STANOWISKO RZĄDU

I. METRYKA DOKUMENTU

Tytuł
KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego.

Data skierowania wniosku przez Parlament RP	Data przyjęcia stanowiska przez Komitet do Spraw Europejskich
22 lipca 2016 r.	

Sygnatura Komisji Europejskiej	COM(2016)410

Instytucja wiodąca
Ministerstwo Cyfryzacji

Instytucje współpracujące
Ministerstwo Obrony Narodowej Ministerstwo Spraw Zagranicznych Ministerstwo Spraw Wewnętrznych i Administracji Ministerstwo Rozwoju Ministerstwo Finansów Ministerstwo Sprawiedliwości Ministerstwo Zdrowia Ministerstwo Infrastruktury i Budownictwa Agencja Bezpieczeństwa Wewnętrznego Rządowe Centrum Bezpieczeństwa Generalny Inspektor Ochrony Danych Osobowych Kancelaria Prezesa Rady Ministrów Urząd Regulacji Energetyki Urząd Komunikacji Elektronicznej Urząd Lotnictwa Cywilnego Centrum Usług Wspólnych Komenda Główna Policji

II. CEL DOKUMENTU

Komisja Europejska wskazuje że celem Komunikatu jest znalezienie sposobów na radzenie siebie ze zmieniającą się rzeczywistością w dziedzinie bezpieczeństwa cybernetycznego oraz ocena dodatkowych środków, które mogą być potrzebne do zwiększenia odporności cybernetycznej UE oraz usprawnienia reagowania na incydenty komputerowe.

Komisja zwraca uwagę na zdolności przemysłowe Unii Europejskiej – dostarczanie produktów i usług, które zapewnią najwyższy poziom bezpieczeństwa cybernetycznego jest szansą dla europejskiej branży bezpieczeństwa cybernetycznego i w konsekwencji może stanowić przewagę konkurencyjną europejskiego przemysłu.

W związku z tym, zdaniem Komisji, niezbędne jest silne zaangażowanie polityczne poprzez m.in.:

- zintensyfikowanie współpracy w celu zwiększenia gotowości i reagowania na incydenty cybernetyczne;
- pokonywanie wyzwań stojących przez jednolitym rynkiem bezpieczeństwa cybernetycznego Europy;
- rozwijanie zdolności przemysłowych w dziedzinie bezpieczeństwa cybernetycznego.

III. DOKUMENTY POWIĄZANE

- Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń;
- Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013r. dotycząca ataków na systemy informatyczne;
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii;
- Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno – Społecznego i Komitetu Regionów pn. Strategia jednolitego rynku cyfrowego dla Europy, COM (2015) 192;
- Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej i Rady pn. Realizacja Europejskiej agendy bezpieczeństwa w celu zwalczania terroryzmu i utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa, COM (2016) 230.

IV. STANOWISKO RZĄDU

Rząd RP popiera zapowiedziane działania mające na celu wzmocnienie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego. Rozpoczęta w drugiej połowie XX wieku rewolucja informacyjna spowodowała usprawnienie środków komunikowania i umiędzynarodowiła przepływ informacji.

Rząd RP dostrzega istotę nowych zagrożeń w cyberprzestrzeni, które wciąż ewoluują i nabierają większego znaczenia, w związku z przenoszeniem kolejnych sfer życia i działalności człowieka do wymiaru wirtualnego. W życiu społecznym i gospodarczym bardzo istotną rolę odgrywają obecnie nowe technologie oraz Internet. Są to zasoby o znaczeniu krytycznym, ponieważ opierają się na nich

wszystkie sektory gospodarki. Dlatego bardzo ważne jest wzmacnianie odporności na incydenty cybernetyczne, tak aby gospodarka i społeczeństwo mogły bez zakłóceń funkcjonować i rozwijać się.

Zagrożenia cybernetyczne mają charakter transnarodowy. Dotyczą całych sektorów krytycznych, a nie konkretnych państw. Niezbędna staje się więc współpraca międzynarodowa w zakresie wymiany informacji o incydentach, a także wymiany wiedzy i technologii. Jednocześnie jednak należy pamiętać o tym, że bezpieczeństwo narodowe jest jedną z prerogatyw państw członkowskich. W związku z tym wszelkie działania podejmowane przez KE w zakresie cyberbezpieczeństwa, zarówno w zakresie rozbudowy potencjału cyberbezpieczeństwa UE, jak i wymiany informacji na temat incydentów powinny być szczegółowo konsultowane z państwami członkowskimi.

Dyrektywa Parlamentu Europejskiego i Rady z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, daje prawne podstawy współpracy pomiędzy państwami członkowskimi zarówno na poziomie polityczno – strategicznym, jak i operacyjnym. Utworzenie Grupy Współpracy oraz sieci CSIRT to bardzo ważne elementy systemu i potencjał na zwiększenie odporności cybernetycznej UE. Aby polityczna i operacyjna współpraca mogła się rozwinąć i funkcjonować bez zakłóceń konieczne są nowe działania, pod warunkiem, że są one komplementarne w stosunku do już istniejących inicjatyw i działań.

Rząd RP z zadowoleniem odnotowuje zintensyfikowane działania na poziomie UE w celu zwiększenia odporności Unii pod względem bezpieczeństwa w cyberprzestrzeni oraz usprawnienia reagowania na zagrożenia w tym obszarze. Transgraniczność, elastyczność i innowacyjność tego rodzaju przestępczości powoduje, że założenia w tym obszarze muszą być stale aktualizowane. Biorąc powyższe pod uwagę, pierwszą linią obrony przed cyberprzestępczością powinno być dążenie do stałego wzmacniania bezpieczeństwa i budowania zdolności w cyberprzestrzeni. W tym kontekście na szczególną uwagę zasługuje dalsze rozwijanie zdolności Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu oraz synergii pomiędzy istniejącymi i rozwijanymi inicjatywami, celem zwiększenia skuteczności współpracy w tym obszarze.

Nie bez znaczenia pozostają postanowienia Szczytu NATO w Warszawie dotyczące przyjęcia cyberprzestrzeni jako kolejnej domeny działań militarnych oraz związane z tym zobowiązania rozwijania zdolności w zakresie obrony cybernetycznej, które nadały nową wagę zagadnieniom bezpieczeństwa cybernetycznego. Osiągane zdolności w zakresie obrony cybernetycznej będą regularnie sprawdzane praktycznie podczas testów oraz ćwiczeń narodowych i międzynarodowych, w których pożądane jest aby uczestniczyły również właściwe podmioty UE. Celem optymalizacji i racjonalizacji ponoszonych przez Polskę kosztów związanych z członkostwem w UE i NATO oraz ustanowienia jednolitych kierunków działania, wszelkie inicjatywy podejmowane w obszarze bezpieczeństwa cybernetycznego w ramach Unii Europejskiej powinny być rozważane w kontekście działań już prowadzonych, bądź planowanych przez Sojusz Północnoatlantycki.

