E-BOOK

LE 8 INSIDIE PRINCIPALI DELLA SICUREZZA DEGLI ENDPOINT

Introduzione

La gestione e la sicurezza degli endpoint sono di fondamentale importanza nel contesto aziendale attuale. Con gli utenti finali che entrano ed escono dalla rete utilizzando dispositivi con vulnerabilità non corrette da patch e minacce crittografate che raggiungono gli endpoint in modo incontrollato, occorre proteggere i dispositivi per garantire la sicurezza sia degli endpoint sia della rete nel suo complesso. Mentre i ransomware e i furti di credenziali diventano sempre più pervasivi, gli endpoint sono diventati il campo di battaglia delle odierne minacce.

Nonostante l'ampia offerta di soluzioni disponibili sul mercato, gli amministratori faticano ancora a monitorare e gestire l'infrastruttura di sicurezza aziendale. Oltre a ciò devono garantire la sicurezza costante dei client e la disponibilità di funzioni di intelligence e reportistica fruibili e semplici da utilizzare. In questo documento illustriamo alcune insidie che potrebbero presentarsi durante la creazione di una strategia per la protezione degli endpoint.

SONICWALL®

Soluzioni di sicurezza obsolete

Gli amministratori devono assicurarsi che sugli endpoint gestiti sia installata la versione corretta dei componenti del software di sicurezza in uso, come previsto dalla policy di conformità. Questo problema si aggrava nel caso delle soluzioni antivirus tradizionali, che si affidano a un database di firme aggiornate per fornire protezione dalle minacce più recenti. Le soluzioni di protezione avanzata degli endpoint (AEP), che analizzano il comportamento del sistema con metodi euristici, sono più efficaci contro questi attacchi e possono anche bloccare script dannosi come quelli usati negli attacchi fileless.

"L'85% dei codebase conteneva dipendenze open source obsolete di almeno quattro anni."

Rapporto Open Source Security and Risk Analysis (OSSRA) del 2021 di Synopsis

Applicare le policy e la conformità Web

Gli amministratori faticano a mitigare i rischi associati agli utenti che usano i loro dispositivi su reti esterne a casa, negli internet cafè, in hotel o in aeroporto. Allo stesso tempo hanno difficoltà ad applicare le politiche di utilizzo web aziendali anche all'esterno dell'ufficio. Al di fuori del posto di lavoro, le persone hanno maggiori probabilità di imbattersi in pagine web dannose e tendono a visitare siti web non legati al lavoro, con una conseguente perdita di produttività. E se gli utenti caricano tutti i loro dati dal data center aziendale tramite la VPN, potrebbe essere necessario limitare i contenuti a elevato consumo di banda come i video. Nei primi giorni della pandemia, gli amministratori lamentavano il fatto che le loro reti erano sommerse da traffico proveniente da TikTok, YouTube, Netflix e altri servizi di streaming. Purtroppo questo problema continuerà a crescere man mano che la qualità delle immagini migliora e le persone utilizzano sempre di più queste app per l'intrattenimento.

"Il 30-40% delle attività svolte dai dipendenti in Internet non è collegato al lavoro"

Fonte: IDC Research

SONICWALL®

Reportistica e gestione degli accessi

In alcuni casi gli amministratori possono gestire diversi tenant attraverso i firewall, ma i loro utenti sono configurati in un unico pool. Questo rende più difficile ottenere un single sign-on (SSO) dall'amministratore di un firewall o da una soluzione di gestione della sicurezza quando si tenta di gestire le policy dei client. Allo stesso tempo, le normative di conformità prevedono spesso che tutti i ruoli degli amministratori rispettino il principio del privilegio minimo, per cui una suite di gestione client unificata che non è in grado di gestire il controllo degli accessi basato sui ruoli causerà numerosi problemi. Ad esempio, un utente può essere limitato a due ruoli: uno con accesso in lettura/scrittura e l'altro con accesso in sola lettura.

