Katarzyna Chałubińska-Jentkiewicz*
Monika Nowikowska**

Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2)

Streszczenie

14 grudnia 2022 roku ustawodawca unijny przyjął dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2). Celem NIS 2 było ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w poszczególnych państwach członkowskich oraz aktualizacja listy sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa. W artykule dokonano analizy podmiotów działających na rzecz zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2. W pierwszej części artykułu („Cybercecurity and Law" 2024, nr 1) omówiono podmioty kluczowe, krytyczne i ważne, rejestr nazw domen najwyższego poziomu oraz dostawców usług DNS. W części drugiej autorki analizują takie podmioty, jak: organy właściwe ds. cyberbezpieczeństwa, pojedynczy punkt kontaktowy, zespoły reagowania na incydenty komputerowe (CSIRT), sektorowe zespoły cyberbezpieczeństwa, właściwy organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie, Europejska Sieć Organizacji Łącznikowych do spraw Kryzysów Cyberbezpieczeństwa (EU-CyCLONe), Grupa Współpracy, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci ENISA.

Słowa kluczowe: cyberbezpieczeństwo, incydent, ENISA, podmioty kluczowe, podmioty ważne, EU-CyCLONe, CERT

* Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj, Wydział Prawa i Administracji, Akademia Sztuki Wojennej w Warszawie, e-mail: kasiachalubinska@gmail.com, ORCID:0000-0003-0188-5704.
** Dr Monika Nowikowska, Wydział Prawa i Administracji, Akademia Sztuki Wojennej w Warszawie, e-mail: monika.nowikowska@gmail.com, ORCID:0000-0001-5166-8375.

Wstęp

Ustawodawca unijny 14 grudnia 2022 roku przyjął dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zwaną dyrektywa NIS 2[1] i uchylającą dyrektywę (UE) 2016/1148[2]. Przegląd dyrektywy z 2016 roku pokazał, że stanowiła ona katalizator zmian w instytucjonalnym i regulacyjnym podejściu do cyberbezpieczeństwa w Unii oraz spowodowała znaczącą zmianę w sposobie myślenia. Utworzono dzięki niej zasady krajowe dotyczące bezpieczeństwa sieci i systemów informatycznych poprzez przyjęcie krajowych strategii w obszarze bezpieczeństwa sieci i systemów informatycznych. Dyrektywa 2016/1148 przyczyniła się także do współpracy w Unii dzięki ustanowieniu Grupy Współpracy oraz sieci krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego. Pomimo tych osiągnięć przegląd dyrektywy 2016/1148 ujawnił w niej istotne braki, które uniemożliwiają skuteczne zaradzenie obecnym i mogącym wystąpić wyzwaniom w zakresie cyberbezpieczeństwa. To spowodowało konieczność uchwalenia i przyjęcia nowej dyrektywy. Analiza przepisów dyrektywy NIS 2 pozwala na wyróżnienie nowych kategorii podmiotów zaangażowanych w zapewnienie wysokiego poziomu cyberbezpieczeństwa. W artykule opublikowanym w „Cybersecurity and Law" 2024, nr 1 zostały omówione podmioty kluczowe, ważne i krytyczne oraz rejestry nazw domen. W niniejszym artykule autorki dokonały analizy kolejnych podmiotów systemu zapewnienia bezpieczeństwa sieci i systemów informatycznych na podstawie dyrektywy NIS 2. Należą do nich: właściwy organ ds. cyberbezpieczeństwa, pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa, organ ds. zarządzania kryzysowego w cyberbezpieczeństwie, EU-CyCLONe, zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), sektorowy zespół ds. cyberbezpieczeństwa, ENISA oraz Grupa Współpracy.

1 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz. Urz. UE 2022, L 333/80.
2 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS), ibidem 2016, L 194/1.

Organy właściwe ds. cyberbezpieczeństwa

Artykuł 8 ust. 1 dyrektywy NIS 2 stanowi, że każde państwo członkowskie jest zobowiązane do wyznaczenia co najmniej jednego właściwego organu odpowiedzialnego za cyberbezpieczeństwo oraz za zadania nadzorcze, które zostały określone w rozdziale VII rzeczonej dyrektywy. W ustawie o krajowym systemie cyberbezpieczeństwa (u.k.s.c)[3], wdrażającej NIS 2016/1148, został określony katalog podmiotów – organów właściwych w sprawach bezpieczeństwa sieci i systemów teleinformatycznych dla sektorów i usług. Podmioty te stanowią ministrowie, którzy kierują określonymi działami administracji rządowej[4]. Przykładowo, dla sektora energii jako organ właściwy został wskazany minister właściwy do spraw energii. W art. 41 u.k.s.c. wskazanych zostało 11 organów właściwych[5]. W NIS 2 stwierdzono, że właściwe organy monitorują wdrażanie niniejszej dyrektywy w kraju. Dodatkowo polski ustawodawca poświęcił w u.k.s.c. rozdział 9 pt. „Zadania ministra właściwego do spraw informatyzacji". Jest on odpowiedzialny m.in. za monitorowanie wdrażania „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej", prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń w celu pogłębiania wiedzy i budowania świadomości

3 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz. U. 2023, poz. 913 (dalej: u.k.s.c.).

