PRZEGLĄD SYSTEMATYCZNY/SYSTEMATIC REVIEW
Otrzymano/Submitted: 09.03.2021 • Zaakceptowano/Accepted: 12.05.2021

Cyberzagrożenia w sektorze ochrony zdrowia, w tym w anestezjologii i ratownictwie. Charakterystyka wybranych zagrożeń i sposoby zapobiegania

Cyber threats in the healthcare sector, including in anaesthesiology and emergency services. Characteristics of selected threats and methods of prevention

Szymon Nawrocki
Wydział Nauk Stosowanych, Wyższa Szkoła Przedsiębiorczości im. Księcia Kazimierza Kujawskiego w Inowrocławiu

Streszczenie

Celem artykułu jest zaprezentowanie możliwych typów ataków, które mogą dotknąć system opieki zdrowotnej zarówno w sektorze publicznym jak i prywatnym. W niniejszym artykule przedstawiono najbardziej znane typy cyberataków. Autor prezentuje sposoby na minimalizowanie skutków w przypadku wystąpienia udanego ataku na systemy informatyczne i urządzenia wykorzystywane w Służbie Zdrowia, a także sposoby na ich zapobieganie. Przeanalizowane zostają najgłośniejsze zagraniczne ataki na instytucje, których celem jest świadczenie opieki medycznej. Przedstawiono także wybrane zagrożenia, które dotyczą anestezjologii i ratownictwa medycznego. Poruszona zostaje tematyka bezpieczeństwa cybernetycznego pracowników ochrony zdrowia. *Anestezjologia i Ratownictwo 2021; 15: 102-109. doi:10.53139/AIR.20211510*

Słowa kluczowe: cyberzagrożenia, cyberataki, sektor ochrony zdrowia, ransomware, phishing

Abstract

The aim of the article is to present the possible types of attacks that may affect the health care system, both in the public and private sectors. This article presents the most known types of cyber attacks. The author presents ways to minimize the effects in the event of a successful attack on information systems and devices used in the Health Service, as well as ways to prevent them. The most famous foreign attacks on institutions aimed at providing medical care are analyzed. Selected risks related to anaesthesiology and emergency medical services are also presented. The subject of cybersecurity of healthcare professionals is discussed. *Anestezjologia i Ratownictwo 2021; 15: 102-109. doi:10.53139/AIR.20211510*

Keywords: cyber threats, cyber attacks, health sector, ransomware, phishing

Cel pracy

Celem pracy jest przedstawienie realnych zagrożeń, które mogą dotknąć Polski System Opieki Zdrowotnej w zakresie cyberprzestępstwa. Autor pragnie uświadomić pracowników sektora ochrony zdrowia, odnośnie tego typu zachowań przestępnych, na które mogą się natknąć ramach wykonywania obo-

wiązków służbowych. Przedstawione zostają podstawowe metody na ochronę i zapobieganie cyberatakom na sektor zdrowia.

Materiał i metody

W niniejszej pracy autor opiera się na artykułach i książkach naukowych z zakresu cyberbezpieczeństwa, dokonuje on również przeglądu artykułów internetowych ze specjalistycznych stron z zakresu cyberbezpieczeństwa, a które dotyczą omawianego zagadnienia.

Wstęp

Poprzez systemy informatyczne podmiotów odpowiedzialnych za świadczenie usług medycznych każdego dnia przesyłane są ogromne ilości danych, ich potencjalny wyciek niesie za sobą konsekwencje znacznie poważniejsze niż tylko te finansowe. Dane, które są przez te systemy przetwarzane zawierają informacje odnośnie chorób, leków czy miejsc zamieszkania pacjentów. Posiadanie takich informacji przez cyberprzestępców, stwarza im ogromne możliwości, przede wszystkim mogą oni zażądać od danej placówki, z której wyciekły dane, okupu za „oddanie" ich i odblokowanie dysku, jednakże należy mieć na uwadze, że przestępcy nie kierują się zasadami etyki, stąd istnieje prawdopodobieństwo szantażowania także pojedynczych osób fizycznych, których dane mogą posiadać. Wycieki danych są bardzo dotkliwe zarówno dla placówek medycznych, jaki i dla pacjentów, niemniej w ostatnim czasie pojawiły się nowe, bardziej poważne konsekwencje, chodzi tu o ingerencje w systemy maszyn używanych do hospitalizacji pacjentów. Problemem w tym wypadku jest fakt, iż nowoczesne maszyny medyczne, pomimo zaawansowanych systemów służących do ratowania ludzkiego życia same są dość podatne na ingerencje z zewnątrz, w tym zdalną za pośrednictwem sieci komputerowej, co może nieść za sobą nawet skutki w postaci spowodowania zgonu u pacjenta. Ostatnią kwestią, którą autor uznał za istotną dla przedmiotu niniejszego artykułu jest kwestia związana z fizyczną ochroną urządzeń, które przebywają na terenie danej placówki medycznej, oraz zwrócenie uwagi na wnoszenie urządzeń prywatnych przez pracowników czy osoby postronne na teren zakładu pracy, niesie to bowiem realne ryzyko, poprzez zainfekowanie urządzeń służących do świadczenia usług medycznych.

