Jarosław Greser*

Regulacja cyberbezpieczeństwa w sektorze energetycznym w świetle projektu dyrektywy NIS 2

Spis treści

Streszczenie

Rozwój sektora energetycznego jest współzależny z rozwojem technologii informatyczno-komunikacyjnych. Ich wdrażanie pozwala na tworzenie wydajniejszych systemów wytwarzania i zarządzania energią oraz jest kluczowe w przejściu do energetyki opartej na odnawialnych źródłach energii, która jest jednym z głównych celów Unii Europejskiej. Jednocześnie wdrażanie ICT rodzi wyzwania związane z bezpieczeństwem używania tej technologii, która bezpośrednio jest związana z całym spektrum zagrożeń związanych z wykorzystaniem internetu. Problematyka ta znalazła się w polu zainteresowania prawodawcy unijnego, który podjął działania na rzecz podniesienie poziomu cyberbezpieczeństwa w krajach członkowskich. W niniejszym artykule zanalizuję działania podjęte w tym zakresie. Będzie on podzielony na cztery części. W pierwszej odniosę się do problematyki cyberbezpieczeństwa w sektorze energetycznym w kontekście polityk UE. W drugim przedstawię obecnie obowiązujące regulacje w tym zakresie skupiając się na Akcie o cyberbezpieczeństwie (Cybersecurity Act) oraz Dyrektywie 2016/1148 określanej w literaturze jako Dyrektywa NIS. W trzecim przeanalizuje planowane zmiany zawarte we wniosku legislacyjnym Komisji mającym doprowadzić do uchwalenia Dyrektywy NIS 2. W czwartej natomiast podsumuję i ocenię propozycje KE.

Słowa kluczowe: cyberbezpieczeństwo; energetyka; NIS 2; podmioty istotne; podmioty niezbędne.

JEL: K20, K32

* Adiunkt na Uniwersytecie im. Adama Mickiewicza; adres e-mail: greser@amu.edu.pl; ORCID: 0000-0002-1021-6142. Tekst powstał w oparciu o badania prowadzone w ramach realizacji grantu „Cyberbezpieczeństwo urządzeń medycznego Internetu Rzeczy – perspektywa prawna" finansowanego ze środków Narodowego Centrum Nauki, nr umowy 2020/04/X/HS5/00135.

I. Wprowadzenie

Problematyka wytwarzania i dystrybuowania energii jest strategicznym zagadnieniem dla bezpieczeństwa organizacji państwowej. Zmiany w otoczeniu geopolitycznym, środowiskowym i technologicznym spowodowały jednocześnie konieczność przekształcenia dotychczasowych modeli funkcjonowania sektora energetycznego. W literaturze jako kluczowy czynnik wskazuje się przejście na odnawialne źródła energii i intensyfikację procesów jej oszczędzania (Hordeski, 2020). Zagadnienie to stało się centrum agendy politycznej Unii Europejskiej przedstawionej w Wytycznych politycznych przewodniczącej Komisji Europejskiej Ursuli von der Leyen, priorytetach Parlamentu Europejskiego oraz programie strategicznym Rady Europejskiej na lata 2019–2024[1]. Celem, który ma zostać osiągnięty jest transformacja cyfrowa i ekologiczna, która ma objąć wszystkie aktywności gospodarcze i społeczne, w efekcie zaś doprowadzić do wzrostu konkurencyjności i dobrobytu Europy, suwerenności gospodarczej i technologicznej oraz odporności na wstrząsy zewnętrzne[2], neutralności klimatycznej i przywództwa cyfrowego[3].

Sposoby realizacji tych założeń są precyzowane w innych dokumentach, wśród których podstawowe znaczenie ma Europejski Zielony Ład[4] oraz strategia „Kształtowanie cyfrowej przyszłości Europy"[5]. Zgodnie z nimi zmiany w sektorze energetycznym są współzależne z rozwojem sektora cyfrowego, który ma być źródłem innowacji w zakresie czystej technologii[6] oraz dostarczycielem usług ograniczających zużycie energii[7].

Jednocześnie wraz z postępującą digitalizacją powstaje pytanie o bezpieczeństwo usług i infrastruktury połączonej z internetem. W tym kontekście warto przywołać opinię byłego dyrektora FBI, Roberta Muellera, który stwierdził, że przedsiębiorstwa dzielą się na dwa typy: te które padły ofiarą ataku i te które nimi się staną (Mueller, 2012). Liczne przykłady potwierdzają tę tezę. Trzeba zauważyć, że duże organizacje pomimo dysponowania wiedzą i zasobami nie są wolne od zagrożeń, czego przykładem jest atak nazwany przez badaczy *Soliorgate* skutkujący naruszeniem systemów informacyjnych ponad 400 największych globalnych korporacji według listy *Fortune 500* (Fireeye, 2020). Jednocześnie małe i średnie przedsiębiorstwa, oprócz bycia celem samym w sobie, mogą być ważnym celem dla napastników, szczególnie gdy znajdują się w łańcuchu dostaw właściwego celu. W takiej sytuacji mogą być one wykorzystane jako wektor ataku lub do zakłócenia funkcjonowania podmiotu, w który atak był wymierzony.

Szczególnym celem atakujących są podmioty operujące infrastrukturą krytyczną ze względu na skutki społeczne, jakie może wywołać takie działanie. Dlatego też istnieje bardzo szeroki krąg podmiotów, które mogą, potencjalnie, zainicjować taki atak. Można do nich zaliczyć osoby

[1] Komunikat Komisji z 10.03.2020 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Nowa strategia przemysłowa dla Europy", COM(2020) 102 final, s. 1.

[2] Komunikat Komisji z 10.03.2020 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia MŚP na rzecz zrównoważonej i cyfrowej Europy", COM(2020) 103 final, s. 1.

[3] Komunikat Komisji z 10.03.2020 r do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „w sprawie określenia i usuwania barier na jednolitym rynku", COM(2020) 93 final, s. 1.

[4] Komunikat Komisji z 11.12.2019 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Europejski Zielony Ład" COM(2019) 640 final.

[5] Komunikat Komisji z 19.2.2020 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Kształtowanie cyfrowej przyszłości Europy", COM(2020) 67 final.

[6] Komunikat Komisji z 10.03.2020 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Nowa strategia przemysłowa dla Europy", COM(2020) 102 final, s. 4.

[7] Unia, która mierzy wyżej Mój program dla Europy. Wytyczne polityczne na następną kadencję komisji europejskiej (2019–2024), s. 3.

kierujące się chęcią zysku, służb wywiadowcze obcych państw, grupy ekstremistyczne czy hacktywistów działających dla dobra wspólnego. Produkcja i dystrybucja energii elektrycznej ma wyjątkowy status ze względu na efekty potencjalnych zakłóceń wpływające na wszystkie aspekty życia społecznego i gospodarczego. Przykładowo, można tu przywołać udany atak na ukraińską sieć dystrybucyjną energii elektrycznej, który skutkował pozbawieniem dostaw prądu 225 tysięcy odbiorców i sparaliżował funkcjonowanie wielu instytucji (Rojszczak, 2020, s. 314).

