Zeszyty Prawnicze
23.3 / 2023, s. 95-108
DOI 10.21697/zp.2023.23.3.04

Agnieszka Brzostek

Akademia Sztuki Wojennej w Warszawie

CYBERBEZPIECZEŃSTWO W ADMINISTRACJI PUBLICZNEJ – ASPEKTY PRAWNE

I. Wprowadzenie

Według szacunków Parlamentu Europejskiego do 2030 r. do Internetu może być podłączonych 125 miliardów urządzeń, w porównaniu z 27 miliardami w 2017 r.; oczekuje się jednocześnie, że 90% osób w wieku powyżej sześciu lat będzie online. Oznacza to nowe możliwości korzystania z sieci, ale także wyzwania i zagrożenia. Obecnie unijny wskaźnik umiejętności cyfrowych wynosi 56%, według założeń UE wskaźnik podstawowych umiejętności cyfrowych do roku 2030 wzrośnie do 80%[1]. Szacunkowe dane wskazują na taką powszechność dostępu do Internetu, która nieść będzie ze sobą zagrożenia: te, które dotyczą naszego bezpieczeństwa i bezpieczeństwa usług kluczowych. Zwłaszcza że, jak zauważyła Agencja UE do spraw Cyberbezpieczeństwa (ENISA), pandemia COVID-19 znacznie przyczyniła się do zwiększenia zagrożeń w cyberprzestrzeni, wskazując na możliwości, jakie daje praca zdalna, a także działania wojenne na Ukrainie. Według raportu

[1] Przepaść cyfrowa: różnice społeczne wynikające z cyfryzacji, Rezolucja Parlamentu Europejskiego z 13 grudnia 2022 r. w sprawie przepaści cyfrowej: różnice społeczne wynikające z cyfryzacji (2022/2810(RSP)) (Dz. Urz. UE C 177, s. 57).

Threat Landscape 2022[2] przygotowanego przez ENISA wśród sześciu najważniejszych sektorów dotkniętych zagrożeniami dla cyberbezpieczeństwa w UE administracja publiczna zajęła pierwsze miejsce. Pojęcie „administracja publiczna" jest traktowane szeroko, bowiem rozumie się przez nie zarówno rząd, organy administracji publicznej, jak i organy administracji samorządowej. W tym zakresie, wszystkich zgłoszonych incydentów było 24%[3]. Jak znaczący jest to odsetek, świadczy fakt, że w podobnym raporcie obejmującym okres od kwietnia 2020 r. do lipca 2021 r. w stosunku do tak samo zakwalifikowanych podmiotów zgłoszonych było 198 incydentów[4]. Pozostałe obszary to dostawcy usług cyfrowych (13%), ogół społeczeństwa (12%), usługi (12%), finanse i bankowość (9%), opieka zdrowotna (9%) oraz pozostałe sektory oznaczone jako inne (23%)[5]. Sektor administracji publicznej był tym, w którym odnotowano największą liczbę incydentów dotyczących skutków społecznych, które w większości dotyczyły zakłóceń w świadczeniu usług lub naruszeń danych osobowych. Ponadto zaobserwowano, że w sektorze opieki zdrowotnej również wystąpiła duża liczba incydentów o poważnym wpływie z powodu przypadków naruszenia danych wrażliwych lub braku dostępności usług zdrowotnych, takich jak umawianie rezerwacji. Stąd też celem niniejszego artykułu jest wskazanie prawnych uregulowań i możliwości systemowych umożliwiających zmniejszanie zagrożeń w sektorze publicznym i jak najbardziej skuteczne podniesienie poziomu cyberbezpieczeństwa.

---

[2] Enisa Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [dostęp 24 maja 2023 r.].

[3] https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia [dostęp 24 maja 2023 r.].

[4] Enisa Threat Landscape 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [dostęp 24 maja 2023 r.].

[5] https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia [dostęp 24 maja 2023 r.].

