Sicurezza informatica della rete sanitaria nell'era della trasformazione digitale

Con un'intervista speciale a Silvia Piai,
Research Director per IDC Health Insights

IDC ANALYZE THE FUTURE

Brochure

Alcatel·Lucent Enterprise

Riepilogo generale

La sicurezza informatica è da tempo una priorità fondamentale per le organizzazioni sanitarie. Tuttavia, le richieste ad essa relative stanno cambiando a causa della trasformazione digitale in corso. La trasformazione digitale implica che le organizzazioni sanitarie utilizzino un maggior numero di dispositivi mobili e connessi sulle loro reti e che medici, partner e consulenti accedano sempre più spesso ad applicazioni e a dati dall'esterno. E mentre il cambiamento accelera, i vecchi metodi per garantire la sicurezza della rete non tengono più il passo.

In questo documento, Silvia Piai, Research Director presso International Data Corporation (IDC), condivide le sue visioni sulle forze che cambiano gli attuali requisiti di sicurezza informatica in ambito sanitario, raccomandando le strategie che le organizzazioni di questo settore possono adottare e le tecnologie che possono implementare per mantenere i dati e i sistemi sicuri nell'era della trasformazione digitale. Alcatel-Lucent Enterprise presenta il modo in Digital Age Networking (DAN) soddisfa le esigenze di un'impresa trasformata digitalmente. Grazie a un approccio sfaccettato alla sicurezza informatica, DAN 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.

Lo stato della sicurezza informatica in ambito sanitario oggi

Nel 2019 le organizzazioni sanitarie hanno investito **5,5 miliardi di dollari a livello globale** nella sicurezza informatica.

Tra un sondaggio e l'altro IDC ha rilevato che le organizzazioni sanitarie riferiscono che la sicurezza informatica è una priorità assoluta.[1] Questo non è sorprendente. L'assistenza sanitaria è stata a lungo, e rimane, uno dei settori maggiormente presi di mira dagli hacker. E il problema continua a crescere. 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 secondo il Protenus Breach Barometer.[2]

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.[3]

Non solo le violazioni della sicurezza informatica si traducono in furti di dati, ma possono anche portare a interruzioni operative, danni alla reputazione dell'ospedale e multe per violazioni di regolamenti come Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti e General Data Protection Regulation (GDPR) nell'Unione Europea. Una situazione ancora peggiore è la possibilità di causare danni ai pazienti. Per esempio, una pompa di insulina potrebbe fornire la quantità sbagliata di medicinale. Oppure, alcune informazioni potrebbero non essere recapitate per tempo a un medico che ha in cura un paziente, lasciandolo all'oscuro di eventuali allergie o di altri farmaci che il paziente assume.

IDC stima che nel 2019 le organizzazioni sanitarie hanno investito 5,5 miliardi di dollari a livello globale nella sicurezza informatica per mitigare questi rischi. Da oggi fino al 2022, IDC prevede una crescita annua complessiva di spesa per sicurezza informatica in ambito sanitario, pari all '8,7%, un dato simile a quello registrato per altri settori.[4]

Nonostante questi investimenti la sicurezza informatica presenta, in questo settore, ancora lacune di lungo corso. Mentre molte organizzazioni affermano che la sicurezza informatica è una priorità, spesso nella pratica quotidiana rimane solo un'idea. Dopo tutto, la priorità per i medici è la cura delle persone, non la sicurezza informatica. Tuttavia, potrebbero resistere attivamente agli sforzi impiegati per l'applicazione della sicurezza informatica se ciò impedisse i flussi di lavoro medici. Per esempio, se medici, infermieri e personale clinico dovessero dedicare molto tempo ad autenticarsi per accedere alle cartelle elettroniche o al sistema di cartelle cliniche (EMR/EHR), cercherebbero scorciatoie per risparmiare tempo prezioso, senza essere abbastanza consapevoli delle minacce e degli impatti sulla sicurezza informatica.

