DOBRE PRAKTYKI

cyberbezpieczeństwo w szpitalach

OGÓLNOPOLSKIE STOWARZYSZENIE
SZPITALI PRYWATNYCH

medycynaprywatna.pl
PRACODAWCY MEDYCYNY PRYWATNEJ

Projekt graficzny i skład:
Joanna Piekarska-Norek

Partner merytoryczny: koma nord®

Wydawcy: OGÓLNOPOLSKIE STOWARZYSZENIE SZPITALI PRYWATNYCH

medycynaprywatna.pl
PRACODAWCY MEDYCYNY PRYWATNEJ

Druk: TOTEM

ISBN: 978-83-946197-2-5

Szanowni Państwo, członkowie PMP

wspólnie z Ogólnopolskim Stowarzyszeniem Szpitali Prywatnych podjęliśmy się realizacji działań, mających na celu poprawę i wzmocnienie cyberbezpieczeństwa wśród naszych członkowskich organizacji. Pracodawcy Medycyny Prywatnej kwestią cyberbezpieczeństwa w ochronie zdrowia zajmują się od dosyć dawana, są współtwórcami Kodeksu Branżowego RODO w Ochronie Zdrowia, który co roku jest głównym punktem Konferencji „RODO & Cyberbezpieczeństwo w Zdrowiu", której byliśmy współinicjatorem i która w tym roku ma kolejną edycję.

Dr Andrzej Mądrala
prezes zarządu
Pracodawców Medycyny Prywatnej

Szanowni Państwo, członkowie OSSP

przekazujemy do Państwa rąk kolejne opracowanie z serii „dobrych praktyk" – tym razem tematem jest cyberbezpieczeństwo – problem coraz bardziej palący, gdyż ilość ataków na jednostki publiczne i prywatne rośnie z każdym miesiącem, a świadomość potrzeby ochrony u właścicieli i menedżerów zarządzających placówkami medycznymi jest niewystarczająca. Niniejsza publikacja, będąca wspólnym dokumentem Ogólnopolskiego Stowarzyszenia Szpitali Prywatnych i Pracodawców Medycyny Prywatnej, ma zwrócić na ten problem uwagę.

Andrzej Sokołowski
prezes Ogólnopolskiego
Stowarzyszenia Szpitali Prywatnych

SPIS TREŚCI

Paulina Prencel

Cyberbezpieczeństwo – czy da się je zapewnić w jednostkach ochrony zdrowia?

Przeglądając serwisy internetowe czy nagłówki gazet z kraju i ze świata, z roku na rok, a nawet z miesiąca na miesiąc, można znaleźć coraz więcej doniesień dotyczących ataków hakerskich na jednostki ochrony zdrowia.

Tylko w grudniu 2022 r. pojawiło się sporo takich informacji:

- Cyberatak w brooklyńskim szpitalu, który zapewnia opiekę ubogim nowojorczykom („New York Times", 12 grudnia 2022 r.) (1);
- Wiodący szpital stanowy w Indiach przywraca systemy po cyberataku (Reuters, 6 grudnia 2022 r.) (2);
- Francuski szpital zawiesza działalność po cyberatakach (France 24, 5 grudnia 2022 r.) (3).
- W minionym roku do tego typu incydentów dochodziło także w Polsce, głośno było o cyberatakach na Lotnicze Pogotowie Ratunkowe (w lutym 2022 r.) czy Instytut Centrum Zdrowia Matki Polki (w listopadzie 2022 r.).

Wzrost cyberataków w ochronie zdrowia

Tego typu ataki, wymierzone w obszar ochrony zdrowia, są niezwykle niebezpieczne, a ich konsekwencje najbardziej dotkliwe, ponieważ stanowią bezpośrednie zagrożenie dla pacjentów.

Jak podaje portal Cyberdefence24.pl, trzy lata temu w Niemczech zmarła kobieta po cyberataku na klinikę w Düsseldorfie, a w marcu ubiegłego roku po ataku hakerów na szpital na Korsyce, trudno było przeprowadzać zgodnie z planem operacje na szpitalnym oddziale onkologicznym (4). Na początku grudnia ubiegłego roku zarząd jednego ze szpitali na przedmieściach Paryża po tym, jak zaszyfrowano mu systemy telefoniczne i komputerowe, został zmuszony do przeniesienia noworodków i pacjentów oddziału intensywnej terapii do innych placówek (5). Z kolei, jak informowało pod koniec 2022 r. francuskie ministerstwo zdrowia, kierujący szpitalem w Wersalu pod Paryżem po tym, jak został dotknięty cyberatakiem, musieli odwołać operacje i przenieść niektórych pacjentów do innych jednostek. Incydent doprowadził do całkowitej reorganizacji tej placówki (6). Wiodący szpital w stolicy Indii, jak podaje Reuters, po cyberataku, który sparaliżował jego działalność, wrócił do normalności dopiero po prawie dwóch tygodniach (2).

Najczęściej skutkiem cyberataków są utrudnienia w funkcjonowaniu jednostek ochrony zdrowia, związane z czasowym brakiem możliwości korzystania z rozwiązań cyfrowych, co pośrednio również może stać się zagrożeniem dla zdrowia i życia pacjentów.

W trzech szpitalach, wchodzących w skład One Brooklyn Health, na przełomie listopada i grudnia, podczas gdy eksperci pracowali nad pełnym przywróceniem tych jednostek w tryb online, lekarze i pielęgniarki zmuszeni byli wrócić do tradycyjnych narzędzi – długopisu i papieru, bowiem elektroniczny system medyczny nie działał tam przez kilka tygodni. Sama opieka nad pacjentem w tym czasie znacząco się nie zmieniła, natomiast wydłużał się czas kompletowania wyników badań laboratoryjnych czy radiologicznych (1).

Tego typu przykłady można by mnożyć. W Polsce 14 lutego ub.r. ofiarą bezprecedensowego ataku stało się Lotnicze Pogotowie Ratunkowe. Zgodnie z oświadczeniem, wydanym przez LPR, po raz pierwszy w jego hi-

storii ktoś próbował zachwiać działaniem Śmigłowcowej Służby Ratownictwa Medycznego oraz lotniczego transportu sanitarnego. Zdarzenie miało postać ransomware, a przestępcy zażądali 390 tysięcy dolarów okupu za odszyfrowanie danych (7). W listopadzie hakerzy zaatakowali Instytut Centrum Zdrowia Matki Polki w Łodzi. Aby zminimalizować skutki cyberataku, zdecydowano się na czasowe wyłączenie systemów informatycznych. Szpital starał się prowadzić standardową obsługę pacjentów z wykorzystaniem tradycyjnej dokumentacji (8).

Obie instytucje podejmowały po cyberatakach intensywne działania, których celem było doprowadzenie do jak najszybszego pełnego ich uruchomienia. W działaniach tych uczestniczyły zespoły IT przy wsparciu Ministerstwa Zdrowia, Centrum e-Zdrowia, NASK – Państwowego Instytutu Badawczego, CERT Polska, Komendy Głównej Policji czy Komendy Stołecznej Policji (7, 8).

Atrakcyjny cel dla cyberprzestępców

Jednostki ochrony zdrowia są atrakcyjnym celem dla cyberprzestępców. Charakter ich działalności powoduje, że gromadzą wrażliwe dane medyczne oraz używa się w nich technologii i rozwiązaniach cyfrowych. Na co dzień wykorzystywana jest tu zarówno nowoczesna aparatura niezbędna do diagnozowania i leczenia chorych, jak i systemy potrzebne do obsługi pacjentów, które służą do rejestracji czy zarządzania ich danymi. Urządzenia medyczne, takie jak na przykład aparaty rentgenowskie, pompy insulinowe czy defibrylatory, odgrywają kluczową rolę we współczesnej opiece zdrowotnej. Jednak dla osób odpowiedzialnych za bezpieczeństwo online i ochronę danych pacjentów nowoczesny sprzęt medyczny spełniający określone cele, jak na przykład monitorowanie tętna czy wydawanie leków, jest kolejnym ogniwem, na którym mogą koncentrować się ataki. Mimo, że same urządzenia nie przechowują danych pacjentów, cyberprzestępcy mogą wykorzystać je do przeprowadzenia ataku na serwer, który zawiera cenne informacje, a w najgorszym przypadku całkowicie przejąć kontrolę nad aparaturą, uniemożliwiając niezbędne leczenie ratujące życie (9).

W raporcie specjalnym, opracowanym przez ECRI, amerykańską niezależną instytucję zajmującą się technologią i bezpieczeństwem opieki zdrowotnej, dotyczącym 10 największych zagrożeń związanych z technologią medyczną w roku 2022, pierwsze miejsce zajęły cyberataki, mogące zakłócić realizację świadczeń opieki zdrowotnej i zagrozić bezpieczeństwu pacjenta (10).

Priorytet dla zarządzających szpitalami

Patrząc na skalę ataków hakerskich trudno nie wysnuć wniosku, że cyberbezpieczeństwo powinno być dziś jednym z najwyższych priorytetów dla zarządzających szpitalami, którzy nie mają już chyba wątpliwości, że stanowi ono olbrzymie ryzyko dla jednostek ochrony zdrowia. Ryzyko finansowe, prawne, ale przede wszystkim związane z zagrożeniem bezpieczeństwa pacjentów. W tej sytuacji istotne jest podejmowanie wszelkiego rodzaju działań, prowadzących do jego minimalizowania.

Na pewno ważnym elementem w tym zakresie jest edukowanie personelu szpitalnego. Wszyscy pracownicy powinni mieć poczucie, jak istotny jest wpływ zagrożeń cybernetycznych na funkcjonowanie jednostek ochrony zdrowia i zachowywać ostrożność, by chronić pacjentów.

Znaczącą rolę w minimalizowaniu ryzyka pełni także uwierzytelnianie wieloskładnikowe. Organizacje opieki zdrowotnej powinny wymagać od użytkowników systemu podania więcej niż jednego czynnika weryfikacyjnego w celu uzyskania dostępu (11). Aby zwiększyć ochronę, zaleca się także okresowe wymuszanie zmian hasła. Często również automatyzacja – dzięki temu, że zmniejsza prawdopodobieństwo wystąpienia błędu ludzkiego – może pomóc minimalizować ryzyko związane z cyberatakami.

Istotne znaczenie w tym aspekcie mają także zapory sieciowe, które są pierwszą linią obrony w obszarze bezpieczeństwa sieci. Stanowią one barierę pomiędzy zabezpieczoną siecią wewnętrzną, która jest kontrolowana, a siecią zewnętrzną – Internetem. Zapory sieciowe wdraża się po to, aby zatrzymywać zagrożenia, takie jak zaawansowane złośliwe oprogramowania czy ataki na poziomie aplikacji (12).

Najczęstsze incydenty związane z cyberbezpieczeństwem

W przygotowanym przez zespół CERT Polska działający w strukturach NASK – Państwowego Instytutu Badawczego raporcie rocznym za 2021 rok, dotyczącym zgłoszonych incydentów związanych z cyberbezpieczeństwem, odnotowano wzrost obsłużonych incydentów na poziomie 182% w porównaniu do roku poprzedniego (13). Wydaje się, że statystyki, wskazujące na liczbę tego typu incydentów za rok 2022, będą jeszcze wyższe.

Jak wskazuje raport, najczęstszy w 2021 r. był phishing, który stanowił aż 76,57% wszystkich obsłużonych incydentów, a w stosunku do 2020 r. odnotował wzrost

o 196%, osiągając wartość 22 575 incydentów. Ta metoda oszustwa była wskazywana jako najbardziej powszechna także przez amerykańską Agencję ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA), która wskazuje, że ponad 90% udanych cyberataków rozpoczyna się od phishingowej wiadomości e-mail (9). Drugie pod względem częstości było szkodliwe oprogramowanie. Ten typ stanowił w 2021 r. 9,66% wszystkich obsłużonych incydentów, a w porównaniu do roku 2020 odnotował wzrost wartości o 281% (13).

CERT Polska rejestruje incydenty dotyczące cyberbezpieczeństwa, klasyfikuje je, a następnie przypisuje do odpowiednich sektorów, których dotyczyły. Z danych opublikowanych w raporcie z 2021 roku wynika, że sektor ochrony zdrowia znalazł się na 13. miejscu spośród 29 różnych obszarów, odnotowując liczbę 150 takich incydentów. Najprawdopodobniej w raporcie za 2022 rok należy oczekiwać wzrostu tej liczby. Sektory, które w 2021 r. najczęściej były atakowane, to: media (8339 incydentów), handel hurtowy i detaliczny (5125), poczta i usługi kurierskie (4338), energetyka (4084), osoby fizyczne (2464), infrastruktura cyfrowa (1606) oraz bankowość (947).

Program wsparcia dla jednostek ochrony zdrowia

Dostrzegając wagę problemu, pod koniec maja 2022 r. Narodowy Fundusz Zdrowia ogłosił program wsparcia cyberbezpieczeństwa w placówkach medycznych. Zgodnie z jego założeniami, jednostki ochrony zdrowia mają otrzymać nawet 900 tys. zł na podniesienie bezpieczeństwa systemów teleinformatycznych (17). O te środki mogły wnioskować szpitale, które realizują świadczenia w ramach leczenia szpitalnego, rehabilitacji leczniczej, lecznictwa uzdrowiskowego oraz opieki psychiatrycznej i leczenia uzależnień. Finansowane są wydatki poniesione od 29 kwietnia do 31 grudnia 2022 r., a środki na ten cel pochodzą z Funduszu Przeciwdziałania COVID-19.

Finansowaniu podlegają zakup i wdrożenie systemów teleinformatycznych oraz związanych z nimi usług, których celem jest nie sama informatyzacja jako taka, lecz podniesienie poziomu bezpieczeństwa w placówkach leczniczych. Szpitale mogły więc wnioskować o środki na urządzenia, oprogramowanie i usługi teleinformatyczne, które zapobiegają, wykrywają lub zwalczają cyberataki (jak np. systemy do tworzenia kopii danych, systemy antywirusowe, systemy kontroli dostępu administracyjnego i zarządzania uprawnieniami, urządzenia i oprogramowanie zabezpieczające sieć, tzw. firewall czy systemy zapewniające bezpieczeństwo poczty elektronicznej). Te środki można było również przeznaczyć na wsparcie eksperckie, dotyczące cyberbezpieczeństwa oraz szkolenia z cyberbezpieczeństwa dla kadry zarządzającej i pracowników.

Aby skorzystać z finansowania, należało do 30 listopada 2022 r. złożyć do dyrektora właściwego oddziału wojewódzkiego NFZ wniosek o zawarcie umowy. Do wniosku trzeba było dołączyć raport z Systemu Statystyki Ochrony Zdrowia, który potwierdzał wypełnienie ankiety badającej poziom bezpieczeństwa systemów teleinformatycznych.

Najczęstsze incydenty związane z cyberbezpieczeństwem

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia poufnych informacji (np. danych logowania), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań (14).

Szkodliwe oprogramowanie (z ang. *malware* – zbitka słów *malicious* – „złośliwy" i *software* – „oprogramowanie") – ogół programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkownika. Wśród rodzajów szkodliwego oprogramowania wyróżnia się m.in.: wirusy, konie trojańskie, oprogramowanie szpiegujące czy oprogramowanie wymuszające okup (ang. *ransomware*) (15).

Ransomware (zbitka słów ang. *ransom* – „okup" i *software* – „oprogramowanie") – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego. Programy typu *ransomware* należą do tzw. szkodliwego oprogramowania (16).

Warunkiem uzyskania wsparcia przez szpital było zawarcie umowy i złożenie w siedzibie właściwego oddziału Funduszu, nie później niż do 16 grudnia 2022 r., dokumentacji: wniosku o wypłatę finansowania, specyfikacji finansowania, kopii dokumentów, które potwierdzają nabycie i sfinansowanie, w okresie od 29 kwietnia 2022 roku do 31 grudnia 2022 roku, przedmiotu finansowania oraz wyniku audytu bezpieczeństwa.

Program ogłoszony przez Narodowy Fundusz Zdrowia na pewno okaże się pomocny dzięki wprowadzanym do szpitali rozwiązaniom prowadzącym do minimalizowania ryzyka związanego z cyberatakami. Należy natomiast pamiętać, że digitalizacja różnych obszarów, w tym sektora ochrony zdrowia, wciąż się rozwija, wobec czego wprowadzanie zabezpieczeń przed tego typu przestępczością, będzie procesem długotrwałym.

Podsumowanie

W ostatnich latach liczba cyberataków w różnych obszarach sukcesywnie rośnie. Coraz częściej dotyczą one również ochrony zdrowia. Cyfryzacja tego sektora bez rzeczywistych zabezpieczeń skupia na sobie uwagę cyberprzestępców, których ataki mogą w zasadzie wyłączyć z funkcjonowania cały szpital.

Podniesienie bezpieczeństwa informatycznego powinno być dziś jednym z najwyższych priorytetów dla zarządzających szpitalami. Ryzyko, związane z cyberprzestępczością, nie tylko finansowe czy prawne, ale przede wszystkim dotyczące bezpieczeństwa pacjentów, należy brać pod uwagę oraz umiejętnie nim zarządzać.

Odpowiadając na pytanie postawione w tytule tego tekstu: „Czy da się zapewnić cyberbezpieczeństwo w jednostkach ochrony zdrowia?", można stwierdzić, że jest to bardzo trudne zadanie. Jednak należy dodać, że trzeba podejmować wszelkie konieczne działania, które będą prowadzić do minimalizowania ryzyka związanego z tym obszarem.

Paulina Prencel

menedżer redakcji w Elamed Media Group. Od 2011 roku prowadzi czasopismo „Ogólnopolski Przegląd Medyczny", które dostarcza informacji z zakresu najnowszych technologii medycznych, wyposażenia i infrastruktury szpitalnej oraz informatyki i komunikacji w jednostkach ochrony zdrowia. Odpowiada za koordynację wielu projektów z tego obszaru, m.in.: serwisu dlaSzpitali.pl, kongresu Nowoczesny Pion Techniczny czy konferencji Szpital XXI wieku – planowanie, projektowanie, budowa, działalność.

Piśmiennictwo

https://www.nytimes.com/2022/12/12/nyregion/brooklyn-hospital-cyberattack.html.
https://www.reuters.com/world/india/indias-leading-state-hospital-recovers-systems-after-cyber-attack-2022-12-06/.
https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks.
https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-szpital-zadanie-10-mln-dolarow-okupu.
https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638.
https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks.
https://www.lpr.com.pl/pl/oswiadczenie-lpr/.
https://www.iczmp.edu.pl/2022/11/03/cyberatak-na-iczmp/.
https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.
https://www.ecri.org/top-10-health-technology-hazards-2022-executive-brief.
https://www.healthcaredive.com/news/hospital-cyberattack-prevention-commonspirit-hack-breach/635407/.
https://dlaszpitali.pl/polecamy/cyberbezpieczenstwo-placowek-medycznych/.
https://cert.pl/raporty-roczne/.
https://pl.wikipedia.org/wiki/Phishing.
https://pl.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency.
https://pl.wikipedia.org/wiki/Ransomware.
https://www.nfz.gov.pl/aktualnosci/aktualnosci-centrali/wsparcie-cyberbezpieczenstwa-w-placowkach-medycznych,8211.html.

Katarzyna Fortak-Karasińska, Marzena Garstka

F/K LEGAL

Cyberbezpieczeństwo placówek medycznych – aspekty prawne

Informacje o cyberatakach hackerskich w polskich placówkach medycznych pojawiają się coraz częściej. Niezależnie od tego czy cyberatak dotknie placówkę prywatną, czy publiczną, działającą na rynku komercyjnym, czy w oparciu o współpracę z NFZ, skutki cyberataku mogą być bardzo poważne, tak w zakresie odpowiedzialności wobec pacjenta, jak i w sferze odpowiedzialności finansowej właścicieli i osób zarządzajacych.

W ramach rozwoju cyfryzacji w Polsce na przestrzeni lat zostało wdrożonych wiele projektów teleinformatycznych, usprawniających system polskiej ochrony zdrowia oraz ułatwiających pacjentom dostęp do świadczeń zdrowotnych. Postęp technologiczny oraz brak odpowiednich zabezpieczeń sieci teleinformatycznych sprawia jednak, iż placówki medyczne, w szczególności szpitale, stają się łatwym celem dla hackerów. Należy mieć przy tym świadomość, iż dane medyczne stanowią ogromną wartość na nielegalnym rynku. Dzieje się tak niezależnie od rodzaju placówki medycznej oraz obowiązujących ją przepisów.

Dlatego też jest niezwykle istotne, aby placówka medyczna podjęła jak najdalej idące działania zabezpieczające ją przed włamaniem, a jeżeli nawet uznać, iż nie zawsze możliwe jest uniknięcie cyberataku – była przygotowana prawnie na zminimalizowanie negatywnych skutków jego wystąpienia.

CYBERBEZPIECZEŃSTWO – JAK WIDZI TO USTAWODAWCA?

Do polskiego porządku prawnego wprowadzono szereg aktów prawnych, dotyczących zagadnień szeroko rozumianego cyberbezpieczeństwa, z których najważniejszym jest *ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej zwana ustawą o KSC)*, a także *rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*. Wspomniane akty prawne zawierają szereg regulacji, których celem jest ochrona podmiotów przed cyberatakami oraz zabezpieczenie przetwarzanych danych.

Przepisy ustawy o KSC dotyczą szeregu podmiotów, wśród których znajdziemy m.in. placówki medyczne, w stosunku do których minister zdrowia wydał decyzję o uznaniu ich za operatora usługi kluczowej. Do usług kluczowych zaliczamy m.in. udzielanie świadczeń opieki zdrowotnej przez podmiot leczniczy, czy gromadzenie i udostępnianie Elektronicznej Dokumentacji Medycznej.

