Piotr Marek Balcerzak
Piotr Durbajło

Organizacyjno-prawne aspekty implementacji dyrektywy Parlamentu Europejskiego i Rady z 6.7.2016 r.

1. Podział kompetencji i zadań w krajowym systemie cyberbezpieczeństwa

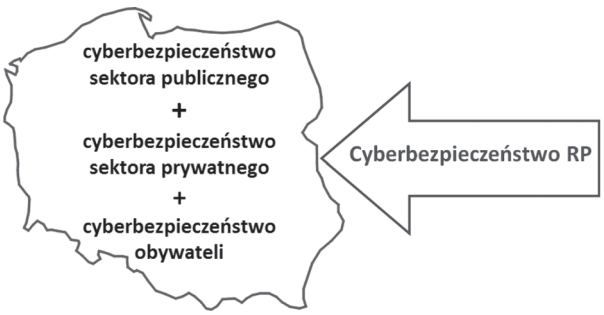
Przewrotnie ktoś może zadać pytanie czy potrzebujemy krajowego systemu cyberbezpieczeństwa. Ten sam obywatel bardzo często jest klientem banku, korzystając ze zdalnego dostępu do produktów i usług bankowych. Korzysta również z usług telekomunikacyjnych i dostawców usług internetowych. Czasami również dokonuje zakupów w sieci i coraz częściej także korzysta z usług e-państwa.

Wszyscy wyżej wymienieni przedsiębiorcy i instytucje oferując usługi, dbają przecież również o ich bezpieczeństwo. Jednak bezpieczeństwo to ma charakter „wyspowy" to znaczy, że każda z tych z tych usługodawców dba o bezpieczeństwo we własnym zakresie. Co prawda sektor bankowy w obszarze bezpieczeństwa, a w szczególności cyberbezpieczeństwa dokonał dużej konsolidacji i współpracuje ze sobą od wielu lat jednak, to przykład ten stanowi tylko wyjątek potwierdzający wyżej zacytowaną regułę. Było to możliwe gdyż sektor bankowy wypracował zasadę, że w obszarze bezpieczeństwa banki ze sobą nie konkurują tylko współpracują. Reguła to byłaby tylko pustym frazesem gdyby nie to, że banki obdarzyły się nawzajem zaufanie. Zaufanie to wynikało ze świadomości, że rozwój bankowego biznesu jest uzależniony od współpracy w obszarze bezpieczeństwa.

Ten sam obywatel korzystając z usług bankowych, zakupów z Internetu czy usług e-państwa oczekuję od tych usługodawców, że usługi te będą świadczone na najwyższym poziomie, a to oznacza również że będą bezpieczne. Wymogiem naszych czasów jest więc współpraca pomiędzy poszczególnymi instytucjami z sektora publicznego oraz przedsiębiorcami z sektora prywatne-

go na rzecz cyberbezpieczeństwa. Oznacza to że musi powstać system cyberbezpieczeństwa państwa, który będzie się składał z 3 równorzędnych elementów (rys.1): cyberbezpieczeństwa sektora publicznego, cyberbezpieczeństwa sektora prywatnego oraz cyberbezpieczeństwa obywateli[1]. Tylko takie działania komplementarne pozwolą na osiągnięcie akceptowanego z punktu widzenia państwa poziomu bezpieczeństwa.

Rys. 1 Cyberbezpieczeństwo RP – elementy składowe



Źródło: Opracowanie własne.

Można byłoby postawić kolejne pytanie, czy posiadamy krajowy system cyberbezpieczeństwa. Na tak postawione pytanie odpowiedź niestety brzmi NIE, nie posiadamy jednolitego rozwiązania systemowego. Jednak nie oznacza to że jako państwo nie zaimplementowaliśmy wielorakich mechanizmów zwiększających cyberbezpieczesństwo[2]. Jednakże właśnie brak podejścia systemowego powoduje, iż z jednej strony posiadając przepisy prawa, instytucje i podmioty, które umożliwiają zwalczanie cyberprzestępczości, to z drugiej strony podejmowane działania w tym zakresie są dalekie pod względem efektywności od oczekiwań i potrzeb. Analogiczny problem zidentyfikowano zresztą nie tylko w Polsce i poszczególnych państwach ale także całościowo w Unii Europejskiej gdzie, rozumiejąc anachronizm funkcjonowania jedynie ENISA (Europejskiej Agencji Bezpieczeństwa Sieci i Informacji) podjęto próbę określenia wzorca idealnego w zakresie współpracy w obszarze cyberbezpieczeństwa i zwalczania cyberprzestępczości. Efektem jest dyrektywa Parlamentu Europejskiego i Rady z 6.7.2016 r. sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i syste-

[1] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020, Minister Cyfryzacji, https://mc.gov.pl/files/strategia_v_29_09_2016.odt.

[2] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 – Tworzenie warunków do rozwoju zintegrowanego systemu bezpieczeństwa narodowego, priorytet 5.3 Zapewnienie bezpieczeństwa informacyjnego i telekomunikacyjnego, kierunek interwencji 5.3.2 – Rozwijanie Systemu Reagowania na Incydenty Komputerowe w kontekście zintegrowanego systemu bezpieczeństwa narodowego.

mów informatycznych[3] (dyrektywa NIS). Niestety dyrektywa ta nie stanowi do końca idealnego rozwiązania, gdyż np. w wyniku niezdrowego kompromisu nie obejmuje przedsiębiorców telekomunikacyjnych lub niektóre jej przepisy budzą duże wątpliwości interpretacyjne – wyznaczania operatorów usług kluczowych i spójnego podejścia do tej kwestii na poziomie europejskim. Z uwagi na rozwój e-społeczeństwa, a w szczególności zaawansowanych usług elektronicznych, w tym świadczonych w relacji państwo – obywatel, państwo – przedsiębiorca, dyrektywa ta musi być niezwłocznie implementowana w Polsce i według obecnych planów prac rządu stanie się tak poprzez dedykowaną ustawę o krajowym systemie cyberbezpieczeństwa. Przy czym państwa członkowskie Unii Europejskiej mają nieprzekraczalny termin wdrożenia rozwiązań prawnych zawartych w dyrektywie NIS do krajowego porządku prawnego do dnia 9 maja 2018 r.