1 Per esempio: Priorities, Strategies, and Investments: Overcoming DX Challenges in European Healthcare https://www.idc.com/getdoc.jsp?containerId=EMEA44355219

2 https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

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

4 Worldwide Semiannual Security Spending Guide di IDC https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

Minacce alla sicurezza informatica in continuo mutamento

La natura delle minacce alla sicurezza informatica sta cambiando. Gli hacker utilizzano l'intelligenza Artificiale (AI) e l'apprendimento automatico (ML - Machine Learning) per creare attacchi più sofisticati e automatizzati. Le nuove tecniche di ingegneria sociale permettono ai criminali di connettere tra loro frammenti di informazioni reperiti attraverso i social media per creare ottimi profili di individui o di dati detenuti dalle organizzazioni sanitarie.

La trasformazione digitale del settore sanitario sta cambiando ulteriormente i requisiti di sicurezza, con conseguente maggiore complessità, maggiore uso di dispositivi connessi e confini che scompaiono, il tutto ad un ritmo sempre più veloce.

Maggiore complessità

Le organizzazioni sanitarie stanno adottando nuove tecnologie, tra cui cloud, mobile, IoT, Big Data e sistemi di analisi dei dati avanzati, che portano un ulteriore livello di complessità e che richiede un nuovo modo di guardare alla sicurezza.

Aumento dell'uso di dispositivi connessi

Entro il 2022, il 97% degli infermieri di reparto, il 98% dei medici, il 96% dei farmacisti e il 94% degli infermieri di pronto soccorso utilizzeranno dispositivi mobili.[5] Poiché le organizzazioni sanitarie e i pazienti utilizzano sempre più spesso dispositivi mobili, IoT e per la cura a domicilio come i Fitbit, sono emerse nuove vulnerabilità.

Per esempio, la prima generazione di dispositivi medici connessi non richiedeva password. Poiché si collegavano alla rete, gli hacker potevano usarli come un gateway. Oggi, la FDA e gli equivalenti enti europei impongono caratteristiche di sicurezza come le password hardcoded. Eppure le violazioni rimangono inevitabili e, quando si verificano, gli hacker possono ancora ottenere l'accesso

Entro il 2022, il 97% degli infermieri di corsia, il 98% dei medici, il 96% dei farmacisti e il 94% degli infermieri di pronto soccorso utilizzeranno dispositivi mobili.

5 https://www.aiin.healthcare/topics/connected-care/over-90-nurses-physicians-will-use-mobile-devices-2022

all'intera rete. La ricerca IDC mostra che in Europa solo il 6% dei fornitori di servizi sanitari prevede una strategia di sicurezza per i dispositivi medici connessi integrata nella propria architettura di sicurezza aziendale e, dato preoccupante, il 16% non ha neppure iniziato a valutare le potenziali minacce ai dispositivi medici in rete.[6] In effetti, i relatori durante la quinta conferenza sulla sicurezza eHealth dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) hanno stimato un aumento del 600% degli attacchi ai dispositivi IoT, in particolare ai dispositivi medici.[7]

In Europa solo il 6% dei fornitori di assistenza sanitaria prevede una strategia di sicurezza per i dispositivi medici connessi.