Ataki typu ransomware

Ransomware (ransom w tłum. z ang. Oznacza okup, zaś ware jest to końcówka od angielskiego słowa software, poprzez to w wolnym tłumaczeniu całość „ransomware" można rozumieć jako program do okupu.) jest to oprogramowanie, którego celem jest blokowanie dostępu do danego komputera czy bazy danych. Uniemożliwia on dostęp i odczyt informacji, które przechowywane są na danym urządzeniu, po włączaniu urządzenia wyświetlana jest jedynie informacja od „porywaczy", którzy informują ofiarę o tym, że musi ona zapłacić okup, a oni wtedy przekażą odpowiedni deszyfrator. W przeciwnym wypadku upublicznią oni dane, lub wykorzystają je w dalszych celach przestępnych [1]. Zazwyczaj w tego typu atakach im dłużej ofiara zwleka, tym większą kwotę powinna wpłacić, by uzyskać dostęp do swoich danych. Problemem w tym przypadku jest to, że wpłacenie okupu nie rozwiązuje sprawy, przestępcy i tak mają dostęp do danych nawet po oddaniu deszyfratora, co więcej po wpłaceniu okupu zdarzają się sytuacje, gdzie zachodzą ponowne ataki na tą samą osobę/firmę. Specjaliści z zakresu cyberbezpieczeństwa są co do zasady zgodni, by okupu nie płacić, zamiast tego należy skupić się na niwelowaniu skutków ataku, poprzez odłączenie od sieci zainfekowanych urządzeń i usprawnieniu systemów bezpieczeństwa sieci komputerowych, oraz podjęciu kroków prewencyjnych, które w przyszłości pozwolą na mniejsze szkody. Takim środkiem prewencyjnym jest przede wszystkim regularne wykonywanie kopii zapasowych dysków, które zawierają cenne dane. Wtedy w momencie, gdy dojdzie do wycieku danych nie doświadczymy paraliżu informacyjnego ze względu na fakt posiadania kopii danych, które można odtworzyć na niezainfekowanym systemie. Istotnymi środkami są także: używanie aktualnych oprogramowań komputerowych, programów antywirusowych oraz korzystanie z testów penetracyjnych przygotowywanych przez wyspecjalizowane firmy, o czym szerzej w dalszej części niniejszej pracy. W kwestii całkowitej ochrony przed zainfekowaniem systemu/komputera przez ransomware, nie istnieje środek, który by temu zapobiegł ze 100% skutecznością. W przypadku ośrodków dysponujących cennymi danymi nie należy zadawać pytania czy atak nastąpi, tylko kiedy, zwłaszcza biorąc pod uwagę fakt nasilających się tego typu ataków na świecie. Dane statystyczne mówią o tym, że w samym listopadzie 2020 na całym świecie nastąpił wzrost

ataków na placówki zajmujące się opieką zdrowotną o 45%, dla porównania w innych sektorach wzrost wynosił około 22%. Co istotne z punktu widzenia Polski, największy bo aż 145% wzrost w regionie nastąpił w Europie środkowej. Zaś najbardziej atakowanymi państwami były Kanada (wzrost o 250%), oraz Niemcy (wzrost o 220%) [2].

Wybrane ataki typu ransomware na przykładzie USA, Niemiec i Polski

Poprzez pandemię COVID-19 nasiliły się cyberataki na służbę zdrowia, jednym z największych był atak na amerykańskiego operatora sieci szpitali Universal Health Service inc. Atak nastąpił we wrześniu 2020. W wyniku ataku została odłączona sieć ww. firmy, należy przy tym zaznaczyć, że posiada ona ponad 400 szpitali w USA i Wielkiej Brytanii. W obliczu tak poważnego ataku Universal Health Service jest przykładem tego, w jaki sposób powinny być zabezpieczone duże firmy, które przetwarzają dane. Pomimo odłączenia od kluczowego dla ich funkcjonowania systemu, uruchomiono kopie zapasowe offline, natychmiast wróżono procedury bezpieczeństwa, które uwzględniały również tworzenie papierowej dokumentacji medycznej na czas ataku, dzięki czemu zachowano ciągłość w leczeniu pacjentów. [3]. W wyniku ataku firma poniosła straty w wysokości 67 milionów dolarów. Najważniejsze jest jednak w tym wypadku to, że zachowano ciągłość funkcjonowania placówek. [4].

