PROTOKÓŁ z VII posiedzenia Rady do Spraw Cyfryzacji VI kadencji, które odbyło się 24 kwietnia 2026 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

Otwarcie posiedzenia – p. Agnieszka Jankowska, Przewodnicząca Rady ds. Cyfryzacji.

Posiedzenie otworzyła Przewodnicząca Rady, Pani Agnieszka Jankowska, która powitała obecnych na posiedzeniu Rady ds. Cyfryzacji.

Cyberbezpieczeństwo jednostek samorządu terytorialnego – „Wsparcie cyberbezpieczeństwa jednostek samorządu terytorialnego - wyzwania, doświadczenia i rekomendacje”- Pan Jakub Jędrzejczak, członek Rady ds. Cyfryzacji.

Pan Minister Rafał Rosiński pogratulował członkom powołania do Rady ds. Cyfryzacji. Wskazał, że prezentowany temat jest bardzo istotny nie tylko dla MC. Cyberbezpieczeństwo jest zasadniczym priorytetem – wiele programów realizowanych w MC jest poświęconych szeroko rozumianemu cyberbezpieczeństwu w zakresie sektora publicznego, poczynając od sektora centralnego (administracja rządowa i samorządowa) oraz współpracy z sektorem prywatnym. W odniesieniu do bezpieczeństwa samorządów terytorialnych w czerwcu br. zostanie ogłoszony konkurs na tzw. Lokalne Centra Cyberbezpieczeństwa, mający na celu wzmocnienie najmniejszych jednostek ze wskazaniem wiodącej jednostki samorządu terytorialnego, głównie powiatu czy związków powiatów.

Pan Jakub Jędrzejczak, członek Rady ds. Cyfryzacji wskazał, że jednym z pomysłów do rozważenia na poprawę cyberbezpieczeństwa w samorządach jest utworzenie Krajowego Centrum Wsparcia Cyberbezpieczeństwa Samorządów (KCWCS) wspierającego projekt „Cyberbezpieczny Samorząd” oraz wzmacniającego obecny ekosystem, ponieważ cyberbezpieczeństwo w JST jest bardzo ważne. Na terenie JST działa znaczna część infrastruktury krytycznej i usług publicznych. Poziom dojrzałości cyberbezpieczeństwa jest silnie zróżnicowany – najsłabsze ogniwa determinują odporność całości. Zakłócenia w JST szybko przenoszą się na ciągłość świadczenia usług publicznych. Pan J. Jędrzejczak wskazał mocne strony obecnego ekosystemu – Projekt „Cyberbezpieczny Samorząd” przełożył się na realne umowy i inwestycje JST, ISAC-JST tworzy pierwszy trwały kanał współpracy, CERT Polska daje skanowanie, ostrzeżenia i informacje o podatnościach, a NASK rozwija szkolenia i praktyczne wsparcie dla administracji oraz operatorów. MC, CPPC oraz NASK budują fundament państwowy. To inicjatywy, które już przynoszą efekty, a nowy program powinien je wzmacniać, a nie zastępować. Pan J. Jedrzejczak uznał, że Polska ma już filary technologiczne, edukacyjne i informacyjne – brakuje jednak trwałego, zintegrowanego modelu operacyjnego dla JST. KCWCS dodaje brakujący poziom: stałe, regionalne, zakorzenione wsparcie operacyjne dla JST. Przy pomocy Lokalnych Centrów Cyberbezpieczeństwa z konceptem KCWCS mogłoby powstać 16 węzłów regionalnych, w

których bardzo zróżnicowane dojrzałością samorządy w zakresie cyberbezpieczeństwa mogłyby otrzymywać wsparcie.

Pan J. Jędrzejczak wskazał, że obecnie dominujący model wsparcia ma charakter okresowy, projektowy oraz grantowy. Problemem jest brak metodyki, kompetencji i bieżącej wymiany doświadczeń. KCWCS może zaistnieć poprzez zorganizowanie społeczności praktyków JST – szybka wymiana doświadczeń, wspólne standardy, uczenie się, współpraca między JST. Pan J. Jędrzejak opisał koncepcję KCWCS wskazując na potrzebę utworzenia koordynatora w każdym województwie i określając jego rolę, a także podział ról na poziomie krajowym, wojewódzkim oraz JST czy stworzenie Rady Programowej KCWCS. Krajowe Centrum mogłoby być stałym łącznikiem między samorządami a partnerami dziś wspierającymi cyberbezpieczeństwo, takimi jak CERT Polska, Ministerstwo Cyfryzacji, NASK czy ISAC-JST.