DYREKTORZE/WŁAŚCICIELU SZPITALA – CO TO DLA CIEBIE OZNACZA?

Każdy właściciel szpitala czy też jego dyrektor zobowiązany jest do przestrzegania obowiązków, wynikających z zasad cyberbezpieczeństwa. Wdrożenie i realizacja tych zasad pozwoli na zminimalizowanie, a może nawet uniknięcie odpowiedzialności z tytułu naruszenia przepisów prawa, obowiązujących w tym zakresie.

Jakie zatem działania winien podjąć dyrektor szpitala?

1. Wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym, na co składa się m.in:

- prowadzenie systematycznej oceny ryzyka wystąpienia ataku hackerskiego czy wycieku danych, w tym również możliwości wystąpienia sytuacji szczególnego zagrożenia,

- wdrożenie środków technicznych i organizacyjnych, które pozwolą na bezpieczne utrzymanie systemu teleinformatycznego, który wykorzystuje szpital, takich jak kontrola dostępu czy działanie w sposób, który zapewni poufność, integralność, dostępność i autentyczność informacji,
- bieżące aktualizowanie oprogramowania,
- zapewnienie ochrony przed dokonaniem modyfikacji w systemie przez osobę nieuprawnioną,
- natychmiastowe reagowanie w przypadku dostrzeżenia zagrożenia cyberbezpieczeństwa lub podatności systemu na takie zagrożenie,
- zapewnienie środków łączności i komunikacji w ramach krajowego systemu cyberbezpieczeństwa;

2. Wyznaczenie w szpitalu osoby, odpowiedzialnej za utrzymanie kontaktu w ramach krajowego systemu cyberbezpieczeństwa.

   Taka osoba pełni funkcję łącznika między placówką a podmiotami należącymi do krajowego systemu cyberbezpieczeństwa (np. z właściwym zespołem CSIRT w zakresie obsługi incydentu) i jest odpowiedzialna za bieżące kontakty z tymi instytucjami. Przepisy nie precyzują, jakie kompetencje powinna mieć taka osoba, ale z praktycznego punktu widzenia ważne jest, aby posiadała wiedzę dotyczącą zasad działania szpitala oraz systemów informacyjnych, które wykorzystuje dana placówka. Najczęściej są to pracownicy działów IT lub pionów bezpieczeństwa. Wyznaczając taką osobę, trzeba również pamiętać o tym, aby kontakt z nią nie był utrudniony. Ważne jest bowiem, aby komunikacja ze wspomnianymi podmiotami była bieżąca, szczególnie że szpitale funkcjonują w trybie 24/7.

3. Opracowanie, aktualizowanie oraz stałe zapewnianie bezpieczeństwa dokumentacji, która dotyczy cyberbezpieczeństwa (np. dotyczącej systemu zarządzania bezpieczeństwem informacji, dokumentacji technicznej systemu informacyjnego, z którego korzysta placówka czy dokumentacji wynikającej ze specyfiki usług, które świadczy).

4. Opracowanie oraz wdrożenie odpowiednich regulacji, które umożliwią zapewnienie cyberbezpieczeństwa. Tutaj możemy wskazać przede wszystkim na:

- wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Na tę dokumentację składa się szereg rozbudowanych regulacji, które należy dostosować do potrzeb konkretnej placówki. W jej skład powinny wejść, np. regulamin korzystania ze sprzętu i systemów informatycznych, zarządzania uprawnieniami do pracy w tych systemach czy chociażby procedura bezpiecznej utylizacji sprzętu,
- wprowadzenie odpowiednich regulacji zawartych w regulaminach pracowniczych, regulaminach korzystania z danego sprzętu medycznego, ogólnym regulaminie organizacyjnym oraz regulaminie każdego z oddziałów,
- utworzenie regulaminów dla osób przebywających w szpitalu (np. regulaminu korzystania z bezpłatnej sieci szpitala, regulaminu odwiedzin oraz polityki bezpieczeństwa w relacjach z dostawcami i usługodawcami),
- uwzględnianie we wszelkiego rodzaju umowach zawieranymi zarówno z osobami zatrudnionymi w placówce, jak i w umowach, które szpital podpisuje w toku swojej bieżącej działalności (np. z usługodawcami, serwisantami czy umowach zakupu sprzętu medycznego, komputerowego, zaopatrzenia itd.) postanowień, które zabezpieczą placówkę oraz udostępniane przez nią dane. Szczególnie ważne są zapisy dotyczące o ochronie powierzonych danych czy o poufności.

5. Powołanie wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo . Możliwe jest też zawarcie umowy z podmiotem, który świadczy usługi z zakresu cyberbezpieczeństwa.

   Głównym zadaniem struktury lub ww. podmiotów jest spełnianie warunków technicznych i organizacyjnych, które pozwolą na zapewnienie szpitalowi cyberbezpieczeństwa. Dodatkowo powinny one dysponować pomieszczaniami, które będą przeznaczone do świadczenia usług związanych z reagowaniem na incydenty. Pomieszczenia te muszą być należycie zabezpieczone przed różnego rodzaju zagrożeniami. Zadaniem takiej struktury lub podmiotu jest również stosowanie zabezpieczeń, które zagwarantują bezpieczeństwo informacjom przetwarzanym przez szpital.

   Zrealizowanie tego obowiązku jest obwarowane terminem, a mianowicie powołanie struktury lub podpisanie umowy z podmiotem zewnętrznym winno nastąpić w terminie **trzech miesięcy od daty doręczenia szpitalowi decyzji o uznaniu za operatora usługi kluczowej.** Dodatkowo, jeśli szpital zdecyduje się zawrzeć umowę z podmiotem zewnętrznym, zobowiązany jest **w terminie 14 dni** poinformować Ministra Zdrowia i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV oraz sektorowy zespół cyberbezpieczeństwa (jeśli został powołany) o podmiocie, z którym została zawarta umowa. W takim samym terminie należy informować o wszelkich zmianach i o rozwiązaniu takiej umowy.

6. Regularne przeprowadzanie **audytu bezpieczeństwa systemu informacyjnego**. Taki audyt powinien być przeprowadzany **przynajmniej raz na 2 lata.**

A NA CO DZIEŃ...?

Aby placówka medyczna nie stała się łatwym celem hackera, niezbędne jest wdrożenie do codziennego funkcjonowania placówki odpowiednich zasad bezpieczeństwa W praktyce na cyberbezpieczeństwo składa się bowiem szereg czynności, nie tylko prawnych, ale również faktycznych związanych z dostosowaniem sprzętu komputerowego, systemowego czy szkoleniem pracowników służby zdrowia.

W swojej codziennej działalności szpitale powinny pamiętać o:

- aktualizowaniu swoich regulacji wewnętrznych w ślad za zmieniającym się otoczeniem,
- inwentaryzowaniu sprzętu, jego odpowiednim skonfigurowaniu oraz zapewnieniu aktualności oprogramowania,
- zapewnieniu pracownikom uprawnień odpowiednich do ich stanowiska i zakresu obowiązków, a także do ich aktualizowania (np. w przypadku zmiany stanowiska),
- monitorowaniu dostępu do systemu, wykrywaniu działań nieautoryzowanych oraz zapewnieniu środków do zapobieżenia dostępu przez podmioty nieuprawnione,
- zabezpieczeniu informacji w sposób, który uniemożliwi osobom nieuprawnionym jej ujawienie, modyfikację, usunięcie lub zniszczenie,
- wdrożeniu szkoleń dla pracowników dotyczących w szczególności rodzajów zagrożeń bezpieczeństwa informacji, stosowaniu środków zapewniających bezpieczeństwo informacji,
- zawieraniu w umowach zapisów, które zagwarantują odpowiedni poziom bezpieczeństwa informacji.

Najczęstszym źródłem ataków hackerskich jest zwykły błąd lub niewiedza ludzka. Pracownicy szpitala mający dostęp do systemów informacyjnych powinni zostać uczuleni na czynności, na które powinni szczególnie zwracać uwagę przy wykonywaniu swoich bieżących obowiązków. Istotna jest również rola działu IT, który powinien zadbać o odpowiednie zabezpieczenie nie tylko informacji i danych, ale także wykorzystywanego w placówce oprogramowania i sprzętu.

Tutaj szczególną uwagę należy zwrócić na:

1. **tworzenie kopii zapasowych** – kopie zapasowe powinny być wykonywane na bieżąco, tak aby zapewnić ciągłość działania i umożliwić odtworzenie informacji. Zaleca się przechowywanie 3 kopii danych, w tym dwóch z nich na różnych nośnikach danych i co najmniej jednej odizolowanej w celu uniknięcia jej zaszyfrowania w przypadku ataku hackerskiego.
2. **zabezpieczenie poczty elektronicznej** – dostęp zarówno do poczty, jak również do używanych w szpitalu systemów powinien być uwierzytelniony, autoryzowany oraz zaszyfrowany. Warto jest wprowadzić dwuetapową weryfikację tożsamości. Pracownicy powinni pamiętać o tym, aby nie otwierali maili o podejrzanej treści oraz nie pobierali niezidentyfikowanych załączników. Dodatkowo w przypadku przesyłania e-maili zawierających dane wrażliwe konieczne jest stosowanie szyfrowania w celu uniemożliwienia przechwycenia zawartych tam danych.
3. **zabezpieczenie sprzętu** – istotnymi elementami ochrony są tutaj:

- wdrożenie ochrony brzegu sieci – zainwestowanie w urządzenia typu firewall, zapewnienie ich aktualizacji oraz odpowiedniej konfiguracji,
- wdrożenie ochrony stacji roboczych – zastosowanie narzędzi takich jak EDR, który skutecznie izoluje poszczególne urządzenia od całej infrastruktury systemu oraz dokonuje detekcji ukrytych zagrożeń, instalacja programów antywirusowych, programów informujących administratora na bieżąco o zaistnieniu incydentu oraz reagujących w czasie rzeczywistym,
- bieżąca aktualizacja oprogramowania i konfiguracji użytkowanych systemów,
- zabezpieczenie sieci wewnętrznej oraz zewnętrznej w postaci VPNu oraz oddzielenie tych sieci od siebie (segmentacja sieci),
- bieżące monitorowanie zdarzeń w sieci,
- wprowadzenie kontroli dostępu oraz uwierzytelniania wieloskładnikowego,
- w przypadku ataku – zapewnienie możliwości odseparowania poszczególnych urządzeń od sieci,
- regularne audyty bezpieczeństwa.

W swojej codziennej działalności szpitale powinny także czynnie współpracować z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT NASK). Jest to zespół ekspertów ds. bezpieczeństwa informatycznego. Jego głównym zadaniem jest reagowanie na incydenty dotyczące bezpieczeństwa komputerowego, a także przeciwdziałanie wystąpieniu kolejnych zdarzeń. Celem takiej współpracy jest budowanie jednolitego systemu ochrony danych medycznych.

STAŁO SIĘ...

JAK DZIAŁAĆ W PRZYPADKU CYBERATAKU?

Środki bezpieczeństwa zostały wdrożone, ale jednak hackerowi udało się dostać do szpitalnego systemu... Trzeba działać!

- **Do kogo zgłosić incydent?** Zgłoszenie należy przesłać do CERT Polska. Jest to jeden z trzech Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego na poziomie krajowym (w skrócie CSIRT od ang. *Computer Security Incident Response Team).*
- **Jak to zrobić?** Zgłoszenia najlepiej dokonać elektronicznie na stronie internetowej CSIRT NASK https://incydent.cert.pl/. Możesz także wypełnić odpowiedni formularz (znajdziesz go na stronie Biuletynu Informacji Publicznej NASK) i przesłać go za pośrednictwem poczty elektronicznej na adres cert@cert.pl
- **Ile masz czasu? Jak najszybciej, jednak nie później niż w ciągu 24 godzin od momentu wykrycia incydentu.** Czas reakcji na zgłoszenie jest bardzo ważny z punktu widzenia rozwiązania zaistniałego problemu.
- **Co, jeśli nie masz wszystkich informacji, których podania wymaga formularz?** Nie martw się! Przekaż informacje, które posiadasz. Jeśli będzie taka konieczność, zespół analizujący zgłoszenie dopyta Cię o dodatkowe kwestie.
- **Co jeszcze powinieneś zrobić?** Szpital ma obowiązek powiadomienia Policji o dokonanym ataku hackerskim. Jeśli doszło do wycieku danych osobowych konieczne jest także powiadomienie Urzędu Ochrony Danych Osobowych. Dobrze, aby szpital powiadomił o ataku prawnika, który będzie stanowił łącznik pomiędzy placówką a Policją czy też Urzędem Ochrony Danych Osobowych i ułatwi przejście przez wszelkie procedury.
- **Czy jest coś, o czym dodatkowo musisz pamiętać?** Przede wszystkim postaraj się nie wpadać w panikę. Pozwól specjalistom z zakresu cyberbezpieczeństwa i informatykom, z którymi współpracujesz wdrożyć odpowiednie działania i środki techniczne, które zminimalizują skutki

Warto również śledzić wszelkiego rodzaju działania podejmowane przez państwo, które mają na celu poniesienie poziomu cyberbezpieczeństwa w placówkach medycznych. Dla przykładu, w 2022 roku Narodowy Fundusz Zdrowia uruchomił program dofinansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w szpitalach oraz innych jednostkach medycznych. Program ten umożliwia refundację m.in. zakupionych urządzeń, oprogramowania oraz usług teleinformatycznych, mających na celu zapobieganie, wykrywanie i zwalczanie cyberataków, takich jak np. systemy do tworzenia kopii zapasowych danych, programów antywirusowych, urządzeń umożliwiających wprowadzenie cyberbezpieczeństwa oraz monitorowanie i identyfikowanie zagrożeń, czy organizowanie szkoleń z cyberbezpieczeństwa dla pracowników szpitali. W ramach programu placówki medyczne mogą uzyskać nawet do 900 tys. zł.

KONSEKWENCJE NIEZASTOSOWANIA SIĘ DO OBOWIĄZKÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM

Placówka medyczna musi pamiętać, że możliwe skutki cyberataku to nie jedyne konsekwencje, jakie mogą ją spotkać, jeśli nie zastosuje się do obowiązków i nie wdroży działań, na które wskazują aktualnie obowiązujące przepisy. Samo niewypełnienie obowiązków prawnych, nawet przy braku wystąpienia cyberataku rodzi odpowiedzialność w postaci chociażby kar finansowych.

Za naruszenie przepisów z zakresu cyberbezpieczeństwa szpital może być ukarany karą finansową, która **przy najcięższych przewinieniach może wynieść nawet do 200 tys. zł. W przypadku uporczywych naruszeń**, na szpital może zostać nałożona **kara nawet 1 mln zł.** W niektórych sytuacjach odpowiedzialność finansową mogą ponieść również członkowie kadry zarządzającej. Tutaj wymierzona kara nie może być wyższa niż 200% miesięcznego wynagrodzenia.

MOŻLIWE SKUTKI PRAWNE CYBERATAKU

Oprócz konsekwencji finansowych z tytułu niewypełnienia obowiązków z zakresu cyberbezpieczeństwa, skutki cyberataku są daleko idące. Ataki hackerskie blokują działalność szpitali, a to stanowi **naruszenie przepisów prawa w zakresie zgodności działania szpitala z przepisami o działalności leczniczej, przepisami mającymi na celu ochronę praw pacjenta czy przepisami określającymi współpracę z NFZ.** Naruszenia

w tym zakresie mogą być podstawą wielu roszczeń skierowanych przez pacjenta do placówki. Cyberatak stwarza utrudnienia w następujących obszarach:

- **rejestracja pacjentów** – obowiązkiem placówki medycznej (zwłaszcza działającej w oparciu o współpracę z NFZ) jest rejestracja pacjentów w stanie ciągłym. Nie ma podstaw, które uzasadnią choćby czasową odmowę ich rejestracji na podstawie zgłoszenia osobistego, telefonicznego, za pośrednictwem osoby trzeciej lub też drogą elektroniczną. Wyjątkiem może być jedynie okoliczność przerwy w udzielaniu świadczeń opieki zdrowotnej.
- **obsługa pacjentów** – w przypadku cyberataku wszystkie czynności od przyjęcia pacjenta do placówki medycznej, które są wykonywane zdalnie musiałyby odbywać się w formie tradycyjnej, papierowej.
- **prowadzenie i wykorzystanie elektronicznej dokumentacji medycznej,** która jest niezbędna do udzielania świadczeń ratujących zdrowie i życie pacjentów. Skoro nie jest możliwe wykorzystanie elektronicznej dokumentacji medycznej to wszystkie dokumenty, w tym recepty, czy skierowania są wypisywane w formie papierowej, co niewątpliwie powoduje dalsze utrudnienia w obsłudze pacjenta.
- **ujawnienie danych pacjentów** znajdujących się w elektronicznej dokumentacji medycznej, w tym informacji o stanie ich zdrowia.
- **realizowanie zaplanowanych do wykonania badań i innych świadczeń zdrowotnych** – większość urządzeń do wykonywania badań jest całkowicie skomputeryzowana i nie działa bez podłączenia do sieci. To z kolei powoduje brak możliwości wykonywania badań pacjentom w ustalonym terminie.
- **działanie systemów administracyjnych** – w wyniku cyberataku może dojść do zablokowania m.in. systemu księgowego placówki medyczne. Z tym z kolei wiąże się wstrzymanie dostaw wyrobów medycznych oraz leków, a także wstrzymanie płatności, do których zobowiązana jest placówka medyczna.

Brak sprawnego działania szpitala w ww. obszarach może skutkować:

- indywidualnymi roszczeniami pacjenta z tytułu naruszenia jego praw;
- roszczeniami pacjentów do sądu cywilnego z tytułu poniesionej szkody na skutek nieudzielenia świadczenia zdrowotnego w terminie;
- skargami indywidualnymi pacjenta do rzecznika praw pacjenta;
- uznaniem przez Rzecznika Praw Pacjenta, iż doszło do naruszenia zbiorowych praw pacjentów (kary pieniężne do 50 000zł);
- karami finansowymi nałożonymi przez NFZ z tytułu nieprawidłowej realizacji umowy o udzielanie świadczeń zdrowotnych;
- odpowiedzialnością karną, zawodową oraz cywilną właścicieli szpitala jak personelu medycznego;

SANKCJE ZA NARUSZENIE RODO

Cyberatak może narazić szpital także na poważne konsekwencje wynikające z naruszenia przepisów RODO. Naruszenie RODO może polegać na wycieku danych, naruszeniu praw pacjenta związanych z ochroną jego danych np. nieprawidłowym przetwarzaniu jego danych osobowych, czy braku lub niestosowaniu się do dokumentacji dotyczącej ochrony osobowych w ramach instytucji.

Placówka medyczna w ramach swojej działalności bez wątpienia przetwarza dane osobowe, a zatem musi przestrzegać odpowiednich zasad i wymogów ich dotyczących, w tym poprzez zapewnienie odpowiedniego bezpieczeństwa przetwarzanych danych.

W przypadku, gdy dojdzie do incydentu bezpieczeństwa np. wycieku danych, dyrektor szpitala winien przede wszystkim:

- ocenić, czy doszło do naruszenia danych osobowych, a jeśli takie naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych – zgłosić w odpowiednim terminie takie naruszenie do organu nadzorczego, którym jest prezes Urzędu Ochrony Danych Osobowych,
- niekiedy dodatkowo poinformować osoby fizyczne, na które to naruszenie wywiera wpływ,
- zarejestrować każde naruszenie ochrony danych w **wewnętrznej dokumentacji szpitala.**

W przypadku wystąpienia nieprawidłowości prezes Urzędu Ochrony Danych Osobowych może wszcząć postępowanie wyjaśniające w celu ustalenia, czy doszło do naruszenia przepisów o ochronie danych osobowych, a jeśli uzna, że tak – za takie naruszenie może zostać nałożona administracyjna kara pieniężna. Postępowanie może zostać również wszczęte z własnej inicjatywy Urzędu lub na wniosek osoby, która złożyła skargę, jeśli naruszenie jej bezpośrednio dotyczyło.

Maksymalna wysokość kary, która grozi szpitalowi, to 20.000.000,00 EUR (w przypadku przedsiębiorstwa – maksymalnie 4% jego całkowitego rocznego światowe-

go obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa). Wysokość kary zależy od wielu czynników, tj. stopnia i wagi naruszenia przepisów, kategorii i rodzaju danych osobowych, których dotyczyło naruszenie, czy kształtu współpracy z organem nadzorczym w trakcie trwania postępowania wyjaśniającego.

Co ważne, kara pieniężna za zaistniałe naruszenie ochrony danych może zostać nałożona nawet wtedy, gdy nieprawidłowości zostaną usunięte przed zakończeniem postępowania przed Urzędem.

Jeśli z okoliczności danej sprawy wyniknie, że nałożenie kary nie jest konieczne, organ nadzorczy może poprzestać na środkach niepieniężnych, zmierzających do usunięcia naruszenia i przywrócenia stanu zgodnego z prawem.

Dodatkowo RODO przewiduje również roszczenia z tytułu odpowiedzialności cywilnej. Osoba poszkodowana w wyniku naruszenia przepisów RODO ma prawo uzyskać odszkodowanie za poniesioną stratę. Przepisy nie precyzują maksymalnych kwot takiego odszkodowania. Jego wysokość będzie zależała od oceny danego stanu faktycznego, a stopień m.in. współpracy z organem nadzorczym oraz działania naprawcze, podejmowane przez podmiot, u którego wystąpiło naruszenie, z pewnością mogą mieć znaczący wpływ na ocenę sprawy.

