PROTOKÓŁ z XXXVI posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 2 października 2020 roku, o godzinie 13:00 w formie wideokonferencji.

Spotkanie z Panem Robertem Koślą, Dyrektorem Departamentu Cyberbezpieczeństwa MC nt. zmiany ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz Strategii cyberbezpieczeństwa na lata 2019-2024: plan wdrażania tej strategii oraz stan prac.

Pan Dyrektor R. Kośla swoje wystąpienie zaczął od informacji, że został zainicjowany proces nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, biorąc pod uwagę dwa lata doświadczeń z obowiązywania przepisów dyrektywy NIS i wprowadzenia ich w Polsce w postaci Krajowego Systemu Cyberbezpieczeństwa. Dwa lata były kwestią wyznaczania operatorów usług kluczowych (obecnie jest ich ponad 160), a także opracowania strategii cyberbezpieczeństwa, która zdefiniowała kierunki działań na lata 2019-2024. Do strategii powstał także plan działań zawierający konkretne propozycje przedsięwzięć, które mają być realizowane przez poszczególne podmioty wraz ze wskazaniem źródeł finansowania. Dokument był konsultowany ze wszystkimi podmiotami zidentyfikowanymi jako uczestnicy realizowanych przedsięwzięć. Aktualizowane zostały również źródła finansowania – dotyczą zarówno budżetu, realizacji zadań statutowych, jak również dwóch nowych mechanizmów, które MC planuje do wykorzystania. Pierwszy – programowanie nowego Programu Operacyjnego Polska Cyfrowa (PO PC 2.0). Drugi instrument wynika bezpośrednio z decyzji na poziomie europejskim, czyli tzw. Funduszu Odbudowy i Odporności. MC przewiduje interwencję w obszar cyberbezpieczeństwa. Z uwagi na wcześniejszą dostępność funduszy w ramach KPO bazującego na Funduszu Odbudowy i Odporności, część tych zadań, które powinny być zrealizowane w pierwszej kolejności została przeniesiona, by podnieść odporność, wpłynąć na funkcjonowanie jednostek samorządu terytorialnego. Te działania, które zostały przewidziane w pierwszej kolejności to: większe wykorzystanie środowisk i usług chmur obliczeniowych, gdzie interwencja powinna dotyczyć jednostek samorządu terytorialnego dla wzmocnienia ich infrastruktury do świadczenia usług dla obywateli, większej ochrony przed atakami typu ransomware, wzmocnienie możliwości w zakresie świadczenia usług informacyjnych dla obywateli, czyli samorząd.gov.pl i dalsze kroki w celu wsparcia samorządów. Również rozwiązania mające na celu przyspieszenie prac nad budową rządowej chmury obliczeniowej tak, aby uzyskała szybszą zdolność operacyjną do umieszczenia tam dużej części systemów, od których zależy funkcjonowanie administracji, świadczących także usługi dla przedsiębiorców i obywateli. Są to przedsięwzięcia, które MC przewiduje.

Następnie Pan Dyrektor R. Kośla omówił kierunki projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. W ramach Zespołu Doraźnego przy Kolegium ds. Cyberbezpieczeństwa zostały prowadzone konsultacje. Zespół został uformowany w celu dokonania przeglądu funkcjonowania Krajowego Systemu Cyberbezpieczeństwa. Przyjrzano

się w jaki sposób realizowane są przepisy ustawy o KSC i w jaki sposób ustawa wpływa na podniesienie poziomu cyberbezpieczeństwa w poszczególnych sektorach objętych KSC.

Główne postulaty, które były formułowane pokazywały, że operatorzy usług kluczowych przede wszystkim oczekują większego zrozumienia po stronie szefów firm, w których te usługi kluczowe są świadczone po to, by inwestować w strukturę zajmującą się zarządzaniem bezpieczeństwem, monitorowaniem bezpieczeństwa, reagowaniem na incydenty.