W niniejszym artykule przybliżę inicjatywy legislacyjne podejmowane przez Unię Europejską w celu wzmocnienia cyberbezpieczeństwa sektora energetycznego. Będzie składał się on z dwóch części. W pierwszej przedstawię obecnie istniejące rozwiązania i ich mankamenty. Natomiast w drugiej – zaprezentuję projekty nowych rozwiązań legislacyjnych, skupiając się na inicjatywie zrewidowania dyrektywy 2016/1148[8] (dalej: dyrektywa NIS 2).

II. Aktualne regulacje sektora energetycznego w zakresie cyberbezpieczeństwa

Zagadnienia dotyczące cyberbezpieczeństwa są regulowane na poziomie UE w różnego rodzaju aktach prawnych. Można wśród nich wyróżnić regulacje sektorowe, dotyczące przykładowo sektora telekomunikacyjnego, które wprost wyłączają zastosowanie ogólnych przepisów (Piątek, 2020, s. 29) oraz regulacje tematyczne. Wśród tych drugich największe znaczenie dla energetyki mają regulacje o ochronie danych osobowych. Trzeba zauważyć, że zagadnienie to dotyczy w bardzo szerokim zakresie sprzedawców oraz podmiotów dostarczających energię elektryczną konsumentom. Ogólne rozporządzenie o ochronie danych[9] w artykule 32 wprowadza wymóg odpowiedniego zabezpieczenia danych, którego podstawą jest przeprowadzenie analizy ryzyka zagrożeń dla ich bezpieczeństwa oraz przyjęcie i stałe testowanie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych[10]. Obowiązek ten dotyczy zarówno wewnętrznych systemów przedsiębiorstwa, w ramach których dane są przetwarzane, jak i urządzeń za pomocą których są one pozyskiwane. W tym kontekście warto zwrócić uwagę na wyzwania, jakie są związane z korzystaniem z tak zwanych inteligentnych liczników prądu. Dla zapewnienia bezpieczeństwa wytwarzanych przez nie danych konieczna jest ocena czy rozwiązania techniczne wprowadzone przez producenta urządzenia są adekwatne, np. jakich algorytmów kryptograficznych używa urządzenie do szyfrowania danych. Ponadto konieczne jest monitorowanie pojawiających się zagrożeń i aktualizacja aplikacji mająca im przeciwdziałać, ponieważ, zgodnie ze stanowiskiem Prezesa Urzędu Ochrony Danych Osobowych, brak aktualnego oprogramowania stanowi naruszenie przepisów RODO[11]. Można więc przyjąć, że przepisy RODO narzucają procesowe podejście do cyberbezpieczeństwa, które jest wskazywane w literaturze jako modelowe (Łuczak, 2020, s. 77), niemniej jednak ograniczają się one do jednego z aspektów tego zagadnienia, jakim jest ochrona danych osobowych.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE L194/1).

[9] 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) (Dz. Urz. UE. L 119/1).

[10] Decyzja Prezesa Urzędu Danych Osobowych z 11 lutego 2021 r., DKN.5130.2024.2020. Pozyskano z: https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020 (20.04.2021).

[11] Ibidem.

Unia Europejska podejmuje również próby systemowej regulacji zagadnienia cyberbezpieczeństwa. Jej efektem jest przyjęcie rozporządzenia 2019/881[12] (dalej: akt o cyberbezpieczeństwie) oraz wspomnianej powyżej dyrektywy 2016/1148 określanej w literaturze jako Dyrektywa NIS. Analizując przepisy pierwszego ze wskazanych aktów pod kątem sektora energetycznego, trzeba zauważyć, że jego zakres przedmiotowy obejmuje wyznaczenie celów i zadań Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz ram ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa. Nie ma zatem bezpośredniego przełożenia na normowanie sytuacji podmiotów operujących w branży energetycznej, mimo że ENISA jest zobligowana do współpracy z Agencją Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki (ACER). Przepisy te mogą mieć jednak duże oddziaływanie pośrednie. Trzeba tu zwrócić szczególną uwagę na wynikający z art. 9 obowiązek przeprowadzania przez agencję analiz powstających technologii i przedstawiania tematycznych ocen dotyczących spodziewanego społecznego, prawnego, gospodarczego i regulacyjnego ich wpływu na cyberbezpieczeństwo oraz gromadzenia i analizowania publicznie dostępnych informacji dotyczących istotnych incydentów. Zebrane w ten sposób informacje mogą mieć znaczący wpływ na usprawnianie działania oraz decyzję w zakresie wdrożenia określonych rozwiązań w sektorze energetycznym.

Podobny efekt będzie miało wdrożenie europejskich ram certyfikacji cyberbezpieczeństwa. Rozporządzenie 2019/881 przewiduje powstanie systemu niezależnego od innych systemów certyfikacyjnych i nieuchylającego obowiązków z nich wynikających (Żywicka, 2021). Zgodnie z Motywem 13, zadaniem tego systemu jest potwierdzenie, że produkty ICT są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenia dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych bądź funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Trzeba zauważyć, że „produkt ICT" zgodnie z definicją zawartą w art. 2 pkt 12 będzie obejmował element lub grupę elementów sieci lub systemów informatycznych. Jednocześnie przez „system informatyczny" należy rozumieć zgodnie z brzmieniem art. 4 pkt 1 dyrektywy NIS, a więc będzie on obejmował wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych. Na tej podstawie należy wnioskować, że zdecydowana większość elementów współczesnych systemów wytwarzania i przesyłania energii będzie mogła być poddana certyfikacji. Trzeba również zauważyć, że zgodnie z artykułem 56 ust. 2 rozporządzenia 2019/881 jest ona dobrowolna, o ile prawo Unii lub prawo państwa członkowskiego nie stanowi inaczej. Należy rozważyć czy ze względu na istotność sektora energetycznego dla gospodarki nie wprowadzić obowiązku certyfikacji urządzeń wykorzystywanych przynajmniej w kluczowych procesach wytwórczych i przesyłowych.