Mając na uwadze powyższe oraz wolę członków Sojuszu Północnoatlantyckiego wzmacniania bezpieczeństwa cybernetycznego w regionie Euro-Atlantyckim, poprzez wspieranie współpracy między NATO i Unią Europejską, Rząd RP popiera wszelkie inicjatywy UE na rzecz wzmocnienia europejskiego systemu odporności cybernetycznej. Inicjatywy te powinny być spójne z inicjatywami realizowanymi przez NATO oraz jednocześnie nie powinny się duplikować. Takie podejście powinno zapewnić synergię między działaniami państwa, które podejmuje jako członek Sojuszu Północnoatlantyckiego oraz Unii Europejskiej, a także optymalizacji i racjonalizacji ponoszonych z tego tytułu kosztów.

Rząd RP popiera stanowisko KE, mówiące że konieczne jest zaangażowanie polityczne poprzez zintensyfikowanie współpracy w celu zwiększenia gotowości i zdolności do reagowania na incydenty

cybernetyczne oraz pokonywanie wyzwań stojących przed jednolitym rynkiem bezpieczeństwa cybernetycznego Europy. Niemniej ważne jest ażeby działania te były dobrze zaplanowane, przy ich wykonywaniu wykorzystywano potencjał już istniejących i sprawdzonych struktur, a nowe podmioty powoływane były jedynie w przypadku niemożności realizacji powierzonych zadań przez już istniejące struktury/ciała. Główną korzyścią wykorzystania istniejących struktur jest unikanie powielania mandatów i zadań prowadzących do braku jasności i nieefektywności realizowanych działań.

Warto zauważyć, że niektóre z przedstawionych w Komunikacie rozwiązań mających na celu wzmocnienie europejskiego systemu odporności cybernetycznej już w Polsce funkcjonują m.in. w resorcie obrony narodowej (RON). W szczególności od 2008r. w strukturach RON działa System Reagowania na Incydenty Komputerowe, który współpracuje z NATO Cyber Incident Response Capability oraz innymi Zespołami Reagowania na Incydenty Komputerowe w zakresie reagowania na incydenty w sferze bezpieczeństwa cybernetycznego oraz wymiany informacji o potencjalnych zagrożeniach cybernetycznych. Zgodnie z planami UE odpowiednie aspekty bezpieczeństwa cybernetycznego mają także zostać włączone do istniejących mechanizmów zarządzania kryzysowego, co miało już miejsce w przypadku RON.

Nie ulega wątpliwości, że wzmacnianie europejskiego systemu odporności cybernetycznej powinno iść w parze z ochroną praw jednostki. W związku z powyższym Komisja powinna rozważyć, jaką rolę pełni obywatel w procesie tworzenia ram bezpieczeństwa cybernetycznego w Europie. Projektując rozwiązania na szczeblu unijnym koniecznym wydaje się tworzenie ram prawnych zgodnych z Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które będzie stosowane od dnia 25 maja 2018r. oraz z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych. Należy rozważyć realną pomoc jaką mogą oferować organy unijne stanowiące centrum kompetencyjne w tym zakresie, co może wiązać się z koniecznością poniesienia pewnych kosztów.

Wszelkie decyzje związane z wykonywaniem zadań przewidzianych Komunikatem powinny być, na każdym etapie, konsultowane z Państwami Członkowskimi. Zależy nam na zbudowaniu spójnego systemu cyberbezpieczeństwa Europy, w oparciu o współpracę i jasne zasady zaakceptowane przez wszystkie Państwa. Najlepszym Forum do tego rodzaju zaangażowania i dyskusji jest działająca przy Radzie tzw. Grupa Przyjaciół Prezydencji ds. Cyberbezpieczeństwa (*Friends of the Presidency Group on Cyber Issues*). To właśnie na forum tej grupy toczą się dyskusje obejmujące szerokie spektrum tematów z zakresu cyberbezpieczeństwa. Mandat tej Grupy na kolejne lata powinien być skonstruowany tak, ażeby Państwa Członkowskie mogły w pełni wykorzystać jej potencjał. W szczególności zakomunikowana ewentualna aktualizacja unijnej strategii w zakresie bezpieczeństwa cybernetycznego z 2013r. powinna być szeroko dyskutowana. Polska w ten proces chciałaby się szczególnie zaangażować.

I. Rząd RP opowiada się za jak najpełniejszym wykorzystaniem mechanizmów współpracy w zakresie bezpieczeństwa sieci i informacji.

Budowanie Wspólnego Centrum Badawczego (dalej: Centrum) we współpracy z ENISĄ oraz CERT-UE, tak aby wiedza na temat bezpieczeństwa cybernetycznego na poziomie UE została scentralizowana to bardzo ambitne zadanie. Niezbędne jest wypracowanie takich mechanizmów/ procedur powstania Centrum aby w pełni wykorzystać potencjał specjalistów z poszczególnych państw członkowskich. Z

punktu widzenia odporności na ataki, Centrum powinno funkcjonować bardziej w formie chmury niż wydzielonej geograficznie instytucji. Wszyscy partnerzy takiego Centrum powinni otrzymywać pełne informacje o aktualnie pojawiających się zagrożeniach. Polska chciałaby aktywnie uczestniczyć w procesie tworzenia Centrum. Jako rozwinięcie pomysłu stworzenia 'ośrodka informacji' warto rozważyć stworzenie *Cybersecurity Observatory* jako podstrony prowadzonego przez Komisję Europejską portalu https://joinup.ec.europa.eu/ lub agencji ENISA. Jednocześnie, z punktu widzenia praw jednostki oraz bezpieczeństwa narodowego a także transparentności przetwarzania danych, należy uszczegółowić zasady funkcjonowania Centrum oraz uściślić w jakim zakresie i w jakim celu gromadzone będą dane oraz tryb dostępu przez wszystkie państwa członkowskie do gromadzonych informacji.

Ponadto Rząd RP stoi na stanowisku, że przy tworzeniu grupy doradczej wysokiego szczebla ds. bezpieczeństwa cybernetycznego (dalej: grupa doradcza) złożonej z ekspertów i decydentów ważne jest zaangażowanie wszystkich podmiotów wchodzących w skład systemu cyberbezpieczeństwa, poczynając od przedstawicieli przemysłu, środowiska akademickiego oraz społeczeństwa obywatelskiego i innych pozarządowych organizacji. Ustanawiając grupę doradczą należy zadbać by uwzględniono zasady transparentnego i bezpiecznego przetwarzania danych z uwagi na skalę i ich rodzaj.