4 J. Kostrubiec, *Katalog organów właściwych do spraw cyberbezpieczeństwa* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022, s. 207–208.

5 1) dla sektora energii – minister właściwy do spraw energii 2) dla sektora transportu, z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu; 3) dla podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej; 4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego; 5) dla sektora ochrony zdrowia, z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 - minister właściwy do spraw zdrowia; 6) dla sektora ochrony zdrowia obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej; 7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej; 8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw informatyzacji; 9) dla sektora infrastruktury cyfrowej obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej; 10) dla dostawców usług cyfrowych, z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw informatyzacji; 11) dla dostawców usług cyfrowych obejmujących podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej.

z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z internetu przez różne kategorie użytkowników[6].

Podsumowując powyższe, właściwe organy ds. cyberbezpieczeństwa są odpowiedzialne za cyberbezpieczeństwo w danym sektorze oraz wykonują zadania nadzorcze w celu zapewnienia sprawnego funkcjonowania systemu cyberbezpieczeństwa państwa.

Pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa

Pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa został utworzony zgodnie z dyrektywą NIS 2016/1148. Organy państw członkowskich, żeby były w stanie skutecznie współpracować z podmiotami gospodarczymi, muszą mieć odpowiednią strukturę. Stąd w dyrektywie NIS wyróżniono pojedyncze punkty kontaktowe oraz zespoły reagowania na incydenty bezpieczeństwa komputerowego (zwane CSIRT-ami).

Pojedyncze punkty kontaktowe nie powinny bezpośrednio odbierać żadnych zgłoszeń incydentów. Zadanie to należy do CSIRT-ów. Wyznaczony punkt kontaktowy był zobowiązany do przekazywania zgłoszeń incydentów pojedynczym punktom kontaktowym innych państw członkowskich, których incydent może dotyczyć. Żeby zapewnić efektywne przekazywanie informacji państwom członkowskim i Komisji, pojedynczy punkt kontaktowy powinien przedkładać grupie współpracy sprawozdania podsumowujące, które powinny być zanonimizowane w celu zachowania poufności zgłoszeń oraz tożsamości operatorów usług kluczowych i dostawców usług cyfrowych, ponieważ informacje dotyczące tożsamości zgłaszających podmiotów nie są wymagane do wymiany najlepszych praktyk w grupie współpracy[7].

W pkt 31 preambuły dyrektywy NIS 2016/1148 wskazano, że w celu ułatwienia współpracy i komunikacji transgranicznej każde państwo członkowskie

6 K. Chałubińska-Jentkiewicz, *Zadania ministra* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 284; M. Nowikowska, *Zadania i zakres odpowiedzialności ministra właściwego ds. informatyzacji* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec..., s. 222.

7 M. Nowikowska, *Cooperation Mechanisms to Ensure the Security of Network and Information Systems in the Light of the NIS Directive* [w:] *The Role of Cybersecurity in the Public Sphere – the European Dimension*, red. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022, s. 89.

jest zobowiązane utworzyć krajowy pojedynczy punkt kontaktowy odpowiedzialny za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracę transgraniczną na poziomie Unii. Właściwym organom i pojedynczym punktom kontaktowym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, żeby mogły skutecznie i efektywnie wykonywać powierzone im zadania i osiągnąć cele dyrektywy[8].

Pojedynczy punkt kontaktowy miał w swym zamierzeniu służyć komunikacji w ramach współpracy w Unii Europejskiej. Wymiana informacji pomiędzy państwami członkowskimi UE służy realizacji celów dyrektywy NIS w zakresie osiągnięcia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w UE. W polskiej ustawie o krajowym systemie cyberbezpieczeństwa pojedynczy punkt kontaktowy przekazuje, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej. Jest on zobowiązany także do odbierania zgłoszeń incydentu poważnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a następnie przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowych zespołów cyberbezpieczeństwa[9].

Wprowadzając dyrektywę NIS 2016/1148, ustawodawca polski przyjął, że minister do spraw informatyzacji, który pełni funkcję pojedynczego punktu kontaktowego, odpowiada za odbiór i przekazywanie, na wniosek właściwych CSIRT, zgłoszeń incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej. Ponadto odpowiada za zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy, wymianę informacji na rzecz organów władz publicznych, organów właściwych w Polsce i za granicą, CSIRT, realizację obowiązków sprawozdawczych wobec Grupy Współpracy i Komisji Europejskiej.

Do głównych zadań punktu kontaktowego należy: 1) odbieranie zgłoszeń incydentów z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowych zespołów

8 M. Nowikowska, *Pojedynczy punkt kontaktowy* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec..., s. 222.
9 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, s. 296.

cyberbezpieczeństwa – czyli pozyskiwanie i przekazywanie informacji o zaistniałej sytuacji zagrożenia od innych punktów kontaktowych w UE, jeżeli sytuacja tam ma charakter szerszy, dotyczący więcej niż jednego państwa; 2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej – czyli pozyskiwanie i przekazywanie informacji o takich incydentach do innych punktów kontaktowych, których incydent dotyczy; 3) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy – czyli pełnienie funkcji reprezentacyjnej; 4) zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa – czyli realizowanie polityki współpracy z UE w zakresie cyberbezpieczeństwa; 5) koordynacja współpracy między organami właściwymi do spraw cyberbezpieczeństwa i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej – czyli koordynacja współpracy państwa z innymi państwami UE w sprawach cyberbezpieczeństwa; 6) zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz sieci CSIRT – czyli współpraca informacyjna[10].