Dyrektywa 2016/1148 została wprowadzona, aby doprowadzić do osiągnięcia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, a przez to poprawić funkcjonowanie rynku wewnętrznego. Sposobem na jego osiągnięcie ma być powstanie sieci wymiany informacji i współpracy w tym zakresie pomiędzy państwami UE oraz krajowych

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds.Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151/15).

systemów cyberbezpieczeństwa, które mają się opierać na zdefiniowaniu określonych grup podmiotów i nałożeniu na nich obowiązków z zakresu cyberbezpieczeństwa oraz wyznaczeniu organów w ramach struktury państwa, których zadaniem jest obsługa incydentów, w tym działania kryzysowe oraz analiza przeprowadzonych ataków i formułowanie rekomendacji z nich wynikających. Dyrektywa przewiduje dwa rodzaje adresatów nakładanych przez nią obowiązków. Są nimi operatorzy usług kluczowych i dostawcy usług cyfrowych. Do pierwszej grupy zaliczane są podmioty publiczne lub prywatne, które należą do jednej z kategorii wskazanych w załączniku do dyrektywy, a jednocześnie świadczące usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej przy czym świadczenie tej usługi zależy od sieci i systemów informatycznych, a incydent miałby istotny skutek zakłócający dla świadczenia tej usługi. Druga grupa obejmuje wszystkie osoby prawne świadczące usługi cyfrowe i jest wskazana w załączniku do dyrektywy. Należy zauważyć, że w przypadku podmiotów z sektora energetycznego, jeśli nie będą one spełniać przesłanek do uznania ich za świadczące usługi cyfrowe, w wielu przypadkach podmioty te będą kwalifikować się do uznania ich za operatorów usług kluczowych. Wynika to z bezpośredniego wskazania w załączniku, że podmiotami, które muszą być badane pod kątem spełnienia przesłanek do uznania za takich operatorów: są przedsiębiorstwa energetyczne w rozumieniu art. 2 pkt 35 dyrektywy 2009/72[13], które wykonują funkcję „dostawy" zgodnie z definicją w art. 2 pkt 19 tej dyrektywy, operatorzy systemu dystrybucyjnego zgodnie z art. 2 pkt 6 dyrektywy 2009/72 oraz operatorzy systemu przesyłowego zgodnie z art. 2 pkt 4 dyrektywy 2009/72.

III. Planowane zmiany legislacyjne

Uchwalenie unijnych regulacji w zakresie cyberbezpieczeństwa można uznać za przełomowy moment dla tworzenia ponadpaństwowego systemu ochrony systemów informatycznych. Nie pozostaje on jednak bez wad i luk w ochronie, które ujawniły się w toku jego funkcjonowania. Prawodawca unijny szczególnie skupił się na dyrektywie NIS, co można uznać za słuszny wybór ze względu na fakt najszerszej regulacji zagadnień cyberbezpieczeństwa. W czasie przeglądu dyrektywy, który Komisja Europejska rozpoczęła w 2020 roku (dalej: przegląd NIS), zdefiniowano problem spójności z regulacjami sektorowymi, duże różnice w implementacji dyrektywy i identyfikacji operatorów usług kluczowych, niski poziom cyberodporności przedsiębiorstw działających w UE oraz niski poziom wspólnej orientacji sytuacyjnej i brak wspólnego reagowania kryzysowego. Jako problem wskazano również brak objęcia przepisami sektorów istotnych z perspektywy cyberbezpieczeństwa, czego przykładem w zakresie energetyki może być pozostawienie poza zakresem regulacji właściwie całego sektora elektromobilności (Greser, 2019, s. 116). Ponadto Komisja stwierdziła, że niektóra państwa wykroczyły poza zakres minimalnej harmonizacji i stworzyły nadmierne obciążenia wpływające spójność jednolitego rynku i transgraniczne świadczenie usług[14]. Mankamenty dyrektywy wskazywano również w doktrynie, podnosząc między innymi brak definicji cyberbezpieczeństwa (Szpor, 2020, s. 1189) oraz ograniczenia zakresu przedmio-

[13] Dyrektywa Parlamentu Europejskiego i Rady 2009/72/WE z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego energii elektrycznej i uchylająca dyrektywę 2003/54/WE (Dz. U. L 211/55).

[14] Komunikat Komisji z 10 marca 2020 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „w sprawie określenia i usuwania barier na jednolitym rynku", COM(2020) 93 final, s. 13.

towego do oceny poziomu odporności sieci i systemów informatycznych, a nie całego systemu teleinformatycznego (Świtała, 2020, s. 1249). Do planowania zmian w dyrektywie przyczyniło się również ustalenie rozwoju jednolitego rynku cyfrowego jako jednego z priorytetów UE. Przyjęto założenie, ujawnione już w preambule rozporządzenia 2019/881, że im bardziej połączona staje się gospodarka i społeczeństwo, tym większa jest podatność na ataki i tym szersze są ich skutki. Jednocześnie organy unijne podkreślają, że cyberzagrożenia stanowią niebezpieczeństwo dla demokracji i europejskich wartości i dlatego nie mogą być pojmowane wyłącznie w kategoriach ekonomicznych.

Wszystkie te czynniki łącznie doprowadziły do objęcia dyrektywy NIS programem sprawności i wydajności regulacyjnej (REFIT), którego celem jest ograniczenie obciążenia regulacyjnego dla właściwych organów oraz kosztów przestrzegania przepisów dla podmiotów publicznych i prywatnych, co doprowadziło do przedstawienia 16 grudnia 2020 roku wniosku legislacyjnego mającego na celu uchwalenie nowej dyrektywy roboczo nazywanej NIS 2[15]. Celem prawodawcy wskazanym w motywie 5 jest określenie minimalnych przepisów dotyczących funkcjonowania skoordynowanych ram regulacyjnych, ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w każdym państwie członkowskim, dokonanie aktualizacji wykazu sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa oraz ustanowienie skutecznych środków naprawczych i sankcji, które są kluczowe dla skutecznego egzekwowania tych obowiązków.

1. Obowiązki podmiotów kluczowych i podmiotów istotnych

Wniosek legislacyjny przewiduje nałożenie obowiązków, co do zasady, na państwa członkowskie. Natomiast prawodawca przyjął konstrukcję, że część obowiązków będzie miała być zrealizowana przez nie samodzielnie, część zaś ma zostać nałożona na inne podmioty. Do tej drugiej grupy należą obowiązki, związane z zarządzaniem ryzykiem w cyberprzestrzeni oraz zgłaszaniem incydentów Określając grupę podmiotów zobowiązanych w tym zakresie, prawodawca przewidział zasadnicze zamiany w stosunku do dyrektywy NIS. W miejsce dostawcy usług cyfrowych rozumianego jako każdą osobę prawną, która świadczy usługi cyfrowe oraz operatorów usług kluczowych, do których zaliczono podmioty publiczne lub prywatne należącego do grup wskazanych w załączniku, wprowadzono nowy sposób określania adresatów norm. W art. 4 pkt 24 zawarto definicję podmiotu rozumianego jako każda osoba fizyczna lub prawna utworzona i uznawana za taką na podstawie prawa krajowego obowiązującego w miejscu, w którym osoba ta ma siedzibę, która może, działając we własnym imieniu, wykonywać prawa i podlegać obowiązkom. Objaśnienie to, sprowadzające się w polskich warunkach do posiadania zdolności do czynności prawnych, ma znaczenie porządkujące, biorąc pod uwagę różne możliwe regulacje w porządkach krajowych państw członkowskich. Należy jednak zwrócić uwagę, że już na tym poziomie mamy rozszerzenie zakresu normowania w przypadku podmiotów świadczących usługi cyfrowe, ponieważ w obecnie obowiązującym stanie prawnym obejmuje ona wyłącznie osoby prawne, co należy uznać za zbyt wąską regulację. Dlatego należy w pełni zaaprobować przywołaną propozycję,

[15] Wniosek z dnia 16 grudnia 2020 r. „Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148", COM(2020) 823 final.

gdyż nie wydaje się aby właściwym kryterium realizacji zadań z zakresu cyberbezpieczeństwa była forma podmiotowości prawnej.

