



Cyberbezpieczeństwo sektora opieki zdrowotnej w dobie cyfrowej transformacji

Zawiera wywiad z Silvią Piai, dyrektor ds. badań
w IDC Health Insights



Broszura

Alcatel•Lucent 
Enterprise

Stan cyberbezpieczeństwa w opiece zdrowotnej

Organizacje
opieki zdrowotnej
zainwestowały globalnie

**5,5
miliardów
dolarów**

w cyberbezpieczeństwo
w 2019 r.

W kolejnych badaniach przeprowadzonych przez IDC, organizacje opieki zdrowotnej donoszą, że cyberbezpieczeństwo jest ich najwyższym priorytetem.¹ Nie jest to zaskakujące. Opieka zdrowotna od dawna była i pozostaje jednym z sektorów, który stanowi największy cel ataków hakerów. A problem ten stale się powiększa. W 2018 r. sektor opieki zdrowotnej odnotował 15 milionów rekordów pacjentów zagrożonych w 503 naruszeniach; według barometru naruszeń Protenusa (Protenus Breach Barometer) to trzykrotnie więcej niż w 2017 r.²

Do naruszeń dochodzi, ponieważ dane dotyczące opieki zdrowotnej są niezwykle cenne. Indywidualna dokumentacja pacjenta zawiera wiele informacji, w tym imię i nazwisko, aktualne i poprzednie adresy zamieszkania, historię pracy, nazwiska i wiek krewnych oraz informacje finansowe, takie jak numery kart kredytowych i banków.³

Naruszenia cyberbezpieczeństwa skutkują nie tylko kradzieżą danych, ale mogą również prowadzić do przerw w działalności operacyjnej, uszczerbku na reputacji szpitala oraz kar za naruszenie przepisów, takich jak ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) w Stanach Zjednoczonych i ogólne rozporządzenie o ochronie danych (RODO) w Unii Europejskiej. Jeszcze gorsza sytuacja to możliwość wyrządzenia krzywdy pacjentowi. Na przykład pompa może podawać niewłaściwą ilość insuliny. Informacje mogą też nie zostać przekazane lekarzowi w trakcie leczenia pacjenta, przez co nie posiada on wiedzy o alergiach lub innych lekach przyjmowanych przez pacjenta.

IDC szacuje, że w 2019 r. organizacje opieki zdrowotnej zainwestowały 5,5 miliarda dolarów w globalne cyberbezpieczeństwo, aby zmniejszyć to ryzyko. IDC przewiduje, że od dziś do 2022 r. wydatki na cyberbezpieczeństwo w służbie zdrowia będą rosły w tempie 8,7 procent rocznie, czyli podobnie jak w innych sektorach.⁴

Pomimo tych inwestycji, nadal istnieją długotrwałe luki w bezpieczeństwie cybernetycznym opieki zdrowotnej. Chociaż wiele organizacji twierdzi, że cyberbezpieczeństwo jest dla nich priorytetem, w codziennej praktyce często pozostaje ono na dalszym planie. Wszakże lekarze zajmują się leczeniem ludzi, a nie myśleniem o cyberbezpieczeństwie. Ponadto mogą oni aktywnie opierać się wysiłkom mającym na celu egzekwowanie cyberbezpieczeństwa, jeśli utrudnia to procesy kliniczne. Na przykład, jeśli lekarze, pielęgniarki i pozostali klinicyści muszą poświęcić dużo czasu na logowanie się w celu uwierzytelnienia i uzyskania dostępu do elektronicznej dokumentacji medycznej lub systemu dokumentacji medycznej (EMR/EHR), będą szukać „drogi na skróty”, aby zaoszczędzić swój cenny czas. Wielu lekarzy po prostu nie ma wystarczającej świadomości zagrożeń i skutków dla cyberbezpieczeństwa.

