Dr Emilia Chronowska-Sioła
Uniwersytet Kazimierza Wielkiego w Bydgoszczy
ORCID: 000-0001-6996-5503
e-mail: emilia.chronowska@ukw.edu.pl

UNIJNA DYREKTYWA NIS 2 W OBSZARZE CYBERBEZPIECZEŃSTWA – ANALIZA PODMIOTÓW KLUCZOWYCH I PODMIOTÓW WAŻNYCH

Streszczenie

Urządzenia stacjonarne i mobilne z dostępem do Internetu stanowią podstawowe narzędzie wykorzystywane zarówno na użytek jednostki, jak również przedsiębiorstw i instytucji publicznych, stanowiąc podstawowe narzędzie pracy. Świadomość różnorodności cyberzagrożeń i konsekwencji, które ze sobą niosą stwarza potrzebę wprowadzenia regulacji o charakterze ponadnarodowym, ukierunkowanych na podniesienie poziomu cyberbezpieczeństwa i odporności systemów informatycznych. Celem artykułu jest analiza dyrektywy NIS 2 w zakresie podmiotów kluczowych i ważnych, na które unijny dokument nakłada określone obowiązki, a także ukazanie wynikających z niej pewnych wątpliwości dla ustawodawcy polskiego. Posłużono się metodą instytucjonalno-prawną oraz analizą literatury przedmiotu.

Słowa kluczowe: cyberbezpieczeństwo, dyrektywa NIS 2, podmioty kluczowe, podmioty ważne

WSTĘP

Rozwój technologiczny obejmujący niemalże wszystkie sfery ludzkiej działalności przyczynia się do wielu udogodnień i możliwości, ale również problemów oraz zagrożeń. Przybierające na sile cyberzagrożenia i rosnąca cyberprzestępczość stwarzają potrzebę zastosowania środków umożliwiających skuteczne przeciwdziałanie wspomnianym zjawiskom, a także minimalizowanie ich negatywnych konsekwencji. Cyberbezpieczeństwo, które w najbardziej ogólnym ujęciu można rozumieć jako ochronę sieci i systemów informatycznych, a także ich użytkowników i podmiotów

narażonych na cyberzagrożenia, wymaga wprowadzenia regulacji kluczowych z perspektywy omawianej tematyki. Dążenie Unii Europejskiej do promowania cyberodporności, budowy otwartej i bezpiecznej cyberprzestrzeni, a także wiarygodnych narzędzi i usług cyfrowych ma odzwierciedlenie w sferze ustawodawczej w postaci opracowania i przyjęcia dokumentów podejmujących kwestię cyberbezpieczeństwa.

Polityka cyberbezpieczeństwa Unii Europejskiej i jej charakter na przestrzeni lat ulegał zmianom z uwagi na ewolucję katalogu współczesnych zagrożeń. Aktywność Unii Europejskiej we wspomnianym obszarze przestała koncentrować się głównie na aspektach gospodarczych czy ekonomicznych i objęła również sferę obronności. Spośród najistotniejszych elementów polityki cyberbezpieczeństwa Unii Europejskiej stanowiącej zbiór strategii, regulacji i inicjatyw ukierunkowanych na zwiększenie odporności Europy na cyberzagrożenia oraz zapewnienie bezpiecznego i chronionego środowiska cyfrowego, należy wymienić: ENISA będącą Agencją Unii Europejskiej ds. Cyberbezpieczeństwa ustanowioną w 2005 roku, unijną strategię bezpieczeństwa przedstawioną w grudniu 2020 r. przez Komisję Europejską i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, dyrektywę 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 oraz najnowszą dyrektywę 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, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 zwaną dyrektywą NIS 2 i przekształcającą dotychczasowe ramy cyberbezpieczeństwa w UE. Przedmiotem niniejszego artykułu jest zakres podmiotowy dyrektywy NIS 2.