W art. 4 pkt 25 i 26 prawodawca wyróżnia dwa rodzaje podmiotów: niezbędne (*essential entities*) i istotne (*important entities*). Przynależność do pierwszej grupy określa się według sektorów określonych w załączniku I do dyrektywy NIS 2. Wśród nich znajdują się takie obszary, które były przedmiotem regulacji dotychczasowych przepisów, jak bankowość i infrastruktura rynków finansowych, transport i dostawa i dystrybucja wody pitnej. Prawodawca postanowił objąć regulacjami także nowe grupy podmiotów, między innymi takie jak: świadczeniodawcy usług medycznych, o których mowa w art. 3 lit. g) dyrektywy 2011/24[16]; podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych; podmioty produkujące wyroby medyczne, dla których uznano, że mają one krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego; podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym oraz dla regionów na poziomie NUTS 1 i NUTS 2, co w polskich warunkach odpowiada województwom i obszarowi metropolitalnemu Warszawy (Wojnarowski, 2019, s. 51–53); przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe i przemysłowe; operatorzy infrastruktury naziemnej należącej do państw członkowskich oraz podmiotów prywatnych lub przez te podmioty zarządzane i obsługiwane. Osobną kategorię stanowią podmioty operujące w sektorze infrastruktury cyfrowej, która obejmuje między innymi dostawców punktu wymiany ruchu internetowego, usług DNS, rejestrów nazw TLD czy usług chmurowych. Częściowo podlegają oni przepisom dyrektywy NIS, lecz są tam klasyfikowani jako dostawcy usług cyfrowych, co wiąże się z mniejszym zakresem obowiązków w porównaniu z przewidzianymi w nowych regulacjach (por. Szpor, Gryszczyńska i Czaplicki, 2019, s. 52).

W odniesieniu do sektora energetycznego prawodawca przewiduje rozciągnięcie regulacji na podmioty z pięciu podsektorów. Pierwszy z nich obejmuje energię elektryczną i w jego ramach mieszczą się wytwórcy, przedsiębiorstwa energetyczne wykonujące dostawy, operatorzy systemu dystrybucyjnego oraz operatorzy systemu przesyłowego. Definicje legalne tych podmiotów znajdują się w dyrektywie 2019/944[17]. Ponadto prawodawca zdecydował o objęciu obowiązkami wyznaczonych operatorów energii elektrycznej, o których mowa w art. 2 pkt 8 rozporządzenia 2019/943[18]. Ostatnią grupą są uczestnicy rynku energii elektrycznej, o których mowa w art. 2 pkt 25 rozporządzenia 2019/943, ale podmioty te muszą świadczyć jednocześnie usługi agregacji, odpowiedzi odbioru lub magazynowania energii w sposób zdefiniowany w dyrektywie 2019/944. Trzeba zauważyć tu znaczne rozszerzenie zakresu podmiotowego w stosunku do obecnie obowiązujących przepisów, które obejmują przedsiębiorstwa energetyczne, operatorów systemu dystrybucyjnego i operatorów systemu przesyłowego.

Drugim podsektorem energetycznym jest system ciepłowniczy lub system chłodniczy, który w rozumieniu art. 2 pkt 19 dyrektywy 2018/2001[19] obejmuje dystrybucję energii termicznej w postaci pary, gorącej wody lub schłodzonych płynów z centralnych lub zdecentralizowanych źródeł

[16] Dyrektywa Parlamentu Europejskiego i Rady 2011/24 z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz. U. UE L 88/45).

[17] Dyrektywa Parlamentu Europejskiego i Rady 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz. U. UE L 158/125).

[18] Rozporządzenie Parlamentu Europejskiego i Rady 2019/943 w sprawie rynku wewnętrznego energii elektrycznej (Dz. U. UE L 158/54).

[19] Dyrektywa Parlamentu Europejskiego i Rady 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych (Dz. U. UE L 328/82).

produkcji przez sieć do wielu budynków lub punktów w celu wykorzystania jej do ogrzewania lub chłodzenia pomieszczeń lub procesów. Podsektor ten nie był objęty unormowaniami dyrektywy 2016/1148. Podobna sytuacja dotyczy kolejnego podsektora, jakim są operatorzy instalacji służących do produkcji, magazynowania i przesyłu wodoru.

Czwartym – są operatorzy ropociągów, operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej, którzy byli objęci dotychczasowymi regulacjami. W tym podsektorze ustawodawca zdecydował się na dodanie również krajowych central zapasów naftowych, o których mowa w art. 2 pkt f) dyrektywy 2009/119[20].

Ostatnim wyróżnionym podsektorem jest działalność związana z gazem ziemnym. Wśród podmiotów podlegających przepisom dyrektywy NIS 2 prawodawca wyróżnia przedsiębiorstwa dostarczające gaz, operatorów systemu dystrybucyjnego, operatorów systemu przesyłowego, operatorów systemów magazynowania, operatorów systemu LNG, przedsiębiorstwa gazowe oraz operatorów instalacji służących do rafinacji i przetwarzania gazu ziemnego. Definicji legalnych tych podmiotów należy poszukiwać w dyrektywie 2009/73[21], która wyznacza ramy regulacyjne zasad unijnego rynku gazu ziemnego.

Drugą grupą podmiotów, które wyróżnia prawodawca są podmioty istotne. Należą do nich podmioty operujące w sektorze usług pocztowych i kurierskich, gospodarowania odpadami, produkcji i dystrybucji chemikaliów, produkcji i dystrybucja żywności. Do podmiotów istotnych zaliczono również dostawców usług cyfrowych, rozumianych jako dostawców internetowych platform handlowych, wyszukiwarek internetowych, platform usług sieci społecznościowych. Ponadto przepisami objęte są liczne przedsiębiorstwa produkcyjne, w tym produkujące: wyroby medyczne, komputery, wyroby optyczne i elektroniczne, urządzenia elektryczne oraz sprzęt transportowy. Warto zauważyć, że poza dostawcami cyfrowymi, żaden z tych sektorów nie był objęty dyrektywą NIS. Rozszerzenie zakresu podmiotowego stanowi realizację postulatu podnoszonego w literaturze. Wskazuje się, że spowoduje to zwiększenie ogólnego poziomu cyberbezpieczeństwa, ponieważ dotychczasowa praktyka działań cyberprzestępców dowodzi, że nie ograniczają lub skupiają się oni na jakiejś branży (Greser, 2020, s. 79).