PODSUMOWANIE

W obecnych czasach szpitale nie są wolne od obowiązku budowania świadomości na temat zagrożeń nadchodzących ze strony cyberświata. W związku z tym na każdym ze szpitali spoczywa powinność wdrożenia szeregu działań – prawnych, proceduralnych, systemowych oraz innych, które zminimalizują skutki potencjalnego cyberataku.

Tylko kompleksowe wprowadzenie rozwiązań zwiększających i gwarantujących bezpieczeństwo, może przynieść oczekiwany skutek. Wybiórcze zastosowanie takich środków może doprowadzi

do powstania luk, których znalezienie zajmie hakerowi bardzo mało czasu, a które będą prostym środkiem do przedostania się do danych szpitala.

Wypełnienie obowiązków prawnych w obszarze cyberbezpieczeństwa zabezpiecza nie tylko samą placówkę medyczną, jej właścicieli czy personel medyczny, ale chroni pacjenta i jego dane. Konsekwencje naruszeń w tym zakresie mogą być i poważne, i drogie.

PAMIĘTAJ! CYBERBEZPIECZEŃSTWO SZPITALA TO BEZPIECZEŃSTWO PACJENTA!

Katarzyna Fortak-Karasińska

radca prawny, partner F/K LEGAL, ekspert w zakresie ochrony zdrowia; posiada ponad 15-letnie doświadczenie w doradztwie prawnym i biznesowym na rzecz podmiotów prowadzących działalność medyczną. Wspiera inwestorów, grupy medyczne oraz placówki medyczne w opracowaniu strategii rozwoju działalności. Prowadzi obsługę prawną współpracy z NFZ. Uczestniczy wdrażaniu badań klinicznych w szpitalach i przychodniach. Jest wykładowcą i prelegentem podczas ogólnopolskich seminariów i konferencji dotyczących ochrony zdrowia.

Marzena Garstka

radca prawny, senior lawyer w F/K LEGAL. Specjalizuje się w prawie autorskim oraz szeroko rozumianym prawie nowoczesnych technologii, w tym prawie IT, prawie Internetu, a także prawie reklamy i konkurencji. Od 2007 roku związana z branżą IT, a w latach 2009-2021 zatrudniona jako radca prawny w polskich spółkach Grupy Uniqa, gdzie obok prawa ubezpieczeniowego zajmowała się głównie obsługą wdrożeń informatycznych, w tym złożonych projektów dla całej grupy kapitałowej, z udziałem największych światowych dostawców.
Członek Stowarzyszenia Praktyków Ochrony Danych.

Jakub Syta

Po co szpitalom to całe „cyberbezpieczeństwo”?

Zapewnianie bezpieczeństwa informacjom, przetwarzanym w systemach teleinformatycznych, jest złożonym zagadnieniem. Wymaga między innymi spojrzenia na procesy, zachodzące w organizacjach, zachowania pracowników, a także – z perspektywy cyberprzestępcy – na wykorzystywane technologie. To z kolei wymaga nie tylko znajomości technik i procedur stosowanych przez hakerów, ale również umiejscowienia ich w kontekście organizacji takiej, jak szpital. W niniejszym artykule postaram się pokazać szereg scenariuszy, charakterystycznych dla sektora ochrony zdrowia, których przede wszystkim należy się obawiać i którym należy skutecznie przeciwdziałać.

Konsekwencje zaniechań w tym obszarze mogą bowiem być bardzo bolesne i obejmować straty:

- finansowe, związane zarówno z bezpośrednimi stratami powstałymi w trakcie cyberataku, takimi jak kradzież środków finansowych czy koszty związane z przerwaniem procesów;
- wizerunkowe – np. negatywnie publikacje czy ataki na portalach społecznościowych;
- regulacyjne, które mogą mieć postać kar finansowych, ograniczenia dostępu do publicznych funduszy, działalności nakazowej, a nawet postępowania skierowanego personalnie przeciwko osobom odpowiedzialnym za zaniechania. Wszystkie z tych akcji mogą mieć znaczny wpływ na reputację ukaranej organizacji.

A biorąc pod uwagę specyfikę takich organizacji jakimi są szpitale – skutki udanych cyberataków mogą dotykać również ich pacjentów.

Najbardziej istotne scenariusze cyberzagrożeń

Cyberataki dotyczą poszczególnych własności bezpieczeństwa informacji i to ich znajomość jest kluczowa dla dalszych rozważań. Nie chodzi bowiem wyłącznie o przechwycenie informacji, czyli atak na ich **poufność**. Często znacznie groźniejsza może być modyfikacja informacji, czyli atak na ich **integralność** lub przerwanie procesu wymiany informacji, czyli atak na ich **dostępność**. Wreszcie nie należy zapominać o podrobieniu informacji, czyli atakach na ich **autentyczność**, co bardzo często wykorzystywane jest jako tzw. wektor wejścia, czyli sposób w taki ataki się rozpoczynają.

Kluczowym scenariuszem, który przede wszystkim powinien być uwzględniany podczas analiz, jest doprowadzenie przez cyberprzestępców do **niedostępności systemów**. Nie chodzi tu o dostępność strony www czy nawet systemu rejestracji pacjentów, ale baz danych zawierających szczegółowe informacje o stanie zdrowia i przebiegu leczenia, a także konfiguracji urządzeń medycznych. Tomografy, rezonanse magnetyczne, systemy monitorujące stan pacjentów... – wszystkie te systemy są podłączane do sieci i tym samym są podatne na te same zagrożenia, co każdy komputer. Można wykraść z nich dane, można modyfikować parametry czy też można uniemożliwić ich pracę. Z tego faktu korzystają grupy przestępców specjalizujące się w atakach typu ransomware. Szyfrują infrastrukturę szpitali i większości z nich nie przeszkadza to, że w wyniku ich działań mogą umierać pacjenci. Przeciwnie, wykorzystywane jest jako argument mający przekonać ofiary ataku (szpitale) do jak najszybszej zapłaty okupu.

Opisany powyżej atak może dotyczyć pojedynczego szpitala, całej grupy lub wręcz całego sektora. Tak to wyglądało w maju 2021 roku, gdy cyberatak sparaliżował pracę szpitali w Irlandii. Najbardziej oczywisty sposób szybkiej reakcji w przypadku ransomware, którym byłaby ewakuacja pacjentów do innego szpitala, jak widać może okazać się niemożliwy.

Kolejny scenariusz dotyczy **ujawniania wrażliwych danych** pacjentów – szczególnie danych dotyczących osób o statusie VIP: polityków, celebrytów, przedsiębiorców. Informacje o problemach psychiatrycznych, odbytych terapiach uzależnieniowych, bezpłodności, aborcji... byłyby na wiele tygodni pożywką dla internetowych trolli i mniej etycznych dziennikarzy. Miały już na świecie miejsce kampanie nakierowane na kradzież danych z klinik chirurgii plastycznych po to, by wykorzystując materiały sprzed, w trakcie i po zabiegu, szantażować swoje ofiary. Warto też dodać, że kradzież danych może być niezależnym atakiem, ale często jest również elementem ataku typu ransomware.

Masowy wyciek danych przede wszystkim może się jednak wiązać z próbą kradzieży tożsamości pacjentów. Posiadając dostęp do imienia i nazwiska, imion i nazwisk rodziców, danych teleadresowych i numerów dokumentów tożsamości, przestępcy mogą starać się podszywać pod swoje ofiary by gromadzić na ich temat więcej, tym razem bardziej wrażliwych informacji. Atak może być jednak również znacznie prostszy – na przejęte adresy e-mail czy smsy można wysyłać wiadomości phishingowe podszywające się pod szpital, by wykorzystać je do masowej kradzieży danych uwierzytelniających – na przykład do poczty elektronicznej lub konta bankowości online.

Cyberatak skierowany na szpital mógłby również mieć charakter terrorystyczny, gdyby jego celem była **modyfikacja parametrów funkcjonowania urządzeń**. A ponieważ większość nowoczesnych urządzeń jest podłączona do sieci wewnętrznej i za jej pośrednictwem do sieci Internet, takie ataki są jak najbardziej możliwe. Znane są przypadki zdalnego modyfikowania przez hakerów pracy pomp insulinowych. Znamy przypadki błędnego ustawienia aparatów Rtg prowadzące do poparzeń, które co prawda nie były rezultatem cyberataku, ale wydaje się to wyłącznie kwestią czasu. Można również zdalnie manipulować rozrusznikami serca... każda nowa technologia niesie na sobą szereg zagrożeń, których trzeba być świadomym, by móc w razie potrzeby zareagować w sytuacji.

Warto dodać, że poziom bezpieczeństwa jest bardzo obniżony przez trudności związane z aktualizacją oprogramowania na urządzeniach, co czasami wręcz wiąże się z ponownymi procedurami dopuszczającymi do używania. Znane luki w oprogramowaniu należą do głównych wektorów ataku.

Atak mogłoby również dotyczyć **nieautoryzowanej modyfikacji przetwarzanych danych.** Nieautoryzowana zmiana grupy krwi, informacji o alergiach, przebytych lub planowanych zabiegach – to wszystko staje się możliwe. Nie należy spodziewać się masowości tego typu ataków, gdyż najprawdopodobniej bardzo szybko zostałoby one wykryte i – wykorzystując kopie zapasowe – można by było przywrócić integralność danych. Jednak tego typu cyberataki, wycelowane w konkretne osoby, mogą mieć w przyszłości miejsce. Stąd tak istotna powinna być troska o zapewnienie nadzorowania integralności tych danych.

Kolejne dwa zagrożenia, biorąc pod uwagę dotychczas nakreślone scenariusze, mogą wydawać się mało istotne. Pamiętać jednak należy, że ryzyko związane jest zarówno ze skutkami ataków, jak i ich prawdopodobieństwem. A w obu przypadkach prawdopodobieństwo będzie bardzo wysokie.

Pierwszy związany jest z **haktywizmem**, czyli wykorzystywaniem technik i narzędzi hakerskich do promowania/demonstrowania swoich poglądów przez cyberprzestępców. Tego typu ataki najczęściej mają formę niegroźnych zmian treści na stronach www, jednak po latach względnej ciszy, wraz z początkiem wojny na Ukrainie, można zaobserwować zwiększenie ilości tego typu prób.

Drugi scenariusz dotyczy atakowania pacjentów. Pamiętać należy, że cyberprzestępcy również bywają pacjentami. W trakcie leczenia, bądź rehabilitacji, mogą starać się wykorzystywać szpitalne sieci WiFi do atakowania towarzyszy. A w przypadku, gdy sieć WiFi będzie źle odseparowana od sieci szpitalnej, można będzie spodziewać się wszystkich opisywanych wcześniej ataków z wewnątrz, czyli z ominięciem systemów ochrony brzegowej.

Na koniec chciałbym zwrócić uwagę na jeszcze jedną kwestię. To, że szpitale ucierpią w wyniku cyberataku, niekoniecznie musi oznaczać, że to one padną jego ofiarą. Silne łańcuchy zależności z dostawcami i partnerami, niezbędne w obecnych czasach, również mogą być źródłem ryzyka. Udany **cyberatak na partnera biznesowego** może doprowadzić do wstrzymanych dostaw, przerwanych usług czy też wycieku powierzonych danych. A konsekwencje tego może ponosić przede wszystkim partner.

Powyższa lista w żadnych wypadku nie wyczerpuje wszystkich scenariuszy cyberzagrożeń, które dotknąć mogą organizacje. Są to jednak zagrożenia w znacznej mierze specyficzne dla sektora ochrony zdrowia i jako takie powinny być szczególnie nadzorowane przez władze szpitali.

Budowanie organizacji odpornych na cyberzagrożenia

W tej sytuacji pojawia się pytanie: co robić, w jaki sposób powinny zachowywać się placówki ochrony zdrowia, by nie narazić się na zarzuty nienależytego nadzoru. Warto bowiem przypomnieć, że oprócz członków zarządów, odpowiedzialność za zapewnianie cyberbezpieczeństwa, po ubiegłorocznej nowelizacji kodeksu handlowego, mają również rady nadzorcze.

Wbrew pozorom najlepszym z rozwiązań wcale nie jest zakup kolejnych urządzeń firewall czy licencji dla „systemów opartych na rozwiązaniach co najmniej klasy Endpoint Detection and Response w architekturze serwera". To, co w zakresie cyberbezpieczeństwa jest kluczowe, to kadry. To zapewnienie, że architektura IT będzie możliwie odporna na zagrożenia a sprzęt i oprogramowanie będzie dobierane pod kątem skuteczności oraz skonfigurowane tak, by efektywnie realizowało swoje cele. Nowe architektury bezpieczeństwa wręcz tworzone są z założeniem, że przestępcom uda się zdobyć przyczółek w chronionej sieci – to tzw. model „zero trust".

Istnieje jednak kilka opcji jak można zapewnić wsparcie doświadczonych pracowników. Przede wszystkim szpitale mogą budować **własne zespoły, specjalizujące się w zapewnianiu cyberbezpieczeństwa**. Warto je rozróżnić od zespołów IT, gdyż kompetencje IT oraz „bezpieczników" znacząco się różnią. Zresztą nawet w zakresie samego zapewniania cyberbezpieczeństwa model NICE, opracowany przez amerykański NIST, wylicza pół setki specjalizacji. Zbudowanie zespołu zdecydowanie pozwoli na prowadzenie samodzielnej polityki w tym zakresie – najlepiej zgodnie z **międzynarodową normą ISO 27799**, która przedstawia wytyczne w zakresie budowania systemów zarządzania bezpieczeństwem informacji w placówkach ochrony zdrowia. Biorąc pod uwagę koszty zatrudniania ekspertów w zakresie cyberbezpieczeństwa oraz ich bardzo małą dostępność, niekoniecznie jest to optymalne rozwiązane. Szczególnie, że jakby nie patrzeć, cyberbezpieczeństwo niekoniecznie jest kluczową specjalizacją szpitali i raczej powinny one doskonalić się w aspektach ratowania życia i zdrowia.

Można więc zminimalizować czynności operacyjne w tym zakresie, pozostawiając po stronie szpitala np. jedynie rolę koordynatora i zacząć korzystać z usług wyspecjalizowanych podmiotów. Tutaj można wyróżnić trzy opcje:

1. skorzystanie z **usług wyspecjalizowanego podmiotu** w zakresie cyberbezpieczeństwa. Musi to być podmiot godny zaufania oraz pokrywający kompetencyjnie co najmniej kilka ze specjalizacji w zakresie cyberbezpieczeństwa.
2. przeniesienie części systemów do wyspecjalizowanego podmiotu, oferującego **usługi w chmurze obliczeniowej.** W takim wypadku znów kluczowe będzie ustalenie, czy podmiot daje rękojmię należytej ochrony przetwarzanych danych oraz niezbędnej dostępności usług. Pamiętać też należy, że w takiej sytuacji tylko część danych (tych najcenniejszych) byłaby właściwie chroniona. Niemniej po stronie szpitala sieci i systemy wciąż wymagany byłby poprawny nadzór.
3. stworzenie wraz z innymi szpitalami własnego, **wyspecjalizowanego centrum usług wspólnych.** Taka spółka, kontrolowana przez kilka podmiotów, zapewniałaby należytą jakość usług, a koszty związane z jej początkową działalnością rozkładałyby się na kilka podmiotów. Możliwe, że z czasem zaczęłaby generować zyski.

Każda z tych opcji na wady i zalety. Podczas podejmowania decyzji odnoście strategii postępowania należy wziąć pod uwagę koszty, możliwość wpływu na kształt usług, dostępność niezbędnych kompetencji oraz zaufanie do osób w to zaangażowanych (że będą poważnie podchodzić do obowiązków oraz nie będą udostępniać wewnętrznych danych). Pamiętać też należy o tym, że można również myśleć o modelach hybrydowych.

Podsumowanie

Cyberprzestępczość rozwija się w zastraszającym tempie. Przychody osiągane przez zorganizowane grupy są gigantyczne – istnieje nawet porównanie, że gdyby utworzyły one państwo, stałoby się ono trzecią ekonomią świata, tuż po USA oraz Chinach. Z tego powodu przestępcy mają dostęp do najnowszych technologii, które wykorzystując do zwiększenia skali działalności – atakowania na masową skalę, choć niekoniecznie w znacznie bardziej wyrafinowany sposób. Pamiętajmy bowiem, że dla cyberprzestępców rozwijanie nowoczesnych technologii to element swoiście pojmowanej „przewagi konkurencyjnej", że jest to inwestycja a nie koszt.

Często można usłyszeć, że „nie da się obronić przed wszystkimi atakami". Ale to stwierdzenie przede wszystkim dotyczy najbardziej istotnych podmiotów, które będą atakowane przez rządy wrogich państw czy międzynarodowe przestępcze syndykaty. Zdecydowana większość z organizacji jest zbyt mało znacząca, by stać się celem dla takich podmiotów. To, przed czym wszystkie szpitale powinny jednak się zabezpieczyć, to skutki cyberataków w wykonaniu script-kiddies, mniejszych grup przestępców motywowanych finansowo, skutki awarii i błędów oraz działalności sił natury. Cyberbezpieczeństwo jest bowiem kolejnym obszarem, którym trzeba zarządzać. Każdy szpital spełniać musi szereg wymagań w zakresie ochrony przeciwpożarowej, bezpieczeństwa i higieny pracy, musi przestrzegać norm sanitarnych i standardów w zakresie zapewniania bezpieczeństwa fizycznego. Przez lata podmioty już się nauczyły z żyć z tymi wymaganiami, stworzyły niezbędne struktury organizacyjne i wdrożyły niezbędne zabezpieczenia. Pędzący do przodu świat wymaga od zarządów zdobycia kompetencji w kolejnym obszarze i nikt na to nic nie poradzi.

Dr inż. Jakub Syta
zastępca dyrektora Morskiego Centrum Cyberbezpieczeństwa,
Akademia Marynarki Wojennej w Gdyni

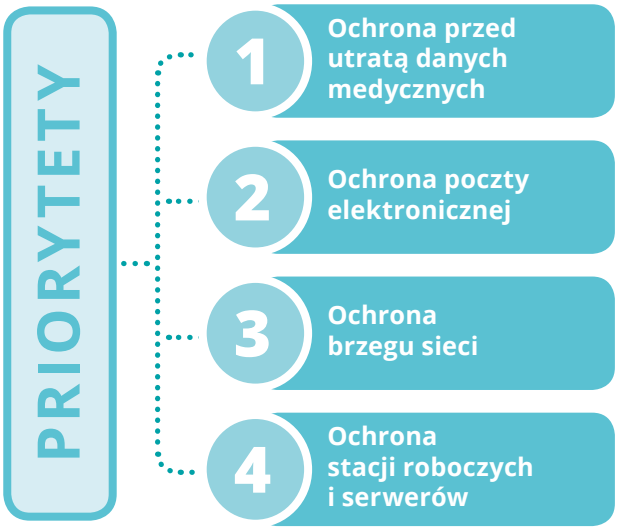
Image by rawpixel.com on Freepik

Rodzaje zabezpieczeń infrastruktury informatycznej

Sposoby zabezpieczenia danych medycznych – ochrona przed utratą lub wyciekiem

Ochrona danych medycznych powinna być szczególnie skoncentrowana na zabezpieczeniu miejsc składowania danych wrażliwych, w obszarach najbardziej narażonych na zewnętrzne ataki na infrastrukturę danej organizacji oraz o największym ryzyku wycieku danych. Zgodnie z rekomendacjami Centrum e-zdrowia, budowa systemu zabezpieczeń powinna być zgodna z czterema zidentyfikowanymi priorytetami (Rys. 1).

Priorytetyzacja ta jest szczególnie istotna dla właściwego zaplanowania modernizacji i rozwoju infrastruktury technicznej, tak aby w pierwszej kolejności mitygować największe ryzyka.



Rys. 1 Priorytety ochrony zasobów

Źródło: Opracowanie własne na podstawie „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia", Rekomendacje Centrum e-Zdrowia w zakresie budowy systemów cyberbezpieczeństwa, str. 7.

Ochrona przed utratą danych medycznych

System kopii zapasowych

Kluczowym zagadnieniem jest zapewnienie stałego dostępu do danych, w tym do medycznych danych archiwalnych. Konieczne jest utworzenie kopii zapasowych i takie ich zabezpieczenie, aby w przypadku ataku zewnętrznego przynajmniej jedna kopia była poza siecią i znajdowała się w innej lokalizacji. Zaleca się przy tym stosowanie zasady 3-2-1-1, zgodnie z którą powinno się posiadać minimum 3 kopie danych, przechowywane na przynajmniej 2 różnych nośnikach, z których jeden powinien być przechowywany w innej lokalizacji niż system produkcyjny. Jest to tak zwane odmiejscowienie kopii zapasowej, które może być realizowane na wiele sposobów

- repozytorium elektroniczne znajduje się w innej lokalizacji niż system produkcyjny,
- kopia zapasowa przechowywana jest w chmurze,
- biblioteka taśmowa znajdująca się w tej samej lokalizacji co system, ale taśma z danymi jest wynoszona regularnie do innej lokalizacji.

Ostatnia jedynka oznacza, że przynajmniej jedna kopia powinna pozostawać w trybie "offline", a więc być niedostępna dla systemów informatycznych. Za takie kopie uznaje się np.:

- dane na taśmach LTO przechowywanych w sejfie,
- dane na urządzeniach odłączonych od sieci,
- dane na macierzach obiektowych i urządzeniach, które wspierają tzw. retention lock, czyli mechanizm uniemożliwiający skasowanie bądź zmianę zapisanych danych nawet przez administratorów systemu.

W przypadku zastosowania chmury jako repozytorium dodatkowego, nowoczesne systemy kopii zapasowych, nie tylko pozwalają na sprawne tworzenie kopii ale zapewniają również granularne odzyskiwanie danych (np. pojedyncze pliki).