W Polsce trwają obecnie prace nad kompleksową Strategią Cyberbezpieczeństwa dla RP, która m.in. wypełni obowiązki wynikające z dyrektywy NIS. Jednym z elementów będzie Forum ds. Cyberbezpieczeństwa (dalej: Forum), w którego prace chcemy zaangażować wszystkie chętne do współpracy podmioty. Widzimy potencjał na współpracę pomiędzy planowaną grupą doradczą a polskim Forum.

Rząd RP popiera także jak najszybsze odnowienie mandatu Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (dalej: ENISA). W obliczu wzrastających zagrożeń cybernetycznych niezwykle ważne jest aby agencja ta wspierała państwa członkowskie swoją wiedzą ekspercką. Niezbędne jest przeanalizowanie zadań ENISY w kontekście dyrektywy w sprawie bezpieczeństwa sieci i informacji, min. jako sekretariatu sieci CSIRTów. Takie działania mogą zostać podjęte m.in. na forum, wspomnianej powyżej, Grupy Przyjaciół Prezydencji ds. Cyberbezpieczeństwa.

Uważamy, że warto angażować we współpracę inne, już istniejące regionalne organizacje/ podmioty zajmujące się sprawami cyberbezpieczeństwa. Do takich podmiotów należy m.in. Central European CyberSecurity Platform (CECSP), w skład której wchodzą Polska, Austria, Czechy, Słowacja i Węgry. Państwa CECSP spotykają się zazwyczaj 2 razy do roku. Kilkudniowe spotkania poświęcone są zarówno kwestiom strategicznym jak i czysto technicznym. W tym roku Polska sprawuje roczne przewodnictwo w CECSP.

II. Rząd RP popiera zwiększanie wysiłków w zakresie kształcenia, szkoleń i ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego.

Inicjatywą Unii Europejskiej godną szczególnego poparcia jest propozycja rozwijania współpracy cywilno-wojskowej i budowanie synergii w obszarze szkoleń i ćwiczeń. Praktyczne sprawdzenie zdolności w zakresie reagowania na incydenty komputerowe oraz wymiany informacji w środowisku międzynarodowym pozwala uzyskać unikatowe doświadczenia oraz w sposób obiektywny ocenić słuszność przyjętych założeń w zakresie struktur organizacyjnych, procedur oraz szkoleń stanowiących ścieżkę rozwoju specjalistów. Potwierdzeniem tego jest ćwiczenie Anakonda-16, podczas którego w środowisku międzynarodowym, równolegle do działań operacyjnych, realizowane były praktyczne działania z zakresu cyber. Mając na uwadze powyższe integracja udziału w ćwiczeniach kolejnych podmiotów wojskowych i cywilnych oraz podmiotów funkcjonujących w ramach struktur UE pozwoliłaby na dalsze wzbogacenie formuły prowadzonych szkoleń i ćwiczeń

obronnych. Słusznym wydaje się więc ustanowienie przez UE platformy na rzecz edukacji, ćwiczeń i szkoleń w dziedzinie bezpieczeństwa cybernetycznego, której zadaniem byłoby propagowanie synergii między szkoleniami/ćwiczeniami cywilnymi a szkoleniami/ćwiczeniami obronnymi. Wspólne ćwiczenia bez wątpienia podniosą bezpieczeństwo cybernetyczne Europy.

Należy jednak uwzględnić inną specyfikę szkoleń organizowanych na wypadek kryzysu cybernetycznego w sferze cywilnej (w szczególności dotyczących sektorów krytycznych) oraz odmienną od niej, związaną z cybernetycznym komponentem ćwiczeń wojskowych. Warto zauważyć, że na poziomie europejskim przeprowadzane jest już kilka bardzo istotnych ćwiczeń m.in. organizowane przez ENISA ćwiczenia CyberEurope. Jednak to wciąż za mało.

Konieczny jest jasny i precyzyjny europejski system kształcenia, szkoleń, treningów i testów. System ten powinien zostać opracowany tak, ażeby odpowiadał potrzebom i zdolnościom Państw członkowskich oraz powinien być organizowany przy ich współudziale. Warto przy okazji wykorzystać fora tj. niedawno powołane Europejskie Stowarzyszenie Cyberbezpieczeństwa (ECSO), w ramach którego rozpoczną się wkrótce prace grupy roboczej poświęconej właśnie tej problematyce. Jednocześnie w celu zapewnienia spójności działań i zwiększania zdolności w zakresie kształcenia i szkoleń w dziedzinie bezpieczeństwa cybernetycznego bardzo istotne jest stałe rozwijanie współpracy w tym zakresie z Europejskim Centrum ds. Walki z Cyberprzestępczości przy Europolu (EC3) oraz Agencją Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL).

III. Rząd RP jednoznacznie opowiada się za współpracą transgraniczną i międzysektorową w celu osiągnięcia wyższej gotowości i odporności na incydenty cybernetyczne.

Konieczne jest skoordynowane podejście do współpracy w sytuacjach kryzysowych. Dlatego bardzo ważnym elementem są, wspomniane powyżej, ćwiczenia cybernetyczne, pozwalające testować procedury i zasady współpracy pomiędzy państwami członkowskimi. Nie mogą mieć one jednak charakteru „wyspowego", a powinny odpowiadać konkretnym potrzebom i aktualnym realnym zagrożeniom. Ochrona infrastruktury krytycznej oraz mechanizmy zarządzania kryzysowego powinny uwzględniać specyfikę zagrożeń cybernetycznych. Ważne jest więc, aby w zaprezentowanym przez KE planie działań w zakresie współpracy uwzględniono również te elementy.

Warto także zaznaczyć, że choć dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej (dalej: EIK) oraz oceny potrzeb w zakresie poprawy jej ochrony nie odnosi się w sposób bezpośredni do zagrożeń teleinformatycznych, to zakres rozwiązań służących ochronie EIK uzależniony jest od oceny ryzyka zakłócenia jej funkcjonowania i nie wyklucza ujęcia w planie ochrony zapewnienia bezpieczeństwa teleinformatycznego (zakres POI określono w załączniku nr 2 do dyrektywy). W treści samej dyrektywy zaznaczono również, że: „W stosownym przypadku i w połączeniu z przeglądem niniejszej dyrektywy, jak określono w art. 11, można określić kolejne sektory, które będą wykorzystane do celów wprowadzenia niniejszej dyrektywy w życie. Priorytet nadaje się sektorowi ICT".

