Ustawa o krajowym systemie cyberbezpieczeństwa

1 sierpnia 2018 r. Prezydent RP podpisał ustawę o krajowym systemie cyberbezpieczeństwa, implementującą do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. Dyrektywa NIS. Ustawa została opublikowana w Dzienniku Ustaw RP 13 sierpnia br. i zacznie obowiązywać po 14 dniach od jej ogłoszenia tj. od 28 sierpnia br. Pełne wdrożenie Dyrektywy NIS wymaga ponadto przyjęcia dwóch rozporządzeń Rady Ministrów: w sprawie uznania incydentu za poważny, jak i w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

Celem przygotowanej przez Ministerstwo Cyfryzacji ustawy o krajowym systemie cyberbezpieczeństwa było opracowanie uregulowań prawnych umożliwiających implementacje dyrektywy NIS oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym.

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w szczególności :

* niezakłóconego świadczenia usług kluczowych i usług cyfrowych
* osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług.

Budowany system obejmuje operatorów usług kluczowych (m.in.: z sektora energetycznego, transportowego, zdrowotnego i bankowości), dostawców usług cyfrowych, zespoły CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa oraz pojedynczy punkt kontaktowy do komunikacji w ramach współpracy w Unii Europejskiej w dziedzinie spraw cyberbezpieczeństwa. 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.

Do krajowego systemu cyberbezpieczeństwa będą również włączone organy administracji publicznej, a także przedsiębiorcy telekomunikacyjni – w sposób zharmonizowany z istniejącymi uregulowaniami w tym zakresie.

Wymaganiami z zakresu cyberbezpieczeństwa zostali także objęci dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Z racji międzynarodowej specyfiki tych podmiotów, obowiązki dla dostawców usług cyfrowych są objęte zharmonizowanym na poziomie UE reżimem regulacyjnym. Ustawa odwołuje się tutaj do decyzji wykonawczej Komisji Europejskiej.

Szpitale Pomorskie Sp. z o.o., zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) zapewnienia pacjentom oraz podmiotom współpracującym dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami kluczowymi.

Do najważniejszych grup obowiązków operatora usługi kluczowej należą:

* zarządzanie ryzykiem (w tym szacowanie ryzyka) Maksymalnym interwałem pomiędzy kolejnymi szacowaniami ryzyka jest jeden rok. Szacowanie ryzyka odbywa się również w przypadku zaistnienia zmian organizacyjnych, lokalowych lub po incydencie wewnątrz podmiotu świadczącego usługę cyberbezpieczeństwa.;
* wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym utrzymanie i bezpieczną eksploatację systemu informacyjnego; bezpieczeństwo fizyczne i środowiskowe; bezpieczeństwo i ciągłość dostaw; wdrażanie, dokumentowanie i utrzymywanie planów działania);
* zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty;
* obsługa incydentów i współpraca w tym zakresie z właściwym CSIRT; wyznaczenie osoby kontaktowej na potrzeby KSC.

Szpitale Pomorskie Sp. z o.o. wdrożyły i eksploatują system zarządzania bezpieczeństwem informacji w oparciu o wymagania międzynarodowego standardu ISO/IEC 27001.

W Szpitalach Pomorskich Sp. z o.o. ochronę fizyczną zapewniają systemy kontroli dostępu, systemy CCTV, systemy przeciwpożarowe. Ponadto stworzono procedury alarmowe na wypadek zagrożeń różnego rodzaju.

Szpitale Pomorskie Sp. z o.o. posiadają redundantne zabezpieczenia na wypadek zakłóceń lub utraty zasilania. Zgłaszanie awarii służbom technicznym i serwisowym jest określone i przetestowane.

Wszystkie systemy IT projektuje się tak aby zapewnić redundantność elementów infrastruktury, a także poufność, integralność, dostępność, autentyczność, niezaprzeczalność i rozliczalność w korzystaniu z systemów przechowywania i przetwarzania informacji.

Wdrożono zabezpieczenia minimalizujące ryzyko pozyskania przez osoby niepowołane informacji o zdrowiu swoich pacjentów.

Połączenie pomiędzy systemami IT zbudowano tak aby zapewnić redundancję oraz bezpieczeństwo przesyłanych danych. Szpitale Pomorskie Sp. z o.o. korzystają 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.

Zapraszamy do zapoznania się z materiałami o bezpieczeństwie, przygotowanymi przez Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej).

<https://www.cert.pl/publikacje/>

Źródła:

<https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo>

<https://www.su.krakow.pl/strefa-pacjenta/cyberbezpieczenstwo>