II. Cyberbezpieczeństwo

Pojęcie cyberbezpieczeństwa doczekało się zarówno na gruncie przepisów prawa, jak i w doktrynie licznych definicji. Wartościując rodzaj tych definicji, należy wskazać, że w pewnym zakresie odnoszą się one już do zjawiska zidentyfikowanego i wyjaśnionego przez ustawodawcę albo inny właściwy w tym zakresie organ. Katarzyna Chałubińska-Jentkiewicz zauważyła, że samo pojęcie cyberbezpieczeństwa odnosić się może do ściśle określonego obszaru działań związanych z metodą, procedurą, rozwiązaniem prawnym, podejmowanym przez właściwe w tym względzie podmioty, które mają na celu zachowanie integralności zgromadzonych zasobów informacyjnych, ich przetwarzanie, przechowywanie i ochronę przed nieuprawnionym, niepożądanym ujawnieniem, zniszczeniem lub zmianą[6]. Pojęciami pomocniczymi w definiowaniu cyberbezpieczeństwa są „bezpieczeństwo informacyjne" i „cyberprzestępczość"[7]. Cezary Banasiński napisał, że przez pojęcie cyberbezpieczeństwa należy rozumieć proces zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych, prawnych i innych podmiotów oraz zasobów informacyjnych w globalnej cyberprzestrzeni[8].

Cyberbezpieczeństwo jako bezpieczeństwo sieci i systemów teleinformatycznych, zwłaszcza jako odporność systemów teleinformatycznych na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywania, przekazywania, przetwarzania danych lub związanych z nimi usług cyfrowych lub dostępnych przez te sieci i systemy informatyczne zostało określone w Strategii

---

[6] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, «Cybersecurity and Law» 2/2019, s. 13-15.

[7] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 351.

[8] C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018, s. 31.

Cyberbezpieczeństwa Rzeczypospolitej Polskiej[9]. Dyrektywa NIS nie zawiera definicji cyberbezpieczeństwa, natomiast takie znamiona, jakie przypisuje się pojęciu cyberbezpieczeństwa, zawiera definicja bezpieczeństwa sieci i systemów informatycznych, gdzie oznacza to odporność systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub związanych z nimi usług oferowanych przez te sieci i systemy informatyczne[10]. Zgodzić się należy ze stanowiskiem Grażyny Szpor, że w sytuacji wyeliminowania pojęcia cyberbezpieczeństwa z dyrektywy NIS i zastąpienia je pojęciem bezpieczeństwa sieci i systemów informatycznych ustawodawca europejski powinien wskazać, że oba pojęcia rozumie jako tożsame[11].

Dyrektywa NIS 2 jako pojęcie cyberbezpieczeństwa[12] wskazuje definicję zawartą w art. 2 pkt 1 dyrektywy 9(UE) 2018/1972, według której cyberbezpieczeństwo to działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników tych systemów oraz innych osób przed cyberzagrożeniami[13]. Definicja legalna cyberbezpieczeństwa zawarta w ustawie o Krajowym Systemie Cyberbezpieczeństwa określiła cyberbezpieczeństwo jako odporność systemów informacyjnych na działania

---

[9] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2020, Warszawa 2017, s. 28. Przeglądu definicji cyberbezpieczeństwa w strategiach innych państw członkowskich UE dokonała A. Warchoł, *Pojęcie cyberprzestrzeni w strategiach bezpieczeństwa państw członkowskich Unii Europejskiej*, «Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate» 4/2019, s. 99-104.

[10] Art. 4 pkt 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 2016 r., s. 1); dalej: dyrektywa NIS.

[11] G. Szpor, *Komentarz do art. 2*, [w:] *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, s. 42-43.

[12] Art. 6 pkt 3 dyrektywy NIS 2.

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 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 z 2019 r., s. 15).

naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nim usług oferowanych przez te systemy[14]. Jak zauważył Filip Radoniewicz, poufność oznacza dostęp do danych tylko przez osoby do tego uprawnione, z wyłączeniem osób trzecich. Wiąże się to z ochroną przed ich odczytaniem i kopiowaniem przez osoby nieuprawnione. Dostępność oznacza możliwość korzystania z informacji przez uprawnione osoby, ilekroć zajdzie taka potrzeba, przy czym dostępność oznacza, że dane są osiągalne i mogą być używane w każdym czasie i w wymagany sposób. Przez integralność rozumie się cechę danych i informacji oznaczającą ich dokładność i kompletność oraz utrzymywanie ich w tym stanie. Odnosi się do nienaruszalności zarówno danych, jak i systemów komputerowych[15].

