Trust della rete Interna al perimetro aziendale

Questo articolo fa parte della serie dedicata al tema dell'architettura Zero Trust. In questo focus esploriamo la ridefinizione del perimetro aziendale nell'era del lavoro remoto e del cloud, analizzando i livelli di fiducia nei segmenti di rete, le tecnologie avanzate per l'implementazione della sicurezza Zero Trust nelle infrastrutture di rete e le strategie di mitigazione dei rischi associati agli attacchi moderni.

La Ridefinizione del Perimetro di Rete nell'Architettura Zero Trust

In questa sezione estendiamo il perimetro di azione e controllo oltre l'utente e il suo dispositivo. Sebbene il perimetro aziendale non sia più limitato al solo perimetro fisico dietro il firewall, a causa del lavoro remoto, delle interazioni con la supply chain e delle estensioni verso il cloud, il concetto di perimetro aziendale rimane comunque rilevante, ma deve essere ridefinito rispetto alle modalità tradizionali.

Il nuovo concetto di perimetro aziendale può essere inteso come il contesto in cui viene eseguita un'autenticazione: ogni volta che ci autentichiamo, ci troviamo all'interno del perimetro aziendale e proiettiamo il nostro dispositivo all'interno di questo perimetro in modo più o meno forte. In questo senso, il perimetro aziendale comprende non solo la rete cablata dell'organizzazione dietro il firewall, ma anche le VPN, i servizi cloud, le reti wireless autenticate e le aree riservate dei siti web aziendali.

Tutto ciò che non rientra in queste definizioni deve essere

considerato come non trusted e, quindi, come una potenziale fonte di rischio. Analogamente a quanto fatto per utenti e dispositivi, anche i segmenti di rete del perimetro devono essere differenziati in base al livello di fiducia.

Una prima suddivisione è tra ciò che è esterno e ciò che è interno al perimetro aziendale, ma all'interno del perimetro stesso esistono ulteriori livelli di fiducia che possiamo classificare come segue:

- **Reti o segmenti di rete a bassa fiducia:** Questi segmenti di rete, pur rientrando all'interno del perimetro aziendale, sono caratterizzati da un basso livello di fiducia, poiché sono popolati principalmente da dispositivi non gestiti dall'organizzazione o soggetti a un'autenticazione debole. Un esempio comune sono le reti Wi-Fi, che richiedono cautele particolari, come l'isolamento dei dispositivi tra loro e l'accesso limitato solo a servizi pubblici o a risorse ben definite. Un altro esempio sono i segmenti di rete in cui vengono posizionati i dispositivi che non hanno ancora soddisfatto le policy di conformità o che non riescono ad autenticarsi con successo con i sistemi di Network Access Control (NAC). Alcune tipologie di VPN possono rientrare in questa categoria, specialmente quando l'autenticazione richiesta è debole e consente l'accesso solo a servizi secondari.
- **Reti o segmenti di rete con livello di fiducia normale**: Questi segmenti consentono il collegamento tra dispositivi all'interno del perimetro aziendale e l'accesso a settori non protetti da ulteriori livelli di firewall. Rappresentano il perimetro normale in cui operano dispositivi e utenti che soddisfano i criteri di sicurezza necessari per essere considerati affidabili.
- **Reti privilegiate o segmenti di infrastruttura:** Questi segmenti di rete sono particolarmente sensibili e limitano l'accesso solo a utenti e dispositivi con

elevati privilegi. Sono generalmente protetti da più livelli di firewall e spesso implementano una micro-segmentazione all'interno delle VLAN per garantire il massimo isolamento. Includono i segmenti dedicati alla gestione dell'infrastruttura, dei servizi di rete, dei sistemi e della sicurezza. L'accesso è spesso consentito solo tramite bastion host o VPN specifiche, anche quando ci si trova all'interno del perimetro aziendale.