2. Implementacja Dyrektywy NIS w Polsce[4]

2.1. Obowiązki i zadania wynikające z Dyrektywy NIS

Dyrektywa NIS nakłada na państwa członkowskie konkretne wymagania, które poprzez implementację do krajowego porządku prawnego, stworzą ramy prawne dla funkcjonowania spójnego systemu cyberbezpieczeństwa. Obowiązki te są związane z:

- przyjęciem krajowej strategii bezpieczeństwa sieci i informacji;
- identyfikacją usług kluczowych oraz operatorów usług kluczowych (tab. 1);
- wyznaczeniem pojedynczego punktu kontaktowego;
- wyznaczeniem organów właściwych dla operatorów usług kluczowych i dostawców usług cyfrowych;
- wyznaczeniem CSIRT'ów dla operatorów usług kluczowych oraz dostawców usług kluczowych;
- udziałem w pracach Grupy Współpracy – relacje międzynarodowe – poziom strategiczny;
- udziałem w tworzeniu sieci CSIRT – relacja międzynarodowa – poziom operacyjny;
- utworzeniem rejestru incydentów dla operatorów usług kluczowych oraz dostawców usług cyfrowych.

[3] Dz.Urz. L 194 z 19.7.2016 r., s. 1–30.

[4] Dyrektywa Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, http://data.consilium.europa.eu/doc/document/ST-5581-2016-INIT/pl/pdf.

Tab. 1. Systematyka podziału na operatorów i dostawców usług w ramach dyrektywy NIS

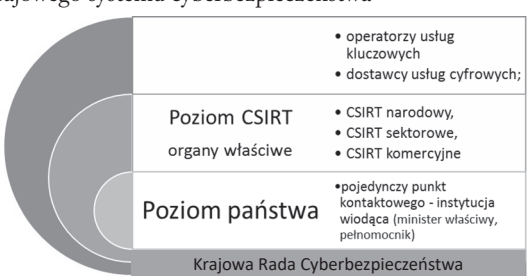
ZAKRES PODMIOTOWY DYREKTYWY NIS	
OPERATORZY USŁUG KLUCZOWYCH, ŚWIADCZĄCY USŁUGI W SEKTORACH: •energetycznym; •transportu; •bankowym; •infrastruktury rynków finansowych – giełd; •służby zdrowia; •zaopatrzenia w wodę pitną i jej dystrybucji; •infrastruktury cyfrowej.	**DOSTAWCY USŁUG CYFROWYCH, ŚWIADCZĄCY USŁUGI:** •przetwarzania danych w chmurze obliczeniowej; •wyszukiwarek internetowych; •e-commerce

Źródło: Opracowanie własne na podstawie NIS.

Wiąże się to ściśle z określeniem konkretnych kompetencji oraz podmiotów, którym te kompetencje zostaną przyznane (tab. 2). W związku z tym krajowy system cyberbezpieczeństwa winien składać się w szczególności z:

1) operatorów usług kluczowych;
2) dostawców usług cyfrowych;
3) Krajowej Rady Cyberbezpieczeństwa.
4) pojedynczego punktu kontaktowego;
5) organów właściwych;
6) CSIRT narodowego, w tym przedstawicieli CSIRT sektorowych (np. CERT.GOV.PL, MIL-CERT, SCIRT bankowego, telekomunikacyjnego, energetycznego) CSIRT międzysektorowego – CERT Polska oraz Policji;
7) CSIRT operatorów usług kluczowych oraz dostawców usług cyfrowych.

Tab. 2. Struktura krajowego systemu cyberbezpieczeństwa



Źródło: Opracowanie własne.

2.2. Usługi kluczowe i operatorzy usług kluczowych oraz usługi cyfrowe i dostawcy usług cyfrowych

Dyrektywa NIS definiuje dwie grupy podmiotów, które oferują usługi: operatorów usług kluczowych oraz dostawców usług cyfrowych. Operatorzy usług kluczowych zostali wskazani w załączniku Nr 2 do dyrektywy NIS i są to podmioty, które oferują swoje usługi w ramach 7 sektorów (energetycznego, transportu, bankowości, infrastruktury rynków finansowych – giełd, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji, oraz infrastruktury cyfrowej.

