PROTOKÓŁ z XIII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 10 maja 2024 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

Cyberbezpieczeństwo – przedstawienie aktualnych działań Ministerstwa Cyfryzacji oraz omówienie propozycji tematów współpracy Rady ds. Cyfryzacji z Ministerstwem:

Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji; Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji; Krzysztof Silicki, lider zespołu roboczego RdC ds. cyberbezpieczeństwa.

Pan Dyrektor Łukasz Wojewoda na początku swojej wypowiedzi wskazał, że resort jako produkt pracy z Radą chciałby zyskać przede wszystkim działania, które nie będą duplikowały przedsięwzięć Ministerstwa. Jest kilka zagadnień, które Departament Cyberbezpieczeństwa MC planuje zaadresować do Rady. Elementem, który powoduje pewne emocje jest projekt ustawy o Krajowym Systemie Cyberbezpieczeństwa, a termin na zgłaszanie uwag do projektu w ramach konsultacji publicznych jest bardzo bliski. Kolejną kwestią jest certyfikacja – ta wynikająca z Cybersecurity Act znajdzie się w odrębnej regulacji. Departament Cyberbezpieczeństwa MC nie zamierza zamknąć się na certyfikację wynikającą z Cybersecurity Act. Jest jeszcze duże przedsięwzięcie i wyzwanie pod kątem certyfikacji osób i ich zdolności do wykonywania zadań.

Pan Dyrektor wspomniał o ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa - udało się zatrzymać grono dobrych specjalistów w administracji publicznej. Poza certyfikacją Cybersecurity Act jest także Program Certyfikacji i wytworzone centra, które potrafią certyfikować w oparciu o Common Criteria. Trwają przygotowania do Europejskiego Programu Certyfikacji – w tym zakresie Pan Dyrektor zwrócił się do Rady o pomoc, aby ośrodki, jednostki, laboratoria, które są w Polsce uczynić bardziej rozpoznawalnymi. Jeśli w ramach formuły Rady udałoby się wypracować rekomendacje czy zalecenia, które kierowałyby w stronę podmiotów krajowych, to zostałaby uzyskana obopólna wartość dodana.

Pan Dyrektor M. Wysocki zwrócił się z zapytaniem, czy Rada mogłaby oszacować w jakim kierunku powinna wyspecjalizować się jednostka certyfikująca w NASK, potencjalne jednostki certyfikujące i laboratoria. Poza Europejskim Programem Certyfikacji Cyberbezpieczeństwa, w drodze są kolejne. Z pewnością nie uda się wyspecjalizować we wszystkim, stąd pytanie w którą stronę się rozwijać – Common Criteria, chmura czy certyfikacja z zakresu sieci 5G.

Pan Dyrektor Ł. Wojewoda wspomniał o istotnej kwestii dla małych i średnich przedsiębiorstw, tj. jakie koszty podmioty te są w stanie poświęcić na ten proces. W praktyce zostały zakończone dwa przedsięwzięcia – Departament Cyberbezpieczeństwa MC zbierze doświadczenie firm, jakie nabyły w procesie certyfikacji. Pan Dyrektor wspomniał o chęci wsparcia jednostek, laboratoriów, np. Laboratorium Instytutu Łączności – wspieranie ma

odbywać się w taki sposób, by procesy certyfikacyjne, jakie się toczą i służą na rzecz Krajowego Systemu Cyberbezpieczeństwa miały zapewnioną linię optymalności dla przedsiębiorców.

Po wystąpieniu Dyrekcji Departamentu Cyberbezpieczeństwa MC, rozpoczęła się dyskusja na temat szacowania kosztów procesu akceptowalnych dla małych i średnich firm oraz o oczekiwaniach z zakresu narzędzi wsparcia, aby przekonały przedsiębiorców do wejścia w proces certyfikacji.

Pan Dyrektor Ł. Wojewoda wskazał, że słowo koszt niekoniecznie oznacza monetyzację, ale bardziej szerokie zagadnienie związane z tym w co przedsiębiorca musi zainwestować nie tylko finansowo, tak żeby certyfikacja była wykonalna i była korzystna dla jego biznesu.

Ministerstwo Rozwoju i Technologii uruchamia programy, które mają zachęcać polskich przedsiębiorców do certyfikowania się, m.in. zabierając ich w sposób bezkosztowy na różne przedsięwzięcia międzynarodowe. Są inne formy wsparcia, nie tylko bezpośrednio finansowe, które mogą zredukować koszt finalny, ale także być zachętą do podjęcia inwestycji w certyfikację.

Ponadto, podczas dyskusji poruszony został temat zachęcania firm spoza Polski do certyfikowania się w naszych instytutach, a także obszarów w jakich warto dokonać certyfikacji.

Pani Przewodnicząca zaproponowała członkom Rady zgłoszenie do organizacji reprezentowanych przez poszczególnych członków z prośbą o przygotowanie materiału w przedmiotowym temacie certyfikacji z uwagi na różną perspektywę w Radzie, który zostanie przekazany do Departamentu Cyberbezpieczeństwa MC.