Collegarsi fisicamente a una porta di rete cablata, a una rete Wi-Fi o a una VPN non deve garantire un accesso indiscriminato alle risorse più sensibili. Ad esempio, anche se ci si collega alla rete cablata, solo nel caso in cui il dispositivo disponga di certificati adeguati e sia conforme alle policy di conformità, sarà possibile proiettare il dispositivo in una rete con livello di fiducia normale; altrimenti, verrà relegato a un segmento a bassa fiducia fino a quando non saranno soddisfatte tutte le condizioni per una sua promozione.

Evoluzione della Sicurezza di Rete: dal Perimetro Tradizionale allo Zero Trust

L'evoluzione del concetto di perimetro di rete ha portato all'emergere del "Software-Defined Perimeter" (SDP), un approccio che secondo il Cloud Security Alliance offre vantaggi significativi rispetto alle tradizionali architetture di rete. L'SDP implementa il principio "Black Cloud", dove le risorse di rete sono invisibili sia agli utenti interni che esterni fino a quando non viene stabilita un'identità verificata e autorizzata con un dispositivo che rispetti i vincoli relativi alla postura di sicurezza richiesta per l'accesso a quella risorsa.

La diffusione delle tecnologie (SDN) Software-defined

Networking permettono di andare incontro alle necessità di limitazione della visibilità con le tecnologie di micro-segmentazione, componente cruciale del modello Zero Trust, che si sono evolute anche oltre la semplice separazione intra-VLAN; le organizzazioni stanno adottando infatti anche approcci basati su:

1. Identity-Based Micro-Segmentation in cui la segmentazione di rete non viene effettuata solo in base all'IP ma anche all'identità ed agli attributi o metadati di chi cerca di connettersi alla risorsa. L'accesso quindi si basa non solo sull'identità ma anche sulla postura dell'utente collegato in quel momento sulla base dei metadati di riferimento;
2. Intent-Based Networking: Permette di definire policy di sicurezza definite ad alto livello in termini di intenti di business, che sono poi automaticamente convertite in configurazioni di degli apparati di rete.

Il NIST ha recentemente pubblicato linee guida per l'implementazione di "Zero Trust Architecture" (SP 800-207) che enfatizzano l'importanza di:

- Policy Engine centralizzato
- Policy Administrator per l'enforcement delle decisioni
- Policy Enforcement Points distribuiti
- Continuous Diagnostics and Mitigation (CDM)
- Industry Compliance Monitor
- Threat Intelligence Feed
- Network and System Activity Logs
- Data Access Policy

Tecnologie Utili

Per implementare i diversi livelli di sicurezza nell'accesso ai vari segmenti di rete, è possibile utilizzare sistemi di Network Access Control (NAC) che consentono una gestione dinamica degli accessi, proiettando i dispositivi nei segmenti

appropriati in base alla loro postura di sicurezza. Tecnologie VPN, mediate da autenticazione multi-fattore, gestione passwordless o basata su certificati e verifica della postura di sicurezza del dispositivo, possono contribuire a migliorare la sicurezza e garantire l'accesso ai segmenti di rete più sensibili.

L'uso di bastion host o di infrastrutture di Virtual Desktop Infrastructure (VDI) gestite dall'organizzazione rappresenta un'altra tecnologia utile per mediare l'accesso, consentendo che sia il bastion host o la VDI il dispositivo di accesso effettivo, piuttosto che il dispositivo fisico dell'utente. Inoltre l'evoluzione delle architetture di rete moderne ha portato a un significativo ampliamento delle tecnologie disponibili per implementare un modello Zero Trust efficace nel contesto della rete interna.

Di seguito alcuni spunti di approfondimento per tecnologie utili e comunque correlate alla messa in sicurezza ed al controllo dell'accesso alla rete.