I confini scompaiono

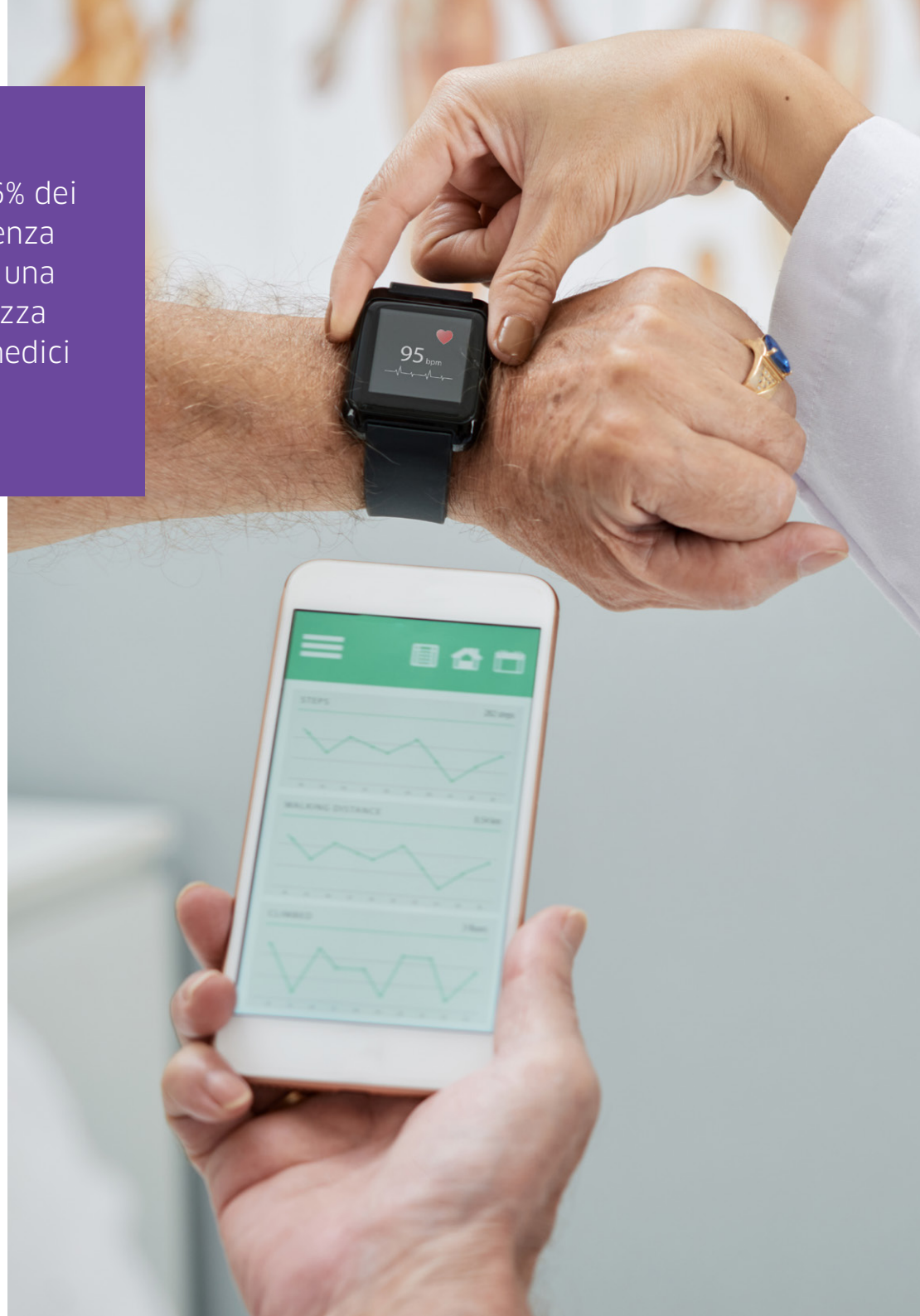
La maggior parte delle organizzazioni ha, per molto tempo, suddiviso chiaramente gli utenti e le risorse interni ed esterni alla rete.

Tuttavia, quando le organizzazioni sanitarie abbracciano la trasformazione digitale, diventano più aperte agli scambi con un ecosistema più ampio, che comprende pazienti, partner, contribuienti, autorità sanitarie governative e altri fornitori in un ambiente di cura integrata/collaborativa. Gli utenti non accedono più alle risorse solo dall'interno dei confini della rete, ma possono essere ovunque. I chirurghi potrebbero scambiare informazioni con i medici di assistenza primaria su una rete diversa. Gli ospedali potrebbero monitorare i pazienti a distanza dopo la dimissione dall'ospedale. I medici potrebbero usare i dati dei dispositivi sanitari personali dei pazienti per la diagnosi e la cura.

Anche le risorse IT non sono più confinate all'interno di confini prestabiliti. Sono on-premises e nel cloud e collegati tramite API. Quando i confini spariscono, le organizzazioni sanitarie hanno bisogno nuove modalità per proteggere le risorse.

Accelerazione del cambiamento

In un mondo trasformato digitalmente, tutto si muove più velocemente. Gli strumenti di sicurezza devono gestire questa velocità.



