Warszawa, dnia listopada 2017 r.

MINISTER OBRONY NARODOWEJ
Nr 200/1251-2/17/MTK

MINISTER CYFRYZACJI
Pani Anna STREŻYŃSKA

Szanowna Pani Minister,

W odpowiedzi na pismo Pani Minister Nr DP-III.0211.16.2017 z dnia 31 października 2017 r., dotyczące zaopiniowania ***projektu ustawy o krajowym systemie cyberbezpieczeństwa***, uprzejmie informuję, że resort obrony narodowej opiniuje negatywnie przedstawiony projekt oraz zgłasza poniższe zastrzeżenia:

1. Projekt ustawy skupia się na implementacji dyrektywy 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, natomiast krajowy system cyberbezpieczeństwa jest zagadnieniem bardziej obszernym, które wymaga nie tylko precyzyjnej regulacji i opisu tworzących go procesów, ale przede wszystkim uwzględnienia roli przedmiotów go tworzących, m. in. Ministra Obrony Narodowej w procesie nadzoru nad cyberobroną państwa.
2. W projekcie ustawy brakuje jednoznacznego podziału obszarów odpowiedzialności. Podmiotem odpowiedzialnym za sferę militarną krajowego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej powinien być wyraźnie wskazany Minister Obrony Narodowej.
3. Projekt nie uwzględnia funkcjonowania krajowego systemu cyberbezpieczeństwa w stanach nadzwyczajnych i w czasie wojny, w którym odpowiedzialność za cały krajowy system cyberbezpieczeństwa przejmuje Minister Obrony Narodowej.
4. W projekcie ustawy zbyt wiele uprawnień zostało przypisanych ministrowi właściwemu do spraw informatyzacji, który nie dysponuje potencjałem umożliwiającym ich realizację. Z tego względu, uzasadnione jest przypisanie tych kompetencji podmiotom lub organom posiadającym odpowiednie siły i środki, np. Ministrowi Obrony Narodowej, Ministrowi Spraw Wewnętrznych i Administracji, czy Rządowemu Centrum Bezpieczeństwa.
5. W projekcie nie sformułowano definicji krajowego systemu cyberbezpieczeństwa. Opracowanie definicji krajowego systemu cyberbezpieczeństwa powinno być poprzedzone fazą analityczną, w ramach której określonoby wszystkie jego elementy, ich wzajemne relacje oraz procesy zachodzące między nimi.

6. Projekt ustawy uwzględnia przede wszystkim działania reaktywne – skupia się na zarządzaniu incydentami, a jedynie szczątkowo wspomina kwestie związane z zarządzaniem ryzykiem, szczególnie na poziomie krajowym.
7. W projekcie brak definicji istotnych z punktu widzenia ustawy, a używane pojęcia zdefiniowane są nieprecyzyjnie, co utrudnia analizę i stosowanie przepisów ustawy.
8. Treść art. 38 ust. 1 pkt 7 projektu ustawy wkracza w zakres kompetencyjny Ministra Obrony Narodowej. Niezbędnym jest wyłączenie wojskowej infrastruktury cyfrowej z zakresu tego przepisu.
9. Ustawa powinna brać pod uwagę model etapowego (np. w okresie kilkuletnim) wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa. Aktywizację krajowego sektora cyberbezpieczeństwa należy powiązać z rozwojem krajowej gospodarki (również w obszarze cyberobronności), zgodnie ze „Strategią Zrównoważonego Rozwoju Polski do 2025 roku".
10. Projekt nie zabezpiecza rozwoju polskiej technologii w obszarze cyberbezpieczeństwa. W krajowym systemie cyberbezpieczeństwa powinny być uwzględnione działania powodujące stymulację rozwoju innowacyjności polskiego sektora technologii informacyjno-komunikacyjnych, np. poprzez promowanie używania cybernarzędzi wytworzonych przez krajowe przedsiębiorstwa.
11. W ustawie oprócz kar dla podmiotów zobowiązanych do informowania o incydentach, należałoby także przewidzieć szerszą ochronę ich interesów w kontekście zwiększonej odpowiedzialności wynikającej ze zgłoszenia incydentu.
12. Projekt ustawy nie przewiduje współpracy z organizacjami innymi niż Unia Europejska. Projekt wymaga uzupełnienia o regulacje dotyczące „Narodowego Punktu Kontaktowego" do współpracy z NATO i wskazanie organu kompetentnego w tym zakresie, tj. Ministra Obrony Narodowej.
13. Stworzenie krajowego systemu cyberbezpieczeństwa wymaga zmian w innych ustawach z uwagi na zachowanie żywotnych interesów bezpieczeństwa państwa, co nie zostało ujęte w przedmiotowym projekcie.

Ponadto uprzejmie informuję, że w ramach spotkań międzyresortowego zespołu roboczego w Ministerstwie Cyfryzacji (m in. z udziałem MON, MSWiA, MSZ, MS, MZ, MNiSW) oraz spotkań zespołu roboczego MIL-CERT (MON), CERT.GOV.PL (ABW), CERT Polska (NASK) i RCB, zostało wskazanych szereg istotnych zagadnień koniecznych do doprecyzowania w procedowanej ustawie, a które nie zostały uwzględnione w przedstawianym projekcie, np.:

a) brak zrównania infrastruktury krytycznej i usług kluczowych ze stosownymi propozycjami zmian do ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209);
b) brak sposobu przetwarzania danych osobowych przez CSIRT (w tym poziomu krajowego);
c) w ustawie opisano inny, niż rekomendowany przez CSIRTy, sposób zgłaszania incydentów;
d) nie zidentyfikowano zadań dla poszczególnych ról w krajowym systemie cyberbezpieczeństwa;
e) nie wskazano koordynacji operacyjnej oraz strategiczno-politycznej krajowego systemu cyberbezpieczeństwa.

W związku z powyższym, w opinii resortu obrony narodowej, konieczne są dalsze prace nad projektem ustawy, z uwzględnieniem powyższy zastrzeżeń oraz stanowisk innych podmiotów zaangażowanych w proces legislacyjny.

Resort obrony narodowej pozostaje w stałej gotowości do aktywnego wsparcia tych działań.

Z poważaniem,

z up. Bartosz KOWNACKI
SEKRETARZ STANU

M.T.K. 261-871-642
T1/28/II