Soluzione di Cybersecurity di Alcatel-Lucent Enterprise per le imprese

Brochure

Alcatel·Lucent Enterprise

Panoramica

La sicurezza informatica è da tempo una priorità fondamentale per le imprese. Tuttavia, le richieste relative ad essa stanno cambiando a causa della trasformazione digitale in corso. La trasformazione digitale implica che le organizzazioni utilizzino un maggior numero di dispositivi mobili connessi sulle loro reti e che i dipendenti accedano sempre più spesso ad applicazioni e dati dall'esterno.

E mentre il cambiamento accelera, i vecchi metodi per garantire la sicurezza della rete non tengono più il passo. Questo documento condivide le informazioni sulle forze che cambiano gli attuali requisiti di sicurezza informatica in ambito aziendale, raccomandando le strategie che le imprese possono adottare e le tecnologie che possono implementare per mantenere i dati e i sistemi sicuri nell'era della trasformazione digitale.

La soluzione di Cybersecurity di Alcatel-Lucent Enterprise soddisfa le esigenze di un'impresa digitale. Grazie a un approccio diversificato alla sicurezza informatica, le aziende possono fornire un accesso sicuro basato sulle policy dei dispositivi connessi, ai dati sicuri e alle applicazioni software in tutto l'ecosistema aziendale.

Sfide che cambiano

La natura delle minacce alla cybersecurity sta cambiando. Gli hacker utilizzano l'intelligenza artificiale (IA) e l'apprendimento automatico detto Machine Learning (ML) per creare attacchi più sofisticati e automatizzati. Le nuove tecniche di ingegneria sociale permettono ai criminali di connettere tra loro informazioni reperite attraverso i social media per creare profili di individui o di dati detenuti dalle organizzazioni.

La trasformazione digitale aziendale incide inoltre sui requisiti di sicurezza informatica, con conseguente maggiore complessità, uso più intensivo di dispositivi connessi e confini che scompaiono, il tutto a un ritmo sempre più sostenuto.

Più dispositivi, più complessità

Le imprese stanno adottando nuove tecnologie, tra cui cloud, mobile, IoT, Big Data e sistemi di analisi dei dati avanzati, che introducono un ulteriore livello di complessità che richiede un nuovo modo di guardare alla sicurezza. Inoltre, man mano che il numero di dispositivi connessi aumenta, si moltiplicano anche le vulnerabilità e le opportunità di violazione.

Ad esempio, in molti casi la prima generazione di dispositivi connessi non richiedeva password. Poiché i dispositivi si collegavano alla rete, gli hacker potevano usarli come un gateway. Oggi, le caratteristiche di sicurezza come le password hardcoded sono spesso obbligatorie nei dispositivi, tuttavia, le violazioni rimangono inevitabili e quando si verificano, gli hacker riescono ancora a ottenere l'accesso alla rete.

I confini che svaniscono

La maggior parte delle organizzazioni ha, per molto tempo, suddiviso chiaramente gli utenti e le risorse all'interno e all'esterno della rete. Tuttavia, quando le organizzazioni abbracciano la trasformazione digitale, diventano più aperte agli scambi con un ecosistema più ampio, che comprende altri partner e fornitori in un ambiente collaborativo integrato. Gli utenti non accedono più alle risorse solo dall'interno dei confini della rete, ma possono essere ovunque. Le informazioni possono essere scambiate con contatti in un'altra rete. Anche le risorse IT non sono più confinate all'interno del perimetro aziendale. Possono essere on-premise e nel cloud e collegate tramite API. Quando i confini spariscono, alle imprese occorrono nuove modalità per proteggere le risorse.

Macro e microsegmentazione in un mondo zero trust

Ci sono due tipi di segmentazione, macro e micro. Nella macrosegmentazione, la rete fisica è ripartita in diversi segmenti logici. Tutte le imprese usano la segmentazione, ma non sempre per ragioni di sicurezza. Spesso, la macrosegmentazione è usata a fini di scalabilità, amministrativi o organizzativi. Questi segmenti possono essere una VLAN, una combinazione di VLAN + VRF, potrebbe anche essere una VPN quando si parla di Shortest Path Bridging, MPLS, o anche tunnel VXLAN o GRE. Il traffico tra utenti o dispositivi su segmenti diversi è controllato da un firewall fisico. Se due dispositivi sono mappati su VLAN diverse e possono comunicare senza passare attraverso un firewall, si trovano sullo stesso macrosegmento. Ad esempio, le telecamere e le chiavi potrebbero rientrare sotto il controllo del gruppo di sicurezza degli accessi, mentre i termostati potrebbero essere sotto il controllo del gruppo di manutenzione dell'edificio.

