La cybersécurité des réseaux de santé à l'ère de la transformation numérique

inclut un entretien exclusif avec Silvia Piai, directrice de recherche chez IDC Health Insights

IDC ANALYZE THE FUTURE

Brochure

Alcatel·Lucent Enterprise

Synthèse

La cybersécurité est depuis longtemps considérée comme une priorité absolue pour les établissements de santé. Cependant, en raison de la transformation numérique en cours, les exigences en matière de cybersécurité évoluent. La transformation numérique va de pair avec une utilisation accrue des appareils connectés et mobiles au sein du réseau des établissements de santé, alors que les médecins, les partenaires et les médecins consultants accèdent de plus en plus à des applications et à des données situées au-delà du périmètre du réseau. En raison de l'accélération des changements, les anciennes méthodes de sécurité des réseaux ne suffisent plus.

Dans le présent document, Silvia Piai, directrice de recherche chez International Data Corporation (IDC), nous fait part de ses réflexions sur les forces qui modifient les exigences actuelles en matière de cybersécurité dans le domaine de la santé. Elle recommande des stratégies que peuvent adopter les établissements de santé et des technologies que ces derniers peuvent déployer afin d'assurer la sécurité des données et des systèmes à l'ère de la transformation numérique. Alcatel-Lucent Enterprise indique ensuite comment sa solution Digital Age Networking (DAN) répond aux exigences des entreprises entrées dans la révolution numérique. Avec une approche multidimensionnelle de la cybersécurité, le Digital Age Networking permet de maintenir la confiance par le biais d'un accès sécurisé aux dispositifs médicaux connectés basé sur des politiques, aux données des patients et aux applications logicielles dans tout l'écosystème de santé.

L'état de la cybersécurité dans la santé aujourd'hui

En 2019, les établissements de santé ont investi **5,5 milliards de dollars** dans la cybersécurité à l'échelle mondiale.

Les enquêtes successives réalisées par IDC ont révélé que les établissements de santé accordaient une priorité absolue à la cybersécurité.[1] Ce n'est pas surprenant. La santé constitue depuis longtemps l'un des secteurs les plus ciblés par les pirates informatiques. Ce problème ne cesse de s'aggraver. Ainsi, en 2018, le secteur de la santé a vu 15 millions de dossiers de patients compromis en lien avec 503 failles de sécurité, soit trois fois plus qu'en 2017, selon le baromètre Protenus Breach.[2]

Les violations se produisent en raison du caractère extrêmement précieux des données de santé. Les dossiers médicaux des patients contiennent toutes leurs données personnelles, notamment leurs noms, leurs adresses actuelle et antérieures, leurs antécédents professionnels, le nom et l'âge de leurs proches, ainsi que des informations financières telles que leurs numéros de cartes de crédit et coordonnées bancaires.[3]

Non seulement les failles de cybersécurité ont pour conséquence le vol de données, mais elles peuvent également provoquer des interruptions de fonctionnement, nuire à la réputation de l'hôpital et entraîner des amendes pour violation de réglementations telles que la loi américaine sur l'assurance maladie (Health Insurance Portability and Accountability Act - HIPAA) et le règlement général sur la protection des données (RGPD) dans l'Union Européenne. Le risque potentiel de préjudice encouru par les patients est encore bien pire. Par exemple, une pompe pourrait injecter une quantité d'insuline trop élevée ou trop faible. Il se peut également que des informations ne soient pas transmises au médecin pendant le traitement d'un patient, le laissant alors dans l'ignorance d'allergies éventuelles ou des médicaments pris par ce patient.

IDC estime qu'en 2019, les établissements de santé ont investi 5,5 milliards de dollars dans la cybersécurité à l'échelle mondiale afin de minimiser ces risques. D'ici à 2022, IDC prévoit une croissance annuelle des dépenses en matière de cybersécurité de 8,7 % dans le secteur de la santé, soit un montant équivalent à celui dépensé par d'autres secteurs d'activité.[4]

Malgré ces investissements, des lacunes dans la cybersécurité de la santé subsistent depuis longtemps. Bien que de nombreux établissements affirment que la cybersécurité figure en tête de leurs priorités, dans la pratique quotidienne, elle reste souvent une réflexion après coup. La mission des médecins n'est-elle pas de soigner les gens, et non de réfléchir à la cybersécurité ? Par ailleurs, ils risquent de résister activement aux efforts de renforcement de la cybersécurité si celle-ci entrave la productivité médicale. Ainsi, si les médecins et les infirmières doivent passer beaucoup de temps pour s'authentifier afin d'accéder aux dossiers médicaux électroniques ou au système de dossiers de santé (DMP/DPI), ils rechercheront tous les moyens possibles pour gagner un temps précieux. Beaucoup d'entre eux ne sont tout simplement pas suffisamment conscients des menaces en termes de cybersécurité et de ses impacts.

