Costruire una rete zero trust economicamente vantaggiosa

Massimizzare la sicurezza della rete e ridurre al minimo i costi

Solution Brief

Alcatel·Lucent Enterprise

Sicurezza informatica e 'zero trust'

La sicurezza informatica è una preoccupazione sempre più importante, dato che la tecnologia continua a svilupparsi, il numero e la complessità delle minacce informatiche si moltiplicano. Le minacce in rapida evoluzione rendono difficile per le organizzazioni prevederle e difendersi, imponendo agli esperti di cybersecurity di rimanere aggiornati sulle ultime tendenze e vulnerabilità.

Con molte fonti e vettori di attacco diversi, come le e-mail di phishing, il social engineering e le vulnerabilità del software, la difesa dalle minacce informatiche richiede un approccio unico per ogni tipo di attacco.

Può essere difficile identificare e proteggere tutte le potenziali vulnerabilità di un sistema complesso, per cui è fondamentale che gli esperti di cybersecurity comprendano come i diversi sistemi e le varie reti lavorino insieme per sviluppare misure di sicurezza efficaci.

L'errore umano è una causa comune delle violazioni della sicurezza informatica ed entro il 2025 si stima che la mancanza di talento o il fallimento umano saranno responsabili di oltre la metà degli incidenti informatici significativi.[1]

Il rispetto di normative e standard complessi in materia di cybersecurity, come il Regolamento generale sulla protezione dei dati (GDPR) e l'Health Insurance Portability and Accountability Act (HIPAA), è un'altra sfida che richiede conoscenze e competenze specialistiche.

1 Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight, gennaio 2023.

Processo di violazione della sicurezza informatica

La figura in basso mostra le fasi che un aggressore informatico segue per violare una rete e sottrarre dati preziosi. Si inizia con l'esplorazione fase, in cui gli aggressori studiano, individuano e selezionano gli obiettivi e scansionano le vulnerabilità della rete.

La fase successiva è l'armamento o weaponisation, in cui gli aggressori stabiliscono come compromettere un endpoint e fornire un payload weaponised, ossia un carico utile armato.

Successivamente si passa allo sfruttamento, fase in cui l'aggressore attiva il payload armato e aumenta i privilegi sull'endpoint compromesso per spostarsi lateralmente attraverso la rete.

La fase successiva è l'installazione, in cui gli aggressori stabiliscono l'accesso remoto alla struttura e installano il malware per stabilire la persistenza.

Nella fase di comando e controllo, gli aggressori stabiliscono canali di comunicazione crittografati verso i server di comando e controllo per gestire da remoto l'attacco ed eseguire gli obiettivi.

L'ultima fase è quella del movimento laterale e dell'esfiltrazione, durante la quale gli aggressori potrebbero avere obiettivi multipli, tra cui il furto di dati, la distruzione o la modifica di sistemi critici e il denial of service.

La chiave per fermare gli aggressori è individuare precocemente le diverse fasi del ciclo di vita dell'attacco e interromperne lo sviluppo.

Per evitare che ciò accada, occorre adottare una serie di misure quali la gestione delle vulnerabilità e delle patch, il rilevamento e la prevenzione di malware, il blocco delle applicazioni e dei servizi a rischio e la registrazione e il monitoraggio di tutte le attività di rete, degli endpoint e, naturalmente, del cloud.

Dal lato della rete, è necessario implementare tecnologie che forniscano un controllo granulare delle applicazioni e che monitorino il traffico tra le zone o i segmenti in un modello basato sul principio zero trust. Il concetto di zero trust si basa sul principio che tutto deve essere considerato non attendibile per impostazione predefinita.

È stato sviluppato in risposta al crescente numero di sofisticati attacchi informatici alle reti informatiche. Tradizionalmente, le organizzazioni si sono affidate a soluzioni di sicurezza perimetrali, come firewall e software antivirus, per proteggere le proprie reti. Tuttavia, poiché gli attacchi informatici sono diventati più avanzati e complessi, queste soluzioni basate sul perimetro si sono rivelate insufficienti pertanto ogni richiesta di accesso deve essere verificata e autenticata in anticipo.