Przytoczone wyżej definicje mają charakter poglądowy, a ich wyraz jest szczególnie istotny, gdy analizie poddane zostaną sposoby naruszeń cyberbezpieczeństwa. Według wspomnianego już raportu ENISA *Threat Landscape 2022* można wyróżnić osiem głównych i największych jednocześnie zagrożeń dla cyberbezpieczeństwa. Jako pierwszy i w 2022 r. główny wskazany został *ransomware*, gdzie w ankiecie przeprowadzonej przez ENISA ponad połowa respondentów została taką formą ataków hakerskich dotknięta. *Ransomware* to atak, w którym hakerzy przejmują kontrolę nad danymi lub siecią i żądają opłaty w zamian za przywrócenie danych lub dostępu do sieci. Z raportu ENISA wynika, że średnia wartość okupu zapłaconego w atakach *ransomware* podwoiła się z 71 tysięcy euro w 2019 r. do 150 tysięcy w 2020 r., a w 2021 r. szkody w wyniku takich ataków wyniosły 18 miliardów[16].

Drugim wskazanym zagrożeniem jest *malware*, czyli złośliwe oprogramowanie, takie jak wirusy, konie trojańskie i oprogramowanie

---

[14] Art. 2 pkt 4 ustawy z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913); dalej: ustawa o KSC.

[15] F. Radoniewicz, *Komentarz do art. 2*, [w:] *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 31.

[16] ENISA Threat Landscape 2022, s. 43-89. Zob. https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia [dostęp 26 maja 2023 r.].

szpiegowskie. W 2020 r i na początku 2021 r. z powodu pandemii COVID-19 liczba ataków diametralnie spadła, natomiast wzrosła znacząco pod koniec 2021 r. w związku z powrotem pracy zdalnej oraz wykorzystaniem tzw. *Cryptojacking*, czyli potajemnego wykorzystania komputera ofiary do nielegalnego wydobywania kryptowalut, oraz złośliwego oprogramowania atakującego tzw. Internet rzeczy, tj. urządzenia podłączonego do routera lub kamery[17].

Trzecią formą są zagrożenia związane z wykorzystaniem socjotechniki poprzez nakłanianie ofiar podstępem do otwierania złośliwych dokumentów, plików lub wiadomości e-mail czy odwiedzania stron i udzielania w sposób nieautoryzowany dostępu do systemu lub usług. Najczęściej takie działania przybierają formę *phishingu* za pośrednictwem e-mail lub *smishingu* z wykorzystaniem wiadomości SMS. Według badań cytowanych przez ENISA taki sposób działań hakerskich stanowi prawie 60% naruszeń cyberbezpieczeństwa w Europie, na Bliskim Wschodzie i w Afryce[18].

Czwartym typem zagrożenia dla danych jest dążenie do uzyskania nieautoryzowanego dostępu lub ich ujawnienia. Dotyczy to naruszenia bezpieczeństwa danych w postaci zamierzonych działań hakerskich oraz przypadków niezamierzonych, tj. wycieków danych. Najczęstszym powodem są wyłudzenia finansowe, rzadziej szpiegostwo[19].

Następną wyróżnioną przez ENISA formą ataków są tzw. zagrożenia dla dostępności w formie odmowy usługi oraz uniemożliwianie użytkownikom dostępu do danych lub usług. Ataki tego typu są jedną z najbardziej krytycznych zagrożeń dla systemów informatycznych, tj. przeciążenie infrastruktury sieciowej i uniemożliwienie dostępu do systemu. Najczęściej dotyczy to sieci komórkowych[20].

