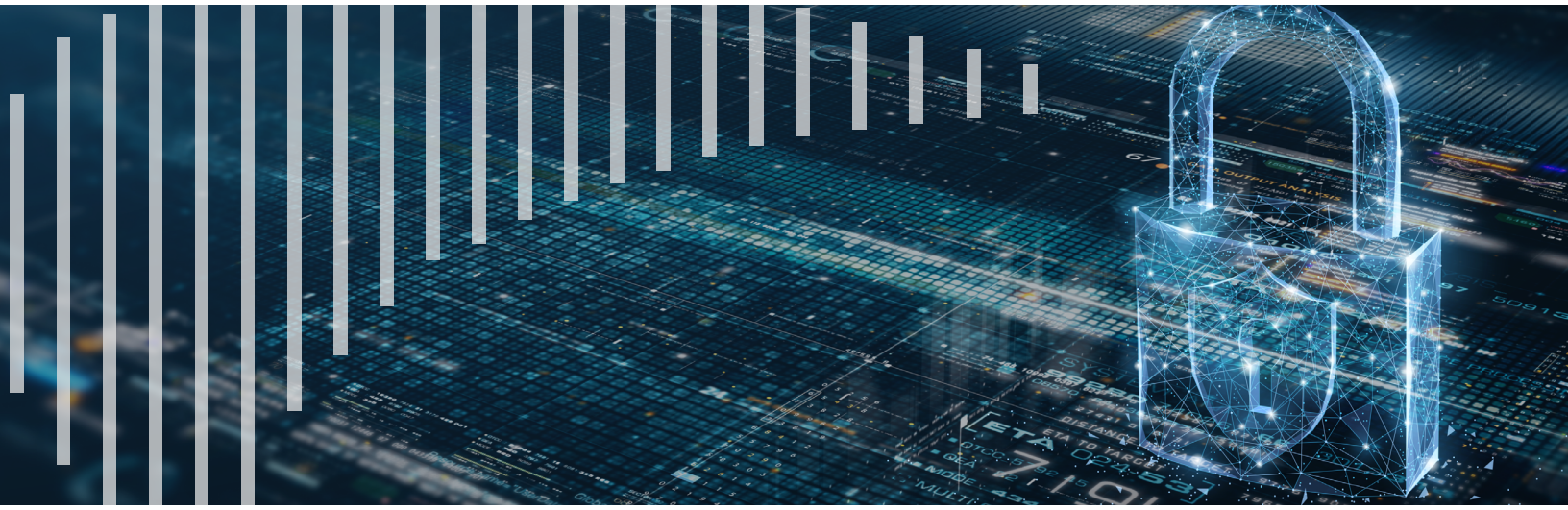
SONICWALL



EXECUTIVE BRIEF

Strategie evolute contro le minacce in evoluzione

Introduzione

Il mondo della cybersecurity è in continua evoluzione e cambia rapidamente, e le aziende devono stare al passo con questi cambiamenti.

La realtà informatica distribuita e in forte espansione sta provocando un aumento senza precedenti di punti di esposizione che i cybercriminali più abili possono sfruttare.

Con la crescente diffusione di ambienti ibridi e completamente remoti aumentano i punti di esposizione e, di conseguenza, anche i vettori di cyber attacco. Le minacce comuni e gli attacchi multilivello sono sempre più difficili da rilevare. Molte aziende cercano nuovi modi per potenziare la loro sicurezza informatica e stare un passo avanti rispetto ai cyber criminali. In realtà esistono diverse strategie e tecnologie che le aziende possono utilizzare per rafforzare la postura di sicurezza e proteggere la loro organizzazione.

Implementare l'autenticazione multifattore

L'autenticazione multifattore (MFA) è uno strumento indispensabile sia per le aziende che per uso privato. L'autenticazione MFA funge da ulteriore barriera tra le reti e i cybercriminali, e può rendere gli attacchi più difficili da realizzare e proibitivi in termini di costi per gli aggressori. L'autenticazione MFA può prevenire attacchi comuni come phishing, keylogger, forza bruta e man-in-the-middle (MITM). Esistono diversi tipi di MFA:

- Per dispositivi personali: può trattarsi di un messaggio di testo o di un'app di autenticazione
- Basata su hardware: utilizza un dispositivo hardware tipo USB, smart card o token RSA
- Biologica: ad esempio un'impronta digitale o una scansione della retina

Come per ogni tecnologia o software, le aziende devono svolgere accurati protocolli di ricerca e verifica per poter implementare la policy MFA più adeguata alle loro esigenze di sicurezza.

Imparare a valutare meglio il rischio

Per creare una strategia di sicurezza efficace, le aziende devono sapere come valutare correttamente i rischi, che sono diversi per ogni organizzazione. Un'agenzia governativa può avere necessità di proteggere risorse globali e documenti relativi alla difesa nazionale. Una piccola impresa con una crescente reputazione del marchio potrebbe voler salvaguardare le proprie risorse finanziarie. Indipendentemente dalle dimensioni dell'azienda, molti professionisti della sicurezza si attengono ai requisiti del NIST (National Institute of Standards and Technology) per garantire il rispetto degli standard e delle buone prassi normative. Sebbene i quadri normativi offrano una base solida, ogni azienda deve valutare un profilo di rischio specifico per la propria realtà. Le aziende devono adottare una prospettiva ampia, ma con un'attenzione particolare al proprio livello di rischio. I responsabili dei vari reparti aziendali possono fornire il loro contributo. I professionisti della cybersecurity potrebbero scoprire che altri reparti hanno opinioni differenti ma valide per quanto riguarda il rischio. Una volta acquisita una conoscenza approfondita del rischio nell'intero ecosistema aziendale, i professionisti della cybersecurity possono tracciare un percorso da seguire per adottare una postura di sicurezza più robusta.

