PROTOKÓŁ z V posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 14 maja 2021 roku, o godzinie 13:00 w formie wideokonferencji.

Dyskusja nad agendą Rady.

Kierownicy Zespołów poinformowali o spotkaniach z liderami grup roboczych oraz o stanie prac zespołów.

Dyrektor Departamentu Architektury Informacyjnej Państwa Pan Jacek Paziewski zgłosił wkład merytoryczny do grupy Usług Cyfrowych. Wspomniał o przygotowaniach programu odmiejscowienia usług publicznych, czyli skoordynowania sposobu i harmonogramu wytwarzania usług publicznych w różnych resortach, który będzie nadzorowany przez Radę Monitorowania Projektów Strategicznych. Został przygotowany plan wdrażania usług publicznych nowej generacji z wykorzystaniem komponentów funkcjonalnych i architektonicznych.

Spotkanie z Panem Robertem Koślą, Dyrektorem Departamentu Cyberbezpieczeństwa KPRM na temat etapu prac nad ustawą o Krajowym Systemie Cyberbezpieczeństwa.

Głównym celem prac nad nowelizacją ustawy o Krajowym Systemie Cyberbezpieczeństwa jest efektywność regulacji, przejrzystość, jak również prostota w stosowaniu. Pan Dyrektor Robert Kośla przedstawił aktualny stan prac nad ustawą o Krajowym Systemie Cyberbezpieczeństwa odnosząc się do procesu legislacyjnego. Do tej pory dokument został przyjęty przez Komitet Rady Ministrów ds. Cyfryzacji oraz został zarekomendowany Stałemu Komitetowi Rady Ministrów lub właściwym komitetom z zaleceniem przeprowadzenia konsultacji. Jest również po opinii Komitetu ds. Europejskich. Po pierwszym posiedzeniu Stałego Komitetu Rady Ministrów pojawiły się rozbieżności. Zdecydowano o spotkaniu Komitetu Rady Ministrów ds. Bezpieczeństwa Narodowego i Spraw Obronnych. Komitet w trybie niejawnym dyskutował o zaistniałych rozbieżnościach, które dotyczyły głównie funkcjonowania zakresu usług i obligatoryjności korzystania z usług operatora strategicznej sieci bezpieczeństwa. Nie ma natomiast rozbieżności co do sposobu identyfikacji, sposobu uznawania dostawców za dostawców wysokiego ryzyka. Nie pojawiły się także wątpliwości dotyczące nowych mechanizmów prawnych takich jak ostrzeżenie czy polecenie zabezpieczające. Duże wsparcie ze strony Komitetu uzyskała koncepcja stworzenia zespołów analitycznych. W przygotowaniu znajduje się rozszerzona koncepcja, która pierwotnie zakładała powstanie Krajowego Centrum Analitycznego wspierającego pełnomocnika rządu w zakresie analizy predykcyjnej zagrożeń, które będzie również zbierało i przygotowywało materiał dotyczący bezpieczeństwa łańcucha dostaw.

Uwaga, która została uwzględniona w wersji projektu ustawy o KSC zgłoszona przez Ministerstwo Obrony Narodowej, dotyczyła postępowania w sytuacjach szczególnych zagrożeń - z jednej strony niekwestionowanej konieczności wyasygnowania i lepszej koordynacji w sytuacji bardzo poważnego zagrożenia dla Krajowego Systemu Cyberbezpieczeństwa. Jednym z argumentów podnoszonych w trakcie dyskusji była kwestia, na ile tego typu sytuacja, czyli zewnętrzne zagrożenie bezpieczeństwa jest związane z

definicją, która jest już w ustawie o stanie wojennym. Precyzyjnie sformułowano, że w sytuacji, gdy istnieje zagrożenie, które jest podstawą do ogłoszenia stanu wojennego, koordynację będzie przejmowało Ministerstwo Obrony Narodowej i struktury podległe Ministrowi Obrony Narodowej, czyli CSIRT MON. Ta uwaga znajdzie się w wersji projektu ustawy o KSC, która zostanie przedłożona po raz kolejny na posiedzeniu Stałego Komitetu Rady Ministrów.

Pan Dyrektor zwrócił uwagę, iż równolegle do tego, wprowadzono nowy mechanizm, tj. art. 36 a, który umożliwia Prezesowi Rady Ministrów wnioskowanie do Ministra Obrony Narodowej o wskazanie/udostępnienie podległych mu podmiotów i instytucji do bezpośredniego reagowania na sytuację kryzysową bez ogłoszenia stanu wojennego. Taka propozycja będzie przedmiotem dyskusji na posiedzeniu Rządowego Zespołu Zarządzania Kryzysowego. Poinformowano, że trwają dyskusje dotyczące kwestii operatora strategicznej sieci bezpieczeństwa. Wcześniej pojawiły się postulaty, aby określić zakres usług i w tej chwili prawdopodobnie ten zakres usług jest doprecyzowywany – znajdzie się delegacja w rozdziale dotyczącym operatora strategicznej sieci bezpieczeństwa do wydania rozporządzenia bądź przez Prezesa Rady Ministrów bądź Radę Ministrów dotyczącego katalogu usług podstawowych świadczonych przez operatora strategicznej sieci bezpieczeństwa i usług, które będą jednocześnie podstawowe, czyli minimalne chociażby w zakresie transmisji danych, głosu czy obrazu. Dla potrzeb procesów obronności, zarządzania kryzysowego w tym rozporządzeniu należałoby ująć listę podmiotów, które obowiązkowo z tych usług powinny korzystać, aby zapewnić interoperacyjność i możliwość współdziałania w sytuacji kryzysowej. Ta propozycja będzie musiała zostać zatwierdzona i przyjęta przez Komitet ds. Bezpieczeństwa Narodowego i Spraw Obronnych. Wtedy formalnie usunięcie tych rozbieżności będzie potwierdzone ponownie na posiedzeniu Stałego Komitetu Rady Ministrów, po którym dokument będzie równolegle przedłożony Radzie Ministrów. Zostanie także opiniowany przez Radę Legislacyjną. Wskazano, że utrzymywany jest kontakt z Rządowym Centrum Legislacji, aby niezwłocznie w sytuacji potwierdzenia wersji projektu ustawy o KSC przez Stały Komitet Rady Ministrów, Rada Legislacji dokonała przeglądu poprawności legislacyjnej projektu, tak aby dokument jeszcze w tym miesiącu trafił na Radę Ministrów, a w przypadku braku dodatkowych rozbieżności, aby projekt został przyjęty i przekazany do parlamentu.