Zagrożenia dla dostępności Internetu obejmują fizyczne przejmowanie i niszczenie infrastruktury internetowej, zaobserwowane na

---

17 ENISA Threat Landscape 2022, s. 49.

18 *Ibidem*, s. 54 i n.

19 *Ibidem*, s. 63.

20 *Ibidem*, s. 69 i n.

okupowanych terytoriach Ukrainy i cenzurowanie serwisów informacyjnych lub mediów społecznościowych[21].

Jako siódma w kolejności została wskazana dezinformacja lub informacje wprowadzające w błąd. Rosnące wykorzystanie mediów społecznościowych i mediów internetowych doprowadziło do nasilenia kampanii rozpowszechniających dezinformację (celowo sfałszowane informacje) i informacje wprowadzające w błąd (udostępnianie błędnych informacji)[22].

Ostatnim wyróżnionym zagrożeniem były ataki dotyczące płynności w łańcuchu dostaw pomiędzy organizacjami a dostawcami[23].

W corocznym raporcie z działalności CERT Polska w 2022 r. wskazał, że CSIRT NASK obsłużył 937 incydentów dotyczących podmiotów publicznych. Incydentów odnoszących się do podmiotów sektora administracji publicznej było 547, do sektora oświaty – 134, do sektora infrastruktury cyfrowej – 81. W analizie dotyczącej zagrożeń w wybranych sektorach gospodarki, w administracji publicznej liczba incydentów wynosiła 757, co dawało 1,91% wszystkich incydentów[24].

Incydenty związane z bezpieczeństwem cybernetycznym są złożonymi i wieloaspektowymi wydarzeniami, a ich pełne skutki nie zawsze mogą urzeczywistnić się natychmiast[25].

III. Podstawy prawne działania

Cyberbezpieczeństwo wymaga ochrony na różnych płaszczyznach, co jest skutkiem różnorodności możliwych form ataków. Zabiegi zmierzające do zapewnienia jak najwyższego poziomu bezpieczeństwa

---

[21] *Ibidem*, s. 78.

[22] *Ibidem*, s. 83 i n.

[23] *Ibidem*, s. 88 i n.

[24] Raport roczny z działalności Cert Polska 2022, s. 37. https://cert.pl/uploads/docs/Raport_CP_2022.pdf [dostęp 27 maja 2023 r.].

[25] P. Rosati, F. Gogol, T. Lynn, *Cyber-security incidents and audit quality*, «European Accounting Review» 29/2020, s. 4.

podejmowane były od dawna, a ich rezultatem[26] była przyjęta w dniu 6 lipca 2016 r. dyrektywa NIS[27]. Dyrektywa nałożyła na państwa członkowskie wiele obowiązków, obligując je do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. Dyrektywa zobowiązała wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Jej przepisy umożliwiły stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty w formie bardziej zdecentralizowanej. Dyrektywa NIS nie dotyczyła bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w dyrektywie. Dokument stanowił jednak harmonizację minimalną, a zatem wyznaczał pewne minimalne warunki, które należało spełniać. Nie ograniczał przy tym możliwości państw członkowskich do regulowania problematyki cyberbezpieczeństwa administracji publicznej we własnym ustawowym zakresie. Dyrektywa wskazała wiele zadań organów właściwych w zakresie bezpieczeństwa sieci i informacji, a do najważniejszych należało: badanie przypadków niewypełniania przez operatorów usług kluczowych zobowiązań z zakresu bezpieczeństwa sieci i informacji; ocena wyników audytów bezpieczeństwa teleinformatycznego; wydawanie wytycznych w zakresie bezpieczeństwa teleinformatycznego oraz wprowadzenie sankcji za nieprzestrzeganie przepisów. Dyrektywa NIS określiła też status CSIRT, czyli Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego. Kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju bądź zbudować sieć CSIRT-ów sektorowych, obejmujących sektory rynkowe[28]. Dyrektywa NIS dała organom publicznym konkretne narzędzia do przeciwdziałania incydentom w cyberprzestrzeni i reagowania na nie. Są to między innymi obowiązkowe raportowanie, przygotowanie krajowej strategii NIS,

[26] D. Fleszer, A. Rogacka-Łukasik, *Europejskie podstawy prawne ochrony informacji*, «Studia Prawnicze KUL» 78.2/2019, s. 67.