¹ Na przykład: 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/#2b1f96b50cf>

⁴ Ogólnosiwiatowy przewodnik IDC dotyczący półrocznych wydatków na bezpieczeństwo https://www.idc.com/getdoc.jsp?containerId=IDC_P33461



Zmieniające się zagrożenia dla cyberbezpieczeństwa

Jednocześnie zmienia się charakter zagrożeń dla cyberbezpieczeństwa. Hakerzy używają sztucznej inteligencji (AI) i uczenia maszynowego (ML) do tworzenia bardziej wyrafinowanych, zautomatyzowanych ataków. Nowe techniki inżynierii społecznej umożliwiają przestępcom łączenie okruszków informacji znalezionych w mediach społecznościowych w celu tworzenia bardzo dobrych profili osób lub danych przechowywanych przez organizacje opieki zdrowotnej.

Cyfrowa transformacja w sektorze opieki zdrowotnej dodatkowo zmienia wymagania w zakresie bezpieczeństwa cybernetycznego, co skutkuje większą złożonością, zwiększonym wykorzystaniem połączonych urządzeń, zanikającymi granicami, a wszystko to w coraz szybszym tempie.

Większa złożoność

Organizacje opieki zdrowotnej wdrażają nowe technologie, w tym chmurę, urządzenia mobilne, IoT, Big Data i zaawansowaną analitykę. Rozwiązania te wprowadzają nowy poziom złożoności, który wymaga nowego spojrzenia na bezpieczeństwo.

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

Broszura

Cyberbezpieczeństwo sieci opieki zdrowotnej w dobie cyfrowej transformacji

Rosnące wykorzystanie połączonych urządzeń

Do 2022 roku 97 procent pielęgniarek przyłóżkowych, 98 procent lekarzy, 96 procent farmaceutów i 94 procent pielęgniarek na izbach przyjęć będzie korzystało z urządzeń mobilnych.⁵ W miarę jak organizacje opieki zdrowotnej i pacjenci coraz częściej korzystają z urządzeń mobilnych, IoT i domowych urządzeń zdrowotnych, takich jak Fitbits, pojawiają się nowe podatności.

Na przykład, pierwsza generacja połączonych urządzeń medycznych nie wymagała haseł. Ponieważ urządzenia te są podłączone do sieci, hakerzy mogą używać ich jako sposób na nieautoryzowane wejście do sieci. Obecnie FDA i europejskie odpowiedniki nakazują stosowanie zabezpieczeń, takich jak hasła zakodowane sprzętowo. Mimo to naruszenia pozostają nieuniknione, a kiedy już do nich dojdzie, hakerzy nadal mogą uzyskać dostęp do całej sieci. Badania firmy IDC pokazują, że tylko 6 procent europejskich dostawców opieki

Do 2022,
97 procent
pielęgniarek
przyłóżkowych, 98
procent lekarzy, 96
procent farmaceutów
i 94 procent
pielęgniarek w
izbach przyjęć będzie
korzystało z urządzeń
mobilnych.

zdrowotnej posiada strategię bezpieczeństwa połączonych urządzeń medycznych zintegrowaną z ich korporacyjną architekturą bezpieczeństwa, a co niepokojące, 16 procent nie zaczęło jeszcze oceniać potencjalnych zagrożeń dla sieciowych urządzeń medycznych.⁶ W istocie, prezeszy na piątej konferencji eHealth Security zorganizowanej przez Europejską Agencję Bezpieczeństwa Sieci i Informacji (ENISA) oszacowali, że nastąpił 600-procentowy wzrost ataków na urządzenia IoT, w szczególności na urządzenia medyczne.⁷

Granice zanikają

Większość organizacji przez długi czas wyraźnie rozgraniczała użytkowników i zasoby wewnątrz i na zewnątrz sieci.

Jednak w miarę jak organizacje opieki zdrowotnej przechodzą cyfrową transformację, stają się bardziej otwarte na wymianę z szerszym ekosystemem, w tym z pacjentami, partnerami, płatnikami, rządowymi organami opieki zdrowotnej i innymi świadczeniodawcami w środowisku opieki zintegrowanej/współpracy. Użytkownicy nie mają już dostępu do zasobów z sieci granicznej, a te mogą być wszędzie. Chirurdzy mogą wymieniać informacje z lekarzami podstawowej opieki zdrowotnej w innej sieci. Szpitale mogą zdalnie monitorować pacjentów po ich wypisaniu ze szpitala. Lekarze mogą wykorzystywać dane z osobistych urządzeń medycznych pacjentów do pomocy w diagnozowaniu i opiece.

