SOPHOS
Cybersecurity delivered.

Perché ZTNA È Importante: Il Futuro Della Protezione Della Rete

ZTNA protegge l'accesso remoto e difende i sistemi dal ransomware

Whitepaper Sophos. Febbraio 2022

Il rischio e l'attendibilità sono le due misure su cui si basa la cybersecurity. È giusto considerare attendibile l'utente che si è appena connesso alla rete? E quello che sta provando ad accedere alle applicazioni aziendali? Poi ci sono i messaggi e-mail che sembrano essere stati inviati dal tuo business partner, ma che contengono richieste insolite, il che probabilmente indica un attacco di tipo Business Email Compromise. Uno slogan degli anni '80 diceva "fidati ma verifica". Oggi la tendenza è cambiata in "non fidarti mai, verifica tutto".

Nel modello Zero Trust, chiunque si trova all'interno della rete deve autenticarsi per ottenere l'accesso, ma c'è di più: per qualsiasi tentativo di accedere a una risorsa di rete (ad esempio un server, un'applicazione o dei dati), anche il dispositivo utilizzato per accedere alla risorsa va esaminato ai fini della conformità, e successivamente deve essere ri-autenticato e convalidato a ogni nuova richiesta.

Dal punto di vista della cybersecurity, l'attendibilità va guadagnata, non regalata. Ogni volta che l'utente, il dispositivo e l'applicazione cercano di effettuare un'azione nella rete, il processo di autenticazione deve essere nuovamente eseguito.

Che cos'è ZTNA?

Zero Trust Network Access (ZTNA) si basa sui principi dell'approccio Zero Trust, il cui motto è "mai fidarsi di niente, meglio controllare tutto". Il risultato è una sicurezza superiore, grazie al fatto che ogni singolo utente, applicazione e dispositivo viene considerato come un perimetro a sé stante nel proprio microsegmento di rete, la cui identità e integrità vanno costantemente valutate e verificate, prima che ottenga l'accesso ad applicazioni e dati aziendali. Gli utenti possono accedere solamente alle applicazioni e ai dati definiti esplicitamente nelle loro policy, riducendo così i movimenti laterali e i potenziali rischi che tali movimenti implicano.

Le persone che sono cadute vittima del ransomware conoscono molto bene l'approccio ZTNA, probabilmente motivate dal desiderio di prevenire attacchi futuri. Approfondiremo questo concetto e osserveremo come viene considerata la tecnologia ZTNA dagli utenti Sophos più avanti in questo documento.

ZTNA è un componente essenziale per il framework di sicurezza Secure Access Service Edge (SASE), che descrive come rete e cloud security stanno convergendo in un'unica piattaforma basata sul cloud. SASE, un concetto descritto per la prima volta da Gartner nel 2019, è essenzialmente la fusione tra la gestione della Wide Area Network (WAN) e le funzionalità di sicurezza che sfruttano architetture native del cloud. Oltre a ZTNA, l'architettura SASE include broker di sicurezza per l'accesso al cloud, firewall-as-a-service, sistemi di prevenzione delle intrusioni e gateway di accesso sicuro.

La gestione dal cloud offre enormi vantaggi: consente di utilizzare subito la soluzione, presenta un'infrastruttura di gestione dalle dimensioni ridotte, offre opzioni di distribuzione e registrazione e permette di accedere da qualsiasi posizione. Uno dei vantaggi principali della gestione dal cloud è la possibilità di cominciare subito dopo aver effettuato il login, senza bisogno di aggiungere altre infrastrutture o altri server di gestione. La gestione dal cloud offre inoltre accesso sicuro e immediato da qualsiasi luogo e su qualsiasi dispositivo, per una modalità di lavoro più flessibile. In aggiunta, semplifica il processo di registrazione di nuovi utenti, indipendentemente da dove si trovino.

Tuttavia, l'implementazione di ZTNA è un fattore essenziale per incrementare la protezione degli utenti remoti, nonché un miglioramento importante per la sicurezza negli ambienti di rete caratterizzati dalla presenza di utenti remoti, che sono diventati più comuni a causa della pandemia. Inoltre, protegge la rete aziendale dagli attacchi malware e ransomware.

Anatomia del pericolo della VPN

Per quanto sia stata terribile la pandemia dal punto di vista umano, tecnologicamente ha avuto l'inatteso ma importante vantaggio di migliorare l'accesso remoto, grazie all'implementazione di ZTNA come sostituto della vulnerabile VPN. La pandemia ha costretto milioni di dipendenti a lasciare la sicurezza degli ambienti di rete aziendali e lavorare da casa, introducendo l'uso di milioni di nuovi endpoint vulnerabili e spesso impossibili da controllare per i responsabili IT.