W celu harmonizacji i wzajemnego uzupełniania się dyrektyw 2008/114/WE oraz dyrektywy NIS warto rozważyć podjęcie działań w tym temacie. W kontekście oceny międzysektorowej należy mieć na uwadze potrzebę rozróżnienia ryzyka incydentów cybernetycznych, którego oceny dokona Komisja, od oceny ryzyka na szczeblu krajowym lub odpowiednim niższym szczeblu dokonywanym przez państwa członkowskie, a wynikającym z Unijnego Mechanizmu Ochrony Ludności. Na tej podstawie kraje członkowskie były zobowiązane do 22 grudnia 2015 r. udostępnić Komisji streszczenia istotnych elementów oceny ryzyka opracowanego na poziomie krajowym lub odpowiednio niższym szczeblu, co Polska uczyniła. Istnienie krajowej albo regionalnej oceny ryzyka jest także jednym z warunków *ex-ante* zawartych w dziale A5 Poradnika z zakresu warunków *ex-ante* dla europejskich funduszy strukturalnych i inwestycyjnych („Guidance on Ex Ante Conditionalities for

the European Structural and Investment Funds”). W obydwu przypadkach, może być wzięte pod uwagę, zakłócenie dostaw kluczowych usług na skutek ataku teleinformatycznego. Niepożądane byłoby zatem nakładanie się tych ocen.

Uzupełniając działania określone w komunikacie Komisja Europejska mogłaby rozważyć stworzenie metodologii oceny postępów w osiąganiu dojrzałości w obszarze bezpieczeństwa sieci i informacji w sektorach objętych zakresem dyrektywy NIS. Wprowadzenie metody pomiaru mogłoby mieć na celu lepsze zrozumienie istniejących luk, a tym samym bardziej właściwe formułowanie wniosków co do dalszych działań podejmowanych przez Komisję Europejską gdzie priorytet powinien zostać przyznany prawidłowemu wdrożeniu obecnie obowiązującej legislacji. W proponowaniu i ocenie realizacji swoich działań Komisja Europejska powinna kierować się *Programem UE – Lepsze wyniki dzięki lepszemu stanowieniu prawa* przyjętym w maju 2015 roku, w szczególności pkt. 2.2. *Bardziej zrozumiałe wyjaśnianie, co robimy i dlaczego.*[1]

IV. Rząd RP popiera zwiększenie skali inwestycji w dziedzinie bezpieczeństwa cybernetycznego w Europie i wsparcia dla MŚP oraz opowiada się za pobudzeniem i wspieraniem rozwoju europejskiej branży bezpieczeństwa cybernetycznego przez innowację oraz utworzenie kontraktowego partnerstwa publiczno – prywatnego (dalej: cPPP).

Polskę cieszy fakt, że 5 lipca w Brukseli podpisano umowę o współpracy pomiędzy European Cyber Security Organisation (ECSO), a Komisją Europejską. Przedstawiciel Polski będzie zasiadał w pierwszej kadencji Rady Dyrektorów. Popieramy ideę cPPP, tzn. wzmacnianie konkurencyjności europejskiego przemysłu, m.in. poprzez wykorzystanie przez przedsiębiorców funduszy dostępnych z programu HORYZONT 2020. Rząd RP wierzy, że wspólne działania przedsiębiorców i wspólnie realizowane projekty pomogą nie tylko zwiększyć innowacyjność sektora, ale też przyczynią się do wymiany doświadczeń i wiedzy pomiędzy zaangażowanymi europejskimi partnerami. Należy dążyć do budowy silnych europejskich firm branży IT, które będą mogły z powodzeniem konkurować w globalnej gospodarce. Bez posiadania przez UE zdolności do rozwoju technologicznego, nie będzie możliwe zbudowanie bezpieczeństwa cybernetycznego. Szczególną uwagę trzeba zwrócić na europejskie MŚP – które mają ogromny potencjał rozwoju na skalę światową. Wieloletnie zapóźnienia w tym zakresie należy jak najszybciej zlikwidować. Nie będzie to możliwe bez dostępu do funduszy, które powinny być zapewnione na poziomie EU poprzez różne źródła tj. HORYZONT 2020.

V. W dziedzinie certyfikacji i oznakowania Rząd RP stoi na stanowisku, że KE powinna w swoich pracach wziąć pod uwagę istniejące już lub wypracowywane obecnie krajowe zdolności w zakresie certyfikacji.

Obecnie w Polsce trwają prace nad wdrożeniem krajowego systemu oceny i certyfikacji w oparciu o międzynarodową normę ISO/IEC 15408 (tzw. Common Criteria). Docelowo planowane jest włączenie tego systemu do systemu europejskiego SOG-IS. Koniecznym może okazać się ustanowienie na poziomie europejskim profili ochrony (protection profile) dla określonych kategorii produktów przemysłu ICT, tak aby można było w pełni wdrożyć wzajemne uznawanie certyfikatów. Niemniej Rząd RP stoi na stanowisku, że w zakresie bezpieczeństwa narodowego wzajemne uznawanie certyfikatów powinno mieć charakter fakultatywny.

V. UZASADNIENIE STANOWISKA RZĄDU

[1] W każdym przypadku musimy lepiej tłumaczyć, dlaczego podejmujemy określone działania, jakich wyników oczekujemy i jakie mogą być ich skutki. Każdemu wnioskowi Komisji będzie towarzyszyło lepsze niż dotychczas uzasadnienie 5 . Oprócz wyjaśnienia celu proponowanego środka będzie ono zawierało informacje, w jaki sposób zastosowano zasady lepszego stanowienia prawa: dlaczego konieczne jest dana inicjatywa, dlaczego jest najlepszym instrumentem, który może w danej sytuacji wykorzystać UE, jaka jest opinia zainteresowanych stron i jakie są prawdopodobne skutki środowiskowe, społeczne i gospodarcze, zwłaszcza dla konkurencyjności oraz małych i średnich przedsiębiorstw (MŚP). Uzasadnienie będzie również zawierało bardziej szczegółowe wyjaśnienie, w jaki sposób dana inicjatywa jest zgodna z dwiema zasadami: pomocniczości (dlaczego cel nie może zostać osiągnięty samodzielnie przez państwa członkowskie) oraz proporcjonalności (dlaczego proponowany środek nie wykracza poza to, co jest konieczne dla osiągnięcia celu).

Wobec zmienianej się sytuacji międzynarodowej i wzrostu znaczenia nowych technologii, cyberbezpieczeństwo jest obecnie równie istotnie dla bezpieczeństwa poszczególnych państw, w tym Polski, jak bezpieczeństwo militarne czy ekonomiczne. Cyberprzestrzeń nie posiada granic, analogicznych do tych państwowych. Dlatego aby skutecznie przeciwdziałać zagrożeniom cybernetycznym i minimalizować ich skutki niezwykle ważna jest umiejętność skutecznego działania i współpracy ponad granicami.

Świadomość zagrożeń istniejących w cyberświecie i świadomość tego, jak można ich uniknąć, mimo niemal 20 lat istnienia Internetu i stopniowego przenoszenia się życia społecznego do wirtualnej rzeczywistości, wciąż jest stosunkowo niska.

