FORTINET

La segmentazione tradizionale fallisce di fronte all'odierna espansione della superficie di attacco

Perché i responsabili della gestione tecnica e operativa della rete devono preoccuparsi

Sommario

FORTINET

Panoramica preliminare

L'espansione e la frammentazione della superficie di attacco derivante dalla mobilità e dall'adozione del multi-cloud stanno compromettendo la capacità dei responsabili della gestione tecnica e operativa di una rete di garantirne prestazioni, sicurezza, affidabilità e disponibilità. La segmentazione tradizionale basata sulla rete, unitamente alle tecniche di microsegmentazione ancora più recenti, sono insufficienti perché non consentono di rilevare e prevenire le minacce. Limitate dall'architettura di rete, sono infatti di natura tattica più che strategica, e sono focalizzate su una logica di business. Sono inoltre tipicamente statiche, permettendo a utenti, dispositivi e applicazioni, una volta giudicati affidabili, di operare liberamente nei relativi segmenti. Mancano infine di visibilità completa della sicurezza, in tutta la rete e nei flussi crittografati, che è essenziale per un'efficace gestione del rischio.

Introduzione: Difficoltà nel gestire reti disparate: la segmentazione è la risposta?

La base di utenti di una tipica rete aziendale è sempre più dispersa geograficamente, così come i dispositivi e le applicazioni che si collegano alle risorse IT aziendali. Man mano che le reti aziendali hanno dato spazio a tecnologie mobili e IoT (Internet of Things) e hanno adottato applicazioni Software-as-a-Service (SaaS) in più cloud pubblici, le loro superfici di attacco sono diventate sempre più difficili da proteggere, anche con una forte sicurezza perimetrale.

Una sfida derivante dall'espansione e dalla frammentazione delle superfici di attacco consiste è determinata dal fatto che creano una serie di nuovi percorsi attraverso i quali i criminali possono sferrare il proprio attacco. Un altro problema è che le minacce sono sempre più sofisticate, cercando e sfruttando automaticamente qualsiasi vulnerabilità. A complicare ulteriormente la situazione, le operazioni di fusione e acquisizione (M&A) possono tradursi in un'infrastruttura diversificata con una visibilità o un coordinamento limitato tra le diverse parti dell'organizzazione. In molte, la sicurezza è diventata un esercizio di reazione perché il reparto IT non è in grado di impedire il movimento laterale delle intrusioni tra le applicazioni e i dispositivi connessi alla rete e che la attraversano.

Per anni, i responsabili della gestione tecnica e operativa della rete hanno risposto a tali sfide segmentando le reti. Le tecniche di segmentazione tradizionali basate sugli indirizzi IP sono state integrate dalla segmentazione in VLAN e VMware NSX per carichi di lavoro virtualizzati. Le reti basate su dispositivi Cisco si affidano alla segmentazione Cisco ACI utilizzando switch fisici e VXLAN. Queste tecniche di microsegmentazione consentono di definire le policy di controllo degli accessi in base a carichi di lavoro e applicazioni o ad attributi architettonici come le macchine virtuali (VM) su cui risiedono applicazioni, dati e sistemi operativi.

In questi approcci di segmentazione si utilizzano firewall per separare le risorse di rete di ogni gruppo, precludendo in tal modo a qualsiasi traffico non autorizzato la possibilità di muoversi tra i segmenti. Pertanto, quando un attacco viola la sicurezza della rete in un'area, tale approccio dovrebbe teoricamente impedirne la diffusione laterale ad altre aree della rete.