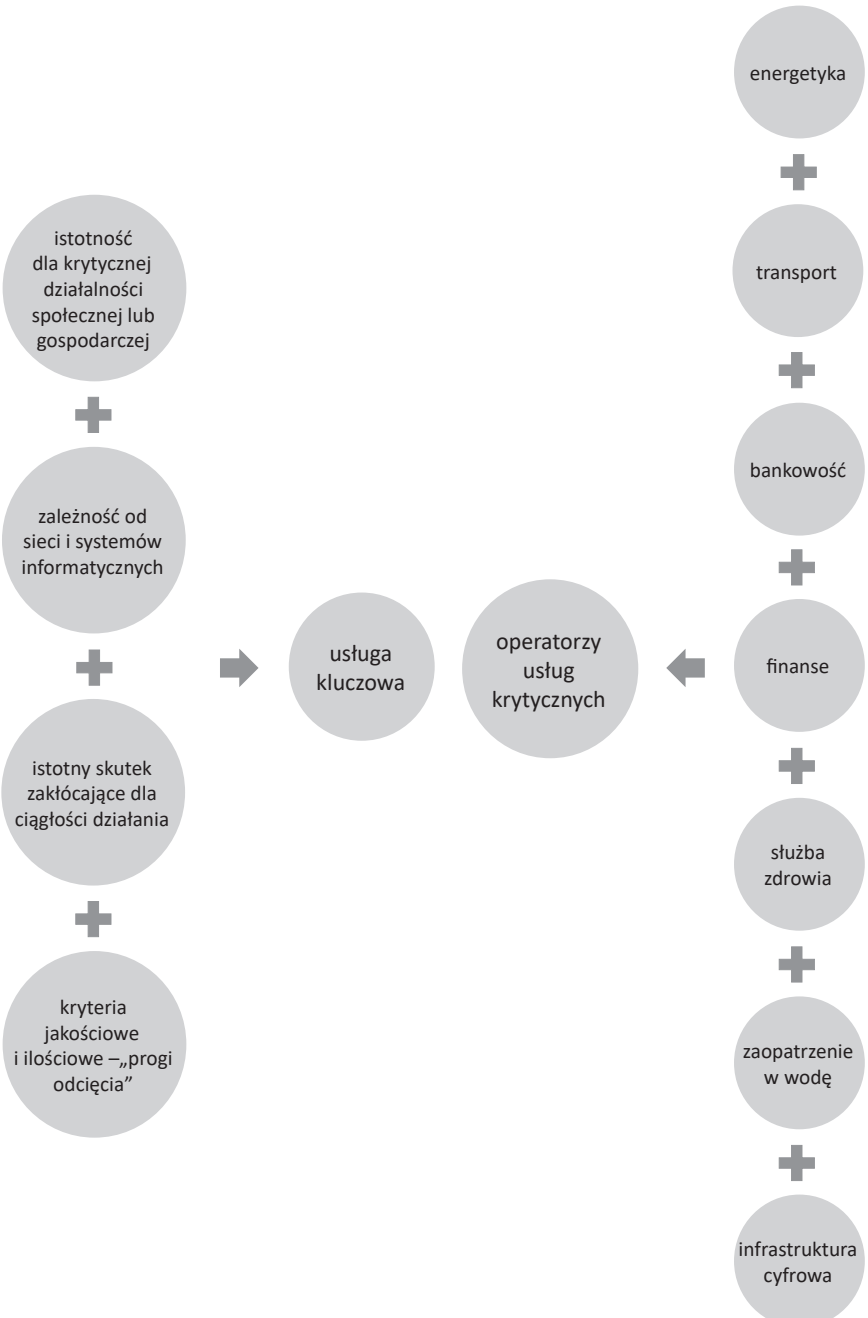
Motyw 25 dyrektywy NIS określa metodę identyfikacji podmiotów, które powinny podlegać obowiązkom dotyczącym bezpieczeństwa sieci i systemów informatycznych. Identyfikacja ta może być przeprowadzona w na dwa sposoby: poprzez przyjęcie wykazu zawierającego wszystkich operatorów usług kluczowych lub przez określenie obiektywnych kryteriów ilościowych np. liczba użytkowników, dzięki którym zostaną wskazane podmioty podlegające przepisom dotyczącym bezpieczeństwa sieci i systemów informatycznych.

W celu zapewnienia szczelności krajowego systemu cyberbezpieczeństwa należy dokonać przeglądu wszystkich podmiotów, które świadczą tzw. usługi kluczowe (rys. 2). Aby daną usługę można było uznać za usługę kluczową musi ona spełnić 4 następujące warunki łącznie:

- usługa musi mieć istotne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;
- świadczenie tej usługi zależna jest od sieci i systemów informatycznych;
- incydent związany z daną usługą miałby istotny skutek zakłócające dla świadczenia tej usługi;
- kryteria jakościowe i ilościowe – tzw. progi odcięcia.

Warunek ten wprowadza zasadę proporcjonalności, której celem jest, poprzez wprowadzenie limitów jakościowych i ilościowych, nienakładanie nadmiernych obowiązków, wynikających z projektowanej ustawy, wobec tych podmiotów, które świadczą usługi w cyberprzestrzeni gdyż ich zakres świadczenia i ich istotność nie mają kluczowego znaczenia dla cyberbezpieczeństwa RP. Wprowadzenie progów spowoduję, że bussines prowadzony przez te podmioty będzie opłacalny i wciąż konkurencyjny.

Rys. 2. Klasyfikacja i kryteria wyboru usług i operatorów



Źródło: Opracowanie własne.

2.3. Klasyfikowanie podmiotów

Uznając powyższe do krajowego systemu cyberbezpieczeństwa należy włączyć podmioty z sektora publicznego, telekomunikacyjnego, dostawców usług płatniczych innych niż banki, podmioty np. odpowiedzialne za odprowadzanie i oczyszczanie ścieków, a także uwzględnić ocenę zasadności włączenia podmiotów związanych z usługami zaufania i usługami publicznymi świadczonymi przez sektor prywatny. Może pojawić się wątpliwość, czy np. zakłady produkujące chemię przemysłową lub zakłady zbrojeniowe, czy przemysł ciężki należy zaliczyć do operatorów usług kluczowych i objąć ich przepisami ustawy o krajowym systemie cyberbezpieczeństwa. Analizując przytoczone powyżej kryteria za włączeniem przemawiają następujące przesłanki:

- wytwarzane przez ww. zakłady produkty mają istotne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej Polski;
- jeśli wystąpiłby incydent w tych zakładach związany z wytwarzaniem produktu to bez wątpienia mógłby mieć istotny skutek na ciągłość produkcji własnej i powiązanej;
- produkcja dóbr jest także uzależniona od systemów informatycznych, i bez ich prawidłowego działania przy dzisiejszym zaawansowaniu procesów technologicznych jest niemożliwa
- zapewne w części przypadków byłyby również spełnione kryteria jakościowe i ilościowe.

Jednak podmioty te nie mogą być uznane za operatorów usług kluczowych gdyż nie świadczą usługi tylko wytwarzają produkty oraz nawet jeśli pominęlibyśmy to pierwsze i fundamentalne kryterium, to jednak produkcja co prawda opiera się o systemy informatyczne SCADA, ale zgodnie z zasadami są on odseparowane od sieci zewnętrznych, tak więc atak na nie musiałby wiązać z przełamaniem zabezpieczeń fizycznych i ingerencją od środka. Wobec powyższego nasuwa się pytanie, czym te zakłady są i jak je można umiejscowić w krajowym systemie cyberbezpieczeństwa? Podmioty te są niczym innym jak tzw. użytkownikiem końcowym, który korzysta z usług operatorów usług kluczowych takich jak: zakładów energetycznych, dostawców gazu, czy firm telekomunikacyjnych. Bez wątpienia są oni istotnymi podmiotami, które mogą mieć wpływ na utrzymanie krytycznej działalności społecznej i gospodarczej Polski i dlatego podmioty te są elementami infrastruktury krytycznej, co zresztą potwierdza podstawowe kryterium IK, czyli incydent z udziałem tych podmiotów miałby skutek kinetyczny. Z tego względu nie można stawiać znaku równości pomiędzy operatorami usług kluczowych a podmiotami będącymi elementami infrastruktury krytycznej. Dobrym przykładem może być cyberincydent w sektorze bankowym. Jeśli wystąpiłby atak na klientów banków np. phishing, to incydent ten nie wywoływałby żadnych skutków kinetycznych.

