PROTOKÓŁ z XXII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 6 grudnia 2024 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

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

Pani Przewodnicząca powitała obecnych członków Rady ds. Cyfryzacji oraz zaproszonych na posiedzenie gości.

Projekt Strategii Cyberbezpieczeństwa oraz projekt ustawy o Krajowym Systemie Cyberbezpieczeństwa- Pan Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w MC oraz Pan Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC, dyskusja.

Pan Dyrektor Ł. Wojewoda przedstawił informacje dotyczące etapu na jakim znajduje się Strategia Cyberbezpieczeństwa obejmująca okres 2025-2029. Podkreślił, że Strategia nie będzie już jedynym dokumentem poziomu strategicznego opisującym zagadnienia związane z cyberbezpieczeństwem, gdyż będą one ujęte również w Strategii Cyfryzacji Polski. Departament Cyberbezpieczeństwa MC opiekuje się tymi dwoma dokumentami – Strategią Cyberbezpieczeństwa w pełnym zakresie, Strategią Cyfryzacji Polski w zakresie związanym z cyberbezpieczeństwem. Pracuje nad zapewnieniem pełnej zgodności tych dokumentów, natomiast nie będą one tożsame. Strategia Cyberbezpieczeństwa jest priorytetowa, natomiast wspólnie ze Strategią Cyfryzacji Polski będą obie dokumentami równoważnymi, powołanymi w drodze ustawowej. Nie zaproponowano przepisów, które powodowałyby, że Strategia Cyberbezpieczeństwa zostanie podporządkowana Strategii Cyfryzacji Polski. Dokumentem bardziej szczegółowym będzie Strategia Cyberbezpieczeństwa z przyjętym podejściem ewolucyjnym, mającym na uwadze istnienie kilku dokumentów strategicznych. Udało się opracować wewnątrzresortową propozycję Strategii, która powstała w drodze uzgodnień wewnątrzresortowych pomiędzy departamentami MC, ale także pomiędzy jednostkami podległą/nadzorowanymi. Kolejnym krokiem będzie zebranie wkładu od innych resortów w zakresie propozycji MC i przede wszystkim w zakresie planu działań jako dokumentu, z którego ma wynikać praktyka Strategii. Z uwagi na to, że Strategia zostanie przyjęta razem z planem działań jako uchwała Rady Ministrów, będzie musiała pojawić się ocena skutków regulacji. Strategia została twardo umiejscowiona w obowiązujących przepisach prawa – w przypadku wejścia w życie ustawy o Krajowym Systemie Cyberbezpieczeństwa zostanie dokonany przegląd Strategii i będą naniesione poprawki zgodnie ze zmienionymi przepisami.

W toku dyskusji jeden z przedstawicieli DC dodał, że istnieje możliwość zaplanowania działań, które dopiero przewidują dalsze zmiany prawne – nie każde zadanie ujęte w planie działań musi mieć już obecnie podstawę prawną, ponieważ Strategia jest po to, by wyznaczać kierunek działania. Odnośnie do finansowania wskazano, że Strategia nie powoduje żadnych

bezpośrednich skutków finansowych. Do resortów będzie należało, by znaleźć środki na zaplanowane działania.

W odniesieniu do zawartości merytorycznej Strategii podkreślone zostało, że głównym celem jest podniesienie poziomu odporności. Cele szczegółowe to rozwój, podniesienie odporności systemów informacyjnych, zwiększanie potencjału, budowa świadomości oraz budowa rozpoznawalności silnej międzynarodowej pozycji Polski, tak aby we wszystkich indeksach *Cybersecurity* Polska pojawiała się na podium. W Strategii znajduje się centralna instytucja odpowiedzialna za cyberbezpieczeństwo na poziomie krajowym. Pan Dyrektor Ł. Wojewoda wspomniał o instytucji koordynującej obsługę incydentów na poziomie krajowym. Potrzebna będzie kompleksowa dyskusja na temat tego jakie zasoby i z jakich instytucji będą mogły zasilić podmiot koordynujący.

