Warszawa, dnia 21 listopada 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.152.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 2 listopada 2017 r. Posła na Sejm RP Pana Arkadiusza Marchewki w sprawie *transpozycji dyrektywy PE dotyczącej bezpieczeństwa sieci i systemów informatycznych* (interpelacja nr 16664)

Szanowny Panie Marszałku,

według danych szacunkowych opracowanych przez Ministerstwo Cyfryzacji w ramach oceny skutków regulacji projektu ustawy o krajowym systemie cyberbezpieczeństwa, obowiązkiem stosowania norm dyrektywy NIS[1] objętych zostanie w Polsce około 330 podmiotów, które otrzymają status operatorów usług kluczowych.

Prawdopodobni operatorzy usług kluczowych będą reprezentować:

- sektor energetyczny (około 46 podmiotów), w tym operatorów sieci przesyłowej, operatora ropociągów, przedsiębiorstwa zajmujące się wydobyciem, przetwarzaniem, magazynowaniem i przesyłem ropy naftowej, przedsiębiorstwa dostarczające gaz, operatorów systemu dystrybucji oraz m.in. systemu magazynowania;
- sektor transportowy (około 70 podmiotów), takich jak PLL LOT, zarządców największych portów lotniczych, zarządców infrastruktury kolejowej, kolejowe przedsiębiorstwa pasażerskie oraz towarowe, a także największych armatorów, organy zarządzające portami morskimi i śródlądowymi oraz związane z podsektorem transportu drogowego, m.in. GDDKiA oraz samorządy wojewódzkie;
- sektor bankowy i infrastruktury rynków finansowych (47 podmiotów), w tym duże banki, operator systemu obrotu, czyli Giełda Papierów Wartościowych S.A. i jej spółki zależne, oraz kontrahenci centralni (KIR);
- sektor związany ze służbą zdrowia (około 131 podmiotów), będą to szpitale i zakłady lecznicze zarówno z sektora publicznego jak i prywatnego, w tym te prowadzone

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*.

przez NGO (za czynnik decydujący o objęciu regulacją wstępnie uznano wskaźnik hospitalizacji powyżej 18 000 pacjentów rocznie);

- sektor związany z przedsiębiorstwem wodno-kanalizacyjne (około 31 podmiotów) z sektora zaopatrzenia w wodę i jej dystrybucji;
- sektor infrastruktury cyfrowej (około 10 podmiotów).

Zgodnie z treścią projektu ustawy[2], przedstawionego przez Ministerstwo Cyfryzacji, uznanie podmiotu za operatora usługi kluczowej następuje, jeżeli podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych. Wykaz określony zostanie przez Radę Ministrów w drodze rozporządzenia, z podziałem na sektory i podsektory wymienione w załączniku do ustawy, kierując się znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej. Wyznaczanie operatorów usług kluczowych będzie następowało w drodze decyzji. Okres realizowania poszczególnych obowiązków będzie wynosił od trzech do sześciu miesięcy od momentu otrzymania decyzji.

W projekcie ustawy zawarto przepisy o karach pieniężnych, nakładanych przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora[3].

- kara w wysokości do 100 000 zł grozi operatorowi usług kluczowych, który nie wdrożył systemu zarządzania bezpieczeństwem;
- kara w wysokości do 50 000 zł grozi operatorowi usług kluczowych, który nie opracował dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, w ciągu sześciu miesięcy od otrzymania decyzji o uznaniu za operatora usługi kluczowej, a także nie wykonuje zobowiązań identyfikacji incydentu, jego rejestracji, zgłoszenia, oraz zapewnienia obsługi incydentu zwykłego, lub poważnego bądź krytycznego, we współpracy z właściwym CSIRT poziomu krajowego (Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego). Taki sam wymiar kary pieniężnej jest przewidziany w przypadku, gdy operator co najmniej raz na dwa lata nie przeprowadził audytu bezpieczeństwa teleinformatycznego, nie realizuje wiążących poleceń wprowadzenia środków zaradczych zleconych przez właściwy organ lub nie usunął w wyznaczonym terminie nieprawidłowości stwierdzonych w wyniku kontroli;
- kara w wysokości do 10 000 zł grozi operatorowi usług kluczowych, który nie wyznaczy osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych;

[2] art. 5 ust. 2 pkt 1 projektu ustawy o krajowym systemie cyberbezpieczeństwa
[3] o którym mowa w art. 38 w/w projektu

- kara w wysokości do 5 000 zł grozi operatorowi usług kluczowych, który uniemożliwi lub utrudni osobie przeprowadzającej czynności kontrolne;
- kara w wysokości 1 000 zł grozi operatorowi usług kluczowych, który nie poinformował organu właściwego o zmianie jego danych wpisanych do wykazu operatorów usług kluczowych w terminie 14 dni od zmiany tych danych.

Ministerstwo Cyfryzacji nie posiada informacji o planowanych działaniach wymienionych spółek. Jednocześnie wyrażamy pełne poparcie dla wszelkich inicjatyw, które podwyższą poziom cyberbezpieczeństwa w różnych sektorach gospodarki i staramy się wspierać ich realizację.

Warto zaznaczyć, że projekt ustawy umożliwi również tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach[4], które umożliwią współpracę m.in. obecnym partnerom Narodowego Centrum Cyberbezpieczeństwa[5]. Partnerzy NC Cyber wymieniają się informacjami o zagrożeniach i prowadzą wspólne przedsięwzięcia dotyczące cyberbezpieczeństwa. Jest to struktura oparta na kooperacji i dobrowolności, która będzie uzupełniać podstawowy system określony w ustawie. Jest też możliwe, aby inne podmioty prywatne i publiczne, dołączały do NC Cyber.

Z wyrazami szacunku,
Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów

[4] art. 28 ust. 6 pkt 5 w/w projektu
[5] znajdującego się w strukturze NASK – dalej jako NC Cyber