Cyberbezpieczeństwo

Samodzielny Szpital Wojewódzki im. Mikołaja Kopernika w Piotrkowie Trybunalskim zgodnie z decyzją Ministra Zdrowia został ustanowiony operatorem usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560).

Za operatora usługi kluczowej uznaje się podmiot, jeżeli:

- świadczy usługę kluczową
- świadczenie tej usługi zależy od systemów informacyjnych
- incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora

Uznanie Samodzielnego Szpitala Wojewódzkiego im. Mikołaja Kopernika w Piotrkowie Trybunalskim za Operatora Usługi Kluczowej (w skrócie OUK) wynika z uwagi na świadczenie opieki zdrowotnej przez podmiot leczniczy oraz obrót i dystrybucję produktów leczniczych. Operator usługi kluczowej ma podejmować odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez niego sieci i systemy informatyczne oraz odpowiednie środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia takich usług kluczowych, z myślą o zapewnieniu ciągłości tych usług.

Samodzielny Szpital Wojewódzki im. Mikołaja Kopernika w Piotrkowie Trybunalskim egzekwuje stosowanie wewnętrznych procedur i instrukcji. Każda osoba mająca dostęp do informacji zobowiązana, jest zgodnie z posiadanymi uprawnieniami do zapoznania się z Polityką Bezpieczeństwa Informacyjnego oraz złożenia stosownego oświadczenie, potwierdzającego znajomość jej treści oraz przestrzegania jej zapisów.
Samodzielny Szpital Wojewódzki im. Mikołaja Kopernika w Piotrkowie Trybunalskim zobowiązany jest do szacowania ryzyka dla swoich usług kluczowych, zbierania informacji o zagrożeniach i podatnościach, stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego oraz zgłaszania incydentów poważnych do CSIRT GOV.

Podstawę do identyfikacji ryzyka stanowią procesy i aktywa Samodzielnego Szpitala Wojewódzkiego im. Mikołaja Kopernika w Piotrkowie Trybunalskim, których realizacja ma bezpośredni wpływ na świadczenie usługi cyfrowej w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, a tym samym na określenie poziomu akceptowalności ryzyka.

Reakcja na niepożądane zdarzenia (incydenty) lub podatności:

Każdy pacjent, osoba odwiedzająca pacjentów, pracownik, współpracownik Szpitala w przypadku zauważenia:

- próby przełamania zabezpieczeń, próby nieautoryzowanego wejścia na chroniony obszar
- powzięcia wątpliwości co do stanu technicznego urządzeń informatycznych na których

przetwarzane są dane osobowe
- innych nieprawidłowości budzących wątpliwości w zakresie przestrzegania bezpieczeństwa informacji, a mogących wpłynąć na świadczenie usług, proszony jest o zgłoszenia niezwłocznie zaobserwowanej sytuacji na adres e-mail: incydenty@szpital-piotrkow.pl.

Każdy użytkownik (pracownik lub osoba z firmy zewnętrznej współpracującej ze Szpitalem) ma obowiązek zgłaszania zauważonych przez siebie incydentów oraz notować wszystkie szczegóły związane z incydentem.

Ponadto każda osoba dostrzegająca:

- zdarzenie, incydent bezpieczeństwa informacji
- nieprawidłowe działanie systemów w aspekcie bezpieczeństwa informacji
- próby podszywania się pod pacjenta, nieautoryzowane próby podłączeń do infrastruktury Szpitala, fałszywe wiadomości mailowe wysyłane do personelu Szpitala
- inne zdarzenie mogące mieć wpływ na bezpieczeństwo informacji

jest zobowiązana zaobserwowaną sytuację niezwłocznie zgłosić na adres e-mail: incydenty@szpital-piotrkow.pl

Zabrania się użytkownikowi zgłaszającemu problem lub naruszenie bezpieczeństwa wykonywania jakichkolwiek działań „na własną rękę" rozwiązujących problem, za wyjątkiem działań niezbędnych dla zapewnienia bezpieczeństwa osobom i mieniu. Użytkownik w miarę możliwości powinien zabezpieczyć materiał dowodowy. Powyższe działania mają na celu zapobieganie incydentom na wczesnym etapie ich rozwoju. Za szybką reakcję na pojawiające się incydenty z góry dziękujemy.

Do jednych z wielu obowiązków nałożonych na Operatora Usługi Kluczowej, należy obowiązek opublikowania na stronie internetowej Szpitala podstawowych informacji związanych z zagrożeniami cyberbezpieczeństwa. Ma to na celu umożliwienie pacjentom oraz podmiotom współpracującym, zrozumienia zagrożeń cyberbezpieczeństwa i zastosowanych skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

Cyberbezpieczeństwo zgodnie z obowiązującymi przepisami to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy" (art. 2 pkt 4) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).

Do najpopularniejszych zagrożeń w cyberprzestrzeni możemy zaliczyć:

- Ataki z użyciem szkodliwego oprogramowania
- Kradzieże tożsamości
- Ataki mające na celu wyłudzenie lub zniszczenie danych
- Blokada dostępu do usług (DDoS)
- Niechciana poczta (SPAM)
- Socjotechnika