Architettura zero trust
Cos'è e come ottenerla

Alcatel·Lucent Enterprise

Indice

Cos'è l'architettura zero trust?

Cosa significa architettura zero trust (ZTA)? Significa che ogni utente e dispositivo deve essere autenticato e autorizzato prima di poter accedere ai dati. È una strategia basata sul principio "non fidarti di nessuno, autentica tutto".

Per comprendere di che si tratta, proviamo con un'analogia.

Se pensiamo alla sicurezza tradizionale come a una fortezza che protegge un villaggio, costruiremmo il muro della fortezza (altrimenti noto come firewall) intorno al villaggio (altrimenti noto come impresa). Qualsiasi elemento che giunge dall'esterno della fortezza è considerato inaffidabile e deve essere monitorato, mentre tutto ciò che è all'interno è implicitamente fidato e permesso. Questo confine di fiducia è sia fisico che implicito, a seconda del lato della fortezza in cui ci si trova, perché finché si è dalla parte "giusta" del muro, non sono necessari altri controlli. Se pensiamo a questo approccio in termini di rete aziendale, ci può essere qualche segmentazione di base statica sotto forma di VLAN, SSID, sottoreti o interfacce legate a un firewall, che ha più a che fare con la scalabilità e la gestibilità della rete piuttosto che con la sicurezza.

Oggi, tuttavia, l'approccio firewall (fortezza) si rivela meno efficace se utilizzato da solo, per una serie di motivi. Il primo è la mobilità. Gli utenti si connettono ad altre reti al di fuori dell'azienda e possono portare con sé una serie di minacce. In secondo luogo, gli ospiti non sono necessariamente affidabili. Si potrebbe obiettare che non ci si dovrebbe fidare ciecamente neanche dei dipendenti (quelli all'interno della fortezza). In terzo luogo, il numero di dispositivi IoT aggiunti alla rete è in continuo aumento. Questi presentano rischi di sicurezza più elevati perché non possono essere sanzionati e gestiti dall'IT e di norma non hanno funzionalità di sicurezza. Con il tradizionale approccio "fortezza/villaggio", "firewall/enterprise", se un utente o un dispositivo viene compromesso, c'è poco o niente che impedisce alla minaccia di estendersi ad altri utenti e dispositivi. Una volta che sei dentro, sei libero di muoverti.

Proseguendo nell'analogia della fortezza, se l'unica cosa che protegge il villaggio dagli intrusi è il muro, il giorno in cui scopriranno come scalarlo - e lo faranno - ci sarà un caos.

La domanda è: cosa possiamo fare? Riflettiamo partendo dall'approccio "trust no one" o "zero trust".

Secondo l'approccio zero trust, nessun utente o dispositivo è fidato. Che siano in sede o fuori sede, passano attraverso gli stessi controlli. Non esiste nulla che eguagli gli utenti interni. Ogni accesso è autenticato e autorizzato.

Nell'analogia della fortezza significherebbe che oltre alla fortezza che protegge il villaggio dalle minacce esterne, ogni casa, ogni edificio dovrebbe disporre della propria sicurezza per proteggersi dai rischi di soggetti malvagi che vivono all'interno della fortezza. In termini di impresa ciò è noto come 'software-defined micro-segmentation'. Oltre alla fortezza e alla sicurezza intorno agli edifici, abbiamo anche guardie di sicurezza personali che ci seguono ovunque andiamo e qualunque sia la nostra destinazione, ci verrà chiesto il passaporto. Nella rete aziendale questo confine di fiducia è vago, è distribuito ed è mobile. Non è legato a una specifica posizione, porta dello switch o VLAN. Dipende, tra i vari fattori, dall'identità, dal dispositivo, dalla situazione e dall'ora del giorno. È software-defined e si regola in tempo reale. Con questo approccio i componenti devono essere gestiti e dovrebbero essere in grado di reagire e riconfigurarsi come necessario per rispondere alle minacce o ai cambiamenti nel flusso di lavoro

Comprendere la macro e la microsegmentazione

In un'architettura zero trust ci sono due tipi di segmentazione, macro e microsegmentazione. Per rimanere nell'ambito della nostra analogia, il muro della fortezza è la macrosegmentazione, e le guardie di sicurezza personali sono la microsegmentazione.

