PROTOKÓŁ z V posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 26 kwietnia 2019 roku, o godzinie 11:00 w siedzibie Ministerstwa Cyfryzacji.

Spotkanie z Panią dr Elżbietą Andrukiewicz, reprezentującą Instytut Łączności – PIB, Kierownikiem Projektu KSO3C, w sprawie stanu realizacji projektu KSO3C - „Ocena bezpieczeństwa produktów, procesów i usług IT w świetle nowego Rozporządzenia Rady i Parlamentu Europejskiego dot. europejskich ram certyfikacji bezpieczeństwa".

Instytut Łączności – Państwowy Instytut Badawczy jest liderem projektu pn. *Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria* (KSO3C). Projekt został rozpoczęty 1 marca 2018 r. i jest finansowany przez Narodowe Centrum Badań i Rozwoju (NCBR). Jego celem jest stworzenie metod oraz technik ewaluacji bezpieczeństwa oraz prywatności na wysokim poziomie uzasadnienia pewności, opartych na nowatorskim podejściu do oceny podatności związanych z kształtowaniem zaawansowanych technik ataków.

Projekt jest realizowany przez Konsorcjum naukowe złożone z trzech jednostek naukowo-badawczych – są to:

- Instytut Łączności – Państwowy Instytut Badawczy (IŁ – PIB), lider projektu, który pełni rolę laboratorium świadczącego usługi ewaluacji, oceny bezpieczeństwa;
- Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB), który pełni rolę jednostki certyfikującej;
- Instytut Technik Innowacyjnych EMAG (ITI EMAG), który również pełni rolę laboratorium oceniającego.

Jednostki te stworzą system oceny i certyfikacji bezpieczeństwa i prywatności produktów i usług teleinformatycznych. Co istotne, schemat jest strukturą otwartą, w której mogą pojawiać się nowe laboratoria oceniające zgodność z Common Criteria, jeśli tylko spełnią one wymagania, jednakowe dla wszystkich laboratoriów oceniających (ITSEF), określone przez jednostkę certyfikującą z poszanowaniem zasady transparentności i bezstronności, zgodnie z przyjętymi w UE regułami oceny zgodności produktów, usług oraz procesów.

Projekt jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach Programu CyberSecIdent.

Docelowym produktem projektu będzie w pełni funkcjonująca organizacja zdolna do wydawania globalnie akceptowanych certyfikatów. Na dzień dzisiejszy Projekt KSO3C jest w stanie bardzo dynamicznego rozwoju, jest to pierwszy schemat z części nowej Europy. Planowane zakończenie projektu to pierwszy kwartał 2021r.

Projekt przygotowany został w odpowiedzi m.in. na inicjatywę Komisji Europejskiej mającą na celu utworzenie Europejskich Ram Certyfikacji Bezpieczeństwa i Prywatności dla produktów i usług (zaproponowany w Rozporządzeniu „the Cybersecurity Act").

Pani Elżbieta Andrukiewicz poruszyła temat Cybersecurity Act – tj. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) – który dotyczy (jak wskazuje sam tytuł dokumentu) dwóch kwestii:

- Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA.
- europejskich ram certyfikacji Cyberbezpieczeństwa.

Oficjalne prace nad dokumentem rozpoczęły się we wrześniu 2017r., gdy projekt został ogłoszony, uzgodnienie wersji państw członkowskich nastąpiło w czerwcu 2018r., procedura trilogu zakończyła się natomiast w grudniu ubiegłego roku. Parlament Europejski uchwalił rozporządzenie w marcu br., a 9 kwietnia br. na posiedzeniu Rady Unii Europejskiej Rozporządzenie Cybersecurity Act zostało przegłosowane (wszystkie kraje - poza Chorwacją, która wstrzymała się od głosu - głosowały „za") – obecnie dokument czeka na publikację w Dzienniku Urzędowym UE.

Najważniejszym celem tych przepisów jest unikanie fragmentacji rynku - producent, który otrzyma certyfikat cyberbezpieczeństwa w jednym kraju Unii Europejskim nie musi już zyskiwać go gdzie indziej. Certyfikat, wydany w ramach europejskiego programu certyfikacji będzie bezwzględnie uznawany we wszystkich krajach Unii Europejskiej i na całym europejskim obszarze gospodarczym. Podkreślone zostało również wygaszanie krajowych programów certyfikacji w tym samym zakresie przedmiotowym. Drugim celem przepisów jest zwiększenie zaufania rynku dla tego, co jest na tym rynku oferowane. Europejskie programy certyfikacji tworzone będą z uwzględnieniem zasad nadzoru nad rynkiem.