We wrześniu 2020 doszło również do ataku na Niemiecką Służbę Zdrowia, dotknął on m.in. Uniwersytecki Szpital w Düsseldorfie. Przez tydzień systemy szpitala ulegały regularnym awariom, serwery często restartowano, w wyniku czego część pacjentów była przekierowywana do innych szpitali a wiele operacji nie było wstanie się odbyć. W wyniku tego ataku jedna z pacjentek nie została przyjęta do szpitala i musiano ją przewieźć do innej placówki, wskutek czego zmarła. Jest to pierwszy potwierdzony przypadek, w którym poprzez atak ransomware osoba poniosła śmierć. Co ciekawe przestępcy nie ustalili kwoty, zamiast tego chcieli skontaktować się z władzami, by z nimi ją wynegocjować, te jednakże nie postanowiły nawiązać kontaktu. W sumie w wyniku ataku zaszyfrowano 30 serwerów, zaś miejscowa prokuratora wszczęła śledztwo przeciwko niezidentyfikowanym sprawcom, są podejrzani o nieumyślne spowodowanie śmierci [5].

Wartym uwagi przypadkiem jest sytuacja z 12 grudnia 2020 r., która miała miejsce we Wrocławiu. W wyniku ataku ransomware na Pogotowie Ratunkowe we Wrocławiu przez kilka godzin tego dnia występowały poważne problemy związane z systemem odpowiedzialnym za wsparcie dyspozytorów. Atak udało się jednak szybko wyeliminować, prawdopodobną przyczyną było nieaktualne oprogramowanie wykorzystywane przez pracowników do obsługi sytemu. Był to mały atak, niemniej nie wiemy jakie jakie dane zostały wykradzione, na chwilę obecną szacuje się, że jego skutki były niewielkie. Był on jednak o tyle istotny z tego względu, że zdarzył się w Polsce, zatem był on swego rodzajem ostrzeżeniem do podjęcia odpowiednich działań, gdyż jak widać Polska stała się jednym z obiektów zainteresowań cyberprzestępców w dziedzinie placówek medycznych, w tym tak ważnego sektora jakim jest ratownictwo medyczne. Jest to ostatni moment na podjęcie dodatkowych środków zabezpieczeń w pozostałych placówkach, tak by ograniczyć tego typu działania. Sam atak mógł być również jedynie testem przed dużą operacją, sprawdzeniem jakie kroki podejmą polskie służby, a także czy zwróci on odpowiednią uwagę wśród personelu.

Ataki socjotechniczne

Następną kategorią cyberzagrożeń, które są kluczowe dla sektora ochrony zdrowia zdaniem autora są ataki socjotechniczne. Mogłoby się wydawać, że jest to stosunkowo łatwe do uniknięcia zagrożenie ze względu na niewielkie środki, jakie muszą stosować atakujący, jednakże jest to mylne przeświadczenia. Każdy, nawet najbardziej zaawansowany system zabezpieczeń ma swój słaby punkt, tym punktem może być człowiek i tak właśnie zazwyczaj jest. Należy przy tym pamiętać, że system jest na tyle mocny, na ile jest silny właśnie ten najsłabszy punkt. Prawdopodobnie najbardziej znany socjotechnik świata, a zarazem haker Kevin Mittnick, mawiał „łamałem ludzi, nie hasła" [6], tak też zatytułował on jedną ze swoich książek na łamach której opisywał swoje doświadczenia z włamywaniem się m.in. do systemów informatycznych. Same ataki socjotechniczne polegają na zmuszeniu ofiary do wykonania określonej czynności, jednocześnie sprawiając, by osoba myślała, że sama zadecydowała o danym działaniu. W przypadku bezpieczeństwa placówek medycznych największym zagrożeniem jest phishing. Jest to cyberzgrożenie polegające na wysyłaniu przede wszystkim e-maili, które z pozoru