[27] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 2016 r., s. 1).

[28] D. Fleszer, A. Rogacka-Łukasik, *op. cit.*, s. 71.

skoordynowanie przepływu informacji czy też zinstytucjonalizowanie współpracy CSIRT-ów[29].

Implementacja dyrektywy NIS do porządku krajowego nastąpiła w drodze ustawy o Krajowym Systemie Cyberbezpieczeństwa z 5 lipca 2018 r. Pełne wdrożenie ustawy wymagało przyjęcia rozporządzeń Rady Ministrów w sprawie uznania incydentu za poważny[30], jak i w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[31]. Stworzony w ten sposób system cyberbezpieczeństwa ma na celu zapewnienie cyberbepiczeństwa na poziomie krajowym, a w szczególności niezakłóconego świadczenia usług kluczowych i usług cyfrowych przez osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów[32]. Polski ustawodawca włączył w zakres ustawy również administrację publiczną oraz sektor telekomunikacyjny[33].

Z przeprowadzonego przez UE przeglądu wynikło, że zaistniały istotne różnice przy wdrażaniu dyrektywy przez państwo członkowskie. Margines swobody, jaki zapewniła UE w tym procesie, przyczynił się do różnej formy jej implementacji. Skutkowało to fragmentacją rynku wewnętrznego, co szkodliwie wpływało na transgraniczne funkcjonowanie

---

[29] G. Christou, *Cybersecurity in the European Union*, London 2016, s. 133.

[30] Rozporządzenie Rady Ministrów z 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180).

[31] Rozporządzenie Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806).

[32] M. Toumi, *Zmiany w strukturze centralnej administracji publicznej w świetle ustawy o Krajowym Systemie Cyberbezpieczeństwa z 2018 r.*, «Przegląd Prawa Konstytucyjnego» 60.2/2021, s. 329.

[33] M. Wilbrandt-Gotowicz, *Wielopostaciowość form działania administracji publicznej na przykładzie wymogu implementacji dyrektywy 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*, «Opolskie Studia Administracyjno-Prawne» 4.1/2018, s. 174.

usług i poziom cyberodporności[34]. Wszystkie te czynniki stały się powodem uchwalenia dyrektywy NIS 2.

W dyrektywie przyjętej przez Parlament Europejski i Radę 14 grudnia 2022 r.[35] – dyrektywa NIS 2 – rozszerzono zakres podmiotowy jej stosowania między innymi o administrację publiczną, sektor żywności, ścieki, przemysł, zarządzanie odpadami i przestrzeń kosmiczną; ponadto szerzej potraktowano niektóre sektory (m.in. rozszerzenie zakresu infrastruktury cyfrowej)[36]. Wyłączenie podmiotów administracji publicznej z zakresu stosowania dyrektywy powinno mieć zastosowanie do podmiotów, które prowadzą działalność głównie w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym działania związane z zapobieganiem przestępstwom, prowadzeniem postępowań w ich sprawie, wykrywaniem ich i ściganiem. Jednakże podmioty administracji publicznej, których działalność jedynie w niewielkim stopniu wiąże się z tymi obszarami, nie są wyłączone z zakresu stosowania dyrektywy[37]. W art. 2 pkt 5 wskazano, że to państwa członkowskie mogą postanowić o zastosowaniu postanowień dyrektyw do administracji publicznej na poziomie lokalnym. Zgodnie z postanowieniami art. 3 pkt 1d administracja publiczna została uznana za podmiot kluczowy. W załączniku do dyrektywy NIS 2 w pkt 10 wprost wskazano, że są to: podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym i podmioty administracji publicznej na szczeblu regionalnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym. Dyrektywa nakłada na państwa członkowskie obowiązek stworzenia, do 17 kwietnia 2025 r., wykazu podmiotów kluczowych i ważnych, a także podmiotów

---

[34] Pkt 4 i 5 dyrektywy NIS 2.