Co jednak istotne w niektórych przypadkach rozporządzenie będzie dopuszczało samoocenę oraz deklaracje zgodności.

Wskazane zostało, że przedmiotem certyfikacji są produkty, usługi i procesy teleinformatyczne. Badany produkt, usługa lub proces będą miały określony poziom uzasadnienia zaufania wyznaczony przez rygor i wnikliwość oceny. W Rozporządzeniu określono trzy poziomy tego zaufania. Najwyższe poziomy zaufania mają być ograniczone do tych programów certyfikacji, które będą sterowane przez jednostkę oceny zgodności będącą podmiotem publicznym (lub podmiotem prywatnym, któremu podmiot publiczny takie zadanie delegował) – chodzi o to, by poziom zaufania do oceny był jak najwyższy. Certyfikacja jest dobrowolna z zastrzeżeniem aktów dziedzinowych, chociażby dyrektywy o zamówieniach publicznych.

W europejskich ramach może funkcjonować bardzo wiele programów o różnych zakresach przedmiotowych i o różnych poziomach uzasadniania zaufania. Co istotne uzasadnienie zaufania (*assurance level*) dotyczy oceny, a nie bezpieczeństwa produktu/usługi/procesu. Strona trzecia może zaświadczyć tylko o tym, że producent/twórca/deweloper stworzył produkt, który ma spójne, kompletne wymagania bezpieczeństwa i te wymagania w produkcie są

spełnione. Ocena bezpieczeństwa nie odpowiada na pytanie, czy te wymagania są wystarczające. Ocena bezpieczeństwa dotyczy więc tego, co w tym produkcie zostało wprowadzone jako mechanizm bezpieczeństwa.

Poruszona została kwestia norm referencyjnych. Rozporządzenie mówi w sposób bardzo stanowczy o tym, jakie są podstawy oceny bezpieczeństwa i ewentualnej certyfikacji bezpieczeństwa w ocenie. Odsyła do międzynarodowych, europejskich lub krajowych norm, a jeśli ich nie ma to specyfikacji technicznych, które muszą spełniać wymogi określone w odpowiednim załączniku rozporządzenia dotyczącego normalizacji europejskiej[1] (zapewnienie, że proces tworzenia takiej specyfikacji był transparentny, otwarty i zapewniający równy dostęp oraz że istnieje odpowiednia organizacja, która zagwarantuje utrzymanie tej specyfikacji). Dopiero jeśli dany program certyfikujący wykaże, że nie ma odpowiednich norm/specyfikacji, to jest możliwość przyjęcia innych dokumentów jako podstawy oceny bezpieczeństwa. Europejskie ramy certyfikacji cyberbezpieczeństwa są bardzo mocno osadzone w normach.

Wskazany został program SOG-IS (Senior Official Group Information Security Systems) – istnieje na rynku od 1997r. i jest najstarszym światowym schematem certyfikacji bezpieczeństwa produktów ICT. Porozumienie SOG-IS reguluje współpracę państw UE i EFTA w obszarze koordynowania polityk certyfikacji wyrobów sektora technologii informatyczno-komunikacyjnych. Aktualnie jest 17 sygnatariuszy porozumienia SOG-IS, jednym z nich jest Polska (od kwietnia 2017r.) - dzięki uczestnictwu w porozumieniu Polska będzie mogła docelowo samodzielnie wystawiać certyfikaty, zgodnie z normą ISO/IEC 15408: Technika informatyczna – Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych (znana jako Common Criteria). Norma ta jest jedyną światową normą referencyjną odnosząca się do oceny cyberbezpieczeństwa. Aktualnie trwają prace nad nową edycją serii norm międzynarodowych ISO/IEC 15408, która jest znacznie bardziej przyjazna dla użytkowników – definiuje znacznie bardziej pragmatyczne podejście do produktów złożonych (np. z modułów).

Podkreślone zostało, że certyfikacja cyberbezpieczeństwa istnieje na rynku od ponad 20 lat i coraz więcej produktów poddawanych jest certyfikacji.

Spotkanie z Panem Bartoszem Wernikiem, Naczelnikiem Wydziału Informatyki w MC w sprawie narzędzi pracy grupowej dla Rady ds. Cyfryzacji.

