

Cyberbezpieczeństwo

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Łukowie, jako operator usługi kluczowej, zobowiązany został ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa do zapewnienia pacjentom oraz podmiotom współpracującym dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

Szpital wdrożył i eksploatuje system zarządzania bezpieczeństwem informacji w oparciu o wymagania międzynarodowego standardu ISO/IEC 27001, celem minimalizowania ryzyka zmaterializowania się zagrożeń mających niekorzystny wpływ na proces świadczenia usługi kluczowej. W celu zapewnienia ciągłego monitoringu skuteczności wdrożonych zabezpieczeń organizacyjnych, technicznych, zmian w otoczeniu prawnym i technologii, Szpital stworzył podstawowe grupy celów ochrony.

- Bezpieczeństwo fizyczne
- Bezpieczeństwo dostaw niezbędnych mediów
- Bezpieczeństwo współpracy z dostawcami towarów i usług
- Bezpieczeństwo technologiczne
- Bezpieczeństwo osobowe
- Bezpieczeństwo komunikacji

Takie podejście ma zapewnić możliwość przypisania zadań do odpowiednich ról w szpitalu, przy jednoczesnym uwzględnieniu wpływu podmiotów zewnętrznych na poziom bezpieczeństwa. Dla powyższych celów bezpieczeństwa operator usługi kluczowej prowadzi systematyczne analizy podatności, incydentów, które mogą zakłócić ciągłość usługi lub wpłynąć na utratę podstawowych atrybutów bezpieczeństwa przetwarzanych informacji.

Bezpieczeństwo fizyczne

Szpital posiada kilka lokalizacji, dla których ustalono spójne, proceduralne zasady ochrony pomieszczeń istotnych z punktu widzenia bezpieczeństwa procesu świadczenia usługi kluczowej. Ochronę fizyczną zapewniają w szczególności systemy kontroli dostępu (zamki mechaniczne i elektroniczne), system monitoringu wizyjnego, system identyfikacji pracowników oraz służby ochrony fizycznej (osobowej) oraz system przeciwpożarowy (dla ochrony przed ogniem). Ponadto w Szpitalu obowiązują procedury alarmowe na wypadek zagrożeń różnego rodzaju.

Ze względu na dostęp osób trzecich (pacjenci, odwiedzający, dostawcy i podwykonawcy usług) na teren Szpitala w trybie 24 h, służby ochrony muszą podejmować specjalne środki wobec osób próbujących uzyskać dostęp do pomieszczeń i obszarów o ograniczonym dostępie. Wszystkie osoby korzystające z usług Szpitala lub odwiedzające pacjentów uprasza się o szczególny nadzór nad bagażami (torby, walizki). Pozostawienie, bez opieki, bagażu może wywołać po stronie służb ochrony fizycznej nadmiarowe działania i narazić na niepotrzebny stres pacjentów i osoby przebywające na terenie Szpitala.

W przypadku zauważenia próby przełamania zabezpieczeń, próby nieautoryzowanego wejścia na chroniony obszar proszę o pilny kontakt: Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji, tel. (25) 7980409, e-mail: incydenty@spzoz.lukow.pl

Bezpieczeństwo dostaw niezbędnych mediów

Ze względu na krytyczność systemów informacyjnych, urządzeń i narzędzi wspomagających proces utrzymania pacjenta przy życiu, Szpital został wyposażony w redundantne zabezpieczenia na wypadek zakłóceń lub utraty zasilania. Ponadto, ze względu na rozległość terenu, liczbę punktów, rozdzielni oraz zdarzające się kradzieże i dewastacje infrastruktury Szpitala, podpisane

zostały stosowane umowy serwisowe. Ponadto w Szpitalu przyjęto jednolity system zgłaszania awarii odpowiednim służbom technicznym i serwisowym. Priorytetowym zadaniem jest informowanie na wczesnym etapie o zdarzeniach mogących mieć wpływ na ciągłość zasilania, tras kablowych telekomunikacyjnych i sieciowych.

W przypadku zauważenia powyżej opisanego zagrożenia, proszę o niezwłoczne poinformowanie: Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji, tel. (25) 7980409, e-mail: incydenty@spzoz.lukow.pl

Bezpieczeństwo współpracy z dostawcami towarów i usług

Każdy współpracownik, w tym dostawca towarów i usług, ze względu na możliwe powiązanie z procesem świadczenia usługi kluczowej jest badany pod kątem zaufania i zgodności prawnej. Przed udzieleniem informacji na temat infrastruktury Szpitala, obowiązkiem obu stron jest podpisanie umowy poufności, zobowiązującej obie strony do zachowania, bezterminowo, wiedzy o zabezpieczeniach organizacyjnych, technicznych, infrastrukturze Szpitala.

Szpital wdrożył system zarządzania bezpieczeństwem informacji i restrykcyjnie egzekwuje stosowanie wewnętrznych procedur i instrukcji, Zagrożenie dla aktywów Szpitala może być dostawca, który nie wdrożył w swojej organizacji systemowego podejścia do ochrony informacji. Wobec takich podmiotów Szpital, w umowach, zastrzega sobie prawo audytu drugiej strony w celu zbadania stanu bezpieczeństwa w obszarze dotyczącym przedmiotu umowy.