CYBERPRZESTRZEŃ I CYBERBEZPIECZEŃSTWO – UJĘCIE TEORETYCZNE

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[1], czyli dyrektywa NIS 2, wprowadza istotne regulacje mające na celu podniesienie poziomu cyberbezpieczeństwa, do których państwa członkowskie musiały dostosować ustawodawstwo wewnętrzne w czasie 21 miesięcy od wejścia w życie unijnego dokumentu, czyli do 18 października 2024 roku. Rozważania nad znaczeniem wprowadzonych na mocy wspomnianej dyrektywy zmian warto poprzedzić przedstawieniem teoretycznego ujęcia cyberprzestrzeni i cyberbezpieczeństwa.

Rozpowszechniająca się globalizacja środowiska cyfrowego i cyfryzacja systemów teleinformatycznych przyczyniła się do przeniesienia wielu sfer życia do przestrzeni Internetu, co skutkuje powszechnym przetwarzaniem różnego rodzaju danych. Intensywnie rozwijająca się komputeryzacja, cyfryzacja i telekomunikacja sprawiły, że korzystanie z Internetu, komputerów i innych urządzeń mobilnych jest już stałym elementem ludzkiej codzienności. Nowoczesna technologia umożliwia użytkownikom połączenie z Internetem dowolnego urządzenia i zdalne nim sterowanie z niemalże każdego miejsca na Ziemi. Żyjemy w czasach, w których Internet wykorzystywany jest na niespotykaną wcześniej skalę. Ta rewolucja informatyczna doprowadziła do powstania przestrzeni teleinformatycznej, czyli inaczej cyberprzestrzeni[2].

Określenie cyberprzestrzeń po raz pierwszy zastosował i spopularyzował William Gibson w swojej powieści *Neuromancer* wydanej w 1984 roku[3]. Autor wskazywał charakterystyczne cechy tego zjawiska, wśród których wyszczególnił przede wszystkim rozciągłość na cały świat oraz wszechstronną bazę danych. Gibson uznał, iż cyberprzestrzeni nie sposób porównać z jakimkolwiek fizycznym wymiarem. W dyskursie naukowym istnieje wiele definicji cyberprzestrzeni. Możemy ją rozumieć jako „zależny od czasu zestaw wzajemnie połączonych systemów informatycznych oraz ludzkich

[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 (Dz.U. L 333 z 27.12.2022).
[2] J. Krawiec, Cyberbezpieczeństwo. Podejście systemowe, Warszawa 2020, s. 120-122.
[3] W. Gibson, Neuromancer, Poznań 2001, s. 256.

użytkowników, którzy wchodzą z tymi systemami w interakcję”[4]. Tomasz Aleksandrowicz definiuje cyberprzestrzeń jako „przestrzeń operacyjną, w której wykonywane są przez ludzi działania mające przynieść określony cel, ze swej strony mają wywołać efekty w samej cyberprzestrzeni, jak i poza nią”[5]. Autor wyróżnia również określone cechy cyberprzestrzeni, do których zalicza: niezależność od czasu, niezależność od miejsca, niezależność od odległości, niezależność od granic, względną anonimowość oraz możliwość ustalenia sprzętu, a nie osoby[6]. Dotychczasowe rozważania na gruncie naukowym pozwalają wyodrębnić różne płaszczyzny cyberprzestrzeni, które stanowią również obszary ludzkiej aktywności. Jak słusznie zauważył Józef Bednarek, cyberprzestrzeń charakteryzuje się kilkoma fundamentalnymi funkcjami: informacyjną, ludyczną, stymulującą, wzorotwórczą i interpersonalną[7].

Bezdyskusyjnie można stwierdzić, iż współcześnie cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa. W literaturze przedmiotu cyberbezpieczeństwo, podobnie jak cyberprzestrzeń, jest rozmaicie definiowane. Można je rozumieć jako „proces zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni”[8]. Nieco inaczej definicje cyberbezpieczeństwa ujmowane są w środowisku naukowym, gdzie szczególną uwagę kładzie się przede wszystkim na wymiar strategiczny bezpieczeństwa. Wówczas prezentowane bezpieczeństwo cybernetyczne można podzielić na obszar cyberobrony (cyberbezpieczeństwo militarne, które jest związane z prowadzoną walką zbrojną i z siłami zbrojnymi) i obszar cyberochrony (cyberbezpieczeństwo o