Nella macrosegmentazione, la rete fisica è ripartita in diversi segmenti logici. Questi segmenti possono essere una VLAN, una combinazione di VLAN e VRF, o potrebbe anche essere una VPN quando si parla di Shortest Path Bridging (SBP), MPLS, o anche tunnel VXLAN o GRE. Il traffico tra utenti o dispositivi su segmenti diversi è controllato da un firewall. Tutte le imprese usano una qualche forma o soluzione di segmentazione, ma non sempre per ragioni di sicurezza. Molto spesso, questo tipo di segmentazione è utilizzato per motivi di scalabilità, amministrativi o organizzativi. Se due dispositivi sono mappati su VLAN diverse, ma possono comunicare senza passare attraverso un firewall, si trovano sullo stesso macrosegmento. Un esempio tipico di questo tipo di segmentazione è la gestione della telefonia IP su VLAN e VRF separate che sono logicamente isolate dai PC.

La domanda che ci si pone è la seguente: come è possibile mappare gli utenti o i dispositivi a questi segmenti? Si potrebbe optare per una soluzione statica, per porta dello switch o SSID per esempio, ma in realtà è un modo obsoleto di affrontare il problema. È troppo rigido e non è particolarmente vantaggioso per gli utenti mobili. Idealmente, si dovrebbe disporre di un sistema di autenticazione software-defined così che quando un utente o un dispositivo si connette e si autentica gli venga assegnato un profilo. Il profilo indirizzerà l'utente o il dispositivo sul segmento corretto indipendentemente dalla posizione fisica, dalla porta dello switch o dall'SSID.

La macrosegmentazione presenta una serie di vantaggi in termini di sicurezza, tuttavia in molti casi viene adottata per ragioni organizzative o amministrative. Ad esempio, le telecamere e le chiavi rientrano sotto il controllo del gruppo di sicurezza degli accessi, mentre i termostati sono sotto il controllo del gruppo di manutenzione dell'edificio.

La microsegmentazione consente di fare un passo avanti. Non tutti gli utenti sono uguali e non tutti hanno un'esigenza legittima ad accedere a tutte le risorse. Lo stesso profilo che mappa gli utenti in un segmento include anche un insieme di policy che aggiungono un controllo specifico sui privilegi di utenti/dispositivi che sono diversi a seconda dei ruoli come HR rispetto a Finance. Questo approccio è noto come **"role-based access"** (accesso basato sul ruolo), ed è direttamente collegato al **"principio del privilegio** minimo". E così, anche se le telecamere e le serrature delle porte sono sullo stesso segmento, non hanno bisogno di usare le stesse risorse. La telecamera deve comunicare con il videoregistratore e la serratura della porta con il suo server. Non occorre che una telecamera comunichi con la serratura di una porta, così come non occorre che la serratura di una porta comunichi con un'altra serratura. Queste autorizzazioni specifiche sono attuate attraverso policy che fanno parte del profilo e sono applicate dinamicamente al dispositivo dopo l'autenticazione.

La microsegmentazione deve essere 'software-defined' per diversi motivi. Gli utenti e i dispositivi IoT non sono statici, ma si muovono, si connettono e si disconnettono, le policy non possono essere vincolate a un luogo o a una porta. Infatti, le configurazioni di microsegmentazione devono essere dinamiche in base alla combinazione di più fattori, tra cui, per citarne alcuni, l'identità dell'utente o del dispositivo, l'ora del giorno e la posizione.

In sintesi, quando la comunicazione tra diversi segmenti è controllata da un firewall, si tratta di macrosegmentazione. Quando la comunicazione all'interno dello stesso segmento è controllata da policy di Network Access Control (NAC) associate al dispositivo o al ruolo dell'utente, si tratta di microsegmentazione.

Perché occorrono entrambe

Cosa accade se si usa solo un tipo di segmentazione?