Questi endpoint sono ottimi bersagli per i cybercriminali, poiché nella maggior parte dei casi potrebbero non essere protetti da sistemi di sicurezza endpoint di classe enterprise. Inoltre, i milioni di nuovi utenti improvvisamente creati hanno avuto un impatto molto pesante sulle VPN aziendali, che raramente avevano dovuto gestire carichi di lavoro così elevati.

ZTNA applica i principi dell'approccio Zero Trust e allo stesso tempo offre un'alternativa alla questione spinosa delle VPN, che rappresentavano il metodo tradizionale con cui si connettevano gli utenti remoti alla rete aziendale. Dal punto di vista tecnologico, le VPN presentano tre gravi svantaggi per la moderna forza lavoro remota.

Prima di tutto, le VPN non sono progettate per essere utilizzate su vasta scala, quindi non riescono a soddisfare le esigenze delle imprese di grandi dimensioni, che hanno un numero elevato di dipendenti che lavorano da remoto. In secondo luogo, il software client delle VPN è spesso obsoleto, non aggiornato e complicato, e queste caratteristiche lo rendono un bersaglio facile per gli hacker. Inoltre, le VPN tendono a presentare vulnerabilità di sicurezza, poiché sono state progettate per utilizzare il tradizionale approccio nome utente/password. Infine, gli utenti che riescono ad accedere a una rete tramite VPN hanno piena libertà di movimento una volta connessi: un po' come succederebbe se utilizzassero una workstation situata all'interno del perimetro del firewall. A seconda di come funzionino i controlli di rete interni, questo potrebbe comportare dei rischi.

Procediamo ora ad analizzare uno per uno questi problemi e come possono essere risolti con ZTNA.

Le VPN non offrono una buona scalabilità: presentano limitazioni quali una larghezza di banda massima (spesso a 1 Gbps per le VPN), porte esposte che possono essere attaccate dai cybercriminali, il rischio di subire attacchi Man-in-the-Middle o di utenti che accedono con privilegi eccessivi. Inoltre, le VPN sono realizzate per gestire un volume di utenti remoti specifico, che non può essere aumentato o diminuito dinamicamente. Se il volume è troppo elevato, alcuni utenti non potranno accedere alla VPN fino a quando altri utenti non verranno disconnessi.

In secondo luogo, l'U.S. National Security Agency ha incluso le vulnerabilità delle VPN in diversi avvisi di cybersecurity nel corso degli anni; inoltre, nel 2019 il Canadian Centre for Cyber Security ha pubblicato una serie di consigli, indicando che tre dei prodotti VPN più diffusi presentavano indicatori di compromissione nel rilevamento delle attività pericolose, tra cui casi di ripristino delle credenziali e vulnerabilità in protocolli VPN SSL e TLS proprietari.

Infine, le VPN non offrono filtri, una volta che hanno concesso a un utente l'accesso alla rete. Essenzialmente, l'utente ha tutti i privilegi che avrebbe se utilizzasse una workstation all'interno del perimetro del firewall aziendale.

Il rischio che gli strumenti di accesso remoto vengano utilizzati da un cybercriminale per ottenere libertà di movimento in una rete può essere mitigato in due modi: prima di tutto, facendo in modo che ogni accesso alla rete richieda l'autenticazione dell'utente, del dispositivo e del software solo per un microsegmento specifico e limitato della rete. In questo modo, anche se un hacker dovesse riuscire ad accedere, i suoi movimenti saranno limitati. In secondo luogo, occorre ridurre significativamente i privilegi di chiunque sia connesso alla rete. Se l'hacker non ha i privilegi necessari per ottenere visibilità completa sulla rete, non potrà muoversi al suo interno.

Secondo il report The Forrester NewWave: Zero Trust Network Access, Q3 2021: "Con ZTNA, gli utenti possono accedere alle applicazioni interne secondo i principi dell'approccio Zero Trust, mantenendo la connessione diretta a Internet per il traffico bidirezionale delle chiamate di videoconferenza; questo sistema migliora sia il profilo di sicurezza che l'esperienza dei dipendenti". "In ultima analisi, ZTNA riduce il bisogno di VPN per i dipendenti, mentre per i responsabili delle infrastrutture e della sicurezza prepara il terreno per l'adozione di opzioni di rete e di sicurezza basate sul cloud".

