviste in termini di sicurezza e di prestazioni. Gli errori di configurazione e le incongruenze tra le regole possono rendere la rete vulnerabile alle minacce sofisticate, agli accessi non autorizzati e alle intrusioni.

Anziché per tracciare le lacune e le vulnerabilità di sicurezza, il tempo potrebbe essere impiegato in modo più proficuo per verificare che le configurazioni dei firewall non siano troppo permissive e non aprano backdoor alle infrastrutture di rete. Le organizzazioni devono validare e verificare le politiche e le configurazioni prima di attuarle, e all'occorrenza revocarle rapidamente.

Il passaggio a reti multi-cloud più grandi e più complesse che supportino un maggior numero di applicazioni e di utenti costituisce un nuovo spazio di lavoro digitale. Man mano che le reti crescono, gestire le attività di sicurezza, ottimizzare le prestazioni, risolvere le problematiche operative e garantire le misure di sicurezza e il controllo degli accessi per utenti, dispositivi e applicazioni, continua a costituire una sfida impegnativa.

Le organizzazioni hanno difficoltà ad attuare interventi di sicurezza interna adeguati per soddisfare le politiche sui livelli di servizio interni, che sono finalizzate a tutelare le imprese e i dipendenti, ridurre i rischi di sicurezza e limitare le responsabilità finanziarie e legali.

Quando si tratta di gestire diversi firewall singolarmente e manualmente, spesso le organizzazioni hanno a che fare con politiche e procedure incoerenti. Spesso esse dispongono di pochi o di nessun processo di analisi, prova, verifica e approvazione che possa garantire l'esecuzione corretta e al momento opportuno delle regole per i firewall, nel rispetto dei requisiti di conformità interni.

Destinazione delle risorse

La carenza di figure qualificate nel settore della sicurezza costituisce un grosso problema a livello di personale. Numerose organizzazioni, soprattutto le PMI, non dispongono di personale di sicurezza adeguato né di capacità specifiche per una gestione efficace dei firewall e la soluzione delle gravi problematiche di sicurezza nel momento in cui si presentano.

Ogni singolo firewall richiede una regolare manutenzione programmata, un monitoraggio giornaliero, il riesame e l'amministrazione delle politiche e gli aggiornamenti del firmware. Man mano che le reti si espandono e crescono a livello di imprese distribuite e di fornitori multi-tenant, il carico di lavoro per il personale di sicurezza si moltiplica in modo esponenziale.

A peggiorare le cose, gli addetti alle attività di sicurezza possono dover fare i conti con la gestione e il funzionamento di silos di firewall complessi e frammentati. Le attività amministrative sono spesso complesse, pesanti e richiedono parecchio personale. Le attività e i processi non vengono in genere verificati e corroborati e non risultano conformi. Ciò comporta situazioni in cui le piccole reti possono veder proliferare il numero di regole dei firewall nel corso degli anni, e a loro volta le reti più grandi possono avere migliaia di regole.

Conclusioni

È necessario che le cose migliorino. Sono necessari strumenti di gestione più intelligenti perché il personale di sicurezza possa lavorare in modo più efficace.

SonicWall Network Security Manager (NSM) mette a disposizione tutto ciò che serve per una gestione completa dei firewall, consente una visibilità completa, il controllo granulare e la possibilità di comandare tutte le attività di sicurezza di rete con maggiore chiarezza, precisione e velocità. Il tutto con un'unica interfaccia ricca di funzioni accessibile da qualsiasi postazione con un dispositivo compatibile con i browser.

Ulteriori informazioni Rivolgersi al rappresentante SonicWall o visitare www.sonicwall.com/nsm.

SonicWall

SonicWall fornisce soluzioni di cibersicurezza illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare il sito www.sonicwall.com.

[1] Rapporto SonicWall 2020 sulle ciberminacce
[2] Info Security

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per ulteriori informazioni consultare il nostro sito web.
www.sonicwall.com

ExecutiveBrief-TheChallengeOfNSM-US-VG-1965