Purtroppo, la microsegmentazione non è la panacea, come a volte si sostiene. Le idee sottostanti sono valide, ma se un'infrastruttura di rete microsegmentata non è progettata in maniera corretta, di fatto potrebbe ostacolare la sicurezza. Dividere una rete aziendale complessa in molti piccoli segmenti può limitare la visibilità delle minacce e le attività di attenuazione degli attacchi in tutta la rete.[1]

Dividere una rete aziendale complessa in molti piccoli segmenti può limitare la visibilità delle minacce e le attività di attenuazione degli attacchi in tutta la rete.[2]

3 motivi per i quali lo status quo della segmentazione aumenta il rischio

Le attuali tecniche di segmentazione pongono sostanzialmente tre problemi:

1. Il controllo degli accessi per i segmenti interni della rete è progettato dall'architettura in su, un approccio tattico difficilmente adattabile a esigenze di business in continuo mutamento.
2. Le valutazioni dell'affidabilità su cui si basano le policy di accesso tendono ad essere statiche e diventano rapidamente obsolete.
3. Le policy di controllo degli accessi non sono applicabili efficacemente a causa della mancanza di componenti di sicurezza avanzati (Layer 7) dal data center al perimetro della rete e, inoltre, non sono in grado di vedere e controllare in maniera efficiente questi componenti.

Questi problemi spesso derivano dal fatto che il personale responsabile della gestione tecnica e operativa della rete pianifica l'architettura di segmentazione senza prestare un'adeguata attenzione alla sicurezza. La comprensione di ciascuna di queste problematiche e del loro impatto complessivo può portare ad un approccio alla segmentazione più consapevole del rischio.

“Fin troppo spesso, la rete è progettata senza considerare le esigenze tecniche e operative della sicurezza. I team IT non riescono a rendere il piano per la sicurezza parte del progetto della rete mentre, di fatto, i due vanno di pari passo. Di conseguenza, i due funzionano come capo e sottoposto anziché come collaboratori sullo stesso piano nella spirale IT. Questo disallineamento si amplifica in ambienti di rete complessi e fortemente segmentati”.[3]

Un approccio tattico dal basso verso l'alto per il controllo degli accessi

Presumibilmente, la progettazione di una rete aziendale è dettata dalla costante evoluzione delle esigenze dell'organizzazione. Le regole che stabiliscono chi e cosa può accedere alle varie risorse di rete sono determinate dalle politiche di business, dagli standard di settore e dai regolamenti di governo. Seguendo tali regole, il team responsabile della gestione operativa della rete configura le impostazioni di controllo degli accessi in router e switch, che consentono a utenti, dispositivi o applicazioni di accedere a specifiche risorse di rete.

I responsabili della gestione tecnica e operativa della rete riconosceranno immediatamente due aspetti negativi di tale approccio. In primo luogo, i processi di business, i requisiti di conformità e le esigenze di accesso alla rete di un'organizzazione sono decisamente più complessi della struttura della sua rete. Di conseguenza, è molto difficile usare l'architettura di rete allo scopo di definire segmenti sicuri per risorse di rete che siano contemporaneamente accessibili a tutti gli utenti e le applicazioni autorizzati e assolutamente inaccessibili a tutti gli altri. In pratica, vi saranno lacune di sicurezza, ossia scenari di accesso che gli architetti della rete non hanno ipotizzato, potenzialmente sfruttabili da malintenzionati, cosa che sta già accadendo con malware avanzati e sofisticati.

In secondo luogo, qualsiasi processo, regolamento o struttura organizzativa è suscettibile di modifiche. Pertanto, anche se si riuscisse a progettare una rete con una sicurezza ottimale, sarebbe necessario modificarla. Come detto, le lacune a livello di sicurezza possono manifestarsi in molti modi, per non parlare dei tempi e dei costi di una riconfigurazione che pochi team responsabili della gestione di una rete possono permettersi.

È molto difficile usare l'architettura di rete allo scopo di definire segmenti sicuri. In pratica, vi saranno lacune di sicurezza, ossia scenari di accesso che gli architetti della rete non hanno ipotizzato, potenzialmente sfruttabili da malintenzionati.