W nowelizacji ustawy jest także założenie, aby operacyjne centra bezpieczeństwa, jako integralne komponenty operatorów usług kluczowych, bądź zespoły realizujące funkcję SOC na rzecz operatorów usług kluczowych były również częścią ekosystemu budowanego wokół systemu S46, czyli systemu budowanego na podstawie art. 46 ustawy o KSC nakładającego na ministra właściwego ds. informatyzacji budowę systemu teleinformatycznego do wymiany informacji o zagrożeniach, także zbierania informacji potrzebnych do dynamicznej analizy ryzyka na poziomie krajowym, do wymiany informacji dotyczących zaleceń, rekomendacji ze strony CSIRT poziomu krajowego. System jest obecnie budowany. Ma zostać uruchomiony z początkiem stycznia przyszłego roku. Wykorzystuje on efekty projektu Narodowej Platformy Cyberbezpieczeństwa, realizowanego przez NASK w konsorcjum z innymi podmiotami projektu.

Pojawiła się inicjatywa, aby zaproponować formułę postawania zespołów ISAC. Format pochodzi ze Stanów Zjednoczonych, ale funkcjonuje w modelu europejskim. Są to działania non profit. Natomiast ich formalne umocowanie w ustawie umożliwiło dołączanie zespołów ISAC, które spełniają wymagania oraz tych, które zbudują sieć wymiany informacji z zespołami CSIRT poziomu krajowego.

Kolejny obszar będący przedmiotem dyskusji w ramach Zespołu Doraźnego przy Kolegium ds. Cyberbezpieczeństwa to sposób zwiększenia świadomości sytuacyjnej tego, co dzieje się w sektorze telekomunikacyjnym – w jaki sposób powiązać lepsze reagowanie na incydenty bezpieczeństwa w sektorze telekomunikacyjnym oraz ogólne informacje dotyczące incydentów w sektorze telekomunikacyjnych dostępności usług czy zakłóceń w usługach. Te sektory, które znajdują się w dyrektywnie NIS mają wypracowany model zgłaszania incydentów. Każda dziedzina ma swoją regulację, a w jej ramach wprowadzone są mechanizmy raportowania naruszeń czy incydentów. Na poziomie KE prowadzona jest dyskusja i większość państw zgłosiło postulat, aby doszło do harmonizacji kwestii zgłaszania incydentów - przede wszystkim większej świadomości sytuacyjnej i uspójnienia kanałów komunikacyjnych, co do sytuacji mających miejsce w sektorze telekomunikacyjnym.

MC proponuje odwzorowanie przepisów znajdujących się w Europejskim Kodeksie Łączności Cyfrowej (mówiące o organie właściwym ds. cyberbezpieczeństwa dla przedsiębiorstw komunikacji elektronicznej, a także kwestia włączenia w komunikację z CSIRT-ami) w prawie komunikacji elektronicznej po to, aby informacje od zespołów CSIRT i SOC funkcjonujących po stronie operatorów telekomunikacyjnych, czy przedsiębiorców komunikacji elektronicznej trafiały do sektorowego zespołu CSIRT telco równolegle z propozycją powstania czy

przyspieszenia prac nad powstawaniem dedykowanych zespołów CSIRT sektorowych będących bliżej i lepiej znających specyfikę sektora. Brałyby one udział w całym procesie reagowania na incydenty, w których uczestniczą zespoły CSIRT poziomu krajowego. Te zespoły mogłyby na bieżąco i lepiej wspierać operatorów usług kluczowych w poszczególnych sektorach Krajowego Systemu Cyberbezpieczeństwa czy w przypadku CSIRT telco w sektorze telekomunikacyjnym. Taki zapis znalazł się w projekcie ustawy o KSC. Nowelizowana ustawa także wskazuje na to, że zespoły CSIRT sektorowe powinny powstać w ciągu 18 miesięcy, a jeśli nie powstaną, te funkcje mogą być realizowane przez inne zespoły znajdujące się w danym sektorze na podstawie porozumienia pomiędzy właściwymi organami. Ważne jest, aby CSIRT-y sektorowe powstawały. Pierwszym zespołem CSIRT sektorowym cyberbezpieczeństwa jest CSIRT, który powstał przy Komisji Nadzoru Finansowego dla sektora bankowo-finansowego funkcjonujący od 1 lipca tego roku.