Lo Zen di ZTNA

Dalla prospettiva della governance aziendale, la gestione degli utenti che si possono connettere alla rete e delle loro azioni è una delle sfide principali per un'impresa. Lo scopo della governance aziendale è applicare sia politiche e procedure che definiscono la modalità operativa di una società, sia pratiche commerciali valide ed etiche, volte a garantirne la solidità finanziaria. Nelle reti potrebbero esserci hacker liberi di spostarsi e di compromettere o esfiltrare dati; questi cybercriminali potrebbero installare ransomware e altri programmi di malware, o semplicemente restare in agguato, in attesa del momento più opportuno per sferrare un attacco. Tutto questo rischia non solo di violare le normative sulla conformità, implicando costi molto elevati per l'azienda, ma anche di abbassare notevolmente il suo valore di mercato.

L'implementazione di un modello di rete Zero Trust in generale e ZTNA in particolare può aiutare a identificare gli intrusi presenti nella rete, distinguere le applicazioni pericolose da quelle innocue e individuare gli utenti illegittimi; inoltre, può anche diminuire significativamente la superficie di attacco di una rete aziendale, migliorando ulteriormente il profilo di rischio complessivo dell'organizzazione.

Quando gli utenti effettuano l'accesso a una rete aziendale nella quale è stato implementato l'approccio ZTNA, l'accesso dei dispositivi alle risorse della rete all'interno del perimetro microsegmentato corrispondente viene continuamente convalidato e verificato. Con Zero Trust, gli utenti non sono più "all'interno della rete aziendale", liberi di usufruire di tutto l'accesso e dell'attendibilità implicita che ne derivano. L'accesso viene invece consentito solo alle parti della rete per i quali gli utenti e i dispositivi hanno eseguito l'autenticazione. Le connessioni VPN non funzionano in questo modo.

In una rete tradizionale, nella quale i firewall aziendali bloccano gli hacker ma le difese sono scarse, una volta che le credenziali di un utente vengono accettate, i cybercriminali possono circolare liberamente, alla ricerca di credenziali con privilegi più elevati da sfruttare per accedere alle parti meno accessibili della rete e per trovare dati da rubare, copiare, compromettere o cifrare nel tentativo di estorcere un riscatto.

L'implementazione di un'infrastruttura Zero Trust non riduce solamente il valore delle credenziali sottratte, ma aggiunge al firewall aziendale numerosi altri sistemi di difesa per proteggere dati e applicazioni. Anche se il computer di un dipendente in smart working dovesse essere compromesso, le credenziali dell'utente non daranno all'hacker carta bianca nella rete aziendale estesa.

Grazie all'approccio ZTNA, il cybercriminale avrà invece accesso solo a una parte limitata della rete, e in ogni caso solo ad applicazioni e dati autorizzati, sempre ammesso che disponga delle credenziali per autenticare sé stesso, il suo dispositivo e il software.

Superare gli attacchi ransomware

Secondo il report Sophos La Vera Storia Del Ransomware 2021, il 37% delle persone intervistate ha subito un attacco ransomware l'anno precedente, e il 54% di loro sostiene che i cybercriminali sono riusciti a cifrare i dati. Dal punto di vista della perdita dei dati, ci sono buone notizie, in quanto il 96% dei partecipanti al sondaggio dichiara di avere recuperato almeno parte dei dati. Tuttavia, la cattiva notizia è che di solito il pagamento di un riscatto non permette alle vittime di recuperare tutti i dati, con una percentuale di dati ripristinati dopo il pagamento che raggiunge solo il 65%.

Secondo il report, la somma media dei pagamenti di riscatto delle organizzazioni di medie dimensioni nel 2020 ammonta a 170.404 USD. Tuttavia, questa costituisce solo parte del costo complessivo sostenuto per rimediare ai danni. La spesa media per rimediare all'impatto dell'attacco di ransomware più recente (inclusi tempi di inattività, ore di lavoro del personale, costi associati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto e altri) è pari a 1,85 milioni di USD, più del doppio rispetto ai 761.106 USD del 2020.