Fonte: XDR for Dummies, Palo Alto Networks Special Edition, 2022

Promuovere una strategia zero trust

Alcatel-Lucent Enterprise aiuta i clienti ad acquisire maggiore sicurezza e a passare a un ambiente basato sul principio zero trust in modo semplice ed economico. In ALE siamo consapevoli di quanto sia importante implementare un modello zero trust per garantire la sicurezza della rete e dei dati dei nostri clienti. Offriamo una gamma di soluzioni progettate per aiutare le organizzazioni a implementare una rete strutturata secondo l'approccio zero trust e ad affrontare le sfide poste dalle minacce informatiche.

Protezione della rete

Offriamo una rete protetta **- sia all'interno che all'esterno**. Si inizia con un'infrastruttura sicura e garantendo che il dispositivo stesso non sia compromesso. La nostra famiglia di prodotti Alcatel-Lucent OmniSwitch® si affida al sistema operativo Alcatel-Lucent Operating System (AOS), che utilizza un codice diversificato sicuro per proteggere le reti da potenziali vulnerabilità e attacchi. Il codice viene costantemente aggiornato per affrontare minacce attuali e future, con la diversificazione del software attraverso l'Address Space Layout Randomisation (ASLR) utilizzato per proteggere dagli attacchi di buffer overflow. IV&V (Indipendent Verification & Validation) vengono utilizzate anche per analizzare e testare il codice sorgente dell'AOS alla ricerca di potenziali vulnerabilità, backdoor, malware ed exploit di sistema. Esperti di sicurezza informatica di terze parti conducono questi test, eseguiti su immagini di software a disponibilità generale per garantire l'integrità del software.

Applichiamo la macro e microsegmentazione per garantire l'accesso alla rete basata sul principio zero trust. Entrambi sono componenti fondamentali di una strategia di sicurezza zero trust. La **macrosegmentazione** si riferisce alla suddivisione della rete in zone o domini separati in base a funzione, applicazione o gruppo di utenti. Questo fornisce un elevato livello di segmentazione della rete, consentendo alle organizzazioni di isolare le risorse e gli asset critici dal resto della rete. La **microsegmentazione**, invece, si concentra sulla segmentazione della rete a un livello più granulare, fino al singolo utente o dispositivo. Questo approccio fornisce un controllo molto dettagliato sull'accesso alla rete, consentendo alle organizzazioni di applicare i criteri di sicurezza a livello di singolo utente o dispositivo.

Shortest Path Bridging (SPB) e **Universal Network Profiles** (UNP) offrono una potente soluzione per la macro e microsegmentazione delle reti, che rafforzano la sicurezza e le prestazioni limitando la portata dei potenziali attacchi.

SPB è un protocollo di rete di livello 2 che consente un routing multi-path in reti di grandi dimensioni, semplificando al contempo la configurazione e la gestione dell'infrastruttura di rete. Funzionalità come la segmentazione della rete virtuale offrono una maggiore protezione contro gli accessi non autorizzati e gli attacchi informatici. Utilizzando l'SPB nella propria infrastruttura di rete, le organizzazioni possono beneficiare di una maggiore efficienza e sicurezza della rete, contribuendo a raggiungere gli obiettivi di business.

ALE UNP è il controllo dell'accesso basato sul profilo, una potente funzionalità degli switch Alcatel-Lucent Enterprise che consente agli amministratori di rete di creare e gestire profili utente per l'accesso alla rete in base all'identità, alla posizione e al dispositivo. Possono implementare la gestione centralizzata della policy di rete, semplificando la configurazione e l'applicazione della policy stessa. Affidandosi a ALE UNP, le organizzazioni possono incrementare la visibilità, la sicurezza e il controllo della rete, migliorandone al contempo le performance, proteggendo le risorse e riducendo i tempi di inattività.