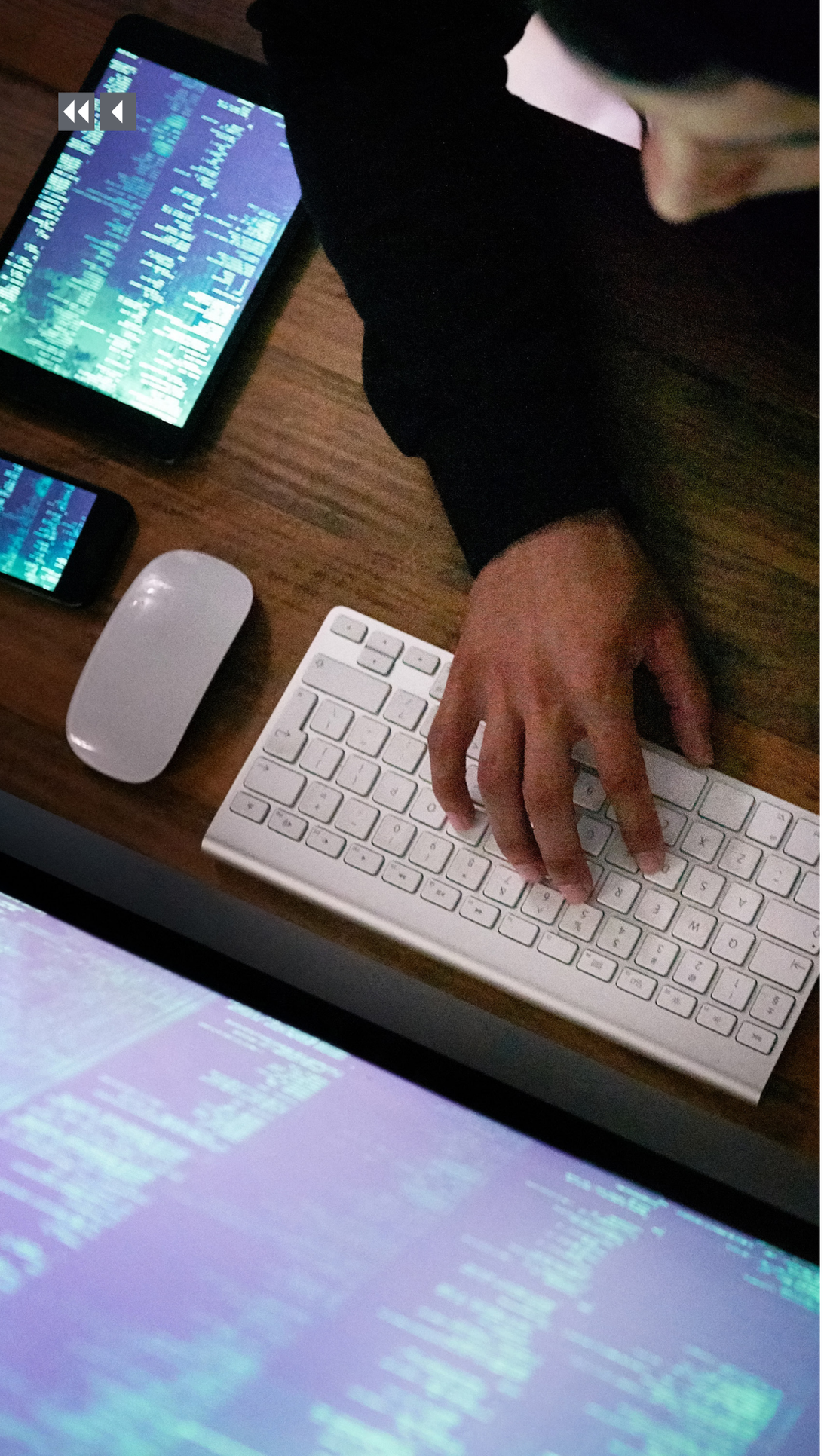
Esaminiamo la macrosegmentazione. Utilizzando solo questo approccio il traffico deve passare attraverso il firewall per l'autenticazione e l'autorizzazione e questo diventa un collo di bottiglia e può causare problemi di performance. Si potrebbero implementare più firewall al livello di distribuzione, ma si tratta di una soluzione piuttosto costosa, che non può necessariamente migliorare le performance in quanto i firewall non sono wire rate. Inoltre, in questo caso ci sono più punti di applicazione delle policy e più luoghi per mantenerle aggiornate, rendendo la gestione poco agevole.

Anche l'opzione di affidarsi solo alla microsegmentazione è problematica. Se l'unica applicazione delle policy si basa sui criteri NAC (Network Access Control), gli elenchi delle policy diventano estremamente lunghi e complessi e possono esaurire i limiti di capacità del dispositivo.