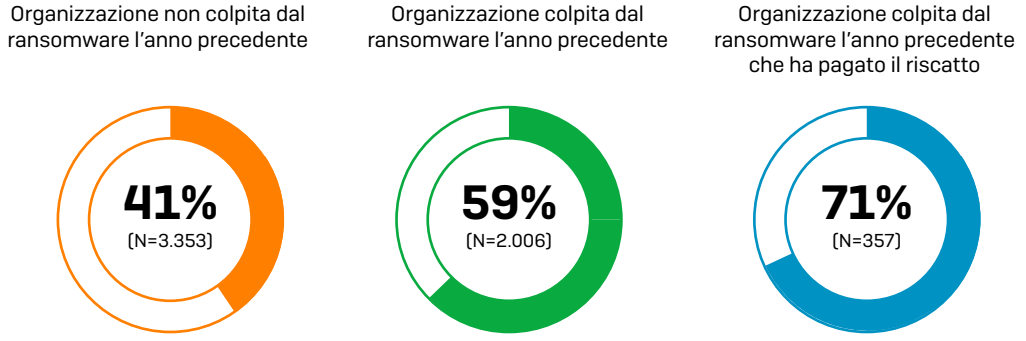
Da un recente sondaggio condotto da Vanson Bourne e commissionato da Sophos, a cui hanno partecipato 5.400 responsabili IT in tutto il mondo, è emerso che il 20% degli intervistati ha già implementato un approccio Zero Trust, mentre un ulteriore 41% sostiene di avere cominciato a implementare Zero Trust, con la prospettiva di completare l'attuazione entro i primi mesi del 2022. Un altro 20% dei partecipanti al sondaggio prevede di farlo entro l'inizio del 2023.

Con le soluzioni ZTNA viene eliminato un vettore di attacco frequentemente utilizzato dal ransomware e da altri attacchi di infiltrazione nella rete. Poiché gli utenti ZTNA non sono più "all'interno della rete", ma piuttosto in un microsegmento della rete aziendale, le minacce che un tempo, con le VPN, avrebbero avuto un appiglio iniziale per l'intera rete non potranno andare da nessuna parte con ZTNA.

Gli attacchi ransomware favoriscono l'adozione dell'approccio ZTNA

Il sondaggio indica che, l'anno scorso, i professionisti IT che lavorano in organizzazioni colpite da attacchi malware hanno quasi il 50% di probabilità in più di avere "molta familiarità" con l'approccio ZTNA rispetto alle organizzazioni che non avevano subito un attacco (59% vs 39%). Questa statistica sale fino a raggiungere il 71% tra le organizzazioni che hanno pagato il riscatto dopo esserne state colpite.

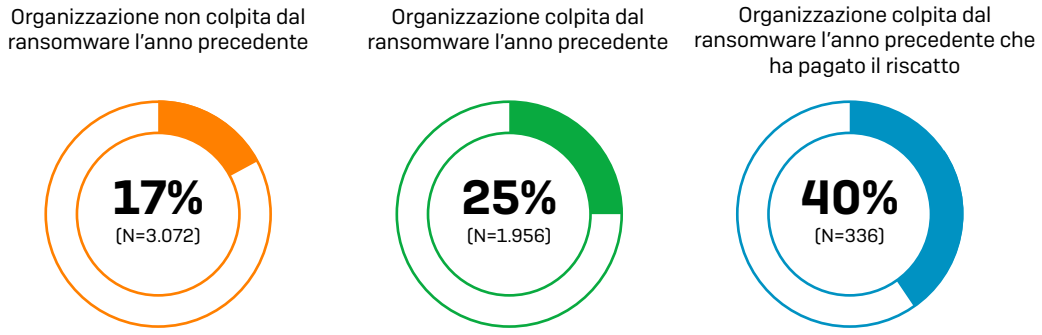
Percentuale degli intervistati che dichiara di avere "molta familiarità" con l'approccio Zero Trust Network Access (ZTNA)



A ulteriore dimostrazione di questo, solo il 10% delle vittime del ransomware dichiara di avere poca o nessuna familiarità con ZTNA, rispetto al 21% degli intervistati la cui organizzazione non ne era stata colpita.

Dal sondaggio emerge anche che chi ha subito un attacco ransomware presenta un maggiore tasso di adozione di Zero Trust. Un quarto (25%) delle organizzazioni che avevano subito un attacco ransomware l'anno precedente ha già implementato un approccio Zero Trust completo, mentre la percentuale sale al 40% tra le organizzazioni che oltre a essere state colpite hanno pagato anche il riscatto. Solo un'organizzazione su sei (17%) tra quelle che invece non avevano subito un attacco ha già effettuato la migrazione completa a questo approccio.

Percentuale degli intervistati la cui organizzazione ha già adottato un approccio Zero Trust



Inoltre, le vittime del ransomware sembrano essere spinte da motivazioni diverse per l'adozione di ZTNA.

