NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.411.5.2.2023

Ireneusz Weryk – Dyrektor
Samodzielny Publiczny Zakład Opieki Zdrowotnej
w Działdowie
ul. Leśna 1, 13-200 Działdowo

WYSTĄPIENIE POKONTROLNE

I/23/003 Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Działdowie, ul. Leśna 1, 13-200 Działdowo (dalej: Szpital, SP ZOZ).

Kierownik jednostki kontrolowanej

Ireneusz Weryk, Dyrektor od dnia 1 września 2019 r.

Zakres przedmiotowy kontroli

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami.
2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami.

Okres objęty kontrolą

Lata 2020-2023 (I półrocze) z uwzględnieniem okresów wcześniejszych i późniejszych, jeżeli miało to wpływ na realizowane zadania.

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Olsztynie

Kontroler

Edyta Piskorz-Zabujść, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/160/2023 z dnia 30 listopada 2023 r.

(akta kontroli str. 1-6)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Funkcjonujące w Szpitalu rozwiązania w zakresie zapewnienia bezpieczeństwa informacji, w tym danych osobowych i medycznych pacjentów, były realizowane zgodnie z przyjętymi przez Szpital zasadami oraz przepisami prawa, a także w sposób rzetelny.

Szpital uznany w dniu 19 lipca 2022 r. za operatora usługi kluczowej w sektorze ochrony zdrowia (dalej: OUK) wywiązał się z wynikających w tym zakresie obowiązków. Zgodnie bowiem z wymogami art. 16 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[3] m.in. dokonano szacowania ryzyka dla swoich usług kluczowych, zarządzano incydentami, wyznaczono osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, prowadzono działania edukacyjne wobec użytkowników, wdrożono odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne, zbierano informacje o zagrożeniach i podatnościach, wdrożono wymaganą dokumentację oraz przeprowadzono audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Wyznaczono również Inspektora Ochrony Danych Osobowych (dalej: IODO), a powierzone mu zadania były zgodne z wymogami art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[4].

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.
[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dz. U. z 2023 r. poz. 913, ze zm. (dalej: UOC).
[4] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1 (dalej: RODO).

W zakresie dotyczącym działań Szpitala związanych z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych osobowych stwierdzono jednak trzy nieprawidłowości. Dotyczyły one:

- nieprzekazania do organu właściwego do spraw cyberbezpieczeństwa, w wymaganym art. 9 ust. 2 UOC terminie, danych osoby wyznaczonej do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
- nieprzypisania formalnie (wg stanu na 22 stycznia 2024 r.) zadań dla Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji oraz Zespołu ds. Bezpieczeństwa Informacji;
- niedostosowania (wg stanu na 11 stycznia 2024 r.) zapisów regulaminu organizacyjnego do faktycznie funkcjonującej w badanym okresie struktury organizacyjnej.

Nieprawidłowości te nie miały jednak wpływu na funkcjonowanie przyjętych w Szpitalu rozwiązań w zakresie przestrzegania zasad bezpieczeństwa informacji oraz ochrony danych pacjentów przed cyberatakami.

Zapewnienie bezpieczeństwa informacji oraz przetwarzanie danych pacjentów było realizowane zgodnie z postanowieniami funkcjonującej w Szpitalu dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (dalej: SZBI). W prawidłowy sposób pracownikom Szpitala nadawano i odbierano uprawnienia do przetwarzania danych osobowych pacjentów, stosowano sprzętowe oraz programowe środki służące ochronie przetwarzanych informacji oraz zarządzano incydentami zagrażającymi bezpieczeństwu systemu informacyjnego Szpitala.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami

Opis stanu faktycznego

1.1. Decyzją Ministra Zdrowia z dnia 19 lipca 2022 r.[6] Szpital został uznany za Operatora Usługi Kluczowej w sektorze ochrony zdrowia, polegającej na:

- udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy,
- obrocie i dystrybucji produktów leczniczych.

W związku z powyższym, zgodnie z wymogami wynikającymi z art. 16 UOC, w Szpitalu w okresie:

a) trzech miesięcy od dnia doręczenia ww. decyzji[7] m.in:
   - opracowano analizę ryzyka, w której w szczególności określono poziom zagrożeń oraz wyliczono podatności na ryzyko utraty poufności, integralności oraz dostępności;
   - w ramach ww. analizy ryzyka systematycznie szacowano ryzyko wystąpienia incydentu;
   - prowadzono rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa;
   - wyznaczono osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

[5] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[6] Decyzja nr DIWP.550.95.2022.MS z dnia 19 lipca 2022 r.
[7] Decyzję Szpital otrzymał w dniu 20 lipca 2022 r.

- organizowano szkolenia dla personelu Szpitala umożliwiające lepsze zrozumienie zagrożeń cyberbezpieczeństwa;
- publikowano na stronie Szpitala informacje dla pacjentów dotyczących cyberbezpieczeństwa;

Pomimo wykonania obowiązku wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, nie zrealizowano jednak wymogu określonego w art. 9 ust. 2 UOC dotyczącego przekazania danych tej osoby w wymaganym terminie do organu właściwego do spraw cyberbezpieczeństwa, tj. do CSIRT NASK. Zgłoszenie to nastąpiło dopiero w dniu 10 stycznia 2023 r. (szerszy opis znajduje się w sekcji dotyczącej stwierdzonych nieprawidłowości).