W dyrektywie NIS 2 funkcjonowanie pojedynczego punktu kontaktowego pozostało w niezmienionej strukturze. Każde państwo członkowskie zostało zobowiązane do wyznaczenia pojedynczego punktu kontaktowego. Pełni on funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów swojego państwa z odpowiednimi organami w innych państwach członkowskich oraz z Komisją i ENISA, a także w celu zapewnienia międzysektorowej współpracy z innymi właściwymi organami krajowymi w swoim państwie. Państwa członkowskie zostały zobowiązane do zapewnienia pojedynczym punktom kontaktowym odpowiednich zasobów, żeby mogły one efektywnie i skutecznie wykonywać powierzone im zadania i tym samym realizować cele niniejszej dyrektywy. Ponadto państwo członkowskie zostało zobowiązane do przekazania Komisji danych identyfikacyjnych pojedynczego punktu kontaktowego.

10 M. Nowikowska, *Pojedynczy punkt kontaktowy…*, s. 230; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność…*, s. 296–297.

Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego

Funkcję Narodowego Punktu Kontaktowego od 28 sierpnia 2018 roku pełni Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni. Ustawodawca w art. 52 u.k.s.c. nałożył na Ministra Obrony Narodowej obowiązek prowadzenia Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego. Obowiązek ten stanowił podstawę prawną do zorganizowania, wyposażenia w odpowiednie środki materialne oraz technologiczne jednostki organizacyjnej, a także zapewnienia wysoko wykwalifikowanej kadry. W art. 52 u.k.s.c. wskazano przykładowe obowiązki Narodowego Punktu Kontaktowego: 1) zapewnienie współpracy w obszarze obrony narodowej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego w zakresie cyberbezpieczeństwa; 2) koordynacja działań na rzecz wzmacniania zdolności obronnych w razie zagrożenia cyberbezpieczeństwa; 3) zapewnienie współpracy między narodowymi i sojuszniczymi siłami zbrojnymi w zapewnieniu cyberbezpieczeństwa; 4) rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej; 5) udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii[11].

Z analizy przepisu art. 52 u.k.s.c. wynika, że Narodowy Punkt Kontaktowy jest jednostką organizacyjną działającą w Ministerstwie Obrony Narodowej („Minister prowadzi"). Zgodnie z decyzją Ministra Obrony Narodowej z 28 sierpnia 2018 roku zmieniającą decyzję w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej[12] funkcję Narodowego Punktu Kontaktowego pełni Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni. Zadania dotyczące współpracy z Organizacją Traktatu Północnoatlantyckiego wynikały już wcześniej z decyzji Ministra Obrony Narodowej z 13 lipca 2015 roku w sprawie organizacji

11 K. Wąsowski, *Prowadzenie Narodowego Punktu Kontaktowego* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, K. Chałubińska-Jentkiewicz, F. Radoniewicz, Warszawa 2019, s. 291; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, nr 1 s. 46; T. Zdzikot, *Narodowy Punkt Kontaktowy* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec..., s. 247.

12 Decyzja Nr 108/MON Ministra Obrony Narodowej z dnia 28.08.2018 r. zmieniającą decyzję w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej, Dz. Urz. MON 2018, poz. 125.

i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej[13]. Zgodnie z pkt 5 ppkt 2 lit. f Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej, którego funkcję pełni właściwa komórka wewnętrzna Służby Kontrwywiadu Wojskowego, ma obowiązek współpracy przy ustalaniu formalno-prawnych zasad funkcjonowania systemu reagowania na incydenty komputerowe oraz planów jego rozwoju w wymiarze krajowym i międzynarodowym, m.in. z Centrum Koordynacyjnym Systemu Reagowania na Incydenty Komputerowe Organizacji Traktatu Północnoatlantyckiego[14]. Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego na mocy art. 52 u.k.s.c został utworzony przez Ministra Obrony Narodowej do zagwarantowania współpracy w obszarze obrony narodowej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego w zakresie cyberbezpieczeństwa, koordynacji działań, zapewnienia współpracy między narodowymi i sojuszniczymi siłami zbrojnymi na rzecz cyberbezpieczeństwa oraz rozwijania systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej.

Właściwy organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie

W art. 9 dyrektywy NIS ustawodawca ustanowił nowy podmiot – „właściwy organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie". Każde państwo członkowskie zostało zobowiązane do wyznaczenia co najmniej jednego właściwego organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę (organy ds. zarządzania kryzysowego w cyberbezpieczeństwie). W ust. 2 wskazano, że jeżeli państwo członkowskie wyznaczy lub ustanowi więcej niż jeden organ ds. zarządzania kryzysowego w cyberbezpieczeństwie,

13 Decyzja Nr 275/MON Ministra Obrony Narodowej z 13 lipca 2015 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej, Dz. Urz. MON 2015, poz. 208.