Pan Bartosz Wernik przedstawił narzędzie, które Ministerstwo Cyfryzacji może udostępnić Członkom Rady ds. Cyfryzacji do usprawnienia współpracy zbiorowej – pokazał jego funkcjonalności i obsługę.

[1] Załącznik 2 do Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE

Wystąpienie Pani Izabeli Albrycht na temat Cyfrowego Trójmorza oraz Autostrady Cyfrowej Trójmorza.

Pani Izabela Albrycht przedstawiła temat Cyfrowego Trójmorza i Cyfrowej Autostrady.

Inicjatywa Trójmorza, zainicjowana w 2016r., służy zacieśnianiu powiązań w regionie szerzej rozumianej Europy Środkowo-Wschodniej (między Morzem Bałtyckim, Adriatyckim i Czarnym). Inicjatywa ta ma zniwelować zauważoną lukę infrastrukturalną, dlatego oparta jest na trzech filarach: transportowym, energetycznym i cyfrowym. Podkreślone zostało, że widoczny jest rozwój współpracy zwłaszcza w dwóch pierwszych filarach – z tego względu Instytut Kościuszki przygotował projekt rozwoju współpracy w filarze cyfrowym. Dodatkowy nacisk położony jest na wzmocnienie cyberbezpieczeństwa regionu we wszystkich trzech filarach – postulowane jest, by wszelka infrastruktura, która w regionie będzie budowana w ramach Inicjatywy Trójmorza brała pod uwagę współczesne zagrożenia cyfrowe i tym samym implementowała bezpieczne rozwiązania. Przy budowaniu tej koncepcji Instytut Kościuszki współpracuje z think-tankami ze Słowacji, Chorwacji, Rumunii i Węgier a także USA.

Podkreślone zostało, że Trójmorze to 12 krajów UE, zamieszkiwanych przez 114 milionów obywateli. Region ten zajmuje ponad 28 procent terytorium UE, generujących 1,6 bilionów dolarów przychodów rocznie.

Współpraca cyfrowa i Cyfrowe Trójmorze ma duże znaczenie i jest niezwykle potrzebne – bez cyfrowego rozwoju regionu nie ma możliwości osiągnięcia w pełni głównego celu Trójmorza, jakim jest połączenie gospodarek i infrastruktur Europy Środkowo-Wschodniej z północy na południe. Nie będzie również możliwości poprawy konkurencyjności, spójności i odporności regionu. Nie będzie można zniwelować różnic w poziomie rozwoju infrastruktury pomiędzy regionem Trójmorza a Europą Zachodnią. Nie będzie też można dokończyć tworzenia jednolitego rynku europejskiego, nie mówiąc już o jednolitym rynku cyfrowym. To, co łączy kraje Europy Środkowo-Wschodniej, to dość niskie pozycje w rankingach, w tym Digital Economy and Society Index (DESI).

Trójmorze zajmuje się projektami, które mają doprowadzić do budowy nowych dróg, połączeń kolejowych, gazociągów. W wymiarze cyfrowym zaproponowanych zostało kilka projektów, z czego najbardziej zaawansowany jest projekt Autostrady Cyfrowej Trójmorza (*3 Seas Digital Highway*), która przewiduje budowę infrastruktury światłowodowej i 5G wzdłuż już zaplanowanych dróg transportowych i/lub linii energetycznych. Sieć światłowodów, która składałaby się na Cyfrową Autostradę, byłaby budowana zarówno w obszarze szkieletowym, jak i dostępowym, mogłaby być uzupełniona o technologię 5G, mogłaby doprowadzić do zniwelowania luki infrastruktury komunikacyjnej w obszarze Europy Środkowo-Wschodniej. Pozwoliłoby to na dalsze pogłębienie cyfrowej współpracy w całej Europie, wpływając na zwiększenie konkurencyjności regionu i realizację założeń jednolitego rynku cyfrowego. Szkielet takiej międzynarodowej sieci światłowodowej pozwoliłby na wymianę ruchu roamingowego, który wzrasta.

Pomysłem jest, aby budowa Cyfrowej Autostrady przebiegała wzdłuż Via Carpatia, czyli trasy, która ma być kluczowym transeuropejskim korytarzem transportowym. Trasa ta ma powstać wzdłuż wschodniej granicy Polski, ma połączyć północ Europy z południem i ma być gotowa w 2025 roku. Obecnie podpisana została Deklaracja Łańcucka III, dotycząca wzmocnienia współpracy w zakresie transportu w Europie Środkowej i Południowej. Docelowo trasa Via Carpatia ma przebiegać z Kłajpedy i Kowna na Litwie przez Białystok, Lublin, Rzeszów i słowackie Koszyce do Debreczyna na Węgrzech, a dalej do Rumunii, Bułgarii i Grecji. Możliwe także, że ten projekt zostanie poszerzony o inne kraje.