Odnosząc się do zakresu podmiotowego, należy wskazać, że projekt dyrektywy NIS 2 co do zasady wykluczył możliwość uznania za podmioty niezbędne lub istotne przedsiębiorstwa należące go grupy mikro, małych lub średnich w rozumieniu zalecenia Komisji 2003/361[22]. Takie unormowanie mogłoby wprowadzić sporą lukę regulacyjną, dlatego prawodawca zdecydował się na wyjątek umieszczony w art. 2 ust. 2 dyrektywy. Zgodnie z nim MŚP będzie adresatem obowiązków wynikających z dyrektywy, jeżeli przedmiot jego działalności zawiera się w definicji podmiotów niezbędnych lub istotnych oraz równocześnie spełni jedną z przesłanek wskazanych w tym przepisie. Z perspektywy sektora energetycznego największe znaczenie mają przesłanki bycia: jedynym dostawcą danej usługi w państwie członkowskim lub świadczenie takich usług, których zakłócenie mogłoby mieć wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne

[20] Dyrektywa Rady 2009/119 z dnia 14 września 2009 r. nakładająca na państwa członkowskie obowiązek utrzymywania minimalnych zapasów ropy naftowej lub produktów ropopochodnych (Dz. U. WE L 265/9).

[21] Dyrektywa Parlamentu Europejskiego i Rady 2009/73 z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego gazu ziemnego i uchylająca dyrektywę 2003/55/WE (Dz. U. WE L 211/94).

[22] Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. Urz. UE L 124/36).

albo prowadzić do powstania ryzyka systemowego w szczególności jeśli takie zakłócenie mogłoby mieć wpływ transgraniczny. Taka regulacja ma odnosić się w głównej mierze do przedsiębiorstw znajdujących się w łańcuchu dostaw podmiotów z sektora energetycznego. W praktyce może mieć ona podstawowe znaczenie, ponieważ coraz liczniejsze są cyberoperacje wymierzone w duże podmioty, gdzie wektorem ataku są dostawcy lub podwykonawcy (Kozłowski, 2021).

Wśród obowiązków nałożonych na podmioty niezbędne i podmioty istotne do najważniejszych należy zapewnienie środków zarządzania ryzykiem w cyberprzestrzeni, o których mówi art. 18 projektu dyrektywy NIS 2. Ich podstawą są środki techniczne i organizacyjne w celu zarządzania rodzajami ryzyka dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. Trzeba zauważyć, że prawodawca posłużył się przy formułowaniu obowiązków metodą *risk based approach*, którą wykorzystywał szeroko już wcześniej i która jest uznawana przez specjalistów z zakresu cyberbezpieczeństwa za najbardziej skuteczną (Marzec, 2020, s. 1243). Metoda ta stosowana jest również w innych aktach prawnych, które są częściowo związane z problematyką cyberbezpieczeństwa, jak na przykład RODO. W odróżnieniu jednak od tego aktu (Litwiński, 2017, s. 54) prawodawca wskazał minimalny zakres środków, które muszą być wdrożone. Obejmują one analizę ryzyka i politykę bezpieczeństwa systemów informatycznych, postępowanie w przypadku incydentu, w tym zapobieganie incydentom, wykrywanie ich i reagowanie na nie, ciągłość działania i zarządzanie kryzysowe, bezpieczeństwo łańcucha dostaw z uwzględnieniem podatności charakterystycznych dla każdego dostawcy, procedury bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberprzestrzeni oraz stosowanie kryptografii i szyfrowania. Prawodawca nie nakłada obowiązku stosowania określonej metodologii lub systemu certyfikacyjnego w czasie wdrażania wymaganych przez niego środków technicznych i organizacyjnych, jednakże wymaga, aby uwzględniały one najnowszy stan wiedzy i były proporcjonalne do ryzyka. Rozwiązanie to należy uznać za trafne ze względu na spełnienie wymogu neutralności technologicznej, a przez możliwość dostosowania się do dynamicznie zmieniających się wyzwań z zakresu cyberbezpieczeństwa, a jednocześnie umożliwiający korzystanie ze sprawdzonych standardów, takich jak ISO 27001 (Łuczak, 2020, s. 71–75).

Nowością normatywną przewidzianą przez projekt dyrektywy NIS 2 jest nałożenie obowiązków na członków organów zarządzających podmiotów istotnych i podmiotów niezbędnych w zakresie podnoszenia swojej wiedzy z zakresu cyberbezpieczeństwa. Trzeba zauważyć, że prawodawca wskazał, że mają być to wąsko ukierunkowane zajęcia, które pozwolą na zdobycie wiedzy i umiejętności wystarczających do zrozumienia i oceny różnych rodzajów ryzyka w cyberprzestrzeni, praktyk z zakresu zarządzania nimi oraz ich wpływu na działalność podmiotu. Tym samym wykluczone jest uczestnictwo w szkoleniach ogólnych albo wprowadzających do tematyki cyberbezpieczeństwa. Jednocześnie zajęcia nie są nastawione stricte na zagadnienia techniczne, a biorą pod uwagę perspektywę procesową, która jest kluczowa na poziomie zarządczym. Ustanowienie tego obowiązku należy ocenić zdecydowanie pozytywnie. Brak wiedzy, a co za tym idzie zrozumienia dla specyfiki zagrożeń w gronie osób decydujących o budżecie i kierunku działania organizacji może prowadzić do niedoinwestowania sfery związanej z cyberbezpieczeństwem. Nie można oczywiście założyć, że szkolenia będą panaceum na wszelkie bolączki w tym zakresie, trzeba jednak stwierdzić, że jest to krok poczyniony w prawidłowym kierunku.

Ostatnią grupą obowiązków, którą warto wyróżnić z perspektywy sektora energetycznego jest nakaz zgłaszania właściwym organom lub zespołom reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) każdego incydentu mającego istotny wpływ na świadczenie przez nich usług. Zgłaszane mają być również sytuacje, które mogą prowadzić do powstania incydentu, o ile są one znaczące dla określonego podmiotu, co jest rozumiane jako spowodowanie lub możliwość spowodowania istotnych zakłóceń operacyjnych lub strat finansowych dla danego podmiotu albo wywołanie wpływu lub możliwości wpływu na osoby fizyczne lub prawne, powodującego znaczne straty materialne lub niematerialne. W stosownych przypadkach, które zależą od dyskrecjonalnej decyzji podmiotu, mają oni również obowiązek powiadomienia odbiorców swoich usług o wystąpieniu lub możliwości wystąpienia incydentu.

Podmiot dotknięty incydentem ma na zgłoszenie maksymalnie 24 godziny od jego ujawnienia. Zawiadomienie właściwego organu powinno zawierać informacje czy incydent został wywołany działaniem bezprawnym, czy działaniem w złym zamiarze. Nadto na wniosek organu lub CSIRT powinien przekazywać sprawozdania okresowe dotyczące zmian w sytuacji związanej z incydentem. Ponadto w ciągu miesiąca od zgłoszenia należy przekazać sprawozdanie końcowe z incydentu obejmujące w szczególności szczegółowy opis incydentu, jego dotkliwości i skutków, rodzaj zagrożenia lub pierwotną przyczynę, które prawdopodobnie były źródłem incydentu, zastosowane i bieżące środki ograniczające ryzyko.

