FORTINET

WHITE PAPER

La promessa della SD-WAN è realizzabile in ambienti OT

Panoramica preliminare

La digitalizzazione della tecnologia operativa (OT) rende sempre più importante mantenere solide connessioni a Internet e al cloud. La SD-WAN (Software-Defined Wide-Area Network) sta emergendo come una potenziale soluzione per sostituire le lente e costose infrastrutture WAN tradizionali. Ma poiché le tecnologie informatiche collegate a Internet (IT) si fondono sempre più con l'OT, le organizzazioni devono affrontare la necessità di una maggiore visibilità di tutte le sedi dislocate in diversi luoghi geografici, della distribuzione remota e di una più facile gestione delle soluzioni. Forse l'aspetto più critico di tutti, però, è il potenziamento dei controlli di sicurezza per proteggersi da un numero crescente di attacchi specifici per l'OT.

La convergenza IT/OT crea nuove capacità e nuovi rischi

A livello di industria, produzione e infrastrutture critiche, i sistemi OT stanno convergendo sempre più verso le tecnologie IT per consentire nuove efficienze e capacità. Questa crescente intersezione, tuttavia, sta determinando la necessità di nuovi strumenti e soluzioni per affrontare la diversa natura dell'OT.

La digitalizzazione comporta maggiore complessità e maggiore esposizione al rischio per le organizzazioni OT connesse. Di conseguenza, i responsabili dell'OT ora hanno bisogno di una visione olistica dell'infrastruttura di rete estesa dell'organizzazione. La maggioranza (78%) delle organizzazioni oggi ha una visibilità centralizzata dei propri ambienti OT solo parziale.[1] Senza una visibilità completa, qualsiasi parte dell'infrastruttura che non può essere vista non può essere protetta.

A seguito della diffusa convergenza IT/OT, l'"air gap" che teneva al sicuro i sistemi OT attraverso l'isolamento è pressoché scomparso. Ciò significa che Ciò significa che qualsiasi minaccia in grado di garantire una violazione IT ha ora la strada aperta verso obiettivi vulnerabili e potenzialmente preziosi sul versante OT. Gli avversari possono penetrare nelle organizzazioni lungo un asse nord-sud (dall'esterno all'interno degli ambienti OT) e muoversi lateralmente attraverso l'organizzazione lungo un asse est-ovest. Senza strumenti di visibilità per individuare immediatamente gli intrusi, i danni tendono ad aggravarsi. Il tempo che intercorre tra la prima azione di un aggressore in una catena di eventi e la compromissione iniziale di un asset viene generalmente misurato in minuti, mentre il tempo per scoprirla è più probabilmente di mesi.[2]

Le organizzazioni hanno inoltre bisogno di nuove infrastrutture in grado di svolgere un doppio lavoro sia in ambienti IT che OT, al fine di semplificare le attività, la formazione e il reporting, riducendo al contempo i costi complessivi. La complessità dell'infrastruttura, che consiste nell'aggiungere strumenti e prodotti disparati di diversi fornitori, non solo aumenta le spese in conto capitale (CapEx), ma anche l'onere della distribuzione, della gestione e del monitoraggio a carico di risorse umane limitate. Aumentano dunque anche le spese di esercizio (OpEx).

Le connessioni WAN tradizionali hanno costi elevati

I costi sono un problema costante per la maggior parte delle organizzazioni OT e l'infrastruttura WAN esistente offre un'opportunità di risparmio. La WAN tradizionale si basa principalmente sulla costosa tecnologia MPLS (Multiprotocol Label Switching) o su collegamenti satellitari. Per mantenere il controllo e la visibilità centralizzati, il traffico viene reindirizzato verso un data center on-premises, il che può avere un impatto sulle prestazioni a causa di colli di bottiglia a livello di sicurezza.