Zasoby IT nie są już również ograniczone do granic sieci. Znajdują się one zarówno w siedzibie firmy, jak i w chmurze i są połączone za pomocą interfejsów API. Organizacje opieki zdrowotnej potrzebują nowoczesnych sposobów ochrony zasobów, gdy granice zanikają.

Przyspieszenie tempa zmian

W cyfrowo przekształconym świecie wszystko dzieje się szybciej. Narzędzia zabezpieczające muszą radzić sobie z tym tempem zmian.

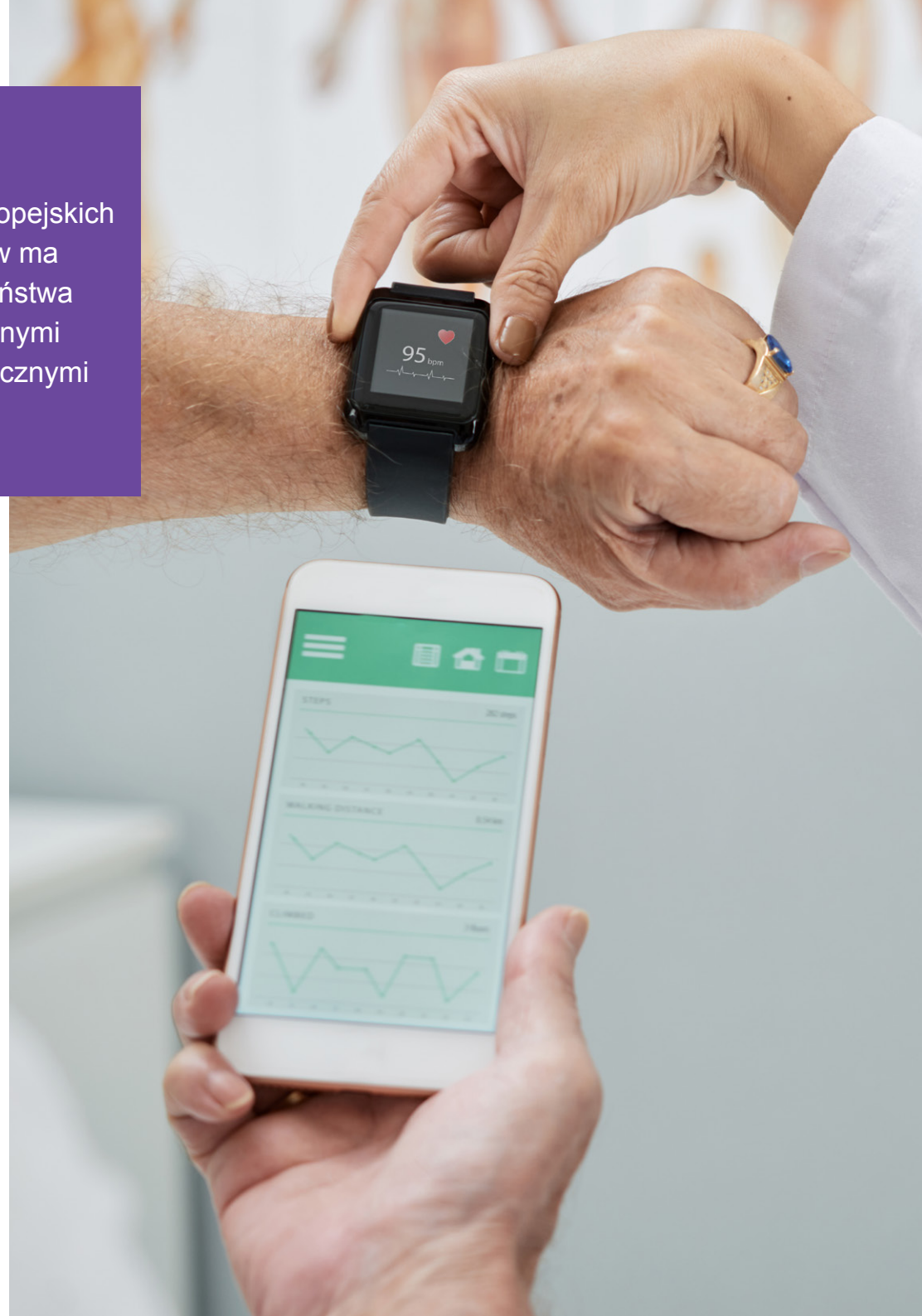
Tylko 6 procent europejskich świadczeniodawców ma strategię bezpieczeństwa związane z połączonymi urządzeniami medycznymi