14 A. Besiekierska [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. eadem, Warszawa 2019.

to jest zobowiązane jednoznacznie wskazać, który z tych organów ma pełnić funkcję koordynatora. Ponadto każde państwo członkowskie jest zobowiązane przekazać Komisji dane indentyfikacyjne swojego organu.

Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa

W motywie 68 NIS 2 podkreślono, że państwa członkowskie powinny wnosić wkład w ustanowienie unijnych zasad reagowania w sytuacji kryzysu cybernetycznego poprzez istniejące sieci współpracy, w szczególności Europejską Sieć Organizacji Łącznikowych do spraw Kryzysów Cyberbezpieczeństwa (EU-CyCLONe), sieć CSIRT i Grupę Współpracy. EU-CyCLONe i sieć CSIRT powinny współpracować na podstawie uzgodnień proceduralnych, które określają szczegóły tej współpracy, i unikać powielania zadań.

U-CyCLONe ma pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii. EU-CyCLONe składa się z przedstawicieli organów państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie, a jeżeli potencjalny lub trwający incydent w cyberbezpieczeństwie na dużą skalę ma lub może mieć znaczny wpływ na usługi i działania objęte NIS 2, to także Komisji. W pozostałych przypadkach Komisja uczestniczy w działaniach EU-CyCLONe jako obserwator. Obsługę sekretariatu EU-CyCLONe zapewnia ENISA, która pomaga w bezpiecznej wymianie informacji, a także dostarcza podstawowe narzędzia do wsparcia współpracy między państwami członkowskimi przez zapewnienie bezpiecznej wymiany informacji.

Do zdań EU-CyCLONe należy: podnoszenie poziomu gotowości do zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę, rozwijanie wspólnej świadomości sytuacyjnej pod kątem incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę, ocena konsekwencji i wpływu istotnych incydentów oraz proponowanie możliwych środków ograniczających ryzyko, koordynowanie zarządzania incydentami oraz wspieranie procesu decyzyjnego na szczeblu politycznym w odniesieniu do takich incydentów i sytuacji kryzysowych.

EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania z zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na

dużą skalę, a także z tendencji w tej dziedzinie, koncentrując się zwłaszcza na ich wpływie na podmioty kluczowe i ważne.

Reasumując, EU-CyCLONe powinna pośredniczyć między poziomem technicznym i politycznym podczas incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę oraz zacieśnić współpracę na szczeblu operacyjnym i wspierać proces decyzyjny na szczeblu politycznym. Podstawą współpracy EU-CyCLONe z Komisją powinny być ustalenia sieci CSIRT i własne zdolności do sporządzania analizy skutków incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę.

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w sposób szczegółowy regulowała dyrektywa NIS 2016/1148. Postanowienia te zostały powtórzone w NIS 2. W motywie 44 wskazano, że państwa członkowskie powinny być odpowiednio wyposażone zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, żeby zapobiegać incydentom i ryzyku, wykrywać je, reagować na nie i przywracać normalne działanie po ich wystąpieniu oraz łagodzić ich skutki. Państwa członkowskie powinny ustanowić lub wyznaczyć co najmniej jeden CSIRT oraz zapewnić im odpowiednie zasoby i możliwości techniczne. Zadaniem CSIRT jest obsługa incydentów. Obejmuje ona przetwarzanie dużych ilości danych, w niektórych przypadkach danych szczególnie chronionych. Państwa członkowskie powinny zapewnić CSIRT infrastrukturę służącą do wymiany i przetwarzania informacji, a także kompetentną kadrę, co zapewni poufność i wiarygodność ich operacji.

Ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła CSIRT GOV, CSIRT MON oraz CSIRT NASK.

CSIRT GOV

CSIRT GOV – Rządowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działa od stycznia 2008 roku w Agencji Bezpieczeństwa Wewnętrznego (jako CERT.GOV.PL). Jego zadaniem jest koordynacja obsługi incydentów zgłaszanych przez podmioty wskazane w art. 26 ust. 7 ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, tj.:

administrację rządową, Narodowy Bank Polski, Bank Gospodarstwa Krajowego. Ponadto odpowiada za rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemów i sieci teleinformatycznych wchodzących w skład infrastruktury krytycznej. CSIRT GOV jest zawsze – tj. bez względu na kategorię zgłaszającego podmiotu – właściwy w przypadku incydentów o charakterze terrorystycznym

CSIRT MON

Działający w Systemie Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej CSIRT MON odpowiada za koordynację procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych resortu obrony narodowej. Koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne wchodzą w skład infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z 26 kwietnia 2007 roku o zarządzaniu kryzysowym[15], oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym[16]. W razie incydentów związanych z obronnością kraju zawsze właściwy jest CSIRT MON.