[35] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 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 L 333 z 2022 r., s. 80).

[36] Pkt 37 dyrektywy NIS 2.

[37] Pkt 8 dyrektywy NIS 2.

świadczących usługi polegające na rejestracji nazw domen. Państwa członkowskie regularnie i nie rzadziej niż co dwa lata po wyżej wymienionej dacie dokonują przeglądu i aktualizacji tego wykazu[38]. Dyrektywa zakłada, że państwa członkowskie powinny mieć możliwość decydowania, które podmioty kluczowe należy uznać za podmioty zidentyfikowane jako operatorzy usług kluczowych zgodnie z dyrektywą (UE 2016/1148)[39]. Zgodnie z art. 2 pkt 16 ustawy o KSC przez pojęcie „usługa kluczowa" należy rozumieć usługę, która ma kluczowe znaczenia dla utrzymania działalności społecznej, gospodarczej i została wymieniona w wykazie usług kluczowych. Operatorem usługi kluczowej według art. 5 ust. 1 ustawy o KSC pozostają podmioty, które po pierwsze, posiadają jednostkę organizacyjną na terytorium RP (kryterium ustrojowe), a po drugie, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej (kryterium formalne). Należy jeszcze wziąć pod uwagę kryterium materialne, przy uwzględnieniu art. 5 ust. 2 w zw. z art. 4 pkt 4 dyrektywy NIS, do którego odnosi się art. 5 ust. 2 ustawy o KSC. Decyzję identyfikacyjną wydaje się, jeżeli podmiot świadczy usługę kluczową, a świadczenie tej usługi zależne jest od systemów informacyjnych, a ponadto incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora[40].

IV. Wnioski

Kluczowym wyzwaniem dla UE jest sprecyzowanie zakresu obowiązków dotyczących zaangażowanych instytucji i podmiotów gospodarczych, przy obowiązujących różnych ramach prawnych państw UE dotyczących cyberbezpieczeństwa. Biorąc pod uwagę złożoność problemu i różnorodność uczestniczących podmiotów (państwowych i niepaństwowych),

---

[38] Art. 3 pkt 3 dyrektywy NIS 2.

[39] Pkt 17 dyrektywy NIS 2.

[40] M. Wilbrandt-Gotowicz, *Komentarz do art. 5*, [w:] *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, s. 80.

rządy krajowe są najlepiej przygotowane do zapobiegania i reagowania na incydenty i ataki cybernetyczne. Dotyczy to współpracy sektora państwowego z prywatnym oraz indywidualnymi użytkownikami w sieci w ramach ustalonych kierunków działań instytucji europejskich na rzecz podnoszenia poziomu bezpieczeństwa strategii politycznych i ram prawnych[41]. Rozwiązaniem może być systemowa kontrola wielopłaszczyznowa[42]. Zwłaszcza że tylko stworzenie ram prawnych do działania na gruncie prawa europejskiego i krajowego umożliwi kompleksową walkę z zagrożeniami w cyberprzestrzeni. Wyraźnie zaznaczyć należy tu rolę organów administracji publicznej, które wyposażone w odpowiednie kompetencje i środki nadzoru, także przy współpracy z podmiotami prywatnymi, mogą stanowić skuteczną tarczę w walce z cyberzagrożeniami. Powtarzane w literaturze tezy, że pandemia COVID-19 i wojna na Ukrainie przyczyniły się do wzrostu cyberzagrożeń, znajduje swoje odzwierciedlenie w badaniach ENISA[43]. Obecnie największe zagrożenie to właśnie dezinformacja, utrata autorytetu w nadzorze prywatnym czy błąd ludzki i brak umiejętności. Przewidywane scenariusze różnych form zagrożeń realnie wskazują, na jak wielu płaszczyznach takie ataki mogą wystąpić. Administracja publiczna jest jedną z najczęściej atakowanych struktur państwa.