⁶ Bezpieczeństwo IoT w europejskiej opiece zdrowotnej <https://www.idc.com/getdoc.jsp?containerId=EUR145549919>

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

Broszura

Cyberbezpieczeństwo sieci opieki zdrowotnej w dobie cyfrowej transformacji





Wywiad z Silvią Piai, dyrektor ds. badań w IDC Health Insight

Firma Alcatel-Lucent Enterprise miała ostatnio okazję porozmawiać z Silvią Piai, dyrektor ds. badań w IDC Health Insights, aby uzyskać opinie i zalecenia firmy IDC dotyczące cyberbezpieczeństwa w sektorze opieki zdrowotnej.



Zalecenia IDC dotyczące poprawy cyberbezpieczeństwa w sektorze opieki zdrowotnej

Pomimo pojawiających się wyzwań, podejście sektora opieki zdrowotnej w zakresie bezpieczeństwa pozostaje tradycyjne. Organizacje opieki zdrowotnej często wdrażają zabezpieczenia tylko po to, aby „odhaczyć” pola dotyczące zgodności z przepisami i nie biorą pod uwagę zmian wynikających z cyfrowej transformacji, które mają wpływ na wymagania dotyczące bezpieczeństwa.

IDC zaleca, aby organizacje opieki zdrowotnej przyjęły całościowe podejście do bezpieczeństwa sieci, które obejmuje strategię, technologię, ludzi (np. szkolenia) i procesy (np.

sposób, w jaki bezpieczeństwo jest wbudowane w procesy pracy). W tym dokumencie przyjrzymy się zarówno aspektom strategicznym, jak i technologicznym

Strategia

Zamiast wdrażać minimalne zabezpieczenia cybernetyczne w celu osiągnięcia zgodności z przepisami, organizacje opieki zdrowotnej powinny skorzystać z możliwości opracowania strategicznego planu bezpieczeństwa w celu zarządzania ryzykiem w sposób spełniający potrzeby dzisiejszej cyfrowej transformacji. Powinny one:

- **Uznać zgodność z przepisami za punkt wyjścia.** Podczas gdy wiele organizacji zaczyna od zrobienia minimum niezbędnego do przestrzegania RODO lub innych równoważnych przepisów poza Europą, organizacje opieki

zdrowotnej powinny uznać zgodność z przepisami za punkt wyjścia do ponownego przemyślenia sposobu zarządzania danymi w swoich organizacjach i we współpracy z partnerami.

- **Zrozumieć, że bezpieczeństwo zwiększa wartość biznesową** poprzez zapewnienie ciągłości działania. Organizacje opieki zdrowotnej muszą unikać utraty dochodów (i ograniczać obawy o bezpieczeństwo pacjentów), które wynikają z ataków cybernetycznych powodujących awarie systemów informatycznych. Dostosować zabezpieczenia do szerszych celów przedsiębiorstwa i uczynić je częścią swojej codziennej działalności.

Broszura

Cyberbezpieczeństwo sieci opieki zdrowotnej w dobie cyfrowej transformacji

- **Postępować zgodnie z podejściem „bezpieczeństwo według projektu”:** ryzyko idzie w parze z biznesowymi przepływami pracy, które stale ewoluują wraz z technologiami. Organizacje opieki zdrowotnej od samego początku muszą włączać bezpieczeństwo do swoich procesów pracy. Bezpieczeństwo musi być podstawową wartością biznesową i uzupełniać każdą decyzję biznesową podejmowaną przez organizacje opieki zdrowotnej.
- **Współpracować z ekosystemem.** Organizacje opieki zdrowotnej nie mają już wyraźnych granic, które muszą chronić, ponieważ integrują opiekę nad swoimi pacjentami i partnerami, świadczoną przez inne organizacje. Muszą one współpracować z ekosystemem w celu utrzymania cyberbezpieczeństwa.