Wskazano, że na bieżąco dokonywany jest monitoring regulacji w innych państwach w zakresie 5G. Utrzymywane są bilateralne kontakty z państwami członkowskimi, a także przeprowadzane konsultacje w zakresie rozwiązań prawnych.

Pojawiło się pytanie odnośnie planów w zakresie przepisów do projektu ustawy o KSC zmieniających obsługę incydentów.

Wskazano, że trwa dyskusja, na ile i jakie mechanizmy powinny być wprowadzane bezpośrednio w ustawie, jakie rozwiązania powinny być wprowadzone w formie wytycznych i rekomendacji pełnomocnika rządu dla podmiotów. Ogólne wymaganie ustawowe odnosi się do realizacji procesu zarządzania i funkcjonowania systemu zarządzania

bezpieczeństwem informacji. Jednym z jego elementów jest zbieranie i analiza logów. Dla KSC zostaną przygotowane wytyczne/rekomendacje pełnomocnika rządu w tym zakresie. Wskazano, że zmiany nakierowane są na przygotowanie dobrych praktyk, tworzenie dodatkowych struktur operacyjnych, które mają na celu zwiększenie świadomości sytuacyjnej, wzmocnienie zespołów SOC u poszczególnych operatorów usług kluczowych. Jedną z głównych funkcji zespołu operacyjnych centrów bezpieczeństwa jest zbieranie i analiza logów oraz posiadanie systemów, które automatyzują ten proces – chodzi o skuteczne rozwiązania automatyzujące ten proces przy minimalnych zasobach kadrowych, które w większości przedsiębiorstw aktualnie występują, stąd zaplanowano inwestycje ujęte i wpisane do Krajowego Planu Odbudowy oraz zaproponowane w ramach REACT-EU. Trzeci obszar interwencji i finansów to obszar Funduszy Europejskich na Rozwój Cyfrowy. Wypracowywane są najlepsze praktyki i standardy, a równolegle - inwestycje i programy, które mają wesprzeć najmniejsze jednostki samorządu terytorialnego, współpracę z urzędami marszałkowskimi, program regionalnych SOC-ów, które będą mogły wspierać jednostki samorządu i podmioty podległe oraz dołączanie tych podmiotów do systemu S46. Trwa natomiast dyskusja dotycząca dostępu do danych w zakresie reagowania na incydenty - w jaki sposób te regulacje ująć w ramach RODO oraz innych tajemnic prawnie chronionych.

W toku dyskusji Pan Dyrektor R. Kośla wskazał, że notyfikacja Komisji Europejskiej ustawy o KSC będzie przebiegała równolegle z procesem legislacyjnym w parlamencie. Wspominał także o harmonizacji prac nad ustawą Prawo komunikacji elektronicznej oraz nowelizacją ustawy o KSC. Zwrócił także uwagę na trzecią ustawę łączącą dwie ww. ustawy tj. ustawę wprowadzającą Prawo komunikacji elektronicznej - po nowelizacji ustawy o KSC będą dokonywane zmiany w Krajowym Systemie Cyberbezpieczeństwa harmonizujące ją w pełni z Prawem komunikacji elektronicznej.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Konrad Ciesiołkiewicz
4. Janusz Cieszyński – Wiceprzewodniczący
5. Andrzej Dulka
6. Agnieszka Gryszczyńska
7. Michał Kanownik
8. Karol Krawczyk
9. Anna Beata Kwiatkowska
10. Mirosław Maj
11. Dariusz Milka
12. Aleksandra Musielak
13. Józef Orzeł - Przewodniczący
14. Bolesław Piasecki
15. Paweł Śniatała
16. Robert Trętowski
17. Mateusz Tykierko
18. Małgorzata Zakrzewska
19. Marcin Zarzecki

Zaproszeni goście:

20. Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa w KPRM
21. Przemysław Sypniewski, ekspert Rady
22. Wiesław Paluszyński, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

23. Jacek Paziewski, Dyrektor Departamentu Architektury Informacyjnej Państwa w KPRM
24. Monika Skrzyńska, Zastępca Dyrektora Departamentu Architektury Informacyjnej Państwa w KPRM
25. Katarzyna Staromłyńska-Gójska, KPRM

26. Anna Supeł, KPRM
27. Joanna Laskowska, KPRM