Jeden z członków Rady wyraził zadowolenie, że temat certyfikacji w cyberbezpieczeństwie został podniesiony. Zauważył, że kilka lat temu był pomysłodawcą powstania w Polsce takiego systemu. W dyskusji na forach unijnych bardzo zwraca się uwagę na to, aby kraje unijne nie konkurowały między sobą ceną. Zarekomendowano, aby w wyniku prac na przecięciu się różnych interesów i strategicznych priorytetów ustalić pewien model biznesowy systemu certyfikacji w naszym kraju.

W toku dyskusji zauważono, że dobre rozeznanie dla stwierdzenia co zyskuje firma posiadając certyfikat, jest punktem wyjścia do myślenia czy proces jest opłacalny. Drugą poruszoną kwestią jest koszt świadczenia usług certyfikacyjnych. Zauważono, iż może okazać się, że koszt będzie nieakceptowalny/nieosiągalny dla najsłabszych firm. Pojawiła się propozycja, aby tematem certyfikacji zajął się zespół roboczy Rady ds. cyberbezpieczeństwa. Ponadto zaproponowano, by poprosić MRiT o informację na temat planów w zakresie wsparcia polskich firm w certyfikacji.

W dalszej części tego punktu, Pan Krzysztof Silicki - lider zespołu roboczego Rady ds. cyberbezpieczeństwa przedstawił prezentację komunikując, iż z uwagi na wielość zagadnień pochodzących od członków Rady oraz Departamentu Cyberbezpieczeństwa MC, w ramach prac zespołu powstała tabela z 24 przedmiotowymi tematami reprezentującymi różne

poziomy i oddziaływania zagadnień. Są takie, które oddziałują na cały kraj, na sektor lub kilka sektorów, na obywateli, o różnej wadze/znaczeniu i dotyczą różnych obszarów: państwo, gospodarka, społeczeństwo. Z tego względu zespół postanowił zająć się pewną priorytetyzacją tematów, a niektóre z nich wymagają doprecyzowania. Następnie Pan K. Silicki wymienił przedmiotowe tematy:

1. Wdrażanie obowiązującej i planowanej legislacji UE dotyczącej obszaru cyberbezpieczeństwa (NIS2, CER, DORA, CRA, e-IDAS2, EKŁE, CSA);
2. Wdrożenie NIS 2;
3. Cyfrowa Prezydencja - priorytety na I połowę na 2025, w zw. z polską prezydencją w RUE;
4. Synergia sfery cywilnej i militarnej w cyberbezpieczeństwie;
5. Kształcenie z zakresu cyberbezpieczeństwa (wyzwania dot. wykwalifikowanej kadry);
6. Zamówienia publiczne w cyber;
7. Zwiększanie bezpieczeństwa e-usług publicznych;
8. Krajowy schemat oceny i certyfikacji;
9. Priorytety przeciwdziałania cyberprzestępczości;
10. Ochrona przed kradzieżą tożsamości;
11. Odporność cyfrowa państwa;
12. Cyberodpowiedzialność;
13. Cyberbezpieczeństwo w bankowości (ochrona firm, konsumentów);
14. Cyberbezpieczeństwo w sektorze akademickim;
15. Ochrona prywatności użytkowników końcowych w Internecie z uwzględnieniem nowych technologii i zagrożeń;
16. Przygotowanie propozycji dotyczących obszarów i form współpracy z sektorem prywatnym;
17. Cyberbezpieczeństwo AI;
18. Wykorzystanie AI w identyfikowaniu, przewidywaniu i zwalczaniu cyberzagrożeń;
19. Zastosowanie modelu Zero Trust w administracji państwowej;
20. Sztuczna inteligencja w służbie zdrowia;
21. Przeciwdziałanie dezinformacji;
22. Blockchain w sektorze publicznym;
23. Budowa chmury rządowej.

Pan Dyrektor Ł. Wojewoda wyjaśnił, że podejście Zero Trust nie jest nowością, jednak zawsze stanowi problem wykonawczy. Należy o tym modelu myśleć jako takim, który prowadzi do zapewnienia bezpieczeństwa w każdym aspekcie.

Pan K. Silicki wspomniał o synergii pomiędzy zespołami roboczymi Rady. W innych zespołach są tematy, które dotykają cyberbezpieczeństwa: kompetencje cyfrowe, AI, chmura, kwanty, ochrona małoletnich, przeciwdziałanie cyberprzestępczości. Przedstawił również dokumenty wypełniające lub wzbogacające kontekst – legislacyjne – to projekt ustawy wdrażającej NIS 2, ale także inne dokumenty, jak np. Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa, czy dokumenty o charakterze strategicznym – Strategia Cyberbezpieczeństwa RP 2019-2024.

Pan Dyrektor Ł. Wojewoda wskazał, że trwają prace nad nową Strategią Cyberbezpieczeństwa RP. Obecnie są to wewnętrze prace w zespołach międzyresortowych. Zanim Strategia zacznie obowiązywać przejdzie przez Kolegium ds. Cyberbezpieczeństwa. Jednym z głównych elementów, który ma znaleźć się w Strategii jest pytanie jak finansować cyberbezpieczeństwo.