Technologia

Stworzenie bezpiecznego, połączonego ekosystemu staje się niezwykle istotne w miarę jak organizacje opieki zdrowotnej przekształcają swoje działania w sposób cyfrowy. Ten ekosystem wymaga podejścia warstwowego, które przenosi cztery podstawowe dyscypliny bezpieczeństwa – zarządzanie tożsamością, zarządzanie podatnościami, zarządzanie zagrożeniami i zarządzanie zaufaniem – w nowy wymiar, umożliwiający skalowalność, szybkość, inteligencję i automatyzację. Podejście to powinno być zgodne z szerszym środowiskiem cyfrowym przedsiębiorstwa i wynikami, które organizacja chce osiągnąć.

Kluczowe aspekty wielowarstwowej technologii bezpieczeństwa sieciowego powinny obejmować:

- **Bezpieczeństwo punktów końcowych** — do zarządzania lukami w zabezpieczeniach poszczególnych urządzeń.
- **Zarządzanie tożsamością** – uwierzytelnianie użytkowników i kontrola dostępu. Rozwiązanie to powinno zapewniać możliwości uwierzytelniania użytkowników i szczegółowe zasady zabezpieczeń, które zapewniają użytkownikom odpowiedni poziom dostępu tylko do potrzebnych im informacji.
- **Bezpieczną wymianę danych** — stosowanie szyfrowania i protokołów bezpiecznej wymiany plików powinno chronić dane w ruchu.



- **Konteneryzację** — aby zapobiec przechodzeniu zagrożeń z jednego systemu na drugi po uzyskaniu przez nie dostępu do sieci, rozwiązanie to powinno wykorzystywać konteneryzację i segmentację sieci w celu odizolowania poszczególnych systemów.
- **Zarządzanie zaufaniem** – organizacje opieki zdrowotnej potrzebują podejścia do zarządzania ryzykiem, które uwzględnia fakt, że użytkownicy i zasoby mogą znajdować się poza granicami sieci. Jednym ze sposobów na zbudowanie zaufania w takim środowisku jest zrozumienie, co stanowi prawidłowe i nieprawidłowe zachowanie w sieci. Narzędzia oparte na sztucznej inteligencji (AI) do zarządzania tożsamością i autoryzacją umożliwiają ustanowienie normalnego poziomu odniesienia dla zachowań w sieci. Narzędzia te mogą ocenić każdego użytkownika i urządzenie oraz ich wymagania dotyczące aplikacji, bezpieczeństwa i jakości usług w celu ustalenia

normalnego zachowania bazowego. Następnie AI może szybko zidentyfikować wszelkie nietypowe zdarzenia lub działania, takie jak system nadzoru wykorzystujący EMR lub EHR, oraz analizy, które pomogą ustalić, dlaczego coś się zmieniło.

- **Architekturę zdefiniowaną programowo (Software Defined Networking, SDN)** - zautomatyzowane rozwiązanie do zarządzania siecią może zapewnić szybkość wymaganą do nadążenia za cyfrową transformacją.

Broszura

Cyberbezpieczeństwo sieci opieki zdrowotnej w dobie cyfrowej transformacji



Rozwiązanie Alcatel-Lucent Enterprise

Rozwiązanie Digital Age Networking dla sektora opieki zdrowotnej firmy Alcatel-Lucent Enterprise to wieloaspektowe podejście do cyberbezpieczeństwa sieci opieki zdrowotnej, które zapewnia kompleksowe bezpieczeństwo połączonych urządzeń i aplikacji medycznych dzięki wielu warstwom zabezpieczeń.

Elastyczna łączność za pośrednictwem sieci zdefiniowanej przez usługę

Nasze podejście zaczyna się od elastycznej, zdefiniowanej usługowo sieci, która umożliwia szybkie i łatwe konfigurowanie polityk sieciowych i bezpieczeństwa cybernetycznego dla ogromnej liczby podłączonych użytkowników, urządzeń i aplikacji, które napędzają cyfrową transformację.