Insieme, SPB e UNP consentono agli amministratori di gestire e proteggere in modo efficiente la propria infrastruttura di rete:

- Applicare coerentemente le policy in tutta la rete
- Segmentare e isolare i dispositivi IoT da altri dispositivi
- Ridurre al minimo la superficie di attacco della rete

Autenticazione solida

ALE fornisce una solida autenticazione attraverso UPAM (Unified Policy Authentication Manager).

Un fattore fondamentale della sicurezza informatica è l'autenticazione, ovvero il processo di verifica dell'identità di un utente, di un dispositivo o di un sistema. Si tratta di confermare che un utente o un dispositivo è chi dice di essere, di solito fornendo una qualche forma di identificazione, come un nome utente e una password.

La soluzione ALE supporta diversi metodi di autenticazione degli utenti.

- **802.1X**, un protocollo di autenticazione di rete, consente ai dispositivi di connettersi a una rete sicura fornendo credenziali, come un nome utente e una password. Quando un dispositivo tenta di connettersi a una rete utilizzando 802.1X, viene autenticato prima di poter accedere alla rete. In un mondo ideale, l'autenticazione del dispositivo avviene tramite 802.1x. L'autenticazione genera un record che può essere condiviso con un firewall.
- Se il dispositivo non supporta 802.1x, una possibile opzione è l'autenticazione **MAC address**. L'indirizzo MAC è una carta d'identità digitale per ogni dispositivo di una rete. È unico e identifica ogni dispositivo e consente la comunicazione tra le varie unità, simile a una targhetta per il computer o il telefono.
- ALE supporta **l'impronta digitale del dispositivo e del sistema**. Se non viene restituito alcun profilo con l'altra autenticazione 802.1X o MAC, si tenta con l'impronta digitale. L'impronta digitale nella sicurezza informatica è il processo di raccolta di informazioni su un dispositivo o un sistema, come il sistema operativo, il software e le porte aperte, per identificarlo e classificarlo e valutarne potenziali rischi e vulnerabilità. Si può anche usare per mappare il profilo di un dispositivo registrato nel database dell'inventario IoT.
- ALE fornisce anche un "catch all" di default nel caso in cui non venga restituito un profilo. La regola catch-all predefinita può consentire un accesso limitato o negarlo del tutto se l'autenticazione primaria fallisce.

Per eseguire questi diversi tipi di autenticazione occorre un luogo dove creare e gestire le credenziali di utenti e dispositivi. È necessario UPAM, un componente della soluzione ALE Unified Access. Fornisce servizi centralizzati di autenticazione, autorizzazione e gestione degli account (AAA) per la rete. Consente agli amministratori di creare e gestire i profili degli utenti per l'accesso alla rete, in base all'identità e alla posizione, tra le altre cose. UPAM può essere configurato e gestito tramite Alcatel-Lucent OmniVista® Network Management System, consentendo agli amministratori di rete di definire e applicare le policy di accesso alla rete.

Reattività agli incidenti

Rispondere rapidamente agli incidenti di rete è un fattore chiave per ridurre al minimo i danni ai sistemi e alle reti, nonché i tempi di inattività, causati da attacchi di sicurezza come i DDoS (Distributed Denial of Service).

Ridurre al minimo i rischi, massimizzare la qualità dell'esperienza (QoE) e migliorare la sicurezza con Alcatel-Lucent OmniVista Network Advisor. **OmniVista Network Advisor** è un sistema intelligente e autonomo basato sull'intelligenza artificiale che fornisce il monitoraggio della rete in tempo reale, l'emissione di avvisi in caso di problemi e la proposta di soluzioni per varie questioni legate alla rete e alla sicurezza, compresi gli attacchi DDoS. Esegue continuamente verifiche della configurazione e analisi delle prestazioni della rete in modo da **identificare** tempestivamente i potenziali problemi, **ridurli** e **ottimizzare** la rete con un intervento informatico minimo o nullo.