[4] R. Ottis, P. Lorents, Cyberspace: Definition and Implications, [w:] Proceedings of the 5th International
Conference on Information Warfare and Security, L. Armistead (red.), Dayton U.S. 2010, s. 267-270.
[5] T. R. Aleksandrowicz, Podstawy walki informacyjnej, Warszawa 2016, s. 175-176.
[6] Ibidem.
[7] J. Bednarek, Cyberprzestrzeń i roboty humanoidalne nowym wyzwaniem edukacji, [w:] Człowiek, media, edukacja, J. Morbitzer, E. Musiał (red.), Warszawa 2012, s. 120-139.
[8] C. Banasiński, Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni, [w:] Cyberbezpieczeństwo. Zarys wykładu, C. Basiński (red.), Warszawa 2023, s. 31.

wymiarze pozamilitarnym)[9]. Termin cyberbezpieczeństwo może odnosić się do określonego obszaru działań związanego z bezpieczeństwem informacji (zawartości sieci), bezpieczeństwem komunikowania (przekazu), a także bezpieczeństwem samej sieci, która umożliwia proces komunikowania się, co jednakże nie wyczerpuje wszystkich kwestii wiążących się z potrzebami w zakresie ochrony przed niepożądanymi działaniami w cyberprzestrzeni. Jak słusznie zauważa Katarzyna Chałubińska-Jentkiewicz, bezpieczeństwo w cyberprzestrzeni stanowi fundamentalny element postępu naukowo-technicznego i jako takie określa potrzeby ochrony tegoż obszaru zarówno z perspektywy użyteczności jak również ze względu na przeciwdziałanie nieznanym dotąd zagrożeniom w środowisku cyfrowym[10]. W dobie globalnej informatyzacji, która obejmuje również sferę publiczną, dochodzi do nieuprawnionych działań naruszających dobra osobiste, prawa własności oraz zagrożeń dotykających struktury władzy publicznej i samego państwa. Nie ulega wątpliwości, iż cyberbezpieczeństwo stanowi zjawisko interdyscyplinarne, korzystające z dorobku różnych dziedzin. Do wyodrębnienia cyberbezpieczeństwa z systemu prawa i administracji publicznej niezbędne jest określenie zakresu działania, którego ta sfera dotyczy – zarówno w aspekcie podmiotowym, przedmiotowym, organizacyjnym jak i funkcjonalnym. Taki zabieg umożliwi usystematyzowanie podjętej problematyki bezpieczeństwa w cyberprzestrzeni. Należy zwrócić szczególną uwagę na funkcjonalny aspekt cyberbezpieczeństwa, który odnosi się do działań zmierzających do ochrony tego środowiska oraz podmiotów będących jego użytkownikami. Nieustannie postępująca cyfryzacja i automatyzacja wielu dziedzin życia sprawia, że coraz więcej procesów wymaga wsparcia cyfrowego, aby ich realizacja była możliwa. Taka rzeczywistość nieuchronnie prowadzi do uzależnienia się społeczeństw od cyberprzestrzeni, co z kolei stwarza potrzebę niezawodności infrastruktury teleinformatycznej i jej

[9] S. Koziej, Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO, https://koziej.pl/wp-content/uploads/2016/10/IBK-Cyberbezpiecze%C5%84stwo-25.10.2016.pdf.
[10] K. Chałubińska-Jentkiewicz, Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law" 2025, nr 1(13), s. 1-24.