W projekcie ustawy o KSC wprowadzona została także realizacja wspólnych zobowiązań podjętych przez państwa UE podczas prac nad realizacją rekomendacji KE z marca zeszłego roku przyjętej wspólnie z państwami odnośnie podniesienia poziomu bezpieczeństwa sieci w UE, w szczególności w kontekście wdrażania sieci 5G. Po przeprowadzeniu krajowych analiz ryzyka państwa członkowskie przekazały raport z tych analiz do KE, która przygotowała raport szczegółowy z obszarami ryzyk. Dodatkowo także ENISA przygotowała dokument, pokazujący zagrożenia specyficzne dla sieci 5G. Dokumenty te były podstawą do wypracowania zbioru środków technicznych strategicznych oraz działań wspierających, które państwa uzgodniły wspólnie z UE i z agencją ENISA. Mają być wprowadzone w regulacjach krajowych dotyczących regulacji rynku telekomunikacyjnego, aspektów cyberbezpieczeństwa, a także wymiany informacji między państwami.

Największy nacisk został położony na kwestię środka strategicznego nr 3, czyli ocenę ryzyka dostawców oprogramowania urządzeń, usług dla potrzeb budowy sieci 5G. Państwa członkowskie UE zobowiązały się do tego, że nowy mechanizm będzie miał większe wymagania bezpieczeństwa dla operatorów telekomunikacyjnych. Są to środki strategiczne 01, 02 - implementowane bezpośrednio w prawie komunikacji elektronicznej. Natomiast, co do kwestii oceny ryzyka dostawców technologii - wymóg wprowadzony został w projektowanym art. 66 do nowelizacji ustawy o KSC. Ocena powinna obejmować aspekty techniczne oraz poza techniczne. Dotyczy przede wszystkim aspektów bezpieczeństwa narodowego, co wynika z dokumentu „5G Toolbox". KE zachęciła państwa członkowie do stosowania nawet dalej idących środków bezpieczeństwa. Trwają dyskusje w jaki sposób przyjmowane są przez państwa członkowie kryteria do oceny ryzyka. Rolą Kolegium ds. Cyberbezpieczeństwa ma być dokonywanie oceny ryzyka dostawców. Wynikiem oceny jest wskazanie poziomu ryzyka. Są 4 poziomy ryzyka: wysokie, umiarkowane, niskie, bądź brak ryzyka.

Pan Dyrektor R. Kośla wspomniał także o wprowadzeniu dla Pełnomocnika Rządu dwóch instrumentów w postaci ostrzeżeń w przypadku pojawienia się informacji na podstawie własnych badań, bądź ze źródeł przekazanych w ramach UE, bądź innych źródeł publicznych

o tym, że ze względu na nową podatność, nowe zagrożenie istnieje duże prawdopodobieństwo wystąpienia incydentu krytycznego. Wprowadzono instrument ostrzeżeń, aby informować, że określona technologia ma określoną podatność, która może spowodować wystąpienie dużego prawdopodobieństwa incydentu krytycznego i co się z tym wiąże, jakie działania należałoby podejmować. Kolejny instrument to polecenie zabezpieczające – pilna interwencja mająca ograniczyć skutki incydentu krytycznego. Polecenie zabezpieczające ma obowiązywać tylko na czas wyjścia z incydentu krytycznego. Jest ono przedmiotem weryfikacji ze strony Kolegium ds. Cyberbezpieczeństwa.

W projekcie została umocowana kwestia zespołów zarządzania kryzysowego, czyli struktura podległa wojewodzie i współpraca wojewody z jednostkami samorządu terytorialnego, również w kontekście obsługi incydentów. Środki finansowe na wsparcie samorządów w zakresie podniesienia poziomu bezpieczeństwa, wyniesienia usług infrastrukturalnych do modelu chmurowego przewidziane są w ramach KPO.