6 Sicurezza IoT nella sanità europea https://www.idc.com/getdoc.jsp?containerId=EUR145549919

7 https://www.enisa.europa.eu/events/5th-ehealth-security-conference

Intervista a Silvia Piai, Research Director per IDC Health Insights

Alcatel-Lucent Enterprise ha recentemente avuto l'opportunità di parlare con Silvia Piai, Research Director per IDC Health Insights, la quale ha condiviso le opinioni e le raccomandazioni di IDC riguardo alla sicurezza informatica nel settore sanitario.

Raccomandazioni IDC per migliorare la sicurezza informatica nel settore sanitario

Nonostante le sfide emergenti, l'approccio del settore sanitario alla sicurezza rimane tradizionale. Le organizzazioni sanitarie spesso implementano la sicurezza solo per spuntare le caselle di conformità senza considerare i cambiamenti dovuti alla trasformazione digitale, che hanno un grande impatto sui requisiti di sicurezza.

IDC raccomanda alle organizzazioni sanitarie di adottare un approccio olistico alla sicurezza della rete che includa strategia, tecnologia, persone (per esempio, formazione) e processi (per esempio, come la sicurezza si integra nei flussi di lavoro). In questo articolo esamineremo la strategia e la tecnologia.

Strategia

Invece di implementare una sicurezza informatica minima al solo scopo di ottenere la conformità, le organizzazioni sanitarie dovrebbero cogliere l'opportunità di sviluppare un piano strategico di sicurezza che gestisca il rischio in modo da soddisfare le richieste dell'attuale contesto di trasformazione digitale. Nello specifico:

- **Pensare alla conformità normativa come punto di partenza.** Mentre molte organizzazioni fanno il minimo indispensabile per conformarsi al GDPR o ad altri regolamenti equivalenti al di fuori dell'Europa, le organizzazioni sanitarie dovrebbero pensare alla conformità normativa come a un punto di partenza per ripensare il modo in cui stanno gestendo e governando i dati all'interno delle loro organizzazioni e con i loro partner.
- **Capire che la sicurezza guida il valore del business** assicurandone la continuità. Le organizzazioni sanitarie dovrebbero evitare la perdita di entrate (e ridurre i problemi di sicurezza dei pazienti) derivante dagli attacchi che mettono fuori uso i sistemi informatici. Allineare la sicurezza a obiettivi aziendali più ampi e renderla parte del business quotidiano.
- **Seguire un approccio di sicurezza improntato alla progettazione:** il rischio va di pari passo con i flussi di lavoro aziendali, che sono in costante evoluzione insieme alle tecnologie. Le organizzazioni sanitarie

dovrebbero incorporare la sicurezza nei flussi di lavoro fin dall'inizio. La sicurezza deve essere un valore aziendale fondamentale e deve guidare ogni decisione aziendale.

- **Lavorare con l'ecosistema.** Le organizzazioni sanitarie non hanno più un chiaro confine da difendere, perché integrano le cure provenienti da altre organizzazioni per i loro pazienti e partner. Hanno bisogno di lavorare con l'ecosistema per mantenere la sicurezza informatica.

Tecnologia

La creazione di un ecosistema connesso sicuro diventa fondamentale man mano che le organizzazioni sanitarie trasformano digitalmente le loro attività. Questo ecosistema richiede un approccio stratificato che pone le quattro discipline fondamentali della sicurezza - gestione dell'identità, della vulnerabilità, delle minacce e della sicurezza - in una nuova dimensione che permetta scalabilità, velocità, intelligenza e automazione. Questo approccio dovrebbe allinearsi con il più ampio ambiente digitale aziendale e con i risultati che l'organizzazione vuole raggiungere.

Gli aspetti chiave di una tecnologia di sicurezza di rete a più livelli dovrebbero includere:

- **Sicurezza degli endpoint** - per gestire le vulnerabilità dei singoli dispositivi.
- **Gestione dell'identità** - per autenticare gli utenti e controllare l'accesso. La soluzione dovrebbe fornire capacità di autenticazione degli utenti e policy di sicurezza molto specifiche che garantiscano agli utenti solo il giusto livello di accesso alle informazioni di cui hanno bisogno.
- **Scambio di dati sicuro** - l'uso della crittografia e di protocolli per lo scambio di file sicuri dovrebbe proteggere i dati in movimento.