1 Par exemple : 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 IDC's Worldwide Semiannual Security Spending Guide https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

Évolution des menaces de cybersécurité

Dans le même temps, la nature des menaces de cybersécurité évolue. Les pirates informatiques utilisent l'intelligence artificielle (IA) et l'apprentissage automatique (AA) pour créer des attaques plus sophistiquées et automatisées. De nouvelles techniques d'ingénierie sociale permettent aux criminels de relier des miettes d'informations extraites sur les réseaux sociaux pour créer de très bons profils de personnes ou de données détenues par les établissements de santé.

La transformation numérique au sein du secteur de la santé modifie davantage les exigences en matière de cybersécurité, ce qui se traduit par une plus grande complexité, une utilisation accrue d'appareils connectés, un périmètre qui s'estompe, et tout cela à un rythme accéléré.

Une plus grande complexité

Les établissements de santé adoptent de nouvelles technologies, notamment le cloud, la téléphonie mobile, l'IoT, le Big Data et l'analyse avancée. Ces nouvelles solutions apportent un nouveau niveau de complexité qui exige un nouveau regard sur la sécurité.

Utilisation croissante des appareils connectés

D'ici 2022, 97 % des infirmières de chevet, 98 % des médecins, 96 % des pharmaciens et 94 % des infirmières dans les urgences utiliseront des appareils mobiles.[5] L'utilisation accrue des appareils mobiles, de l'IoT et des appareils de santé à domicile, tels que des accessoires Fitbit, par les établissements de santé et les patients entraîne l'apparition de nouvelles vulnérabilités.

D'ici 2022, 97 % des infirmières de chevet, 98 % des médecins, 96 % des pharmaciens et 94 % des infirmières dans les urgences auront recours à des appareils mobiles.

Par exemple, la première génération de dispositifs médicaux connectés n'exigeait aucun mot de passe. Étant donné que ces dispositifs étaient connectés au réseau, les pirates pouvaient s'en servir comme passerelle vers le réseau. Aujourd'hui, la FDA et ses équivalents européens imposent des éléments de sécurité tels que des mots de passe codés en dur. Les violations restent pourtant inévitables et, lorsqu'elles se produisent, les pirates peuvent encore avoir accès à l'ensemble du réseau.

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

Les recherches d'IDC révèlent que seuls 6 % des établissements de soins européens ont intégré une stratégie de sécurité des dispositifs médicaux connectés dans leur architecture de sécurité d'entreprise et, fait inquiétant, 16 % n'ont pas encore commencé à évaluer les menaces potentielles pesant sur les dispositifs médicaux en réseau.[6] En effet, les conférenciers participant à la cinquième conférence sur la sécurité de la santé en ligne de l'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA) ont estimé que les attaques contre les appareils IoT, et plus particulièrement les dispositifs médicaux, avaient augmenté de 600 %.[7]

Seuls 6 % des établissements de soins européens possèdent une stratégie de sécurité relative aux dispositifs médicaux connectés.

Disparition du périmètre

La plupart des établissements ont depuis longtemps clairement délimité les utilisateurs et les ressources situés à l'intérieur et à l'extérieur du réseau.

Toutefois, à mesure que les établissements de santé accélèrent leur transformation numérique, ils s'ouvrent davantage aux échanges avec l'écosystème au sens large, y compris les patients, les partenaires, les payeurs, les autorités sanitaires gouvernementales et d'autres fournisseurs dans un environnement de soins intégrés/collaboratifs. Les utilisateurs ne se contentent plus d'accéder aux ressources depuis le périmètre réseau, ils peuvent le faire de n'importe où. Des chirurgiens sont susceptibles d'échanger des informations avec des médecins généralistes situés sur un réseau distinct. Les hôpitaux pourraient surveiller des patients à distance après leur sortie de l'hôpital. Les médecins pourraient utiliser les données des appareils de soins personnels des patients pour faciliter le diagnostic et le traitement.