Repozytorium danych w chmurze powinno być szyfrowane. Stanowi to istotne zabezpieczenie w przypadku kompromitacji środowiska chmurowego, czego nie można wykluczyć. Sytuacja taka miała miejsce np. w listopadzie 2022 roku w firmie Last Pass, zapewniającej usługę bezpiecznego przechowywania haseł dla ponad 30 milionów klientów. Tylko dzięki stosowaniu przez Last Pass szyfrowania i architektury „Zero Knowledge" wykradzione dane z kopiami bezpieczeństwa pozostają nadal zaszyfrowane.

System kopii bezpieczeństwa powinien:

- zapewniać odtworzenie danych po awarii wewnętrznej lub ataku z zewnątrz (konieczne są regularne testy odtworzeniowe);
- być wykonywany zgodnie z ustalonym harmonogramem i rodzajem kopii (pełne kopie, kopie przyrostowe, etc.);
- zapisywać dane krytyczne na kilku nośnikach, jeden z nich powinien być przechowywany w innej lokalizacji i jeden pozostawać odłączony od pracującego środowiska informatycznego;
- być zgodny z regulacjami określającymi okres przechowywania danych.

Kolejnym istotnym zagadnieniem przy ochronie danych jest ich zabezpieczenie przed zaszyfrowaniem oraz zapewnienie ich niezmienności. Funkcjonalność taką zapewniają systemy typu WORM (*Write Once Read Many*), na których raz zapisane dane są już nieedytowalne.

Warto zwrócić uwagę, na typ urządzenia, które wykorzystuje się do składowania kopii zapasowych. Istnieją dedykowane rozwiązania do przechowywania kopii danych na dyskach twardych tzw. deduplikatory. Poza bardzo dobrą efektywnością przy składowaniu danych, osiąganą przez zaawansowane algorytmy deduplikacji i kompresji, pozwalającą przechowywać ponad dwudziestokrotnie więcej danych kopii zapasowych niż wynika to z natywnej pojemności zastosowanych dysków twardych, posiadają one szereg opcji zabezpieczających zapisane informacje. Po pierwsze, zapis na tego typu urządzeniach wykonywany jest z wykorzystaniem dedykowanych protokołów, co znacząco utrudnia przechwycenie tak przesyłanych danych, a zarazem powoduje, że tylko wyspecjalizowane i certyfikowane przez producenta sprzętu aplikacje, mają możliwość ich odczytu i zapisu. Po drugie, takie urządzenia są wyposażane w dodatkowe zabezpieczenia typu retention lock, uniemożliwiające usunięcie czy modyfikację zapisanych danych przez zdefiniowany okres. Podczas hipotetycznego ataku, haker dostałby się do systemu kopii zapasowych i przejąłby uprawnienia administratora, ale nie mógłby usunąć czy uszkodzić tak zabezpieczonych danych.

Poza typowym systemem kopii zapasowych, dane produkcyjne można zabezpieczyć także poprzez wykonywanie kopii migawkowych, tzw. snapshotów, na macierzach dyskowych. Dzięki wyspecjalizowanym kontrolerom oraz oprogramowaniu macierzy dyskowych, takie kopie można wykonywać z dużą częstotliwością, liczoną w pojedynczych godzinach, a nawet minutach. Bardziej zaawansowane modele macierzy zapewniają

marginalny spadek wydajności w przypadku przetrzymywania nawet wielu tysięcy takich migawek. Dodatkowo istnieją macierze, które mają zaimplementowany, wspomniany wcześniej mechanizm retention lock, który zabezpiecza tak utworzone migawki, przed ich skasowaniem, nawet dla administratora urządzenia. Co więcej, migawki macierzowe są widoczne tylko z poziomu samej macierzy dyskowej, dzięki czemu, są lepiej zabezpieczone w przypadku ataku na system informatyczny.

Szkolenia pracowników i zabezpieczenia mechaniczne

Szkolenia pracowników

Należy pamiętać że nie wystarczy skupić się wyłącznie na technologii. Bardzo istotnym elementem ochrony danych medycznych jest świadomość pracowników. Żaden wyspecjalizowany informatyczny system ochrony, kosztujący grube miliony złotych, nie jest w stanie zabezpieczyć w 100% dostępu do zasobów firmy, jeżeli będą w niej pracowali nieświadomi rodzajów cyberzagrożeń pracownicy.

Dlatego też wskazane jest regularne organizowanie szkoleń z zakresu cyberbezpieczeństwa oraz testowanie nabytej wiedzy przez pracowników, ponieważ w myśl znanego powiedzenia: „najwięksi hakerzy świata nie łamią kodu lecz ludzi", którzy są niezwykle podatni na manipulacje socjotechniczne.

Zabezpieczenia mechaniczne

Dodatkową ochronę przed wyciekiem danych stanowią tak proste rozwiązania jak filtry prywatyzujące na ekran, żeby postronna osoba spoglądając z ukosa na ekran, nie mogła zobaczyć wyświetlanych treści.

Warto też pomyśleć o zabezpieczeniu przed niepożądanym wyniesieniem, szczególnie w otwartych przestrzeniach, coraz częściej wykorzystywanych notebooków. Możemy je łatwo zabezpieczyć za pomocą dedykowanych linek (najpopularniejsze to Kensington lock'i), które korzystając ze specjalnego zamka na kluczyk lub kod dołącza się do niemal każdego notebooka (jest na to dedykowany otwór), a drugi koniec mocuje się do stałego elementu wyposażenia biura.

Ochrona poczty elektronicznej przed cyberzagrożeniami

Silne zabezpieczenie poczty elektronicznej powinno być priorytetem dla każdej organizacji. Poczta elektroniczna stanowi wrażliwy obszar podatny na ataki cyberprzestępców. Przedsiębiorstwa narażone są na ataki phishingowe, wirusy, scamy, itp. Coraz częściej stosowany jest spear-phishing, czyli spersonalizowany atak na osoby lub organizacje, w którym odbiorca ma wrażenie że zna adresata. W obliczu tych zagrożeń przedsiębiorstwa potrzebują szerokiej ochrony obejmującej wszystkie podatne obszary poczty elektronicznej.

Kompleksowa ochrona poczty powinna zapewniać:

- anty-phishing czyli możliwość wykrywania złośliwego oprogramowania wysyłanego jako załączniki lub złośliwe linki,
- wykorzystanie przetwarzania języka naturalnego (NLP – Natural Language Processing) do identyfikacji ataku phishingowego metodami socjotechnicznymi,
- ochronę przed złośliwym oprogramowaniem, takim jak trojany czy ransomware,
- wieloskładnikowe uwierzytelnianie dostępu do skrzynek pocztowych (MFA – Multifactor Authentication).

Dodatkowe systemy, mogące chronić także pocztę elektroniczną, potrafią:

- zapobiec utracie danych poprzez skanowanie maili i blokowanie udostępniania poza organizacje poufnych danych wcześniej zdefiniowanych w systemie jako wrażliwe (DLP – Data Leak Protection),
- zapobiec przejęciu konta poprzez monitorowanie i blokowanie podejrzanych prób dostępu ze stron phishingowych, na których pracownik jest proszony o podanie swoich danych uwierzytelniających.

Równie ważne jest zastosowanie nowoczesnych możliwości technicznych pozwalających na filtrowanie i blokadę niepożądanych wiadomości email. Umożliwiają to zaawansowane narzędzia, takie jak anty-Malware, Sandbox, anty-Wirus, anty-SPAM, anty-Phishing oraz wspomniane wcześniej DLP.

Typ narzędzia	Działanie
Anty-Malware	Ochrona przed różnego typu złośliwym oprogramowaniem
Filtr antyspamowy	Wychwytywanie podejrzanych maili i umieszczanie w dedykowanym folderze lub ich blokowanie
System DLP	Ochrona przed wyciekiem lub kradzieżą krytycznych danych
Sandbox	Analiza podejrzanych plików i linków w bezpiecznym, wyizolowanym środowisku
Anty-wirus	Zablokowanie i pozbycie się potencjalnie szkodliwych wiadomości zawierających rozpoznane sygnatury
Anty-phishing	Odfiltrowanie fałszywych wiadomości podszywających się pod znane marki i zachęcających do klikania w złośliwe linki

Tabela 1. Narzędzia ochrony poczty

Należy również pamiętać, że ważnym sposobem ochrony poczty elektronicznej jest zwiększanie świadomości pracowników poprzez organizowanie szkoleń z zakresu cyberbezpieczeństwa, o czym wspomniano wcześniej.

W dzisiejszych czasach systemy ochrony poczty elektronicznej można realizować poprzez urządzenia fizyczne instalowane w infrastrukturze firmowej, w postaci maszyn wirtualnych w środowisku firmowym lub jako instancje w chmurach publicznych. Jest to o tyle przydatne gdyż często poczta elektroniczna jest hostowana na zewnątrz, np. poczta w ramach licencji Microsoft 365. Niektórzy dostawcy posiadają w swojej ofercie integrację na poziome chmury swoich rozwiązań ochrony poczty.

Ochrona brzegu sieci

Ochrona brzegu sieci jest podstawowym elementem każdej sieci firmowej niezależnie czy jest to mała firma czy duża korporacja. Obecnie, w erze pracy zdalnej, duża część osób pracuje spoza biura, dlatego administratorzy stają przed nowymi wyzwaniami, aby prawidłowo skonfigurować bezpieczne dostępy do zasobów firmy z zewnątrz.

Znaczne rozszerzenie brzegu infrastruktury sieciowej oznacza zwiększenie liczby wrażliwych punktów, czyli potencjalnych celów ataku.

Dlatego też jednym z ważniejszych elementów infrastruktury informatycznej powinien być firewall, stanowiący pierwszą linię ochrony wewnętrznej sieci organizacji, czyli sieci LAN. Firewall stanowi zabezpieczenie sieciowe organizacji filtrujące cały ruch wchodzący i wychodzący. Blokuje on połączenia, które mogą stanowić potencjalne zagrożenie czyli ryzyko. Zapewnia on zarówno ochronę sieci lokalnej przed nieautoryzowanym dostępem z zewnątrz jak i ochronę przed niepożądanym udostępnianiem danych z komputerów lokalnych do sieci zewnętrznej. Dzisiejsze firewalle to urządzenia, które łączą w sobie różne funkcje, potrafią skanować ruch pod kątem zagrożeń jak wirusy czy malware, analizują ruch pod kątem odwiedzanych stron, potrafią rozpoznać typy transferowanych plików i np. blokować pobieranie plików wykonywalnych. Dzisiejszy firewall to urządzenie, które zagląda w połączenia i potrafi rozpoznać oraz kategoryzować rodzaje aplikacji i zezwolić na ruch wyłącznie z aplikacji zaufanych dla organizacji. Urządzenia te niejednokrotnie mają możliwość rozpoznawania podejrzanego ruchu jak skanowanie portów czy próby połączeń z wewnątrz do tzw. BOTNET-ów i skutecznie je blokować.

Wreszcie dzięki firewall'om możemy posegmentować sieć wewnętrzną i stworzyć polityki dostępu między sieciami wewnątrz firmy, np. odseparować komputery używane w administracji, które łączą się z systemami ERP, od komputerów medycznych, które powinny mieć dostęp głównie do systemów typu HIS.

Poza tym, jak wcześniej wspomniano, dzisiejsze firewalle to również punkty połączeń VPN, dzięki którym pracownicy mają dostęp do zasobów firmy ze zdalnych lokalizacji, jednocześnie możemy ruch z tych lokalizacji poddać analizie pod kątem zagrożeń opisanych wyżej.

Docelowo firewall powinien pracować w klastrze, dzięki czemu w razie awarii jednego z urządzeń, dostęp do sieci będzie dalej zapewniony.

Idąc za postępującą migracją systemów oraz danych do chmur publicznych również tam można odnaleźć firewalle. Obecnie kilku producentów, którzy posiadają swoje rozwiązania w formie maszyn wirtualnych, pozwala na uruchomienie takiej instancji u wiodących przedstawicieli chmur publicznych.

Drugim rosnącym na znaczeniu elementem ochrony brzegu sieci jest firewall aplikacyjny, czyli WAF (Web Application Firewall). Dzisiejsze WAF-y to elementy potrzebne na równi z Firewallami. Są to systemy, które potrafią analizować ruch do i z aplikacji webowych, czyli tych aplikacji, których na co dzień używamy wszyscy. Mimo, że można czasem usłyszeć od producentów że ich

klasyczne firewalle mają funkcję WAF to jednak dzisiaj firewall aplikacyjny to oddzielny system, którego należy posiadać w infrastrukturze informatycznej firmy. WAF-y potrafią analizować ruch pod kątem zagrożeń występujących w warstwie aplikacji, czyli w zapytaniach np. do serwisów WWW czy baz danych. Chronią infrastrukturę przed wykonywaniem złośliwego kodu w zapytaniach do serwerów, chronią przed atakami specyficznymi dla aplikacji internetowych/webowych, potrafią również ograniczyć ataki na dostępność usługi tzw. DOS/DDOS (rozproszony DOS – Denial of Service).

Dzięki WAF-om możemy zabezpieczyć m.in. systemy medyczne, które są wystawione dla użytkowników zewnętrznych do Internetu, takie które posiadają e-rejestrację czy podgląd do wyników badań.

WAF podobnie jak Firewall możemy wdrożyć w postaci fizycznego urządzenia, maszyny wirtualnej zainstalowanej w środowisku firmowym lub w chmurze publicznej. Ten ostatni przydaje się szczególnie, gdy posiadamy aplikacje webowe w chmurze.

Ochrona stacji roboczych i serwerów

Rozwiązania do ochrony stacji roboczych i serwerów to zabezpieczenia wdrażane na urządzeniach firmowych w celu zapobiegania cyberatakom, wykrywania złośliwej aktywności i zapewniania natychmiastowego łagodzenia jej skutków. Powinna być ona zapewniona przez centralnie zarządzany system antywirusowy oraz uruchomione lokalnie na stacjach roboczych i serwerach tzw. firewall'ach aplikacyjnych. Nowoczesne rozwiązania „endpoint security" umożliwiają firmom:

- zabezpieczenie się przed złośliwym oprogramowaniem,
- blokowanie ukierunkowanych ataków,
- zapobieganie naruszeniom bezpieczeństwa danych,
- zatrzymywanie ataków bezplikowych,
- wykrywanie zaawansowanych stałych zagrożeń,
- ochronę urządzeń mobilnych oraz zarządzanie nimi – MDM (Mobile Device Management).

Poza systemem antywirusowym, ważnym elementem ochrony stacji roboczych są systemy typu EDR (*EndPoint Detection & Response*). Tradycyjne systemy antywirusowe analizują operacje wykonywane na komputerach (np. otwieranie pliku) pod kątem sygnatur zapisanych w bazie danych. EDR jest rozszerzeniem tej ochrony przez analizę działań wykonywanych na komputerze lub innym urządzeniu przez użytkownika pod kątem wykrycia anomalii w tych działaniach. EDR-y są systemami, które wymagają od administratorów rozpoznania działań podejmowanych przez użytkowników i skategoryzowania działań zaufanych. Wszystkie inne działania zostaną uznane za odstępstwo od standardowego działania i mogą zostać zablokowane, np. wykonanie skryptu PowerShell na komputerze użytkownika lub podłączenie nośnika USB do stacji roboczej.

EDR podobnie jak systemy AV monitorują działania użytkowników poprzez agenta uruchomionego na stacji roboczej, zarządzanie odbywa się poprzez centralną konsolę.

Systemem, który również wpisuje się w pojęcie ochrony stacji roboczych jest system NAC (*Network Access Control*). Systemy NAC występują przeważnie w formie maszyn wirtualnych.

Dzięki NAC możemy sprawdzić stację roboczą lub urządzenie mobilne podczas łączenia się do sieci firmowej i na podstawie zebranych danych zezwolić lub nie na dostęp do zasobów firmy. NAC może działać w trybie bez agentowym lub agentowym. System bada klientów sieci podczas podłączenia oraz w trakcie połączenia. Potrafi monitorować stan zabezpieczeń i na podstawie zdefiniowanych polityk podjąć akcje, np. w przypadku wykrycia na stacji wyłączenia lokalnego antywirusa wyśle sygnał o odłączeniu klienta od sieci, a w przypadku wykrycia stacji z nieaktualnym stanem systemu, przeniesie klienta do kwarantanny celem aktualizacji systemu.

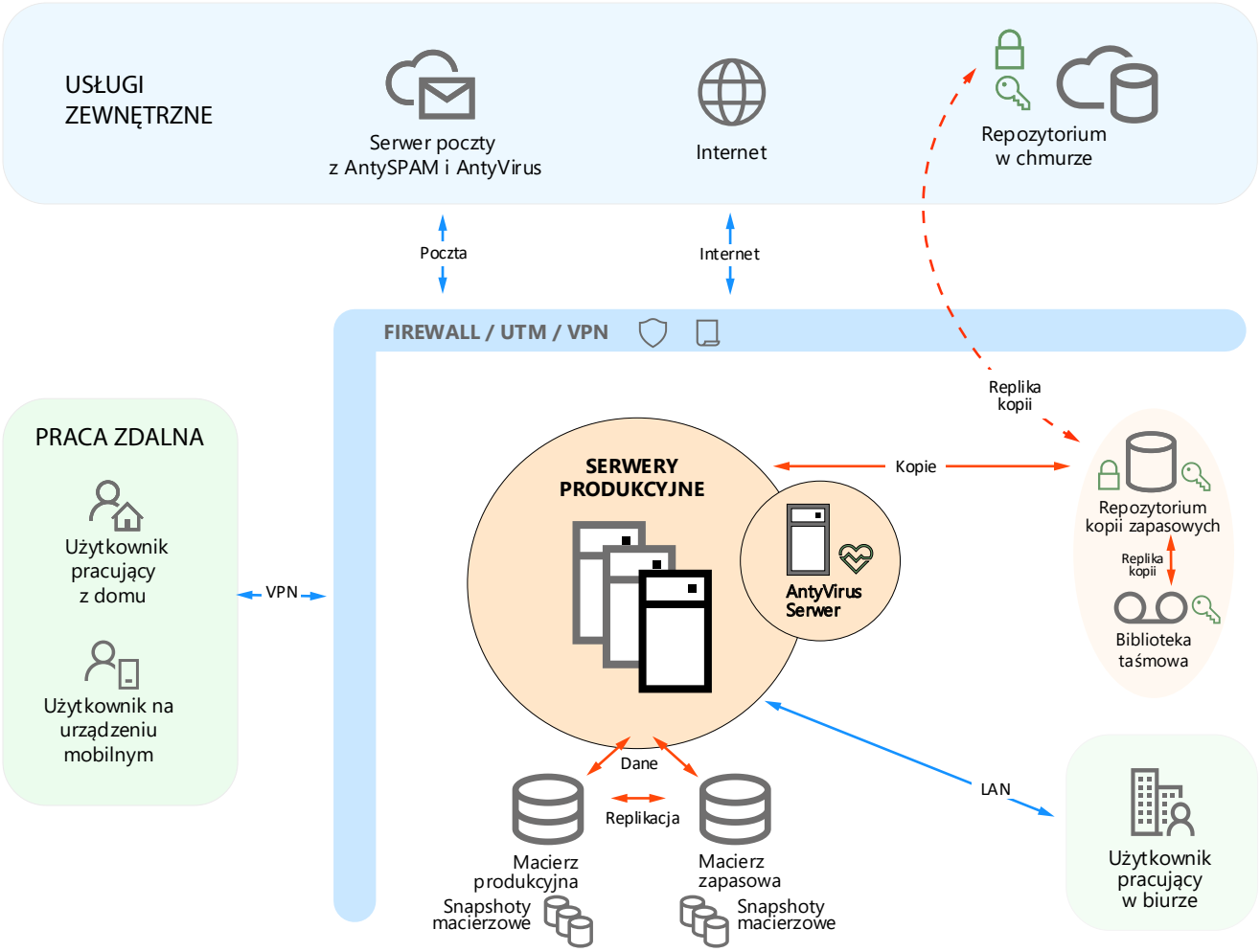
Dzięki tym systemom możemy również rozszerzyć możliwości dostępu dla gości, np. uwierzytelnienie dla gości do sieci bezprzewodowej lub przewodowej.

Centralny system zarządzania informacjami i zdarzeniami (SIEM)

Rozwiązanie klasy SIEM (*Security Information and Event Management*) to system do którego przekazujemy informacje (logi) z różnych systemów i rozwiązań. SIEM zbiera informacje, które przetwarza i unifikuje do jednakowej postaci, a następnie analizuje według zdefiniowanych reguł. SIEM koreluje zdarzenia z różnych systemów, odfiltrowuje standardowe komunikaty zostawiając na koniec informację o incydentach. Na tej podstawie administrator dostaje szybką informację o anomaliach w infrastrukturze. Skraca to czas na wykrycie incydentu i daje więcej czasu na reakcję.

Systemy SIEM są podstawą dla działów bezpieczeństwa, tzw. SOC (Security Operation Center), zajmujących się analizowaniem ruchu sieciowego w celu wykrycia incydentów, zagrożeń itp. Są też coraz powszechniej stosowane w coraz mniejszych firmach lub instytucjach.

Przykładowe składniki podstawowej architektury docelowej



Rys 2. Przykładowe składniki podstawowej architektury docelowej

Źródło: Opracowanie własne inspirowane „Planem działania w zakresie cyberbezpieczeństwa w ochronie zdrowia", Rekomendacje Centrum e-Zdrowia w zakresie budowy systemów cyberbezpieczeństwa, str. 48.