ochrony przed różnej kategorii atakami[11]. Cyberprzestrzeń stanowi miejsce aktywnego i kreatywnego działania oraz wykorzystania nowoczesnych narzędzi przez grupy przestępcze. W wymiarze geopolitycznym i instytucjonalnym jest to miejsce, w którym wiele państw realizuje własne cele polityczne. Ponadto działania w przestrzeni cyfrowej mogą mieć również formę operacji militarnych[12]. W tak określonej rzeczywistości niezbędnym jest podejmowanie działań i inicjatyw zmierzających do zapewnienia bezpieczeństwa, zarówno w wymiarze wewnętrznym jak i zewnętrznym, co stwarza konieczność dostosowania regulacji prawnych zarówno na poziomie ponadnarodowym, jak i narodowym do sytuacji, w której polem aktywnego działania jest cyberprzestrzeń. Należy wyraźnie podkreślić, iż zapewnienie bezpieczeństwa cyfrowego obywateli oraz podnoszenie odporności i ochrona własnych sieci i systemów teleinformatycznych stanowi podstawowy element bezpieczeństwa narodowego.

DYREKTYWA NIS 2 – ZAKRES PODMIOTOWY

Dyrektywa NIS 2 zastępuje dyrektywę 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 zwaną również dyrektywą NIS i będącą pierwszym europejskim prawem podejmującym kwestię cyberprzestrzeni[13]. Dyrektywa NIS 2 nowelizuje przepisy zawarte w poprzednim dokumencie i wprowadza zmiany w zakresie obowiązków nałożonych na podmioty uznane jako kluczowe i ważne.

Pierwsza istotna zmiana wprowadzona na mocy dyrektywy NIS 2 dotyczy podmiotów, na które dokument nakłada określone obowiązki. Zniesiony został obowiązujący do tej pory podział na dostawców usług cyfrowych, operatorów usług kluczowych oraz podmioty publiczne i wprowadzono rozgraniczenie na

[11] B. Terebiński, Bezpieczeństwo teleinformatyczne jako podstawa funkcjonowania współczesnego świata, „OBRONNOŚĆ. Zeszyty Naukowe" 2018, nr 1(25), s. 215-216.
[12] P. Mickiewicz, System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11, nr 1, s. 65-80.
[13] 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 (Dz. U. UE. L. 2016.194.1).

podmioty kluczowe i podmioty ważne (zarówno publiczne, jak i prywatne). Wspomnieć należy również o tym, iż rozszerzono katalog sektorów objętych działaniem dyrektywy. Jako przyczynę takiego rozwiązania można wskazać nieaktualność wcześniej obowiązującego podziału, ponieważ nie odzwierciedlało ono faktycznego znaczenia danych sektorów czy też usług w obszarze działalności społecznej i gospodarczej Unii Europejskiej. Podmioty kluczowe wymieniono w załączniku I do dyrektywy, natomiast podmioty ważne w załączniku II. Co więcej, art. 2 ust. 1 wskazuje, iż dyrektywa ma zastosowanie do podmiotów wyszczególnionych we wskazanych załącznikach jeśli kwalifikują się one jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu[14] oraz świadczą usługi czy też prowadzą działalność w UE. W załączniku I do dyrektywy NIS 2 ujęto następujące sektory kluczowe: energetyka (w tym podsektory: energia elektryczna, system ciepłowniczy lub chłodniczy, ropa naftowa, gaz, wodór), transport (w tym podsektory: transport lotniczy, wodny, kolejowy i drogowy), bankowość, infrastruktura rynków finansowych, opieka zdrowotna, woda pitna, ścieki, infrastruktura cyfrowa, zarządzanie usługami ICT (między przedsiębiorstwami), podmioty administracji publicznej, przestrzeń kosmiczna. Natomiast jako podmioty kluczowe należy rozumieć:

- podmioty z wymienionych wyżej sektorów, które przekraczają pułap dla średnich przedsiębiorstw;
- kwalifikowanych dostawców usług zaufania oraz rejestry nazw domen najwyższego poziomu, a ponadto dostawców usług DNS bez względu na ich wielkość;
- dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej z zastrzeżeniem, iż podmioty te kwalifikują się jako średnie przedsiębiorstwa;

[14] Art. 2 ust 1. Zalecenia Komisji z dnia 6 maja 2003 r. dotyczącego definicji przedsiębiorstw mikro, małych i średnich (Dz.U. L 124 z 20.5.2003, s. 36) określa kategorię tych przedsiębiorstw na podstawie liczby zatrudnionych osób oraz pułapów finansowych.

- podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym i szczeblu regionalnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym;
- podmioty krytyczne w rozumieniu dyrektywy (UE) 2022/2557 o odporności podmiotów krytycznych[15].

Ponadto, należy wyraźnie podkreślić, iż za podmioty kluczowe mogą być uznane podmioty w rodzaju tych wyszczególnionych w załączniku I oraz II, które państwo członkowskie UE wskazało jako podmioty kluczowe, jeśli ma do nich zastosowanie art. 2 ust. 2 lit. b)-e) dyrektywy, czyli:

- podmiot stanowi jedynego w państwie członkowskim dostawcę usługi mającej kluczowe znaczenie w zakresie utrzymania krytycznej działalności społecznej lub gospodarczej;
- zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na bezpieczeństwo i porządek publiczny oraz zdrowie publiczne;
- zakłócenie usługi świadczonej przez podmiot mogłoby doprowadzić do zaistnienia poważnego ryzyka systemowego (ze szczególnym uwzględnieniem sektorów, w których mogłoby to mieć wpływ transgraniczny);
- podmiot ma charakter krytyczny z uwagi na jego szczególne znaczenie na poziomie regionalnym lub krajowym dla konkretnego sektora, określonego rodzaju usługi lub innych współzależnych sektorów w państwie członkowskim UE.

Warto zaakcentować, iż dyrektywa NIS 2 poza wprowadzeniem regulacji określających kryteria i warunki, zgodnie z którymi podmiot może zostać uznany za kluczowy, pozostawia państwom członkowskim pewną dowolność w tym zakresie. Mianowicie za podmioty kluczowe mogą zostać uznane te, które państwa członkowskie przed wejściem w życie NIS 2 określiło na mocy dyrektywy NIS lub prawa krajowego jako operatorów usług kluczowych[16].

[15] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U.UE.L.2022.333.164) definiuje podmioty krytyczne w art. 2.

[16] Obowiązki podmiotów kluczowych i ważnych w dyrektywie NIS 2, https://cyberpolicy.nask.pl/obowiazki-podmiotow-kluczowych-i-waznych-w-dyrektywie-nis2/.

Uznanie podmiotu za ważny wydaje się być mniej skomplikowane z uwagi na to, iż unijna regulacja w art. 3 ust. 2 wskazuje tylko dwa warunki w tym zakresie. Zgodnie z pierwszym za podmioty ważne należy uznać te, o których mowa w załączniku I lub II i które nie kwalifikują się jako podmioty kluczowe zgodnie z art. 3 ust. 1. Co więcej odnosi się to również do podmiotów, które państwa członkowskie wskazały jako podmioty ważne zgodnie z wytycznymi określonymi w art. 2 ust. 2 lit b-e, czyli:

- podmiot stanowi jedynego w państwie członkowskim dostawcę usługi mającej kluczowe znaczenie w zakresie utrzymania krytycznej działalności społecznej lub gospodarczej;
- zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na bezpieczeństwo i porządek publiczny oraz zdrowie publiczne;
- zakłócenie usługi świadczonej przez podmiot mogłoby doprowadzić do zaistnienia poważnego ryzyka systemowego (ze szczególnym uwzględnieniem sektorów, w których mogłoby to mieć wpływ transgraniczny);
- podmiot ma charakter krytyczny z uwagi na jego szczególne znaczenie na poziomie regionalnym lub krajowym dla konkretnego sektora, określonego rodzaju usługi lub innych współzależnych sektorów w państwie członkowskim UE.