Pomimo powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo w Szpitalu, nie dostosowano zapisów Regulaminu Organizacyjnego Szpitala[8] do tych zmian (szerszy opis znajduje się w sekcji dotyczącej stwierdzonych nieprawidłowości).

b) sześciu miesięcy od dnia doręczenia ww. decyzji m.in.:
   - zakupiono i oddano do użytkowania przez pracowników Szpitala komputery z systemem Windows 11 PRO (w celu wymiany za komputery z niewspieranymi, starszymi wersjami systemu Windows);
   - zakupiono i uruchomiono urządzenia zapory sieciowej Stormshield SN720;
   - zakupiono i wdrożono do funkcjonowania oprogramowanie ESET Protect Enterprise ON-PREM (oprogramowanie antywirusowe dla stacji roboczych i serwerów);
   - zakupiono i uruchomiono macierz przeznaczoną do tworzenia kopii zapasowej;
   - zakupiono i wdrożono SZBI;
   - w celu wykrywania luk bezpieczeństwa w systemach informacyjnych Szpitala, prowadzono odpowiednie testy, a o stwierdzonych lukach informowano bezpośrednio producentów oprogramowania;
   - odseparowano kopie bezpieczeństwa od sieci wewnętrznej (zakupiono urządzenie typu NAS, służące do przechowywania kopii zapasowych w oddzielnej infrastrukturze niż sieć wewnętrzna).
c) roku od dnia doręczenia ww. decyzji przeprowadzono audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej oraz przekazano jego kopię do wymaganego UOC podmiotu, tj. do Ministerstwa Zdrowia.

(akta kontroli str. 7-519)

1.2. Zgodnie z wymogami art. 22 ust. 1 pkt 4 UOC Szpital informował pacjentów o obowiązujących w nim zasadach cyberbezpieczeństwa. Realizował to m.in. poprzez:

- publikacje treści dotyczących ww. zagadnienia na stronie internetowej Szpitala, tj. www.spzoz-dzialdowo.pl, w zakładkach „Dla pacjenta – cyberbezpieczeństwo" oraz „O stronie – cyberbezpieczeństwo";
- zamieszczanie ww. treści na tablicach informacyjnych Szpitala (przy wejściu głównym do budynku Szpitala, na terenie oddziałów, poradni, rejestracji centralnej oraz punktu pobrań laboratoryjnych SP ZOZ oraz budynku administracji);
- opisanie zasad dotyczących cyberbezpieczeństwa w broszurze informacyjnej, w formie ulotek znajdujących się w punkcie informacyjnym Szpitala.

[8] Wprowadzonego zarządzeniem nr 3/2018 Dyrektora SP ZOZ w Działdowie z dnia 1 marca 2018 r. w sprawie Regulaminu Organizacyjnego SP ZOZ w Działdowie, zmienionego zarządzeniem nr 10/2023 z dnia 28 lutego 2023 r.

Wszystkie ww. formy informowania pacjentów o cyberzagrożeniach funkcjonowały nieprzerwanie od 15 września 2022 r.

(akta kontroli str. 520-530)

1.3. W opracowanej za 2021 rok oraz 2022 rok analizie ryzyka dla SP ZOZ, oszacowano poziom ryzyka, określono poziom zagrożeń jego wystąpienia oraz wyliczono podatności na ryzyka utraty poufności, integralności oraz dostępności. W ramach ww. analiz, corocznie szacowano ryzyko wystąpienia incydentu utraty ww. atrybutów. Przy wsparciu Systemu S46[9] m.in. na bieżąco monitorowano możliwość wystąpienia incydentów, możliwych zagrożeń oraz zbierano informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Poprzez ww. system, Szpital miał możliwość zgłoszenia wystąpienia potencjalnych incydentów poważnych do właściwego CSIRT[10].
Zasady zarządzania incydentami, przed wdrożeniem w Szpitalu SZBI, zostały opisane w ustanowionej zarządzeniem Dyrektora z dnia 22 grudnia 2014 r.[11] Polityce Ochrony Danych Osobowych[12]. Dokumentacja ta zawierała m.in. opis zagadnień z zakresu oceny skutków ryzyka[13], planu postępowania z ryzykiem, zabezpieczeń danych osobowych, szkoleń użytkowników oraz instrukcji postępowania z incydentem. Dodatkowo utworzony został rejestr naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych, w którym prowadzone były systematyczne zapisy dotyczące zaistniałych incydentów. Po uznaniu Szpitala przez Ministra Zdrowia za OUK, m.in. ww. zasady zarządzania incydentami zostały szerzej opisane w SZBI, tj. w Polityce Bezpieczeństwa Informacji oraz Polityce Ciągłości Działania. Stwierdzone w ww. rejestrze incydenty dotyczyły przede wszystkim drobnych naruszeń bezpieczeństwa dokonanych przez użytkowników (np. zapisanych haseł w przeglądarce, braku wygaszacza ekranu czy zapisanych haseł na kartce). Zgodnie z ww. rejestrem działania naprawcze podejmowane były natychmiast. Do końca 2023 r. w Szpitalu nie stwierdzono żadnych incydentów poważnych wymagających zgłoszenia do właściwego dla Szpitala CSIRT.

(akta kontroli str. 159-177, 531-591)

1.4. W dniu 13 października 2022 r. opracowano SZBI[14]. Zarządzeniem Dyrektora z dnia 17 października 2022 r.[15] dokumentacja ta została wdrożona do stosowania w Szpitalu. Określone w niej zasady dotyczyły m.in.:

- zarządzania uprawnieniami użytkowników,
- pozostawiania sprzętu bez nadzoru,
- zabezpieczenia przed szkodliwym oprogramowaniem,
- zabezpieczenia sieci,
- przesyłania informacji,
- zabezpieczenia wiadomości w formie elektronicznej,
- zarządzania incydentami związanymi z bezpieczeństwem informacji.

[9] W dniu 19 maja 2023 r. zawarto porozumienie nr 62923 z Ministrem Cyfryzacji w sprawie. podłączenia Szpitala do zintegrowanego systemu zarządzania cyberbezpieczeństwem, natomiast w dniu 30 czerwca 2023 r. podpisano umowę nr 63786 z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym, w sprawie użyczenia sprzętu niezbędnego do działania ww. systemu.

[10] Computer Security Incident Response Team.

[11] Zarządzenie nr 28/2014 Dyrektora SP ZOZ z dnia 22 grudnia 2014 r. w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Przetwarzania Danych Osobowych w SP ZOZ. Aktualizacja dokumentacji została dokonana w dniu 1 września 2018 r.

