Stanowisko Rady do Spraw Cyfryzacji w sprawie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Opiniowana nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa (zwanej dalej UKSC) stanowi kluczowy projekt legislacyjny, który będzie definiować oraz wpływać na bezpieczeństwo cybernetyczne Polski.

Zgadzamy się z podejściem zaprezentowanym w przedmiotowym projekcie Ustawy, że sprawę cyberbezpieczeństwa Rzeczypospolitej Polskiej należy rozpatrywać w perspektywie szerszej niż tylko krajowego rynku telekomunikacyjnego. Obejmuje ona bowiem również inne istotne kwestie, takie jak stosunki między państwami, bezpieczeństwo narodowe czy równie ważne bezpieczeństwo obecnych i przyszłych użytkowników sieci piątej generacji – a w szczególności bezpieczeństwo ich danych i praw własności intelektualnej. Cyfrowe bezpieczeństwo ma dziś wyjątkowe znaczenie ze względu na właściwości budowanej sieci 5G oraz związanych z nią perspektyw rozwoju Przemysłu 4.0, opartego na Internecie Rzeczy (IoT) oraz Sztucznej Inteligencji (AI).

Rada wyraźnie podkreśla, że **Ustawa nie jest skierowana przeciwko jakiejkolwiek firmie z jakiegokolwiek państwa** na świecie. Jednak należy pamiętać, że Polska musi posiadać stosowne instrumenty prawne do ochrony swojej cyberprzestrzeni w całym obszarze gospodarki – ze szczególnym uwzględnieniem sektora publicznego, infrastruktury krytycznej i telekomunikacji. Uważamy, że dyskusji nie powinien podlegać fakt, że bezpieczeństwo narodowe jest dobrem nadrzędnym.

Rada ds. Cyfryzacji z zadowoleniem przyjmuje projekt nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa, który zawiera zapisy spełniające postulaty opisane w Stanowisku Rady ds. Cyfryzacji dotyczące rozwoju technologii 5G w Polsce w kontekście cyberbezpieczeństwa (PDF), w którym Rada uznała za konieczne m.in.: *„wprowadzenie oceny wiarygodności operatorów oraz dostawców sieci 5G i dostawców sprzętu dla sieci 5G – ocena możliwych zależności natury prawnej, organizacyjnej i finansowej”*.

Przyjęte w proponowanych nowych artykułach 66a - 67c UKSC mechanizmy niwelowania zagrożeń – zwłaszcza ze strony obcych państw – stanowią także wypełnienie celu zawartego w przyjętej na wniosek Prezesa Rady Ministrów i zatwierdzonej w maju b.r. przez Prezydenta Rzeczypospolitej Polskiej „Strategii Bezpieczeństwa Rzeczypospolitej Polski”, a w szczególności zawartej w I Filarze „Cyberbezpieczeństwo”. Punkt 4.1 nakazuje, by *„zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia”*. Polska musi posiadać instrumenty prawne niwelujące ryzyka zagrożeń związanych z możliwościami wykorzystywania technologii pochodzących od tzw. Dostawców Wysokiego Ryzyka, nie tylko np. w zakresie telekomunikacji 5G i kolejnych generacji.

Podobne mechanizmy bezpieczeństwa zastosowało już w ślad za Stanami Zjednoczonymi kilka kolejnych państw Europy Zachodniej i w różnych segmentach nowych technologii.

Przewidziane w projektowanych nowych art. 66a - 67c UKSC kompetencje Kolegium ds. Cyberbezpieczeństwa oraz Pełnomocnika ds. Cyberbezpieczeństwa wyposażają organy państwa w kompetencje pozwalające na zapobieganie zagrożeniom ze strony dostawców sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa w oparciu o Ocenę Ryzyka sporządzaną przez Kolegium do spraw cyberbezpieczeństwa i eliminowanie produktów stanowiących podwyższone lub wysokie ryzyko. Ocena Ryzyka winna brać pod uwagę takie czynniki, jak: analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania oraz ocenę, jakie prawdopodobieństwa, że dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego (art.66 a ust.4). Projekt ustawy wyposaża także pełnomocnika Rządu ds. Cyberbezpieczeństwa w prawo do operacyjnego działania w warunkach zagrożeń obejmujące wydawanie wiążących (art.67 a projektu):

1) ostrzeżeń – w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego lub
2) poleceń zabezpieczających – w przypadku wystąpienia incydentu krytycznego – po zatwierdzeniu przez Kolegium.