Należy wyraźnie podkreślić, iż mimo że dyrektywa NIS 2 w zakresie podmiotów kluczowych i ważnych co do zasady odnosi się do podmiotów będących co najmniej średnim przedsiębiorstwem, to jednak prawodawca unijny przewidział szereg wyjątków w tym zakresie. Zostały one określone w art. 2 ust. 2 dokumentu, zgodnie z którym przypadki, w których NIS 2 ma zastosowanie do podmiotów w rodzaju tych wyszczególnionych w załączniku I i II bez względu na ich wielkość mają miejsce, jeśli:

- usługi są świadczone przez dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej; dostawców usług zaufania; rejestry nazw domen najwyższego poziomu oraz dostawców usług systemów nazw domen;

- podmiot stanowi jedynego w państwie członkowskim dostawcę usługi mającej kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;
- zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne;
- wystąpienie zakłócenia usługi świadczonej przez podmiot mogłoby skutkować zaistnieniem poważnego ryzyka systemowego przede wszystkim z uwzględnieniem sektorów, w których takie zakłócenie mogłoby mieć wpływ transgraniczny;
- podmiot ma charakter krytyczny z uwagi na jego szczególne znaczenie na poziomie krajowym czy też regionalnym dla określonego sektora, rodzaju usługi lub dla innych współzależnych sektorów w państwie członkowskim;
- podmiot jest podmiotem administracji publicznej zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym: na poziomie centralnym lub na poziomie regionalnym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą[17].

Poza wyżej wskazanymi przypadkami dyrektywa NIS 2 ma również zastosowanie do podmiotów nienależących do rodzaju tych wymienionych w I i II załączniku i bez względu na ich wielkość, jeśli:

- zostały one zidentyfikowane jako podmioty o charakterze krytycznym na mocy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE[18];
- świadczą one usługi rejestracji nazw domen;
- państwo członkowskie postanowi, iż dyrektywa NIS 2 ma zastosowanie do określonych podmiotów administracji publicznej na poziomie lokalnym,

[17] 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 (Dz.U. L 333 z 27.12.2022).
[18] Szczegółowe kryteria identyfikacji podmiotów o charakterze krytycznym zawiera art. 6 „Identyfikacja podmiotów krytycznych" oraz załącznik do dyrektywy (EU) 2022/2557 określający sektory, podsektory i kategorie podmiotów, do których dyrektywa ma zastosowanie.

instytucji edukacyjnych (szczególnie, gdy prowadzą one działalność badawczą o znaczeniu krytycznym).

Wobec wskazanych powyżej kryteriów odnoszących się do zakresu podmiotowego unijnej regulacji warto wyraźnie wskazać dla jakich podmiotów nie ma ona zastosowania. W tej grupie znajdują się podmioty administracji publicznej, które prowadzą działalność w obszarze bezpieczeństwa narodowego lub publicznego, obronności lub egzekwowania prawa, a także określone podmioty prowadzące działania w obszarze bezpieczeństwa narodowego lub publicznego, obronności lub egzekwowania prawa (w tym zapobiegania przestępstwom, prowadzenia postępowań w ich sprawie, wykrywania i ścigania przestępstw) lub które świadczą usługi wyłącznie na rzecz podmiotów administracji publicznej działającej we wspomnianym powyżej obszarze i które zostaną zwolnione przez państwa członkowskie z obowiązków ustanowionych w art. 21 lub 23 w odniesieniu do tych działań lub tych usług[19]. Jednocześnie należy podkreślić, iż zwolniony podmiot nie podlega przepisom odnoszącym się do nadzoru i egzekwowania, zawartym w rozdziale VII dyrektywy NIS 2 w zakresie zwolnionej działalności. Jeżeli tak określona działalność jest jedyną, jaką prowadzi podmiot, może on zostać zwolniony również z obowiązków wynikających z przepisów zawartych w art. 3 i 27 dyrektywy związanych z przekazaniem danych w celach rejestracyjnych. Jednakże na tak określonych zasadach nie można zwolnić z obowiązków wynikających z przepisów dyrektywy NIS 2 dostawców usług zaufania.