mają wyglądać na takie ze zweryfikowanego źródła, w rzeczywistości zaś są to wiadomości mające na celu wyrządzić szkodę odbiorcy [7]. Najprostszą formą tego typu ataków jest zwykła wiadomość e-mail, w której nie ma żadnych złośliwych linków, znajduje się tam prośba, polecenie, informacja, która ma wymóc na odbiorcy określone zachowanie. W innych, bardziej zaawansowanych atakach, przestępcy posługują się takimi technikami jak e-mail spoofing, czyli podmienienie adresu nadawcy na taki, który będzie podobny do rzeczywistego, bądź całkowite sklonowanie go, tak by uwiarygodnić wiadomość e-mail. Zawierają one również często załączniki, w których po otwarciu infekowane są komputery, a czasem nawet całe systemy informatyczne. Jest to jeden ze sposobów dostania się ransomware do firmy. Zagrożeniem są także linki zawarte w tych wiadomościach, zawierają one przekierowania do podstawionych stron, które mogą zainstalować na urządzeniu szkodliwe oprogramowania np. malware (różnego rodzaju złośliwe i wyrządzające szkody oprogramowanie), keylogger (urządzenie służące do sczytywania wprowadzanych znaków z klawiatury). W ramach phishingu można wyróżnić taką odmianę jaką jest spearphishing, polegający na ataku socjotechnicznym na konkretna osobę w oparciu o działania typu OSINT (Open Source Intelligence tłum. Z ang, wywiad na podstawie źródeł otwartych, są to działania oparte na zbieraniu danych na temat osób/firm na podstawie danych ogólnodostępnych w internecie, technika ta występuje również pod nazwą"biały wywiad") [8]. Należy szczególnie pochylić się względem tego konkretnego przypadku, gdyż cyberprzestępcy za pomocą białego wywiadu są wstanie zebrać informacje praktycznie o każdym pracowniku danej placówki zdrowia po to, by zainfekować jego konto pocztowe, a potem także wgrać złośliwe oprogramowanie do całego zakładu pracy. Może się tak zdarzyć w momencie, gdy pracownik zaloguje się na prywatną skrzynkę pocztową ze służbowego komputera, wtedy cyberprzestępca jest w stanie dostać się do systemu całej placówki. Stąd tak ważne jest, aby kategorycznie nigdy nie logować się do prywatnych kont na służbowym urządzeniu. Co więcej nie należy przechowywać żadnych danych służbowych na prywatnym komputerze, ze względu na fakt iż jeśli zostanie on zainfekowany nie wyciekają jedynie dane prywatne, ale także dane służbowe. Mogłoby się to wydawać oczywiste, jednakże przykład ostatnich miesięcy [9] , pokazuje, że nawet najważniejsze osoby w państwie nie przestrzegają zasad podstawowej higieny korzystania z internetu.

W celu ochrony przed atakami socjotechnicznymi należy przede wszystkim czytać uważnie każdą wiadomość, którą odczytujemy, nie wolno wchodzić w linki, co do których pochodzenia nie jesteśmy pewni. Częstym mitem jest to, że przekopiowanie linku bezpośrednio do pola wyszukiwarki internetowej chroni przed wczytaniem złośliwej domeny. Jest to całkowita nieprawda, gdyż nie ma znaczenia, czy naciśniemy na link w programie do przeglądania poczty, czy go wkleimy do wyszukiwarki, tak czy inaczej przekieruje nas na daną stronę. To co należy jednak robić to wykonywanie tzw. zwisu nad linkiem, należy go wykonać poprzez najechanie na hiperłącze kursorem, bez naciskania klawiszy myszy, wtedy powinien wyświetlić się cały adres strony, następnie możemy sprawdzić, czy nie zawiera on błędów. Chodzi tu o to adres strony głównej, który znajduje się pomiędzy ukośnikami (konkretnie pomiędzy 2 a 3 ukośnikiem np. https://……/, w miejscu, gdzie znajdują się kropki powinien być widoczny adres strony głównej, do której prowadzi link). Obecnie uważa się również, że samo posiadanie przez daną stronę certyfikatu bezpieczeństwa, czyli https, zamiast zwykłego http, nie chroni przed wgraniem złośliwego oprogramowania ze względu na fakt, iż to, że połączenie jest zabezpieczone nie oznacza, że sama strona nie zawiera np. malware. Zatem nie należy się tym kierować przy ocenie wiarygodności linku, zamiast tego należy zwróci uwagę na literówki w adresie strony głównej np. Czy zamiast „https://www.pkobp.pl", nie mamy do czynienia z „https://www.pkobq.pl".

Przed atakiem socjotechnicznym bardzo trudno jest się obronić, niemniej najważniejsze jest zachowanie spokoju i niepopadanie w rutynę, za każdym razem zanim wejdziemy w dany link, czy wykonamy polecenie z wiadomości, powinno się odpowiedzieć na pytania: czy spodziewałem się tej wiadomości? Czy muszę ją teraz otworzyć? Jakie konsekwencje poniosę, jeśli nie wykonam polecenia z e-maila? Co do zasady, jeśli nie jesteśmy pewni, nie wchodźmy w linki, nie pobierajmy plików. Jeśli jest to wiadomość od znajomego, której się nie spodziewamy, zadzwońmy do niego z pytaniem, czy wysłał on ją do nas. Trzeba wyłączyć automatyczne myślenie wszędzie tam, gdzie jest to możliwe [10] Tego typu działania są istotne zwłaszcza w przypadku lekarzy i ratowników medycznych, którzy mają dostęp w pracy do systemów zawierające dane pacjentów.