Rada z zadowoleniem przyjmuje fakt, że w projekcie UKSC uwzględniono kwestię, na którą uwagę zwracała Rada także w pracach nad projektem rozporządzenia o bezpieczeństwie sieci 5G, a mianowicie, że Polska brała udział w opracowaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G („5G Toolbox"), który ma ograniczyć cyber-ryzyka dla europejskich sieci piątej generacji. W uzasadnieniu do projektu UKSC przypomniano, że *„państwa członkowskie UE zobowiązały się w 5G Toolbox w szczególności do: zaostrzenia wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych, oceniania profili ryzyka dostawców, stosowania odpowiednich ograniczeń w odniesieniu do dostawców stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe oraz wdrożenia strategii mających na celu zapewnienie dywersyfikacji dostawców w celu unikania uzależnienia od dostawców stwarzających wysokie ryzyko. Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia postanowień tego dokumentu"*.

Uważamy jednak, że stosowanie środków przewidzianych w projekcie UKSC, zwłaszcza tych najostrzejszych musi być poprzedzone nie tylko analizą ryzyk, ale realną oceną kosztów opartych o wiarygodne informacje, w tym także audyty zwłaszcza w takich obszarach, jak sieci

szerokopasmowe, edukacyjne czy sieci technologiczne (OT). Z zadowoleniem przyjmujemy fakt, że projekt opiniowanej Ustawy przewiduje cały zespół różnych środków w zależności od wynikającego z analizy zagrożenia.

Za bardzo wartościowe uznajemy także wprowadzanie do polskiego systemu cyberbezpieczeństwa, takich instytucji i mechanizmów, jak:

- Operacyjnych centrów bezpieczeństwa**,** czyli SOC oraz doprecyzowanie zadań i roli SOC w systemie cyberbezpieczeństwa RP;
- Rozszerzenie i doprecyzowanie roli CSIRT, w tym wprowadzenie CSIRTów sektorowych;
- Powołanie **„**CSIRT telco**”** dla branży telekomunikacyjnej;
- Stworzenie ISAC, czyli specjalistycznych organizacji, dzięki którym podmioty Krajowego Systemu Cyberbezpieczeństwa będą miały możliwość bieżącej wymiany informacji o incydentach, zagrożeniach, podatnościach oraz dobrych praktykach. ISAC usprawnią także współpracę podmiotów z zespołami CSIRT poziomu krajowego, co zapewni koordynację komunikacji postulowaną przez środowisko IT;
- Koordynacja zadań z zakresu cyberbezpieczeństwa na poziomie województw – przy czym Rada uznaje za konieczne bardzo poważne wzmocnienie zasobów Wojewodów w tym zakresie.

Ponadto Rada stoi na stanowisku, że Polska powinna rozwijać produkty i usługi telekomunikacyjne z wykorzystaniem potencjału firm działających w Polsce, w tym w szczególności rozwijać własne projekty takie jak #Polskie5G czy model oparty o OPEN RAN. Tylko w ten sposób nie dopuścimy do sytuacji uzależnienia od jednego dostawcy, co jest także w interesie bezpieczeństwa narodowego.

Rada wyraża również nadzieję, że mimo trwającej pandemii w budżecie państwa zostaną przewidziane dostateczne środki na realizacje dodatkowych zadań wynikających z projektowanej Ustawy.

Józef Orzeł
Przewodniczący Rady
/podpisano elektronicznie/