In conclusione, la soluzione migliore è quella di avere un equilibrio tra queste due forme di segmentazione. Consentire al firewall di controllare il traffico tra diversi segmenti (verticali), e alle policy NAC di controllare il traffico all'interno di un dato segmento (laterale).

Combinando questi due aspetti, è possibile intervenire sulle minacce alla sicurezza che si riversano da un segmento all'altro, nonché su quelle che si muovono lateralmente attraverso lo stesso segmento. In termini più tangibili, la microsegmentazione è ciò che impedisce a un aggressore che è riuscito a compromettere una telecamera, di utilizzare la violazione come perno per compromettere altre risorse come la serratura di una porta.

L'obiettivo è autenticare ogni connessione e assegnare autorizzazioni a ogni utente o dispositivo. Questo significa ricorrere alla segmentazione per impedire la diffusione delle minacce strutturandola con il movimento laterale, il monitoraggio continuo e la messa in quarantena di qualsiasi utente o dispositivo che diventa non conforme.



Come ottenerla

In una situazione greenfield, incontaminata e aperta a qualsiasi trasformazione, sarebbe relativamente facile costruire un'architettura zero trust introducendo la microsegmentazione ex novo. Ma, in situazioni opposte, cosiddette brownfield, ammodernare la rete con la microsegmentazione potrebbe portare a utenti, dispositivi e applicazioni bloccati fuori dalla rete stessa a causa di autenticazioni non riuscite o policy incomplete. Sarebbe difficile o addirittura improbabile che un'azienda riesca a migrare in un'unica volta, con un unico ciclo di aggiornamento.

Negli ambienti brownfield, ci sarà un periodo durante il quale coesisteranno architetture non zero trust e zero trust, e la migrazione interesserà un livello o una posizione alla volta. Ciò che è importante è assicurarsi che gli elementi dell'infrastruttura che si implementano e il modo in cui vengono implementati, siano flessibili e in grado di funzionare in modalità zero trust o microsegmentata quando altri elementi dell'infrastruttura sono pronti. Questo significa che l'infrastruttura dovrà essere in grado di interoperare con i componenti esistenti e quelli futuri.

La metodologia

Ci sono cinque step da considerare per passare a un'architettura zero trust: monitorare, convalidare e valutare, pianificare, simulare e applicare.

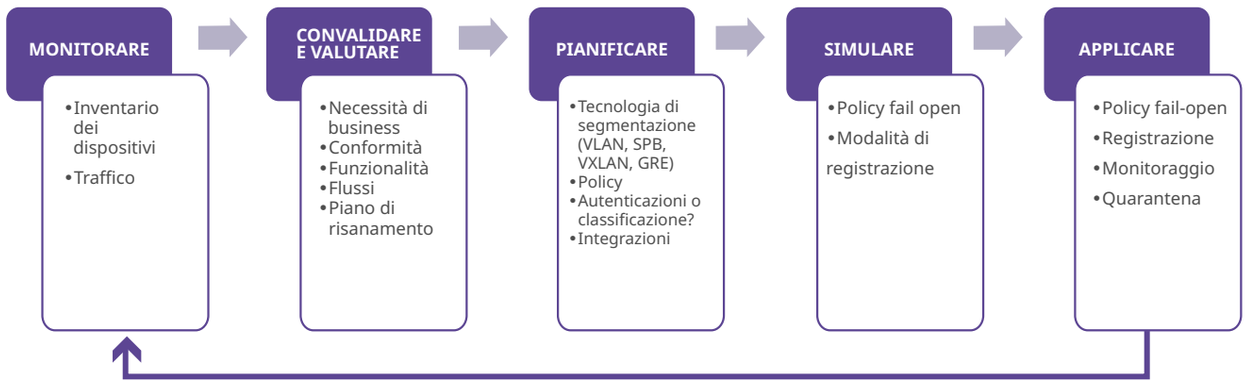


Figura 1 - La metodologia

Step 1: Monitorare

Prima di fare qualsiasi altra cosa è necessario iniziare a monitorare e costruire una mappa e un inventario degli elementi disponibili nella rete.