[12] Szczegółowy opis tych zagadnień znajdował się w załącznikach do Polityki Ochrony Danych Osobowych, tj. w Regulaminie Ochrony Danych Osobowych oraz w Instrukcji Zarządzania RODO.

[13] Analiza ryzyka.

[14] Aktualizację SZBI opracowano w dniu 19 października 2023 r.

[15] Zarządzenie nr 69/2022 Dyrektora SP ZOZ z dnia 17 października 2022 r. w sprawie stosowania Standardów Zarządzania Bezpieczeństwem Informacji na podstawie art. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Ww. dokumentacja była zgodna z normą PN-EN ISO/IEC 27001, tj. m.in. obejmowała ona ustalenia dotyczące:

- charakterystyki usługi kluczowej oraz infrastruktury;
- szacowania ryzyka dla obiektów infrastruktury;
- oceny aktualnego stanu ochrony infrastruktury;
- opisu zabezpieczeń infrastruktury.

Pracownicy Szpitala zostali zapoznani z SZBI. Nastąpiło to poprzez:

- przekazanie ww. zarządzenia w formie papierowej dla kierowników komórek organizacyjnych Szpitala podczas odprawy ordynatorów SP ZOZ[16];
- komunikat dla każdego zalogowanego użytkownika w systemie szpitalnym o wprowadzeniu ww. zarządzenia;
- umieszczenie dokumentacji SZBI na stronie internetowej dostępnej z poziomu sieci wewnętrznej Szpitala w zakładce „dla pracownika".

Zgodnie z dokumentacją SZBI, osobami odpowiedzialnymi za bezpieczeństwo informacji oraz danych osobowych byli:

a) Pełnomocnik ds. SZBI[17] – sprawujący nadzór nad wdrożonym w Szpitalu SZBI oraz nad przestrzeganiem zasad bezpieczeństwa informacji;
b) Inspektor Ochrony Danych Osobowych (dalej: IODO) – sprawujący nadzór nad przestrzeganiem przetwarzania i obowiązujących zasad bezpieczeństwa danych osobowych (powołanie oraz zakres realizowanych zadań IODO opisano w punkcie 1.7. niniejszego wystąpienia pokontrolnego);
c) Administrator Systemów Informatycznych[18] – dbający o bezpieczeństwo i utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania używanego w SP ZOZ;
d) Zespół ds. Bezpieczeństwa Informacji (dalej: Zespół ds. BI)[19].

(akta kontroli str. 352-474, 531-591)

1.5. Zarządzeniem Dyrektora Szpitala z dnia 17 października 2022 r.[20] powołano osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Wyznaczonym do pełnienia tej funkcji został Kierownik Działu IT Szpitala. Jak wskazano w ww. zarządzeniu, osoba ta była odpowiedzialna za realizację zadań określonych w UOC, a przydzielone szczegółowe zadania i obowiązki dotyczyły m.in.:

- prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz współpracy w zarządzaniu tym ryzykiem;
- wdrażania odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy;
- zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
- współpracy w zarządzaniu incydentami;
- stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
- stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa,

[16] Potwierdzenie – listy obecności.
[17] W praktyce funkcję tę pełnił Kierownik ds. IT, pełniący równolegle funkcję Administratora Systemów Informatycznych (dalej: ASI).
[18] Dyrektor z dniem 1 września 2018 r. powołał na to stanowisko Kierownika ds. IT.
[19] W wydaniu drugim SZBI nie wskazano takiego zespołu.
[20] Zarządzenie nr 68/2022 Dyrektora SP ZOZ w Działdowie z dnia 17 października 2022 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

- zgłaszanie niezwłocznie incydentów, nie później niż w ciągu 24 godzin od momentu wykrycia do właściwego CSIRT;
- współpracy podczas obsługi incydentu poważnego i krytycznego z właściwym CSIRT;
- usuwania wskazanej podatności oraz informowania o ich usunięciu właściwego organu;
- ścisłej współpracy z użytkownikami i pracownikami Szpitala w przypadku wystąpienia incydentu cyberbezpieczeństwa;
- prowadzenia rejestru incydentów cyberbezpieczeństwa.

Zgłoszenie ww. osoby do właściwego dla Szpitala CSIRT – tj. Ministerstwa Zdrowia, nastąpiło dopiero w dniu 10 stycznia 2023 r. (szerszy opis znajduje się w sekcji dotyczącej stwierdzonych nieprawidłowości).
W dniu 19 października 2023 r. Dyrektor wyznaczył dwie dodatkowe osoby do zasilenia wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo Szpitala. Byli to pracownicy SP ZOZ pełniący funkcję informatyków. Zakres ich zadań i obowiązków był taki sam jak ww. pracownika.
Zgłoszenie aktualizacji osób kontaktowych do CSIRT NASK nastąpiło w tym samym dniu, tj. 19 października 2023 r.

(akta kontroli str. 224-250)

1.6. Zgodnie z wymogami art. 15 UOC, w dniach 12-13 lipca 2023 r. podmiot wybrany w trybie zapytania ofertowego[21] przeprowadził w Szpitalu audyt, którego celem była ocena bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług kluczowych realizowanych przez Szpital oraz identyfikacja i analiza luki zgodności z wymaganiami UOC. Koszt przeprowadzenia audytu wyniósł 16 tys. zł. Audytorzy wydali dla Szpitala opinię pozytywną z zastrzeżeniami.
Do końca 2023 r. część zaleceń audytu została wdrożona. I tak, stwierdzone przez audytorów kwestie dotyczące m.in.:

- braku monitoringu wizyjnego pomieszczeń serwerowni;
- braku oprogramowania i wiedzy do zabezpieczenia śladów kryminalistycznych oraz do przeprowadzania analizy złośliwego kodu;
- braku wdrożenia w Szpitalu rozwiązania klasy SIEM[22];
- braku systematycznej weryfikacji podatności systemów informatycznych:
- modyfikacji procedury zarządzania incydentami, która w nikły sposób odnosiła się do obszaru cyberbezpieczeństwa, a głównie dotyczyła danych osobowych;
- braku narzędzi do uzyskiwania informacji o podatnościach,

zostały zrealizowane. W ww. zakresie m.in. pozyskano i wdrożono darmowe narzędzia DEFT Linux i Kali Linux[23] oraz oprogramowanie AlienVault, system Szpitala podłączono do systemu S46 NASK[24], uruchomiono monitoring wizyjny pomieszczeń serwerowni, zmodyfikowano plany postępowania z ryzykiem w celu dokładniejszego ich opisu, procedury zarządzania incydentami poszerzono o obszar cyberbezpieczeństwa oraz poddano weryfikacji podatności systemów informatycznych (dodatkowo, zgodnie z zapisami dokumentu „Planowanie jakości”[25]

[21] W sprawie przeprowadzenia procedury udzielenia zamówienia o wartości szacunkowej nieprzekraczającej równowartości kwoty 130 tys. zł netto.