Software-Defined Networking (SDN)

L'implementazione di reti definite via software rappresenta un elemento fondamentale per una moderna architettura Zero Trust. Le piattaforme SDN moderne offrono capacità avanzate di:

- Orchestrazione dinamica della rete basata su policy
- Micro-segmentazione adattiva
- Routing intelligente basato sul contesto
- Automazione della configurazione di rete
- Visibilità granulare sul traffico

Le SDN permettono di implementare controlli di sicurezza dinamici che si adattano automaticamente alle condizioni della rete e al comportamento degli utenti. La capacità di programmare dinamicamente gli apparati di rete attraverso API multi-vendor consente l'integrazione con sistemi di sicurezza

e automazione, creando un ambiente di rete più resiliente e adattivo.

Network Detection and Response (NDR)

I sistemi NDR moderni rappresentano un'evoluzione significativa rispetto ai tradizionali IDS/IPS, offrendo:

- Analisi comportamentale del traffico di rete
- Rilevamento di minacce basato su machine learning
- Risposta automatizzata agli incidenti
- Integrazione con threat intelligence
- Capacità di threat hunting
- Analisi forense del traffico di rete

L'NDR permette di identificare e rispondere a minacce sofisticate che potrebbero sfuggire ai controlli tradizionali, fornendo visibilità profonda sul traffico di rete e capacità avanzate di analisi delle minacce.

Secure Access Service Edge (SASE)

L'architettura SASE rappresenta una convergenza tra networking e sicurezza in tutte le situazioni in cui l'infrastruttura aziendale si ibridi fortemente verso il cloud, offrendo:

- SD-WAN integrato con sicurezza
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)
- Firewall as a Service (FWaaS)
- Data Loss Prevention (DLP)

SASE permette di estendere i controlli di sicurezza Zero Trust oltre il perimetro tradizionale, proteggendo gli accessi alle risorse aziendali indipendentemente dalla loro localizzazione, ma in maniera centralizzata e seguendo policy univoche indipendenti dai provider e dalla localizzazione.

Network Access Control (NAC) di Nuova Generazione

I sistemi NAC moderni hanno evoluto le loro capacità includendo:

- Posture assessment continuo
- Integrazione con sistemi EDR/XDR
- Orchestrazione automatizzata delle policy
- Quarantena dinamica
- Remediation guidata
- Profiling IoT avanzato

Questi sistemi permettono un controllo granulare degli accessi alla rete basato non solo sull'identità ma anche sullo stato di sicurezza dei dispositivi e sul contesto dell'accesso.

Microsegmentation Platforms

Come riportato in precedenza le piattaforme di micro-segmentazione moderne con il contributo in alcuni contesti dei firewall distribuiti, offrono:

- Segmentazione basata sull'identità
- Policy automation e orchestration
- Visualizzazione delle dipendenze applicative
- Analisi del rischio in tempo reale
- Enforcement distribuito delle policy
- Integrazione con cloud native security

La micro-segmentazione permette di implementare un modello Zero Trust granulare, limitando efficacemente la superficie di attacco e il potenziale impatto di una compromissione.

Cloud Native Network Security

Per le architetture cloud native, sono disponibili tecnologie specifiche come:

- Service mesh security
- Container network security
- Kubernetes network policies
- API gateway security
- Serverless security controls
- Cloud workload protection

Queste tecnologie permettono di estendere i controlli Zero Trust agli ambienti cloud moderni, mantenendo coerenza nelle policy di sicurezza.

Hybrid Cloud Networking

Per ambienti ibridi, sono essenziali tecnologie che permettono:

- Network connectivity management
- Multi-cloud networking
- Transit gateway security
- Cloud interconnect security
- Hybrid cloud segmentation
- Policy consistency across environments

Queste soluzioni permettono di mantenere un modello di sicurezza coerente attraverso diversi ambienti cloud e on-premise.

Network Performance Monitoring and Diagnostics (NPMD)

I sistemi NPMD moderni integrano funzionalità di sicurezza come:

- Network behavior analytics
- Performance baseline monitoring
- Anomaly detection
- Application performance correlation
- Network forensics
- Capacity planning

L’integrazione di monitoring avanzato permette di identificare rapidamente anomalie che potrebbero indicare problemi di sicurezza.