Internet i technologie cyfrowe dokonują prawdziwej rewolucji w naszym codziennym życiu. Z dnia na dzień do sieci Internet podpinanych zostaje coraz więcej urządzeń. W Polsce liczbę takich urządzeń szacuje się już w dziesiątkach milionów. Urządzania te wykorzystywane w różnych celach, prywatnych bądź służbowych, czy biznesowych mogą w każdym czasie zostać zainfekowane złośliwym oprogramowaniem.

Dlatego też tak ważne są wszelkie inicjatywy, w tym te wskazane w Komunikacie, które w konsekwencji wzmocnią system cyberbezpieczeństwa nie tylko poszczególnych państw członkowskich ale i całej Unii Europejskiej.

Konsekwencje Komunikatu COM 11013/16

GOSPODARCZE: Komunikat, odwołuje się do wzrostu konkurencyjności europejskiego przemysłu segmentu cyberbezpieczeństwa m.in. poprzez kontraktowe Partnerstwo Publiczno-Prywatne. Aktywne uczestnictwo polskich podmiotów w projekcie ECSO – da naszym krajowym przedsiębiorcom nie tylko dostęp do funduszy z programu HORYZONT 2020, ale także możliwość zdobycia dodatkowej wiedzy i nowych partnerów biznesowych.

BUDŻETOWE: Trudno jest oszacować, bez podania przez KE szczegółów dotyczących poszczególnych inicjatyw, jakie potencjalne konsekwencje finansowe może wywołać dla Polski niniejszy Komunikat.

LEGISLACYJNE: Komunikat *per se* nie niesie za sobą konieczności zmiany obowiązujących w Polsce przepisów prawa. Natomiast, w świetle przyjęcia dyrektywy NIS w lipcu br. Polska, jak i pozostałe państwa członkowskie jest zobowiązania wdrożyć postanowienia dyrektyw do polskiego porządku prawnego. Obecnie w Ministerstwie Cyfryzacji trwają zaawansowane prace nad projektem ustawy o krajowym systemie cyberbezpieczeństwa.

VI. STANOWISKO PARTNERÓW SPOŁECZNYCH

FUNDACJA CYBERETYKA

W nawiązaniu do komunikatu KE dot. konsultacji społecznych odnośnie cyberbezpieczeństwa pragniemy jako Fundacja CyberEtyka wyrazić swoje pełne poparcie dla wszelkich działań polskiego rządu dot. wzmocnienia w pierwszej kolejności polskiego systemu odporności cyberetycznej jak i wypracowywaniu wspólnych rozwiązań w ramach systemów europejskich.

Przeglądając załączony na stronie Ministerstwa dokument cieszymy się z opisanych tam planowanych przez KE działań i pragniemy wyrazić swoją gotowość do współpracy z polskimi instytucjami rządowym w tym zakresie.

Dostrzegamy jednak, że o ile kierunek tych działań w naszej ocenie jest jak najbardziej prawidłowy o tyle brakuje w tych dokumentach specjalnego akcentu na Edukację najmłodszych obywateli. W

dokumencie (rozdział 2.2) jest co prawda mowa o kształceniu, szkoleniach i ćwiczeniach w dziedzinie bezpieczeństwa cybernetycznego, nie mniej zawężając ten zakres do wyłącznie zapobiegania incydentom w sferze bezpieczeństwa i postępowania z ich skutkami może być nie wystarczający.

Jesteśmy zdania, że naukę tzw. "CyberEtyki" należy rozpocząć u podstaw, od najmłodszych lat. Zachęcamy do skorzystania z naszych jako Fundacji doświadczeń w tej kwestii, być może wspólnego rozwijania programu edukacyjnego dla szkół elementarnych, do wspólnego opracowania w ramach partnerstwa programu informatyka 2.0 czy nawet wprowadzenia dodatkowego przedmiotu nauczania tzw "CyberEtyki" - podchodzącego kompleksowo do kwestii zw. z bezpieczeństwem teleinformatycznym i cyberbezpieczeństwem.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki w pełni wspiera wszelkie działania podejmowane na rzecz wzmacniania cyberbezpieczeństwa Unii Europejskiej, jak również przyczyniające się do propagowania wzrostu podaży produktów i usług ze strony unijnego sektora bezpieczeństwa cybernetycznego. Realizując swoje projekty (przede wszystkim organizując Europejskie Forum Cyberbezpieczeństwa – CYBERSEC oraz Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL), angażując się w inicjatywy krajowe i międzynarodowe działamy na rzecz realizacji tych celów. Wspierając idee jakie przyświecają działaniom przewidzianym w KOMUNIKACIE KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW: *Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego*, chcielibyśmy zwrócić uwagę na kilka poniżej zawartych elementów.

Komunikat ma charakter dokumentu strategicznego na wysokim poziomie ogólności. Tezy z pkt. 3-4 (Stawianie czoła wyzwaniom stojącym przed jednolitym rynkiem bezpieczeństwa cybernetycznego) stanowią powtórzenie postulatów z Komunikatu o utworzeniu kontraktowego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa (PPP) oraz towarzyszących mu dokumentów (przede wszystkim: European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe - A report to M. Günther H. Oettinger European Commissioner for Digital Economy and Society). Dlatego dopiero uszczegółowienie zapisów pozwoli lepiej ocenić proponowane w Komunikacie działania.

Komunikat zakłada wzmocnienie istniejących oraz uzgodnienie nowych mechanizmów współpracy i szybkiej wymiany informacji w obliczu kryzysów cybernetycznych. Intencją KE jest przeciwdziałanie rozproszeniu i brakowi organizacji wiedzy eksperckiej poprzez utworzenie unijnego ośrodka informacji, który gromadziłby oraz ułatwiał dostęp do uporządkowanej informacji na temat ryzyka dla bezpieczeństwa cybernetycznego i potencjalnych środków zaradczych. Jakkolwiek zacieśnianie współpracy międzynarodowej w obszarze cyberbezpieczeństwa stanowi niezaprzeczalną wartość, warto, aby z uwagi na ostatnie doświadczenia unijnej praktyki legislacyjnej (np. modyfikacje pkt. 10 preambuły Rozporządzenia o Europejskiej Straży Granicznej i Przybrzeżnej) już na wczesnym etapie prac ustawodawczych, zastrzec, iż w związku z art. 4 ust. 2 TUE oraz art. 72 TfUE, propozycje KE nie mogą zobowiązywać państw członkowskich do udostępniania informacji, których ujawnienie jest sprzeczne z podstawowymi interesami ich bezpieczeństwa narodowego. Komunikat wskazuje, że dostarczanie produktów i usług, które zapewniają najwyższy poziom bezpieczeństwa cybernetycznego, jest ważną szansą rozwoju dla branży bezpieczeństwa cybernetycznego w Europie i mogłoby stać się silną przewagą konkurencyjną. Należy podkreślić także, iż obok korzyści ekonomicznych, budowanie zdolności unijnych jest ważne także z punktu widzenia zapewnienia cyberbezpieczeństwa całej UE i każdego kraju członkowskiego.