CSIRT NASK

Naukowa i Akademicka Sieć Komputerowa (NASK) powstała w 1993 roku jako państwowy instytut badawczy prowadzący działalność naukową, krajowy rejestr domen „.pl" i dostarczający zaawansowane usługi teleinformatyczne. W jego ramach od 1996 roku działa CERT POLSKA koordynujący – obecnie jako CSIRT NASK – obsługę incydentów naruszających bezpieczeństwo sieci „sfery cywilnej", mających miejsce w sieciach publicznych, czyli zgłaszane przez pozostałe podmioty (tj. niekwalifikujące się do grup wskazanych wyżej),

15 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, t.j., Dz. U. 2023, poz. 122.
16 C. Banasiński, W. Nowak, *Europejski i krajowy system cyberbezpieczeństwa* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018 s. 161–162; M. Nowikowska *Zadania CSIRT MON, CSIRT NASK i CSIRT GOV* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz..., s. 191.

np. samorządu terytorialnego. CSIRT NASK obejmuje swoją właściwością wszystkie incydenty zgłaszane przez podmioty, które nie są we właściwości CSIRT GOV i CSIRT MON. Podmiot ten jest określany jako CERT ostatniej szansy (*CERT of last resort*), gdyż każda osoba fizyczna i każda jednostka organizacyjna (bez względu na obywatelstwo lub jego brak czy siedzibę), dla których nie są właściwe pozostałe CSIRT-y, może zgłosić do niego incydent. Ponadto, jeżeli jakiś podmiot nie jest w stanie uzyskać bezpośredniego kontaktu lub oczekiwanej pomocy od podmiotu, który jest zaangażowany w incydent bezpośrednio, to zgłaszający przekazuje zapytanie właśnie do CSIRT ostatniej szansy[17].

Sektorowy zespół cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa z 2018 roku wprowadziła pojęcie „sektorowy zespół cyberbezpieczeństwa". Artykuł 44 stanowi, że może być on powołany przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku do ustawy. Powołanie sektorowego zespołu cyberbezpieczeństwa może być wsparciem zarówno dla operatorów usług kluczowych w danym sektorze, właściwego CSIRT, jak i organów właściwych.

Do zalet sektorowych zespołów cyberbezpieczeństwa zalicza się duże zrozumienie specyfiki danego sektora, potrzeb i wyzwań stojących przed operatorami usług kluczowych; wiedzę o możliwych ryzykach, występujących incydentach i sposobach ich skutecznej obsługi. Sektorowe zespoły tworzą tzw. platformy wymiany dobrych praktyk i budowania zdolności reagowania na zagrożenia w sektorze, gromadzą wiedzę na temat sektora nie tylko ze źródeł krajowych, lecz także zagranicznych.

W ogólnym dyskursie sektorowy zespół cyberbezpieczeństwa jest utożsamiany z sektorowym CERT lub CSIRT. Wypełnianie obowiązków ustawowych spoczywa na operatorach usług kluczowych jako głównych zobowiązanych do stosowania ustawy, zespołach CSIRT zapewniających obsługę techniczną incydentu oraz na organach właściwych, które zajmują się stroną administracyjną i nadzorczą krajowego systemu cyberbezpieczeństwa.

17 C. Banasiński, W. Nowak, op. cit., s. 161–162; M. Nowikowska, *Zadania CIRT MON…*, s. 192.

Uzupełnieniem tego systemu od strony technicznej są sektorowe zespoły cyberbezpieczeństwa, które mogą tworzyć organy właściwe we właściwych dla siebie sektorach[18].

Ustawodawca na podstawie art. 44 u.k.s.c. ustanowił możliwość tworzenia dodatkowych zespołów o charakterze specjalistycznym, wyspecjalizowanym dla danej usługi kluczowej. Zespoły te zostały umiejscowione w krajowym systemie cyberbezpieczeństwa. Określono ich minimalny zakres zadań oraz uprawnienia, nie wskazano jednak żadnego zespołu z nazwy ani nie określono formy, w jakiej mają działać. Tworzenie sektorowych zespołów cyberbezpieczeństwa jest uzasadnione ich specyfiką, a tym samym koniecznością współpracy i koordynacją podejmowanych działań. Katalog określonych zadań zespołu nie ma charakteru zamkniętego, ponieważ ustawodawca użył określenia „w szczególności"[19].

Sektorowy zespół cyberbezpieczeństwa jest odpowiedzialny za przyjmowanie zgłoszeń o incydentach wraz z właściwym zespołem CSIRT) oraz wspieranie operatorów usług kluczowych (OUK) w danym sektorze podczas wykonywania ich obowiązków. Sektorowe zespoły pełnią uzupełniającą funkcję względem CSIRT. Mają one wspierać zespół CSIRT swoją wiedzą i zadaniami oraz uprawnieniami sektorowymi, a nie go zastępować.

Do katalogu zadań sektorowych zespołów cyberbezpieczeństwa zalicza się: 1) przyjmowanie zgłoszeń o incydentach poważnych od operatorów; 2) wsparcie OUK w obsłudze incydentów poważnych i współpracę z zespołami CSIRT w koordynowaniu obsługi incydentów poważnych; 3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu; 4) wspieranie OUK m.in. we wdrażaniu systemu zarządzania bezpieczeństwem, w wyznaczaniu osób kontaktowych, zapewnianiu użytkownikom dostępu do wiedzy[20].

Sektorowym zespołem cyberbezpieczeństwa jest m.in. zespół CSIRT KNF. Został utworzony przez KNF w celu koordynacji działań i wsparcia obsługi incydentów bezpieczeństwa w podmiotach rynku finansowego uznanych za

18 Eadem, *The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland* [w:] *Cybersecurity in Poland Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022, s. 225.