Tomasz Dębicki

kierownik Działu Technicznego w KOMA NORD, absolwent Politechniki Gdańskiej oraz ENSPM przy IFP w Paryżu. Posiada ponad 25-letnie doświadczenie zawodowe związane z działalnością IT, w tym w zarządzaniu spółką IT, prowadzącą outsourcing informatyczny oraz software-house. W swojej karierze zawodowej był odpowiedzialny za implementację rozwiązań z zakresu m.in. restrukturyzacji IT, cyberbezpieczeństwa, a także za zarządzania zmianą i incydentem (ITIL).

Kinga Szczygieł

Bezpieczeństwo informacji w placówkach medycznych – czy faktycznie jest tak ważne?

Wyobraź sobie, że jesteś rolnikiem, który wpadł pod kombajn i został ciężko poszkodowany, a śmigłowiec LPR nie może do ciebie przylecieć…

Wyobraź sobie, że jesteś pacjentem szpitala, który nagle gorzej się poczuł, ale nie możesz wezwać pomocy, bo przycisk alarmowy nie działa…

Wyobraź sobie, że jesteś pielęgniarką na nocnym dyżurze i agresywny pacjent zaatakował cię w ciemnym zaułku szpitalnego korytarza, ale nie masz systemu wzywania pomocy i nikt nie wie, gdzie jesteś i co się z tobą dzieje…

Wyobraź sobie, że jesteś lekarzem, który trzyma w ramionach chore dziecko i nie jesteś w stanie mu pomóc, bo wszystkie jego dane medyczne zostały zaszyfrowane…

Takie historie to dziś nie *science-fiction*, ale smutna rzeczywistość niektórych placówek ochrony zdrowia. W dobie ogromnej inflacji, wszechobecnego cięcia kosztów i oglądania każdej złotówki przed jej wydaniem, nakłady na cyberbezpieczeństwo w ochronie zdrowia często uznawane są za zbędny wydatek. Wydaje się, że posiadane środki lepiej przecież przeznaczyć na zakup nowego sprzętu, wypłatę dodatków do pensji dla przemęczonego personelu, remont pomieszczeń - ale czy na pewno?

Wprowadzonych zostało już kilka, istotnych z punktu widzenia pacjentów, projektów teleinformatycznych, takich jak e-recepta, e-skierowanie. To ułatwia funkcjonowanie pacjentów, ale też zmusza do przywiązania większej wagi do cyberbezpieczeństwa.

Prawdopodobieństwo ataków hakerskich na podmioty ochrony zdrowia rośnie z każdym dniem. Nie wszyscy zarządzający szpitalami zdają sobie sprawę z konsekwencji, jakie może za sobą nieść cyberatak. To nie tylko straty finansowe, ale przede wszystkim zagrożenie życia i zdrowia pacjentów. I nie są to czarne scenariusze na przyszłość, ale rzeczywistość i doświadczenia niektórych placówek. Ofiarą hackerów padł już m.in. w 2022 roku szpital w pajęcznie oraz Instytut Centrum Zdrowia Matki Polki w Łodzi, czy wiosną 2021 r. wspomniane przeze mnie na wstępie Lotnicze Pogotowie Ratunkowe. W szpitalu w Düsseldorfie atak hakerski w 2020 r. doprowadził nawet do śmierci pacjentki.

Dziś placówki medyczne mogą otrzymać środki z NFZ na podniesienie poziomu bezpieczeństwa systemów teleinformatycznych. O środki mogą ubiegać się szpitale, które realizują świadczenia w ramach leczenia szpitalnego, rehabilitacji leczniczej, lecznictwa uzdrowiskowego oraz opieki psychiatrycznej i leczenia uzależnień. NFZ finansuje zakup i wdrożenie systemów teleinformatycznych oraz związanych z nimi usług, dotyczących podniesienia poziomu bezpieczeństwa w placówkach leczniczych (nie tylko obszaru informatycznego). Inwestycje mogą obejmować m.in. zakup: urządzeń, oprogramowania i usług, które zapobiegają, wykrywają lub zwalczają cyberataki; systemów kontroli dostępu; oprogramowania zabezpieczającego sieć i pocztę elektroniczną; szkolenia z cyberbezpieczeństwa dla kadry zarządzającej i pracowników oraz wykonanie audytu cyberbezpieczeństwa.

Zabezpieczenie infrastruktury IT w szpitalach i innych jednostkach ochrony zdrowia to dziś kluczowa kwestia, wiele z nich nie nadąża jednak za zmianami, jakie narzuca pomysłowość hakerów. Do najczęstszych problemów, z jakimi borykają się jednostki ochrony zdrowia należą luki w aplikacjach i w architekturze sieci, m.in. brak skutecznego backupu, szyfrowania i anonimizacji danych czy brak aktualizacji oprogramowania, także wewnętrznego kodu urządzeń. Sposobem na szybkie usunięcie tych i innych błędów, są regularne audyty i testy bezpieczeństwa. Pozwalają one wykryć nieprawidłowości i znaleźć sposób na ich skorygowanie. Bardzo ważne są też cykliczne szkolenia pracowników szpitali i innych placówek medycznych w zakresie bezpieczeństwa IT. Atak może wywołać prosty błąd ludzki – każdy kto ma kontakt z danymi pacjentów, musi znać zagrożenia i rozumieć, czym jest cyberbezpieczeństwo.

Jak jednak przeprowadzić taki audyt, by nie był on jedynie „sztuką dla sztuki", lecz rzeczywiście wskazywał potencjały do doskonalenia i dawał pełną wiedzę o organizacji i jej bezpieczeństwie? Wynik audytu jest uzależniony od tego, co przyjmiemy jako punkt odniesienia. W przypadku chęci pozyskania refundacji, audyt w szpitalu czy innej placówce ochrony zdrowia powinien być przeprowadzany według wytycznych odpowiedniego Zarządzenia Prezesa NFZ.

Podobnie jak w medycynie, również w IT każdą poważną operację należy poprzeć odpowiednią i profesjonalną diagnozą. Audyt infrastruktury IT w szpitalu powinien zacząć się od zebrania informacji nt. stosowanych aktualnie zabezpieczeń, po czym powinno nastąpić badanie infrastruktury poprzez odpowiednie testy. Umożliwiają one sprawdzenie m.in. czy możliwy jest nieautoryzowany dostęp z zewnątrz do systemu czy bazy danych np. za pomocą symulowanego ataku na sieć bezprzewodową (testy zewnętrzne), a także kontrolę potencjalnie słabych punktów w konfiguracji urządzeń (testy wewnętrzne). Szczególną uwagę należy poświęcić właśnie urządzeniom podłączonym do wewnętrznej sieci szpitalnej, tworzącej „Internet Rzeczy" czyli IoT. W takie rozwiązanie inwestuje coraz więcej jednostek, tworząc kolejne furtki, którymi hakerzy mogą dostać się do wrażliwych danych - tym bardziej, że tworzą oni specjalnie przygotowane do tego szkodliwe oprogramowanie malware jak Mirai czy Katana. Bardzo ważne jest weryfikowanie w tym momencie zachowania pracowników, ale o tym szerzej nieco później.

Następnie należy przeanalizować wyniki i na ich podstawie opracować raport, który przedstawi wnioski z audytu i propozycje obszarów niezbędnych do doskonalenia. Najczęściej zalecenia dotyczą m.in. nadawania i odbierania uprawnień w systemach, inwentaryzacji sprzętu, szyfrowania urządzeń, przeprowadzania analizy ryzyka czy podnoszenia świadomości wśród użytkowników.

Wpuszczając audytora do swojej organizacji, otwieramy przed nim wszystkie swoje „tajemnice", dlatego niezwykle ważnym jest, by nie kierować się tylko kryterium ceny, tylko świadomie wybierać osobę z doświadczeniem i rekomendacjami. Audytorem powinna być osoba spełniająca wymagania, opublikowane w rozporządzeniu ministra cyfryzacji z 12 października 2018 r. (np. posiadająca certyfikat Audytora Wiodącego ISO 27001, akredytowany przez PCA).

Audyt bezpieczeństwa należy przeprowadzić na zakończenie realizacji projektu, w terminie do końca października 2023 r. - będzie on podstawą refundacji wydatków. Po wykonanym audycie cyberbezpieczeństwa, zgodnie z KRI, przynajmniej raz w roku należy badać system zarządzania bezpieczeństwem informacji.

Niezwykle ważnym aspektem, często pomijanym w procesie podnoszenia cyberbezpieczeństwa, jest konieczność odpowiedniego przeszkolenia personelu. Powiedzenie, że to człowiek jest najsłabszym ogniwem, nie straciło na aktualności, a w dzisiejszych czasach jest wręcz kluczowe dla prawidłowego działania każdego systemu. Oprócz zakupu systemów i oprogramowania, sprzętu, programów antywirusowych, które zapewniają prewencję i reakcję w razie zagrożenia, konieczna jest także edukacja personelu w tym zakresie. Nawet najlepsze zabezpieczenia będą nic niewarte, jeśli zawiedzie czynnik ludzki. Sprawdzanie skrupulatności w stosowaniu zasad bezpieczeństwa, odporności na techniki manipulacyjne oraz sposobu reakcji w razie zagrożenia, to absolutne minimum. Większość ataków typu ransomware zaczyna się od wysłania fałszywego maila z linkiem do szeregowego pracownika, dzięki któremu haker dostaje się do zasobów organizacji - wystarczy, że jedna osoba kliknie... hakerzy najczęściej wykorzystują nasze naturalne obawy oraz kontekst sytuacyjny (np. często z wykorzystaniem hasła COVID). Tu liczy się efekt skali, dlatego każda, nawet najmniejsza organizacja jest narażona na atak.

Ważne jest, aby wszystkie te działania przeprowadzać cyklicznie – hackerzy bardzo często wykazują się dużym sprytem i penetrują system etapami, by nie wzbudzać zbyt wielkich podejrzeń.

Najczęściej spotykaną barierą, która utrudnia szpitalom podniesienie poziomu cyberbezpieczeństwa, jest brak środków na ten cel, dlatego program dofinansowania,

który uruchomiło Ministerstwo Zdrowia, pozwala placówkom medycznym zainwestować w swoje cyberbezpieczeństwo (w formie refundacji kosztów). W zależności od wysokości kontraktu NFZ, może to być nawet od 240 do 900 tysięcy złotych. Czas na składanie wniosków na ten cel został przedłużony do 31 października 2023 roku.

Każdy zarządzający placówką medyczną chciałby wiedzieć, czy jego szpital jest bezpieczny i odporny na cyberataki. Jak to zrobić? Najlepszym narzędziem do zarządzania bezpieczeństwem informacji wydaje się być norma ISO 27001. Wdrożenie jej wymagań oraz cykliczne audyty, realizowane przez wewnętrznych audytorów oraz niezależnych audytorów jednostki certyfikującej, zwiększają szanse na uniknięcie incydentu i problemy wynikające z tego faktu. Wdrożenie i certyfikowanie się na zgodność z ISO 27001 to nie tylko zwiększenie bezpieczeństwa i spokojny sen, ale również poprawa swojej pozycji podczas kontraktowania z NFZ.

Wzmacniając bezpieczeństwo szpitali, wzmacniamy bezpieczeństwo danych pacjentów i ich samych.

Kinga Szczygieł

doradca klienta ds. bezpieczeństwa informacji w TUV NORD Polska. Firma TUV NORD Polska posiada ponad 140-letnią tradycję działalności na świecie, a od ponad 25 lat działa w Polsce. Wspiera kluczowe branże: spożywczą w zakresie bezpieczeństwa żywności, wyrobów medycznych skierowaną do producentów i importerów, techniczną, mając na uwadze środowisko naturalne oraz efektywność eneregetyczną i cybernetyczną, związaną z szeroko pojętym bezpieczeństwem procesowym oraz bezpieczeństwem informacji.

Image by rawpixel.com on Freepik

Marcin Majchrzak

yubico

Przyszłość uwierzytelniania na potrzeby szpitali i placówek medycznych

Ponieważ ataki cybernetyczne stają się coraz bardziej wyrafinowane, zabezpieczanie danych stanowi coraz większe wyzwanie dla organizacji opieki zdrowotnej.

Organizacje w całym sektorze opieki zdrowotnej stoją w obliczu rosnącego wskaźnika cyberataków. W porównaniu z rokiem ubiegłym, zanotowano wzrost liczby incydentów, jak również ich skuteczności. Opieka zdrowotna jest trzecim najczęściej atakowanym sektorem w Polsce zaraz po edukacji i placówkach rządowych. Dochodzi tam średnio do 1426 ataków tygodniowo, co oznacza wzrost o 60% w porównaniu ubiegłymi latami.

Według raportu, opublikowanego niedawno przez firmę Sophos, liczba ataków *ransomware* wzrosła w ostatnim roku o 94%, przy czym 66% dotkniętych organizacji specjalizuje się w opiece zdrowotnej, w porównaniu do 34% w roku poprzednim. W związku z tym zakłady w tym sektorze muszą wzmocnić swoje systemy obronne i wdrożyć całościową strategię, aby udaremnić wszelkie próby włamań.

Według badania bezpieczeństwa cybernetycznego HIMSS, najwięcej incydentów bezpieczeństwa w służbie zdrowia można przypisać *phishingowi* (45%) i atakom *ransomware* (17%).

Większość cyberataków wymierzonych w opiekę zdrowotną koncentruje się na słabościach kontroli bezpieczeństwa, takich jak brak uwierzytelniania wieloskładnikowego (MFA) w całej organizacji (34%).

Te niezabezpieczone luki w całym ekosystemie opieki zdrowotnej sprawiają, że dane i życie pacjenta często stają się zagrożone.

Sektor zdrowotny dochodowym celem dla hakerów

Sektor zdrowotny jest podwójnie dochodowy dla hakerów: jego duże budżety operacyjne i umowy ubezpieczeniowe sprawiają, że jest to cel opłacalny finansowo, a ponadto złożone i przestarzałe systemy informatyczne sprawiają, że jest on bardziej podatny na cyberataki.

Cyberprzestępcy wiedzą również, że prawie wszystkie organizacje podlegają konieczności szybkiego przywrócenia swojej działalności, aby zapewnić ciągłość usług, a tym samym zagwarantować zdrowie i bezpieczeństwo pacjentów. Obowiązki te dotyczą całego ekosystemu medycznego, niezależnie od tego, czy jest to szpital, łańcuch dostaw czy dostawca ubezpieczeń zdrowotnych.

Słabe strony hasła

Aby ograniczyć szkody, placówki służby zdrowia muszą bezzwłocznie zabezpieczyć się przed rosnącym zagrożeniem i zapewnić ochronę danych krytycznych.

Jednak rzeczywistość jest taka, że większość hakerów nie włamuje się: oni się logują. Konkretnie, poświadczenia są wykorzystywane w 61% naruszeń danych, zgodnie z raportem Verizon Data Breach, z czego 25% jest spowodowanych oprogramowaniem *ransomware*. W związku z tym placówki służby zdrowia muszą wdrażać rozwiązania uwierzytelniające, które gwarantują użytkownikom zwiększone bezpieczeństwo krytycznych systemów i ich wrażliwych informacji. Niezbędne jest również skonsolidowanie ochrony ich krytycznych danych, a tym samym udaremnienie żądań okupu ze strony cyberprzestępców. W tym celu niezbędna jest zgodność z RODO oraz wdrożenie urządzeń z odpowiednimi zintegrowanymi zabezpieczeniami lub narzędziami do ochrony przechowywanych informacji.

Przeciwdziałanie cyberatakom za pomocą silnego uwierzytelniania

Aby zapewnić optymalną ochronę przed cyberzagrożeniami, fundamentalne znaczenie ma ograniczenie najczęściej wykorzystywanych przez hakerów punktów dostępowych, czyli zabezpieczenie procesu logowania i ochrona przed *phishingiem*. Ich wspólnym mianownikiem jest użytkownik, który w przypadku nieprzestrzegania dobrych praktyk, w połączeniu z podstawową metodą uwierzytelniania, jaką jest hasło, często pozwala cyberprzestępcom otworzyć drzwi organizacji.

Co więcej, wysiłki związane z wdrożeniem są minimalne w porównaniu ze skutkami ataku ransomware, biorąc pod uwagę utratę danych i tytaniczne prace naprawcze. Jeśli chodzi o zapobieganie, istnieje bardzo proste rozwiązanie: zabezpieczyć dostęp użytkowników do krytycznych systemów, poprzez wdrożenie odpornej na *phishing*, silnej metody uwierzytelniania wieloskładnikowego (MFA).

To MFA, najlepiej wdrożone za pomocą karty kryptograficznej (SmartCard) lub klucza bezpieczeństwa FIDO2, pozwala organizacjom opieki zdrowotnej radzić sobie z próbami naruszenia tożsamości i obejścia uwierzytelniania. Zdalne hakowanie jest rzeczywiście niemożliwe, ponieważ opiera się wyłącznie na fizycznym urządzeniu odblokowywanym unikalnym kodem PIN lub biometrycznym odciskiem palca, aby zalogować się na konto. Ponadto zapewnia rozwiązanie nieodłącznych problemów, związanych z przestarzałymi metodami uwierzytelniania, takimi jak naruszenia w przypadku udostępniania hasła. Rzeczywiście, narzędzie, które skraca czas logowania lub jego etapy, znacznie zmniejsza zmęczenie cybernetyczne pracowników. Organizacje są zatem zainteresowane wzięciem tego aspektu pod uwagę przy wdrażaniu strategii cybernetycznej, która z jednej strony musi obejmować bezpieczeństwo danych, a z drugiej strony ma pozytywny wpływ na doświadczenia użytkowników.

Cyberprzestępcy nadal wykorzystują luki w zabezpieczeniach w branży medycznej, co czyni ją głównym celem ataków *ransomware*. Aby zabezpieczyć swoje krytyczne dane i udaremnić wszelkie żądania przestępcze, organizacje te muszą znacznie wzmocnić swoją obronę. Wdrożenie MFA, odpornego na phishing i łatwego w obsłudze, umożliwia w szczególności blokowanie dostępu do istotnych systemów oraz obronę przed kradzieżą identyfikatorów. Włączając to rozwiązanie do swojej strategii cybernetycznej, organizacje opieki zdrowotnej będą w stanie skutecznie przeciwdziałać zagrożeniom cybernetycznym wiszącym nad sektorem.

Marcin Majchrzak

dyrektor handlowy Yubico, od ponad 10 lat specjalizuje się w cyberbezpieczeństwie. Swoje doświadczenie managerskie zdobywał m.in. wspierając organizacje rządowe, komercyjne oraz służby mundurowe w regionach EMEA i APAC. Zaangażowany był w ich staraniach zredukowania ryzyka i zabezpieczenia systemów poprzez wdrożenia projektów z zakresu Zarządzania Przywilejami (Privilege Management), Uwierzytelniana Wieloskładnikowego (MFA) Infrastruktury PKI oraz FIDO.

Krzysztof Tomkowicz

Hewlett Packard Enterprise

W ochronie wrażliwych danych najważniejsze są szybkość i niezawodność

Ochrona danych ma wiele wspólnego z medycyną – lepiej jest zapobiegać niż leczyć. W internecie zagrożenia czyhają na użytkowników na każdym kroku. Można się jednak przed nimi obronić.

W ostatnich latach różne aspekty naszego życia coraz częściej przybierają formę cyfrową. Dzięki postępowi technicznemu wiele czynności uległo uproszczeniu. Nowe możliwości zrodziły jednak nowe zagrożenia. Jeszcze dwadzieścia lat temu mało kto przejmował się przestępczością w internecie, ale wraz z rozwojem technologii rozwinęły się też metody działania niezgodne z prawem. W badaniu z 2022 roku przeprowadzonym przez firmę SW Research na zlecenie strony kwestiabezpieczeństwa.pl prawie 1/4 Polaków przyznała, że padła ofiarą oszustwa internetowego. Przestępcy opracowują kolejne sposoby podszywając się pod sklepy, dostawców energii, spółdzielnie mieszkaniowe, a nawet banki i instytucje publiczne. Niektórzy opracowali swoje metody niemal do perfekcji i tylko osoba z wprawnym okiem jest w stanie szybko odróżnić prawdziwą wiadomość od fałszywej. Jedno kliknięcie może umożliwić cyberzłodziejom kradzież wrażliwych danych. A im więcej informacji przestępcy posiadają, tym łatwiej jest im okraść ofiarę.

Przypadki kradzieży danych ze szpitali

Nie tylko osoby prywatne padają ofiarami kradzieży danych. Przestępcy wykwalifikowani do działań w sieci coraz częściej biorą sobie za cel firmy i instytucje, w których coraz częściej tradycyjne księgi rachunkowe i adresowe zostały zastąpione plikami na serwerach. Wrażliwe dane, takie jak imię i nazwisko, numer PESEL, czy adres mogą posłużyć oszustom we wzbogaceniu się, a ich ofiarom sprawić poważne problemy.

Kradzieże danych zdarzają się także w placówkach medycznych. W marcu 2022 roku ze Szpitala Miejskiego w Gliwicach skradziono dane pacjentów. Co prawda w zrabowanych materiałach nie było dokumentacji medycznych, ale znalazły się tam m.in. numery PESEL. Do podobnej sytuacji doszło w lutym 2019 roku w Bełchatowie, gdzie oprócz imion, nazwisk i numerów PESEL cyberprzestępcy ukradli także wzory podpisów pacjentów szpitala. Dwa lata wcześniej doszło do innej bardzo groźnej sytuacji. Przez pewien czas każdy użytkownik internetu miał łatwy dostęp do danych pacjentów szpitala w Kole. Wśród niezabezpieczonych danych znajdowały się nawet prywatne adresy.

Te przypadki pokazują, że ofiarami przestępców internetowych nie padają tylko wielkie firmy, ale i placówki na pozór mniej atrakcyjne dla złodzieja.