Natomiast za operatora usługi kluczowej należy uznać organ administracji publicznej bądź przedsiębiorcę, który świadczy lub który zamierza świadczyć usługi kluczowe. Co to w praktyce oznacza? Za operatora usługi kluczowej należy również uznać przedsiębiorcę, który np. nie jest bankiem ale który faktycznie świadczy usługę bankowe np. tzw. parabanki. Takie podejście ma zabezpieczyć użytkowników końcowych – obywateli – przed nadmiernym apetytem na ryzyko takich przedsiębiorców, którzy nie mając statusu banku ale którzy faktycznie oferują czynności bankowe i którzy nie dbają w należyty sposób o cyberbezpieczeństwa świadczonych przez nich usług.

Zgodnie z wymogami dyrektywy NIS, w przypadku gdy operator usługi kluczowej świadczy lub będzie ją świadczył w dwóch lub większej liczbie państw członkowskich Unii Europejskiej, decyzja o uznaniu za operatora usług kluczowych jest poprzedzona konsultacją z tymi państwami członkowskimi. Jest to kolejny problem na drodze do ujednolicenia podejścia do usług kluczowych i operatorów je świadczących. W praktyce może się tak zdarzyć, że przedsiębiorca świadczący usługi kluczowe transgranicznie może być różnie postrzegany w poszczególnych państwach w kontekście uznania go za operatora usługi kluczowej. Może to wynikać np. z różnych kryteriów w tych państwach, gdzie świadczy usługi, związanych z uznaniem ich za usługi kluczowe. Może mieć to negatywne skutki w kontekście obsługi cyberincydentów o charakterze transgranicznym z udziałem takiego przedsiębiorcy, do czego dyrektywa NIS przykłada wielką wagę. Oczywiście z czasem państwa członkowskie UE ujednolicą podejście w tej kwestii ale zanim to się stanie będziemy mieli do czynienia z tzw. chorobą wieku dziecięcego.

Natomiast dostawcami usług cyfrowych są podmioty wymienione enumeratywnie w załączniku Nr 3 do dyrektywy NIS i stanowią grupę dostawców świadczących usługi cyfrowe: przetwarzanie danych w chmurze obliczeniowej, dostawców wyszukiwarek internetowych oraz e-commerce.

3. Propozycja struktur krajowych zarządzania cyberbezpieczeństwem

3.1. Krajowa Rada Cyberbezpieczeństwa

W cyberbezpieczeństwie jest wiele czynników, które wpływają na skuteczność działania podejmowanych w tym obszarze. Jednak, chyba najważniejszym czynnikiem jest czas, który wpływa na to, czy cyberincydent zostanie skutecznie obsłużony, a jego negatywne skutki zarówno dla podmiotu świadczącego usługi jak i użytkownika końcowego (obywateli-klientów, przedsiębiorców, instytucji itd.) zostaną zneutralizowane. Działania w obszarze cyberbezpieczeństwa są tym bardziej istotne, w kontekście czasu reakcji za incydent, że jego skutki mogą mieć również wpływ nie tylko na kwestie materialne, utratę reputacji, ale również i życie obywateli.

Tab. 3. Podmioty instytucjonalne związane obecnie z ochroną cyberprzestrzeni.

Ilość podmiotów instytucjonalnych po stronie administracji państwowej mających znaczący związek z ochroną cyberprzestrzeni (techniczny, organizacyjny, budżetowo-finansowy, innowacyjno-rozwojowy) o działaniu często równoległym	
Minister Cyfryzacji	Rządowe Centrum Bezpieczeństwa
Minister Spraw Wewnętrznych i Administracji	Biuro Bezpieczeństwa Narodowego
Minister Obrony Narodowej (MIL-CERT oraz Narodowe Centrum Kryptologii)	Naukowa i Akademicka Sieć Komputerowa (CERT.PL)
Prezes Urzędu Komunikacji Elektronicznej	Narodowe Centrum Badań i Rozwoju
Szef Agencji Bezpieczeństwa Wewnętrznego (w tym CERT.GOV.PL	
Komendant Główny Policji	
Szef Służby Kontrwywiadu Wojskowego	

Innym istotnym czynnikiem, o czym wspomniano już na początku, wpływającym na skuteczność działań w obszarze cyberbezpieczeństwa jest właściwa koordynacja działań. W chwili obecnej w Polsce jest kilka instytucji odpowiedzialnych za cyberbezpieczeństwo (tab. 3), jednak ich działania mają charakter „wyspowy" i są związane z konkretnymi uprawnieniami wynikającymi z przepisów ustaw i aktów wykonawczych określających ich kompetencje[5]. Są to w zakresie działu obrony narodowej resort obrony narodowej[6], w ramach którego funkcjonuje Służba Kontrwywiadu Wojskowego[7], w zakresie działań antyterrorystycznych, w szczególności cyberterroryzmu i cyberbezpieczeństwa sektora publicznego Agencja Bezpieczeństwa Wewnętrznego[8] z wyspecjalizowaną komórką CERT.GOV.PL oraz Policja[9], która jest uprawniona do ścigania przestępstw popełnianych z wykorzystaniem cyberprzestrzeni na szkodę sektora prywatnego oraz obywateli. Efektem tego jest obecny stan, w którym współdziałanie w sytuacjach incydentów czy zagrożeń jest raczej oparte o wypracowane nieformalnie zasady współdziałania. Brak dziś zaimplementowanego mechanizmu koordynacji czy hierarchiczności procesów i działań powoduje, że w przypadku incydentów wykraczających poza sektor, czy nawet kompetencję pojedynczej instytucji może dojść do dublowania działań, ich

[5] Ustawa z 4.9.1997 r. o działach administracji rządowej (t.j. Dz.U. z 2016 r. poz. 543).
[6] Ustawa z 14.12.1995 r. o urzędzie Ministra Obrony Narodowej (t.j. Dz.U.z 2013 r. poz. 189).
[7] Ustawa z 9.6.2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz.U.z 2016 r. poz. 1318).
[8] Ustawa z 24.5.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2016 r. poz. 1897).
[9] Ustawa z 6.4.1990 r. o Policji (t.j. Dz.U.2016 r. poz. 1782).