Colmare il gap di competenze

Le aziende hanno bisogno di professionisti qualificati per difendere la propria infrastruttura dai cyber attacchi. Al crescere della complessità della rete, aumenta anche la necessità di personale tecnico competente. Molte aziende

scoprono così di aver bisogno di personale altamente qualificato per proteggere in modo efficace l'hardware, il software e la rete aziendale dai cybercriminali. Attirare i migliori talenti è un'esigenza ormai imprescindibile, ma molte aziende hanno difficoltà a trovare personale qualificato. Riuscire ad assumere e trattenere i professionisti di cybersecurity non è semplice. SonicWall dispone di un'ampia rete di partner che consente di aiutare le imprese di ogni dimensione a raggiungere i loro scopi e obiettivi di sicurezza.

Scegliere la tecnologia giusta

Le difese di sicurezza si sono evolute, migliorando la capacità dei team di gestione IT di salvaguardare le risorse e proteggere le reti. Una solida strategia di sicurezza include la protezione multilivello e la copertura completa di tutte le superfici di attacco.

I cybercriminali tentano di colpire le aziende sfruttando un'ampia gamma di applicazioni, dispositivi, reti e infrastrutture. Lanciano attacchi con ogni mezzo possibile, dal phishing a varianti di malware finora sconosciute fino a ransomware, attacchi al canale laterale, attacchi IoT e altre tecniche particolarmente difficili da rilevare.

SonicWall vi aiuta a eliminare i punti ciechi e a proteggere in qualsiasi ambiente una forza lavoro che opera ormai "senza confini". Potrete vedere ogni risorsa in ogni luogo e agire velocemente per gli eventi più rilevanti.

Il nostro Capture Security Center elimina la cosiddetta visibilità a compartimenti stagni. Da un unico pannello di controllo è possibile visualizzare ogni superficie di attacco su diverse generazioni di infrastrutture IT (on premise, cloud, endpoint e reti sicure as-a-service).

Il rilevamento delle minacce in tempo reale, 24 ore su 24, registra le vulnerabilità nel momento in cui vengono scoperte e sa sempre cosa sono e cosa tentano di violare. Le metriche di rischio personalizzate riducono ulteriormente l'esposizione e consentono di prioritizzare le azioni in base al profilo di rischio, mentre le analisi e i report velocizzano i tempi di risposta e contribuiscono a definire la strategia.

La tecnologia Real-Time Deep Memory Inspection™ (RTDMI) brevettata da SonicWall blocca le minacce zero-day e sconosciute a livello del gateway, anche quelle nascoste tramite crittografia o che non mostrano un comportamento dannoso. La tecnologia è stata concepita per comprendere come operano gli autori delle minacce. Le minacce zero-day non hanno una firma riconoscibile finché non vengono utilizzate per la prima volta, e questo rende le aziende vulnerabili. RTDMI rileva queste minacce e offre un livello di visibilità che consente di rilevare ogni modifica nel comportamento degli aggressori.

Pretendere di più dai fornitori

Le aziende devono avere la certezza che i loro fornitori adottano misure di sicurezza adeguate nello sviluppo dei prodotti. Idealmente, i fornitori di soluzioni dovrebbero disporre di sistemi come l'analisi della composizione del software (SCA) e il test statico della sicurezza delle applicazioni (SAST). Per comprendere l'esposizione al rischio per diverse vulnerabilità, è fondamentale avere visibilità nelle varie fasi di sviluppo. I cybercriminali sanno che il perimetro è il punto più difficile per accedere all'interno di un'azienda. Per questo cercano vulnerabilità in tutta l'organizzazione, compresi i software e hardware di terze parti. Le aziende possono creare dei questionari per i fornitori in cui definire gli standard che i

fornitori devono rispettare. Questo tipo di verifica fornisce numerose informazioni per decidere quale fornitore è più adatto per la vostra azienda. La scelta di fornitori qualificati può aiutare le aziende a rafforzare la propria postura di cybersecurity complessiva.

Conclusioni

Gli autori delle minacce cambiano costantemente i loro piani di attacco per riuscire a infiltrarsi nelle aziende e causare il maggior danno possibile. In un mondo in cui i cybercriminali cambiano continuamente tattica per cogliere di sorpresa le aziende, occorre implementare alcune strategie per stare sempre un passo avanti.

- Utilizzate l'autenticazione multifattore per rendere più difficile l'infiltrazione nelle vostre reti.
- Sviluppate strategie di valutazione del rischio migliori per garantire la protezione dell'azienda in tutti i potenziali punti di accesso.
- Assumete e formate personale altamente qualificato per ottimizzare e gestire tutti i sistemi di sicurezza.
- Scegliete la tecnologia migliore per le reti, gli endpoint e i punti di accesso che proteggono i dati e gli utenti.
- Definite requisiti stringenti per i fornitori, per garantire che gli hardware e software di terze parti non introducano vulnerabilità nell'azienda.

In definitiva, è compito delle aziende stabilire quali strategie di cybersecurity funzionano meglio per la loro organizzazione. Per maggiori informazioni su come creare, scalare e gestire la sicurezza in ambienti cloud, ibridi e tradizionali, contattate subito un esperto di sicurezza SonicWall.

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

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