Środki ochronne dla pracowników systemu opieki zdrowotnej w celu zapobiegania cyberzagrożeniom

Pracownicy medyczni bez względu na zajmowane stanowisko (pielęgniarki, lekarze, ratownicy, dyspozytorzy i inni) wszyscy są równo narażeni na cyberzagrożenia i każdy z nich nieświadomie może przyczynić się do zainfekowania swojego zakładu pracy. W dobie Elektronicznej Dokumentacji Medycznej i stosowania wielu systemów wymiany informacji w służbie zdrowia [11] kontakt z komputerami ma większość pracowników służb medycznych, istotne jest zatem, by korzystali oni z niego odpowiedzialnie, stąd potrzeba informowania ich na temat zagrożeń w sieci i nie tylko.

Zadaniem każdego pracownika w tym temacie powinna być przede wszystkim ochrona urządzenia, którym dysponują. Nie mogą dopuszczać do tego, by ktokolwiek wkładał do komputerów/innych urządzeń pendrive, czy jakikolwiek sprzęt. Każdy podejrzany sprzęt elektroniczny, którego wcześniej nie zauważyli powinno być zgłaszane przełożonym, należy mieć na uwadze, że mogą być to urządzenia mające na celu przekierowywanie danych, czy wgranie złośliwego oprogramowania. Pamiętać trzeba również o tym, że nawet nasze własne urządzenie typu pen-drive, czy dysk przenośny mogą zawierać nieświadomie przyniesione szkodliwe oprogramowania. Pracownicy nie powinni w pracy korzystać z internetu do celów prywatnych, gdyż mogą oni niechcący wejść na stronę ze złośliwym oprogramowaniem. Należy w tym miejscu postawić sobie wyraźną granice między sferą zawodową a prywatną. Dobrym nawykiem, który powinien przerodzić się w normę jest wylogowywanie się z komputera za każdym razem, gdy dany pracownik od niego odchodzi, hasło do komputera musi być zapamiętane, kategorycznie zabronione jest trzymanie go zapisanego na kartce znajdującej się na biurku.

W celu ochrony własnych danych pracownicy systemu opieki zdrowotnej powinni korzystać również prywatnie z oprogramowań antywirusowych, a także posiadać długie i skomplikowane hasła (co najmniej 20 znaków) do każdego z kont internetowych, takie hasło powinno być użyte raz tylko do jednego konta. Dobrym rozwiązaniem jest w tym wypadku korzystanie z menedżerów haseł np. 1password, czy pęk kluczy od Apple (dotyczy tylko sprzętu od firmy Apple). Takie oprogramowania są na chwilę obecną zalecane przez specjalistów z dziedziny cyberbezpieczeństwa, tworzą i zapamiętują one również skomplikowane hasła, takie aplikacja jest z kolei chroniona przez tzw. master password, czyli bardzo silne hasło, które tylko my jako właściciele powinniśmy pamiętać, by zalogować się do menedżera, jest ono najważniejsze. Ponadto warto rozważyć zakup fizycznego klucza uwierzytelniania dwuskładnikowego U2f (jest to urządzenie przypominające pen-drive) np. YubiKey, który chroni przed phishingiem, przy logowaniu do konta, gdyż nawet jeśli przestępcy posiadają hasło i login, nie są jednak wstanie się zalogować bez posiadania tego konkretnego klucza. Na dzień dzisiejszy chroni ono przed nieautoryzowanym logowaniem. Do jednego konta należy przypiąć dwa takie klucze, jeden powinno się nosi przy sobie, drugi powinno się schować w bezpiecznym miejscu [12]. Jest to rozwiązanie dość drogie, gdyż koszt 2 kluczy to wydatek kilkuset złotych, niemniej w ocenie autora jest to absolutne minimum w przypadku kluczowych pracowników sektora ochrony zdrowi tj. dyrektorzy, ordynatorzy itp.. W przypadku gdy jednak zakup klucza przerasta możliwości finansowe danej osoby zaleca się korzystanie z jakiekolwiek sposobu uwierzytelniania wielopoziomowego, może być to np. kod z wiadomości sms, wiadomość e-mail, czy dedykowana aplikacja do uwierzytelniania logowania.

