Samodzielny Publiczny Zespół Opieki Zdrowotnej w Proszowicach jest operatorem usługi kluczowej w sektorze ochrony zdrowia, polegającej na udzielaniu świadczeń opieki zdrowotnej oraz obrocie i dystrybucji produktów leczniczych, zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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 (t.j. Dz. U. z 2022 r. poz. 1863).

Ustawa o krajowym systemie cyberbezpieczeństwa zobowiązuje Szpital do zapewnienia użytkownikom usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych praktyk zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

Poniżej przedstawiamy najważniejsze informacje dotyczące najczęściej występujących cyberzagrożeń oraz sposoby ochrony przed nimi.
Za operatora usługi kluczowej uznaje się podmiot, jeżeli:

1. świadczy usługę kluczową,
2. świadczenie tej usługi zależy od systemów informacyjnych,
3. incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

Operatorzy usług kluczowych są zobowiązani do wdrożenia skutecznych zabezpieczeń, szacowania ryzyka związanego z cyberbezpieczeństwem oraz przekazywania informacji o poważnych incydentach oraz ich obsługi we współpracy z CSIRT poziomu krajowego.
W tym celu operator usługi kluczowej ma podejmować odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem, 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.

Do jednych z wielu obowiązków nałożonych na Operatora Usługi Kluczowej, jest obowiązek opublikowania na stronie internetowej Szpitala podstawowych informacji związanych z zagrożeniami cyberbezpieczeństwa. Ma to na celu umożliwienie pacjentom oraz podmiotom współpracującym, zrozumienia zagrożeń cyberbezpieczeństwa.
Nieodłącznymi elementami definicji cyberbezpieczeństwa są pojęcia ściśle związane z charakterystyką dobrze działających systemów informacyjnych, tj.:
- poufność danych – właściwość polegająca na tym, że informacja nie jest udostępniona lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,
- integralność danych – właściwość polegająca na zapewnieniu dokładności i kompletności danych,
- dostępność danych – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu,
- autentyczność danych – właściwość polegająca na zapewnieniu, że przetwarzane dane są prawdziwe, tj. są danymi, które w sposób autoryzowany zostały wprowadzone do systemu.

Najczęściej występujące incydenty, czyli zdarzenie, które ma lub może mieć niekorzystny wpływ na Cyberbezpieczeństwo to:

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

Przykładowe sposoby na uniknięcie zagrożeń związanych z korzystaniem z cyberprzestrzeni:

- Instalacja, użytkowanie i bieżące aktualizowanie oprogramowania antywirusowego.
- Aktualizowanie systemu operacyjnego urządzenia oraz aplikacji na nim zainstalowanych.
- Sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego.
- Korzystanie ze stron internetowych posiadających ważny certyfikat bezpieczeństwa.
- Regularne skanowanie komputera i sprawdzanie procesów sieciowych.

- Każdorazowa weryfikacja adresu nadawcy wiadomości e-mail.
- Niewysyłanie danych osobowych, logowania, karty kredytowej w niezabezpieczonej treści wiadomości e-mail.
- Unikanie odwiedzin stron zawierających darmowe pliki muzyczne, obrazy, filmy.
- Regularne tworzenie kopii zapasowych ważnych danych.
- Baczne obserwowanie i czytanie komunikatów pojawiających się na ekranie komputera.

Podmioty oraz firmy zajmujące się cyberbezpieczeństwem:

- Ministerstwo Cyfryzacji,
- CERT Polska,
- CSIRT GOV,
- CSIRT NASK,
- CyberDefence24,
- Cyberrescue,