19 J. Kostrubiec, *Sektorowy zespół cyberbezpieczeństwa* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec..., s. 219.

20 *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska…

operatorów usług kluczowych w rozumieniu u.k.s.c. Wspiera on OUK w obsłudze incydentów poważnych występujących w tych podmiotach a także prowadzi działania mające na celu analizę pozostałych incydentów, trendów i zagrożeń w obszarze cyberbezpieczeństwa.

Podsumowując, sektorowy zespół cyberbezpieczeństwa jest tworzony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora w celu wsparcia zarówno operatorów usług kluczowych w danym sektorze, właściwego CSIRT, jak i organów właściwych. Zespół sektorowy wspiera operatorów usług kluczowych w obsłudze incydentów poważnych występujących w tych podmiotach, a także prowadzi działania mające za zadanie analizę pozostałych incydentów, tendencji i zagrożeń w obszarze cyberbezpieczeństwa.

W NIS 2 pozostawiono instytucję sektorowych zespołów bezpieczeństwa. W art. 10 ust. 4 wskazano, że CSIRT-y współpracują z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje.

Grupa Współpracy

Grupa Współpracy została ustanowiona na podstawie dyrektywy NIS. W celu skutecznego reagowania na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów informatycznych w cyberprzestrzeni ustawodawca unijny wskazał konieczność budowy wspólnego, kompleksowego podejścia obejmującego m.in. wymianę informacji oraz współpracę pomiędzy państwami członkowskimi. W rzeczonej dyrektywie wyodrębniono zasady współpracy technicznej oraz polityczno-strategicznej.

Współpraca polityczno-strategiczna ma być realizowana przez Grupę Współpracy (Cooperation Group), której głównym zadaniem miało być wypracowanie wspólnych koncepcji strategicznych oraz przyjmowanie rocznych raportów od właściwych organów. Współpracę techniczną ma zapewniać europejska sieć CISRT (CSIRT network) oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych pomiędzy CSIRT-ami wyznaczonymi dla operatorów usług kluczowych oraz dostawcami usług cyfrowych[21].

21 M. Nowikowska, *Cooperation Mechanisms…*, s. 88–89.

W celu propagowania zaawansowanych systemów bezpieczeństwa sieci i systemów informatycznych Grupa Współpracy jest zobowiązana współpracować z odpowiednimi instytucjami, organami, urzędami i agencjami Unii, żeby wymieniać się wiedzą i najlepszymi praktykami oraz doradzać w sprawie bezpieczeństwa sieci i systemów informatycznych, które mogłyby mieć wpływ na ich pracę, i jednocześnie przestrzegać istniejących ustaleń dotyczących wymiany informacji zastrzeżonych. Współpracując z organami ścigania w kwestiach dotyczących bezpieczeństwa sieci i systemów informatycznych, które mogłyby mieć wpływ na jej pracę, Grupa Współpracy jest zobowiązana uwzględniać istniejące kanały informacji i ustanowione sieci[22]. Żeby Grupa Współpracy mogła wykonać powierzone jej zadania, pojedyncze punkty kontaktowe muszą przekazywać jej określone informacje. Najważniejszym elementem w działaniach związanych z zapewnieniem cyberbezpieczeństwa jest polityka informacyjna.

W NIS 2 powtórzono, że Grupa Współpracy ma wspierać i ułatwiać strategiczną współpracy i wymianę informacji między państwami członkowskimi. Zadania wykonuje na podstawie dwuletnich programów prac. Grupę Współpracy tworzą przedstawiciele państw członkowskich, Komisji i ENISA. W jej pracach uczestniczy w charakterze obserwatora Europejska Służba Działań Zewnętrznych. Grupa Współpracy jest miejscem wymiany najlepszych praktyk, dyskusji na temat zdolności i gotowości państw członkowskich. Zadaniem Grupy Współpracy jest także pomoc państwom członkowskim w ocenie krajowych strategii bezpieczeństwa sieci i systemów informatycznych, w budowaniu potencjału i ocenie ćwiczeń z bezpieczeństwa sieci i systemów informatycznych.

Agencja Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji

Agencja Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA) została utworzona w 2004 roku na podstawie rozporządzenia Parlamentu Europejskiego i Rady z 10 marca 2004 roku[23] w celu zapewnienia jak najwyższego

22 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*..., s. 298.

23 Rozporządzenie (WE) Nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. w celu zapewnienia jak najwyższego poziomu bezpieczeństwa w cyberprzestrzeni, Dz. Urz. UE 2004, L 77/1.

poziomu bezpieczeństwa w cyberprzestrzeni[24]. W 2013 roku rzeczone rozporządzenie zostało zastąpione przez rozporządzenie Parlamentu Europejskiego i Rady z 21 maja 2013 roku[25].

Obecne podstawy prawne jej działalności określa rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 roku[26].