Partnership e integrazioni

Un aspetto importante dell'autenticazione è l'integrazione con i firewall. Ad esempio, grazie all'integrazione con Fortinet, gli utenti o i dispositivi autenticati alle reti LAN e/o WLAN possono essere autenticati contemporaneamente e senza soluzione di continuità anche al firewall Fortinet.

Con l'integrazione del firewall di nuova generazione Palo Alto Networks (PAN), gli utenti o i dispositivi autenticati alle reti LAN e/o WLAN possono essere autenticati contemporaneamente e senza soluzione di continuità anche al firewall PAN.

La nostra partnership con Versa Networks consente un accesso sicuro alle risorse critiche, indipendentemente dalla posizione di utenti, dati, applicazioni o dispositivi. Ciò è particolarmente vantaggioso per le aziende con uffici regionali o filiali distanti dal sito centrale o dal centro dati. A differenza delle reti WAN (Wide Area Network) tradizionali, che richiedono più passaggi di rete che possono comportare costi aggiuntivi, SASE e SD-WAN offrono una soluzione economica e sicura per l'era client-to-cloud. Combinando queste due soluzioni, le aziende possono semplificare la gestione dell'infrastruttura IT e consentire un accesso sicuro a Internet e alle applicazioni aziendali quando si lavorare da qualsiasi luogo, inlcusi azienda/DC, uffici regionali/filiali e lavoro da casa/in movimento.

L'offerta ALE-Versa Titan è una soluzione completa che combina servizi Secure Access Service Edge (SASE) e SD-WAN dal cloud. Questo include Versa Titan SD-WAN, che fornisce una SD-WAN distribuita nel cloud per un IT snello, e Versa Secure Access (VSA), che propone funzionalità firewall di nuova generazione e blocco geografico, oltre a Zero Trust Network Access (ZTNA) per scenari di lavoro da qualsiasi luogo. Inoltre, il Versa Secure Web Gateway (SWG) offre una navigazione web sicura e un accesso alle applicazioni Internet (SaaS) per una connettività sicura da remoto/in home office. Il portale web e l'app Versa Titan offrono servizi integrati di rete e sicurezza su un'unica piattaforma, con tutti i componenti SASE da uno stesso fornitore. Con un unico archivio di policy che comprende i criteri di rete e di sicurezza, le aziende possono semplificare la gestione IT e garantire un accesso sicuro alle risorse critiche.

La metodologia basata sul principio zero trust

Per attuare un modello zero trust, le organizzazioni devono innanzitutto affrontare le problematiche dell'infrastruttura di sicurezza esistente, quali policy incoerenti, affidabilità implicita e dispositivi IoT vulnerabili. Per contrastare questi problemi, l'obiettivo è creare capacità di controllo di accesso alla rete e di accesso basato sul ruolo , di segmentazione e monitoraggio, con un'adeguata segmentazione che consenta di suddividere le risorse sensibili e di limitare l'accesso solo a coloro che lo richiedono. Le funzionalità di monitoraggio e quarantena consentono ai clienti di individuare e isolare le potenziali minacce.

Una metodologia semplice ma efficace per costruire una rete basata sull'approccio zero trust con le soluzioni ALE prevede diverse fasi.