Pojawiło się pytanie odnośnie działań w zakresie cyberbezpieczeństwa zdalnego nauczania. Pan Dyrektor R. Kośla zwrócił uwagę, że podjęto działania wskazujące na wykorzystanie platform wideokonferencyjnych. Równolegle zostały przygotowane materiały w wersji online i udostępnione przez NASK do prowadzenia lekcji wraz z zawartością merytoryczną. Dokonane zostały także inwestycje bezpośrednio w sprzęt w ramach Funduszu Odbudowy i Odporności. Będzie doinwestowywana baza sprzętowa dla nauczycieli. Równolegle kontynuowana zostanie realizacja programu Ogólnopolskiej Sieci Edukacyjnej, która podłączy szkoły do bezpiecznej sieci z możliwością filtrowania zawartości pod katem niebezpiecznych treści, a także ataków. MC pracuje nad platformą edukacyjna, narzędziami, które będą udostępniane dla nauczycieli. Oprócz tego przewidywane są szkolenia dla nauczycieli w zakresie cyberbezpieczeństwa, podnoszenie kwalifikacji nauczycieli. W ramach „zdalnych lekcji" przekazane zostały środki samorządom na zakup urządzeń. Do samorządów należała decyzja czy sprzęt trafiał do nauczycieli czy uczniów.

Pan Dyrektor R. Kośla w kontekście pytania o systemowe zmiany i dofinansowanie wskazał, że obecnie jest uzgodniony plan do strategii cyberbezpieczeństwa – jakie działania muszą być zrealizowane, jakie mają swoje umocowanie w strategii, w realizacji szczegółowych celów strategii. Jest to dokument uzgodniony ze wszystkimi udziałowcami. Są to udziałowcy na poziomie administracji rządowej. W tym dokumencie wskazano także źródła finansowania - źródła budżetowe, a także KPO oraz PO PC 2.0.

Spotkanie w sprawie kradzieży tożsamości i cyberbezpieczeństwa z przedstawicielami Ministerstwa Sprawiedliwości, Prokuratury Krajowej oraz Ministerstwa Cyfryzacji

Spotkanie zostało zainicjowane w związku z Uchwałą nr 7 Rady ds. Cyfryzacji w sprawie działań mających na celu zapobieganie kradzieży tożsamości.

W Ministerstwie Sprawiedliwości toczą się prace dotyczące wprowadzenia zmian do kodeksu karnego w zakresie przede wszystkim zmian znamion czynu kradzieży tożsamości. Przedstawiciele doktryny wskazywali problem, którym jest konieczność tzw. podwójnej

tożsamości: ta zachodzi aktualnie tylko wtedy, gdy ktoś podszywa się pod daną osobę w celu wyrządzenia szkody tej konkretnej osobie, pod którą się podszywa. Jeśli ktoś podszywa się pod daną osobę chcąc wyrządzić szkodę komuś innemu, to tych znamion nie ma. Jest propozycja zmian w tym zakresie. Jest również propozycja zmian w zakresie regulacji podwyższenia zagrożeń karnych dla innych czynów dotyczących szeroko pojętej cyberprzestępczości. Są to czyny z rozdziału 33 kodeksu karnego, ale również pewne zmiany proceduralne dotyczące ułatwień w ściganiu cyberprzestępców i zabezpieczaniu elektronicznego materiału dowodowego.

O przedstawienie ogólnej wizji i potrzeb co do nowelizacji ustawy o KSC poproszono Pana Prokuratora Tomasza Iwanowskiego z Prokuratury Krajowej.