Gli esperti prevedono un aumento degli attacchi ai danni delle infrastrutture critiche: botnet che sferrano attacchi DDoS (Distributed Denial-of-Service) contro le reti OT; attacchi a sistemi di produzione che utilizzano servizi cloud; attacchi alla catena di fornitura in cui gli autori della minaccia compromettono i fornitori terzi come trampolino di lancio per colpire settori critici.[3]

Le esigenze fisiche particolari dell'OT

Le organizzazioni OT operano in tutti i tipi di ambienti e siti di ogni dimensione, da grandi campus con edifici dotati di aria condizionata a piccole installazioni in luoghi remoti senza spazi propriamente allestiti che possano accogliere apparecchiature elettroniche. Alcuni ambienti possono essere proibitivi per la normale attrezzatura IT a causa della presenza di condizioni fisiche estreme come, ad esempio:

- Sottostazioni elettriche
- Piattaforme petrolifere
- Stabilimenti industriali
- Centrali idroelettriche
- Magazzini/centri di distribuzione
- Aeroporti
- Navi

La SD-WAN è diventata un modo diffuso per collegare le sedi remote delle aziende. La SD-WAN utilizza una serie di connessioni Internet come Long-Term Evolution (LTE), Digital Subscriber Line (DSL) o via cavo al posto della tecnologia MPLS/delle connessioni satellitari con notevole risparmio di costi. Per garantire le prestazioni dell'applicazione e l'esperienza dell'utente, la SD-WAN gestisce l'instradamento del traffico in base alle prestazioni (ad esempio, latenza, jitter) e ai costi di connettività per fornire una connessione affidabile e di alta qualità.

La diffusa adozione della SD-WAN nelle organizzazioni aziendali lascia intendere che gli ambienti OT saranno i prossimi, una volta individuate apparecchiature che soddisfino le esigenze degli ambienti OT, a iniziare da una SD-WAN robusta progettata per situazioni e ambienti industriali, produttivi e con infrastrutture critiche con condizioni ambientali difficili (ad esempio, piattaforme petrolifere, sottostazioni elettriche, linee di assemblaggio, trasporti marittimi).

La SD-WAN risolve allo stesso tempo diverse sfide OT, tra cui rapida distribuzione,connettività veloce e gestione unificata per ridurre i costi di gestione dell'IT.[4] Può inoltre migliorare la produttività. Gli utenti on-site che si connettono a un servizio cloud (ad esempio, Microsoft 365, Oracle Cloud o applicazioni in AWS) in un'architettura multi-cloud possono avere accesso direttamente dal luogo in cui si trovano con una minore latenza e un'esperienza utente di gran lunga migliore rispetto alla connessione a Internet tramite un firewall centrale del data center.[5]

La questione della SD-WAN e della sicurezza

Le implicazioni a livello di sicurezza dell'accesso diretto alle risorse cloud e Internet possono potenzialmente avere un impatto ancora maggiore in un ambiente OT rispetto a quanto accade in una tipica distribuzione SD-WAN.[6] Il passaggio dalla WAN tradizionale alla SD-WAN aggiunge un'ulteriore esposizione al rischio, poiché il traffico connesso a Internet non viene più reindirizzato verso un data center per controlli di sicurezza centralizzati. Purtroppo, la maggior parte dei prodotti SD-WAN si basa su una tecnologia di routing pensata essenzialmente per cercare il miglior percorso di connettività per il traffico. La maggioranza delle soluzioni SD-WAN oggi sul mercato non offre sicurezza integrata.

Qualsiasi aumento della vulnerabilità dell'OT è un problema grave poiché questi settori si trovano ad affrontare un'offensiva di attacchi mirati. La stragrande maggioranza (90%) delle organizzazioni ha subito almeno un'intrusione dei sistemi OT nell'ultimo anno, e il 65% ne ha subiti tre o più.[7]

Le interruzioni o i guasti dell'OT causati da un attacco possono avere enormi ripercussioni sulla produttività, l'efficienza e persino sulla sicurezza. Gli attacchi malware sono ora specificamente orchestrati per colpire i sistemi ICS (Industrial Control System) e SCADA (Supervisory Control and Data Acquisition) e i sistemi di sicurezza.[8] Questa esposizione al rischio riguarda anche le infrastrutture critiche (ad esempio, dighe idroelettriche, centrali nucleari, oleodotti e gasdotti), dove una violazione riuscita può avere gravi conseguenze dirette sulla vita umana o l'ambiente.

Le reti industriali richiedono una connettività protetta e prioritaria ai centri di controllo e alle applicazioni cloud. I sensori intelligenti basati sui protocolli di comunicazione Industrial Internet of Things (IIoT) e Internet-of-Things (IoT) come, ad esempio, Open Platform Communications Unified Architecture (OPC UA), Message Queuing Telemetry Transport (MQTT) e Hypertext Transfer Protocol (HTTP) devono essere protetti. Il trasferimento di informazioni di telemetria e controllo dalla rete di controllo dei processi alla rete IT aziendale o attraverso Internet può utilizzare protocolli intrinsecamente insicuri come Modbus, BACnet o SafetyNET. Questi devono essere collocati in diversi segmenti e devono essere ispezionati, classificati per priorità e protetti. Una tipica soluzione SD-WAN non offre nessuna di queste capacità di sicurezza critiche.