La microsegmentazione compie 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 granulare sui privilegi di utenti/dispositivi che sono diversi a seconda dei ruoli come HR o Finance. Questo approccio è noto come «role-based access», ed è direttamente collegato al «principle of least privilege». 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 c'è bisogno che una telecamera comunichi con la serratura di una porta, così come non c'è bisogno che la serratura di una porta comunichi con un'altra serratura. Questi permessi granulari sono attuati attraverso policy che fanno parte del profilo e sono applicate dinamicamente al dispositivo dopo l'autenticazione.

La domanda è: ci occorrono davvero entrambi? La sfida con un approccio di sola macrosegmentazione è che il firewall diventi un collo di bottiglia, in quanto tutte le VLAN devono terminare sul firewall, e quindi si creano problemi di performance. In alternativa, si possono usare più firewall al livello di distribuzione, tuttavia, questo sarebbe abbastanza costoso e ancora non ottimale dal punto di vista delle performance. Inoltre, avere più firewall significa avere più punti di applicazione delle policy, e più posti per mantenere le policy aggiornate.

La microsegmentazione da sola può anche essere problematica. Se l'unica applicazione delle policy si basa sui criteri NAC (Network Access Control), gli elenchi delle policy diventano lunghi e complessi e possono esaurire i limiti di capacità del dispositivo. Un equilibrio tra questi due tipi di segmentazione permette 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 la macro e la microsegmentazione, è possibile agire 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 di approccio zero trust alla sicurezza della rete, il principio guida è «agire come se gli aggressori fossero già presenti». Questo significa autenticare tutte le connessioni. Nessuna risorsa e nessun utente è intrinsecamente affidabile. Che siano in sede o fuori sede, passano attraverso gli stessi controlli. Non esiste nulla che eguagli gli utenti interni. Ogni accesso è autenticato.

Prendiamo l'esempio di un approccio tradizionale alla sicurezza in cui la rete era vista come una fortezza costruita intorno all'impresa. La fortezza rappresenta il firewall, per cui tutto ciò che è fuori è inaffidabile e monitorato, mentre tutto ciò che è dentro è implicitamente fidato e permesso. Tuttavia, la microsegmentazione, in particolare la software-defined micro-segmentation, compie un passo avanti. Oltre alla fortezza e alla sicurezza intorno all'edificio, ci sono anche guardie di sicurezza che richiedono l'autenticazione. Questo confine di fiducia è distribuito ed è mobile. Non è legato a una particolare posizione, porta dello switch o VLAN. Dipende dall'identità, dal dispositivo, dalla situazione e dall'ora del giorno. È software-defined e si regola in tempo reale. La chiave di questo approccio è che i componenti sono gestiti e dovrebbero essere in grado di reagire secondo l'esigenza alle minacce o ai cambiamenti nel flusso di lavoro.

Una soluzione per l'impresa in evoluzione

Alcatel-Lucent Enterprise offre un approccio diversificato alla sicurezza informatica delle imprese e fornisce sicurezza in profondità per dispositivi e applicazioni connessi attraverso più livelli di protezione.

Connettività flessibile

Il nostro approccio inizia con una rete autonoma che rende facile e veloce la configurazione delle policy di rete e di sicurezza per il vasto numero di utenti, dispositivi e applicazioni connesse che alimentano la trasformazione digitale.

In passato, le attività principali dell'IT consistevano nell'installazione, nella messa in funzione di nuove apparecchiature, e nella gestione della rete attraverso noiosi processi manuali. La Digital Age Networking di Alcatel-Lucent Enterprise offre una rete intelligente e automatizzata che facilita le connessioni di utenti e dispositivi alle loro specifiche applicazioni in modo sicuro. Realizzata avvalendosi della tecnologia ALE Intelligent Fabric (iFab), Digital Age Networking combina iFab con lo standard Shortest Path Bridging (SPB). Insieme, queste tecnologie semplificano la creazione e la configurazione delle reti pur consentendo il routing multipath e l'aggregazione di link per combinare più connessioni di rete in parallelo e quindi aumentare il throughput e fornire ridondanza.