[22] SIEM - Security Information and Event Management. Złożone narzędzie służące do monitorowania bezpieczeństwa w systemach informatycznych.

[23] DEFT Linux - specjalistyczna dystrybucja Systemu Operacyjnego Linux, przeznaczona do analizowania zawartości komputera pod kątem badań kryminalistycznych – informatyka śledcza i testy penetracyjne.
Kali Linux - dystrybucja Systemu Operacyjnego Linux, przeznaczona głównie do łamania zabezpieczeń i testów penetracyjnych czy też audytów bezpieczeństwa.

[24] System S46 - ogólnokrajowy systemem komunikacyjno-analityczno-wizualizacyjny, który zgodnie z art. 46 UOC wspiera współpracę podmiotów wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa.

[25] Dokument systemu zarządzania jakością ISO 9001:2015, opracowany w dniu 5 września 2023 r., dotyczący zaleceń po audycie bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przeprowadzonego w SP ZOZ w dniach 12-13 lipca 2023 r.

nr 4/2023 – dalej: „dokument planowania jakości ISO", zaplanowano systematyczne poddawanie takiej weryfikacji systemów co najmniej jeden raz na kwartał).
Zalecenia związane m.in. z:

- wdrożeniem całodobowego monitoringu zagrożeń cyberbezpieczeństwa;
- dokładniejszym opisem planów postępowania z ryzykiem;
- stworzenia planów ciągłości oraz planów BIA[26] dla procesów aptecznych;
- realizacji audytów dostawców kluczowych systemów informatycznych,

zostały zrealizowane częściowo. I tak, w celu ich realizacji m.in.: podjęto negocjacje w sprawie wyboru i podpisania umowy z NASK na świadczenie usługi SOC[27], której uruchomienie zaplanowano na I kwartał 2024 r., dokumentacja związana z rozbudową rejestru ryzyka, wg stanu na koniec 2023 r., była w trakcie opracowywania, poddano również modyfikacji plany postępowania z ryzykiem w celu dokładniejszego ich opisu, jednakże zakończenie tego procesu, zgodnie z dokumentem planowania jakości ISO, zaplanowane zostało na I i II kwartał 2024 r. W zakresie procesów aptecznych – opracowano plany ciągłości, jak i analizę planów BIA tych procesów, a dokumentacja z tym związana była, wg stanu na koniec 2023 r., w trakcie weryfikacji oraz dalszej modyfikacji w kolejnych komórkach organizacyjnych Szpitala, a zgodnie z dokumentem planowania jakości ISO, planowany termin zakończenia tego działania przypadał na II kwartał 2024 r. Natomiast z zalecenia dotyczącego przeprowadzenia audytu dostawców kluczowych systemów informatycznych, SP ZOZ wywiązał się częściowo, gdyż co prawda Szpital przesłał odpowiednie dokumenty do ww. dostawców z prośbą o ich wypełnienie, jak i kilkukrotnie kontaktował się z nimi telefonicznie w celu przypomnienia o tym działaniu, jednak żaden z nich nie poddał się temu obowiązkowi. Zgodnie z zapisami dokumentu planowania jakości ISO, zrealizowanie ww. zadania powinno nastąpić w 2024 r.
W związku natomiast ze stwierdzonymi podczas audytu kwestiami dotyczącymi:

- niewystarczających zasobów w dziale IT, które uniemożliwiają skuteczne realizowanie zadań związanych z dokumentowaniem zmian w systemach informatycznych na bieżąco;
- braku systemu alarmowego w pomieszczeniach IT;
- braku w ww. pomieszczeniach szaf i sejfów z atestami;
- braku przeprowadzenia audytu po wdrożeniu Systemu Zarządzania Bezpieczeństwem,

m.in. dokonano rozeznania rynku i zebrano oferty dotyczące systemów alarmowych, jak i wyposażenia posiadającego odpowiednie atesty do pomieszczeń IT. Zgodnie z dokumentem planowania jakości, zakup szaf, sejfów i systemu alarmowego, jak i przeprowadzenie ww. audytu, zaplanowano na I kwartał 2024 r.

(akta kontroli str. 475-519, 592-599, 601-709)

1.7. Z dniem 1 września 2018 r., zgodnie z wymogami art. 37 ust. 1 RODO, Dyrektor wyznaczył IODO. Osoba ta spełniała wymagania określone w art. 37 ust. 5 RODO, tj. posiadała odpowiednie kwalifikacje zawodowe, jak i wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych.

Przypisane zadania i obowiązki IODO, wyczerpywały katalog wymaganych czynności określonych w art. 39 RODO, tj. dotyczyły m.in:

- informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

[26] Business Impact Analysis to proces identyfikacji i oceny wpływu potencjalnych zagrożeń na działalność jednostki.
[27] Centrum operacji bezpieczeństwa odpowiadające za ochronę organizacji przed cyberzagrożeniami. Analitycy SOC prowadzą całodobowy monitoring sieci organizacji i badają wszelkie potencjalne incydenty bezpieczeństwa.

- monitorowania przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów;
- udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 RODO;
- współpracy z organem nadzorczym;
- pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach.