Le esigenze fisiche particolari dell'OT (segue)

Luoghi come quelli sopra elencati richiedono apparecchiature elettroniche speciali in grado di funzionare nelle condizioni spesso presenti in un ambiente OT come, ad esempio:

- Temperature estreme
- Umidità
- Vibrazioni estreme o costanti
- Interferenze elettromagnetiche (EMI)
- Spazi ridotti per le apparecchiature
- Impianti che utilizzano diversi tipi di alimentazione (oltre 110V o 220V)
- Servono dunque apparecchiature certificate in base alle regolamentazioni dei vari settori OT

Si prevede che il mercato mondiale delle SD-WAN crescerà del 168% di qui al 2024 superando i 3,2 miliardi di dollari.[10]

I cybercriminali stanno massimizzando le loro opportunità prendendo di mira sia le vulnerabilità OT già individuate che quelle che stanno emergendo con l'espansione della superficie di attacco.[11]

Distribuzione, gestione e monitoraggio a distanza

Un altro problema fondamentale per l'adattamento della SD-WAN agli ambienti OT deriva dalla comune necessità di introdurre queste tecnologie in siti remoti, che possono risultare impegnativi perché spesso hanno personale tecnico limitato o non ne hanno.[9] In situazioni di distribuzione remota, la soluzione SD-WAN ha bisogno di politiche di sicurezza coerenti che proteggano il sito fin dai primi momenti in cui il sistema è attivo e funzionante.

Inoltre, al SOC (Security Operations Center) serve una visibilità centralizzata di ogni singolo sito per monitorare i livelli di minaccia, gestire i gateway tra le reti IT e OT e i sistemi di quarantena trovati infetti al fine di limitare la propagazione del malware.

L'esigenza di una SD-WAN affidabile, sicura ed economica per l'OT

Poiché i cybercriminali di ogni tipo (dagli hacker opportunisti agli aggressori di Stati-nazione e alla criminalità organizzata) cercano sempre più di interrompere o danneggiare i sistemi OT per raggiungere i propri obiettivi, le aziende devono massimizzare i benefici della digitalizzazione, minimizzando al contempo le nuove esposizioni al rischio che queste tecnologie introducono nei loro ambienti sensibili.

Produttività e risparmio sui costi sono fattori critici per qualsiasi azienda. Ma le industrie che si affidano ai sistemi OT non possono permettersi di porre nessuno dei due al di sopra della sicurezza e della protezione delle loro attività. La maggiore esposizione al rischio che le connessioni dirette a Internet creano negli ambienti OT ha bisogno di una SD-WAN con sicurezza integrata, visibilità centralizzata e capacità di gestione remota. Inoltre, per ottenere i vantaggi della SD-WAN nei moderni ambienti industriali, serviranno soluzioni robuste pensate in modo nativo per le esigenze fisiche particolari delle distribuzioni OT.

[1] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

[2] "2019 Data Breach Investigations Report," Verizon, aprile 2019.

[3] Bruce Sussman, "15 Cyber Threat Predictions for 2020," SecureWorld, 12 dicembre 2019.

[4] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, 15 luglio 2020.

[5] Joe Robertson, "What Manufacturing CISOs Need to Know About SD-WAN," LinkedIn, 20 dicembre 2019.

[6] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, 15 luglio 2020.

[7] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

[8] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 8 maggio 2019.

[9] "SD-WAN Isn't Just for Retail," Fortinet, 3 aprile 2020.

[10] "SD-WAN Market Expected to Increase 168 Percent by 2024," BBC Magazine, 8 luglio 2020.

[11] Derek Manky, "Operational Technology: Why Old Networks Need to Learn New Tricks," Dark Reading, 31 dicembre 2019.

FORTINET

www.fortinet.com

febbraio 16, 2021 11:42 AM

839530-0-1-IT

E:\62_Fortinet\Assignment A-428829-1339270\OT\wp-FA-the-promise-of-sdwan-A4\wp-FA-the-promise-of-sdwan-A4_IT