Le valutazioni dell'affidabilità tendono ad essere statiche

Per gestire efficacemente il rischio, i responsabili della gestione tecnica e operativa della rete devono disporre di informazioni precise e aggiornate sull'affidabilità di utenti, applicazioni e asset di rete. I loro firewall interni o altri meccanismi di controllo degli accessi che autorizzano o vietano il flusso di traffico tra i segmenti di rete devono sempre funzionare sulla base di dati sull'affidabilità aggiornati. Se tali valutazioni sono superate, le tecnologie di segmentazione non permettono più di evitare che potenziali minacce si muovano lateralmente attraverso la rete.

La qualità dei dati sull'affidabilità sta diventando un problema pressante nella sicurezza della segmentazione della rete perché l'effettiva affidabilità delle risorse di rete può cambiare inaspettatamente. Numerose organizzazioni, infatti, sono state colte alla sprovvista da attacchi provenienti dalle fila dei loro dipendenti e contraenti di fiducia. Più di un terzo delle violazioni segnalate riguarda utenti interni e il 29% il furto di credenziali.[4]

Alcune organizzazioni hanno reagito a tali pericoli praticamente bloccando le proprie reti, non ritenendo affidabile alcun utente né alcuna applicazione e creando livelli di verifica prima di consentire l'accesso. I responsabili della gestione tecnica e operativa della rete devono proteggere le risorse sensibili, senza però creare vincoli inutili per quanti legittimamente richiedono l'accesso a tali risorse.

"L'affidabilità non è assoluta, binaria o statica. È un'indicazione del livello relativo di forza dell'assicurazione della fiducia. Il livello di affidabilità è inoltre dinamico e cambia nel tempo. L'accesso alle funzionalità deve, dunque, essere adattabile".[5]

Il controllo degli accessi ha ben poco significato senza implementazione

Le policy di controllo degli accessi non possono funzionare come previsto se alla rete mancano elementi chiave per un'infrastruttura di sicurezza efficace. Gli approcci tradizionali alla segmentazione presuppongono l'esistenza di tutti i componenti di sicurezza della rete necessari per attuare qualsiasi policy di controllo degli accessi definita dal team IT. Questo assunto, tuttavia, potrebbe non essere valido per diversi motivi.

Il costo totale di proprietà (TCO) è uno dei principali motivi per i quali le organizzazioni possono non avere una sicurezza avanzata onnipresente. Ad esempio, un team responsabile della gestione tecnica e operativa della rete che stabilisce la segmentazione può decidere che alcuni segmenti della rete con superfici di attacco più piccole sono adeguatamente protetti senza applicare la sicurezza avanzata di livello 7. Per motivi di budget o semplicemente perché la distribuzione e la gestione richiedono troppe risorse, i team responsabili della gestione tecnica e operativa della rete possono esitare a distribuire firewall di nuova generazione (NGFW) e altre soluzioni avanzate di protezione dalle minacce ovunque sono necessarie (all'interno dell'azienda, in ogni cloud in cui operano e in ogni endpoint e dispositivo IoT).

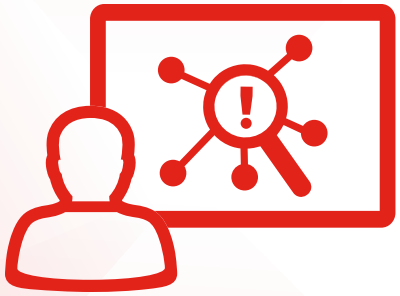
Le componenti di sicurezza presenti possono non essere perfettamente funzionali. Alcuni team responsabili della rete potrebbero intenzionalmente disattivare l'ispezione SSL (Secure Sockets Layer)/TLS (Transport Layer Security) dei loro NGFW per ottimizzare le prestazioni della rete. Limitare in tal modo le soluzioni di sicurezza può contribuire al movimento più rapido del traffico legittimo tra i segmenti della rete, ma contemporaneamente apre la porta al traffico illegittimo. E, con il 72% del traffico di rete ormai crittografato e i cybercriminali che lo sfruttano per infiltrarsi nelle reti ed esfiltrare dati, questo è motivo di grave preoccupazione.[6]

L'efficacia complessiva dei componenti di sicurezza si riduce se non sono perfettamente integrati. La mancanza di integrazione ha diverse conseguenze. In primo luogo, quando un firewall rileva un pacchetto sospettoso, possono essere necessarie diverse ore o più prima che le informazioni vengano prelevate dall'amministratore della sicurezza e diffuse al resto della rete.