- Agli intervistati sono stati chiesti i motivi per cui hanno adottato un approccio Zero Trust e, sebbene ci siano molti punti in comune, sono emerse anche differenze molto nitide. "Per migliorare il nostro profilo di sicurezza complessivo" è stata la risposta più comune sia tra chi aveva subito un attacco ransomware, sia tra chi non ne era mai caduto vittima
- La seconda risposta più comune tra chi era stato colpito dal ransomware è stato il desiderio di "semplificare le nostre operazioni di cybersecurity" (43%), potenzialmente dovuta a un'esperienza negativa in cui l'attacco era stato aggravato dalla complessità della protezione
- Tra le ex vittime del ransomware si è anche riscontrato il maggior numero di risposte "per passare da un modello CAPEX a OPEX", come motivo principale dell'adozione dell'approccio Zero Trust (27% vs 16%, salendo fino al 34% tra le vittime del ransomware che hanno pagato il riscatto)
- Gli intervistati che erano stati colpiti dal ransomware sono anche motivati dal voler "favorire il passaggio a un maggiore utilizzo del cloud" (42%). La percentuale scende al 30% tra chi non aveva subito un attacco recente

Uno sguardo al futuro

I vantaggi di un ambiente Zero Trust possono essere difficili da esporre al consiglio di amministrazione e agli azionisti, in quanto può essere complicato dimostrare che un attacco non ha avuto conseguenze gravi o che non si è verificato solo perché il cybercriminale era stato bloccato prima di avere la possibilità di installare il malware. Detto questo, si può dimostrare che Zero Trust riduce significativamente il rischio, e che la riduzione del rischio può essere monetizzata dall'impresa.

Un minore rischio aziendale può diminuire i costi assicurativi e migliorare i termini delle cyberassicurazioni; inoltre può incrementare il valore stimato dell'organizzazione. Broker assicurativi e assicuratori riconoscono che una riduzione del rischio corrisponde a un minore numero di richieste di indennizzo e quindi anche di pagamenti. Di conseguenza, il settore delle cyberassicurazioni sta rivalutando e modificando i termini di questi tipi di polizze, concedendo appunto condizioni più vantaggiose alle aziende impegnate proattivamente a mitigare i propri rischi.

Il decreto presidenziale statunitense sul miglioramento della cybersecurity nazionale, emesso dal presidente Joseph Biden a maggio del 2021, indica che il governo federale deve "adottare pratiche ottimali di sicurezza [e] muoversi verso un'architettura Zero Trust...". L'adozione di un modello Zero Trust da parte del principale datore di lavoro degli Stati Uniti sottolinea come questo approccio venga riconosciuto come il metodo più efficace per diminuire il rischio.

Anche Gartner concorda sul fatto che Zero Trust è il futuro della cybersecurity. "Sia per le imprese di grandi dimensioni che sono già a buon punto nel loro processo di migrazione verso il cloud che per quelle che lo hanno appena cominciato, la protezione dei dati deve essere una delle priorità principali", sostiene l'azienda. Secondo Gartner, l'82% delle organizzazioni ha da tempo in programma di concedere ai dipendenti la possibilità di lavorare da remoto. "Con aziende che cominciano sempre di più a incorporare lo smart working nei propri progetti a lungo termine, la sicurezza ha assunto maggiore priorità. Tuttavia, molte organizzazioni cominciano a capire che gli approcci tradizionali alla sicurezza non sono idonei per una forza lavoro remota che usa il cloud nativamente", indica Gartner.

Anche Forrester è d'accordo, sostenendo che, invece della rete fisica, Zero Trust protegge le risorse. "Nelle sue forme più semplici, il modello Zero Trust si concentra meno sui vari tipi di autenticazione e controllo degli accessi, focalizzandosi invece sul controllo degli archivi dei dati, delle applicazioni, dei sistemi e delle reti", scrive Forrester. "Questi tipi di controllo sfruttano le identità, concedono e rimuovono le autorizzazioni degli utenti e negoziano il loro accesso in base a ruoli ben definiti".

Se il futuro è Zero Trust, tutto comincia dal controllare chi si trova sulla rete, a che cosa può accedere e come. Questa è la *raison d'être* di ZTNA e il motivo per cui è fondamentale per il futuro della cybersecurity.

Per saperne di più, visitate:
sophos.it/ztna

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

22-02-06 IT (MP)

SOPHOS