Ustawa niespójności czy niepełnego i niewłaściwego obiegu informacji, co może skutkować niewłaściwymi reakcjami na zdarzenia.

Działania tych wszystkich podmiotów mogłyby być bardziej efektywne gdyby były skoordynowane zarówno na poziomie strategiczno-polityczno-decyzyjnym, jak również na poziomie współpracy operacyjnej. Pamiętając, że cyberbezpieczeństwo RP składa się z trzech, uzupełniających się komponentów, czyli cyberbezpieczeństwa sektora publicznego, cyberbezpieczeństwa sektora prywatnego oraz cyberbezpieczeństwo obywateli, należy włączyć do działania w wyżej wymienionych obszarach przedstawicieli nie tylko sektora publicznego, ale również sektora prywatnego oraz reprezentanta obywateli. Rolą autorów ustawy o krajowym systemie cyberbezpieczeństwa jest przygotowanie takich rozwiązań prawnych, które z jednej strony umożliwią sprawną realizację kompetencji w obszarze strategiczno-polityczno-decyzyjnym oraz operacyjnym, a z drugiej wzmocnią wszystkich interesariuszy w zakresie realizacji powierzonych zadań.

Dotychczasowe spojrzenie na kwestie cyberbezpieczeństwa – cyberbezpieczeństwo sektora publicznego ma najwyższy priorytet nie ma już racji bytu. Wynika to z faktu, że jeżeli mówimy o systemie to musimy dostrzegać wszystkie podmioty, które biorą aktywny udział w tworzeniu i wykorzystywaniu cyberprzestrzeni. Dodatkowo, należy również wskazać na fakt, że coraz częściej podmioty sektora prywatnego oferują usługi dotychczas zarezerwowane tylko i wyłącznie dla sektora publicznego na przykład: składanie wniosków w ramach „Programu 500+", dostęp do zasobów Zakładu Ubezpieczeń Społecznych, czy możliwość oferowania profilu zaufanego. Co należy podkreślić właśnie na potrzebę budowania silnego partnerstwa publiczno-prywatnego w obszarze cyberbezpieczeństwa wskazuje dyrektywa NIS.

Na poziomie strategiczną-polityczna-decyzyjnym powinno być utworzona kolegialne ciało – Krajowa Rada Cyberbezpieczeństwa, które powinno podlegać bezpośrednio i być nadzorowane przez Prezesa Rady Ministrów lub jego pełnomocnika. Udział w pracach Rady wszystkich interesariuszy zwiększa pewność określenia i podziały ról w krajowym systemie cyberbezpieczeństwa, eliminując możliwość nachodzenia na siebie kompetencji lub pozostawienia tzw. „pól niczyich", a co najważniejsze transparentność w działaniu oraz osiągnięcie efektu synergii.

Skład Krajowej Rady Cyberbezpieczeństwa powinien być uzależniony od zadań przez nią realizowanych. Rada w składzie – przedstawiciele: Prezydenta RP, Minister Koordynator do spraw Służb Specjalnych, ministrowie odpowiedzialni za działy: obrony narodowej, sprawiedliwości, spraw wewnętrznych i administracji publicznej, finansów publicznych, informatyzacji, nauki, usług społecznych, rolnictwa, przedstawiciele Narodowego Banku Polskiego, CSIRT sektorowych, a także przedstawiciel obywateli powinna realizować w szczególności następujące zadania:

1) podejmowanie działań mających na celu rozwój rynku usług kluczowych i cyfrowych oraz ich konkurencyjności;
2) aktualizowanie listy usług kluczowych oraz wykazu operatorów usług kluczowych;
3) udział w przygotowaniu aktów prawnych;
4) przyjmowanie Strategii Cyberbezpieczeństwa oraz monitorowanie jej realizacji;
5) makro analizy trendów w obszarze cyberbezpieczeństwa;
6) formułowanie rekomendacji;
7) wymiana informacji;
8) przedstawianie propozycji działań w obszarach współpracy sektora publicznego z prywatnym;
9) podejmowanie działań edukacyjnych i informacyjnych;
10) tworzenie możliwości pojednawczego i polubownego rozstrzygania sporów pomiędzy operatorami usług kluczowych lub dostawcami usług cyfrowych;
11) wnioskowanie do organów właściwych o nałożenie sankcji lub kar na operatorów usług klucz;
12) nakładanie kar na operatorów usług kluczowych w przypadku rażącego naruszenia przepisów.

Nadzór nad krajowym systemem cyberbezpieczeństwa winien być sprawowany w składzie jak wyżej z wyłączeniem przedstawicieli CSIRT sektorowych oraz obywateli. Natomiast ze względu na bardzo sensytywne kwestie związane z koordynacją i działaniami w obszarze cyberbezpieczeństwa dotyczącego obronności narodowej oraz bezpieczeństwa wewnętrznego i porządku publicznego, zadania z tego obszaru winny być realizowane w składzie – przedstawicieli: Ministra Koordynatora do spraw Służb Specjalnych, Ministra Obrony Narodowej oraz Ministra Spraw Wewnętrznych i Administracji, oraz Przedstawiciela Prezydenta RP oraz Ministra Cyfryzacji.

Przez przedstawiciela obywateli należy rozumień konstytucyjną instytucję uprawnioną do występowania w interesie obywateli, która może być wspierana przez organizacje pozarządowe.

Ze względu na brak możliwości wydawania aktów delegowanych przez Radę należałoby rozważyć możliwość wydawania ich przez ministra, który zgodnie z ustawą o działach administracji rządowej odpowiedzialny jest za realizację zadań z obszaru cyberbezpieczeństwa, w chwili obecnej jest to minister właściwy do spraw informatyzacji. Wówczas każdorazowe wydanie aktu wykonawczego przez tego ministra wiązałoby się z uzyskaniem pozytywnej opinii Rady.