Komunikat wskazuje, że dążeniu do uczynienia z UE lidera w tej dziedzinie musi towarzyszyć silna kultura bezpieczeństwa danych, w tym danych osobowych i skutecznego reagowania na incydenty. Jednym z kluczowych elementów z punktu widzenia zapewniania UE pozycji lidera jest także

zapewnianie bezpiecznego funkcjonowania systemów sterowania przemysłowego. Jest to istotne zarówno z punktu widzenia bezpieczeństwa jak i rozwoju jednolitego rynku cyfrowego.

Komunikat podkreśla, że przewidziane w treści mechanizmy powinny działać jak jeden spójny system bezpieczeństwa cybernetycznego i zwalczania cyberprzestępczości, pomagający państwom członkowskim lepiej współpracować w walce z terroryzmem, przestępczością zorganizowaną i cyberprzestępczością. Katalog możliwych źródeł zagrożeń jest niepełny i winien zostać uzupełniony, np. o wrogie działania ze strony podmiotów państwowych.

Komunikat zaznacza, że zasadniczym elementem zdolności krajowych wymaganych w dyrektywie w sprawie bezpieczeństwa sieci i informacji są Zespoły Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT), które odpowiadają za szybkie reagowanie na zagrożenia i incydenty cybernetyczne. Z punktu widzenia krajowych systemów cyberbezpieczeństwa, równie istotnymi ogniwami są operatorzy i właściciele infrastrulktury krytycznej, co dostrzega także Dyrektywa NIS.

Komunikat wskazuje, że wiedza ekspercka, na temat bezpieczeństwa cybernetycznego jest obecnie dostępna na poziomie unijnym, ale w sposób rozproszony i niezorganizowany. W celu wspierania mechanizmów współpracy w zakresie bezpieczeństwa sieci i informacji należy gromadzić informacje w ośrodku informacji, aby były łatwo dostępne na życzenie dla wszystkich państw członkowskich. Ten ośrodek stałby się głównym źródłem informacji umożliwiającym instytucjom UE i państwom członkowskim wymianę informacji w stosownych przypadkach. W celu pełnej oceny owego pomysłu potrzebne będzie udostępnienie większej ilości informacji o sposobach jego funkcjonowania.

Z punktu widzenia oceny ENISA, która ma nastąpić do końca 2017 r. i dyskusji na temat ewentualnej potrzeby modyfikacji lub rozszerzenia mandatu ENISA, zwraca się uwagę na kluczową rolę Agencji w zakresie wdrażania Dyrektywy NIS. ENISA winna w tym obszarze pełnić ważną rolę harmonizującą działania prowadzone na poziomie państw członkowskich.

Komunikat wskazuje, że obecnie ENISA, europejska grupa ds. szkolenia i edukacji w zakresie cyberprzestępczości (ECTEG), we współpracy z Europejskim Centrum ds. Cyberprzestępczości przy Europolu, oraz Europejskie Kolegium Policyjne (CEPOL) odgrywają ważną rolę w zapewnianiu wsparcia na potrzeby budowania zdolności – w tym w dziedzinie cybernetycznej kryminalistyki – poprzez opracowywanie podręczników i organizowanie szkoleń oraz ćwiczeń dotyczących bezpieczeństwa cybernetycznego. Ważnym obszarem funkcjonownaia grupy winny być działania nakierowane nie tylko na wzmacnianie umiejętności funkcjonariuszy Policji, ale także działania nakierowane na wzmacnienie wiedzy i umiejętności prokuratorów i sędziów.

Komunikat podkreśla, że cyberprzestrzeń jest jednocześnie szybko rozwijającą się dziedziną, w której zdolności podwójnego zastosowania odgrywają istotną rolę. Dlatego konieczne jest rozwijanie współpracy cywilno-wojskowej i budowanie synergii w obszarze szkoleń i ćwiczeń, aby zwiększyć odporność i zdolności UE w zakresie reagowania na incydenty. Warto w tym kontekście nawiązać do konieczności wzmacniania współpracy z NATO.

Komunikat wskazuje, że pojawiają się krajowe inicjatywy na rzecz ustanowienia wymogów zapewniających wysoki poziom bezpieczeństwa cybernetycznego elementów ICT w infrastrukturze tradycyjnej, w tym wymogów w zakresie certyfikacji. Wyjaśnienia wymaga rozumienie określenia „infrastruktury tradycyjnej".

Z punktu widzenia zapewnienia wysokich standardów transparentności ważne, aby współpraca instytucji UE z różnorodnymi podmiotami wspierającymi realizację działań w ramach budowy jednolitego rynku bezpieczeństwa cybernetycznego Europy (np. PPP) odbywała się na przejrzystych zasadach zapewniających ich równouprawnienie. Partnerem KE w realizacji PPP będzie Europejskie Stowarzyszenie na rzecz Cyberbezpieczeństwa (ECSO, European Cyber Security Organisation). W

założeniu podmiot ten ma reprezentować interesy różnorodnych uczestników rynku wewnętrznego w kontaktach z KE (art. 1 decyzji z 5 lipca 2016 r.), partycypować w kosztach inwestycji oraz przede wszystkim współkształtować priorytety inwestycyjne w obszarze cyberbezpieczeństwa (pkt. 5-6 preambuły decyzji o utworzeniu PPP, np. SRIA – Strategic Research and Innovation Agenda). Udział przedstawicieli sektora prywatnego jest niezbędny dla programowania polityk publicznych w obszarze rynku cyberbezpieczeństwa. W ramach PPP, ECSO będzie odgrywać wiodącą rolę. Biorąc pod uwagę kraje pochodzenia podmiotów wchodzących w jego skład, widoczna jest dominacja zaledwie kilku państw członkowskich (Niemcy, Francja, Hiszpania, Włochy). Polska reprezentowana jest wyłącznie przez 3 podmioty (w tym Ministerstwo Cyfryzacji i NASK) na 134 członków ECSO. Dla porównania - aż 22 podmioty pochodzą z Hiszpanii. Polska nie posiada w ECSO żadnego przedstawiciela z sektora prywatnego (MŚP, duże przedsiębiorstwa, zrzeszenia biznesowe). Dla efektywnego wykorzystania potencjału PPP należy zachęcać do zwiększania obecności polskiego biznesu w ECSO. Instytut Kościuszki planuje włączyć się w działania ECSO a także promować tę inicjatywę w czasie Forum CYBERSEC, w którym udział weźmie Sekretarz Generalny ECSO Luigi Rebuffi.