Cyberbezpieczeństwo w administracji publicznej

Streszczenie

Sektor administracji publicznej jest wymieniany w raportach Agencji UE do spraw Cyberbezpieczeństwa jako najczęściej atakowany. Liczba zgłaszanych incydentów ciągle rośnie. Pandemia COVID-19 i co za tym idzie – upowszechnienie świadczenia pracy w formie zdalnej oraz wojna na Ukrainie realnie wzmacniają to zagrożenie. Tym bardziej że hakerzy na wielką skalę stosują złośliwe oprogramowania,

[41] J. Cichosz, *Kierunki działań instytucji europejskich na rzecz podnoszenia poziomu bezpieczeństwa podmiotów państwowych i niepaństwowych w cyberprzestrzeni – wybrane przykłady*, «Teka Komisji Politologii i Stosunków Międzynarodowych (Teka of Political Science and International Relations)» 13.2/2018, s. 59-60.

[42] P. Rosati, F. Gogoli, T. Lynn, *op. cit.*, s. 22.

[43] https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-203 [dostęp 24 maja 2023 r.].

szczególnie takie, jak *ransomware*, *malware*, zagrożenia związane z socjotechniką czy odmowa dostępu do danych. Unia Europejska jest świadoma zagrożeń dla cyberbezpieczeństwa, stąd Parlament przyjął nową dyrektywę w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej UE, w tym ochrony istotnych sektorów, takich jak między innymi administracja publiczna.

Legal aspects of cybersecurity in public administration

Summary

EU Cybersecurity Agency reports say that public administration is the sector which stands the greatest risk of digital attacks. The number of incidents reported is growing all the time. The Covid-19 pandemic and the resulting spread of remote work as well as the war in Ukraine have aggravated this threat very significantly, especially as hackers are using malware like ransomware, social engineering, data access denial, and other types of malicious software on a large scale. The European Union is aware of these threats to cybersecurity, which is why the European Parliament has adopted a new directive on measures for a high common level of cybersecurity across the EU, including the protection of important sectors such as public administration.

Słowa kluczowe: cyberbepieczeństwo; administracja publiczna; cyberzagrożenia; dyrektywa NIS 2.
Keywords: cybersecurity; public administration; cyber threats; the NIS2 Directive.

Literatura

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018, s. 21-65.

Cichosz J., *Kierunki działań instytucji europejskich na rzecz podnoszenia poziomu bezpieczeństwa podmiotów państwowych i niepaństwowych w cyberprzestrzeni – wybrane przykłady*, «Teka Komisji Politologii i Stosunków Międzynarodowych (Teka of Political Science and International Relations)» 13.2/2018, s. 49-63.

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, «Cybersecurity and Law» 2/2019, s. 7-23.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 351-417.

Christou G., *Cybersecurity in the European Union*, London 2016, s. 119-143.

Fleszer D., Rogacka-Łukasik A., *Europejskie podstawy prawne ochrony informacji*, «Studia Prawnicze KUL» 78.2/2019, s. 57-76.

Radoniewicz F., *Komentarz do art. 2*, [w:] *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 28-52.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Warszawa 2017, s. 28-29.

Rosati P., Gogol F., Lynn T., *Cyber-security incidents and audit quality*, «European Accoutng Review» 29/2020, s. 1-28.

Szpor G., *Komentarz do art. 2*, [w:] *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, s. 39-58.

Toumi M., *Zmiany w strukturze centralnej administracji publicznej w świetle ustawy o Krajowym Systemie Cyberbezpieczeństwa z 2018 r.,* «Przegląd Prawa Konstytucyjnego» 60.2/2021, s. 325-339.

Warchoł A., *Pojęcie cyberprzestrzeni w strategiach bezpieczeństwa państw członkowskich Unii Europejskiej*, «Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate» 9.4/2019, s. 96-107.

Wilbrandt-Gotowicz M., *Komentarz do art. 5*, [w:] *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, s. 79-100.

Wilbrandt-Gotowicz M., *Wielopostaciowość form działania administracji publicznej na przykładzie wymogu implementacji dyrektywy 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*, «Opolskie Studia Administracyjno-Prawne» 4.1/2018, s. 169-174.