(akta kontroli str. 710-736)

1.8. W okresie objętym kontrolą w Szpitalu organizowano szkolenia dla pracowników dotyczące m.in. zagadnień związanych z ochroną danych osobowych, jak i bezpieczeństwa danych. IODO:

- prowadził szkolenia grupowe pracowników, podczas których omawiał zagadnienia związane m.in. z: przetwarzaniem danych osobowych, danych wrażliwych, udostępniania tych danych oraz ich ochroną (zabezpieczanie stanowiska pracy, udzielanie informacji drogą elektroniczną jak i telefoniczną, komunikacją z pacjentem, udostępnianiem dokumentacji medycznej itp.);
- w trakcie pandemii, gdy zawieszono obowiązek szkoleń grupowych, podczas odpraw ordynatorów/kierowników oddziałów/działów oraz pielęgniarek oddziałowych, przekazywał/przypominał o podstawowych informacjach w zakresie ww. ochrony danych (tj. m.in. o zasadzie czystego biurka, wylogowywaniu z systemu przy każdorazowym odejściu od komputera), oraz ukierunkowywał kadrę kierowniczą na zwracanie uwagi podległemu personelowi w przypadku wystąpienia niedociągnięć w ww. zakresie;
- redagował informacje w zakresie ochrony danych osobowych pojawiające się w systemie szpitalnym w formie komunikatów dla użytkowników („Przewodnik po RODO w służbie zdrowia", „RODO w służbie zdrowia. Po pierwsze pacjent");
- w dniu zatrudnienia każdego nowego pracownika w Szpitalu, prowadził przeszkolenie w zakresie podstawowych informacji o ochronie danych osobowych.

W okresie objętym kontrolą dla pracowników Szpitala udostępniano także szkolenia online (przesłane w formie komunikatu widocznego po zalogowaniu się w systemie Szpitala) tj.:

- „Cyfryzacja w ochronie zdrowia oczami pacjenta" – szkolenie obejmowało treści dotyczące m.in. profilu zaufanego, internetowego konta pacjenta, głównych założeń e-recepty oraz e-skierowania, jak i głównych założeń związanych z prowadzeniem elektronicznej dokumentacji medycznej oraz zdarzeń medycznych;
- „Kurs dla osób zatrudnionych w podmiotach leczniczych i wykonujących zadania związane z dokumentacją medyczną" – celem kursu było przygotowanie uczestnika do sprawnego i zgodnego z przepisami realizowania i koordynowania zadań administracyjnych w placówce medycznej, związanych z obsługą procesów medycznych i zarządczych w oparciu o systemy medyczne i informacyjne;
- „Cyberbezpieczeństwo, zagrożenia oraz zasady bezpiecznego korzystania z sieci";
- „Szkolenie z zakresu informacji o cyberatakach na kluczowe usługi sektora ochrony zdrowia na przykładzie ataku na Instytut Zdrowia Matki Polki";

- „Cyberbezpieczeństwo – informacje” – była to broszura informacyjna przekazana przez Warmińsko-Mazurski Urząd Wojewódzki;
- „Szkolenie Sybersec&RODO” – wykłady dotyczące tematyki RODO, cyberbezpieczeństwa oraz sztucznej inteligencji.

Dodatkowo w dniu 14 listopada 2022 r. zorganizowano dla kadry zarządzającej oraz informatyków Szpitala stacjonarne szkolenie w zakresie cyberbezpieczeństwa[28]. Tematyka obejmowała m.in. ochronę przed zaawansowanymi atakami przez pocztę elektroniczną i strony www, tworzenie i zarządzanie polityką haseł i tożsamości, zarządzanie ryzykiem, dokumentacją i polityką bezpieczeństwa oraz wykonywanie kopii zapasowych, tworzenie i utrzymanie polityki ciągłości działania.

(akta kontroli str. 722-739)

1.9. W okresie objętym kontrolą Szpital jednokrotnie wystąpił o wsparcie na dofinansowanie inwestycji poprawiających bezpieczeństwo infrastruktury teleinformatycznej. W dniu 13 grudnia 2022 r. Dyrektor złożył wniosek do Narodowego Funduszu Zdrowia Warmińsko-Mazurskiego Oddziału Wojewódzkiego w Olsztynie o dofinansowanie w wysokości 400 tys. zł:

- opracowania dokumentacji SZBI;
- zakupu zapory sieciowej Stormshield SN720, oprogramowania antywirusowego dla stacji roboczych i serwerów, urządzenia NAS, dysków twardych do urządzenia NAS, zasilacza awaryjnego do urządzenia NAS, komputerów oraz monitorów;
- przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu;
- przeprowadzenia szkolenia w zakresie cyberbezpieczeństwa.

Wypłata ww. środków nastąpiła 29 grudnia 2022 r.

(akta kontroli str. 740-772)

1.10. Jak wskazał Dyrektor, uznanie Szpitala za OUK systematyzuje i porządkuje wymagania w stosunku do zagadnień cyberbezpieczeństwa. Dodał jednakże, iż podejście do tego zagadnienia wydaje się jednak czasami nadmiernie biurokratyczne. Wskazał, że obowiązki z tym związane generują duże wydatki finansowe związane z koniecznością inwestycji w infrastrukturę, koszty utrzymania systemów informatycznych oraz zatrudnienie specjalistycznego personelu. Wskazał, że do wyeliminowania bądź ograniczenia ww. trudności mogłoby przyczynić się zwiększenie finansowania dedykowanego cyberbezpieczeństwu, w tym nieobejmujące tylko wydatki inwestycyjne, ale również środki pozwalające na zatrudnienie dodatkowego, wyspecjalizowanego personelu.

(akta kontroli str. 850-851)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Pomimo że w SZBI, w Polityce Bezpieczeństwa Informacji i Danych Osobowych, w punkcie 4 „Odpowiedzialność i uprawnienia” zapisano, iż Dyrektor powołuje m.in. Pełnomocnika ds. SZBI oraz Zespół ds. BI[29], a ich zakresy obowiązków określa się w Zarządzeniu Dyrektora, to formalnie (wg stanu na 22 stycznia 2024 r.) nie przypisano nikomu takich funkcji. W praktyce, zadania te pełnione były jednak przez Kierownika ds. IT (będącego również ASI) oraz IODO.