Pan Bartosz Drozd, przedstawiciel Urzędu Marszałkowskiego Województwa Mazowieckiego poinformował, że Urząd realizuje projekty finansowane ze środków europejskich w większości w partnerstwie z najmniejszymi jednostkami, czyli JST – urzędy gminy, powiaty, gdzie głównym problemem jest techniczne zaplecze informatyczne. Świadomość kwestii cyberbezpieczeństwa wśród jednostek jest duża, jednak brakuje zasobów kadrowych do ich realizacji. Obecnie Urząd przygotowuje się w ramach nowej perspektywy do zadania związanego m.in. z cyberbezpieczeństwem w wojewódzkich samorządowych jednostkach organizacyjnych. Przedstawiciel Urzędu wskazał, że upatruje dużą szansę na poprawę sytuacji w ujednolicaniu rozwiązań organizacyjnych oraz wdrożeń systemów cyberbezpieczeństwa. W ramach wspólnych centrów kompetencyjnych można byłoby rozważyć wsparcie w zakresie wykorzystania technologii automatyzacji zadań i przepływu pracy oraz zbudowania bazy wiedzy, aby ograniczyć ryzyko braku odpowiednio szybkiej reakcji na incydent bezpieczeństwa informatycznego, wynikającego często z niewystarczających zasobów ludzkich w zespołach IT.

Pan Dyrektor Grzegorz Nowak, pomysłodawca i współzałożyciel ISAC-JST, wskazał, że w Polsce można wyróżnić dwa główne scenariusze cyberataków. Pierwszy ma na celu ośmieszenie dużych, dobrze finansowanych instytucji, natomiast drugi koncentruje się na łatwych celach, wynikających z braku odpowiednich zabezpieczeń, szczególnie w mniejszych miejscowościach. Podkreślił, że cyberbezpieczeństwa nie należy utożsamiać wyłącznie z informatyką, która stanowi tylko jeden z jego elementów. Kluczowe jest mówienie o analizie ryzyka, szkoleniach oraz rozwijaniu kompetencji.

W odpowiedzi na te wyzwania powołano Centrum Cyberbezpieczeństwa i Ochrony Danych, które zajmuje się cyberbezpieczeństwem na różnych płaszczyznach, w szczególności w zakresie GRC oraz ochrony danych, wspierając administratorów w budowie odpowiednich procesów. Pan Dyrektor zwrócił uwagę, że jednym z podstawowych warunków skutecznego mierzenia się z pojawiającymi się wyzwaniami jest budowanie kadr. Podziękował Ministerstwu Cyfryzacji za stworzenie podstawy programowej dla zawodu technika cyberbezpieczeństwa. Wyraził również opinię, że każda Jednostka Samorządu Terytorialnego

powinna dysponować specjalistą ds. cyberbezpieczeństwa, odpowiedzialnym za analizę ryzyka.

Zaproponował także tworzenie lokalnych centrów kompetencyjnych (Lokalnych Centrów Cyberbezpieczeństwa), które mogłyby świadczyć usługi na odpowiednim poziomie dla wielu samorządów jednocześnie, nie koncentrując się jedynie na usłudze SOC, ale także na analizie ryzyka i edukacji cybersecurity-awareness. Poparł również opracowaną przez MC koncepcję utworzenia Lokalnych Centrów Cyberbezpieczeństwa, wskazując jednocześnie na kilka jej słabych punktów. Zaznaczył, że istotne jest rozpoczęcie dyskusji na temat zamówień publicznych realizowanych w trybie niejawnym. Wyjaśnił, że ISAC-JST jest oddolną inicjatywą powstałą w celu usprawnienia współpracy oraz wymiany informacji o incydentach między samorządami, które traktują cyberbezpieczeństwo jako jeden z priorytetów.