Minacce provenienti da canali crittografati

Con l'aumento del numero di applicazioni Web protette tramite canali crittografati come HTTPS e con il ricorso alla crittografia anche da parte del malware per aggirare l'ispezione basata sulla rete, è diventato indispensabile utilizzare l'ispezione deep packet del traffico SSL/TLS (DPI-SSL). Tuttavia, questa soluzione non è facilmente applicabile senza un'implementazione di massa di certificati SSL/TLS affidabili su tutti gli endpoint per evitare problematiche che impattano sull'esperienza dell'utente e sulla sicurezza.

SONICWALL®

Capire gli allarmi e sapere come intervenire

Gli utenti finali sono generalmente meno consapevoli dei rischi per la sicurezza rispetto ai professionisti della sicurezza e, di conseguenza, in molti casi non comprendono gli allarmi generati dai client di sicurezza degli endpoint. Inoltre, la maggior parte dei client non include informazioni per l'autorisoluzione dei problemi, quindi gli utenti ignorano il problema o richiedono assistenza al reparto IT. Se ad esempio il dispositivo di un utente non rientra nella policy e l'utente viene messo in quarantena, questo utente non sa cosa deve fare per ripristinare la conformità.

Gestione delle licenze

A livello backend, un problema dei software di sicurezza degli endpoint è che gli amministratori, in particolare nel caso degli MSSP, non sono in grado di garantire che il loro software utilizzi una licenza corretta. Se le informazioni sulle licenze dei clienti non vengono monitorate e archiviate centralmente, possono verificarsi interruzioni del servizio e problemi di sicurezza. Inoltre, gli amministratori possono avere difficoltà a redigere report di compliance per tutte le licenze di terze parti implementate per pagare i propri partner.

SONICWALL®

Fermare le minacce avanzate come il ransomware

Gli approcci tradizionali alla sicurezza degli endpoint possono talvolta lasciare a desiderare in merito al rispetto dei requisiti amministrativi. L'approccio basato su firme, adottato a lungo dalle tecnologie antivirus tradizionali, non è riuscito a tenere il passo con lo sviluppo di nuovo malware e di tecniche di evasione. Molte soluzioni tradizionali non sono in grado di rilevare le minacce avanzate e non offrono una strategia di difesa multilivello per gli endpoint, compresa l'integrazione con un ambiente sandbox.

Inoltre, senza il livello di protezione aggiuntiva di una soluzione di rilevamento e risposta degli endpoint, gli attacchi avanzati e sofisticati possono eludere la protezione degli endpoint o altre misure di sicurezza.

"Nei primi tre trimestri del 2020, il ransomware è aumentato del 40% rispetto allo stesso periodo del 2019".

Fonte: Dati SonicWall sulle minacce del 3° trimestre

SONICWALL®

Non sapere dove si nascondono le vulnerabilità critiche

Con la forte crescita delle applicazioni aziendali è aumentata in modo esponenziale anche la minaccia delle vulnerabilità delle applicazioni, causando violazioni e non pochi problemi agli amministratori IT. Molte aziende non hanno ancora un metodo per quantificare e classificare le vulnerabilità e quindi hanno difficoltà a creare un piano per l'applicazione di patch o la disinstallazione di applicazioni rischiose.

Oltre al rischio delle vulnerabilità prive di patch, i team IT spesso non dispongono di strumenti per la ricerca proattiva di minacce nascoste che attendono pazientemente il momento giusto per lanciare un attacco (Threat Hunting).

"Nel solo 2019, le CNA hanno assegnato un punteggio CVSS critico superiore a 9.0 ad oltre 16.000 vulnerabilità."

Fonte: National Vulnerability Database del NIST

Conclusioni

Creare un piano di protezione degli endpoint può sembrare estremamente complesso a causa delle potenziali insidie, ma le numerose risorse disponibili consentono di semplificare il processo. Per individuare la soluzione più adatta alla vostra organizzazione potete leggere il nostro documento "Le caratteristiche richieste dagli amministratori per una soluzione di sicurezza degli endpoint."

LEGGI IL DOCUMENTO

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla 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 possibile economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni potete visitare www.sonicwall.com.

Per chiarimenti sul potenziale utilizzo di questo materiale rivolgersi a:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

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