[28] Było to szkolenie sfinansowane w ramach wsparcia Szpitala przez Narodowy Fundusz Zdrowia poprzez dofinansowanie inwestycji poprawiających bezpieczeństwo infrastruktury teleinformatycznej, opisanego w punkcie 1.9. niniejszego wystąpienia pokontrolnego.

[29] W wydaniu pierwszym SZBI z dnia 17 października 2022 r. zarówno Pełnomocnik ds. SZBI, jak i Zespół ds. BI, natomiast w wydaniu drugim z dnia 19 października 2023 r. wyłącznie Pełnomocnik ds. SZBI.

Jak wyjaśnił Dyrektor, pomimo ustnego wskazania pełnienia takich funkcji Kierownikowi ds. IT oraz IODO, z powodu przeoczenia, pominięto sformalizowanie przypisania takich zadań.

(akta kontroli str. 352-474, 600)

2. Pomimo wyznaczenia w dniu 17 października 2022 r. osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, nie zrealizowano wymogu określonego w art. 9 ust. 2 UOC, dotyczącego przekazania danych tej osoby w wymaganym terminie (tj. w terminie 14 dni od dnia jej wyznaczenia) do organu właściwego do spraw cyberbezpieczeństwa, tj. do CSIRT NASK. Zgłoszenie to nastąpiło dopiero w dniu 10 stycznia 2023 r., tj. po 85 dniach licząc od upływu wymaganego terminu.

   Jak wyjaśnił Dyrektor, powodem opóźnienia w wykonaniu ww. obowiązku były błędy w komunikacji wewnętrznej w administracji Szpitala, jak również nagła choroba Dyrektora (zawał serca), dodatkowo opóźniająca dopełnienie omawianego obowiązku.

   (akta kontroli str. 224-237, 591-599)

3. Obowiązujący w latach 2020-2023 regulamin organizacyjny Szpitala[30], nie został dostosowany do aktualnej w tym okresie, faktycznie funkcjonującej struktury organizacyjnej. W §13 obowiązującego regulaminu organizacyjnego[31] wskazano, że: „Struktura organizacyjna Szpitala składa się z trzech pionów, tj. Pionu Opieki Zdrowotnej, Pionu Finansowo-Ekonomicznego i Pionu Techniczno-Administracyjnego, dzielących się na mniejsze jednostki organizacyjne oraz jednostek organizacyjnych i samodzielnych stanowisk pracy poległych bezpośrednio Dyrektorowi Zakładu. W punkcie IV. natomiast wskazano, że Dyrektorowi Zakładu podlega bezpośrednio m.in. samodzielne stanowisko pracy – informatyk. W toku kontroli ustalono jednak, że w Szpitalu zatrudnionych było trzech informatyków, jeden z nich od dnia 21 lipca 2014 r. zajmował stanowisko „Kierownik ds. IT", a jednym z zakresów jego czynności, było sprawowanie nadzoru nad pracą podległych pracowników.

   Jak wyjaśnił Dyrektor, faktycznie w ww. regulaminie organizacyjnym niewłaściwie opisano strukturę organizacyjną komórki zajmującej się IT, w szczególności pominięto uwidocznienie stanowiska Kierownika IT, podległego bezpośrednio Dyrektorowi i nadzorującego pracę pozostałych informatyków. Dyrektor wyjaśnił, że problem został zauważony i omawiany w trakcie prac nad aktualizacją regulaminu organizacyjnego na przełomie 2022 i 2023 r. Dodał jednak, że przez niedopatrzenie pracowników administracji SP ZOZ, opis komórki IT nie został zaktualizowany. Dodał także, że Regulamin Organizacyjny Szpitala zostanie niezwłocznie poprawiony.

   (akta kontroli str. 7-124, 238-250, 591-599)

OCENA CZĄSTKOWA

W Szpitalu, po uznaniu go w dniu 19 lipca 2022 r. za OUK, zostały stworzone odpowiednie rozwiązania organizacyjne w ramach przyjętego SZBI, mające na celu zapewnienie bezpieczeństwa informacji, w tym ochronę danych pacjentów. Dokonano m.in. szacowania ryzyka dla swoich usług kluczowych, zarządzano incydentami, wyznaczono osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, prowadzono działania edukacyjne wobec użytkowników, wdrożono odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne, zbierano informacje o zagrożeniach i podatnościach, wdrożono wymaganą dokumentację oraz

[30] Wprowadzony zarządzeniem nr 3/2018 Dyrektora Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Działdowie z dnia 1 marca 2018 r. w sprawie Regulaminu Organizacyjnego Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Działdowie, zmieniony zarządzeniem nr 10/2023 z dnia 28 lutego 2023 r.

[31] W regulaminie organizacyjnym z 2018 r. – w §12.

przeprowadzono audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Wyznaczono również IODO, a powierzone mu zadania były zgodne z wymogami art. 39 RODO.

W ww. obszarze stwierdzono jednak trzy nieprawidłowości, które dotyczyły:

- nieprzekazania do CSIRT NASK, w wymaganym art. 9 ust. 2 UOC terminie, danych osoby wyznaczonej do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
- nieprzypisania formalnie zadań dla Pełnomocnika ds. SZBI oraz Zespołu ds. BI;
- niedostosowania zapisów regulaminu organizacyjnego do faktycznie funkcjonującej w badanym okresie struktury organizacyjnej.