Pan Dyrektor zwrócił także uwagę na potrzebę wsparcia finansowego dla koncepcji tworzenia ponadlokalnych ambasad danych, które umożliwiałyby samorządom wzajemne przechowywanie kopii bezpieczeństwa w oparciu o zasadę zaufania publicznego. Wspomniał również o znaczących środkach przeznaczanych na licencje zagranicznych korporacji i poddał pod rozwagę działania legislacyjne umożliwiające wspólne zamówienia, z których mogłyby korzystać samorządy. Ostatnią kwestią poruszoną przez Pana Dyrektora było subwencjonowanie obszaru IT na rzecz samorządów lub wymóg określonego, wyrażonego w procentach poziomu finansowania względem budżetu gminy.

Pani Dyrektor Joanna Szafarczyk – Kurek wskazała, że nie tylko mniejsze samorządy stoją przed dużymi wyzwaniami, ale także te większe. Poza Urzędem m.st. Warszawy jest ponad 1000 budżetowych, organizacyjnych jednostek najróżniejszych rozmiarów. Są jednostki, które mają rozbudowane IT, są również takie (objęte krajowym systemem cyberbezpieczeństwa), w których zatrudniane są osoby obsługujące jednocześnie kilka mniejszych jednostek. Pani Dyrektor poinformowała, że przygotowując się do stosowania przepisów nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa z poziomu urzędu podjęto wiele działań edukacyjnych, ale także wypracowywano wspólne standardy obsługi tych jednostek dając wytyczne i organizując szkolenia. Poza technicznymi aspektami - wymiana wiedzy, świadomość, szkolenia, plany awaryjne, plany ciągłości działania, a przede wszystkim testowanie tych planów to kluczowe czynniki, które bardzo wzmacniają cyberodporność.

Pan Dyrektor Maciej Siciarek uznał, iż z doświadczeń obsługi incydentów przez CSIRT NASK wynika, że płacimy wysoką cenę za zachwyt nad cyfryzacją przez ostatnich kilkanaście lat – nakłady na infrastrukturę cyfrową, a zwłaszcza jej zabezpieczenie nie przystają do kwot jakie samorządy przeznaczają na inne cele. Uznał, że jeżeli nie zlikwidujemy podatności, nie będziemy wspólne zarządzali podatnościami urządzeń, nie wyeliminujemy aspektu bezkrytycznego ujawniania sprzętu i jego instalacji, będzie bardzo trudno dojść do dużego poziomu zabezpieczeń. Pewne zamierzenia są możliwe do osiągnięcia tylko poprzez centralizację. Być może centralizacja na poziomie samorządów będzie przynosiła efekty, ale z pewnością nie da się niczego osiągnąć jeżeli model finansowania etatów specjalistów

bezpieczeństwa teleinformatycznego/cyberbezpieczeństwa oraz finansowania samorządów pozostanie ten sam. Inwestycje tylko w infrastrukturę zwiększą liczbę botów i niezabezpieczonych urządzeń.

Pan Dyrektor poinformował, że w ramach projektu Centrum Cyberbezpieczeństwa NASK jest podprojekt Krajowe Centrum Wsparcia JST. NASK widząc zagrożenie incydentami chce wzmocnić współpracę z samorządami poprzez to, że będzie w stanie docierać do samorządów i przeprowadzać proaktywne analizy.

Jeden z członków Rady zaproponował, aby Rada wspólne z samorządami dokonała przeglądu niezbędnych modyfikacji regulacyjnych. Ponadto, być może dobrym pomysłem jest stworzenie repozytorium – bazy danych, narzędzi szkoleniowych, wiedzy eksperckiej czy analiz do wykorzystania. Istotne jest także powszechne budowanie kompetencji cyfrowych.