L’orchestrazione efficace di queste tecnologie richiede una piattaforma di gestione centralizzata che permetta:

- Policy management unificato
- Visibilità end-to-end
- Automazione dei workflow di sicurezza
- Reporting integrato
- Analisi predittiva
- Gestione degli incidenti

La chiave per il successo sta nella capacità di integrare queste diverse tecnologie in modo coerente, creando un ecosistema di sicurezza che possa adattarsi dinamicamente alle minacce emergenti mentre mantiene la semplicità operativa necessaria per una gestione efficace.

Rischi mitigati

La moderna architettura Zero Trust applicata alla rete interna permette di mitigare una gamma sempre più ampia di rischi di rete, che si sono evoluti significativamente con la digitalizzazione delle organizzazioni e l’emergere di nuove minacce.

I Movimenti Laterali consistono nella capacità di un attaccante di muoversi lateralmente all’interno della rete una volta ottenuto l’accesso iniziale e rappresentano una delle minacce più significative per le organizzazioni moderne, in quanto l’attaccante non cerca di forzare direttamente i sistemi di sicurezza centrali, ma inizia ad infiltrarsi tramite vulnerabilità di sistemi satellite per poi spostarsi verso i sistemi di interesse.

L’implementazione di controlli Zero Trust a livello di rete mitiga questo rischio attraverso diversi meccanismi. La micro-

segmentazione dinamica, combinata con policy basate sull'identità, crea barriere efficaci che impediscono agli attaccanti di espandere il loro raggio d'azione anche se riescono a compromettere un singolo segmento. Il monitoraggio continuo del traffico di rete permette di identificare pattern di movimento anomali che potrebbero indicare un tentativo di movimento laterale in corso.

L'implementazione di un sistema di Network Access Control (NAC) permette di limitare e segmentare l'accesso alla rete sulla base di una valutazione dinamica della postura di sicurezza sia dell'utente che del dispositivo, indipendentemente dal mezzo di connessione. Questo approccio consente di garantire che l'accesso sia circoscritto unicamente alle aree e ai segmenti di rete coerenti con il livello di sicurezza rilevato. Nel caso in cui una porta di rete rimanesse attiva per errore, qualsiasi utente che tenti di connettersi non acquisirà privilegi superiori unicamente per il fatto di essersi collegato fisicamente. L'accesso sarà infatti regolato attraverso verifiche in tempo reale dell'identità dell'utente e del livello di fiducia assegnato alla postura di sicurezza del dispositivo.

Diversi rischi possono essere mitigati con la corretta applicazione di una logica zero trust a livello di rete.

Advanced Persistent Threats (APT)

Le APT rappresentano una minaccia sofisticata che richiede una strategia di mitigazione complessa proprio perché una volta infitrati nella rete possono rimanere silenti per un lungo periodo andando quindi a rendere più difficoltosa la correlazione di eventi lontani nel tempo.

L'architettura Zero Trust moderna fornisce protezione attraverso:

- Rilevamento precoce di comportamenti anomali nella rete

- Identificazione di comunicazioni Command & Control
- Blocco di tecniche di evasione avanzate
- Prevenzione dell’esfiltrazione dei dati attraverso canali nascosti

La combinazione di questi controlli rende significativamente più difficile per un APT stabilire una presenza persistente nella rete senza essere individuato.

Attacchi alla Supply Chain

Gli attacchi attraverso la supply chain, come dimostrato da incidenti recenti, possono bypassare i controlli di sicurezza tradizionali. L’architettura Zero Trust mitiga questo rischio attraverso:

- Isolamento dei fornitori in segmenti di rete dedicati
- Monitoraggio continuo delle comunicazioni con i fornitori
- Controlli granulari sugli accessi dei partner
- Rilevamento di comportamenti anomali nelle interazioni con la supply chain

Minacce Insider

Le minacce interne, sia malintenzionate che accidentali, vengono mitigate attraverso:

- Visibilità completa sul traffico di rete interno
- Controlli granulari sugli accessi alle risorse
- Identificazione di pattern di accesso anomali
- Prevenzione dell’accesso non autorizzato a risorse sensibili