Pan K. Silicki omówił wkład do planowanej strategii cyfryzacji, który powstał w ramach zespołu cyberbezpieczeństwo, zawierający diagnozę sytuacji, istotność obszaru cyberbezpieczeństwa oraz stan docelowy. W efekcie w dokumencie zaproponowano szereg priorytetów strategicznych i inicjatyw - horyzontalny wymiar cyberbezpieczeństwa (wszystkie obszary gospodarki, sektory, użytkownicy usług i systemów) – analogicznie jak w samej cyfryzacji, sfera cywilna a sfera militarna obszaru cyberbezpieczeństwa, wymiar krajowy i międzynarodowy. Zdefiniowano cztery filary sukcesu obszaru cyberbezpieczeństwa:

- bieżąca praca podnosząca dojrzałość cyberbezpieczeństwa u wszystkich interesariuszy,
- analizowanie trendów cyberzagrożeń, zjawisk o charakterze przełomowym oraz foresight i badania wybiegające w przyszłość,
- systemowe budowanie i rozwój krajowych zdolności w obszarze cyberbezpieczeństwa w sposób zharmonizowany z działaniami w UE i we współpracy z innymi krajami demokratycznymi,
- walka z cyberprzestępczością.

Podstawa funkcjonowania czterech filarów to:

- współpraca interesariuszy,
- budowa zaufania - szczególnie istotny w cyberbezpieczeństwie proces o charakterze ciągłym, który ułatwia współpracę,
- systemowe kształcenie kadr – w tym punkcie oprócz prowadzonych już działań (np. ZSK) innowacyjną inicjatywą powinno być wykształcenie kadr rozumiejących w równej mierze aspekt technologiczny cyberbezpieczeństwa, jak i strategiczno-formalny (zwany: policy level), co jest rzadkością, a mogłoby się stać polską specjalnością,

pomocną w odgrywaniu kluczowej roli w kreowaniu świata cyfrowego przyszłości przez polskich ekspertów i polityków.

Kontynuując swoje wystąpienie Pan K. Silicki przedstawił rekomendację ogólną:

- Istotne jest też tworzenie, utrzymywanie, wdrażanie i ewaluacja obszarowych dokumentów strategicznych, które uszczegółowiają i operacjonalizują cele zdefiniowane w strategii „parasolowej" jaką jest lub może się stać strategia cyfrowa.
- Przykładem takich strategii obszarowych jest Strategia Cyberbezpieczeństwa RP, ale także powstawać powinny strategie dla rozwoju i wdrażania cyfrowych technologii przełomowych (np. kwantowe, AI), w których aspekt cyberbezpieczeństwa musi odgrywać należną rolę.

Pani Przewodnicząca poinformowała, że Rada przekaże swoją opinię w przedmiocie elementów, które powinny znaleźć się w Strategii Cyberbezpieczeństwa.

Sprawy różne

Pani Przewodnicząca poinformowała o zaproszeniu Pana Premiera Krzysztofa Gawkowskiego na posiedzenie Rady, które odbędzie się 28 czerwca. Na posiedzeniu liderzy zespołów Rady przedstawią efekty prac zespołów roboczych, którym przewodniczą. Pani Przewodnicząca poprosiła członków Rady o propozycje tematów, którymi Rada powinna zająć się na kolejnym posiedzeniu.

Polska prezydencja w Radzie UE – aktualizacja informacji o działaniach Ministerstwa Cyfryzacji - Piotr Kobielski, Dyrektor Departamentu Współpracy Międzynarodowej w Ministerstwie Cyfryzacji.

Pan Dyrektor Piotr Kobielski zaprezentował Radzie propozycje priorytetów polskiej prezydencji w Radzie UE. Zaznaczył, że priorytety zostaną jeszcze poddane konsultacjom społecznym. Konsultacje będą obejmować nie tylko planowane zamierzenia od 1 stycznia do czerwca 2025 r., ale również w toku konsultacji pojawi się zapytanie o ogólne działania, które instytucje unijne, a przede wszystkim Komisja Europejska zamierzają realizować przez najbliższe 4-5 lat. Pan Dyrektor wskazał, że można mówić szeroko o nowej perspektywie instytucjonalnej w UE i programowaniu tej perspektywy.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Katarzyna Chałubińska-Jentkiewicz
2. Jan Maciej Czajkowski
3. Andrzej Dulka
4. Agnieszka Jankowska – Przewodnicząca
5. Jolanta Jaworska
6. Michał Kanownik
7. Katarzyna Kopczewska
8. Jarosław Mojsiejuk
9. Krzysztof Silicki
10. Bianka Siwińska
11. Małgorzata Zakrzewska

Zaproszeni goście:

12. Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w MC
13. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
14. Piotr Kobielski, Dyrektor Departamentu Współpracy Międzynarodowej w MC

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

15. Ryszard Łuczyn, Zastępca Dyrektora Departamentu Projektów i Strategii w MC
16. Karolina Taczalska, Biuro Ministra w MC
17. Joanna Gójska, Biuro Ministra w MC