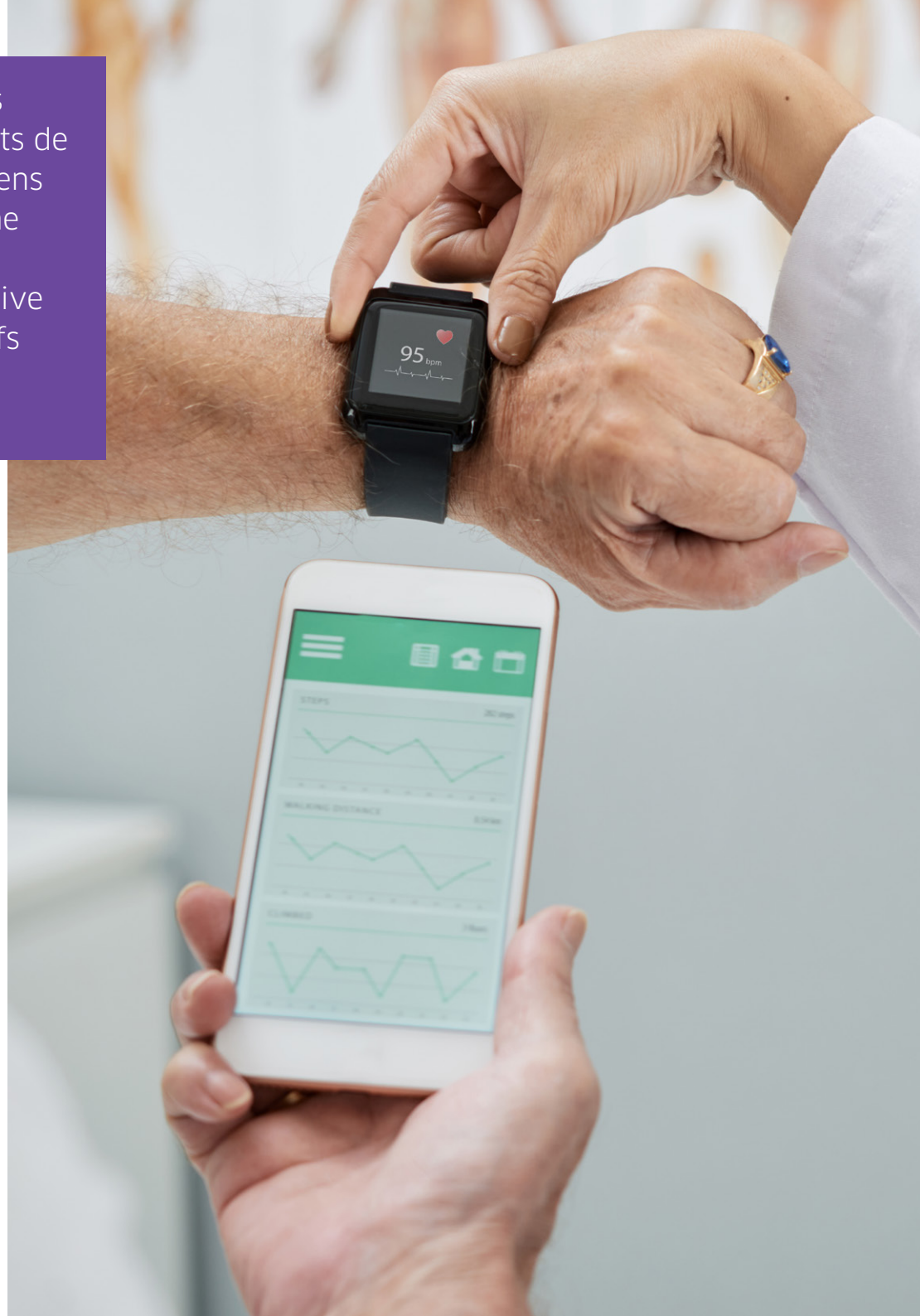
Les ressources informatiques ne sont également plus confinées à l'intérieur du périmètre. Elles se trouvent sur site et dans le cloud, et sont connectées grâce à des API. Les établissements de santé ont besoin de moyens modernes pour protéger les ressources lorsque le périmètre a disparu.