In secondo luogo, soluzioni di sicurezza disparate non possono facilmente condividere threat intelligence, né informazioni acquisite a livello globale su minacce note ed emergenti né threat intelligence su nuove minacce zero-day identificate. Questo può essere uno dei motivi per i quali il tempo medio di identificazione di una violazione rimane elevato, ben 197 giorni.[7]

In terzo luogo, le organizzazioni non sono in grado di rispondere efficacemente per attenuare l'impatto delle violazioni rilevate. Senza una tecnologia di sandboxing integrata per mettere automaticamente in quarantena e testare tutti i pacchetti sospetti, possono verificarsi gravi danni prima che il team responsabile della sicurezza gestisca manualmente la minaccia.

In tali condizioni, i responsabili della gestione tecnica e operativa della rete convinti che la loro rete segmentata sia ben protetta possono lavorare con un falso senso di sicurezza. Una valutazione continua della sicurezza end-to-end direbbe loro come funziona la loro piattaforma di sicurezza e se le loro policy di controllo degli accessi rispondono ai loro obiettivi aziendali. Purtroppo, senza tutta una serie di soluzioni di sicurezza e una visibilità end-to-end, non è possibile ottenere una valutazione attendibile, il che impedisce a molti responsabili della gestione tecnica e operativa della rete di riferire con precisione sulla strategia di sicurezza della loro azienda.



Soluzioni di sicurezza disparate non possono facilmente condividere threat intelligence su minacce note o nuove minacce identificate. Questo può essere uno dei motivi per i quali il tempo medio di identificazione di una violazione rimane elevato, ben 197 giorni.[8]

Conclusione: principali preoccupazioni derivanti dalla segmentazione

La segmentazione della rete è necessaria, ma lo status quo è insufficiente. Le aziende che non incorporano valutazioni dinamiche dell'affidabilità nel controllo degli accessi tra i segmenti lasciano vulnerabili utenti e asset. Le reti in cui l'architettura di segmentazione limita gli obiettivi aziendali non supportano il progressivo conseguimento di tali obiettivi. Allo stesso tempo, se le priorità a livello di prestazioni hanno la meglio sulla salvaguardia della sicurezza, la segmentazione può tradursi in un'attenuazione inefficace delle minacce, limitandosi alla reazione anziché alla prevenzione. E le reti che mancano di un'adeguata visibilità in termini di strategia di sicurezza possono non incorporare la sicurezza di livello 7, che è fondamentale per prevenire minacce avanzate.

Spetta ai responsabili della gestione tecnica e operativa della rete garantire che le policy di controllo degli accessi per i segmenti interni della rete siano adeguate in un'epoca di continua espansione e frammentazione delle superfici di attacco. Solo prestando grande attenzione alla progettazione della segmentazione un'azienda può confidare nella sua capacità di contrastare attacchi che tentano di muoversi lateralmente attraverso la rete.

[1] Keith Townsend, "Get a Quick Primer on How Microsegmentation Can Improve Network Security", BizTech, 26 maggio 2017.

[2] Ibid.

[3] "Friction in the IT Helix: How to Create Harmony between Network Design and Security" Masergy, 8 agosto 2018.

[4] "2019 Data Breach Investigations Report," Verizon, consultato l'8 luglio 2019.

[5] Neil MacDonald, "Zero Trust Is an Initial Step on the Roadmap to CARTA", Gartner, 10 dicembre 2018.

[6] John Maddison, "More Encrypted Traffic Than Ever" Fortinet, 10 dicembre 2018.

[7] "2018 Cost of a Data Breach Study", Ponemon, luglio 2018.

[8] Ibid.

www.fortinet.com

361475-0-0-IT

ottobre 24, 2019 4:09 p.

eb-traditional-segmentation