UCHWAŁA nr 10

RADY do SPRAW CYFRYZACJI

z dnia 8 lutego 2021 roku

dotycząca projektu dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, tzw. “Dyrektywy NIS 2” (ang. Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148).

W związku z konsultacjami projektu „Dyrektywy NIS2”, prowadzonymi przez Kancelarię Prezesa Rady Ministrów, na podstawie art. 17 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 17 Ministra Cyfryzacji z dnia 24 czerwca 2020 r. w sprawie ustanowienia regulaminu Rady do Spraw Cyfryzacji (Dz. Urz. z 2020 r. poz. 19), uchwala się, co następuje:

Projekt Dyrektywy NIS 2 należy postrzegać w szerszej perspektywie związanej z projektem nowej Strategii Cyberbezpieczeństwa – „Zaufanie i bezpieczeństwo w centrum cyfrowej dekady” (ang. The EU’s Cybersecurity Strategy for the Digital Decade), w której m.in. poszukuje się możliwych do wdrożenia przez UE rozwiązań legislacyjnych, po to aby wzmocnić jej możliwości, kompetencje i zasoby, i w konsekwencji zbliżyć się do osiągnięcia satysfakcjonującego poziomu suwerenności technologicznej. Innym integralnym elementem w krajobrazie proponowanych zmian legislacyjnych, jest projekt dyrektywy o odporności infrastruktury krytycznej (ang. Directive on the resilience of critical entities), której treść również została poddana publicznej konsultacji.

W uzasadnieniu projektu „Dyrektywy NIS 2” czytamy m.in.:

„Unijne przepisy dotyczące bezpieczeństwa sieci i systemów informatycznych (NIS) są podstawą jednolitego rynku cyberbezpieczeństwa. Komisja proponuje reformę tych zasad zgodnie z projektem zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji w celu podniesienia poziomu odporności cybernetycznej, zarówno sektora publicznego, jak i prywatnego, które pełnią ważną funkcję dla gospodarki i społeczeństwa.”

„Dyrektywa NIS 2” ma za zadanie zreformować przepisy dotyczące bezpieczeństwa sieci oraz systemów informatycznych. Ma pomóc w budowie wysokiego poziomu cyberbezpieczeństwa w krytycznych sektorach publicznych i prywatnych, takich jak ochrona zdrowia i jej placówki (np. szpitale, laboratoria medyczne), sieci energetyczne, koleje, administracja publiczna, a także

infrastruktura, i ich usługi, a więc znacznie rozszerza krąg podmiotów nią objętych w stosunku do tzw. „Dyrektywy NIS”.

Popieramy, z pewnymi zastrzeżeniami, generalny kierunek objęcia regulacją kluczowych sektorów, a w szczególności sektora telekomunikacyjnego oraz sektora administracji publicznej, we wspólnych ramach dyrektywy NIS 2.

Jesteśmy zdania, że pozwoli to na tworzenie spójnego systemu cyberbezpieczeństwa, zarówno na poziomie UE, jak i w wymiarze krajowym.

Włączenie telekomunikacji, czy szerzej sektora komunikacji elektronicznej, do jednolitego systemu prawnego w skali całej UE jest ważne z kilku kluczowych powodów:

1. Takie rozwiązanie jest zgodne z generalną tendencją rozwoju rynku wynikającą z coraz szerszego wykorzystywania technologii IT w telekomunikacji (efekt konwergencji technologicznej). To telekomunikacja jest dzisiaj dostawcą Internetu, który jest bazą niezbędną do świadczenia wielu strategicznych usług sieciowych, jak np. computing cloud. Rośnie także rola oprogramowania w budowie usług i systemów telekomunikacyjnych. Codziennością jest zjawisko przenikania się mediów. Nieuzasadnionym jest więc rozdzielenie warstwy usług od regulacji infrastruktury telekomunikacyjnej, na której te usługi są „usadowione”. Strategia obrony przed cyberatakami musi być kompleksowa i polegać na ochronie zarówno sieci, jak systemów IT, aż po urządzenia końcowe**.** Dotychczasowy stan prawny zarówno w Dyrektywie NIS, jak i w jej implementacji w polskiej ustawie o Krajowym Systemie Cyberbezpieczeństwa, powodował stan niepewności. Dyrektywa NIS wyłączała przedsiębiorców telekomunikacyjnych na podstawie art. 1 ust. 2 pkt 1 w zakresie wymogów dot. bezpieczeństwa i zgłaszania incydentów, a system prawny UE przewidywał dla nich odrębną regulację dot. bezpieczeństwa i integralności sieci. To paradoksalna sytuacja, bowiem w gruncie rzeczy Dyrektywa NIS dotyczyła „bezpieczeństwa”, a bez bezpieczeństwa warstwy sieciowej, bezpieczeństwo usługi jest w wielu wypadkach niemożliwe do zrealizowania. Ta niemoc precyzyjnej delimitacji wskazuje, że nie da się stworzyć spójnego systemu cyberbezpieczeństwa bez udziału sektora telekomunikacji i sektora dostawców usług dostępu do Internetu.
2. Na wymienione zagrożenia wskazywała już jesienna debata nad projektem nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), która przewidywała szereg instrumentów obejmujących wszystkie sektory, w tym i telekomunikację. Obydwa systemy się przenikają i np. najwięksi polscy operatorzy telekomunikacyjni obecnie nie podlegają regulacji Dyrektywy NIS i ustawy o KSC, w zakresie w jakim świadczą usługi telekomunikacyjne, a jednocześnie podlegają, jeśli świadczą inne usługi uznane za usługi kluczowe.

3. Zwracamy również uwagę, że system raportowania nakładany na operatorów telekomunikacyjnych powinien być jednolity, bez dublowania zgłoszeń tych samych incydentów na podstawie regulacji ogólnej i sektorowej, a w zakresie obowiązków powinien uwzględniać realne możliwości, zwłaszcza firm - przedsiębiorców telekomunikacyjnych z sektora MŚP. Uregulowanie w „Dyrektywie NIS 2" rozwiązań prawnych dotyczących cyberbezpieczeństwa sektora telekomunikacyjnego i dostawców usług dostępu do Internetu jest jak najbardziej właściwe.

Postulat dotyczący objęcia Dyrektywą NIS 2 podmiotów administracji publicznej wymaga szczególnej analizy. W proponowanej redakcji obowiązkami z Dyrektywy NIS 2 mają być objęte podmioty publiczne posiadające osobowość prawną. Oznacza to, że nie będą podlegały jej postanowieniom niektóre jednostki administracji publicznej, nieposiadające osobowości prawnej. Regulacji będą podlegały jednostki samorządu terytorialnego - gminy, powiaty i województwa. Podzielamy pogląd, że cyberbezpieczeństwo podmiotów publicznych powinno ulec zdecydowanej poprawie, ale należy w tym kontekście zbadać możliwości zapewnienia odpowiednich środków finansowych na realizację nowych zadań dla samorządów. Jest to szczególnie ważne z dwóch powodów: obecnie znacząca część realizowanych przez samorządy obowiązków to zadania zlecone z zakresu administracji rządowej, jak np. prowadzenie rejestrów publicznych, ewidencja ludności, rejestracja stanu cywilnego, pojazdów i kierowców itd., a dotacje przekazywane z budżetu w wielu przypadkach nie pokrywają wydatków na ich wykonanie; ponadto największym i corocznie rosnącym obciążeniem finansowym JST jest szybko i od kilku lat narastająca luka finansowa między wydatkami a subwencją oświatową, drastycznie pogarszająca wynik bieżący budżetów samorządowych, a więc i możliwości inwestycyjne.

Zwracamy uwagę, że dla systemowego zapewnienia cyberbezpieczeństwa UE, tj. ścigania i karania osób i organizacji odpowiedzialnych za naruszenia systemów teleinformatycznych, należy wprowadzić nowe, bardziej efektywne środki, w tym dokonać przeglądu dyrektywy 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW. Trzeba też uwzględnić tę problematykę w zapisach nowej Strategii Cyberbezpieczeństwa UE. Wdrożeniu dyrektywy NIS 2 powinna towarzyszyć poważna dyskusja nt. przepisów karnych oraz wzmocnienia organów ścigania na poziomie UE oraz krajowym. Należy też dążyć do wyeliminowania czynników ułatwiających ataki i utrudniających ustalenie tożsamości sprawców naruszeń. O rosnącej skali zjawisk związanych z cyberprzestępczością świadczy np. liczba cyberataków w UE, w tym na Polskę (np. dynamika zjawiska w oparciu o dane dotyczące zgłoszonych incydentów do CSIRT NASK oraz CSIRT ABW). W 2018 r. zespół CERT Polska przyjął 19 439 zgłoszeń i odnotował 3 739 incydentów bezpieczeństwa, co daje wzrost liczby incydentów o 17,5% w stosunku do 2017 r. W 2019 r. CERT Polska (CSIRT NASK) zarejestrował 6 484 incydentów. Oznacza to lawinowy wzrost liczby incydentów – o 73 % w porównaniu z 2018 r. Tylko w I poł. 2020 r. do CSIRT NASK wpłynęło już 16 689 zgłoszeń, zaś 5 205 uznano za incydenty**.** Alarmujące są również dane zaprezentowane w