Accélération du rythme des changements

Dans un monde transformé par le numérique, tout va plus vite. Les outils de sécurité doivent pouvoir gérer cette accélération.

6 IoT Security in European Healthcare https://www.idc.com/getdoc.jsp?containerId=EUR145549919

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



Entretien avec Silvia Piai, directrice de recherche chez IDC Health Insights

Alcatel-Lucent Enterprise a récemment eu l'occasion de s'entretenir avec Silvia Piai, directrice de recherche chez IDC Health Insights, afin de recueillir l'avis et les recommandations d'IDC concernant la cybersécurité en santé.

Recommandations d'IDC pour renforcer la cybersécurité dans le secteur de la santé

Malgré les nouveaux défis, l'approche du secteur de la santé en matière de sécurité reste traditionnelle. Les établissements de santé mettent souvent en œuvre la sécurité simplement pour cocher les cases de conformité sans pour autant tenir compte des changements liés à la transformation numérique qui ont une incidence sur les exigences en matière de sécurité.

IDC recommande à ces établissements d'adopter une approche holistique de la sécurité des réseaux qui englobe la stratégie, la technologie, les personnes (par exemple, la formation) et les processus (par exemple, la manière dont la sécurité est intégrée dans les flux de travail). Dans le présent document, nous nous pencherons sur la stratégie et la technologie.

La stratégie

Au lieu de mettre en œuvre une cybersécurité minimale destinée à se conformer aux règles, les établissements de santé devraient saisir l'occasion pour élaborer un plan de sécurité stratégique de gestion des risques de façon à pouvoir répondre aux exigences du contexte actuel de transformation numérique. Pour y parvenir, ils devraient :

- **Considérer la conformité réglementaire comme un point de départ.** Alors que de nombreuses organisations se limitent au strict minimum pour se conformer au RGPD ou à d'autres réglementations équivalentes à l'extérieur de l'Europe, les établissements de santé devraient se servir de la conformité réglementaire comme une base pour repenser la manière dont ils gèrent les données et les régissent, tant en interne qu'avec leurs partenaires.
- **Comprendre que la sécurité génère de la valeur pour leurs opérations** et assure ainsi la continuité des

activités. Les établissements de santé se doivent d'empêcher une perte des revenus (et réduire les problèmes liés à la sécurité des patients) résultant des cyberattaques qui bloquent les systèmes informatiques. Ils doivent aligner la sécurité sur les objectifs plus larges de leur établissement et les intégrer dans leurs activités quotidiennes.

- **Suivre une approche de la sécurité par conception :** les risques vont de pair avec l'évolution constante des flux de travail, au même rythme que les technologies. Les établissements de santé doivent, dès le début, intégrer la sécurité dans les flux de travail. Il convient de considérer la sécurité comme une valeur ajoutée et de l'associer à chaque décision stratégique prise par les établissements de santé.
- **Travailler avec l'écosystème.** Le périmètre dans lequel évoluent les établissements de santé n'est plus aussi clairement défini, car ces derniers intègrent des soins issus d'autres établissements pour leurs patients et partenaires. Ils doivent travailler avec l'écosystème afin de maintenir la cybersécurité.

La technologie

Créer un écosystème connecté sécurisé devient primordial pour les établissements de santé qui transforment numériquement leurs opérations. Cet écosystème exige une approche par étapes qui place les quatre disciplines fondamentales de la sécurité - gestion des identités, gestion des vulnérabilités, gestion des menaces et gestion de la confiance - dans une nouvelle dimension permettant l'évolutivité, la rapidité, l'intelligence et l'automatisation. Cette approche devrait s'aligner sur l'environnement numérique plus large des établissements et sur les résultats qu'ils recherchent.