Con la nostra soluzione, i team IT definiscono i servizi di rete, l'architettura, le policy di accesso e i container IoT permettendo alla rete di costruirsi automaticamente. Una volta che la rete è architettata, se un componente viene spostato, cambiato o aggiunto, la rete completa gli aggiustamenti necessari in modo automatico e impercettibile. Per esempio, se uno switch va fuori servizio, la rete si reindirizza automaticamente intorno a quello switch.

Controllo degli accessi attraverso policy intelligenti e automatizzate

Le aziende possono utilizzare Digital Age Networking per definire regole e criteri di accesso degli utenti, i quali regolano le applicazioni e i dispositivi a cui accedere, ovunque si trovino. Ad esempio, possono impostare policy che consentono di accedere a:

- Sistemi specifici
- Servizi Internet
- Altri partner su una policy basata sul fornitore

ALE offre anche servizi basati sulla localizzazione, come il wayfinding all'interno delle strutture e l'asset tracking, che consentono alle imprese di impostare policy che tengano conto della posizione degli utenti.

Le funzioni di Unified Policy Access Management (UPAM) applicano automaticamente le policy ogni volta che un utente si connette, garantendo solo i privilegi di accesso consentiti. Quando gli utenti accedono alla rete con un dispositivo e convalidano le loro credenziali, non hanno bisogno di autenticarsi di nuovo. Rimangono connessi se il dispositivo è acceso e il sistema applica automaticamente la policy per quell'utente.

Le policy assicurano che tutti gli utenti, all'interno o all'esterno dell'organizzazione, abbiano accesso solo alle aree consentite e che i controlli di accesso vengano applicati in modo coerente. Semplificano anche i flussi di lavoro dell'impresa applicando la sicurezza informatica. Gli utenti possono accedere rapidamente ai sistemi e alle informazioni di cui hanno bisogno senza onerose procedure di login di sicurezza.

Ridurre la vulnerabilità del dispositivo

Le imprese si connettono a molti dispositivi IoT. La soluzione Digital Age Networking di Alcatel-Lucent Enterprise permette alle organizzazioni sanitarie di contenere ogni dispositivo, creando per ognuno un segmento di rete virtuale per evitare che anche solo uno di questi diventi un vettore di attacco. Il contenimento all'interno della Digital Age Networking genera più reti virtuali da una sola rete fisica, è di semplice attuazione per il settore IT ed è gestita da un unico sistema di gestione. Questa soluzione scopre automaticamente ogni dispositivo sulla rete. Quando un dispositivo viene collegato alla rete, Alcatel-Lucent OmniVista® Network Management System, disponibile on-premise o nel cloud, cerca di identificarlo. Se il dispositivo rilevato non è presente sul database del sistema di gestione, questo consulterà un database basato sul cloud contenente oltre 29 milioni di dispositivi.

Una volta che il dispositivo è identificato, il sistema lo classificherà, per esempio, come una telecamera di sicurezza. Se quel dispositivo è sulla lista dei fornitori approvati per le telecamere di sicurezza, verrà connesso alla rete. In caso contrario, non verrà collegato. La soluzione è quindi impostata in un contenitore virtuale per il dispositivo, segmentandolo dal resto della rete. Se qualcuno penetra in un qualsiasi dispositivo in rete, l'aggressore non sarà in grado di usare quel dispositivo per accedere al resto della rete.

Intelligenza artificiale per un ambiente di fiducia

Una volta che i dispositivi sono collegati, devono essere continuamente monitorati per identificare qualsiasi minaccia e mantenere la sicurezza. Il sistema di analisi dei dati di Alcatel-Lucent Enterprise e la visibilità delle applicazioni permettono agli amministratori di rete di vedere cosa sta succedendo all'interno della rete per ciascun dispositivo. Le analisi dei dati identificano i modelli per il comportamento normale e atteso della rete, così come qualsiasi comportamento insolito quando si verifica. Si può monitorare il comportamento delle applicazioni all'accesso della rete per decidere se connettersi o meno a quell'applicazione, oppure rilevare un eventuale comportamento insolito delle applicazioni permesse, come ad esempio una videocamera che sta producendo più dati del dovuto.

Se si verifica un'anomalia o un comportamento insolito sul dispositivo, l'analisi dei dati lo mostrerà così che il responsabile della sicurezza della rete possa intervenire. Oggi le indagini devono essere eseguite manualmente, ma ALE sta lavorando per automatizzare la risposta utilizzando IA e ML.