Pan Prokurator wskazał, że każde działanie przestępcze, jeśli chodzi o sferę cyberprzestępczości, wiąże się z kradzieżą tożsamości. Nie chodzi w tym przypadku o definicję prawną, ale to co odczuwamy czy rozumiemy jako zawładnięcie czyjąś tożsamością, danymi osobowymi czy też wizerunkiem. W tych przypadkach w sferze cyberprzestępczości począwszy od wykupienia domeny poprzez monetyzację działań przestępczych, na którymś etapie zazwyczaj mamy do czynienia z sytuacją, gdy sprawcy podszywają się pod cudzą tożsamość. Aktualne rozwiązania prawne, tak w sferze norm karnych jak i w sferze regulującej działalność podmiotów świadczących usługi drogą elektroniczną są niewystarczające, aby skutecznie ścigać cyberprzestępczość. Kwestia priorytetowa to odpowiednie sformułowanie regulacji karnej dotyczącej kradzieży tożsamości. W aktualnym brzmieniu jest ona daleko niewystarczająca, ponieważ jej brzmienie wskazuje, że musi być spełniony warunek tzw. podwójnej tożsamości, czyli po pierwsze czynność sprawcza polega na podszyciu się pod daną osobę, a skutek musi dotyczyć tej samej osoby, co w realiach nie odpowiada potocznie rozumianemu odczuciu, w jaki sposób kradzież tożsamości wygląda czy w jaki sposób zazwyczaj następuje. W zasadzie zmiana art. 190 a § 2 Kodeksu karnego polegałaby na sformułowaniu: „w zamiarze wyrządzenia szkody majątkowej lub osobistej” (takie powinno być brzmienie tego przepisu w przekonaniu organów ścigania) ze skreśleniem jednego wyrazu „jej” czyli odnoszącej się do tożsamości osoby, której dane zostały przechwycone czy też wykorzystane. (Obecnie art. 190 a § 2 Kodeksu karnego brzmi: *Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej.)*

Kolejna sprawa wiąże się z kwestią skuteczności ścigania i możliwości gromadzenia przez organy ścigania dowodów, które doprowadzą do sprawcy. Postulat organów ścigania to także nałożenie obowiązku retencji danych na podmioty świadczące usługi drogą elektroniczną. Okres retencji danych powinien być analogiczny jak aktualnie obowiązuje w przypadku telekomów, czyli 12 miesięcy, które pozwolą na dotarcie do danych i ich zabezpieczenie. Istotne jest również to, aby oprócz danych podstawowych była możliwość zabezpieczenia danych dotyczących portów źródłowych. Te dwie kwestie są nierozerwalnie powiązane.

Kolejny postulat to zaostrzenie kar za typowe cyberprzestępstwa, a także przestępstwa, których ściganie jest uzależnione od złożenia odpowiedniego wniosku przez osobę pokrzywdzoną, aby stały się tzw. przestępstwami względnie wnioskowymi.

Następnie o perspektywie czasowej wprowadzenia zmian w prawie karnym, nad którymi Ministerstwo Sprawiedliwości pracuje oraz co do etapu projektu wypowiedział się Pan Sędzia Rafał Kierzynka z Ministerstwa Sprawiedliwości. Wskazał, że obecnie w sytuacji pandemii, kiedy nie do końca wiadomo w jaki sposób nastąpią prace parlamentu oraz przyjmowanie ustaw, tego terminu nie da się dokładnie przewidzieć. Wstępny projekt zmian przepisów, które znajdują się w kompetencji Ministra Sprawiedliwości jest już gotowy. Być może będą poprawki do projektu, ponieważ MS prowadzi analizy. Jeśli w październiku rozpoczną się konsultacje zmian, to być może jeszcze w październiku bądź listopadzie tego roku zakończą się. Zwrócono uwagę, że w MS procedowana jest tzw. duża nowelizacja kodeksu karnego. Kierownictwo Ministerstwa wstępnie zadecydowało, że zmiany dotyczące cyberprzestępczości, które w większości są zmianami właśnie w kodeksie karnym, powinny znaleźć się w ramach tej dużej nowelizacji, a ponieważ jest rozległa i dotyczy różnych sfer trudno wypowiedzieć się na temat potencjalnej możliwej daty uchwalenia przepisów.

Wyrażono przekonanie, że Rząd przyjmie propozycję - czy jako osobną ustawę czy jako część nowelizacji kodeksu karnego, jeszcze w tym roku. Są to zmiany techniczne, mało kontrowersyjne w odniesieniu do prawa karnego, więc można spodziewać się dosyć sprawnego procedowania. Jeżeli Rząd przyjmie projekt ustawy w tym roku, to nic nie stoi na przeszkodzie, aby w I kwartale przyszłego roku ta ustawa została przyjęta przez Sejm.