OBSZAR

2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami

Opis stanu faktycznego

2.1. W latach 2020-2023 w Szpitalu funkcjonowało pięć systemów informacyjnych. Były to:

- Softhard – system kadrowo-płacowy funkcjonujący w Szpitalu od 12 września 2012 r. do 31 listopada 2022 r., zastąpiony od 1 grudnia 2022 r. systemem o nazwie Simple zawierającym moduły: kadry, płace, księgowość, kasa oraz magazyny;
- Medicom – przeznaczony do obsługi całego procesu realizacji badania od momentu planowania i rejestracji pacjenta w pracowni radiologicznej, przez proces wykonania badania, aż po stworzenie i wydanie opisu (RIS - Radiology Information System);
- Centrum – przeznaczony do obsługi całego procesu realizacji badania od momentu pobrania materiału, rejestracji pacjenta, poprzez wykonanie badania i wygenerowanie wyniku (LIS - Laboratory Information System);
- Medicus Online – przeznaczony do archiwizacji, przetwarzania i udostępniania danych związanych z realizacją procesu diagnostyczno-terapeutycznego (HIS - Hospital Information System).

(akta kontroli str. 773-774)

2.2. W okresie objętym kontrolą SP ZOZ nie posiadał wdrożonej usługi katalogowej – Active Directory. Zarządzanie siecią LAN oraz uprawnieniami użytkowników na komputerach końcowych odbywało się za pomocą oprogramowania ESET Protect Enterprise ON-PREM. Administrator podczas pierwszej instalacji danego komputera, przystosowywał go do danego miejsca pracy m.in. zakładając konta użytkowników, instalując stosowne oprogramowanie, konfigurując uprawnienia dostępu. Działania te realizowane były bez udziału konsoli. Pozostałe dalsze już czynności zarządzania realizowane były zdalnie, z poziomu konsoli administratora ESET. Administrator miał możliwość z poziomu ww. konsoli m.in. dodawania i odbierania uprawnień, tworzenia polityk bezpieczeństwa oraz zarządzania zdalnie ustawieniami (tj. m.in. wymuszeniami aktualizacji systemu Windows, programu antywirusowego, filtrowania zawartości odwiedzanych stron www, ograniczeń dostępu do Internetu, powiadomień odnośnie zagrożeń dla bezpieczeństwa, blokowania urządzeń USB, zlecenia instalacji oprogramowania, zdalnego wyłączenia/uruchomienia ponownego urządzenia, odizolowania komputera od sieci w przypadku pojawienia się powiadomienia z konsoli o zagrożeniu).

(akta kontroli str. 775)

2.3. Przeprowadzone w toku kontroli, w dniu 13 grudnia 2023 r., oględziny oprogramowania ESET Protect Enterprise ON-PREM oraz uprawnień dostępu pracowników do systemów Szpitala, wykazały m.in. że:

- Wszyscy pracownicy[32] Szpitala przetwarzający dane osobowe pacjentów posiadali stosowne, pisemne upoważnienia do przetwarzania takich danych w zakresie realizowanych przez nich zadań.
- Personel niemedyczny Szpitala[33] posiadał dostęp do danych medycznych wyłącznie w zakresie niezbędnym do wykonywanych zadań. I tak, każdy z pracowników:
  - mający dostęp do systemów medycznych Szpitala, otrzymał stosowne upoważnienie do przetwarzania danych osobowych,
  - miał dostęp do systemu medycznego wyłącznie po odpowiednim przeprowadzeniu autoryzacji (podaniu loginu i hasła),
  - miał dostęp do danych medycznych wyłącznie w zakresie wydanego upoważnienia,
  - który miał dostęp do danych medycznych, przetwarzał je wyłącznie w ramach wykonywanych obowiązków,
  - który nie wykonywał zadań związanych z przetwarzaniem ww. danych, nie miał dostępu do danych medycznych pacjentów.

  Ww. dostęp był możliwy tylko po odpowiednim przeprowadzeniu autoryzacji użytkownika (podaniu loginu i hasła).
- Na podstawie weryfikacji uprawnień w systemach informatycznych oraz nadanych w wersji papierowej upoważnień wybranych losowo ze wszystkich oddziałów/poradni SP ZOZ 32 pielęgniarek i położnych ustalono, że wszystkie:
  - posiadały wydane przez administratora danych osobowych stosowne upoważnienia do przetwarzania danych osobowych pacjentów Szpitala,
  - miały dostęp do danych medycznych wyłącznie w zakresie wskazanym w ww. upoważnieniu,
  - dostęp do systemu medycznego posiadały wyłącznie po odpowiednim przeprowadzeniu autoryzacji (podaniu loginu i hasła),
  - przetwarzały dane medyczne pacjentów w ramach wykonywanych przez siebie obowiązków.
- Żaden z pracowników Szpitala, który nie był zaangażowany w proces przetwarzania danych medycznych pacjentów (np. sanitariusze, salowe, personel sprzątający), nie posiadał tego w swoim zakresie czynności, nie miał nadanego upoważnienia do przetwarzania takich danych, ani nie miał nadanych uprawnień do dostępu do systemów medycznych Szpitala.
- Na podstawie weryfikacji danych związanych z dostępem[34] pracowników Szpitala do systemów informatycznych, z którymi po 1 stycznia 2022 r. rozwiązano stosunek pracy (wg stanu na dzień oględzin – 90 osób ustalono m.in, że:
  - nie wystąpiły przypadki, gdy po dacie rozwiązania stosunku pracy, pracownik zalogował się do systemu,
  - wszystkie konta ww. osób zostały zablokowane,
  - wszystkim ww. osobom odebrano uprawnienia dostępu do systemów informacyjnych Szpitala.

(akta kontroli str. 776-809)

2.4. Przeprowadzone w toku kontroli, w dniu 18 grudnia 2023 r. oględziny 27 komputerów użytkowanych przez wybranych losowo pracowników (lekarzy, pielęgniarki i położne, pracownicy administracji), wykazały m.in. że:

[32] Wg stanu na dzień oględzin, tj. 13 grudnia 2023 r., w SP ZOZ zatrudnionych było 150 pracowników niemedycznych.

[33] Byli to m.in. Kierownik bloku żywienia, Kierownik działu IT, informatycy, Referent ds. logistyki i zaopatrzenia oraz pracownicy zajmujący się statystyką medyczną.