Administratorzy sieci danego szpitala (jednostki medycznej) powinni także dbać o bezpieczeństwo systemów informatycznych i urządzeń poprzez pilnowanie, by na każdym komputerze była zainstalowana najnowsza wersja oprogramowania, ponadto każdy komputer powinien być wyposażony w system antywirusowy, a samo urządzenie powinno być regularnie skanowany. Warto rozważyć także zabezpieczenie urządzeń tj. drukarki, przez które osoby niepożądane mogą dostać się do sieci wi-fi szpitala, a przez co też są one w stanie zainfekować urządzenia do niej podłączone. Stąd dobrą praktyką jest segmentacja takowej sieci i ustawienie haseł do wi-fi, które nie są domyślnymi dla danego modelu routera.

Podatności w wybranych urządzeniach medycznych

Podatność w urządzeniach GE Datex Ohmeda Aespire 7900 i 7100. W tych aparatach anestezjologicznych w 2019 roku wykryto podatność pozwalającą na zdalne: wyciszenie alarmów, zmianę ustawienia daty i godziny, zmiany danych odnośnie składu podawanego gazu, zmianę ciśnienia barometrycznego, oraz

przełączanie między środkami znieczulającymi. Aby tego dokonać atakującemu wystarczy dostanie się do serwerów danej jednostki świadczącej usługi medyczne. Następnie poprzez ingerencje w protokole jest on wstanie realnie zaszkodzić pacjentowi, jeśli urządzenie było podpięte do sieci komputerowej [13]. Największym problemem w omawianym przypadku jest jednak fakt, że pomimo tego iż opisywane ww. urządzenia są bardzo zaawansowanym sprzętem, nie posiadają one skutecznych systemów zabezpieczenia przed atakami cybernetycznymi, co jest sytuacją stwarzającą ogromne zagrożenie dla pacjentów, jak i dla lekarzy, którzy zmuszeni są pracować na sprzęcie, co do którego nie mają pewności.

Podatność w oprogramowaniu urządzeń CIED (cardiovascular implantable electronic devices, tłum. z ang. Elektroniczne urządzenia kardiologiczne), a konkretnie programatorów Mediatronic CareLink 2090 i CareLink Encore 29901. Sama podatność polegała na tym, że istniała luka w zabezpieczeniach w trakcie aktualizacji urządzenia przez SDN (Software Defined Network, z ang. tłum. Programowalna sieć komputerowa), można było zainstalować oprogramowanie niepochodzące od producenta, wskutek czego mogło dojść do zaburzenia pracy urządzenia, a w konsekwencji spowodować nawet zgon osoby korzystającej z tak zainfekowanego urządzenia medycznego. Problem został wykryty w 2018 i natychmiast został usunięty poprzez wyeliminowanie opcji aktualizacji przez DNS, pozostawiając jedynie na aktualizację przez USB [14]. Firma Medtronic w swojej notatce dotyczącej bezpieczeństwa zaznaczyła, że nie doszło do żadnego ataku na ich urządzenie, niemniej sam fakt tego, iż w ich programatorach występowała tego typu podatność jest bardzo niepokojący, gdyż w przypadku takich urządzeń nie powinno dochodzić do tak poważnych luk, co gorsza nie istniało tam żadne dodatkowe zabezpieczenie przez co cyberprzestępcy mieli łatwe zadanie.

Podatność w niektórych modelach stacji centralnych GE, oraz serwerów telemetrii ApexPro. Niniejszą podatność wykryto w styczniu 2020, polegała ona na tym, że w przypadku gdy nieupoważniona osoba miała dostęp fizyczny podczas podłączania sieci Mission Critical (MC), tudzież Information Exchange (IX) istniało ryzyko na manipulacje w oprogramowaniu, pozwalające na atak cybernetyczny w serwerach telemetrii CARESCAPE Telemetry Server, serwerach telemetrii ApexPro, a także urządzeniom stacji centralnej CARESCAPE Central System (CSCS) w wersji 1, a także w systemach Central Information Center. Poprzez ingerencje do ww. urządzeń i systemów, cyberprzestępcy byli w stanie zablokować monitorowanie pacjentów, a także wyłączyć alarmy działające na urządzeniach. Firma GE Healtcacre, która oferowała powyższe produkty wydała specjalne zawiadomienie, a także wypuściła aktualizację oprogramowań uniemożliwiającą ten typ ataku. Co więcej należy zaznaczyć, że nie odnotowano próby takiego ataku [15]. Przykład produktów od firmy GE Healtcare jest o tyle istotny, ze względu na fakt, iż obrazuje on to, czego może dokonać niepożądana osoba, w miejscu, gdzie dostępne są urządzenia medyczne, wskazuje to na potrzebę zapewnienia nie tylko ochrony od strony zabezpieczeń komputerowych, ale także tych fizycznych w celu zapewnienia bezpieczeństwa systemom informatycznym.