Proteggere la rete

Le organizzazioni oggi sono consapevoli della necessità di proteggere i dispositivi IoT in rete, tuttavia potrebbero omettere di considerare i dispositivi che costituiscono la base della rete, come gli switch e gli access point. Alcatel-Lucent Enterprise mette a disposizione molte tecnologie per ridurre le minacce alla sicurezza di questi dispositivi. Soluzioni ALE:

- Consolidare il sistema operativo per fornire un codice sicuro e diversificato
- Verificare il sistema operativo e affidarne il collaudo a terzi, per garantire l'assenza di punti di ingresso o backdoor facili da raggiungere.
- Assicurare che siano presenti modalità di compilazione e richiamo della memoria sempre diverse a ogni avvio dello switch. Sebbene gli switch funzionino in modo identico, internamente nessuno di essi è configurato allo stesso modo. Se qualcuno dovesse violare uno switch ALE, non sarebbe in grado di accedere ad un altro switch nello stesso modo.
- Fornire una protezione integrata contro gli attacchi DoS. La CPU è in grado di rilevare quantità insolite di traffico di rete e, se necessario, di spegnersi automaticamente.
- Diverse certificazioni di sicurezza come JDIC e FIPS
- Eseguire continui aggiornamenti del software.

Connessioni sicure per il traffico in entrata e in uscita

Per il traffico in entrata, le nostre funzionalità VPN forniscono una connessione criptata alla rete locale, mentre il traffico end-to-end è protetto utilizzando la crittografia MACsec (nota anche come IEEE 802.1AE), che protegge le informazioni mentre attraversano la rete ed è in grado di ricaricare i servizi, ad esempio TLS e HTTPS, senza necessità di riavvio, e quindi di interruzioni di rete

Reporting

Il reporting di Alcatel-Lucent Enterprise consente a soggetti diversi di accedere alle informazioni sullo stato, la salute e le prestazioni della rete, il funzionamento delle applicazioni e la soddisfazione degli utenti. Per esempio, l'IT può leggere i dati sulle prestazioni e le operazioni di rete.

Le unità di linea aziendale possono garantire che attrezzature come i sistemi di imaging (MRI, raggi X) trasmettano i dati ai server e ai tablet senza soluzione di continuità. La divizione IT può determinare se la rete sta fornendo servizi che permettono ai dipendenti di dedicare più tempo allo svolgimento delle loro mansioni e se le prestazioni della rete sono ottimali.

La sicurezza informatica nei diversi settori

Istruzione

Man mano che le istituzioni educative adottano strategie di campus intelligenti, alle loro reti si aggiungeranno più dispositivi connessi e mobili, e i dispositivi Internet of Things (IoT) accederanno sempre più ad applicazioni e dati da spazi all'esterno dei confini della rete.

Quando la connettività e l'innovazione sono attuate nelle grandi infrastrutture del campus, diventano immediatamente vulnerabili alle minacce informatiche. La soluzione Digital Age Networking for smart campuses di Alcatel-Lucent Enterprise mantiene le risorse IT e i dati al sicuro nell'attuale era di trasformazione digitale. Con questa soluzione, le istituzioni possono gestire da vicino l'accesso degli utenti, ridurre le vulnerabilità create dai dispositivi IoT, mobili e di rete, impedire che l'inevitabile violazione fornisca un punto di attacco, il tutto offrendo i servizi e le applicazioni richiesti da studenti e personale.

Settore trasporti

I progressi nei sistemi di trasporto grazie alle innovazioni tecnologiche richiederanno la trasformazione delle basi esistenti su cui sono costruiti. L'integrazione dei dispositivi e dei sistemi che permettono a qualsiasi ecosistema di trasporto di funzionare comporta connessioni veloci, affidabili e sicure. Le reti di dati di trasporto devono essere all'insegna dello IoT, per collegare senza soluzione di continuità sensori, telecamere, segnaletica e sistemi di controllo del traffico. La sicurezza della rete è anche di vitale importanza per proteggere i dati e l'integrità della rete.