- **Containerizzazione** - per evitare che le minacce saltino da un sistema all'altro dopo aver ottenuto l'accesso alla rete, la soluzione dovrebbe utilizzare la containerizzazione e la segmentazione della rete per isolare i singoli sistemi.
- **Gestione della sicurezza** - le organizzazioni sanitarie hanno bisogno di un approccio alla gestione del rischio che affronti l'eventualità che utenti e risorse possano risiedere al di fuori del perimetro della rete. Un modo per stabilire la sicurezza in un ambiente tale è capire cosa costituisce un comportamento normale o anormale sulla rete. Gli strumenti abilitati dall'intelligenza artificiale IA per la gestione delle identità e delle autorizzazioni permettono di stabilire una linea di riferimento normale per i comportamenti sulla rete. Questi strumenti possono valutare ogni utente e dispositivo e le loro applicazioni, la sicurezza e i requisiti di qualità del servizio per stabilire un comportamento normale di base. In seguito, l'IA può identificare rapidamente qualsiasi evento o azione insolita, come un sistema di sorveglianza che si inserisce in un EMR o EHR, e generare analisi che aiutano a determinare le ragioni di un cambiamento.
- **Un'architettura definita dal software** - una soluzione di gestione automatizzata della rete può fornire la velocità necessaria per stare al passo con la trasformazione digitale.

La soluzione Alcatel-Lucent Enterprise

Digital Age Networking (DAN) di Alcatel-Lucent Enterprise è un approccio sfaccettato alla sicurezza informatica delle reti sanitarie e fornisce sicurezza in profondità per dispositivi medici e applicazioni connessi attraverso più livelli di sicurezza.

Connettività flessibile attraverso una rete Service Defined Network (SDN)

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

In passato, le attività principali dell'IT consistevano nell'installazione, la messa in funzione di nuove apparecchiature, nella gestione della rete attraverso noiosi processi manuali. DAN è una rete intelligente e automatizzata che facilita la connessione di utenti e dispositivi alle loro specifiche applicazioni in modo sicuro. Costruita utilizzando la tecnologia Alcatel-Lucent Enterprise Intelligent Fabric (iFab), una rete DAN include il nostro Intelligent Fabric unito allo Shortest Path Bridging (SPB) standard del settore. Insieme, queste tecnologie semplificano la creazione e la configurazione delle reti pur permettendo 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.

Utilizzando una rete SDN, le organizzazioni sanitarie beneficiano di un'automazione che riduce gli errori di configurazione manuale e le aiuta a tenere il passo con l'accelerazione del cambiamento all'interno delle loro organizzazioni. Poiché l'automazione elimina il lavoro manuale, l'IT diventa un motore del business.

Controllo completo degli accessi attraverso policy intelligenti e automatizzate

Le organizzazioni sanitarie possono utilizzare l'approccio DAN di ALE per definire le regole di accesso degli utenti e le policy che governano quali sono le applicazioni e i dispositivi a cui gli utenti possono accedere, seguendoli ovunque vadano. Per esempio, possono impostare policy che:

- Consentano ai medici di accedere a tutti i sistemi tranne quelli finanziari
- Consentano ai pazienti di accedere ai servizi internet
- Assegnino alle aziende del settore scientifico o ad altri partner una policy basata sul fornitore

ALE offre anche servizi basati sulla localizzazione, come il wayfinding all'interno delle strutture e il tracciamento di risorse e persone, che permettono alle organizzazioni sanitarie di impostare policy che tengano conto della posizione degli utenti.

Le funzionalità di Unified Policy Management 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 PC/laptop/dispositivo mobile e convalidano le loro credenziali, non hanno bisogno di continuare ad autenticarsi. 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'ospedale applicando la sicurezza informatica. I medici che curano i pazienti possono accedere rapidamente ai sistemi e alle informazioni di cui hanno bisogno senza onerose procedure di login di sicurezza.