La migrazione all'architettura zero trust richiede una conoscenza dettagliata degli asset (fisici e virtuali), dei soggetti (inclusi i privilegi degli utenti) e dei processi aziendali che toccano o viaggiano sulla rete. Una conoscenza lacunosa si tradurrà il più delle volte in un fallimento quando l'accesso è negato a causa di informazioni insufficienti. Questo è soprattutto un problema se ci sono "Shadow IT" o "Shadow IoT" sconosciuti all'interno dell'organizzazione.

Bisogna iniziare a monitorare i dispositivi e i flussi di traffico. Creare un report di inventario con tutti i dispositivi visti in rete, suddivisi, tra i vari fattori, per tipo, produttore, modello, sistema operativo. Il report dovrebbe anche mostrare dove e in quale porta dello switch o SSID il dispositivo è stato visto l'ultima volta. Queste informazioni si possono reperire da elementi come l'indirizzo MAC, la firma DHCP e l'HTTP user agent.

La maggior parte degli strumenti di terzi fornirà solo un indirizzo IP e non il tipo di apparecchio. La soluzione ideale sarebbe avere uno strumento per creare un inventario di IoT/dispositivi per facilitare la creazione rapida del profilo NAC per ogni tipo di dispositivo.

L'altra informazione necessaria per la creazione delle policy è costituita dai flussi di traffico. A seconda della dotazione di cui si dispone, è possibile ottenere queste informazioni da strumenti di monitoraggio del flusso come sFlow, Netflow o Deep Packet Inspection (DPI).

Il processo sarà iterativo. La prima volta che si attiva il monitoraggio, i report potrebbero non essere così significativi, ma man mano che si procede verso le altre fasi, assumeranno più specificità e utilità. Le informazioni raccolte in questo passaggio saranno fondamentali per quelli successivi.

Step 2: Convalidare e valutare

Il passo successivo consiste nel convalidare questi risultati. Valutare le esigenze del business. Non è possibile giustificare uno Shadow IoT, ma lo si deve eliminare in quanto aumenta inutilmente la superficie di attacco.
Per il resto è necessario identificare i soggetti (utenti e dispositivi), i flussi di traffico e i flussi di lavoro perché sarà fondamentale inserirli nelle policy. Ad esempio, chi avrà accesso ad asset specifici e cosa gli sarà consentito fare con quegli asset. E applicare il principio del privilegio minimo.
La microsegmentazione non significa attenuare altre strategie di sicurezza come quelle relative alle password o agli aggiornamenti del firmware. Si devono valutare le capacità individuali. Questi dispositivi possono supportare l'autenticazione basata sul certificato? Esiste uno strumento di gestione che consente di rilasciare e applicare questi certificati? Quali sono i flussi di traffico richiesti? Potrebbe essere necessario ottenere queste informazioni dal produttore, ma dovrebbe essere possibile anche confrontarle con i report di analisi del traffico.
Se si osservano asset che non sono conformi alla policy aziendale, occorre attivare un piano di rimedio per renderli conformi, oppure inserire controlli aggiuntivi.

Step 3: Pianificare

In questa fase le risorse, i soggetti (utenti), il traffico e i flussi di lavoro sono già noti. Ora è necessario trasformare questa conoscenza in policy di autenticazione e sicurezza per implementare l'architettura di microsegmentazione richiesta. Come menzionato in precedenza, per ottenere i migliori risultati si dovrebbe studiare una combinazione di macro e microsegmentazione. Tenendo presente che nella maggior parte degli scenari brownfield l'architettura esistente costituirà un limite.

Per la macrosegmentazione, sono disponibili diverse opzioni come VLAN, VRF, SPB VPN, VXLAN o tunnel GRE e funzionalità speciali come le VLAN private. Ognuna di queste soluzioni ha i suoi pro e contro e può essere utile in situazioni diverse. Per la microsegmentazione, è necessario sapere quali policy includere nel profilo per ogni utente o tipo di dispositivo. Infine, è necessario definire come mappare gli utenti e i dispositivi in funzione dei rispettivi segmenti e policy. Questo si riduce all'autenticazione o alla classificazione, che può includere l'impronta digitale sul dispositivo.

La soluzione ideale sarebbe investire in una tecnologia (segmentazione software-defined) che consenta di elaborare policy di autenticazione flessibili in modo da poter aggiornare facilmente i profili di rete.