2. Obowiązki innych podmiotów

Druga grupa obowiązków, której adresatem są państwa członkowskie, obejmuje przyjęcie krajowej strategii cyberbezpieczeństwa, wyznaczanie właściwych organów krajowych, pojedynczych punktów kontaktowych oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (dalej: CSIRT). Należy zauważyć, że o ile podobne obowiązki istniały już w dyrektywie NIS, o tyle ich zakres został znacząco poszerzony i uszczegółowiony. Przykładowo, wskazać należy, że w nowym akcie prawnym planuje się określić, że krajowa strategia cyberbezpieczeństwa musi składać się z co najmniej ośmiu polityk szczegółowych obejmujących między innymi politykę dotyczącą cyberbezpieczeństwa w łańcuchu dostaw dla produktów i usług ICT wykorzystywanych przez podmioty niezbędne oraz, istotnych do świadczenia usług, wytycznych dotyczących uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, polityki dotyczącej wspierania instytucji akademickich i naukowych w celu opracowania narzędzi z zakresu cyberbezpieczeństwa oraz zabezpieczenia infrastruktury sieciowej oraz polityki uwzględniającej konkretne potrzeby małych i średnich przedsiębiorstw.

W zakresie zarządzania incydentami nowością jest stworzenie europejskiego rejestru podatności, który ma prowadzić ENISA. Mają się w nim znaleźć informacje na temat podatności, produktu lub usług ICT oraz sposobów jej wykorzystania i potencjalnych skutków, które mogą się z tym wiązać. Ponadto rejestr ma zawierać informację o aktualizacjach oprogramowania usuwających podatność, a w razie ich braku wytyczne skierowane do użytkowników produktów i usług na temat sposobów ograniczania ryzyka wynikającego z ujawnionych luk w bezpieczeństwie.

Nową regulacją jest również projektowany nakaz stworzenia krajowych ram zarządzania kryzysami cyberbezpieczeństwa. Ma on polegać na wyznaczeniu organu odpowiedzialnego

za zarządzanie incydentami i kryzysami na dużą skalę, określeniu zasobów i procedur, które można wykorzystać w przypadku kryzysu oraz przygotowania planu reagowania na cyberincydenty, który ma obejmować działania krajowe oraz procedury pozwalające na skuteczne zarządzanie cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę na szczeblu Unii. Trzeba zauważyć, że to rozwiązanie może mieć szczególne znaczenie w przypadku ataku na infrastrukturę energetyczną. Wydaje się, że przygotowanie odpowiednich planów reakcji usprawni odparcie ataków i zminimalizuje konsekwencje społeczne związane z brakiem dostaw energii.

Trzecią grupą obowiązków przewidzianych w projekcie dyrektywy NIS 2 są regulacje dotyczące wymiany informacji na temat cyberbezpieczeństwa. Adresatem tych norm są również państwa członkowskie, które mogą zrealizować je w dowolny sposób. W ramach omawianych norm możemy wyróżnić przepisy dotyczące współpracy krajowej i międzynarodowej. Do tej pierwszej odnosi się artykuł 11 projektu, który nakazuje współdziałanie podmiotów odpowiedzialnych za cyberbezpieczeństwo, takich jak właściwe organy krajowe, pojedyncze punkty kontaktowe i CSIRT. Szczególnie organy lub CSIRT mają informować punkt kontaktowy o zgłoszeniach incydentów, istotnych cyberzagrożeń i zdarzeń potencjalnie wypadkowych dokonywanych na podstawie dyrektywy. Z perspektywy sektora energetycznego istotne znaczenie ma regulacja przewidziana w art. 11 ust. 4 i 5, która nakazuje stworzyć system współpracy między organami właściwymi do spraw cyberbezpieczeństwa i pojedynczymi punktami kontaktowymi a organami ścigania, organami ochrony danych, krajowymi organami finansowymi oraz organami odpowiedzialnymi za infrastrukturę krytyczną. Ta ostatnia grupa podmiotów, do której będą zaliczały się wytwórcy i dystrybutorzy energii elektrycznej ma dodatkowo otrzymywać informacje na temat rodzajów ryzyka w cyberprzestrzeni, cyberzagrożeń i incydentów mających wpływ na podmioty uznane za podmioty krytyczne, a także na temat środków wprowadzonych przez właściwe organy w odpowiedzi na takie ryzyko i incydenty. Regulację taką należy uznać za trafną. Trzeba jednak odnotować, że podobne rozwiązania mogłyby być wprowadzone w stosunku do wszystkich podmiotów istotnych i krytycznych. Zgodnie z art. 10 ust. 2 lit. a i b projektu CSIRT mają obowiązek monitorowania cyberzagrożeń, podatności i incydentów na poziomie krajowym oraz wczesnego ostrzegania podmiotów niezbędnych i istotnych oraz innych zainteresowanych stron o cyberzagrożeniach, podatnościach i incydentach, a także kierowania do nich ogłoszeń oraz przekazywania im informacji dotyczących cyberzagrożeń, podatności i incydentów. Wydaje się więc, że nie byłoby nadmiernym utrudnieniem stworzenie systemu obejmującego przekazywanie ujednoliconych informacji obu grupom podmiotów, ponieważ obecna regulacja może prowadzić do niepotrzebnego przesyłania tych samych komunikatów.

W zakresie obowiązków dotyczących współpracy międzynarodowej kluczowym podmiotem jest krajowy punkt kontaktowy, który pełni funkcję łącznikową i zapewnia transgraniczną współpracę organów swojego państwa członkowskiego z odpowiednimi organami w innych państwach członkowskich, a także międzysektorową współpracę z innymi właściwymi organami krajowymi w swoim państwie członkowskim. Ponadto w celu wzmocnienia instytucjonalnego i usprawnienia przepływu wiedzy i dobrych praktyk utworzone mają zostać trzy organizacje o charakterze sieciowym. Pierwszą z nich jest Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (dalej: EU-CyCLONe), w skład której wchodzić mają przedstawiciele organów

zarządzania kryzysowego państw członkowskich oraz ENISA. Jej zadaniem jest przede wszystkim koordynacja zarządzania incydentami oraz wymiana informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. Drugą organizacją jest sieć krajowych CSIRT, która jest głównie nastawiona na skuteczną współpracę operacyjną między państwami członkowskimi. Trzecią jest zaś Grupa Współpracy składająca się z przedstawicieli państw członkowskich, Komisji i ENISA. W jej pracach na prawach obserwatora bierze udział Europejska Służba Działań Zewnętrznych. Celem Grupy jest strategiczna współpraca i wymiana informacji między państwami członkowskimi w obszarze stosowania dyrektywy. Przyjęta przez prawodawcę koncepcja różnych ciał mających na celu współpracę międzynarodową może wydawać się kontrproduktywna, trzeba jednak zwrócić uwagę, że każda z nich ma inną specyfikę. Krajowy punkt kontaktowy jest powołany do wymiany informacji o najszerszym charakterze i to na nim będzie spoczywał ciężar bieżącej komunikacji zarówno dwu-, jak i wielostronnej pomiędzy różnymi podmiotami funkcjonującymi w ramach systemu cyberbezpieczeństwa. EU-CyCLONe koncentruje się na działaniach w trakcie poważnych incydentów i przez to jej działania kierowane są do organów skupionych na ich zwalczaniu. Sieć CSIRT, która została powołana art. 12 obecnie obowiązującej dyrektywy, koncentruje się na wymianie i analizie informacji o charakterze technicznym, choć zakres przepisów pozwala na dużo szersze działania. Natomiast Grupa Współpracy, której zalążek również funkcjonuje obecnie, to ciało o charakterze strategicznym. Jego głównym zadaniem jest wyznaczanie kierunków działań w zakresie cyberbezpieczeństwa, a nie reakcja na bieżące wydarzenia. Wydaje się, że taki podział jest efektywny i odpowiada na zróżnicowane potrzeby podmiotów odpowiedzialnych za cyberbezpieczeństwo, a jednocześnie na tyle precyzyjny, że nie dochodzi pokrywania się kompetencji, co mogłoby skutkować sporami kompetencyjnymi. Z perspektywy sektora energetycznego takie rozwiązanie należy przyjąć z zadowoleniem, ponieważ podnosi ono jego bezpieczeństwo.