WNIOSKI

Zakres podmiotowy dyrektywy NIS 2 stanowiący przedmiot analiz niniejszego artykułu zawiera precyzyjne kryteria, zgodnie z którymi państwa członkowskie Unii Europejskiej mogą wskazywać podmioty kluczowe i podmioty ważne. Podsumowując przedstawione analizy można uznać, iż unijny dokument ma zastosowanie do wszystkich podmiotów prowadzących działalność w sektorach gospodarki wyszczególnionych w załącznikach do dyrektywy, które są przedsiębiorstwami średnimi lub dużymi, czyli takimi które zatrudniają między 50 a 250 osób, a ich obroty roczne nie przekraczają 50 mln euro i/lub

[19] NIS2 Directive: new rules on cybersecurity of network and information systems, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

roczna suma bilansowa nie przekracza 43 mln euro. Jednakże należy zaakcentować, iż do stosowania NIS 2 zobowiązane będą również mniejsze podmioty (mikroprzedsiębiorstwa i małe przedsiębiorstwa), które zgodnie z kryteriami zawartymi w unijnym dokumencie mogą zostać uznane za pełniące kluczową rolę dla społeczeństwa, gospodarki czy też określonych sektorów i typów usług.

Istotną zmianą wprowadzoną przez dyrektywę NIS 2, na którą należy zwrócić uwagę jest sposób, w który dokonuje się określenia podmiotów kluczowych i ważnych. Unijny dokument wprowadza zasadę samookreślania podmiotów (*self-assessment*), co oznacza, że to w zakresie obowiązków podmiotów znajduje się przeprowadzenie stosownych analiz oraz oceny, czy zgodnie z kryteriami zawartymi w NIS 2 stanowią one podmiot kluczowy lub ważny. Jednakże wspomniana zasada samookreślania przewiduje pewne wyjątki. W pewnych przypadkach państwa członkowskie będą zmuszone dokonać identyfikacji pewnych podmiotów kluczowych stanowiących mikro lub małe przedsiębiorstwa, wobec których zaistnienie zakłóceń w świadczonych przez nie usługach mogłoby wywrzeć poważny wpływ na bezpieczeństwo i porządek publiczny czy też zdrowie publiczne. Warto również pochylić się nad podmiotami administracji publicznej na poziomie regionalnym. W ich przypadku również musi zostać przeprowadzona ocena w zakresie analizy ryzyka prowadzonej przez te podmioty działalności. W sytuacji, gdy wykaże ona, że zakłócenie świadczonych przez nie usług mogłoby mieć poważny wpływ na krytyczną działalność społeczną czy też gospodarczą, to takie podmioty również będą musiały realizować obowiązki wynikające z dyrektywy NIS 2. Regulacje zawarte w dyrektywnie nie precyzują jednak kto takiej oceny i analizy ma dokonywać. Na podstawie przeprowadzonych analiz można wobec tego uznać, iż przesądzenie tej kwestii będzie należało do ustawodawstwa państwa członkowskiego, a zatem pozostanie uregulowane prawem krajowym. Analizując możliwości w tym zakresie można wskazać kilka potencjalnych wariantów, zgodnie z którymi przeprowadzanie analiz oraz ocena leżałoby w gestii organów wyższego stopnia, organów nadzorczych, organów właściwych do spraw cyberbezpieczeństwa, podmiotu administracji publicznej poddawanego ocenie czy też samego ustawodawcy.

Analizując zakres podmiotowy dyrektywy NIS 2 należy zwrócić szczególną uwagę na kwestie językowe, które mogą przyczyniać się do niejasności i wątpliwości. Na przykładzie polskiego tłumaczenia można odnieść wrażenie, iż podział na podmioty kluczowe i podmioty ważne nie jest intuicyjny. Może o tym świadczyć chociażby to, iż podmioty ważne działają nie tylko w sektorach ważnych, lecz również w kluczowych. Podejmując próbę wskazania źródła tych niejasności o charakterze językowym można skierować się ku polskiemu tłumaczeniu unijnej dyrektywy, w którym dwie kategorie sektorów (kluczowy i ważny) mają nazwy tożsame z dwoma kategoriami podmiotów (kluczowym i ważnym). Odmiennie prezentuje się to w angielskojęzycznej wersji NIS 2[20], w której sektory nazwano *ectors of high criticality* a także *other critical sectors*. Z kolei podmioty zostały określone jako *essential entities* oraz *important entities*.