Suggeriamo di progettare il flusso di autenticazione in questo ordine:

1. Autenticazione tramite certificati 802.1x utilizzando il server RADIUS. L'autenticazione genera un record di autenticazione. Si tratta di informazioni che possono essere condivise con un firewall.
2. Se non si riesce ad autenticare il dispositivo attraverso i certificati 802.1x, si dovrebbe provare l'autenticazione MAC. L'autenticazione MAC non è altrettanto sicura come 802.1x, ma è meglio rispetto all'assenza totale di autenticazione. È opportuno usarla finché non si è pronti a passare a 802.1x.
3. Se non viene recuperato alcun profilo, si può tentare con l'impronta digitale che si può anche usare per mappare un segmento di profilo e di regole. Questo non genera un record di autenticazione o di contabilità, ma viene registrato nel data base dell'inventario IoT.
4. Infine, si può avere un "catch all" predefinito nel caso in cui non vengano recuperati i profili o se tutto il resto fallisce. Nelle prime fasi occorrerà ancora mappare il dispositivo a un profilo che porterà allo stesso segmento e alle stesse regole e registrerà il dispositivo nel data base dell'inventario.

Il flusso dovrebbe essere strutturato in modo flessibile, per poterlo modificare man mano che si procede. Ad esempio, si potrebbe voler eliminare l'autenticazione MAC all'inizio per aggiungerla in seguito, dopo aver ottenuto l'elenco di indirizzi MAC dal report d'inventario. E mentre si perfeziona il processo, si possono, ad esempio, cambiare il segmento e le regole associate al profilo predefinito in regole molto restrittive che consentano l'accesso solo a un bastion host.

Si potrebbe anche voler condividere il ruolo del dispositivo con il firewall in modo che le regole del firewall si possano basare sul ruolo del dispositivo e non solo sulla subnet/sull'indirizzo IP. I vantaggi di questa integrazione sono duplici. In primo luogo, il firewall può applicare policy specifiche a questi dispositivi IoT. In secondo luogo, le policy del firewall sono basate sull'utente o sul ruolo e quindi non sono più vincolate a una subnet o a un indirizzo IP, il che consente una futura riprogettazione e risegmentazione della rete.

Il processo sarà iterativo e occorrerà modificarlo, sintonizzarlo e perfezionarlo man mano che si acquisisce esperienza nell'uso dell'autenticazione e della segmentazione.

Step 4: Simulare

Non importa quanto si pianifichi, è improbabile che la prima volta si riesca a ottenere il risultato desiderato. Qualsiasi errore nella progettazione dello schema di autenticazione, qualsiasi omissione nella policy di sicurezza dell'"elenco consentito" si tradurrà in un processo aziendale interrotto. Si dovranno applicare l'autenticazione e le policy di accesso in modalità "fail open". Questo significa che i dispositivi e gli utenti che non riescono ad autenticarsi saranno ancora ammessi in rete e i flussi di traffico imprevisti saranno ancora permessi. Ma tutto questo sarà registrato e con questi registri sarà possibile perfezionare gli schemi di autenticazione e delle policy.

Step 5: Applicare

Dopo qualche perfezionamento, non si osserveranno autenticazione non riuscite o flussi legittimi rifiutati. Sarà quindi possibile spostare queste policy da "fail open" a "fail close", il che significa che i dispositivi rogue e intrusi saranno bloccati e i flussi inaspettati saranno scartati.
È sottinteso che si dovranno continuare a monitorare eventuali dispositivi e flussi di traffico inaspettati, ripetendo l'intero ciclo se necessario.