Innym wariantem umożliwiającym tworzenie aktów wykonawczych byłoby wydawanie ich przez ministrów właściwych zgodnie z kompetencjami określonymi dla poszczególnych działów ww. ustawie działowej w po-

rozumieniu z ministrem odpowiedzialnym za cyberbezpieczeństwo. Jednak rozwiązanie to może być obarczone pewnymi wadami wynikającymi z braku kompetencji w zakresie cyberbezpieczeństwa po stronie właściwych ministerstw (z wyłączeniem Ministra Obrony Narodowej, Ministra Koordynatora ds. Służb Specjalnych oraz Ministra Spraw Wewnętrznych i Administracji). Dodatkowo zaletą pierwszego wariantu jest gwarancja jaką daje minister właściwy ds. cyberbezpieczeństwa dotycząca dbałości o spójność regulacji prawnych w ramach krajowego systemu cyberbezpieczeństwa.

3.2. Pojedynczy punkt kontaktowy

Dyrektywa NIS wskazuje na potrzebę powołania tak zwanego pojedynczego punktu kontaktowego do spraw bezpieczeństwa sieci i systemów informatycznych zwanych dalej „pojedynczym punktem kontaktowym". Rola i znaczenie pojedynczego punktu kontaktowego zostały określone artykule 8 i 9 dyrektywy NIS. Dodatkowo motyw 31 dyrektywy NIS wskazuje m. in., że pojedynczy punkt kontaktowy jest odpowiedzialny za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracą transgraniczną na poziomie Unii Europejskiej. Dyrektywa zobowiązuje państwa członkowskie do zapewnienia wystarczających zasobów finansowych, technicznych i ludzkich, tak aby pojedyncze punkty kontaktowe mógł skutecznie i efektywnie wykonywać powierzone im zadania i osiągać cel dyrektywy, jakim jest poprawa funkcjonowania rynku wewnętrznego poprzez budowanie zaufania i wiarygodności organów państw członkowskich, które są możliwe do osiągnięcia dzięki skutecznej współpracy z podmiotami gospodarczymi i posiadać odpowiednią strukturę.

Ponadto motyw 33 dyrektywy NIS wskazuje obowiązek przekazywania informacji innym państwom członkowskim i Komisji przez pojedynczy punkt kontaktowy poprzez przedkładanie tzw. grupie współpracy sprawozdań zawierających informacje na temat liczby otrzymanych zgłoszeń, charakteru zgłoszonych cyberincydentów (rodzaj, istotność, czas trwania). Zakłada się przy tym, że sprawozdania te powinny zawierać informacje zanonimizowane, tak aby nie można było zidentyfikować operatora usług kluczowych lub dostawcy usług cyfrowych. Celem przedkładania sprawozdań jest wymiana informacji i najlepszych praktyk w zakresie obsługi cyberincydentów. Niestety dyrektywa nie wskazuje okresów sprawozdawczych, które najprawdopodobniej zostaną określone przez grupę współpracy.

Funkcję pojedynczego punktu kontaktowego w krajowym systemie cyberbezpieczeństwa powinien pełnić minister, który zgodnie z ustawą o działach administracji odpowiada za cyberbezpieczeństwa. Do zadań pojedynczego punktu kontaktowego powinno, w szczególności należeć:

1) koordynacja działań wszystkich interesariuszy krajowego systemu cyberbezpieczeństwa;
2) sprawowanie nadzoru nad CSIRT narodowym, CSIRT sektorowymi oraz CSIRT komercyjnymi w zakresie wymagań organizacyjnych i technicznych;
3) analizowanie usług świadczonych w danym sektorze pod kątem włączenia ich lub usunięcia z listy usług kluczowych;
4) gromadzenie i przetwarzanie informacji dotyczące oferowanych usług kluczowych;
5) zapewnienie transgranicznej współpracy – w obszarze polityczno-strategicznym, w tym przedkładanie Grupie Współpracy sprawozdań, raportów i udział w tworzeniu dobrych praktyk;
6) tworzenie ram prawnych funkcjonowania obszaru cyberbezpieczeństwa RP, w tym czuwanie nad ich spójnością. Ścisła współpraca w tym zakresie ze wszystkimi interesariuszami, w szczególności z tzw. organami właściwymi oraz GIODO;
7) realizacja zadań określonych przez Krajową Radę Cyberbezpieczeństwa np. działania edukacyjno-informacyjne;
8) przewodniczenie pracom Krajowej Rady Cyberbezpieczeństwa;
9) przedstawianie Krajowej Radzie Cyberbezpieczeństwa propozycji działań wynikających z bieżącej analizy architektury systemu cyberbezpieczeństwa RP;
10) przedkładanie Krajowej Radzie Cyberbezpieczeństwa okresowych analiz na temat stanu cyberbezpieczeństwa RP;
11) koordynacja prac Krajowej Radzie Cyberbezpieczeństwa, w szczególności: ustalanie harmonogramu prac Rady, terminów posiedzeń Rady, zwoływanie posiedzeń Rady oraz programów kolejnych posiedzeń Rady.

3.3. Organy właściwe

Dyrektywa NIS wskazuje na potrzebę wyznaczenia tzw. organu właściwego lub organów właściwych. Zgodnie ze swoją właściwością organy właściwe powinny sprawować nadzór nad operatorami usług kluczowych w zakresie stosowania przepisów ustawy o krajowym systemie cyberbezpieczeństwa.