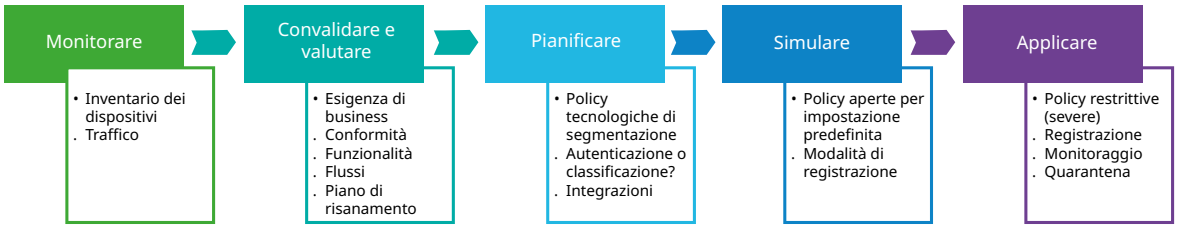
- **Monitoraggio**: è necessario effettuare il monitoraggio, compreso l'inventario dei dispositivi e il traffico.
- **Convalida e valutazione**: la convalida e la valutazione comportano l'analisi delle esigenze aziendali, dei requisiti di conformità, delle capacità e dei flussi.
- **Pianificazione**: occorre creare un piano di correzione in base ai risultati della valutazione. La pianificazione comprende la scelta della giusta tecnologia di segmentazione e delle policy, nonché la considerazione dell'autenticazione rispetto alla classificazione e alle integrazioni.
- **Simulazione**: nella fase di simulazione, le policy sono aperte per impostazione predefinita e in modalità di registrazione e vengono testate altre funzionalità.
- **Applicazione**: questa fase prevede l'attuazione di policy restrittive, la registrazione, il monitoraggio e l'esecuzione di misure di quarantena.

Costo totale di gestione

Il Total Cost of Ownership (TCO) copre tutte le spese associate alla proprietà e al funzionamento di un prodotto o di un servizio per tutta la sua durata. Questi includono, tra l'altro, il prezzo di acquisto, la manutenzione, l'assistenza e gli aggiornamenti. È importante scegliere soluzioni efficaci dal punto di vista dei costi che offrano un valore a lungo termine, in grado di ridurre gli sforamenti di budget e di fornire un ritorno sull'investimento (ROI) più preciso.

È bene tenere presente la distinzione tra l'investimento di capitale iniziale e le spese correnti necessarie per mantenere il sistema autorizzato e operativo. Mentre alcuni componenti, come i firewall, sono puramente incentrati sulla sicurezza, altri sono fondamentali per costruire una strategia di sicurezza più approfondita. Questi includono la gestione delle policy, la tecnologia di separazione efficiente dei percorsi di rete (macro e microsegmentazione avanzata e automatizzata), l'assegnazione automatica di reti virtuali (VLAN), il protocollo di crittografia di rete, la visibilità delle applicazioni e la convalida e attestazione indipendente del codice del sistema operativo.

La strategia di sicurezza informatica di rete di ALE affronta gli elementi essenziali della sicurezza di rete indicati in precedenza senza alcun costo, mentre le alternative di altri fornitori richiedono competenze specifiche nonché licenze e numerosi elementi costosi per il funzionamento e la manutenzione. L'approccio ALE offre ai clienti notevoli vantaggi economici, garantendo al contempo una sicurezza informatica della rete forte ed efficiente.



Conclusioni

È evidente che l'implementazione di una rete basata sul principio zero trust per una sicurezza solida può presentare diverse sfide, come la complessità e il costo in termini di creazione e manutenzione. Tuttavia, ALE offre un approccio unico ed economicamente conveniente per affrontare questi problemi. Le tecnologie avanzate di macro e microsegmentazione, in aggiunta agli altri componenti presentati in questo documento, forniscono un mezzo semplice ed economico per implementare una rete incentrata sull'approccio zero trust che risponda ai moderni requisiti di sicurezza informatica. Siamo impegnati ad aiutare i nostri clienti a risolvere i loro problemi di sicurezza informatica e riteniamo che la nostra strategia possa contribuire a raggiungere l'obiettivo.

Le soluzioni ALE includono i nostri sistemi di resilienza e sicurezza intelligent Fabric (iFab) e UNP, e il robusto Network Access Control (NAC) con UPAM, che fornisce un controllo degli accessi basato sui profili. La nostra innovativa soluzione OmniVista Network Advisor garantisce un funzionamento regolare e un rapido recupero e prevenzione degli attacchi. Inoltre, collaboriamo con fornitori di SASE del calibro di Versa Networks e ci integriamo con fornitori di firewall leader del settore quale Palo Alto Networks per fornire ai clienti soluzioni di sicurezza più complete e integrate.

Alcatel·Lucent Enterprise