Podsumowując rozważania poczynione w niniejszym artykule należy zaakcentować, iż Dyrektywa NIS 2 określa jedynie minimalne standardy w zakresie cyberbezpieczeństwa, które państwa członkowskie mają możliwość rozszerzyć, gdy uznają to za zasadne. Problematyka cyberbezpieczeństwa i cyberodporności obecnie nie jest już niszowa. Na zagrożenia wynikające z cyberataków narażonych jest coraz więcej podmiotów. W obliczu nowych regulacji unijnych nawet te podmioty, które dotychczas nie odnotowały konieczności wdrażania środków i narzędzi zapewniających cyberbezpieczeństwo lub podnoszących jego poziom, mogą zostać do tego prawnie zobowiązane. Warto podkreślić, iż dyrektywa NIS 2 nie tylko rozszerza zakres podmiotowy, lecz również obowiązki nałożone na podmioty kluczowe i ważne. Wobec powyższych nie ulega wątpliwości, iż jako dobrą praktykę należy uznać dokonanie wcześniejszych analiz w zakresie podlegania przez dany podmiot przepisom NIS 2 w celu właściwego przygotowania się do przyjęcia właściwych struktur i mechanizmów zapewniających zgodność z unijnymi regulacjami.

Bibliografia

[20] Angielskojęzyczna wersja dyrektywy NIS 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

Akty normatywne

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 (Dz.U. L 333 z 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U.UE.L.2022.333.164).

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 (Dz. U. UE. L. 2016.194.1).

Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji przedsiębiorstw mikro, małych i średnich, (Dz.U. L 124 z 20.5.2003, s. 36).

Literatura

Aleksandrowicz T. R., Podstawy walki informacyjnej, Warszawa 2016.

Banasiński C., Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni, [w:] Cyberbezpieczeństwo. Zarys wykładu, C. Basiński (red.), Warszawa 2023.

Bednarek J., Cyberprzestrzeń i roboty humanoidalne nowym wyzwaniem edukacji, [w:] Człowiek, media, edukacja, J. Morbitzer, E. Musiał (red.), Warszawa 2012.

Chałubińska-Jentkiewicz K., Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law" 2025, nr 1(13).

Gibson W., Neuromancer, Poznań 2001.

Krawiec J., Cyberbezpieczeństwo. Podejście systemowe, Warszawa 2020.

Mickiewicz P., System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11, nr 1.

Ottis R., Lorents P., Cyberspace: Definition and Implications, [w:] Proceedings of the 5th International Conference on Information Warfare and Security, L. Armistead (red.),Dayton U.S. 2010.

Terebiński B., Bezpieczeństwo teleinformatyczne jako podstawa funkcjonowania współczesnego świata, „OBRONNOŚĆ. Zeszyty Naukowe" 2018, nr 1(25).

Źródła internetowe:

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

Koziej S., Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO,https://koziej.pl/wp-content/uploads/2016/10/IBK-Cyberbezpiecze%C5%84stwo-25.10.2016.pdf.

NIS2 Directive: new rules on cybersecurity of network and information systems, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

Obowiązki podmiotów kluczowych i ważnych w dyrektywie NIS 2, https://cyberpolicy.nask.pl/obowiazki-podmiotow-kluczowych-i-waznych-w-dyrektywie-nis2/.

THE EU NIS 2 DIRECTIVE IN THE AREA OF CYBER SECURITY - AN ANALYSIS OF ESSENTIAL ENTITIES AND IMPORTANT ENTITIES

Abstract

Internet-enabled desktop and mobile devices are an essential tool used by individuals as well as businesses and public institutions as an essential work tool. Awareness of the diversity of cyber threats and the consequences they

bring creates the need for transnational regulations aimed at increasing the level of cyber security and resilience of information systems. The purpose of the article is to analyse the NIS 2 directive with regard to the key and important entities on which the EU document imposes certain obligations, as well as to show certain doubts for the Polish legislator arising from it. The institutional-legal method and analysis of the literature on the subject were used.

Keywords: cyber security, NIS 2 directive, essential entities, important entities