Uwzględniając specyfikę danego państwa członkowskiego może mieć miejsce sytuacja gdy organem właściwym będzie tylko jeden podmiot. Wówczas organ ten pełni równolegle inną rolę – pojedynczego punktu kontaktowego[10]. Analizując kwestie powołania w Polsce jednego organu właściwego, który jednocześnie mógłby pełnić rolę pojedynczego punktu kontaktowego można byłoby przewidzieć taką możliwość w dwóch wariantach: mi-

[10] Art. 8 ust. 3 dyrektywy NIS.

nister właściwy, które zgodnie z ustawą o działach administracji rządowej ma w swoich kompetencjach cyberbezpieczeństwo mógłby poszerzyć swoje kompetencje o zadania przypisane organom właściwym nadzorujących sektory, o których mowa w dyrektywie NIS oraz szeroko rozumiany sektor publiczny. Inną alternatywą dla tego rozwiązania mogłoby być poszerzenie o te kompetencje Urzędu Komunikacji Elektronicznej. Jednak oba warianty obarczone są istotnymi wadami, a mianowicie należałoby zbudować kompetencje merytoryczne, stworzyć infrastrukturę, pozyskać zasoby ludzkie, co wiąże się z dodatkowymi wysokimi kosztami oraz należałoby uzyskać akceptację polityczną, co przy tym procesie byłoby bardzo trudne, gdyż część resortów i istniejących urzędów nadzorujących poszczególne sektory musiałyby oddać swoje kompetencje. Dlatego uwzględniając status quo należy wykorzystać istniejące struktury nadzorcze i jeśli będzie to potrzebne wyposażyć je w dodatkowe kompetencje i źródła finansowania. Ten ostatni wymóg wynika wprost z dyrektywy NIS[11].

Przykładem organów właściwych dla sektorów wymienionych w załączników Nr 2 i Nr 3 do dyrektywy NIS może być Komisja Nadzoru Finansowego dla sektora bankowego i infrastruktury rynków finansowych, Urząd Komunikacji Elektronicznej dla sektora infrastruktury cyfrowej oraz dostawców usług cyfrowych, czy sektora energetycznego to Urząd Regulacji Energetycznej. W przypadku sektora publicznego np. dla działu obrony narodowej organem właściwym winien być Minister Obrony Narodowej, dla działu sprawiedliwości – Minister Sprawiedliwości, dla działu spraw wewnętrznych i działu administracji publicznej – Minister Spraw Wewnętrznych i Administracji, dla działu informatyzacji – Minister Cyfryzacji itd. W ramach swoich kompetencji nadzorczych organy właściwe powinny w szczególności posiadać uprawnienie do:

1) podejmowania czynności związanych z monitorowaniem nadzorowanego przez siebie sektora, w szczególności pod kątem aktualizacji listy usług kluczowych oraz operatorów usług kluczowych;
2) żądania niezwłocznego udostępnienia wszystkich niezbędnych informacji w zakresie:
   a) oceny bezpieczeństwa sieci i systemów informatycznych operatorów usług kluczowych, w tym dokumentów dotyczących polityki bezpieczeństwa,
   b) dowodów skutecznej realizacji polityk bezpieczeństwa, takich jak wyniki audytu bezpieczeństwa, łącznie ze wspierającymi je dowodami, przeprowadzonego przez wykwalifikowanego audytora;
3) przeprowadzania kontroli w zakresie stosowania przez operatorów usług kluczowych oraz dostawców usług cyfrowych środków w zakresie bezpieczeństwa sieci i systemów informatycznych;

[11] Art. 8 ust. 5 dyrektywy NIS.

4) nakładania sankcji i kar przewidzianych w ustawie o krajowym systemie cyberbezpieczeństwa.

Podejmując czynności nadzorcze związane z ustaleniem przyczyn, przebiegu i skutków cyberincydentu, w wyniku którego doszło do wycieku informacji objętych ochroną danych osobowych organ właściwy powinien ściśle współpracować z GIODO, m.in. poprzez włączanie do składu inspekcyjnego organu właściwego przedstawicieli GIODO. Przedstawiciele obu urzędów powinni ściśle ze sobą współpracować podczas inspekcji, wymieniając się na bieżąco informacjami, co pozwoli osiągnąć efekt synergii oraz zwiększyć skuteczność podejmowanych działań nadzorczych. W przypadku materializacji zagrożeń w postaci cyberincydentów projektowana ustawa powinna również zagwarantować szybki przepływ informacji o incydentach pomiędzy organami właściwymi a organami ścigania.

4. Obsługa incydentów

Kwestia działań operacyjnych związanych z monitorowaniem, wykrywaniem i analizowaniem podatności i zagrożeń, a także neutralizacją skutków cyberincydentów oraz ściganiem ich sprawców jest bez wątpienia najważniejszym elementem, powinny być jądrem krajowego systemu cyberbezpieczeństwa. To im powinny być podporządkowane wszystkie elementy i inni interesariusze powinni dołożyć wszelkich starań aby działania te były jak najbardziej efektywne, np. Krajowa Rada Cyberbezpieczeństwa powinna wspierać te działania tworząc właściwe otoczenie prawne.

Współpraca operacyjna jest najważniejszą kwestią. Z tych względów dyrektywa NIS ww. kwestiom poświęca najwięcej uwagi, kładąc bardzo duży nacisk na współpracę wewnętrzną w państwach członkowskich oraz współpracę pomiędzy nimi.

Działanie operacyjne jest to niezmiernie delikatna materia. Jej wrażliwość wynika z istniejącego i zakorzenionego w polskim porządku prawnym podziału kompetencji pomiędzy poszczególne służby odpowiedzialne za bezpieczeństwo narodowe, za bezpieczeństwo wewnętrzne i porządek publiczny oraz działania w obszarze sektora publicznego i przeciwdziałania aktom terroru.

Aby skutecznie działać nie ma potrzeby dokonywania gruntownych zmian w zakresie kompetencji resortu obrony narodowej, Agencji Bezpieczeństwa Wewnętrznego czy Policji. Dzisiaj kompetencje te są czytelne, ale tego czego brakuje, to osiągnięcia efektu synergii. Brakuje trwałych linków komunikacyjnych, które umożliwiałyby szybki i pozbawiony zakłóceń przepływ informacji. Lecz mowa nie tylko o stałych kanałach komunikacyjnych pomiędzy nimi ale także pomiędzy nimi a operatorami usług kluczowych oraz dostawcami usług cyfrowych, sektorowymi i komercyjnymi zespołami reagowania na cyberincydenty. Jednak, aby było to możliwe musimy zlikwidować

„wyspowy" charakter działań poszczególnych interesariuszy odpowiedzialnych za czynności operacyjne w zakresie zwalczania cyberprzestępczości. Będzie to możliwe jedynie wówczas gdy zostanie zbudowana właściwa struktura organizacyjna.

