Oświadczenie złożone
przez senatora Wojciecha Koniecznego
na 45. posiedzeniu Senatu
w dniu 30 czerwca 2022 r.

Oświadczenie skierowane do ministra zdrowia Adama Niedzielskiego

Szanowny Panie Ministrze!

Z przekazanych placówkom medycznym informacji wynika, że z powodu większego ryzyka wystąpienia wzmożonych ataków w cyberprzestrzeni, w tym na placówki medyczne, Ministerstwo Zdrowia we współpracy z Kancelarią Prezesa Rady Ministrów wdroży rozwiązania mające zagwarantować prawidłowy poziom bezpieczeństwa systemów informatycznych, za pośrednictwem których udzielane są świadczenia opieki zdrowotnej. Z przekazanych informacji wynika także, że podmioty medyczne będą mogły otrzymać specjalne fundusze na sfinansowanie budowy infrastruktury cyberbezpieczeństwa, systemów umożliwiających wykonywanie kopii zapasowych oraz odtworzenie infrastruktury po ewentualnej awarii lub ataku w cyberprzestrzeni czy też audyt bezpieczeństwa, którego wynik będzie stanowił podstawę wypłaty refundacji poniesionych wydatków. Wysokość środków dla danego podmiotu będzie uzależniona od wysokości posiadanego kontraktu z NFZ na 2021 r., w związku z czym wspomniane finansowanie pokryje tylko nieznaczny procent faktycznego finansowania placówek niezbędnego do zapewnienia odpowiedniego poziomu cyberbezpieczeństwa.

Jednocześnie w związku z ustawą o krajowym systemie cyberbezpieczeństwa podmioty uznane za operatorów usług kluczowych w momencie otrzymania od organu właściwego decyzji administracyjnej są jako operator usługi kluczowej zobowiązane do następujących działań.

1. W terminie 3 miesięcy od dnia otrzymania decyzji od organu właściwego operator dokonuje szacowania ryzyka dla swoich usług kluczowych, zarządza incydentami, wyznacza osobę kontaktową z właściwym CSIRT i organem właściwym do spraw cyberbezpieczeństwa, prowadzi działania edukacyjne wobec użytkowników, obsługuje incydenty we własnych systemach, zgłasza incydenty poważne, usuwa wskazywane podatności.

2. W terminie 6 miesięcy od dnia otrzymania decyzji operator wdraża odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne, zbiera informacje o zagrożeniach i podatnościach, stosuje środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego, stosuje wymaganą dokumentację.

3. W terminie 12 miesięcy od dnia otrzymania decyzji operator przygotowuje pierwszy audyt w rozumieniu ustawy, przekazuje sprawozdanie z audytu wskazanym w ustawie podmiotom.

Jednocześnie za niewykonanie wymienionych obowiązków wynikających z ustawy przewidziano zastosowanie kar finansowych.

Wymienione wymagania wiążą się z koniecznością bieżącego finansowania np. utworzenia dodatkowych etatów dla pracowników/specjalistów wdrażających i obsługujących kwestie związane z cyberbezpieczeństwem oraz zakupu sprzętu i oprogramowania wartego kilkukrotnie więcej, niż przewiduje zarządzenie nr 68/2022/BBIICD prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.

W związku z tym proszę Pana Ministra o odniesienie się do przedstawionego problemu i odpowiedź na pytanie, jakie rząd przewiduje źródła finansowania dla zakupów oraz działań bieżących niezbędnych do wdrożenia i utrzymania wymaganego poziomu cyberbezpieczeństwa w placówkach uznanych za operatora usługi kluczowej.

Wojciech Konieczny