Jeden z członków Rady zapytał czy koszty związane z wdrożeniem Strategii Cyberbezpieczeństwa są uwzględnione w Strategii Cyfryzacji Polski. Pan Dyrektor Ł. Wojewoda odpowiedział, że obecnie będzie to przedsięwzięcie związane z dodatkowymi kosztami wynikającymi z wdrożenia wymagań znowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa. Będzie to bardziej konsolidacja w jednym miejscu już posiadanych zasobów niż budowanie od zera. O faktycznych kosztach przesądzi akt wprowadzający dany podmiot. Pan Naczelnik M. Strzelczyk wskazał, że pierwszym krokiem będzie uchwalenie Strategii. Kolejny krok to zbudowanie struktury wewnątrz ministerstwa, która na bazie nowelizacji ustawy o KSC zalegitymizuje połączone Centrum Operacyjne Cyberbezpieczeństwa i będzie zapewniało wsparcie merytoryczne Pełnomocnika ds. cyberbezpieczeństwa. W następnym kroku podejmowane zostaną działania w celu zbudowania podmiotu, który scentralizuje cały zakres.

Pojawiło się pytanie o skoordynowanie przez Pełnomocnika ds. cyberbezpieczeństwa współpracy cywilnowojskowej na arenie międzynarodowej. Pan Dyrektor Ł. Wojewoda wskazał, że należy pamiętać, iż Pełnomocnik nie jest tylko w sferze cywilnej. Ustawa o działach administracji rządowej[1] podzieliła cyberbezpieczeństwo na strefę cywilną i rządową, natomiast Pełnomocnik w ustawie ma przypisaną koordynację za rząd. Wydaje się, że na mocy porozumienia pomiędzy Ministerstwem Cyfryzacji a Ministerstwem Obrony Narodowej, w odniesieniu do sfery koordynacyjnej jest dobra wizja na przyszłość. W dalszej części swojej wypowiedzi Pan Dyrektor Ł. Wojewoda wskazał, że najistotniejsza kwestia w ramach Strategii to dążenie, by Strategia była wyznacznikiem kierunku działań. Zwrócił uwagę, że ustawa o KSC jest ustawą bardziej techniczną, gdzie mowa jest o technicznym aspekcie cyberbezpieczeństwa.

Następnie, rozpoczęła się dyskusja w sprawie dezinformacji. Pan Dyrektor Ł. Wojewoda poinformował, że w Strategii Cyberbezpieczeństwa zostało ukazane, iż niektóre działania dezinformacyjne (naruszające atrybut cyberbezpieczeństwa) wywołają incydent związany z cyberbezpieczeństwem, ale w tym momencie nie powinna kończyć się obsługa tego aspektu,

[1] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. 2024 poz. 1370)

lecz są to dalsze działania. Nie sposób opisać tych działań, ponieważ cyberbezpieczeństwo jest o wiele bardziej szerokie – być może ta kwestia powinna znaleźć się w innych dokumentach np. Strategii Cyfryzacji Polski.

W toku dyskusji Pan Dyrektor Ł. Wojewoda opowiedział o systemie S46 i jednym punkcie kontaktowym. System zadecyduje zgodnie z ustanowionym procesem, gdzie trafi incydent zgłoszony przez podmiot. Ideą systemu jest, by docelowo była to platforma, w której uczestnicy systemu będą dostawali informację o działaniach w ich systemach, gdy zaatakowany został łańcuch dostaw innego podmiotu, a podmiot świadczący usługi jest ten sam dla kilku podmiotów. Ponadto, w przyszłości w planach jest także możliwość dokonywania przez wspomniany system zgłoszeń związanych z naruszeniami danych osobowych. S46 będzie odpowiadał, aby wypełnić wymagania ustawowe przekazania zgłoszeń do PUODO. Pan Dyrektor M. Wysocki dodał, że Prezes UODO wskazał kilka kanałów komunikacji. Do zgłoszeń zostanie przeznaczony system S46, by za pośrednictwem jednego formularza uczynić zadość wymaganiom. Uczestnikami Systemu są tylko podmioty objęte ustawą o KSC.

Jeden z członków Rady zapytał czy podczas przygotowywania dokumentu Strategii Cyfryzacji natknięto się na problemy operacyjne, dotyczące podstawy do ujawnienia danych. Zarówno telekomy, medycyna, banki mają szereg regulacji związanych z tajemnicą bankową, medyczną itp. - czy w celu przekazania swoich danych do koordynowanego obsłużenia incydentu, instytucje mają podstawę prawną do ich przekazania. Pan Dyrektor M. Wysocki odpowiedział, że w przypadku większości prawnie chronionych tajemnic to obowiązek dot. dochowania należytej staranności. Celem MC jest zapewnienie takiego sposobu zabezpieczenia informacji, które będą w S46, aby nie było wątpliwości, że podmioty, które kontrybuują do tego systemu dochowują należytej staranności w przypadku dzielenia się tymi informacjami.