W toku dyskusji pojawiła się także propozycja przygotowania zmian w UŚUDE, tak aby możliwe było ustalenie sprawców większości cyberprzestępstw, którzy działają w naszym kraju i wykorzystują polską infrastrukturę.

Zauważono, ze dyskusja toczy się dwutorowo - w zakresie zmian w kodeksie karnym oraz w zakresie szeroko rozumianej retencji podmiotów regulowanych w UŚUDE. Przepisy, na temat których toczy się dyskusja, aby były skuteczne, musiałyby obowiązywać bardzo szeroko i ewentualne zaproponowane zmiany musiałyby objąć podmioty, które regulowane są nie tylko przez UŚUDE, ale także szerzej.

Dostrzeżono także, że zmiany wpłyną na rynek i być może już na poziomie założeń powinny być konsultowane z zainteresowanymi podmiotami.

Obecny na posiedzeniu Pan Dyrektor Robert Kośla wskazał, że przy przygotowywaniu omawianych przepisów trzeba wziąć pod uwagę stanowisko TSUE co do retencji danych, ponieważ w tym roku w styczniu pojawiła się opinia Rzecznika Generalnego TSUE podważająca przepisy regulujące retencje danych i dostęp do danych w trzech państwach. Należy zatem, skonfrontować propozycje przepisów z aktualną wykładnią TSUE w kontekście retencji.

W toku dyskusji uznano, że wprowadzenie proponowanych zmian jest konieczne i trzeba je dokonać jak najszybciej. Dyskutowano o sposobie zwrócenia uwagi strony rządowej na ten ważny temat.

Podsumowując dyskusję Pan Dyrektor Jan Kostrzewa z Ministerstwa Sprawiedliwości wskazał, że MS wyczuwa bardzo silną potrzebę zmian w zakresie wyżej omawianych przepisów i podjęło kroki w zmianach prawa karnego. Te zmiany, jeśli pandemia COVID-19 w tym nie przeszkodzi, powinny nastąpić w I kwartale 2021 r. Są oczekiwania MS, że po zmianach organizacyjnych dotyczących Ministerstwa Cyfryzacji, ten temat zostanie zagospodarowany tak, aby organy ścigania mogły działać efektywnie.

Dyskusja wewnętrzna dotycząca stanowiska Rady w sprawie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Rada uzgodniła treść wspólnego stanowiska w sprawie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska – Jentkiewicz
3. Jan Maciej Czajkowski
4. Jacek Czarnecki
5. Paweł Gora
6. Agnieszka Gryszczyńska
7. Michał Kanownik
8. Anna Beata Kwiatkowska
9. Dariusz Milka - Wiceprzewodniczący
10. Józef Orzeł – Przewodniczący
11. Rafał Rodziewicz
12. Włodzimierz Schmidt
13. Sebastian Szymański

Zaproszeni goście:

14. Jan Kostrzewa, Dyrektor Biura Cyberbezpieczeństwa w Ministerstwie Sprawiedliwości
15. Rafał Kierzynka, Główny Specjalista – Sędzia z Wydziału Prawa Karnego, Departament Legislacyjny Prawa Karnego w Ministerstwie Sprawiedliwości
16. Tomasz Iwanowski, Kierownik Działu do Spraw Cyberprzestępczości, Departament do Spraw Przestępczości Gospodarczej w Prokuraturze Krajowej
17. Wiesław Paluszyński, ekspert
18. Jarosław Mojsiejuk, ekspert
19. Przemysław Sypniewski, ekspert
20. Krzysztof Komorowski, ekspert

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

21. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczpospolitej Polskiej
22. Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa MC
23. Tomasz Proć, Zastępca Dyrektora Departamentu Telekomunikacji w MC
24. Michał Pukaluk, Dyrektor Departamentu Polityki Międzynarodowej w MC

25. Łukasz Wojtachnio, Główny Specjalista ds. legislacji, Departament Prawny MC
26. Monika Skrzyńska, Zastępca Dyrektora Biura Ministra w MC
27. Joanna Laskowska, MC