W przeszłości praca działu IT przypominała operacje typu „zepsuj/napraw”. Instalował on nowy sprzęt, uruchamiał go i zarządzał siecią za pomocą żmudnych, ręcznych procesów. DAN to inteligentna, zautomatyzowana sieć, która ułatwia łączenie użytkowników i urządzeń z ich konkretnymi aplikacjami w bezpieczny sposób. Zbudowana z wykorzystaniem technologii Alcatel-Lucent Enterprise Intelligent Fabric (iFab), sieć DAN obejmuje naszą własną inteligentną sieć szkieletową w połączeniu ze standardem branżowym – protokołem SPB. Razem technologie te upraszczają tworzenie i konfigurację sieci, jednocześnie umożliwiając routing wielościeżkowy i agregację łączy w celu równoległego łączenia wielu połączeń sieciowych, a tym samym zwiększają przepustowość i zapewniają redundancję.

W podejściu ALE dział IT definiuje usługi sieciowe, architekturę, zasady dostępu i kontenery, a sieć tworzy się automatycznie. Po zaprojektowaniu sieci, jeśli cokolwiek zostanie przeniesione, zmienione lub dodane, sieć automatycznie i w sposób niezauważalny wprowadza niezbędne poprawki. Na przykład, jeśli jeden z przełączników przestanie działać, sieć automatycznie go przekieruje.

Korzystając z sieci definiowanej przez usługi, organizacje opieki zdrowotnej czerpią korzyści z automatyzacji, która zmniejsza liczbę błędów związanych z ręczną konfiguracją i pomaga im nadążyć za coraz szybszym tempem zmian w ich organizacjach. Ponieważ automatyzacja eliminuje pracę ręczną, IT staje się w większym stopniu motorem napędowym biznesu.

Kompleksowa kontrola dostępu dzięki inteligentnym, zautomatyzowanym politykom

Organizacje opieki zdrowotnej mogą używać DAN firmy ALE do definiowania reguł i zasad dostępu użytkowników, które określają, do jakich aplikacji i urządzeń użytkownicy mogą mieć dostęp i z jakich mogą korzystać, a także śledzić użytkowników w każdym miejscu. Na przykład mogą skonfigurować zasady, które zapewniają:

- Dostęp lekarzy do wszystkich systemów z wyjątkiem systemów finansowych
- Dostęp pacjentów do usług internetowych
- Politykę opartą na wykonawcach dla firm z dziedziny nauk biologicznych lub innych partnerów

ALE oferuje również usługi oparte na lokalizacji, takie jak nawigacja w pomieszczeniach, śledzenie zasobów i osób, które umożliwiają organizacjom opieki zdrowotnej ustanowienie zasad uwzględniających lokalizację użytkownika.

Funkcje ujednoliconego zarządzania zasadami automatycznie wymuszają zasady za każdym razem, gdy użytkownik łączy się, zapewniając użytkownikom tylko dozwolone uprawnienia dostępu. Gdy użytkownicy zalogują się do sieci za pomocą komputera PC/laptopa/urządzenia mobilnego i ich dane uwierzytelniające zostaną zweryfikowane, nie muszą się już uwierzytelniać. Pozostają połączeni, jeśli urządzenie jest włączone, a system automatycznie egzekwuje politykę dla tego użytkownika.

Zasady zapewniają, że wszyscy użytkownicy, wewnątrz i na zewnątrz organizacji, mają dostęp tylko do dozwolonych obszarów i że te kontrole dostępu są konsekwentnie egzekwowane. Upraszczają one również procesy pracy w szpitalach, zapewniając jednocześnie bezpieczeństwo cybernetyczne. Lekarze opiekujący się pacjentami mogą szybko uzyskać dostęp do systemów i informacji potrzebnych do zapewnienia opieki, bez uciążliwych procedur bezpiecznego logowania.

Zmniejszona podatność na zagrożenia dzięki konteneryzacji i segmentacji

Organizacje opieki zdrowotnej korzystają z wielu urządzeń IoT, w tym aparatów MRI, monitorów pacjenta, pomp infuzyjnych, robotów wydających recepty, a także kamer wideo, systemów HVAC, systemów zraszaczy, systemów wykrywania włamań i wielu innych. Rozwiązanie DAN

Broszura

Cyberbezpieczeństwo sieci opieki zdrowotnej w dobie cyfrowej transformacji





firmy ALE pozwala organizacjom opieki zdrowotnej na konteneryzację każdego urządzenia, tworząc dla niego wirtualny segment sieci, aby zapobiec sytuacji, w której każde urządzenie staje się wektorem ataku. Konteneryzacja w sieci DAN umożliwia zarządzanie wieloma sieciami wirtualnymi w jednej sieci fizycznej przez jeden system zarządzania.