Koncepcja Autostrady Cyfrowej Trójmorza ma wypełnić lukę w infrastrukturze telekomunikacyjnej, ma wesprzeć swobodny przepływ danych (co przyspieszy rozwój gospodarki opartej na danych), a także konkurencyjność i rozwój przemysłu 4.0, może zapewnić lepszy dostęp do nowych technologii mobilnych dla użytkowników indywidualnych i przemysłu, może wzmocnić i pogłębić współpracę pomiędzy krajami Trójmorza, a także wesprzeć transformację krajów Trójmorza i przejście gospodarki na wyższy poziom łańcucha dostaw. Co bardzo istotne infrastruktura cyfrowa musi być odporna na wszelkiego rodzaju e-zagrożenia bezpieczeństwa, musi być budowana zgodnie z koncepcją *security by design* i poparta najnowocześniejszą cyberochroną.

Wskazane zostało, że w przyszłości w obszarze Trójmorza wzdłuż Autostrady Cyfrowej mogą powstawać ośrodki oferujące usługi oparte na chmurze obliczeniowej i przechowywaniu danych (tzw. wyspy danych). Skutkiem budowy takiej infrastruktury w regionie może być też powstanie centrów innowacji cyfrowej (*Digital Innovation Hub*) i centrów kompetencji. Dzięki rozwojowi infrastruktury cyfrowej mogą się w regionie rozwijać również m.in. ośrodki e-handlu, technologie oparte na Sztucznej Inteligencji czy też na Internecie Rzeczy. Infrastruktura Cyfrowa jest również konieczna, aby rozwijać autonomiczny transport w regionie czy inteligentne rozwiązania dla miast i wsi.

Instytut Kościuszki proponuje również, by region Trójmorza współpracował także w zakresie badań naukowych.

Pani Izabela Albrycht wspomniała, że koncepcja Autostrady Cyfrowej Trójmorza narodziła się w 2018 roku, pierwszy raz została przedstawiona na spotkaniu w Biurze Bezpieczeństwa Narodowego, podczas którego obecni byli przedstawiciele administracji publicznej, m.in. BBN, MON, MI, MPiT, NASK. Założenia wstępne koncepcji przedstawione zostały w *white paper* w czerwcu 2018r. Przełomem był szczyt Trójmorza w Bukareszcie we wrześniu w 2018 roku. Przedstawiony został tam projekt przygotowany przez Polskę - jest to koncepcja jeszcze bardzo ogólna, wymaga dopracowania, jednak jest uznawana za jednego z kandydatów do statusu projektu priorytetowego Inicjatywy Trójmorza. Instytut Kościuszki przedstawił go na kilku wydarzeniach, przede wszystkim na Europejskim Forum Cyberbezpieczeństwa - w panelu na ten temat uczestniczył wówczas Pan Minister Marek Zagórski.

Zostały również przedstawione kwestie, które mogłyby pomóc dalej realizować tą koncepcję – niezbędne są więc wola polityczna, wsparcie, zidentyfikowanie jednego lidera, właściciela projektu, współpraca publiczno-prywatna, fundusze.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska – Jentkiewicz
3. Jan Czajkowski
4. Krzysztof Głomb - Wiceprzewodniczący
5. Paweł Gora
6. Michał Kanownik
7. Anna Beata Kwiatkowska
8. Tomasz Łukawski
9. Dariusz Milka
10. Józef Orzeł – Przewodniczący
11. Włodzimierz Schmidt
12. Sebastian Szymański
13. Jacek Zadrożny

Zaproszeni goście:

14. Elżbieta Andrukiewicz, Kierownik Projektu KSO3C, IŁ-PIB
15. Agnieszka Kamińska, IŁ-PIB
16. Jarosław Mosiejuk, ekspert

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

17. Joanna Marczak-Redecka, Zastępca Dyrektora Biura Ministra w MC
18. Monika Skrzyńska, Doradca Ministra Cyfryzacji
19. Bartosz Wernik, Naczelnik Wydziału Informatyki w MC
20. Katarzyna Stopińska (MC)