KE planuje również utworzenie grupy doradczej wysokiego szczebla ds. cyberbezpieczeństwa - gremium eksperckiego umożliwiającego pozyskiwanie zewnętrznej wiedzy specjalistycznej i danych wejściowych dotyczących strategii KE w zakresie cyberbezpieczeństwa oraz ewentualnych środków regulacyjnych i innych dokumentów. W skład grupy doradczej mają wejść przedstawiciele sektora przemysłu, środowiska akademickiego i społeczeństwa obywatelskiego. Oprócz uwag wskazanych w poprzednim akapicie należy zadbać, aby ze względu na materie będące przedmiotem prac grupy doradczej, kompozycja jej składu uwzględniała różnorodność geograficzną i demograficzną państw (w sposób zbliżony do Deklaracji odnoszącej się do art. 15 ust. 5 i 6, art. 17 ust. 6 i 7 oraz art. 18 TUE) w sposób umożliwiający poszanowanie słusznych interesów państw członkowskich w dziedzinach wrażliwych z punktu widzenia wymogów ochrony bezpieczeństwa narodowego. Instytut Kościuszki – organizator CYBERSEC PL, może pomóc w identyfikacji ekspertów i specjalistów zajmujących się różnymi aspektami cyberbezpieczeństwa. Należy też zadbać, aby dobór składu oraz funkcjonowanie grupy doradczej uwzględniały postulaty Europejskiego Rzecznika Praw Obywatelskich, Parlamentu Europejskiego i społeczeństwa obywatelskiego w zakresie jawności, przejrzystości oraz odpowiednich zrównoważonych proporcji w reprezentacji poszczególnych grup interesu. Z uwagi na wrażliwe materie będące przedmiotem obrad grupy doradczej, warto aby zastosować w stosunku do niej podwyższony (względem nowych zasad z 30 maja 2016 r.) standard transparentności biorący pod uwagę rekomendacje Europejskiego Rzecznika Praw Obywatelskich. Dodatkowo, w ramach wspierania realizacji celów stojących przed Grupą doradczą warto wykorzystać już istniejące zasoby pozwalające na budowanie wiedzy eksperckiej, wymianę doświadczeń i budowanie rekomendacji.

W ramach pkt. 3.2 KE zobowiązuje się do rozważenia utworzenia platformy inteligentnej specjalizacji w dziedzinie cyberbezpieczeństwa aby pomóc państwom i regionom zainteresowanym inwestowaniem w sektorze cyberbezpieczeństwa. Celem platformy byłaby koordynacja i planowanie realizacji strategii w zakresie cyberbezpieczeństwa oraz organizację strategicznej współpracy podmiotów w ekosystemach regionalnych. Deklarowane jest również wsparcie dla rozwoju globalnie konkurencyjnych klastrów bezpieczeństwa cybernetycznego i centrów doskonałości w ekosystemach regionalnych sprzyjających wzrostowi cyfrowemu z zastrzeżenie, że wsparcie takie musi być związane z realizacją strategii inteligentnej specjalizacji i innych instrumentów UE, tak aby sektor bezpieczeństwa cybernetycznego w Europie lepiej z nich korzystał.

Plany KE wpisują się w rządową propozycję z zakresu inwestycji w cyberbezpieczeństwo, taka jak np.: Cyberparki Enigma czy działania podejmowane w związku z uznaniem cyberbezpieczeństwa jednym z 10 sektorów strategicznych dla rozwoju polskiej gospodarki (Uchwała nr 14/2016 Rady Ministrów z dnia 16 lutego 2016 r. w sprawie przyjęcia "Planu na rzecz odpowiedzialnego rozwoju"). W kontekście regionalnym warto zwrócić uwagę na inicjatywy podejmowane już przez środowisko

małopolskie. Małopolska jest drugim województwem w Polsce pod względem wskaźnika zatrudnienia w sektorze ICT. Co więcej, plasuje się w ścisłej czołówce w Polsce pod względem liczby absolwentów kierunków związanych z branżą ICT (12%). Kraków to miejsce dynamicznego rozwoju zarówno wielkich krajowych firm (takich jak Comarch), ale i inwestycji bezpośrednich globalnych gigantów branży ICT (IBM, Motorola, Delphi, Cisco) oraz MŚP i start-upów. W stolicy regionu położone są również wiodące ośrodki badawcze – Akademia Górniczo-Hutnicza, Politechnika Krakowska, Uniwersytet Jagielloński, Jagiellońskie Centrum Innowacji czy Krakowski Park Technologiczny. W omawiane plany KE wpisuje się również inicjatywa Instytutu Kościuszki – CYBERSEC HUB, który otrzymując wsparcie polskiego rządu dla swojego rozwoju, w tym w zakresie pozyskania środków unijnych na rozwój, może być zalążkiem pierwszego Cyberparku Enigma. CYBERSEC HUB na tym etapie rozwoju jest programem wsparcia małopolskich przedsiębiorstw z sektora ICT posiadających lub rozwijających produkty i usługi dla cyberbezpieczeństwa. Program ma na celu akceleracją i wzmacnianie ich pozycji konkurencyjnej poprzez promocję innowacyjności i ekspansję międzynarodową, budowanie relacji z inwestorami i klientami. Instytut Kościuszki animuje budowanie relacji i współpracy kluczowych interesariuszy sektora cyberbezpieczeństwa w Małopolsce oraz kumulację kapitału wiedzy i dobrych praktyk dzięki organizowanemu w Krakowie Europejskiemu Forum Cyberbezpieczeństwa - CYBERSEC.

Polska Izba Informatyki i Telekomunikacji [PIIT]

W komunikacie występuje odwołanie do raportu „Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II". Autorem tego raportu jest firma McAfee, a sam raport pochodzi z 2014r. Uważamy, że w komunikacie datowanym na lipiec 2016 korzystniejsze byłoby powołanie się na bardziej aktualne raporty (np. przekazany już wcześniej do Ministerstwa publicznie dostępny raport HPE z roku 2016) oraz przedstawienie trendów obrazujących zwiększające się corocznie straty ekonomiczne z tytułu naruszeń cyberbezpieczeństwa. Korzystne byłoby przedstawienie również pozycji Europy, jak i krajów UE, na tle pozostałych regionów świata.

Należy się zastanowić nad rewizją strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego z 2013 r. W czasie ostatnich trzech lat, które upłynęły od przyjęcia strategii, zaistniało szereg zdarzeń, które w istotny sposób wpłynęły na postrzeganie roli bezpieczeństwa cyberprzestrzeni w współczesnym świecie. Wśród tych zdarzeń można wymienić: ataki terrorystyczne, wojna hybrydowa, ataki lub próby ataków na systemy infrastruktury krytycznej w Europie.