Szybkość w dostępie do danych

Wielu niebezpiecznych sytuacji związanych z przesyłaniem i udostępnianiem danych da się uniknąć, chociażby przez umieszczenie danych w jednym miejscu i tworzenie ich kopii zapasowych. Narzędziem pozwalającym pracownikom na dostęp do plików z niemal każdego miejsca na świecie jest chmura. To nic innego, jak miejsce, gdzie składowane są dane potrzebne do pracy konkretnej organizacji. Firma HPE, której technologie oferuje Koma Nord, od lat przygotowuje rozwiązania ułatwiające pracę w zespole, dzięki czemu zna potrzeby zarówno małych, jak i dużych firm w zakresie wymiany danych.

Szybki dostęp do potrzebnych plików zwiększa produktywność i pozwala skupić się na samych danych, a nie na dostępie do nich. Wśród zmian w codziennym życiu, jakie przyniosła pandemia covid-19, jest większy procent pracy wykonywanej zdanie. Kluczowym w zarządzaniu firmą stał się szybki dostęp do danych przechowywanych na laptopach, komputerach stacjonarnych i w chmurze. Jeśli przedsiębiorstwo nie dysponuje odpowiednimi narzędziami umożliwiającymi płynne działanie, to jego pracownicy w dobrej wierze mogą uciekać się do korzystania z nieautoryzowanych programów.

A to niesie za sobą ogromne ryzyko utraty lub wycieku danych. W 2021 roku firma HPE sfinalizowała przejęcie firmy Zerto, która specjalizuje się w rozwiązaniach do odzyskiwania danych po awarii, odzyskiwania danych po ataku oprogramowania typu ransomware i przenoszenia zasobów między różnymi chmurami. Firma Zerto, będąca obecnie częścią HPE, oferuje ciągłą ochronę i odzyskiwanie aplikacji oraz danych zwirtualizowanych i skonteneryzowanych od brzegu sieci do chmury. Dzięki Zertomożna przywrócić stan sprzed ataku, eliminując długotrwałe i kosztowne przestoje i utratę danych. Zerto zapewnia większą dostępność systemów przy znacznie niższych kosztach administracyjnych niż w przypadku starszych rozwiązań ochrony danych.

Lepiej zapobiegać niż leczyć

Podobnie, jak w medycynie, w dziedzinie zarządzania danymi lepiej jest pomyśleć o tym zawczasu. Jednym z zabezpieczeń jest przechowywanie danych na sprawdzonych i solidnych urządzeniach. Narzędziami, które to umożliwiają, są serwery HPE ProLiant Gen10. Zostały one przetestowane i zoptymalizowane pod kątem wdrożeń lokalnych. Zaprojektowano je także z myślą o obniżeniu kosztów, zwiększeniu dostępności do danych i łatwości użycia.

– Na bazie serwerów HPE ProLiant wdrażamy systemy, które nie tylko chronią pliki, ale także, w sposób bardzo wydajny, tworzą i przywracają ich kopie zapasowe. Dzięki temu ograniczony zostaje czas potrzebny na przywrócenie pracy po ewentualnym przestoju. Pozwala nam to zmniejszyć ryzyko utraty potencjalnego klienta, a obecnych utwierdza w przekonaniu, że firma jest dobrze przygotowana nawet na wydarzenia od niej niezależne, takie jak ataki hakerskie czy klęski żywiołowe, mogące skutkować zniszczeniem fizycznych serwerów – podkreśla Krzysztof Tomkowicz, inżynier systemów informatycznych z firmy KOMA NORD, oferującej rozwiązania i usługi HPE.

Kapitał, który trudno odbudować

Wielu przedsiębiorców podkreśla, że kluczem w prowadzeniu firmy jest zaufanie. Komfort polegania na współpracownikach jest równie ważny, jak niezawodność systemów komputerowych. A to właśnie od nich w dużej mierze zależy, jak w oczach klientów będzie postrzegane przedsiębiorstwo. Historie o wycieku, bądź kradzieży danych to poważne rysy na wizerunku. Firma, która nie jest w stanie zapewnić swoim kontrahentom i klientom należytego bezpieczeństwa, z zasady jest gorzej oceniania.

Gdy wrażliwe dane takie, jak imię nazwisko, PESEL czy numer dokumentu tożsamości dostaną się w niepowołane ręce, ich właściciel powinien jak najszybciej zabezpieczyć się na wypadek np. zaciągnięcia przez niepowołane osoby kredytu. Taki scenariusz z automatu przywołuje myśli o zmianie dostawcy danej usługi na bezpiecznego, bo zaufanie to kapitał, który buduje się latami, a stracić można go w ułamku sekundy.

Nieprzyjemnych incydentów można uniknąć dzięki produktom do przechowywania kopii zapasowych i archiwizacji HPE StoreOnce i StoreEver. Istnieje także rozwiązanie chroniące dane zgromadzone nie w chmurze, a na urządzeniach stacjonarnych. Dzięki bezpiecznemu systemowi szyfrowania HPE Secure Encryption wszystkie pliki pozostaną pod doskonałą ochroną.

Cztery kroki działania

Obok potrzeb fizjologicznych, jedną z najważniejszych potrzeb w życiu człowieka, jest bezpieczeństwo. W ostatnich latach jego definicja uległa przeobrażeniu, ale klucz jest ten sam – komfort psychiczny.

– Mając do dyspozycji narzędzia HPE do obsługi plików i zabezpieczeń, szefowie firm mogą przestać obawiać się nieprzyjemnych incydentów związanych z danymi. Cenny w każdym przedsiębiorstwie czas, dotychczas wkładany w dotarcie do konkretnych plików, przeznaczyć można na inne pilne działania - mówi Krzysztof Tomkowicz.

„Nigdy nie ufaj, zawsze sprawdzaj" – te słowa idealnie określają obchodzenie się z ważnymi i wrażliwymi danymi. Kluczową strategią jest weryfikacja tożsamości przy każdym żądaniu dostępu, a także stosowanie „zasady najmniejszego przywileju" (ang. Principle of Least Privilege, PLP), która polega na przyznawaniu podmiotom wyłącznie tych przywilejów, które są im niezbędne do wykonywania określonych zadań. Mówiąc najprościej, jest to rozwinięcie idei DevOps, która łączy programistów (i pracowników pomocniczych, takich jak testerzy, dokumentaliści i trenerzy) z personelem operacyjnym (administratorzy, wsparcie techniczne oraz technicy lub serwisanci terenowi) w jedną organizację o wspólnych celach i zadaniach.

DevSecOPs idzie o krok dalej i integruje personel bezpieczeństwa w całym cyklu programistycznym, dzięki czemu bezpieczeństwo jest uwzględniane na etapach projektowania, konstruowania, testowania, konserwacji i wycofywania z eksploatacji w ramach obsługi biznesowej IT.

Firma HPE przy tworzeniu serwerów ProLiant kierowała się trzema prostymi krokami zabezpieczającymi przed ryzykiem utraty danych. Pierwszy z nich to identyfikacja luk w zabezpieczeniach, które stanowią rzeczywiste zagrożenie i ocena potencjalnych skutków i konsekwencji. Kolejnym jest ich uszeregowanie pod kątem szkodliwości zarówno wizerunkowym, jak i finansowym. Trzecim krokiem jest plan ograniczenia i eliminacji ryzyka. Taki plan powinien funkcjonować w każdej firmie obracającej wrażliwymi danymi. Nie w każdym przedsiębiorstwie jest jednak rozbudowany zespół, który jest w stanie zadbać o bezpieczeństwo.

Elastyczne rozwiązania dostosowane pod klienta

Każdy biznes jest inny i wymaga innych rozwiązań. Wiedzą to inżynierowie HPE, którzy od lat przygotowują konkretne rozwiązania informatyczne dla konkretnych przedsiębiorstw. Działanie według określonego wzoru niesie za sobą ryzyko pominięcia istotnych szczegółów dla danego odbiorcy. Dział usług HPE Pointnext Services pomaga we wprowadzaniu innowacji i uzyskaniu większych możliwości przy jednoczesnym zmniejszeniu nakładów. Zróżnicowana oferta – od doradztwa w zakresie rozwiązań, przez usługi wsparcia, zapewniają wydajne i niezawodne działanie środowiska danych. Aby dowiedzieć się więcej, skontaktuj się z przedstawicielem handlowym firmy KOMA NORD, a więcej informacji uzyskasz odwiedzając stronę komanord.pl.

Krzysztof Tomkowicz

inżynier systemowy Koma Nord z ponad 15-letnim doświadczeniem w projektowaniu, wdrażaniu oraz administrowaniu systemami informatycznymi zarówno w warstwie sprzętowej (serwery, macierze, urządzenia sieci LAN i SAN) jak i programowej (systemy Linux, Windows, wirtualizatory). Posiada certyfikat HPE Master Accredited Solution Expert, który potwierdza kompetencje techniczne jak i pełną znajomość rozwiązań z portfolio HPE. Czynnie uczestniczy w przygotowywaniu i realizowaniu projektów wdrożeniowych, zarówno tych najmniejszych opartych na pojedynczych serwerach, jak i największych, obejmujących tworzenie całych centrów danych.

Przemysław Zatarski

FORTINET – najnowsza generacja rozwiązań cyberbezpieczeństwa

Cyberbezpieczeństwo stało się jednym z najważniejszych wyzwań współczesnego świata. Skala incydentów i ataków hakerskich przybiera na sile, generując istotne ryzyko dla struktur organizacyjnych państw, biznesu czy sektora publicznego. Wśród najbardziej zagrożonych instytucji są placówki medyczne, które przechowują wiele wrażliwych danych, korzystają ze złożonych systemów informatycznych oraz aktywnie komunikują się z otoczeniem.

Odpowiedzią na takie wyzwania są rozwiązania firmy FORTINET zapewniające najwyższy poziom bezpieczeństwa.

Sektor opieki zdrowotnej w coraz szerszym zakresie wykorzystuje najnowsze rozwiązania IT, sukcesywnie zwiększając swoją aktywność w cyfrowym świecie. Wynika to m.in. z konieczności poprawy komunikacji, przepływu danych oraz zwiększenia komfortu opieki nad pacjentami oraz udoskonalenia warunków pracy personelu medycznego. Nie bez znaczenia pozostaje także wpływ pandemii, która wymusiła przekształcenie wielu procesów do statusu „online".

Niestety zwiększona aktywność cyfrowa placówek medycznych nie zawsze szła w parze z inwestycjami w skuteczne systemy zabezpieczeń. Spowodowało to wzrost liczby cyberzagrożeń, które mogą narazić podmioty lecznicze na olbrzymie straty finansowe, utratę zaufania, a nawet zagrażać życiu wielu ludzi. Problem dotyczy całego świata od USA po Europę – wszędzie tam, gdzie cyberprzestępcy zauważą słabości i luki w zabezpieczeniach. Całkiem niedawno w Stanach Zjednoczonych opieka zdrowotna była jednym z najczęściej atakowanych sektorów życia publicznego. W Polsce również mamy do czynienia z coraz większym zainteresowaniem grup przestępczych wrażliwą infrastrukturą IT szpitali. Problem ten jest coraz szerzej dyskutowany, zwłaszcza po głośnym ataku na Lotnicze Pogotowie Ratunkowe, w którym sparaliżowano komunikację, stronę WWW, skrzynki mailowe i zażądano okupu. Hakerzy potrafią zmusić placówki medyczne do płacenia okupów, grożąc włamaniami do baz danych, wyłączeniem systemów czy infekcjami złośliwym oprogramowaniem. Mogą oni zaszyfrować np. dane o stanie zdrowia chorych, przez co lekarze nie będą mieli wglądu w historię leczenia, diagnostykę itd. Z tego powodu niektóre placówki na świecie decydowały się na zapłacenie wysokich okupów.

O wiele tańszym, a przede wszystkim skutecznym, rozwiązaniem jest inwestycja we właściwe zabezpieczenia przed atakami i złośliwym oprogramowaniem. Bezpieczeństwo cybernetyczne jest bowiem warunkiem koniecznym, aby placówki medyczne mogły swobodnie korzystać ze wszystkich innowacji IT i świadczyć usługi swoim pacjentom. Jest to do tego stopnia palący problem, że zajmują się nim nie tylko pojedyncze państwa, ale także organizacje międzynarodowe. Unia Europejska już w 2016 roku wprowadziła regulacje, aby stworzyć odpowiedni parasol ochronny dla państw członkowskich. Wprowadzono wówczas w życie tzw. Dyrektywę NIS – *Network and Information Systems Directive*. Obecnie gotowa jest już kolejna dyrektywa – NIS 2, która zobowiązuje jeszcze więcej instytucji, w tym także sektor zdrowia, do podejmowania środków technicznych i organizacyjnych w celu zarządzania zagrożeniami dla bezpieczeństwa sieci i systemów informatycznych.

Współczesne podmioty lecznicze oraz firmy branży medycznej muszą zatem zmierzyć się z wyzwaniami cy-

bersecurity, aby bezpiecznie poruszać się w świecie najnowszych, cyfrowych technologii. Muszą także być przygotowane na wiele trudnych do przewidzenia i dynamicznie następujących kryzysów. Pandemia koronawirusa, czy obecnie wojna w Ukrainie, to dramatyczne dowody na to, jak wiele i jak szybko może się zmienić w otaczającej nas rzeczywistości.

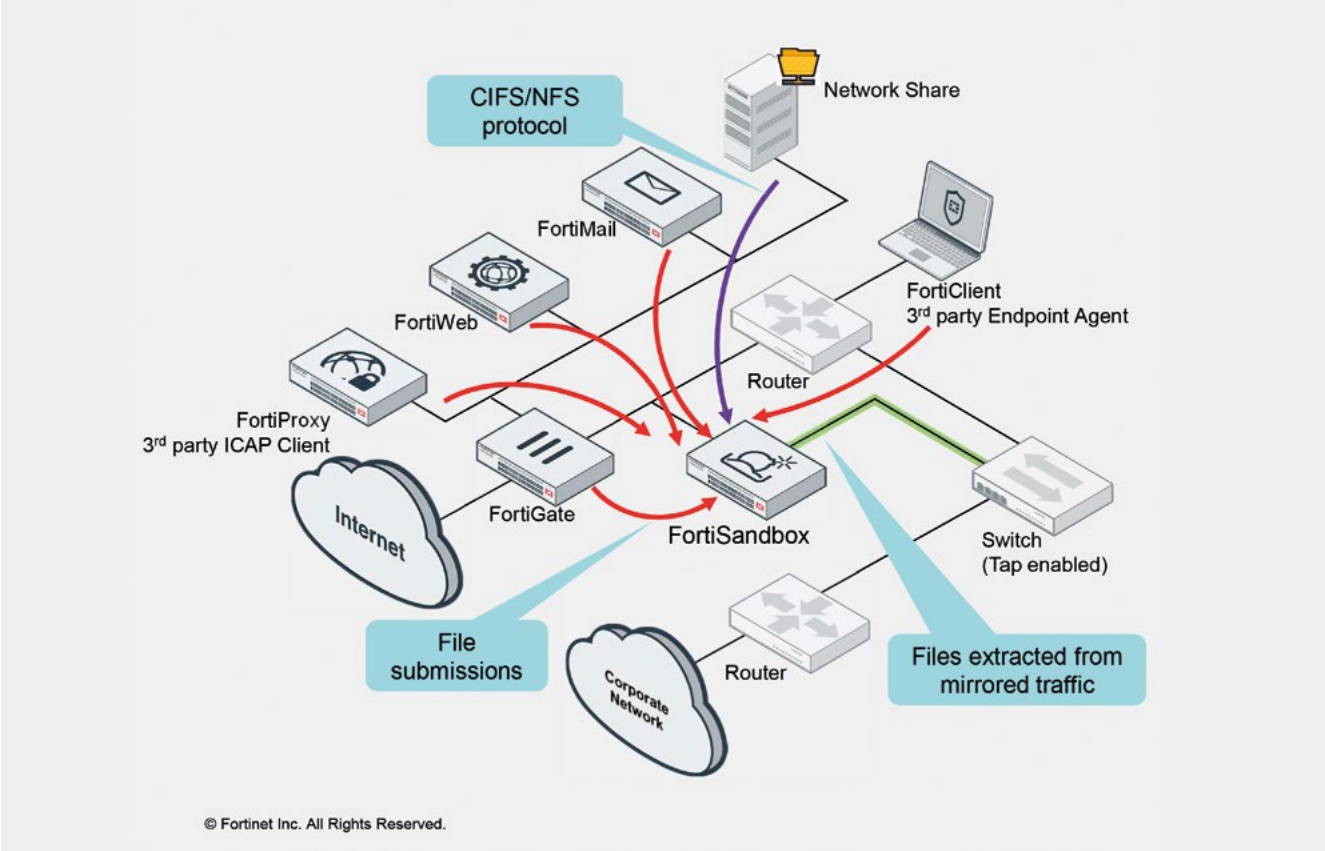
Odpowiedzią na takie potrzeby są produkty proponowane przez firmę Fortinet, światowego lidera z zakresu cyberbezpieczeństwa, która oferuje szerokie i kompleksowe spektrum elastycznych, wydajnych oraz skalowalnych rozwiązań zapewniających najwyższy poziom bezpieczeństwa w sieci, serwerów, poczty elektronicznej oraz monitoringu infrastruktury IT. Można je posegregować w następujących kategoriach:

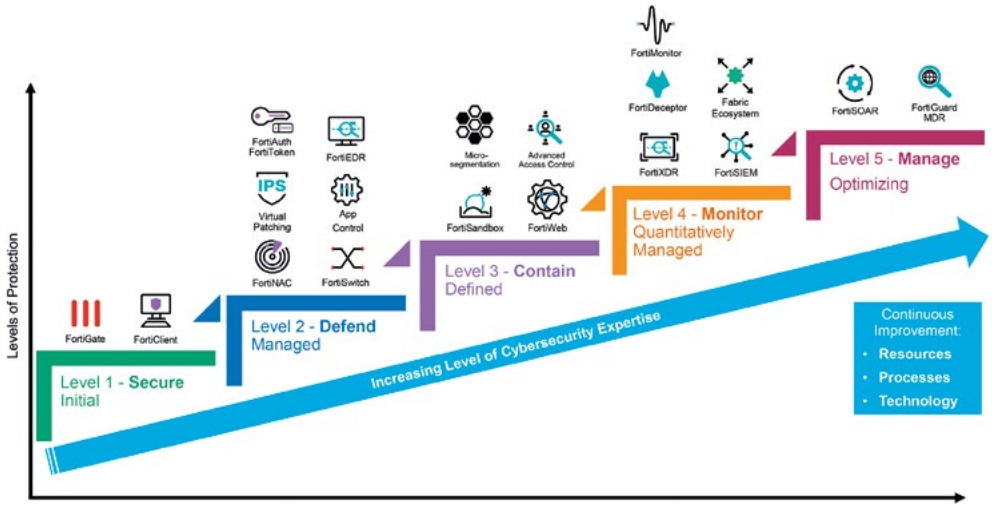
- ochrona poczty elektronicznej,
- ochrona brzegu sieci,
- ochrona infrastruktury IT,
- centralny system informacji i zdarzeń – SIEM.

Systemy ochrony poczty elektronicznej można realizować poprzez urządzenia fizyczne instalowane w infrastrukturze firmowej, w postaci maszyn wirtualnych w środowisku firmowym lub jako instancje w chmurach publicznych. Jest to o tyle przydatne, gdyż często poczta elektroniczna jest hostowana na zewnątrz. Niektórzy producenci posiadają w swojej ofercie integrację na poziomie chmury swoich rozwiązań ochrony poczty. Takim przykładem może być system FortiMail, opracowany przez ekspertów firmy Fortinet.

Kolejną kategorią rozwiązań z zakresu cyberbezpieczeństwa jest ochrona brzegu sieci. To podstawowy element każdej sieci firmowej niezależnie, czy jest to mała placówka, czy duża sieć szpitali. Wynika to z faktu, że duża część osób pracuje poza stacjonarnym miejscem pracy i potrzebuje dostępu do zasobów organizacji. Znaczne rozszerzenie brzegu infrastruktury sieciowej oznacza zwiększenie liczby wrażliwych punktów, czyli potencjalnych celów ataku. Dlatego też jednym z ważniejszych elementów infrastruktury informatycznej powinien być firewall, filtrujący cały ruch wchodzący i wychodzący. Blokuje on połączenia, które mogą stanowić potencjalne zagrożenie, zapewnia zarówno ochronę sieci lokalnej przed nieautoryzowanym dostępem z zewnątrz, jak i ochronę przed niepożądanym udostępnianiem danych z komputerów lokalnych do sieci zewnętrznej.

Dzisiejsze firewalle to urządzenia, które łączą w sobie różne funkcje – potrafią skanować ruch pod kątem zagrożeń takich, jak wirusy czy malware, analizować połączenia, rozpoznać oraz kategoryzować rodzaj aplikacji i zezwalać tylko na te zaufane dla organizacji. Dzięki firewallom można posegmentować sieć wewnętrzną i stwo-





rzyć politykę dostępu między sieciami wewnątrz firmy, np. odseparować komputery używane w administracji, które łączą się z systemami ERP, od komputerów medycznych, które powinny mieć dostęp głównie do systemów typu HIS. Tego typu zabezpieczenia gwarantują firewalle najnowszej generacji Fortigate NGFW, dostarczane przez Fortinet.

Drugim elementem ochrony brzegu sieci, którego znaczenie cały czas rośnie, jest firewall aplikacyjny czyli WAF (Web Application Firewall). Są to systemy, które potrafią analizować ruch pod kątem zagrożeń, występujących w warstwie aplikacji, analizować ruch do i z aplikacji, z których na co dzień korzysta wielu użytkowników. To dzięki firewallom aplikacyjnym można zabezpieczyć m.in. systemy medyczne, które są udostępnione dla użytkowników zewnętrznych (e-rejestracja czy wgląd do wyników badań). Takie zadanie spełnia system FortiWEB, opracowany przez Fortinet.