Na uwagę zasługuje fakt, że prawodawca w art. 26 przewidział podstawę do wymiany informacji w zakresie cyberbezpieczeństwa przez podmioty niezbędne i istotne. Analiza tego przepisu wskazuje, że może do niej dochodzić pomiędzy zarówno dwoma podmiotami, jak i sieciami podmiotów, choć jednocześnie tworzenie grup nie jest wymuszane. Oprócz informacji podmioty takie mogą przekazywać dane dotyczące podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, alarmów dotyczących cyberbezpieczeństwa i narzędzi konfiguracji, jeżeli ich wymiana ma na celu zapobieganie incydentom, ich wykrywanie, reagowanie na nie lub łagodzenie ich skutków albo zwiększa poziom cyberbezpieczeństwa określonych podmiotów. Zasady tworzenia i warunki funkcjonowania mechanizmów wymiany informacji zależą od państw członkowskich z zastrzeżeniem, że nie mogą one naruszać przepisów o ochronie danych osobowych zawartych w RODO. Ustęp 4 analizowanego artykułu wskazuje, że podmiot może się wycofać z uczestnictwa w sieci przez co należy wnioskować, że państwa członkowskie nie mogą nakazać obowiązkowej do niej przynależności. Należałoby rozważyć jednak pozostawienie decyzji w tym zakresie w kompetencji państw, które ze względu na specyfikę funkcjonowania określonego sektora mogłyby być zainteresowane wdrażaniem analizowanego rozwiązania. Jednocześnie trzeba stwierdzić, że narzędzie to może być znaczące dla przedsiębiorstw sektora energetycznego, które w ten sposób są w stanie utworzyć wspólną platformę zajmującą się problemami i wyzwaniami specyficznymi dla tej branży.

IV. Podsumowanie

Zagrożenia związane z cyberprzestępczością są realnym wyzwaniem dla podmiotów z sektora energetycznego. Ich skutki mogą oddziaływać na wszystkie sfery funkcjonowania społeczeństwa, a także mieć dalekosiężne konsekwencje polityczne, gospodarcze czy militarne. Postępująca informatyzacja wszystkich obszarów życia, która jest wspierana przez działania Unii Europejskiej, prowadzi do skokowego zwiększenia liczby zagrożeń. Jednocześnie samoregulacyjne działania przedsiębiorstw w zakresie cyberbezpieczeństwa nie zdały egzaminu ze względu na różny poziom i formy podejmowanych działań, które gwarantowały tylko częściową ochronę. Podobnie regulacje wprowadzane przez państwa członkowskie UE, które dodatkowo prowadziły do zakłóceń w funkcjonowaniu jednolitego rynku cyfrowego. Odpowiedzią na to miało być ujednolicenie ram cyberbezpieczeństwa wprowadzone dyrektywą NIS oraz powołanie aktem o cyberbezpieczeństwie unijnej agencji wspierającej państwa członkowskie w tej kwestii. O ile w tym drugim przypadku można uznać, że cel został zrealizowany, o tyle w pierwszym takiej konkluzji nie można sformułować. Potwierdzają to wnioski wyciągnięte z przeglądu dyrektywy, które nie pozostawiły wątpliwości, że potrzebne są dalsze reformy unijnego systemu cyberbezpieczeństwa. Ich częścią jest wniosek legislacyjny KE dotyczący uchwalenia dyrektywy NIS 2. Dokonując jego ogólnej oceny, trzeba docenić prawodawcę za wyciągnięcie owych wniosków z przeglądu, a także odniesienie się do ram strategicznych UE i ogólnej sytuacji w zakresie bezpieczeństwa, w tym dynamiki zmieniających się wyzwań związanych na przykład z pandemią COVID-19. Jednocześnie rozwiązania zawarte w dyrektywie NIS, które zrealizowały postawione przed nimi cele, takie jak powołanie zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), Sieci Współpracy czy obowiązków w zakresie zgłaszania incydentów zostały przez prawodawcę zachowane w projekcie nowych rozwiązań.

Uwagę zwraca fakt znacznego rozszerzenia liczby podmiotów mających podlegać nowym przepisom. Oprócz dodania nowych sektorów nastąpiło również poszerzenie zakresu grup objętych dyrektywą NIS. Z perspektywy energetyki jest to szczególnie widoczne ze względu na objęcie obowiązkami wszystkich podmiotów w cyklu wytwarzania i dystrybucji energii elektrycznej oraz uwzględnieniu szczególnych z perspektywy społecznej producentów ciepła systemowego. Biorąc pod uwagę kierunki rozwojowe energetyki, zwłaszcza elektromobilność, istotne znaczenie ma objęcie przepisami producentów i dystrybutorów wodoru. Wobec dynamicznego wzrostu tej gałęzi energetyki należy prognozować, że w niedługim czasie uzyska ona znacznie większe znaczenie niż ma obecnie, a tym samym pozostawienie jej poza regulacjami stwarzałoby istotną lukę w cyberbezpieczeństwie sektora energetycznego jako całości.

Ponadto należy zauważyć, że o ile prawodawca zdecydował o nienakładaniu obowiązków na małe i średnie przedsiębiorstwa, o tyle zachował możliwość wprowadzenia wyjątków od tej zasady. Biorąc pod uwagę konstrukcję sieci dostaw produktów i usług dla sektora energetycznego stwierdzić należy, że składa się ona w znacznej mierze z MŚP. Trzeba przyjąć, że bezpieczeństwo producentów czy dystrybutorów energii będzie zależało również od podmiotów, z którymi współpracują. Tym samym wprowadzenie takiego wyjątku należy uznać za dobre rozwiązanie.

Odnosząc się do zakresu przedmiotowego, należy stwierdzić, że jest on zarysowany bardzo szeroko i znacznie przekracza dotychczasowe obciążenia przewidziane w art. 14 dyrektywy NIS,

które wymagały wprowadzenia odpowiednich i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania różnymi rodzajami ryzyka, ale ich dobór pozostawiały obowiązanemu. Wydaje się że dokonanie przez prawodawcę takiego wyboru stanowi odpowiedź na zaobserwowane różnice w działaniu podmiotów obowiązanych w zależności od państwa członkowskiego. Trzeba to uznać za kompromis pomiędzy obecnie istniejącym rozwiązaniem, a tendencją do szczegółowego regulowania konkretnych wymogów w zakresie cyberbezpieczeństwa, które wobec dynamicznego charakteru tego zjawiska, nie są nieefektywne. Wydaje się, że próba innego podejścia prawodawcy do problemu może być skuteczna. Jednocześnie to rozwiązanie powinno być szczególnie uważnie przeanalizowane w trakcie pierwszego po wejściu w życie przeglądu dyrektywy.