Podstawową kwestią powinno być powołanie u operatorów usług kluczowych oraz dostawców usług cyfrowych wewnętrznych struktur odpowiedzialnych za obsługę incydentu. W zależności od zasięgu i wielkości świadczonych usług komórki te powinny działać w trybie ciągłym (24/7) lub *ad hoc* w sytuacjach materializacji cyberzagrożenia w postaci cyberincydentu. Należy podkreślić, że rolą właśnie tych komórek jest obsługa cyberincydentu i niedopuszczalne jest przerzucania odpowiedzialności za neutralizację skutków tego zdarzenia na sektorowy zespół reagowania na incydenty (CSIRT sektorowy) lub narodowy zespół reagowania na incydenty (CSIRT narodowy). Gdyby dopuszczono taką możliwość moglibyśmy mieć do czynienia z „hazardem moralnym" polegającym na niewłaściwym szacowaniu ryzyka i jego neutralizacji lub przerzuceniu odpowiedzialności za jego neutralizację na CSIRT'y sektorowe lub CSIRT narodowy.

Szacując ryzyko powinno się brać pod uwagę wiele parametrów i w zależności od jego wielkości podejmować adekwatne działania w celu jego mitygacji. Jednak najważniejsze z nich to parametr zasięgu (skutku oddziaływania) oraz parametr istotności cyberincydentu. W zależności od skutku odziaływania: lokalnego, sektorowego, międzysektorowego, czy międzynarodowego oraz istotności incydentu: niskiej, średniej, wysokiej lub krytycznej będą podejmowanie adekwatne działania po stronie operatorów usług kluczowych, CSIRT'ów sektorowych i narodowego oraz organów ścigania i wymiaru sprawiedliwości.

Innym problemem jest stworzenie trwałych i niezależnych od relacji personalizowanych struktur komunikacji pomiędzy wszystkimi interesariuszami. W chwili obecnej mamy do czynienia z działaniami operacyjnym m.in. opartymi na pozyskiwaniu informacji w oparciu o relacje personalne pomiędzy organami ścigania a przedstawicielami operatorów usług kluczowych. Wynika to z potrzeby uzyskiwania bardzo szybko informacji, które będą miały przełożenie na skuteczność działania. Czas reakcji na cyberincydent decyduje o skuteczności jego neutralizacji. W chwili obecnej np. uchylenie tajemnicy bankowej może trwać nawet do dwóch tygodni. Taka zwłoka powoduje, że zamiast uzyskać informacje operacyjne uprawnione służby uzyskując je z tak dużym opóźnieniem uzyskują informacje, które mogą być już wykorzystane jedynie w postępowaniu procesowym.

Operatorzy usług kluczowych oraz dostawcy usług cyfrowych powinni tworzy sektorowe zespoły reagowania (CSIRT sektorowe), które powinny być odpowiedzialne za monitorowanie, wykrywanie i analizowanie podatności i zagrożeń, a także koodynację działań w zakresie neutralizacji skutków cyberincy-

dentów oraz współpracę z organami ścigania. Szczególną rolę powinny odgrywać CSIRT'y sektorowe przy obsłudze cyberincydentów o skutku oddziaływania sektorowym, gdzie cyberincydent oddziałuje na co najmniej dwóch operatorów z jednego sektora. Jeżeli skutek oddziaływania miałby charakter międzyresortowy tzn. dany cyberincydent dotyczyłby co najmniej dwóch operatorów z co najmniej dwóch sektorów, to rolę analityczną, wspierającą i koordynującą przy udziale CSIRT sektorowych, miałby CSIRT narodowy. Natomiast jeśli skutek oddziaływania miałby charakter międzynarodowy tzn. dotyczyłby co najmniej dwóch operatorów z co najmniej dwóch krajów, to rolę analityczną, wspierającą i koordynującą miałby podobniej jak to ma mieć miejsce przy incydencie międzysektorowym, CSIRT narodowy ale przy wsparciu CSIRT'ów sektorowy i przy współpracy z tzw. siecią CSIRT'ów (narodowych).

Takie podejście nie tylko zwiększyłoby skuteczność działania wszystkich interesariuszy ale wiązałoby się z optymalizacją kosztów związanych z obsługą cyberincydentów. Oczywiście może pojawić się sytuacja, że ze względu na zakres świadczonych usług i ich skalę, dany sektor po przeprowadzeniu analizy uzna za bezcelowe powoływanie np. przy izbie gospodarczej lub dedykowanej spółki celowej, która będzie CSIRT'em sektorowym. Jednak w takiej sytuacji operatorzy z danego sektora powinni podjąć decyzję o powierzeniu tej roli CSIRT komercyjnemu, który stanie się dla nich CSIRT'em sektorowym. Innym rozwiązaniem może być utworzenie jednego CSIRT sektorowego dla kilku sektorów np. CSIRT sektorowy obejmujący sektor bankowy i infrastrukturę rynków finansowych lub CSIRT dla firm telekomunikacyjnych i infrastruktury cyfrowej i usług cyfrowych. Należy przy tym dodać, że powstał już w Polsce pierwszy CSIRT sektorowy – dla sektora bankowego. Utworzono w ramach izby gospodarczej zrzeszającej banki – Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich. Wspierało ono już banki w zakresie koordynacji cyberincydentów m. in. nakierowanego na Urząd Komisji Nadzoru Bankowego i banki, który miał miejsce na przełomie stycznia i lutego 2017 r.

Na poziomie krajowym powinien funkcjonować zespół reagowania na cyberincydenty, który powinien w modelu docelowym gromadzić przedstawicieli wszystkich interesariuszy. Dlatego powinno się rozważyć stworzenie jednej przestrzeni, w której mogliby współpracować ze sobą przedstawiciele – eksperci od cyberbezpieczeństwa z resortu obrony narodowej, Agencji Bezpieczeństwa Wewnętrznego, Policji, Prokuratury, CERT Polska, jako CSIRT międzysektorowego oraz CSIRT sektorowych i innych akceptowalnych z punktu widzenia państwa podmiotów. Podobny model został już opracowany i skutecznie wdrożony w innym obszarze, a mianowicie zwalczania terroryzmu – Centrum Antyterrorystyczne (CAT), które skupia wszystkich przedstawicieli służb odpowiedzialnych za bezpieczeństwo wewnętrzne i porządek publiczny.