[34] Z poziomu konsoli Administratora oprogramowania ESET wygenerowano czas ostatniego logowania oraz wylogowania z systemu tych osób, dodatkowo zweryfikowano czy konta ww. osób zostały zablokowane.

- Komputery zostały dostosowane do miejsca użytkowania pod względem ograniczenia uprawnień oraz możliwości zalogowania się do systemu szpitalnego zgodnie z nadanymi uprawnieniami (każdy komputer umożliwiał zalogowanie się użytkownikowi w ramach posiadanego upoważnienia i nadanych uprawnień do systemu medycznego Szpitala).
- Każdy z pracowników logował się do systemu podając swój login (ciąg znaków, na które składała się pierwsza litera imienia oraz nazwisko bez polskich znaków) oraz hasło, o liczbie znaków nie mniejszej niż osiem (było to zgodne z polityką bezpieczeństwa Szpitala, tj. Systemem Zarządzania Bezpieczeństwem Informacji).
- Każdy z pracowników miał dostęp wyłącznie do danych, co do których posiadał stosowne upoważnienie.
- Na każdym komputerze zainstalowany był program antywirusowy Eset, w wersji aktualnej[35] na dzień przeprowadzonych oględzin.
- Na komputerach zainstalowany był aktualny na dzień przeprowadzenia oględzin system Windows 10 lub 11.
- Na żadnym z komputerów użytkowanych przez więcej niż jedną osobę, nie znaleziono plików z danymi pacjentów (tj. plików typu .pdf, .jpg itp.). Administrator systemu uniemożliwił zapis plików w katalogach systemu Windows (Pulpit, dokumenty, pobrane) poprzez odebranie użytkownikowi uprawnień do zapisu oraz zainstalował na komputerach użytkowników skrypt sprawdzający i usuwający ewentualne pliki tworzone przez system podczas generowania wydruków.
- Na żadnym z komputerów, żaden z pracowników nie mógł zainstalować żadnego oprogramowania. Podczas próby zainstalowania wybranego programu 7zip.exe, system żądał hasła administratora.
- Na każdym z komputerów porty USB były systemowo zablokowane przy użyciu ustawień oprogramowania ESET.

(akta kontroli str. 810-813)

2.5. W okresie objętym kontrolą w Szpitalu prowadzono rejestr incydentów bezpieczeństwa danych oraz naruszeń ochrony danych osobowych. W latach 2018-2023 zamieszczono w nim 40 wpisów, z czego wszystkie dotyczyły wystąpienia drobnych naruszeń przez użytkowników (np. zapisane hasła w przeglądarce, zapisane hasła na kartce, czy tez brak wygaszacza ekranu). Zgodnie z zapisami ww. rejestru oraz informacją od ASI, w każdym przypadku działania naprawcze były podejmowane natychmiast po ich stwierdzeniu, bez zbędnej zwłoki, w tym samym dniu. Do końca 2023 r. nie odnotowano incydentów, które podlegały zgłoszeniu do właściwego CSIRT.
Szpital systematycznie szacował ryzyko wystąpienia incydentu monitorując zagrożenia dzięki oprogramowaniu System S461. Na skutek ww. czynności, ASI m.in. analizując zapisy ww. rejestru, zidentyfikował podatne miejsca w systemie Windows (pliki pdf zawierające dane osobowe pacjentów, gromadzone podczas wydruku dokumentów z systemu Szpitalnego) i w celach naprawczych utworzył i wdrożył do działania skrypt, który na komputerach wszystkich użytkowników Systemów Szpitalnych był systematycznie uruchamiany[36] w celu skasowania wszystkich niepotrzebnych, ww. zgromadzonych plików.

(akta kontroli str. 175-177)

2.6. W latach 2020-2023 Szpital zawarł z sześcioma podmiotami łącznie 12 umów, w których był stroną powierzającą przetwarzanie danych osobowych (dalej: ADO). Dotyczyły one:

[35] Posiadający aktualną bazę wirusów.
[36] Poprzez ustalony harmonogram, z częstotliwością co pięć minut.

- realizacji umów serwisowych oraz aktualizacji systemów Szpitala;
- wykonywania badań laboratoryjnych;
- udzielania świadczeń opieki zdrowotnej w rodzaju podstawowa opieka zdrowotna w zakresie nocnej i świątecznej pielęgniarskiej opieki zdrowotnej;
- realizacji kształcenia podyplomowego pielęgniarek i położnych.

Na podstawie analizy wybranych losowo pięciu umów powierzenia przetwarzania danych osobowych ustalono, że spełniały one wymogi art. 28 RODO. I tak ww. umowy stanowiły, że podmiot, któremu powierzone zostało przetwarzanie danych, m.in.:

- dokonuje tego wyłącznie na udokumentowane polecenie administratora;
- zapewnia, by osoby upoważnione do przetwarzania osobowych zobowiązały się do zachowania tajemnicy;
- podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzania danych;
- przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o ile dysponuje szczegółową i pisemną zgodą ADO na dalsze powierzenie;
- w miarę możliwości wspiera ADO w wywiązywaniu się przez niego z obowiązków związanych z ochroną danych osobowych oraz udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków;
- uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO;
- po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji ADO, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich kopie, chyba że prawo nakazuje przechowywanie danych osobowych;
- umożliwia ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji.

(akta kontroli str. 814-849)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK ocenia pozytywnie działania Szpitala w zakresie funkcjonowania przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami.

IV. Uwagi i wnioski

Najwyższa Izba Kontroli w wyniku kontroli nie formułuje uwag. W związku natomiast ze stwierdzonymi nieprawidłowościami, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Wyznaczenie Pełnomocnika ds. SZBI oraz określenie jego zadań.
2. Dostosowanie zapisów regulaminu organizacyjnego Szpitala do aktualnie funkcjonującej struktury organizacyjnej Szpitala.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Olsztynie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Olsztyn, 6 lutego 2024 r.

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis

Kontroler
Edyta Piskorz-Zabujść
Specjalista kontroli państwowej

.....
podpis