W treści komunikatu wielokrotnie występuje odwołanie do znaczenia skutecznego reagowania na incydenty w sferze bezpieczeństwa cybernetycznego. Niestety dokument nie precyzuje zakresu tego procesu. Naszym zdaniem należałoby wprost i jednoznacznie określić, że chodzi tu o całościowy proces zarządzania incydentami. A samo reagowanie na incydent jest tylko jednym szeregu zadań występujących w tym procesie. Warto tu zaproponować wykorzystanie zapisów normy SO/IEC 27035: 2011 Information technology -- Security techniques -- Information security incident management.

W podejściu zaproponowanym w komunikacie brak jest odwołania do roli i miejsca szeroko rozumianej architektury bezpieczeństwa, która będzie stanowiła podstawę do budowy europejskiego systemu odporności cybernetycznej. Takie podejście, czyli brak architektury bezpieczeństwa, może w przyszłości skutkować, częstszym występowaniem zagrożeń i incydentów bezpieczeństwa oraz zwiększeniem nakładów finansowych na wyeliminowanie luk i podatności oraz zapewnienia wymaganego poziomu bezpieczeństwa cyberprzestrzeni UE.

Uważamy, że powinno się także określić zasady certyfikacji software/hardware pochodzącego spoza UE w zakresie spełnienia wymagań cyberbezpieczeństwa. Umożliwi to zapewnienie konkurencyjności europejskich (a więc również i polskich) w stosunku do podmiotów działających poza UE.

W proponowanym systemie ochrony cyberprzestrzeni nie przewidziano jakiejkolwiek roli zwykłych obywateli. A to oni właśnie często znacznie szybciej doświadczają lub wykrywają nieprawidłowości związane z atakiem na instytucje publiczne.

IBM Polska Sp. z o.o.

Zdajemy sobie sprawę z konieczność podjęcia nowych, dodatkowych środków w celu wzmocnienia odporności cybersecurity, uważamy, że dyrektywa NIS zapewnia do tego dobre ramy. Środki zaproponowane w Dyrektywie dla operatorów krytycznych usług, przy ich transpozycji do prawa krajowego, podwyższy gotowość operatorów. IBM pomaga klientom w dostosowaniu się do nowych wymagań, poprzez na przykład security operations centers, zapewniając scentralizowane monitorowanie zagrożeń i reagowanie na nie.

Wierzymy, że dyrektywa NIS jest ważnym pierwszym krokiem w poprawie bezpieczeństwa przed cyber atakami. Jest więcej do zrobienia w obszarach, do których dyrektywa NIS się nie odniosła - na przykład umożliwienie lepszych warunków dla przemysłu dzielenia się informacjami o zagrożeniach między sobą. IBM może stanowić doskonały przykład otwartej platformy, która umożliwia wymianę takich informacji, to jest globalna XForce platforma do dzielenia się informacjami dotyczącymi zagrożeń, platforma umożliwiająca użytkownikom szybko zbadać najnowsze zagrożenia bezpieczeństwa, dotrzeć do zagregowanych informacji, współpracować z innymi http://www-03.ibm.com/security/uk/en/xforce/.

W pełni popieramy wspieranie współpracy europejskiej i globalnej na temat zagrożeń cybernetycznych poprzez krajowe CERTy / CSIRTy określonymi w dyrektywie NIS - organizacje te mają już zazwyczaj do czynienia z zagadnieniami cyber na szczeblu krajowym, i często są rozpoznawane jako krajowe wiodące organizacje zaufania w zakresie bezpieczeństwa cybernetycznego.

Naszym zdaniem wprowadzenie szczególnych ram europejskiego systemu certyfikacji cyberbezpieczeństwa byłbym niekorzystny rozwojem sytuacji - to dlatego, że istnieją już uznane międzynarodowe systemy certyfikacji i norm, w których Europa uczestniczy i jakiekolwiek europejskie podejście do certyfikacji powinno obejmować międzynarodowe standardy. Wyłącznie europejskie podejście mogłoby wykluczyć do 80% międzynarodowych dostawców ICT , co miałoby odwrotny do zamierzonego efekt, zarówno z punktu widzenia ekonomicznego jak i bezpieczeństwa oraz w istotny sposób zaszkodzić europejskiej społeczności start-upów szukajacych globalnych partnerów do dalszego rozwoju.

W odniesieniu do promowania bardziej konkurencyjnego europejskiego sektora bezpieczeństwa cybernetycznego, uważamy, że otwarte konkurencyjne podejście jest bardzo ważne. Zamknięcie rynku UE przed międzynarodowymi graczami, czy to poprzez wprowadzenie specjalnych warunków finansowania badań lub preferencji zamówień wyłącznie dla rozwiązań UE może być odwrotny do zamierzonego - stworzenie wyłącznie silosowego europejskiego przemysłu wraz z rozwojem wyłącznie europejskiego podejścia do bezpieczeństwa cybernetycznego, stoi w sprzeczności z faktem, że bezpieczeństwo cybernetyczne jest problemem globalnym i można mu przeciwdziałać tylko poprzez szereg działań na szczeblu międzynarodowym, czy to poprzez międzynarodowe standardy dla operatorów czy współpracę i wymianę informacji o otoczeniu zagrożeń i specyficznych ataków. Najlepszym przykładem globalnej współpracy cyberbezpieczeństwa jest siatka IBM centrów operacyjnych bezpieczeństwa z jednym z 10 we Wrocławiu http://www.zdnet.com/article/ibm-opens-polish-sec-shop/.

Wspieramy także wzmocnienie w Europie wiedzy oraz prac badawczo-rozwojowych w obszarze cyber security poprzez programy H2020 dla projektów bezpieczeństwa, otwartych dla wszystkich kwalifikujących się konsorcjów również z międzynarodowymi partnerami, ale także mocno wierzymy

w potrzebę wzmocnienia edukacji na temat bezpieczeństwa na średnim i wyższym poziomie wykształcenia we wszystkich państwach członkowskich.

VII. WNIOSKI

Przestawione w Komunikacie inicjatywy zasługują na poparcie, chociaż w wielu przypadkach konieczne jest ich doprecyzowanie przez Komisję Europejską. Wskazujemy jednocześnie na konieczność przeprowadzenia pogłębionej analizy, czy powoływanie nowych struktur jest rzeczywiście konieczne i czy przewidziane Komunikatem zadania nie mogą być realizowane przez już istniejące struktury/ ciała. Jednocześnie deklarujemy aktywny udział w podejmowanych na szczeblu unijnym działaniach.

VIII. PRZEDSTAWICIEL KIEROWNICTWA RESORTU WIODĄCEGO UPOWAŻNIONY DO PREZENTOWANIA STANOWISKA

Pani Anna Streżyńska, Minister Cyfryzacji RP