Les principaux aspects de la technologie de sécurité des réseaux par étapes devraient inclure :

- **La sécurité des appareils**—pour gérer les vulnérabilités des appareils individuels.
- **La gestion des identités**—pour authentifier les utilisateurs et contrôler l'accès. La solution devrait fournir des capacités d'authentification des utilisateurs et des politiques de sécurité bien définies qui accordent aux utilisateurs le niveau approprié pour accéder uniquement aux informations dont ils ont besoin.
- **La sécurisation de l'échange de données**—l'utilisation de protocoles de chiffrement et d'échange sécurisé de fichiers devrait permettre de protéger les données échangées.
- **La conteneurisation**—afin d'empêcher une menace de passer d'un système à l'autre une fois qu'elle a accédé au réseau, la solution devrait recourir à la conteneurisation et à la segmentation du réseau pour isoler les systèmes individuels.
- **La gestion de la confiance**—les établissements de santé doivent adopter une approche de gestion des risques qui tient compte du fait que les utilisateurs et les ressources peuvent résider en dehors du périmètre réseau. L'une des solutions préconisées pour établir la confiance dans un tel environnement consiste à comprendre ce qui constitue un comportement normal et anormal sur le réseau. Les outils de gestion des identités et des autorisations basés sur l'intelligence artificielle (IA) permettent d'établir une base de référence normale pour le comportement sur le réseau. Ces outils peuvent évaluer chaque utilisateur et chaque appareil ainsi que leurs exigences en matière d'application, de sécurité et de qualité de service afin d'établir un comportement de base normal. Par la suite, l'IA peut rapidement identifier tout événement ou action inhabituel, tel qu'un système de surveillance qui se connecte à un DMP ou DPI, et des analyses qui permettent d'expliquer les raisons d'un changement.
- **Une architecture définie par logiciel**—une solution de gestion de réseau automatisée peut offrir la vitesse nécessaire pour suivre le rythme de la transformation numérique.

La solution Alcatel-Lucent Enterprise

Digital Age Networking (DAN) d'Alcatel-Lucent Enterprise appliqué à la santé est une approche multi-facettes de la cybersécurité des réseaux de santé qui permet de sécuriser en profondeur les dispositifs médicaux et les applications connectés, grâce à de multiples couches de sécurité.

Une connectivité flexible grâce à un réseau défini par les services

Notre stratégie commence par un réseau flexible, défini par les services, qui permet de configurer rapidement et aisément les politiques en matière de réseau et de cybersécurité pour le nombre important d'utilisateurs, d'appareils connectés et d'applications qui alimentent la transformation numérique.

Dans le passé, l'informatique consistait à réparer ce qui ne fonctionnait pas. Le service IT installait les nouveaux équipements, les mettait en œuvre et gérait le réseau à l'aide de processus manuels fastidieux. La solution DAN forme un réseau intelligent et automatisé qui facilite la connexion sécurisée des utilisateurs et des appareils à leurs applications spécifiques. Conçu à l'aide de la technologie Alcatel-Lucent Enterprise Intelligent Fabric (iFab), le DAN intègre notre propre Intelligent Fabric combiné avec la norme industrielle Shortest Path Bridging (SPB). Ensemble, ces technologies permettent de simplifier la création et la configuration des réseaux tout en permettant le routage à trajets multiples et l'agrégation de liens afin de combiner plusieurs connexions réseau en parallèle et ainsi d'accroître le débit et d'assurer la redondance.

Avec la stratégie d'ALE, le service IT définit les services, l'architecture, les politiques d'accès et les conteneurs du réseau, permettant ainsi au réseau de se construire automatiquement. Une fois l'architecture du réseau établie, en cas de déplacement, de modification ou d'ajout d'un élément, le réseau procède automatiquement aux ajustements nécessaires et ce, de manière indétectable. Par exemple, si un commutateur est mis hors service, le réseau est automatiquement redirigé autour de ce commutateur.

En utilisant un réseau défini par les services, les établissements de santé bénéficient d'une automatisation qui permet de réduire les erreurs de configuration manuelle et de les aider à suivre l'accélération du rythme des changements au sein de leur établissement. En raison de la suppression du travail manuel par l'automatisation, le service IT devient le moteur d'une entreprise.

Un contrôle complet des accès grâce à des politiques intelligentes et automatisées

Les établissements de santé peuvent s'appuyer sur le DAN d'ALE pour définir les règles et les politiques d'accès des utilisateurs qui régissent les applications qu'ils peuvent utiliser et les appareils auxquels ils peuvent accéder – et ainsi suivre l'ensemble des déplacements des utilisateurs. Par exemple, ils peuvent mettre en place des politiques qui permettent :

- Aux médecins d'accéder à l'intégralité des systèmes à l'exception des systèmes financiers.
- Aux patients d'accéder aux services Internet.
- Aux entreprises du secteur des sciences de la vie ou d'autres partenaires de bénéficier d'une politique spécifique aux contractuels.