Ancora una cosa

Come parte del monitoraggio continuo, della registrazione e della messa in quarantena, si consiglia di investire anche in un sistema esterno di rilevamento delle intrusioni (IDS). Anche se lo switch stesso può identificare una serie di attacchi Distributed Denial of Service (DDoS), un IDS esterno può rilevare una gamma più ampia di attacchi quali virus o altre anomalie. Probabilmente ci si ricorderà dell'episodio di qualche anno fa, quando diverse telecamere di videosorveglianza sono state infettate con il malware Mirai, o del giorno in cui questi dispositivi hanno lanciato un attacco coordinato sui server DNS globali che ha colpito servizi come Twitter, Spotify o Paypal. Questi attacchi potrebbero non essere rilevati dagli switch, ma un IDS dedicato ci riuscirebbe senza ombra di dubbio.
Una volta rilevato l'attacco, l'IDS informa il sistema di gestione della rete (NMS) degli indirizzi IP dei dispositivi colpiti. Lo scenario ideale prevede che il proprio NMS sia in grado di localizzare questi dispositivi nel data base in modo da cambiare i profili in un "ruolo di quarantena".
Il "ruolo di quarantena" è un ruolo molto restrittivo, di norma consentirebbe solo la comunicazione con un bastion host in modo da rafforzare il dispositivo, ad esempio, impostando una password forte, o aggiornando il suo firmware, tra le altre cose.

Perché ALE?

Le soluzioni Digital Age Networking di Alcatel-Lucent Enterprise incorporano una segmentazione software-defined robusta e flessibile con policy DPI NAC dinamiche che permettono un'evoluzione graduale verso un'architettura zero trust.

Digital Age Network è il progetto di Alcatel-Lucent Enterprise che consente a imprese e organizzazioni di entrare nell'era digitale e di accrescere le proprie attività digitali. Si basa su tre pilastri:

- Una Rete Autonoma che connette facilmente, automaticamente e in modo sicuro persone, processi, applicazioni e oggetti. La rete autonoma di ALE si basa su un portafoglio semplificato completo di una piattaforma di gestione unificata, che offre policy di sicurezza comuni in tutta la nostra rete LAN e WLAN. Questa soluzione offre flessibilità di integrazione per ambienti indoor, outdoor e industriali. La gestione della rete può essere fornita in loco, in cloud o in modalità ibrida, a seconda delle preferenze del cliente.
- Implementazione sicura ed efficace dei dispositivi IoT: la segmentazione mantiene i dispositivi nei loro segmenti dedicati e riduce al minimo il rischio di attacchi informatici. La segmentazione IoT aiuta le aziende a capire in modo facile e automatico se un dispositivo si comporta correttamente o meno, mantenendo la sicurezza sulla rete.
- Innovazione dei processi di business attraverso l'automazione del flusso di lavoro: l'integrazione di utenti, applicazioni e metriche di IoT in tempo reale, con dati di geolocalizzazione, in piattaforme di collaborazione, semplifica la creazione e il lancio di nuovi processi e servizi di business digitali automatizzati, tra cui la notifica di amministratori di rete e sicurezza in merito a qualsiasi violazione si verifichi.

Hai uno strumento per creare un inventario IoT/dei dispositivi? Hai uno strumento che ti consente di monitorare i flussi delle applicazioni? Gli attuali switch e gli access point wireless sono predisposti per la segmentazione software-defined? Se attualmente non disponi di questi strumenti, contattaci e saremo lieti di poterti aiutare a ottenerli.

Quello che sappiamo con certezza

Concludiamo con alcuni punti chiave:

- Per disporre di un'architettura zero trust davvero efficiente, occorre affidarsi alla macro e alla microsegmentazione
- Ci sono cinque passaggi da compiere per implementare un'architettura zero trust: monitorare, convalidare e valutare, pianificare, simulare e applicare
- L'architettura zero trust basata sulla microsegmentazione si basa su tre pilastri: autenticazione con 802.1x EAP-TLS come regola principale; policy differenziate associate al ruolo dell'utente o del dispositivo che si rifanno al principio del privilegio minimo; monitoraggio continuo e quarantena.
- Negli ambienti ibridi e mobili, la microsegmentazione deve essere software-defined, cioè deve essere dinamica e basata su policy, non definita staticamente, altrimenti sarebbe impraticabile.

La migrazione verso un'architettura zero trust attraverso la microsegmentazione è un processo ed è improbabile che un'impresa di dimensione significativa raggiunga l'obiettivo con un singolo ciclo di aggiornamento. Ma con ogni aggiornamento o riprogettazione o ciclo di miglioramento continuo è possibile avvicinarsi al traguardo se si adottano l'infrastruttura e la progettazione giuste.

Alcatel-Lucent Enterprise si impegna quotidianamente nello sviluppo di tecnologie e soluzioni di rete che aiutano le aziende a realizzare la propria trasformazione digitale.

Alcatel·Lucent
Enterprise