Artykuł 3 ust. 1 aktu o cyberbezpieczeństwie stanowi, że ENISA wykonuje powierzone jej zadania w celu osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aktywnego wspierania państw członkowskich, instytucji, organów i jednostek organizacyjnych Unii w poprawie cyberbezpieczeństwa, zapewnienia fachowej wiedzy i doradztwa z zakresu cyberbezpieczeństwa. Artykuł 4 ust. 1 aktu o cyberbezpieczeństwie wskazuje, że ENISA powinna stanowi ośrodek wiedzy fachowej w dziedzinie cyberbezpieczeństwa z racji swojej niezależności, naukowo-technicznej jakości oferowanego doradztwa i pomocy, przekazywanych informacji, przejrzystości procedur działania, metod działania oraz staranności w wykonywaniu zadań. Zgodnie z art. 7 ust. 1 aktu o cyberbezpieczeństwie ENISA powinna wspierać współpracę operacyjną pomiędzy państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz interesariuszami.

Strukturę administracyjną i kierowniczą ENISA, zgodnie z art. 13 aktu o cyberbezpieczeństwie, tworzą: Zarząd, Rada Wykonawcza, Dyrektor Wykonawczy, Grupa Doradcza ENISA, Sieć Krajowych Urzędów Łącznikowych. W skład Zarządu wchodzi po jednym członku powoływanym przez każde z państw członkowskich oraz dwóch członków powoływanych przez Komisję Europejską. Prawo głosu przysługuje wszystkim członkom Zarządu. Rada Wykonawcza liczy pięciu członków powoływanych spośród członków Zarządu. W skład Rady Wykonawczej musi wchodzić przewodniczący Zarządu, który może również przewodniczyć Radzie Wykonawczej, oraz jeden przedstawiciel

24 C. Banasiński, W. Nowak, op. cit., s. 150, 161–162; M. Nowikowska, *CSIRT GOV* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz..., s. 210; B. Kuś, *Cel krajowego systemu cyberbezpieczeństwa* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec..., s. 20.

25 Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004, Dz. Urz. UE 2013, L 165.

26 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), ibidem 2019, L 151/15.

Komisji Europejskiej. Powołania członków Rady Wykonawczej mają na celu zapewnienie równowagi płci w Radzie Wykonawczej. Dyrektor Wykonawczy bierze udział w posiedzeniach Rady Wykonawczej, ale nie przysługuje mu prawo głosu. ENISA kieruje Dyrektor Wykonawczy, który zachowuje niezależność podczas wykonywania swoich obowiązków. Dyrektor Wykonawczy odpowiada przed Zarządem. Zarząd, działając na wniosek Dyrektora Wykonawczego, ustanawia w przejrzysty sposób Grupę Doradczą ENISA składającą się z uznanych ekspertów reprezentujących odpowiednich interesariuszy. Sieć Krajowych Urzędników Łącznikowych pełni funkcję punktu kontaktowego na poziomie krajowym, żeby ułatwiać współpracę ENISA z ekspertami krajowymi w realizacji rocznego programu prac ENISA. Siedzibą ENISA są Ateny.