Trzeba również odnotować zmiany procedury zgłaszania incydentów. Podział na trzy rodzaje raportów można uznać za bardzo udany, jednak obowiązek złożenia raportu końcowego w ciągu miesiąca od daty zaistnienia incydentu wydaje się być nadmiernie rygorystyczny. Trzeba zauważyć, że w przypadku dużych ataków lub takich, w których brały udział służby specjalne wrogich państw lub powiązani z nimi cyberprzestępcy ustalenie wiarygodnych przyczyn i sposobów ataku może trwać znacznie dłużej niż miesiąc. Dotychczasowa praktyka pokazuje, że takie działania mogą rozciągnąć się na kilka miesięcy i wymagają zaangażowania wielu służb, nierzadko z różnych państw. Tym samym obowiązek ten może być iluzoryczny, a składany raport będzie miał małą wartość poznawczą. Należy raczej postulować, aby był on składany w terminie uzgodnionym przez właściwy organ do spraw cyberbezpieczeństwa, który jest w stanie ocenić postęp prac nad badaniem incydentu.

W zakresie relacji projektu dyrektywy NIS 2 do unijnych sektorowych aktów prawnych prawodawca przyjął, że przepisów dyrektywy nie stosuje się tylko w przypadku, gdy skutki wymogów wynikających z przepisów sektorowych są co najmniej równoważne skutkom obowiązków przewidzianych w tej dyrektywie. Jeżeli taka sytuacja nie ma miejsca, zastosowanie będą miały rozwiązania dyrektywy NIS 2, w tym w kwestiach dotyczących nadzoru. Trzeba zauważyć, że jest to odmienne rozwiązanie od obecnie funkcjonującego, które opiera się pierwszeństwie rozwiązań sektorowych nad dyrektywą NIS (Rojszczak, 2019, s. 200). Rozwiązanie takie należy uznać za trafne, ponieważ zapewni ono minimalną harmonizację bezpieczeństwa. Jednocześnie wydaje się, że prawodawca będzie zmierzał do zastępowania regulacji sektorowych ogólną.

W odniesieniu do obowiązków nałożonych na państwa członkowskie można zauważyć rozbudowanie sieci dotyczącej wymiany informacji. Samo założenie polegające na wyodrębnieniu różnych ciał, które mają się dzielić informacjami jest trafne ze względu na inne cele, jakie są przed nimi stawiane. Obawę może budzić powielanie informacji, które prowadzi do ich nadmiaru. Jest to jednak zagadnienie o charakterze zarządczym a nie prawnym, dlatego należy mieć nadzieję, że funkcjonowanie sieci będzie od nich wolne.

Podsumowując analizę wniosku legislacyjnego zmierzającego do uchwalenia dyrektywy NIS 2, stwierdzić należy, że planowane rozwiązania podnoszą poziom bezpieczeństwa sektora energetycznego. Dzieje się tak z powodów objęcia jego regulacjami szerszej grupy podmiotów w ramach tego sektora, jak również podmiotów, które są dostawcami towarów i usług przez co mogą być wektorem ataku. Same obowiązki, choć rozbudowane i wielowarstwowe, nie mogą być uznane za nadmierne wobec istotności energetyki we współczesnym społeczeństwie. Dlatego też należy wspierać jak najszybsze prace w celu uchwalenia dyrektywy, a następnie transponowania jej do porządków krajowych.

Bibliografia

FireEye. (2020, 13 grudnia). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. FireEye. Pozyskano z: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html (20.04.2021).

Greser, J. (2019). Zadania państwa w zakresie cyberbezpieczeństwa a rozwójelektromobilności. W: K. Kokocińska, J. Kola (red.), *Prawne i ekonomiczne aspekty rozwoju elektromobilności*. Warszawa: C.H. Beck.

Greser, J. (2020). Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745. *internetowy Kwartalnik Antymonopolowy i Regulacyjny,* 2. https://doi.org/10.7172/2299-5749.IKAR.2.9.6

Hordeski, M. (2020). *Megatrends for Energy Efficiency and Renewable Energy*. Gistrup: River Publishers.

KE. (2020). *Cybersecurity – review of EU rules on the security of network and information systems*. Pozyskano z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive (20.04.2021).

Kozłowski, A. (2021, 10 marca). *USA: specjalny zespół zajmie się „chińskim hakiem dekady"*. CyberDeference24.pl. Pozyskano z: https://www.cyberdefence24.pl/usa-specjalny-zespol-zajmie-sie-chinskim-hakiem-dekady (20.04.2021).

Litwiński, P. (2017). Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału sprawiedliwości z 19.10.2016 w sprawie c-582/14 Patrick Breyer. *Europejski Przegląd Sądowy*, 5.

Łuczak, J. (2020). Zarządzanie bezpieczeństwem informacji i cyberbezpieczeństwo w ujęciu procesowym. W: C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*. Warszawa: Wolters Kluwer.

Marzec, E. (2020). Pojęcie ryzyka w regulacji cyberbezpieczeństwa. *Monitor Prawniczy*, 23.

Mueller, R. (2012). *Speeches.* RSA Cyber Security Conference San Francisco, March 1. Pozyskano z: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (20.04.2021).

Piątek, S. (2020). Obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa. *internetowy Kwartalnik Antymonopolowy i Regulacyjny*, 2. https://doi.org/10.7172/2299-5749.IKAR.2.9.2.

Rojszczak, M. (2019). Cyberbezpieczeństwo w łączności elektronicznej. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Rojszczak, M. (2020). Strategie ataków i obrony. W: C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*. Warszawa: Wolters Kluwer.

Świtała, K. (2020). Bezpieczeństwo sieci i usług w projekcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. *Monitor Prawniczy*, 23.

Szpor, G. (2020). Nowelizacja siatki pojęciowej cyberbezpieczeństwa. *Monitor Prawniczy,* 22.

Szpor, G., Gryszczyńska, A. i Czaplicki, K. (red.). (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz.* Warszawa: Wolters Kluwer.

Wojnarowski, K. (2019). Europejska klasyfikacja NUTS i jej znaczenie dla województwa mazowieckiego. *Mazowsze Studia Regionalne*, 28.

Żywicka, A. (2021). Uwarunkowania prawne bezpieczeństwa wyrobów medycznych. Certyfikacja wyrobów medycznych w świetle rozporządzenia Parlamentu Europejskiego i Rady 2017/745 UE. W: K. Kokocińska, J. Greser (red.), *Jakość w opiece medycznej. Teleporady, Internet Rzeczy, aplikacje śledzące, IP Boxy*. Warszawa: Wolter Kluwer (w druku).