Man-in-the-Middle e Attacchi di Rete

Gli attacchi di rete tradizionali vengono mitigati attraverso:

- Crittografia end-to-end delle comunicazioni

- Autenticazione forte di tutti gli endpoint
- Controllo dell’integrità delle comunicazioni
- Prevenzione dello spoofing di rete

Rischi legati al Cloud e agli Ambienti Ibridi

La migrazione verso il cloud introduce nuovi rischi che vengono mitigati attraverso:

- Controlli di sicurezza coerenti tra ambienti on-premise e cloud
- Visibilità centralizzata sul traffico multi-cloud
- Policy di sicurezza unificate per tutti gli ambienti
- Protezione delle interconnessioni cloud

Attacchi DDoS e Volumetrici

- Gli attacchi volumetrici vengono mitigati attraverso:
- Distribuzione intelligente del traffico
- Capacità di assorbimento degli attacchi
- Filtri anti-DDoS distribuiti
- Protezione delle applicazioni critiche

Rischi legati all’IoT e OT

La proliferazione di dispositivi IoT e OT introduce nuovi rischi che vengono mitigati attraverso:

- Segmentazione dedicata per dispositivi IoT/OT
- Monitoraggio comportamentale specifico
- Controlli di accesso basati sul profilo del dispositivo
- Protezione dalle vulnerabilità specifiche IoT/OT

Data Exfiltration

Il rischio di esfiltrazione dei dati viene mitigato attraverso:

- Monitoraggio avanzato del traffico di rete

- Identificazione di canali di comunicazione non autorizzati
- Controlli DLP integrati nella rete
- Prevenzione dell’uso di protocolli non autorizzati

Zero-Day Exploits

La protezione contro minacce sconosciute viene implementata attraverso:

- Analisi comportamentale del traffico
- Identificazione di anomalie nella rete
- Risposta automatica alle minacce emergenti
- Isolamento rapido delle minacce sconosciute

Rischi di Compliance

La conformità normativa viene garantita attraverso:

- Logging completo delle attività di rete
- Segregazione efficace dei dati regolamentati
- Controlli di accesso conformi alle normative
- Reporting automatizzato per audit

L’efficacia di queste mitigazioni dipende dalla capacità dell’organizzazione di mantenere una visibilità continua sulla propria rete e di rispondere rapidamente alle minacce emergenti. L’approccio Zero Trust alla sicurezza della rete deve evolversi continuamente per affrontare nuove classi di minacce, mantenendo al contempo l’equilibrio tra sicurezza e funzionalità operativa.

In questo approfondimento abbiamo esaminato il ruolo cruciale del Network Trust nell’architettura Zero Trust, evidenziando come la segmentazione avanzata della rete e le tecnologie di nuova generazione possano mitigare significativamente i rischi di movimenti laterali e altre minacce sofisticate. Nel prossimo articolo della serie esploreremo il Trust delle Applicazioni e dei privilegi essenziali, un altro elemento

fondamentale nell’ecosistema Zero Trust. Per una comprensione più approfondita dell’integrazione di tutti questi elementi in una strategia Zero Trust coerente, vi invitiamo a scaricare il white paper del Dott. Ing. Fabrizio Fioravanti “Zero Trust: solo un problema tecnologico?” che offre prospettive innovative sull’implementazione di questi principi nelle organizzazioni moderne.

Profilo Autore



Fabrizio Fioravanti è attualmente responsabile dell’Unità di Processo Sistemi, tecnologie cloud e di sicurezza informatica presso l’Università degli Studi di Firenze.

Laureato in Ingegneria Elettronica, ha successivamente conseguito il dottorato di ricerca in Ingegneria Informatica e delle Telecomunicazioni e da oltre 25 anni lavora nel settore ICT.

Ha diverse pubblicazioni scientifiche al suo attivo sia su riviste italiane che internazionali, sia che in conferenze, oltre a monografie complete o contributi a monografie.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/trust-della-rete/