ALE propose également des services de géolocalisation, permettant le guidage et la géonotification au sein des bâtiments, le suivi des équipements et des personnes, destinés à aider les établissements de santé à mettre en place des politiques qui tiennent compte de la localisation des utilisateurs.

Chaque fois qu'un utilisateur se connecte, la gestion unifiée des politiques applique automatiquement les politiques adaptées, afin de garantir qu'il ne dispose que des privilèges d'accès autorisés. Après s'être connecté au réseau à l'aide d'un PC/ordinateur portable/appareil mobile et une fois ses identifiants validés, il n'a plus besoin de s'authentifier. Il reste connecté si l'appareil est allumé, et le système applique alors automatiquement la politique pour cet utilisateur.

Les politiques permettent de garantir que tous les utilisateurs, situés tant à l'intérieur qu'à l'extérieur de l'établissement, n'ont accès qu'aux zones autorisées et que ces contrôles d'accès sont appliqués de manière cohérente. Elles simplifient également les flux de travail des hôpitaux tout en veillant à l'application de la cybersécurité. Les soignants peuvent accéder rapidement aux systèmes et aux informations dont ils ont besoin pour prodiguer des soins, sans avoir à suivre de lourdes procédures de connexion de sécurité.

Réduction de la vulnérabilité grâce à la conteneurisation et à la segmentation

Les établissements de santé utilisent de nombreux appareils IoT, notamment des machines IRM, des moniteurs de patients, des pompes à perfusion, des robots de distribution de médicaments sur ordonnance, ainsi que des caméras vidéo, des systèmes de climatisation, d'extincteur, de détection d'intrusion, et bien d'autres encore. La solution DAN d'ALE permet aux établissements de santé de placer chaque appareil dans un conteneur, créant ainsi un segment de réseau virtuel pour celui-ci afin d'empêcher qu'un appareil ne devienne un

vecteur d'attaque. La conteneurisation au sein du DAN permet de créer plusieurs réseaux virtuels à partir d'un seul réseau physique, lequel est géré par un système de gestion unique.

La mise en œuvre de la conteneurisation par le service IT est simple. La solution DAN détecte automatiquement chaque appareil existant sur le réseau. Lorsqu'un appareil est connecté au réseau, Alcatel-Lucent OmniVista® 2500 Network Management System, accessible sur site ou dans le cloud, tente de l'identifier. Si cet appareil ne figure pas dans la base de données du système de gestion, ce dernier consultera une base de données située dans le cloud qui contient plus de 17 millions d'appareils.

Une fois identifié, le système le classera, par exemple, comme une caméra de sécurité. Si cet appareil figure sur la liste des fournisseurs agréés de caméras de sécurité, il sera connecté au réseau. Sinon, sa connexion ne sera pas autorisée. La solution est alors placée dans un conteneur virtuel pour l'appareil, en le séparant du reste du réseau. Si une personne pirate un appareil en réseau, elle ne pourra pas s'en servir pour accéder au reste du réseau.

Amélioration de la confiance grâce à l'intelligence artificielle

Une fois que les appareils sont connectés, ils doivent être surveillés en permanence afin d'identifier toute menace et de maintenir la confiance. Les analyses et la visibilité des applications fournies par ALE permettent aux administrateurs réseau de voir ce qui se passe au sein du réseau, appareil par appareil. L'analyse identifie les modèles de comportement normal et attendu du réseau, ainsi que toute tendance inhabituelle lorsqu'elle se produit. Le comportement des applications est analysé en périphérie du réseau afin de décider si l'on peut s'y connecter ou non, ainsi que le comportement inhabituel des applications autorisées, comme une caméra vidéo qui produit un plus grand nombre de données qu'elle ne le devrait.

Cette analyse permettra de signaler une anomalie ou un comportement inhabituel sur l'appareil au responsable de la sécurité du réseau afin qu'il puisse intervenir. Aujourd'hui, la recherche doit être effectuée manuellement, mais ALE œuvre à automatiser la réponse à l'aide de l'IA et de l'AA.