ALE utilizza un codice sicuro e diversificato per migliorare l'integrità della rete e fornire una maggiore sicurezza contro gli attacchi informatici alla rete. Il codice diversificato e sicuro protegge le reti da vulnerabilità intrinseche, code exploits, malware e potenziali back door che potrebbero compromettere operazioni di importanza cruciale. ALE fornisce anche il rilevamento delle impronte digitali per IoT per identificare ogni dispositivo, compresi i veicoli, i sensori e le telecamere per garantire che non rappresentino una minaccia alla sicurezza della rete. La strategia di sicurezza approfondita di ALE ha ricevuto i più alti livelli di certificazione dalle agenzie governative, tra cui Common Criteria (EAL2 e NDcPP), JITC, FIPS 140-2 e NIST.

Settore sanitario

L'assistenza sanitaria è stata a lungo, e rimane, uno dei settori maggiormente presi di mira dagli hacker. E il problema continua a crescere. Secondo il Protenus Breach Barometer, nel 2018, il settore sanitario ha registrato 503 violazioni che hanno interessato 15 milioni di cartelle cliniche di pazienti, dato tre volte superiore a quello registrato per il 2017.[1]

Le violazioni si verificano perché i dati sanitari sono estremamente preziosi. Le cartelle dei singoli pazienti contengono moltissimi dati personali, compresi il nome, gli indirizzi attuali e precedenti, la storia lavorativa, i nomi e l'età dei parenti e informazioni finanziarie come carte di credito e numeri di conto corrente.[2]

Grazie a un approccio multiservizio alla sicurezza informatica, ALE Digital Age Networking garantisce un accesso sicuro e basato sulle policy ai dispositivi medici connessi, ai dati dei pazienti e alle applicazioni software in tutto l'ecosistema sanitario.

Pubblica amministrazione

Il ruolo esteso del digitale a livello di amministrazione centrale e locale ha offuscato la linea che protegge le risorse digitali che supportano il trasporto, la manutenzione delle infrastrutture e il monitoraggio dell'ambiente. Le policy governative in materia di sicurezza informatica per la sicurezza dei dati, la vulnerabilità e la gestione della fiducia devono essere riviste.

L'approccio ALE alla sicurezza informatica fornisce un approccio end-to-end, incentrato sul servizio, per proteggere tutti i livelli del servizio, dalla rete al software. Sul lato dei dispositivi, le organizzazioni del settore pubblico possono utilizzare la containerizzazione, per creare un segmento di rete virtuale per evitare che i dispositivi diventino un punto di attacco.

Settore dell'ospitalità

La crescita dell'elemento IoT nel settore dell'ospitalità porta un'esplosione di minacce alla sicurezza informatica, dato che la proliferazione di sensori e dispositivi connessi espande notevolmente la superficie di attacco della rete. L'IoT è particolarmente suscettibile perché molti dispositivi IoT sono concepiti senza sicurezza, o progettati da aziende che non conoscono gli attuali requisiti di sicurezza. Di conseguenza, i sistemi IoT possono potenzialmente rappresentare l'anello debole della sicurezza informatica per le aziende del comparto dell'ospitalità.

La protezione del traffico IoT e dei dispositivi richiede un approccio strategico che sfrutta molteplici livelli di protezione. Per aiutare hotel, casinò, resort e altre aziende nel settore Hospitality a sfruttare i vantaggi e mitigare i rischi dell'introduzione dell'aspetto IoT, ALE fornisce una strategia di sicurezza multilivello che offre protezione a ogni livello dell'infrastruttura, dal singolo utente e dispositivo al livello di rete. Fornisce anche una strategia di contenimento IoT per semplificare e proteggere l'onboarding dei dispositivi e fornire le giuste risorse di rete per far funzionare il sistema in modo corretto ed efficiente, il tutto in un ambiente sicuro per salvaguardare le aziende del settore dell'ospitalità dagli attacchi informatici.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far

2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/#2bb1f96b50cf

Riepilogo

La trasformazione digitale ha cambiato profondamente i requisiti necessari per garantire la sicurezza informatica delle imprese, poiché il numero di dispositivi connessi aumenta, i confini della rete spariscono e il cambiamento continua ad accelerare. La soluzione Digital Age Networking di Alcatel-Lucent Enterprise mantiene le risorse IT e i dati al sicuro nell'attuale era di trasformazione digitale. Grazie a questa soluzione, è possibile gestire da vicino l'accesso degli utenti, ridurre le vulnerabilità create dai dispositivi IoT, mobili e di rete, evitare che le inevitabili violazioni rappresentino un punto di attacco e offrire un ecosistema aziendale da una posizione sicura.