Podstawowe sposoby na zapobieganie cyberatakom na placówki medyczne

Omawiając środki prewencyjne wobec cyberataków, należy na samym początku zaznaczyć, że nie są one ws tanie zapewnić pełnego bezpieczeństwa, niemniej ich stosowanie jest w stanie w znaczący sposób utrudnić działania przestępne ludziom, którzy chcą się włamać do systemów w placówkach medycznych. Jedną z podstawowych zasad odnośnie bezpieczeństwa takich obiektów jak szpitale czy przychodnie jest zapewnienie fizycznego bezpieczeństwa serwerowniom, routerom i innym urządzeniom elektronicznym służącym do przekazywania danych. Należy maksymalnie uniemożliwić dostęp osobom postronnym do tego typu pomieszczeń. Ponadto sieć w danej placówce medycznej powinna być prawidłowo posegmentowana, zaś najbardziej kluczowe sieci m.in. sieć MC i IX powinnny być całkowicie od siebie odizolowane. Na komputerach powinny być zainstalowane aktualne oprogramowania wraz z programami antywirusowymi. Należy także zwrócić uwagę na politykę stosowania haseł w ramach funkcjonowania zakładu opieki zdrowotnej, nie mogą to być hasła domyślne od producentów, powinny być one zmieniane w pewnych odstępach czasowych, a następnie zapamiętywane, a nie zapisywane przez pracowników, w przypadku zaś gdy pracownik odchodzi z pracy należy zmienić hasła na wszystkich urządzeniach co do których miał dostęp. Należy także wykonywać regularne kopie zapasowe przechowywanych danych. Autor proponuje również wprowadzenie

szkoleń dla całego personelu nie pomijając nikogo. Szkolenia takie, aby miały sens powinny być połączone z symulowanymi incydentami z zakresu bezpieczeństwa, chodzi tu o kampanie phishingowe (wynajęta firma z zakresu bezpieczeństwa w cyberprzestrzeni wykonuje symulowane ataki na służbowe konta pracowników w celu sprawdzenia wskaźnika podatności i opracowaniu programu naprawczego), oraz testach penetracyjnych polegających na tym, że wynajęty pracownik wyspecjalizowanej firmy sprawdza podatności poszczególnej placówki, próbuje on uzyskać dostęp do danych przechowywanych na serwerach, a także fizycznie wchodzi do budynku, gdzie wykonuje wcześniej ustalone z zarządem zadania [16]. Tylko w taki sposób możliwe jest zapewnienie bezpieczeństwa na optymalnym poziomie, chodzi tu o przeszkolenie pracowników, uświadamianie ich odnośnie zagrożeń, co może pozytywnie wpłynąć na bezpieczeństwo. Tego typu testy pokazują również słabe punkty, które należy wyeliminować. Oczywiste jest jednak że testy są kosztowne, co może być przeszkodą dla wielu placówek medycznych. Niemniej wprowadzenie takich działań w rzeczywisty sposób podniosłoby bezpieczeństwo urządzeń, a co idzie za tym danych przechowywanych na nich w sektorze zdrowia. Należy także opracować strategię na wypadek, gdy zabezpieczenia nie zadziałają i dojdzie do ingerencji w systemy informatyczne danej placówki. Taka strategia powinna uwzględniać kolejność działania w przypadku takiego zdarzenia, oraz to które systemy można wyłączyć i w jakiej kolejności, a także do jakiego organu należy zgłosić sprawę. Takim organem może być np. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV (z ang Computer Security Incydent Response Team) [17]

W Polsce w chwili obecnej instytucją wspierającą cyfryzację w służbie zdrowia jest Centrum Systemów Informatycznych Ochrony Zdrowia wydaje ona m.in. zalecenia odnośnie stosowania Audytów Zewnętrznych i Wewnętrznych [18], a także innych metod ochrony placówek medycznych, należy ocenić je pozytywnie a zawarte w nich środki ochrony po prawidłowym zaimplementowaniu są wstanie w realny sposób chronić Zakłady Opieki Zdrowotnej. Ponadto przeprowadza ona również szkolenia dla personelu medycznego, w tym te z okresu obsługi Elektronicznej Dokumentacji Medycznej.