Les capacités de l'IA permettent également de supporter les services aux patients à distance. ALE conçoit des équipements qui permettent aux hôpitaux de surveiller à distance les patients à leur domicile pendant leur convalescence de maladie ou d'opération. Les équipements doivent transmettre les données de l'appareil connecté à domicile vers l'hôpital, en toute sécurité. L'IA peut surveiller l'activité des appareils IoT à distance afin de garantir la conformité de leur comportement par rapport au comportement attendu. Par ailleurs, les patients ont de plus en plus recours à des applications pour surveiller leur santé. Lorsqu'un

médecin a la possibilité de suivre une montre connectée Apple Watch® ou un autre dispositif de surveillance porté par un patient, il peut améliorer l'interaction avec ce patient et élaborer de meilleurs diagnostics. Grâce à l'IA d'ALE, les établissements de santé pourront savoir si une application ou une activité qui y est intégrée est fiable.

Un équipement réseau sécurisé permet de réduire les vulnérabilités

Les établissements de santé sont aujourd'hui conscients de la nécessité de sécuriser les appareils IoT sur le réseau. Mais ils sont susceptibles de ne pas tenir compte des appareils qui constituent la base du réseau, tels que les commutateurs et les points d'accès.

ALE offre de nombreuses technologies destinées à réduire la menace pour ces équipements. Nos solutions :

- Renforcer le logiciel du système d'exploitation afin de fournir un code sécurisé et diversifié.
- Envoyer le logiciel du système d'exploitation pour vérification et validation par un tiers afin de s'assurer qu'il ne comporte pas de points d'entrée faciles ou de portes dérobées.
- Vérifier qu'à chaque mise en service d'un commutateur, la mémoire est compilée et affichée d'une manière différente. Bien que les commutateurs fonctionnent de manière identique, il n'existe pas deux configurations de mémoire semblables en interne. Si une personne réussissait percer une brèche dans l'un de nos commutateurs, elle ne pourrait accéder à aucun autre commutateur en procédant de la même manière.
- Fournir une protection intégrée contre le déni de service (DoS). Notre processeur peut détecter toute augmentation inhabituelle du trafic réseau et s'arrêter automatiquement si nécessaire.
- Respecter les critères de plusieurs certifications de sécurité telles que JDIC et FIPS.
- Effectuer des mises à niveau logicielles en continu.

Sécurisation des connexions pour le trafic entrant et sortant

Pour le trafic entrant, nos capacités VPN fournissent une connexion chiffrée au réseau local, alors que le trafic de bout en bout est protégé par le chiffrement MACsec (également connu sous le nom d'IEEE 802.1AE) afin de protéger les informations lorsqu'elles traversent le réseau. En outre, le rechargement des services tels que TLS et HTTPS n'exigeant aucun redémarrage, le réseau n'est pas interrompu.

Reporting

Le reporting d'ALE permet à différents profils d'accéder à des informations sur l'état, l'intégrité et les performances du réseau, le fonctionnement des applications et la satisfaction des utilisateurs. Par exemple, le service IT peut consulter les données sur les performances et le fonctionnement du réseau. Les unités opérationnelles peuvent faire en sorte que les équipements tels que les systèmes d'imagerie (IRM, rayons X) transmettent les données aux serveurs et aux tablettes de façon transparente. Les responsables de l'expérience client/utilisateurs peuvent déterminer si le réseau fournit des services permettant aux médecins de passer plus de temps avec les patients et s'ils bénéficient du réseau selon leurs besoins.

Conclusion

La transformation numérique a profondément modifié les exigences de cybersécurité des hôpitaux en raison de l'augmentation du nombre d'appareils connectés, la disparition du périmètre réseau et l'accélération continue des changements. La solution Alcatel-Lucent Enterprise Digital Age Networking dans le secteur de la santé permet de sécuriser vos équipements informatiques et les données des patients à l'ère de la transformation numérique. Cette solution vous permet de gérer étroitement l'accès des utilisateurs, de réduire les vulnérabilités créées par l'IoT, les appareils mobiles et les équipements de réseau, d'empêcher une inévitable brèche de fournir un vecteur d'attaque et de se répandre à travers l'écosystème de santé.

Nous sommes Alcatel-Lucent Enterprise.
Nous vous aidons à connecter vos patients, votre personnel et votre écosystème de santé En délivrant une technologie éprouvée qui fonctionne pour vos établissements et leurs sites associés.
www.al-enterprise.com/fr-fr/industries/healthcare

Alcatel·Lucent
Enterprise