Konteneryzacja jest prosta do wdrożenia dla działu IT. Rozwiązanie DAN automatycznie wykrywa każde urządzenie w sieci. Gdy urządzenie jest podłączone do sieci, [system zarządzania siecią Alcatel-Lucent OmniVista® 2500](#), dostępny lokalnie lub w chmurze, próbuje zidentyfikować to urządzenie. Jeśli system zarządzania nie ma danego urządzenia w swojej bazie danych, sprawdzi bazę danych w chmurze obejmującą ponad 17 milionów urządzeń.

Po zidentyfikowaniu urządzenia, system sklasyfikuje je np. jako kamerę bezpieczeństwa. Jeśli to urządzenie znajduje się na liście zatwierdzonych dostawców kamer bezpieczeństwa, zostanie podłączone do sieci. Jeśli nie, to nie będzie ono podłączone. Rozwiązanie to jest następnie konfigurowane w wirtualnym kontenerze dla urządzenia, segmentując je od reszty sieci. Jeśli ktoś włamie się do dowolnego urządzenia sieciowego, osoba atakująca nie będzie mogła użyć tego urządzenia, aby uzyskać dostęp do pozostałej części sieci.

Większe zaufanie dzięki sztucznej inteligencji

Po podłączeniu urządzeń, muszą one być stale monitorowane w celu identyfikacji wszelkich zagrożeń i utrzymania zaufania. Analityka ALE i widoczność aplikacji pozwala administratorom sieci zobaczyć, co dzieje się w sieci w podziale na urządzenia. Analityka identyfikuje wzorce normalnego, oczekiwanego zachowania w sieci, a także wszelkie nietypowe wzorce. Możemy przyjrzeć się zachowaniu aplikacji na krawędzi sieci, aby zdecydować, czy połączyć się z daną aplikacją, a także nietypowemu zachowaniu dozwolonych aplikacji, takich jak kamera wideo, która produkuje więcej danych niż powinna.

Jeśli na urządzeniu wystąpi anomalia lub nietypowe zachowanie, analiza pokaże, że menedżer bezpieczeństwa sieci może interweniować. Obecnie dochodzenie musi zostać przeprowadzone ręcznie, ale ALE pracuje nad automatyzacją reakcji przy użyciu AI i ML.

Możliwości AI wspierają również zdalną obsługę pacjentów. ALE opracowuje sprzęt, który umożliwia szpitalom zdalne monitorowanie pacjentów w ich domu, gdy dochodzą do siebie po chorobie lub po zabiegu chirurgicznym. Sprzęt ten musi w bezpieczny sposób przekazywać dane z urządzenia do szpitala. AI może monitorować aktywność zdalnych urządzeń IoT, aby upewnić się, że ich zachowanie jest zgodne z oczekiwanym. Ponadto pacjenci coraz częściej

korzystają z aplikacji do monitorowania swojego stanu zdrowia. Jeśli lekarz może monitorować Apple Watch® lub inne urządzenie monitorujące noszone przez pacjenta, może zwiększyć zaangażowanie pacjenta i postawić lepszą diagnozę. Dzięki AI firmy ALE organizacje opieki zdrowotnej będą miały wgląd w to, czy można zaufać danje aplikacji lub działaniu w ramach AI.

Bezpieczny sprzęt sieciowy zmniejsza podatności.

Organizacje opieki zdrowotnej są dziś świadome konieczności zabezpieczenia urządzeń IoT w sieci. Mogą jednak nie brać pod uwagę urządzeń, które stanowią fundament sieci, takich jak przełączniki i punkty dostępowe.