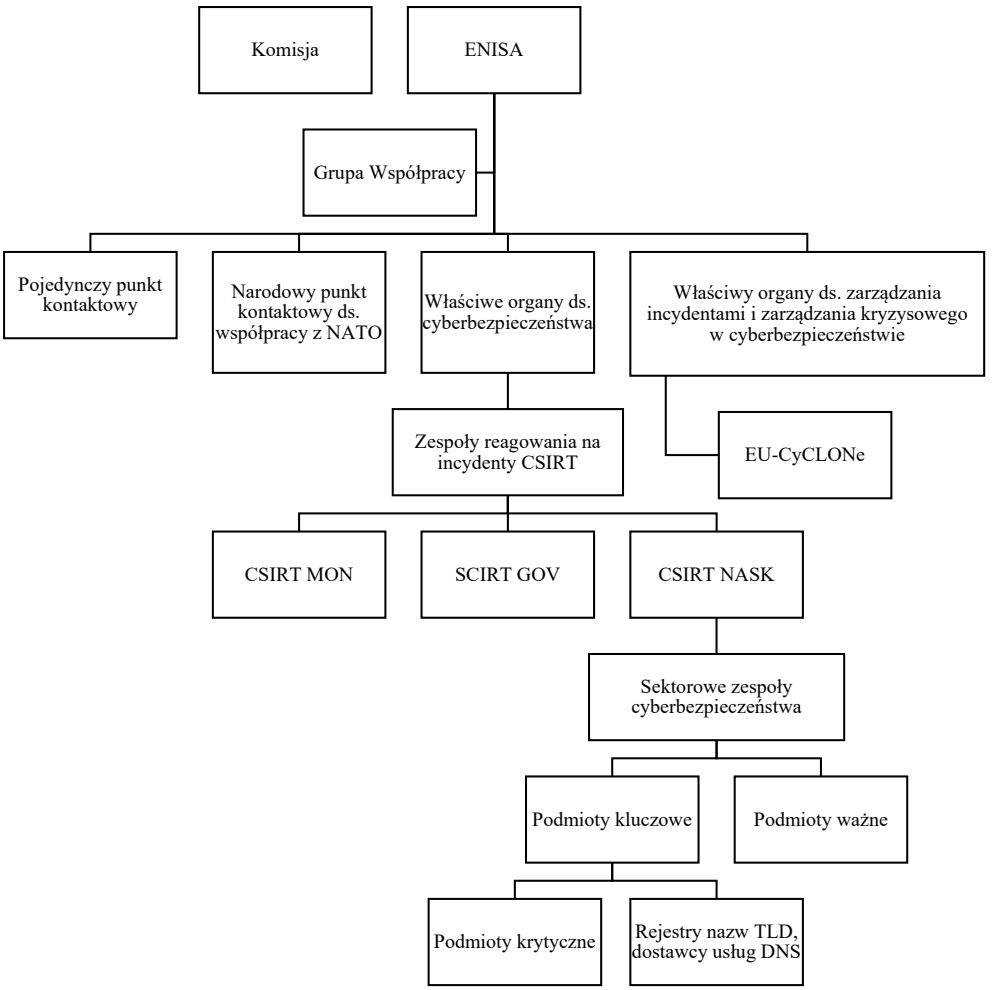
Zakończenie

Jedną z głównych przyczyn uzasadniających konieczność przyjęcia NIS 2 – modyfikującej w sposób istotny dotychczasowe rozwiązania – były różne w poszczególnych państwach członkowskich uregulowania obowiązków podmiotów świadczących usługi lub prowadzących działalność kluczową. Wymogi dotyczące cyberbezpieczeństwa nałożone na te podmioty różniły się znacznie zarówno rodzajem i poziomem szczegółowości, jak i metodami nadzoru.. Rozbieżności te pociągały za sobą dodatkowe koszty i powodowały trudności dla podmiotów, które oferowały towary lub usługi transgraniczne[27].

Analiza podmiotów zaangażowanych w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych na podstawie NIS 2 pozwala na zbudowanie schematu współpracy zaprezentowanego na schemacie poniżej.

Poprawa współpracy między wszystkimi podmiotami zaangażowanymi w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych była najważniejszym elementem stanowiącym podstawę projektowania nowych rozwiązań NIS 2. Zrozumienie ról i celów każdego podmiotu, ustanowienie otwartej komunikacji, ustalenie wspólnych obowiązków, zarządzanie ryzykiem oraz monitorowanie i ocena postępów to skuteczne sposoby poprawy współpracy. Dobra współpraca między wszystkimi podmiotami wymaga zaangażowania i wysiłku ze strony wszystkich państw członkowskich.

27 K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*..., s. 296; *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska...



Postanowienia dyrektywy NIS nakładają wiele nowych obowiązków na określone podmioty, w tym m.in. na organy administracji publicznej i wybranych przedsiębiorców, których zadaniem jest zapewnianie niezakłóconego świadczenia usług kluczowych oraz odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług. Podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa tworzą spójny system pozwalający na podejmowanie działań zarówno przeciwdziałających zagrożeniom, jak i zapewniających skuteczne reagowanie na incydenty cyberbezpieczeństwa.

Bibliografia

Banasiński C., Nowak W., *Europejski i krajowy system cyberbezpieczeństwa* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Besiekierska A. [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Chałubińska-Jentkiewicz K., *Zadania ministra* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, nr 1.

Kostrubiec J., *Katalog organów właściwych do spraw cyberbezpieczeństwa* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Kostrubiec J., *Sektorowy zespół cyberbezpieczeństwa*, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Kuś B., *Cel krajowego systemu cyberbezpieczeństwa* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Nowikowska M., *Cooperation Mechanisms to Ensure the Security of Network and Information Systems in the Light of the NIS Directive* [w:] *The Role of Cybersecurity in the Public Sphere – the European Dimension*, red. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022.

Nowikowska M., *CSIRT GOV* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Nowikowska M., *Pojedynczy punkt kontaktowy* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Nowikowska M., *The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland* [w:] *Cybersecurity in Poland Legal Aspects*, eds, K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022.

Nowikowska M., *Zadania CSIRT MON, CSIRT NASK i CSIRT GOV* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Nowikowska M., *Zadania i zakres odpowiedzialności ministra właściwego ds. informatyzacji* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Wąsowski K., *Prowadzenie Narodowego Punktu Kontaktowego* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, K. Chałubińska-Jentkiewicz, F. Radoniewicz, Warszawa 2019.

Zdzikot T., *Narodowy Punkt Kontaktowy* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Entities Involved in the Policy of Ensuring the Security of Network and IT Systems in the Light of the NIS 2 Directive

Abstract

On December 14, 2022, the EU legislator adopted a directive on measures for a high common level of cybersecurity in the territory of the Union, called the NIS 2 directive. The aim of the new NIS 2 directive was to establish mechanisms for effective cooperation between responsible authorities in the various Member States and to update the list of sectors and activities subject to cybersecurity obligations. The article reviews the entities involved in the policy of ensuring the security of network and IT systems in the light of the NIS 2 directive. In the 1st part of the article, published in „Cybercecurity and Law" 2024, no. 1. 11, the following entities are discussed: key entities, critical entities, registry of top-level domain names and DNS service providers, important entities. In part 2, the authors analyze entities such as the point of single contact, computer emergency response teams (CSIRTs), Cooperation Group, European Union Agency for Network Security.

Key words: ENISA, CSIRT, point of single contact, Cooperation Group. EU-CyCLONe