Każdy współpracownik dostrzegający zdarzenie, incydent bezpieczeństwa informacji jest zobowiązany do zgłoszenia niezwłocznie zaobserwowanej sytuacji do: Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji, tel. (25) 7980409, e-mail: incydenty@spzoz.lukow.pl

Bezpieczeństwo technologiczne

Usługa kluczowa Szpitala św. Tadeusza w Łukowie ściśle zależy od systemów informacyjnych. Szpital wypełniając obowiązki operatora usługi kluczowej dokonał dekompozycji usługi na elementy składowe. Dla zidentyfikowanych elementów zidentyfikowano podatności związane z brakiem wsparcia producenta w zakresie stosowanych technologii. Dla tych elementów Szpital podejmuje działania zmierzające do wymiany lub zastąpienia bezpiecznymi rozwiązaniami. Wszystkie obecne rozwiązania projektuje się tak aby zapewnić redundantność krytycznych elementów infrastruktury, a także poufność, integralność, dostępność, autentyczność, niezaprzeczalność i rozliczalność w korzystaniu z systemów przechowywania i przetwarzania informacji.

Każdy współpracownik dostrzegający nieprawidłowe działanie systemów w aspekcie bezpieczeństwa informacji jest zobowiązany do zgłoszenia niezwłocznie zaobserwowanej sytuacji do: Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji, tel. (25) 7980409, e-mail: incydenty@spzoz.lukow.pl

Bezpieczeństwo osobowe

Każdy pracownik oraz tam gdzie zasadne współpracownik Szpitala św. Tadeusza w Łukowie jest świadomy zapisów Polityki Bezpieczeństwa Informacji oraz swoich obowiązków w tym zakresie. W odniesieniu do zagrożeń wynikających z braku przestrzegania zapisów Polityki Bezpieczeństwa Informacji i dobrych praktyk w zakresie bezpiecznego przetwarzania informacji Szpital podejmuje działania uświadamiające zagrożenia, informując pracowników Szpitala jak i współpracowników o wszelakich próbach ataków środowisk przestępczych na zasoby informacyjne Szpitala.

Bezpieczeństwo w tym obszarze również zależy od naszych Pacjentów, stąd wprowadziliśmy zabezpieczenia organizacyjne w celu zachowania kontroli nad procesem przetwarzania danych naszych pacjentów od chwili ich pozyskania aż do wydania pacjentowi. Ze względu na próby wyłudzeń informacji, podawania

się za krewnych, bliskie osoby, Szpital wdrożył zabezpieczenia minimalizujące ryzyko pozyskania przez osoby niepowołane informacji o zdrowiu swoich pacjentów.

Każdy Pacjent lub współpracownik Szpitala, który będzie świadkiem próby pozyskania w sposób nielegalny danych o innej osobie, proszony jest o zgłoszenie zaobserwowanej sytuacji do Inspektora Ochrony Danych, tel. (25) 798 20 00 do 9, wew. 329, email: ochronadanych@spzoz.lukow.pl

Bezpieczeństwo komunikacji

Kierownictwo Szpitala, personel z najwyższą uwagą traktuje informacje wymieniane z pacjentami, wykonawcami. W celu ich właściwiej ochrony cała komunikacja elektroniczna realizowana w sieciach publicznych, nie będących pod nadzorem Szpitala, jest szyfrowana aby zmniejszyć prawdopodobieństwo nieuprawnionego dostępu do informacji.

Połączenie pomiędzy poszczególnymi jednostkami Szpitala zbudowano tak aby zapewnić redundancję oraz bezpieczeństwo przesyłanych danych. Szpital korzysta z usług zaufanych dostawców Internetu celem zmniejszenia prawdopodobieństwa błędów po stronie dostawcy, które mogłyby wpłynąć na ciągłość usług szpitala, utratę komunikacji lub bezpieczeństwa transmitowanych informacji.

Ustanowienie nowej ścieżki komunikacji, istotne zmiany w istniejących kanałach komunikacji wymagają formalnej zgody właściwych osób, odpowiadających bezpośrednio przed Dyrekcją Szpitala za właściwe ich funkcjonowanie i bezpieczeństwo.

Wszelkie próby podszywania się pod pacjenta, nieautoryzowane próby połączeń do infrastruktury Szpitala, fałszywe wiadomości mailowe wysyłane do personelu Szpitala należy zgłaszać do Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji, tel. (25) 7980409, e-mail: incydenty@spzoz.lukow.pl w celu zapobiegania incydentom na wczesnym etapie ich rozwoju.

Pacjent, współpracownik Szpitala, który w procesie komunikacji elektronicznej nie będzie w stanie udowodnić swojej tożsamości nie będzie obsługiwany. W takich przypadkach wskazany będzie kontakt osobisty lub inny właściwy dla przedmiotu kontaktu, kanał komunikacyjny.

Cyberbezpieczeństwo to nie produkt, a proces !!!

Wszystkich pacjentów oraz pracowników szpitala, zachęcamy do zapoznania się obszerną bazą wiedzy z zakresu cyberhigieny, znajdującą się w poniższych serwisach internetowych:

- <https://cert.pl/>
- <https://cyberprofilaktyka.pl/>