ALE stosuje wiele technologii, aby zmniejszyć zagrożenie ze strony tych urządzeń. Nasze rozwiązania:

- Wzmocnienie oprogramowania systemu operacyjnego w celu zapewnienia bezpiecznego, zróżnicowanego kodu.
- Wysyłanie systemu operacyjnego do weryfikacji i walidacji przez stronę trzecią, aby upewnić się, że nie ma łatwych punktów wejścia lub tylnych drzwi.
- Zapewnienie, że przy każdym uruchomieniu przełącznika pamięć jest kompilowana i przywoływana w inny sposób. Chociaż przełączniki te działają identycznie, żadne dwa nie mają tej samej wewnętrznej konfiguracji pamięci. Jeśli dojdzie do naruszenia jednego z naszych przełączników, dostęp do innego przełącznika nie będzie możliwy w ten sam sposób.
- Zapewnienie wbudowanej ochrony przed odmową usługi (DoS). Nasz procesor może wykrywać nietypowe ilości ruchu sieciowego i w razie potrzeby automatycznie wyłączyć się.
- Wypełnianie wielu certyfikatów zabezpieczeń, takich jak JDIC i FIPS.
- Wykonywanie ciągłych aktualizacji oprogramowania.

Bezpieczne połączenia dla ruchu przychodzącego i wychodzącego

W przypadku ruchu przychodzącego, oferowane przez nas funkcje sieci VPN zapewniają szyfrowane połączenie z siecią lokalną, podczas gdy ruch end-to-end jest chroniony za pomocą szyfrowania MACsec (znanego również jako IEEE 802.1AE) w celu ochrony informacji podczas przechodzenia przez sieć.

Broszura

Cyberbezpieczeństwo sieci opieki zdrowotnej w dobie cyfrowej transformacji



Raportowanie

Raportowanie firmy Alcatel-Lucent Enterprise umożliwia różnym osobom dostęp do informacji o stanie, kondycji i wydajności sieci, sposobie działania aplikacji i zadowoleniu użytkowników. Na przykład, dział IT może przeglądać dane dotyczące wydajności i operacji sieciowych. Linie biznesowe mogą zapewnić, że takie urządzenia jak systemy obrazowania (MRI, RTG) bezproblemowo przesyłają dane do serwerów i tabletów. CXO mogą określić, czy sieć dostarcza usługi, które pozwalają lekarzom spędzać więcej czasu z pacjentami i czy w pełni wykorzystują oni możliwości sieci.

Wniosek

Transformacja cyfrowa znacząco zmieniła wymagania szpitali w zakresie cyberbezpieczeństwa, ponieważ liczba podłączonych urządzeń wzrasta, granice sieci znikają, a zmiany wciąż przyspieszają. Rozwiązanie Digital Age Networking dla opieki zdrowotnej firmy Alcatel-Lucent Enterprise zapewnia bezpieczeństwo zasobów informatycznych i danych pacjentów we współczesnej erze cyfrowej transformacji. Pozwala ono ściśle zarządzać dostępem użytkowników, ograniczać podatności na zagrożenia stwarzane przez urządzenia IoT, urządzenia mobilne i sieciowe, zapobiegać nieuniknionym naruszeniom, które mogą stać się wektorem ataku, oraz komunikować się w całym ekosystemie opieki zdrowotnej z zaufaniem.

www.al-enterprise.com/pl-pl Nazwa i logo Alcatel-Lucent to znaki handlowe Nokia używane przez ALE na podstawie licencji. Inne znaki handlowe używane przez spółki zależne holdingu ALE można znaleźć na stronie www.al-enterprise.com/en/legal/trademarks-copyright. Wszystkie inne znaki handlowe należą do odpowiednich właścicieli. Informacje zawarte w tym dokumencie mogą ulec zmianie bez uprzedzenia. Holding ALE ani żadna z jego spółek zależnych nie ponoszą odpowiedzialności za jakiegokolwiek nieścisłości zawarte w tym dokumencie. © Copyright 2021 ALE International, ALE USA Inc. Wszelkie prawa zastrzeżone w innych krajach. DID20021001PL (marzec 2021 r.)



Jesteśmy Alcatel-Lucent Enterprise.

ALE to my. Pomagamy połączyć pacjentów, personel i ekosystem opieki zdrowotnej. Dostarczanie technologii, która działa w obiektach i poza nimi.

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

Alcatel•Lucent
Enterprise