Dalsza cześć posiedzenia została poświęcona tematyce projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Przedstawiciele MC zostali zapytani o najważniejsze zmiany. Pan Dyrektor M. Wysocki wskazał, że obecnie projekt jest na etapie Komitetu do Spraw Europejskich. Dokonane zostały dodatkowe uzgodnienia zgodnie z zaleceniami roboczymi co do uwag o charakterze europejskim, w związku z tym projekt otrzyma dalsze zmiany w kolejnej wersji, która zostanie niedługo opublikowana. Przeanalizowano konieczność udziału w innych komitetach Rady Ministrów – projekt zostanie skierowany na Stały Komitet Rady Ministrów, który prawdopodobnie zajmie się nim na początku przyszłego roku. Przyjęcie przez KSE nie powoduje, że MC jest pewne sukcesu i sprawnego procesowania przez SKRM, ponieważ wiele uwag nie ma tzw. charakteru europejskiego.

Pani Przewodnicząca zapytała o jednostki samorządu terytorialnego, które będą podlegały karom – czy zasady dla JST np. dla gminy wiejskiej będą tożsame z zasadami obejmującymi podmioty prywatne. Pan Dyrektor M. Wysocki odpowiedział, że poszukiwany jest kompromis, aby te najbardziej skrajne i oczywiste przypadki/podmioty wyjąć z ustawy o KSC, tzn. nie

obciążać ich, by w ciągu 7 miesięcy wdrożyć konglomerat obowiązków związanych z systemem zarządzania bezpieczeństwem informacji. W dalszej części dyskusji Pan Dyrektor wspomniał w odniesieniu do JST, że poszukiwany jest kompromis w kwestii możliwości zlecenia zamówień centralnych - koordynacja wymagań w różnym zakresie poprzez m.in. porozumienia pomiędzy JST, z drugiej strony usprawnienie procesu zamówień publicznych. Pan Dyrektor Ł. Wojewoda dodał, że celem MC jest zapewnienie, aby również JST podnosiły swoją odporność. Wykluczenie poza system nie jest rozwiązaniem, gdy dojdzie do ataku klasy ransom i podmiot będzie potrzebował pomocy, wtedy pojawi się problem. Pani Przewodnicząca wskazała na potrzebę przygotowania odpowiednich instrumentów i sposobów koordynacji w zakresie edukacji wdrażających ustawę o KSC.

Pani Przewodnicząca wspomniała, że zostało przygotowane stanowisko Rady w sprawie przede wszystkim nowelizacji ustawy o KSC. Stanowisko jest apelem o przyspieszenie prac oraz nadania priorytetu wszelkim instrumentom prawnym mającym wpływ na cyberbezpieczeństwo w kraju. Stanowisko ma zostać sfinalizowane w najbliższym czasie. Poddała pod rozwagę ustalenie adresatów stanowiska Rady w przedmiotowym zakresie.

W toku dyskusji Pan Dyrektor Ł. Wojewoda wspomniał, że w ramach *Cyberbezpiecznego Samorządu* został przygotowany poradnik jak przeprowadzać zamówienia publiczne z uwzględnieniem cyberbezpieczeństwa.

Członkowie Rady podjęli dyskusje, że rekomendacje/wytyczne są dla części samorządów nie do końca zrozumiałe w kontekście ich stosowania. Samorządy i UZP apelują o uproszczenie rekomendacji, by były dla każdego samorządu jako zamawiającego jasne i klarowne, na kształt opublikowanych minimalnych wymagań technicznych. Wskazano, by w podobnej formule zostały określone kryteria cyberbezpieczeństwa.

Sprawy różne.

Pani Przewodnicząca poinformowała, że kolejne posiedzenie Rady ds. Cyfryzacji odbędzie się 20 grudnia br.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Agnieszka Jankowska – Przewodnicząca
2. Jolanta Jaworska
3. Michał Kanownik
4. Katarzyna Kopczewska
5. Janusz Kosiński
6. Jarosław Mojsiejuk
7. Krzysztof Silicki
8. Katarzyna Szymielewicz
9. Robert Trętowski
10. Małgorzata Zakrzewska

Zaproszeni goście:

11. Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w MC
12. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
13. Michał Strzelczyk, Naczelnik Wydziału Analiz Cyberbezpieczeństwa w Departamencie Cyberbezpieczeństwa w MC
14. Jacek Meissner, Główny Specjalista, Departament Cyberbezpieczenstwa w MC

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

15. Karolina Taczalska, Biuro Ministra w MC
16. Joanna Gójska, Biuro Ministra w MC