Podsumowanie

Polski sektor ochrony zdrowia jest szczególnie narażony na ataki cybernetyczne ze względu na fakt, iż nie przeprowadzono jeszcze zmasowanego dużego ataku w naszym kraju, jak to miało miejsce w ostatnim czasie w innych państwach. Na podstawie danych z państw tj. Kanada, czy USA jesteśmy wstanie odnotować znaczący wzrost tego typu zdarzeń. Należy zatem skupić się na ochronie systemów informatycznych i urządzeń używanych przez Polską służbę zdrowia. Tego, że atak nastąpi można być niemalże pewnym ze względu na postępującą cyfryzację, a także co za tym idzie rozwój cyberprzestępczości. Ponadto dane, które przechowywane są na tych serwerach są bardzo kuszące dla atakujacych. Stąd bardzo istotną kwestią jest uświadamianie pracowników sektora ochrony zdrowia co do istnienia takich zagrożeniach, a także ich skutków. Przykład z Dusseldorfu obrazuje nam jakie skutki może nieść za sobą niesprawność systemów informatycznych w tym sektorze. Przed osobami odpowiedzialnymi za bezpieczeństwo systemów w placówkach medycznych stoi ogromne zadanie od strony technicznej, by zabezpieczyć tak cenne dane, niemniej równie istotne jest przeszkolenie z zakresu podstawowych cyberzagrożeń każdego z pracowników systemu ochrony zdrowia, tak by wiedzieli oni w jaki sposób reagować w przypadku wystąpienia ataku.

Konflikt interesów / Conflict of interest
Brak / None

Adres do korespondencji / Correspondence address
Szymon Nawrocki
Wydział Nauk Stosowanych
Wyższa Szkoła Przedsiębiorczości
im. Księcia Kazimierza Kujawskiego w Inowrocławiu
ul. Najświętszej Marii Panny 19a, 88-100 Inowrocław
☎ (+48 22) 627 39 86
szymonnawrocki@tutanota.com

Piśmiennictwo/References

1. Richardson, R North, M. M., Ransomware: Evolution, Mitigation and Prevention (2017). Faculty Publications. 4276. 10-17 https://digitalcommons.kennesaw.edu/facpubs/4276/?utm_source=digitalcommons.kennesaw.edu%2Ffacpubs%2F4276&utm_medium=PDF&utm_campaign=PDFCoverPages, dostęp w dniu 03.08.2021.
2. https://www.cyberdefence24.pl/pandemia-cyberprzestepczosci-dotyka-placowki-medyczne dostęp w dniu 03.08.2021.
3. https://www.cyberdefence24.pl/atak-ransomware-w-usa-400-placowek-medycznych-pod-ostrzalem-cyberprzestepcow dostęp w dniu 03.08.2021.
4. https://www.healthcareitnews.com/news/universal-health-services-faces-67-million-loss-after-cyberattack dostęp w dniu 03.08.2021.
5. https://www.cyberdefence24.pl/pierwsza-ofiara-smiertelna-ataku-ransomware-zarzut-nieumyslnego-spowodowania-smierci dostęp w dniu 03.08.2021.
6. Mittnick K.D, Simon W.L. Łamałem ludzi nie hasła. Sztuka Podstępu wydanie II: Helion, Gliwice; 2016.
7. Hadnagy, C., Fincher, M. Mroczne odmęty phishingu. Nie daj się złowić!, Gliwice: Helion. 2016.:27-56
8. Wasiuta O, Klepka R. (red.) Vademecum Bezpieczeństwa Informacyjnego N-Z, - Rokitowska J, Wasiuta O. Social media Intelligence (SOCMINT): Instytut Nauk o Bezpieczeństwie, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej; Kraków 2019, tom 2.:362-371
9. https://niebezpiecznik.pl/post/michal-dworczyk-wyciek-telegram/ dostęp w dniu 03.08.2021
10. Trejderowski, T. Kradzież tożsamości. Terroryzm Informatyczny. Warszawa: ENETEIA Wydawnictwo Psychologii i Kultury; 2013.:24-33
11. https://ezdrowie.gov.pl/portal/artykul/elektroniczna-dokumentacja-medyczna-edm dostęp w dniu 03.08.2021 .
12. Miśko M. Czym jest i jak używać klucza U2F. https://www.geekweb.pl/software/poradniki/item/1377-klucz-u2f-jak-uzywac dostęp w dniu 03.08.2021.
13. https://cisomag.eccouncil.org/anaesthetic-machines-vulnerable-to-cyber-attacks-researchers/ dostęp w dniu 03.08.2021
14. Pilna notatka dotycząca bezpieczeństwa z dnia 12.08.2018, Medtronic. http://www.urpl.gov.pl/sites/default/files/FSN_Medtronic_18.10.2018.pdf dostęp w dniu 03.08.2021
15. Pilne zawiadomienie dotyczące bezpieczeństwa z dnia 27 stycznia 2020, GE Healtcare, http://www.urpl.gov.pl/sites/default/files/FSN_GE_31.01.2020.pdf dostęp w dniu 03.08.2021.
16. Banasiński C, Rojszczyk M. Cyberbezpieczeństwo: Wolters Kluwer, Warszawa; 2020:156-157
17. https://csirt.gov.pl/cer dostęp w dniu 03.08.2021.
18. Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej, Centrum Systemów Informacyjnych Ochrony Zdrowia, Warszawa 2017.