Kolejną kategorią są systemy typu EDR (EndPoint Detection & Response). Poza systemem antywirusowym są one niezwykle ważnym elementem ochrony stacji roboczych. Tradycyjne systemy antywirusowe analizują operacje wykonywane na komputerach np. otwieranie pliku. EDR jest natomiast rozszerzeniem tej ochrony przez analizę anomalii w działaniach, wykonywanych przez użytkowników na komputerze lub innym urządzeniu. W tym obszarze firma Fortinet także dostarcza skuteczne rozwiązanie w postaci systemu FortiEDR, który może m.in. blokować wszystkie działania, uznane za odstępstwa od standardowych czynności.

Systemem, który również wpisuje się w pojęcie ochrony stacji roboczych, jest system NAC (Network Access Control), który bada klientów sieci podczas podłączenia oraz w trakcie połączenia. Potrafi monitorować stan zabezpieczeń i, na podstawie zdefiniowanej polityki, podjąć akcję np. w przypadku wykrycia nieaktualnego oprogramowania i przenieść klienta do kwarantanny, celem aktualizacji systemu. Dzięki takim rozwiązaniom można rozszerzyć sieć firmową z wydzielonym dostępem dla gości. Systemy NAC występują przeważnie w formie maszyn wirtualnych – takie rozwiązanie zastosował, wymieniony już wielokrotnie, Fortinet, który opracował swój własny system NAC o nazwie FortiNAC.

Ostatnią spośród wymienionych powyżej kategorii, są rozwiązania SIEM-Security Information and Event Management. Jest to system, który zbiera informacje, przetwarza je i unifikuje do jednakowej postaci, a następnie analizuje według zdefiniowanych reguł. SIEM koreluje zdarzenia z różnych systemów, odfiltrowuje standardowe komunikaty, zostawiając na koniec informację o incydentach. Na tej podstawie administrator otrzymuje szybką informację o anomaliach w infrastrukturze. Skraca to czas na wykrycie incydentu, umożliwiając natychmiastową reakcję. Jednym z najczęściej wybieranych rozwiązań w tej kategorii jest system FortiSIEM, proponowany przez firmę Fortinet. Jest on przeznaczony dla działów bezpieczeństwa (tzw. SOC), zajmujących się analizowaniem ruchu sieciowego w celu wykrycia incydentów czy zagrożeń.

Cała rodzina narzędzi proponowanych przez Fortinet to kompleksowe rozwiązanie problemów cyberbezpieczeństwa. Inwestycja w te systemy zapewnia niezakłócony rozwój i tworzy bezpieczne środowisko dla funkcjonowania poszczególnych elementów całego systemu, zarówno w skali jednej, jak i wielu rozproszonych placówek.

Przemysław Zatarski

inżynier systemów informatycznych w KOMA NORD,
absolwent Politechniki Łódzkiej na wydziale Elektrotechniki, Elektroniki, Informatyki i Automatyki, kieruneki. Administrator sieci informatycznej z 10-letnim doświadczeniem w administrowaniu sieci komputerowych oraz systemów informatycznych w dużym podmiocie leczniczym. Obecnie odpowiedzialny za obsługę i wdrożenia sieci przewodowych i bezprzewodowych oraz systemów zabezpieczeń w tym firewalli.

Tomasz Turek

Jak zbudować odporne środowisko backupu?

W przypadku ataku na infrastrukturę, mającego na celu uszkodzenie danych, backup staje się narzędziem pozwalającym na najszybsze i najpewniejsze odzyskanie do punktu w czasie, gdzie infekcja nie miała miejsca. Należy jednocześnie zauważyć, że potrzeba sięgnięcia do kopii zapasowych zwyczajowo oznacza, że systemy analizy poczty (jako najczęstszego wektora ataku), antywirusy, systemy uwierzytelniania, dostępu czy segmentacji sieciowej zawiodły.

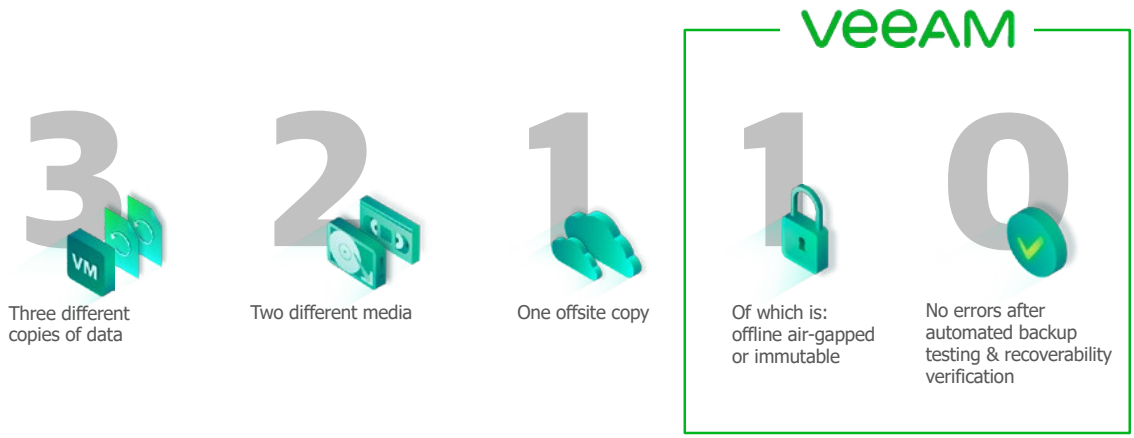
Wykorzystanie backupu neguje cel postawiony przed ransomware, jakim jest uzyskanie od ofiary ataku okupu, stąd coraz częściej zauważa się ataki, mające na celu wyselekcjonowanie systemu backupowego oraz uszkodzenie kopii zapasowych, jako jeden z pierwszych elementów ataku. Z tego względu w czasie projektowania infrastruktury należy wykorzystać dobre praktyki, zarówno z obszaru architektury, jak i użycia funkcjonalności, minimalizujących ryzyko utracenia backupu.

Zasada 3-2-1-1-0

Prawdopodobnie najprostszym i jednocześnie najbardziej skutecznym sposobem na eliminację zagrożenia, wynikającego z niemal dowolnej awarii czy dowolnego typu ataku, jest zastosowanie zasady 3-2-1 – a w jej rozszerzonej wersji 3-2-1-1-0. Polega ona na:

3 – przechowywaniu trzech egzemplarzy danych: egzemplarz pierwszy to dane produkcyjne, a pozostałe dwa to kopie zapasowe, archiwalne czy też repliki danych. Produkcyjne dane oczywiście będą podstawowym źródłem odczytu, ale w przypadku ich niedostępności, uszkodzenia czy utraty, uzyskuje się możliwość odczytu z kopii zapasowej. Aby wyeliminować potencjalny problem uszkodzenia jednej z kopii, rekomenduje się posiadanie minimum dwóch egzemplarzy, szczególnie, że w przypadku awarii całego datacenter, podstawowa kopia zapasowa najczęściej zostaje utracona razem z danymi produkcyjnymi.

2 – dwa różne media przechowywania. Należałoby przede wszystkim zaznaczyć, że dane produkcyjne i kopia zapasowa nie powinny być przechowywane w ramach tej samej macierzy. Awaria sprzętowa czy inne



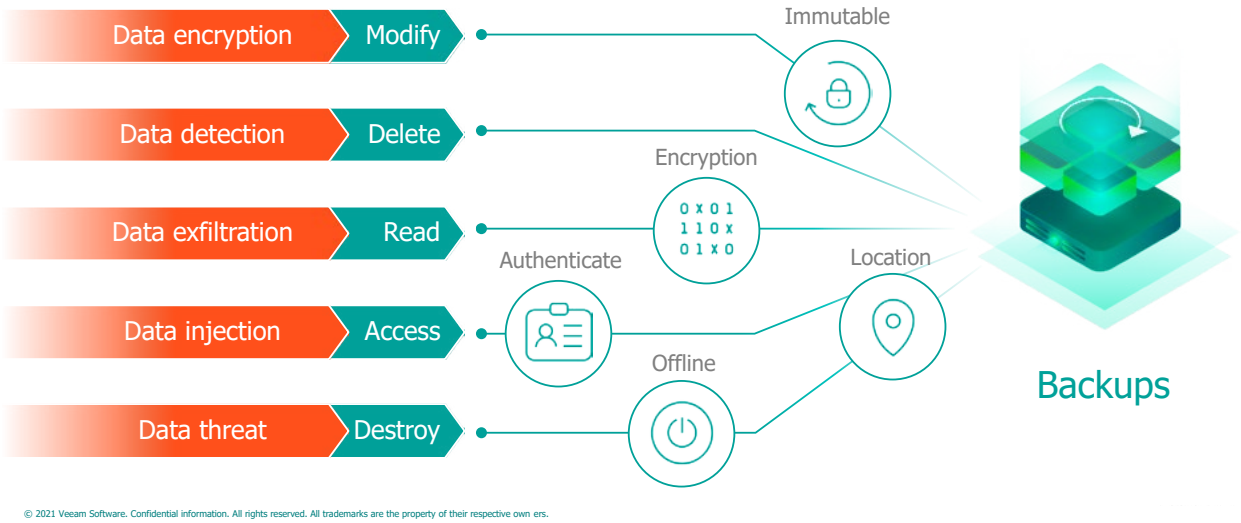
uszkodzenie macierzy, powoduje utratę zarówno danych produkcyjnych, jak i backupowych. Ale należy również rozpatrzyć architekturę repozytoriów w celu utrudnienia ransomware rozprzestrzeniania się po infrastrukturze. Przechowując dane na podstawowym repozytorium opartym o Windows, repozytorium dodatkowe można oprzeć np. o Linux. Jeśli zapisujemy dane na deduplikatory sprzętowe jak np. HPE StoreOnce, zamiast wykorzystywać NFS lub CIFS, będące rozpoznanymi już protokołami, należałoby wykorzystać własny protokół HPE jakim jest Catalyst. Jeśli istnieje możliwość zastosowania macierzy obiektowych – jest to kolejny element utrudniający pracę ransomware, ponieważ nie posiadają one znanego nam systemu plików, jak najczęściej spotykane przy backupie macierze blokowe. Dodatkowo macierze obiektowe wykorzystują kolejny protokół, jakim jest S3, a do uwierzytelniania nie jest wykorzystywany standardowy tandem domena\użytkownik. Wykorzystując kopiowanie między repozytoriami wbudowane w Veeam, również używane są natywne protokoły Veeam i przy poprawnej konfiguracji serwerów, gdzie jest to jedyny dopuszczony rodzaj ruchu, również wymaga znajomości protokołu po stronie ransomware, w celu przedostania się na repozytorium dodatkowe. Mieszając systemy operacyjne, protokoły, macierze plikowe/blokowe/obiektowe wymagamy, aby ransomware rozumiał i potrafił się rozprzestrzenić na znacznie szerszym wachlarzu systemów, wymuszając jego większe skomplikowanie.

1 – jedna kopia powinna być przechowywana offsite. Pozostaje indywidualną decyzją administratorów co stanowi wystarczający offsite. Należy założyć, że musi być to środowisko, na które nie będą miały wpływu te same czynniki, co na infrastrukturę produkcyjną.

1 – jest to rozszerzenie podstawowej zasady 3-2-1. Jedna z kopii powinna być niemodyfikowalna, nieusuwalna – tzw. immutable. Niezmienność kopii ma za zadanie uniemożliwić zaszyfrowanie danych przez ransomware lub ich uszkodzenie, czy usunięcie przez inny typ malware. Najczęściej stosowanym sposobem na osiągniecie niezmienności, jest wysłanie backupu na nośniki taśmowe, przechowywane później w zewnętrznej lokalizacji. Jednocześnie należy pamiętać, że taśma jest urządzeniem sekwencyjnym i nie pozwala w prosty sposób na granularne odzyskiwanie danych, które może być niezbędne w przypadku awarii. Warto rozpatrzyć możliwość przechowywania danych w chmurze, gdzie jedną z funkcjonalności protokołu S3 jest Object Lock, dający możliwość ustanowienia czasu ochrony danych przed modyfikacją oraz usunięciem. Można więc zdefiniować politykę, gdzie ostatni miesiąc będzie podlegał ochronie, przez co nawet w przypadku udanego ataku na infrastrukturę, ostatni miesiąc kopii zapasowych nadal pozwoli na dowolne odzyskanie danych. Dodatkowo chmura i wykorzystanie protokołu S3 daje zalety przechowywania danych na przestrzeni obiektowej, o czym wspomniano już wcześniej. Veeam dodatkowo wprowadza możliwość użycia flagi immutable na repozytoriach, opartych o systemy Linux, co znacznie ułatwia wdrożenie funkcjonalności w istniejących infrastrukturach. W czasie definiowania repozytorium, jednorazowo wykorzystuje się konto root, w celu ustanowienia flagi immutable, a następnie usługi Veeam działają, wykorzystując użytkownika o niższym poziomie uprawnień na potrzeby wykonywania backupu. Użytkownik taki nie ma możliwości zdjęcia lub skrócenia czasu ochrony danych, więc w przypadku, gdyby system backupu był wektorem ataku, przejęte konto administratora takiego systemu nadal nie pozwala na usunięcie kopii zapasowych.

0 – czyli zero błędów przy odtwarzaniu. Kolejny element rozszerzający formułę 3-2-1, nakładający na administratora obowiązek cyklicznej weryfikacji odzyskiwalności kopii zapasowych. Nierzadko ransomware po infekcji systemu pozostaje nieaktywny, w celu rozprzestrzenienia się po jak największej liczbie serwerów. W tym czasie wykonywane są normalne polityki backupowe, więc zainfekowane maszyny zostają zabezpieczone i często również zarchiwizowane. W skrajnych przypadkach może dojść do uszkodzenia plików lub ich zaszyfrowania, które nie będzie widoczne dla administratora, do czasu ponownego uruchomienia takiego serwera. Manualne testy pozwalają zweryfikować, czy maszyna zostanie poprawnie zainicjalizowana, czy nie wystąpią błędy związane z uszkodzeniem plików i czy aplikacje działają poprawnie. Zwyczajowo tego typu testy wykonywane są na dedykowanej infrastrukturze, aby możliwe było odtworzenie topologii aplikacji oraz w celu uzyskania separacji od środowiska produkcyjnego. Jednocześnie, przy znacznym wolumenie maszyn w środowisku, tego typu manualne testy nie są możliwe do zrealizowania ze względu na wymagany nakład czasowy administratora. Z tego powodu Veeam wprowadził funkcjonalność SureBackup, która umożliwia zautomatyzowanie tego typu testów.

Wykorzystując komponent wirtualnego laboratorium, Veeam pozwala na automatyczne utworzenie wyizolowanej strefy sieciowej na istniejącej infrastrukturze, co eliminuje potrzebę dedykowania serwerów pod środowisko testowe. W ramach wyizolowanej strefy istnieje możliwość zdefiniowania wielu sieci, aby odtworzyć topologię sieciową, pozwalając na weryfikację działania na-



wet rozproszonych aplikacji, a nie jedynie pojedynczych serwerów. W ramach procedury testowej wykorzystywana jest funkcjonalność Instant VM Recovery, pozwalająca na uruchomienie maszyny wirtualnej bezpośrednio ze zdeduplikowanej i skompresowanej kopii zapasowej. Następnie zostają podmienione adaptery sieciowe takich maszyn, aby zapewnić izolację sieciową. W następnym kroku maszyny zostają uruchomione na wirtualizatorze, weryfikuje się heartbeat VM, weryfikuje się, czy maszyna odpowiada na ping dla swojego IP oraz wykonywane są testy aplikacyjne – zarówno te wbudowane w oprogramowanie, jak i dowolne skrypty, zdefiniowane przez administratora. Po zakończeniu testów środowisko zostaje automatycznie wygaszone, aby nie konsumować zasobów hosta wirtualizacyjnego.

Dodatkowo, jako rozwinięcie testów, udostępniona została funkcjonalność weryfikacji zawartości backupu poprzez wykonanie skanu antywirusowego. Secure Restore wykorzystuje istniejącego w infrastrukturze klienta oprogramowania antywirusowego w celu przeskanowania zawartości kopii zapasowej, z wykorzystaniem najnowszych sygnatur. Jak zostało wcześniej wspomniane, kiedy ransomware przedostanie się do infrastruktury i zainfekuje maszynę, zanim zostanie on uaktywniony lub wykryty, jest on zabezpieczany razem z maszyną produkcyjną.

W momencie uzyskania świadomości danego zagrożenia przez dostawcę antywirusa, udostępniona zostaje sygnatura, pozwalająca wykryć zagrożenie. W przypadku wystąpienia awarii lub po ataku szyfrującym infrastrukturę produkcyjną, jeśli nowsze sygnatury są dostępne, istnieje możliwość ponownej weryfikacji, czy backup może i powinien zostać odzyskany, czy jest on zainfekowany i należy albo odzyskać go do wyizolowanej strefy i tam ręcznie usunąć złośliwy kod, czy należy cofnąć się do wcześniejszego punktu przywracania. Tego typu wiedza pomaga w upewnieniu się, że odzyskiwana maszyna nie doprowadzi do ponownej infekcji środowiska produkcyjnego.

Jak łatwo zauważyć, już samo przestrzeganie zasady 3-2-1-1-0 pomaga w zabezpieczeniu infrastruktury backupu, poprzez ustanowienie separacji między środowiskami oraz redundancji w posiadanych kopiach zapasowych, przy jednoczesnym eliminowaniu zagrożeń, wynikających z możliwości przypadkowego czy intencjonalnego uszkodzenia danych. Dodając do tego funkcjonalności, oferowane przez nowoczesne rozwiązania backupowe takie jak automatyczne testy odzyskiwania, umiejętność wykorzystania chmury, czy przestrzeni obiektowych, integracja z wieloma protokołami przesyłu danych, wsparcie dla flag immutable czy możliwość wykorzystania oprogramowania antywirusowego w czasie odzyskiwania po awarii – otrzymujemy bezpieczny backup, którego możemy być pewni, gdy przyjdzie potrzeba odzyskania danych po ataku.

O Veeam Software

Veeam® jest liderem w obszarze rozwiązań do tworzenia i odzyskiwania kopii zapasowych oraz zarządzania danymi, które zapewniają nowoczesną ochronę danych. Firma udostępnia kompleksową platformę przeznaczoną do środowisk chmurowych, wirtualnych, fizycznych, SaaS i Kubernetes.

Klienci Veeam mają pewność, że ich aplikacje i dane są chronione przed oprogramowaniem ransomware, zagrożeniami oraz złośliwymi manipulacjami, a przy tym zawsze dostępne w najprostszej, niezawodnej, wydajnej i najbardziej elastycznej platformie w branży.

Veeam chroni ponad 400 000 klientów na całym świecie, w tym 81% z listy Fortune 500 i 70% z rankingu Global 2000. Globalny ekosystem Veeam obejmuje ponad 35 000 partnerów technologicznych i handlowych oraz usługodawców i członków sojuszy partnerskich, a lokalne oddziały znajdują się w ponad 30 krajach.

