Cyberbezpieczeństwo

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - życie obowiązuje od dnia 28 sierpnia 2018 r. Celem ustawy jest stworzenie Krajowego Systemu Cyberbezpieczeństwa (KSC), który umożliwi sprawne działania na rzecz wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo RP.

Ustawa oraz towarzyszące jej rozporządzenia wykonawcze w pełni wdrożą do polskiego porządku prawnego tzw. dyrektywę NIS. Nowe regulacje tworzą prawne podstawy funkcjonowania krajowego systemu cyberbezpieczeństwa, ustalają zasady jego rozbudowy i zwiększenia poziomu zabezpieczeń systemów teleinformatycznych a także pozwalają ograniczyć potencjalne skutki incydentów oraz cyberzagrożeń, w tym straty finansowe.

Najważniejszym elementem krajowego systemu cyberbezpieczeństwa są tzw. Operatorzy Usług Kluczowych, czyli dostawcy ważnych usług zależnych od systemów informacyjnych (np. firmy energetyczne, przewoźnicy lotniczy i kolejowi, szpitale, podmioty istotne dla infrastruktury ICT itd.).

Podmioty te są zobowiązane m.in. 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 tzw. CSIRT-ów (tj. Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego).

W czerwcu 2019 r. Szpital, na mocy decyzji administracyjnej, został uznaniu za operatora usługi kluczowej.

Cyberbezpieczeństwo oraz ochrona danych osobowych

Dolnośląski Szpital Specjalistyczny im. T. Marciniaka Centrum Medycyny Ratunkowej

Do jednych z wielu obowiązków nałożonych na Szpital obowiązków prawnych jest przekazanie pacjentom podstawowych informacji związanych z zagrożeniami cyberbezpieczeństwa.

Ma to na celu umożliwienie pacjentom 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 (t.j. Dz. U. z 2022 r. poz. 1863).

W związku z powyższym w Szpitalu został wdrożony System Zarządzania Bezpieczeństwem Informacji (dalej SZBI), a także System Zarządzania Ciągłością Działania (dalej: SZCD).

Z punktu widzenia zapewnienia cyberbezpieczeństwa, są to dwa kluczowe obszary, które zapewniają poufność, dostępność, integralność oraz autentyczność informacji i działań Szpitala.

Cztery atrybuty informacji

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 udostępniana 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.

Najpopularniejsze zagrożenia w cyberprzestrzeni

Phishing

- Przestępcy tworzą fałszywe strony Internetowe, żeby wyłudzić Twoje dane (loginy i hasła). Najczęściej wysyłają maile zawierające odnośniki do tych stron.
  - Jak się chronić?
  - Dokładnie weryfikuj adres witryny zanim się na niej zalogujesz. Nie wpisuj swojego loginu i hasła na podejrzanych stronach internetowych.

Malware / ransomware

- Często stosowane są ataki z użyciem szkodliwego oprogramowania (malware, ransomware itp.), hakerzy mogą wysyłać złośliwe oprogramowanie za pośrednictwem e-mail, dołączonego do e-mail załącznika.
  - Jak się chronić?
  - Nie otwieraj podejrzanych wiadomości oraz załączników, ponieważ w przypadku instalacji złośliwego oprogramowania na Twoim urządzeniu, hakerzy mogą przejąć dostęp np. do konta w Twoim banku.

Vishing

- Przestępcy mogą do Ciebie zadzwonić i podawać się za pracownika Szpitala, instytucji np. SANEPID, Policji, Twojego przełożonego i prosić Cię o przekazanie Twojego loginu, hasła, nr PESEL, nr dowodu osobistego. Podanie tych danych może skutkować kradzieżą Twojej tożsamości, umożliwieniem przestępcy zalogowania się do Systemu.
  - Jak się chronić?
  - Nigdy nie podawaj swoich danych, dopóki nie upewnisz się z kim rozmawiasz.

W celu ochrony przed zabezpieczeniami można stosować poniższe wskazówki

W celu ochrony przed zagrożeniami należy stosować zabezpieczenia:

- Nie udostępniaj nikomu swojego loginu i hasła do systemu,
- Unikaj stosowania haseł które można łatwo z Tobą powiązać,
- Unikaj logowania się do systemów z cudzych urządzeń i publicznych nieznanych sieci,
- Używaj aktualnego oprogramowania antywirusowego – stosuj ochronę w czasie rzeczywistym, włącz aktualizacje automatyczne,
- Nie otwieraj plików nieznanego pochodzenia,
- Wszystkie pobrane pliki skanuj programem antywirusowym,
- Nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa,
- Cyklicznie skanuj komputer oprogramowaniem antywirusowym i sprawdzaj procesy sieciowe,
- Nie odwiedzaj stron oferujących darmowe filmy, muzykę albo łatwe pieniądze – najczęściej na takich stronach znajduje się złośliwe oprogramowanie,
- Nie podawaj swoich danych osobowych na stronach internetowych, co do których nie masz pewności, że nie są one widoczne dla osób trzecich,
- Zawsze weryfikuj adres nadawcy wiadomości e-mail,
- Zawsze zabezpieczaj hasłem lub szyfruj wiadomości e-mail zawierające poufne dane – hasło przekazuj innym sposobem komunikacji,
- Cyklicznie wykonuj kopie zapasowe ważnych danych,
- Zawsze miej włączoną – zaporę sieciową „firewall"
- Nie uruchamiaj linków w wiadomościach SMS lub e-mail, jeżeli nie masz pewności,że pochodzą z bezpiecznego źródła,
- Zwracaj uwagę na komunikaty wyświetlane na ekranie komputera,

Zgłaszanie incydentów

Każdy pacjent, osoba odwiedzająca pacjentów w przypadku zauważenia:

- próby przełamania zabezpieczeń, próby nieautoryzowanego wejścia na chroniony obszar szpitala;
- powzięcia wątpliwości co do stanu technicznego urządzeń informatycznych, na których przetwarzane są dane osobowe w szpitalu;
- innych budzących wątpliwości w zakresie przestrzegania bezpieczeństwa informacji, a mogących wpłynąć na świadczenie usług, proszony jest o zgłoszenia niezwłocznie zaobserwowanej sytuacji na adres e-mail: it@szpital-marciniak.wroclaw.pl.