Riduzione della vulnerabilità con la containerizzazione e la segmentazione

Le organizzazioni sanitarie utilizzano molti dispositivi IoT, tra cui macchine per la risonanza magnetica, monitor per pazienti, pompe di infusione, robot per la distribuzione delle prescrizioni, così come videocamere, sistemi HVAC, sistemi di irrigazione, sistemi di rilevamento delle intrusioni e molti altri. L'approccio DAN di Alcatel-Lucent Enterprise permette alle organizzazioni sanitarie di containerizzare ogni dispositivo, creando per ognuno un segmento di rete virtuale per evitare che anche solo uno di questi diventi un vettore di attacco. La containerizzazione all'interno della DAN genera più reti virtuali da una sola rete fisica, gestita da un unico sistema di gestione.

La containerizzazione è semplice da implementare per l'IT. La soluzione DAN scopre automaticamente ogni dispositivo sulla rete. Quando un dispositivo viene collegato alla rete, il sistema di gestione Alcatel-Lucent OmniVista® 2500 Network Management System, disponibile on-premises 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 17 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 crea dunque un contenitore virtuale per il dispositivo, segmentandolo dal resto della rete. Se un hacker entra in un qualsiasi dispositivo in rete non potrà usarlo per accedere al resto della rete.

Maggiore sicurezza grazie all'intelligenza artificiale

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 osservare il comportamento delle applicazioni all'accesso della rete per decidere se connettersi o meno a quell'applicazione, oppure il 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.

Le funzionalità di IA supportano anche i servizi remoti per i pazienti. ALE sta sviluppando attrezzature per permettere agli ospedali di monitorare a distanza la convalescenza di pazienti dopo una malattia o un intervento chirurgico. L'attrezzatura deve comunicare in modo sicuro i dati dal dispositivo all'ospedale. L'IA può monitorare l'attività dei dispositivi IoT remoti per garantire che il loro comportamento sia coerente con quello previsto. Oggi i pazienti usano sempre più spesso le app per monitorare la loro salute. Se un medico potesse monitorare un Apple Watch® o un altro dispositivo di monitoraggio indossato da un paziente, poterebbe migliorare il coinvolgimento del paziente e fare diagnosi migliori. Con l'IA di ALE, le organizzazioni sanitarie saranno in grado di capire se un'applicazione o un'attività al suo interno può essere affidabile.

Apparecchiature di rete sicure riducono le vulnerabilità

Le organizzazioni sanitarie oggi sono consapevoli della necessità di proteggere i dispositivi IoT sulla rete. Tuttavia, a volte, non comprendono l'importanza di proteggere i dispositivi alla base della rete, come switch e access point.

ALE mette a disposizione molte tecnologie per ridurre le minacce alla sicurezza di questi dispositivi. Le nostre soluzioni consentono di:

- 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 dei nostri switch, non sarebbe in grado di accedere ad un altro switch con la stessa modalità.
- Fornire una protezione integrata contro gli attacchi DoS. La nostra CPU è in grado di rilevare quantità insolite di traffico di rete e, se necessario, di spegnersi automaticamente.
- Ottenere 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 possono garantire che attrezzature come i sistemi di imaging (MRI, raggi X) trasmettano i dati ai server e ai tablet senza soluzione di continuità. I CXO possono determinare se la rete sta fornendo servizi che permettono ai medici di trascorrere più tempo con i pazienti e se le prestazioni della rete sono ottimali.

Conclusione

La trasformazione digitale ha cambiato profondamente i requisiti necessari per garantire la sicurezza informatica degli ospedali, poiché il numero di dispositivi connessi aumenta, i confini della rete spariscono e il cambiamento continua ad accelerare. La soluzione Alcatel-Lucent Enterprise Digital Age Networkingper il settore sanitario mantiene le risorse IT e i dati dei pazienti al sicuro nell'attuale era di trasformazione digitale. Attraverso 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 vettore di attacco e comunicare attraverso l'ecosistema sanitario da una posizione sicura.

Noi siamo Alcatel-Lucent Enterprise.

Noi siamo ALE. Ti aiutiamo a connettere i tuoi pazienti, il personale e l'ecosistema sanitario. Fornitura di tecnologia che funziona attraverso e al di là delle tue strutture.

www.al-enterprise.com/it-it/industries/healthcare

Alcatel·Lucent
Enterprise