Pan Dyrektor Marcin Wysocki wskazał, że w kontekście cyberbezpieczeństwa analiza ryzyk, poza ustaleniem kontekstu organizacji, zaczyna się od inwentaryzacji istniejących zasobów. Rozwiązania, które są nowością w ustawie o ksc to np. porozumienia pomiędzy JST do wspólnego wykonywania obowiązków. Ponadto programowany jest także projekt Lokalnych Centrów Cyberbezpieczeństwa. W odniesieniu do repozytorium mechanizmu współpracy na poziomie odgórnym Pan Dyrektor zasugerował, że nie jest to dobre rozwiązanie, ponieważ informacje o incydentach są dość wrażliwe i do tego rodzaju współpracy należy zachęcać, a nie jej narzucać. Tym bardziej, że jest możliwość dzielenia się informacjami, są do tego podstawy prawne, ale zakładają one dobrowolność i podmioty nie będą skore do wymiany informacji wrażliwej, do której dostęp będą mieli wszyscy lub bardzo szerokie grono. Ogólną wskazówką byłaby inwentaryzacja projektów względem projektu KCWCS i na tej podstawie możliwa ocena jakie aspekty działają, na jakie kwestie potrzeba czasu dla oceny zaadresowania i rozważenia wspomnianej wcześniej formuły KCWCS. Wskazał, że administracja publiczna ma mieć swój CSIRT sektorowy i zgodnie z ustawą o ksc powinna być z nimi połączona oraz wspomagać swoimi rekomendacjami podmioty publiczne. Pan Dyrektor odnosząc się do akredytacji cyberbezpieczeństwa wskazał konieczność rekomendacji UZP. MC rozważa stworzenie i propozycję usprawniającego procesu np. jako krajowy program certyfikacji cyberbezpieczeństwa dla samorządów czy sektora MŚP. Co do budowania sytuacji z zakresu cyber w samorządach, to w ramach programu „Cyberbezpieczny Samorząd” nałożony został obowiązek przekazywania audytów do MC przeprowadzonych u grantobiorców, a na ich podstawie resort zamierza w sposób systemowy dokonać analizy i wyciągnąć wnioski, aby kolejne środki z budżetu oraz współfinansowane z funduszy europejskich faktycznie kierować w odpowiedzi na potrzeby JST. W dalszej części wypowiedzi Pan Dyrektor odniósł się także do transparentności w kontekście umów i zamówień publicznych.

W toku dyskusji pojawiało się stwierdzenie, że należy zastanowić się po czyjej stronie – państwa czy samorządu jest odpowiedzialność za cyberbezpieczeństwo i rozważyć jakie zadania wydobyć z samorządu, by od nowa poukładać infrastrukturę odpowiedzialności.

Pojawiło się także zdanie, iż należy zacząć rozumieć, edukować oraz mówić o tym, że cyberbezpieczeństwo to nie tylko odpowiedzialność rządu, lecz zaczyna się od każdego z nas – obywatela, przedsiębiorcy czy samorządu. Stwierdzono, że wyzwaniem jest dotarcie do samorządów, zwłaszcza tych mniejszych, z informacją nt. korzystania z dostępnych serwisów zawierających narzędzia z zakresu cyberbezpieczeństwa. Ponadto należy zadbać, by w samorządzie znajdowali się wykwalifikowani i zaangażowani ludzie, którzy będą chcieli pracować i ponosić odpowiedzialność za kwestie cyberbezpieczeństwa.

Pani Przewodnicząca poinformowała, że w przedmiotowej sprawie powstanie stanowisko Rady.

Zamknięcie posiedzenia.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Andrzej Dulka
2. Agnieszka Jankowska - Przewodnicząca
3. Joanna Jaworek-Korjakowska
4. Jolanta Jaworska
5. Jakub Jędrzejczak
6. Michał Kanownik
7. Agnieszka Kasprzak
8. Patryk Kuzior
9. Marcin Lis
10. Krzysztof Madej
11. Magdalena Mike
12. Robert Pękal
13. Elżbieta Żuraw

Zaproszeni goście:

14. Rafał Rosiński, Podsekretarz Stanu w MC
15. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
16. Maciej Siciarek, Dyrektor Pionu CSIRT NASK-PIB
17. Grzegorz Nowak, Dyrektor Centrum Cyberbezpieczeństwa i Ochrony Danych we Władysławowe, ISAC-JST
18. Bartosz Drozd, Kierownik Wydziału ds. Infrastruktury i Udostępniania E-Usług w Departamencie Cyfryzacji, Geodezji i Kartografii w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie
19. Michał Szwarc, Urząd Marszałkowski Województwa Mazowieckiego w Warszawie
20. Tomasz Komorowski, Dyrektor Wydziału Społeczeństwa Informacyjnego i Informatyki w Urzędzie Marszałkowskim Województwa Zachodniopomorskiego
21. Joanna Szafarczyk – Kurek, Dyrektor Biura Informatyki w Urzędzie Miasta Stołecznego Warszawy

Sekretariat Rady i Pracownicy Ministerstwa Cyfryzacji:

22. Karolina Taczalska, Biuro Ministra w MC

23. Katarzyna Gójska, Biuro Ministra w MC