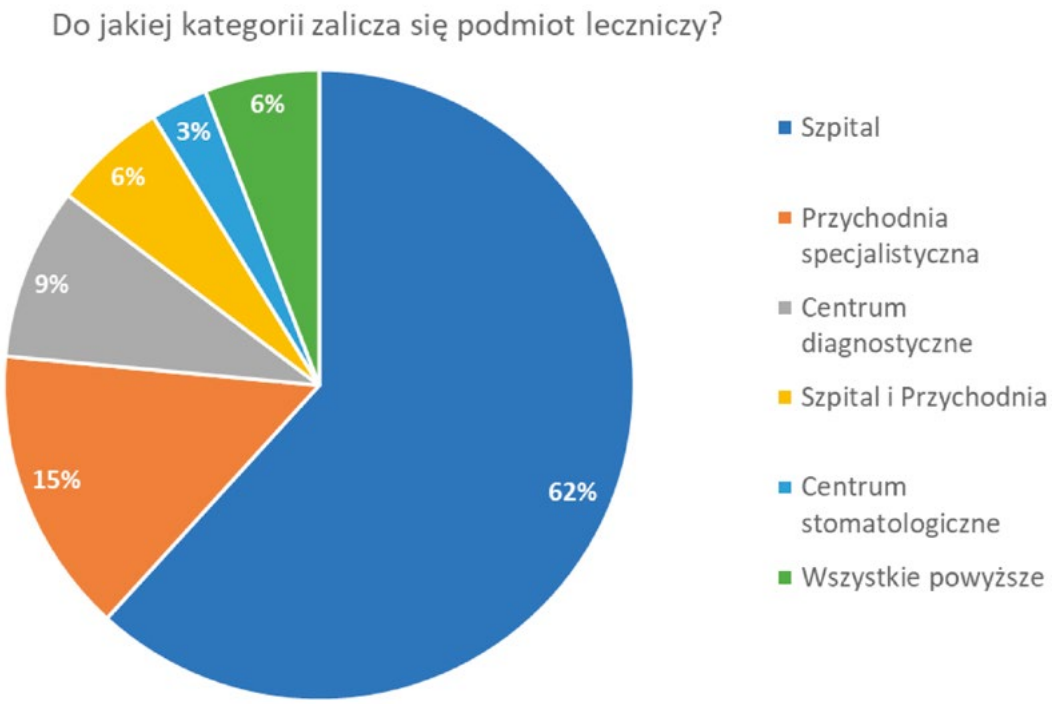
Tomasz Turek

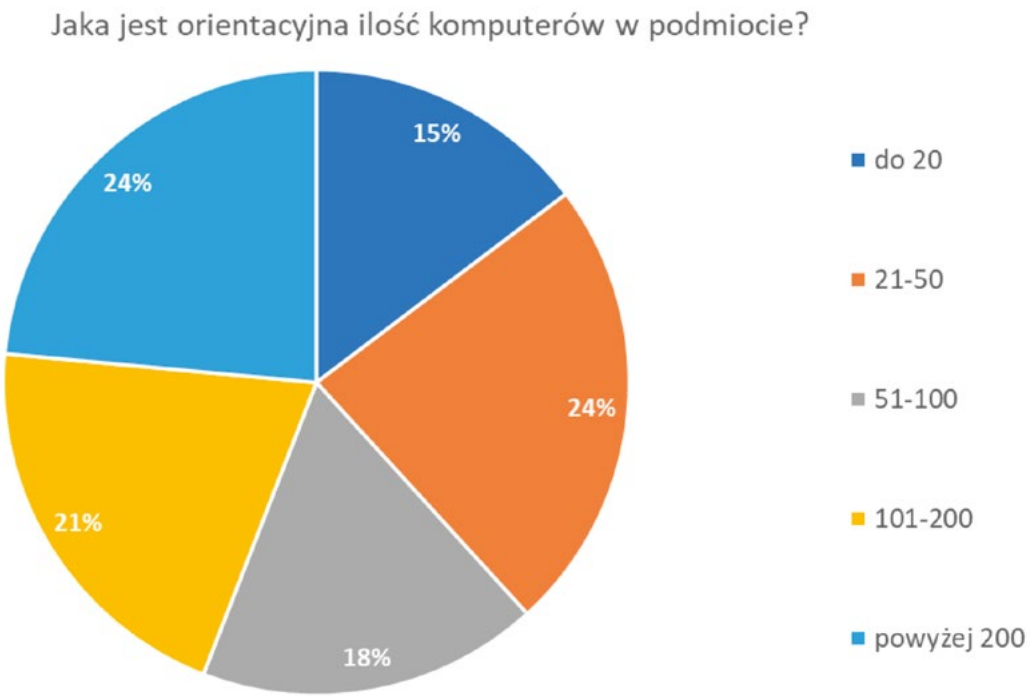
Senior Systems Engineer w Veeam, architekt rozwiązań z zakresu zabezpieczania, zarządzania oraz planowania disaster recovery w infrastrukturach fizycznych i wirtualnych, opartych o platformy VMware i Microsoft, jak również w środowiskach chmurowych. Odpowiada m. in. za techniczne wsparcie największych projektów, doradztwo z zakresu najlepszych praktyk zabezpieczania maszyn fizycznych i zwirtualizowanych, projektowanie architektury środowisk backupowych oraz planowania polityki odzyskiwania danych.

Image by rawpixel.com on Freepik

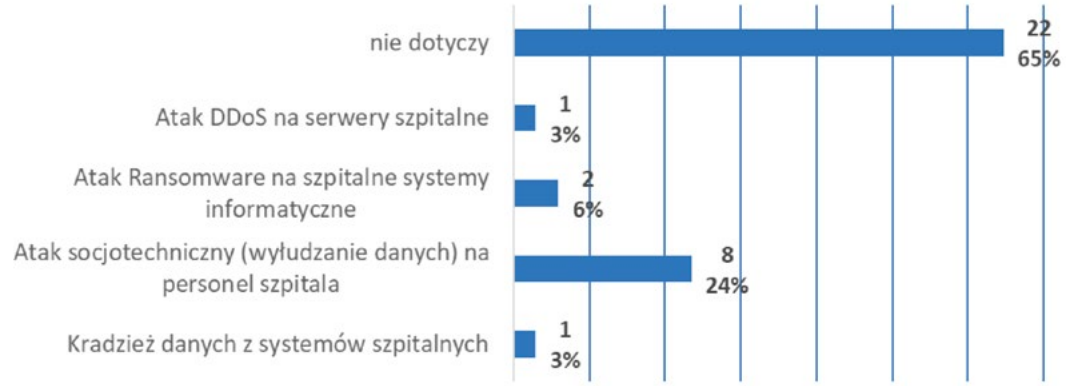
Anonimowa ankieta, dotycząca cyberbezpieczeństwa w szpitalach, przeprowadzona została w styczniu 2023 r. przez Ogólnopolskie Stowarzyszenie Szpitali Prywatnych, Pracodawców Medycyny Prywatnej oraz firmę Koma Nord – wśród członków stowarzyszeń.

Wyniki (34 ankietowanych):

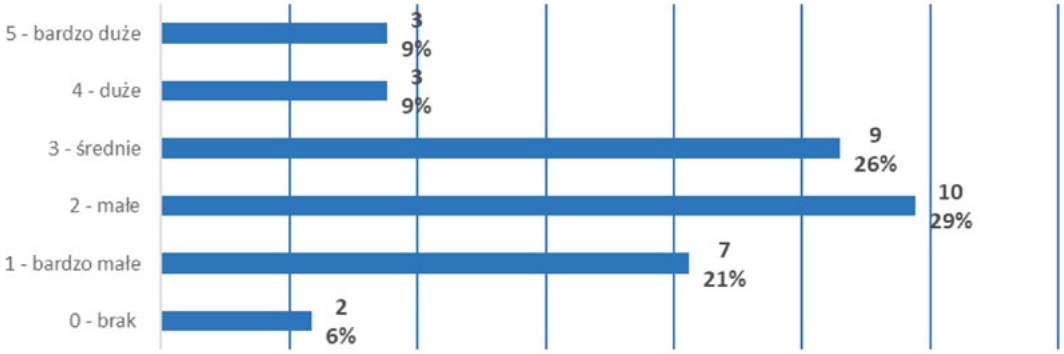




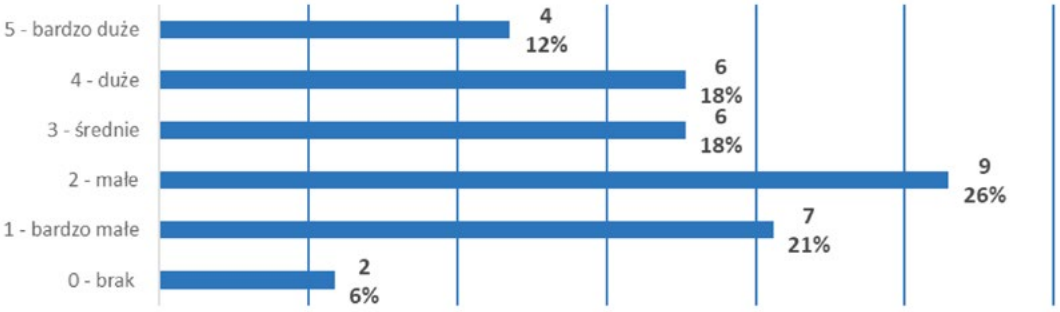
Czy podmiot doświadczył kiedykolwiek jednego z niżej wymienionych typów ataku:



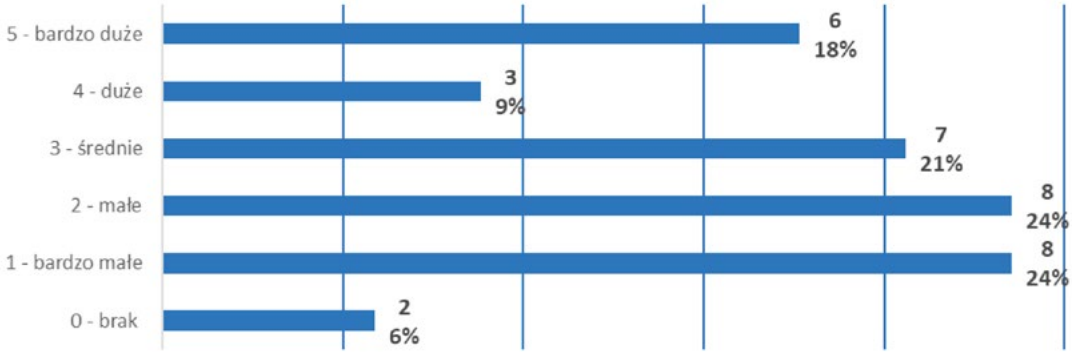
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii:
a) Kradzież danych z systemów szpitalnych



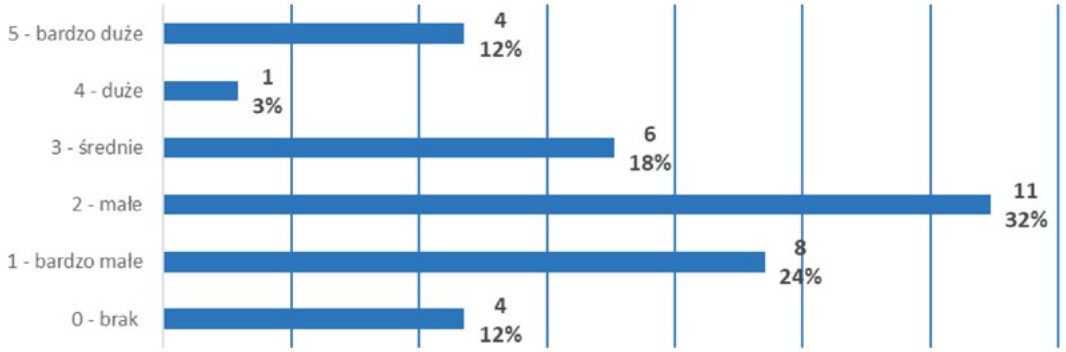
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii:
b) Atak socjotechniczny (wyłudzanie danych) na personel szpitala



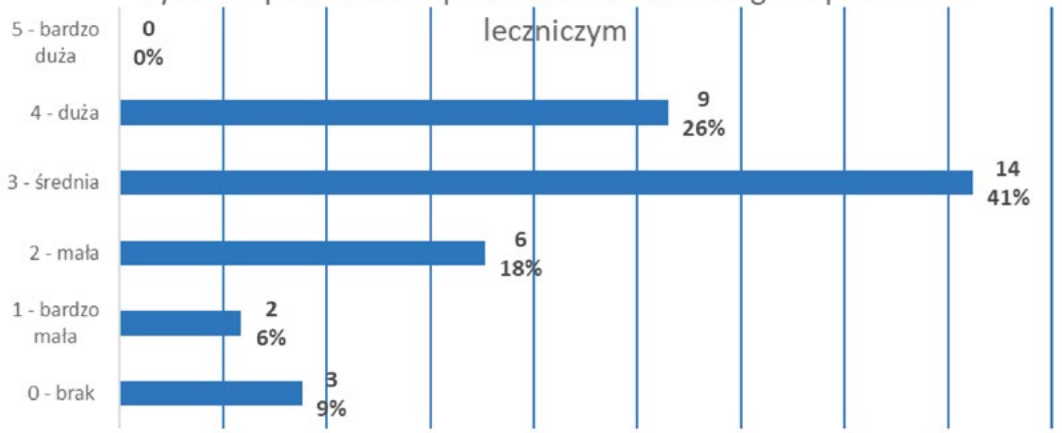
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii:
c) Atak Ransomware na szpitalne systemy informatyczne

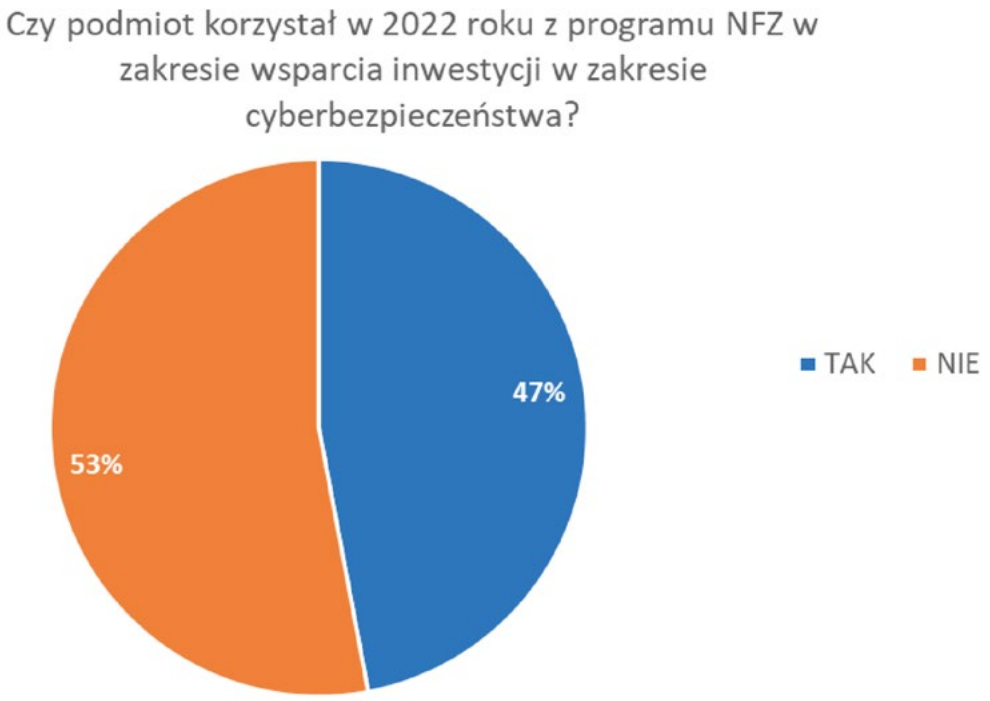


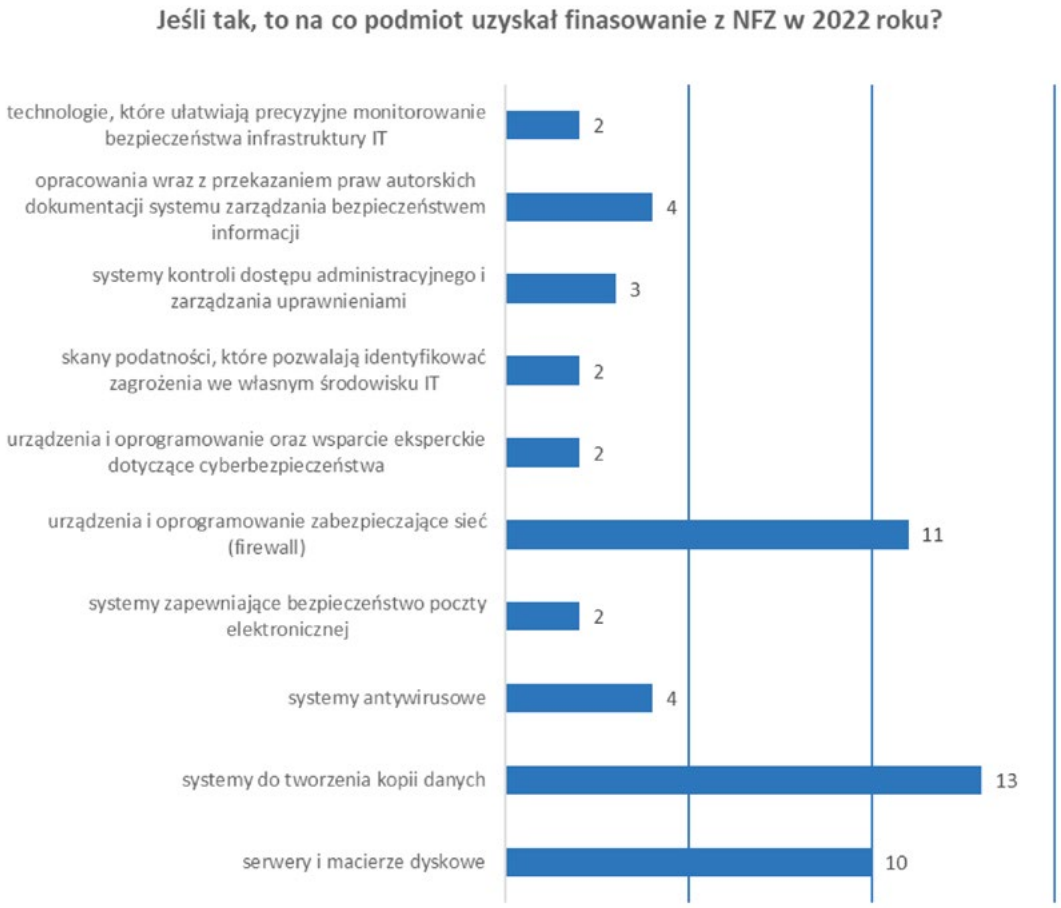
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii:
d) Atak DDoS na serwery szpitalne

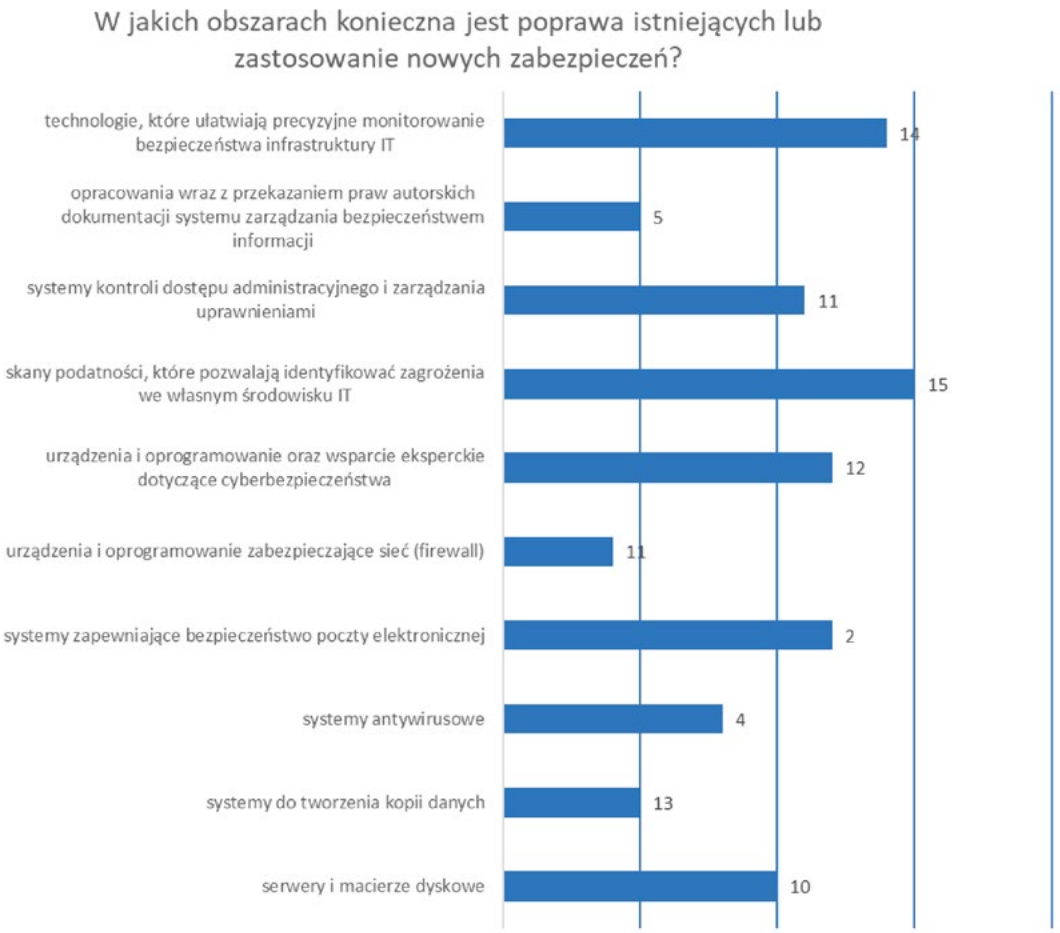


Proszę o ogólną ocenę świadomości w zakresie cyberbezpieczeństwa personelu zatrudnionego w podmiocie leczniczym




Czy podmiot korzystał w 2022 roku z programu NFZ w zakresie wsparcia inwestycji w zakresie cyberbezpieczeństwa?
47%
53%
TAK
NIE


Jeśli tak, to na co podmiot uzyskał finasowanie z NFZ w 2022 roku?
technologie, które ułatwiają precyzyjne monitorowanie bezpieczeństwa infrastruktury IT
2
opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji
4
systemy kontroli dostępu administracyjnego i zarządzania uprawnieniami
3
skany podatności, które pozwalają identyfikować zagrożenia we własnym środowisku IT
2
urządzenia i oprogramowanie oraz wsparcie eksperckie dotyczące cyberbezpieczeństwa
2
urządzenia i oprogramowanie zabezpieczające sieć (firewall)
11
systemy zapewniające bezpieczeństwo poczty elektronicznej
2
systemy antywirusowe
4
systemy do tworzenia kopii danych
13
serwery i macierze dyskowe
10


W jakich obszarach konieczna jest poprawa istniejących lub zastosowanie nowych zabezpieczeń?
technologie, które ułatwiają precyzyjne monitorowanie bezpieczeństwa infrastruktury IT
14
opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji
5
systemy kontroli dostępu administracyjnego i zarządzania uprawnieniami
11
skany podatności, które pozwalają identyfikować zagrożenia we własnym środowisku IT
15
urządzenia i oprogramowanie oraz wsparcie eksperckie dotyczące cyberbezpieczeństwa
12
urządzenia i oprogramowanie zabezpieczające sieć (firewall)
11
systemy zapewniające bezpieczeństwo poczty elektronicznej
2
systemy antywirusowe
4
systemy do tworzenia kopii danych
13
serwery i macierze dyskowe
10


Jaki wkład własny podmiot jest gotowy przeznaczyć na wzmocnienie cyberbezpieczeństwa przy założeniu dofinasowania 50%?
800 000 zł
13%
400 000 zł
10%
200 000 zł
6%
100 000 zł
23%
50 000 zł
48%