raportach CSIRT ABW. W 2018 r. CSIRT ABW odnotował 31 865 zgłoszeń, z których 6 236 uznano za incydenty, zaś w 2019 r. odnotował on 226 914 zgłoszeń, z których 12 405 uznano za incydenty. Zgodnie z przedstawianymi w raportach analizami incydentów znaczną ich większość stanowią przestępstwa.

Lockdown i związane z nim przejście do zdalnej pracy, edukacji czy realizacji zadań publicznych online uwypukliło dodatkowo problemy cyberbezpieczeństwa. Pandemia COVID-19 jest okresem wzmożonej aktywności cyberprzestępców, którzy niezwykle szybko dostosowali się do nowych warunków i dopasowali scenariusze ataków do bieżącej sytuacji pandemicznej. Wymuszone przejście do zdalnej realizacji wielu procesów doprowadziło również do obniżenia poziomu bezpieczeństwa świadczonych usług, w tym w szczególności do słabszej weryfikacji tożsamości klientów. Sprzyja to nie tylko kradzieży tożsamości, ale również dokonywaniu wyłudzeń przy pomocy pozyskanych danych. Obserwowane negatywne zjawiska skłaniają do podjęcia pilnych działań mających na celu przeciwdziałanie kradzieży tożsamości, gromadzenie danych niezbędnych do ustalenia przebiegu i sprawców incydentów oraz pociągnięcia ich do odpowiedzialności karnej. Dlatego celowe jest wprowadzenie obowiązków związanych z przechowywaniem logów dostępowych oraz danych abonentów usług świadczonych drogą elektroniczną, wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług elektronicznych, zmiany regulacji karnej (w tym również podniesienie górnej granicy zagrożenia karnego za przestępstwo z art. 267 § 1 kk, tzw. hacking, aktualnie wynoszącej 2 lata pozbawienia wolności).

Tym samym, implementacja Dyrektywy NIS 2 może stać się przyczynkiem do poszerzenia polityki regulacyjnej także o obszar cyberprzestępczości.

Projekt dyrektywy NIS 2 eksponuje również konieczność zapewnienia wiarygodności danych dotyczących abonentów domen. Problem ten podniesiony został w uchwale nr 7 Rady ds. Cyfryzacji z dnia 14.4.2020 r. w sprawie działań mających na celu zapobieganie kradzieży tożsamości. Stanowisko Rady nie stanowiło jednak wystarczającego impulsu do wprowadzenia systemowych zmian w tym zakresie. Projekt nowej dyrektywy w motywie 15 wskazuje, że utrzymywanie i zachowanie wiarygodnego, odpornego i bezpiecznego systemu nazw domen (DNS) odgrywa decydującą rolę w utrzymaniu integralności Internetu oraz ma istotne znaczenie dla jego nieprzerwanego i stabilnego działania. Dlatego też prowadzenie prawidłowych i kompletnych baz danych zawierających nazwy domen i dane rejestracyjne („dane WHOIS") oraz zapewnienie zgodnego z prawem dostępu do takich danych jest niezbędne do zapewnienia bezpieczeństwa, stabilności i odporności systemu nazw domen, co z kolei przyczynia się do wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (motyw 59). Art. 23 projektu dyrektywy NIS 2 nakłada na państwa członkowskie obowiązek zapewnienia, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD z należytą starannością gromadziły i zachowywały dokładne i kompletne dane dotyczące rejestracji nazw domen.

Realizacja tego obowiązku powinna prowadzić do lepszej weryfikacji tożsamości abonentów domeny .pl i nałożenia obowiązków należytej weryfikacji danych przez pośredników. W wielu atakach, jakie miały miejsce w 2020 r., sprawcy wykorzystali nazwy z domeny .pl podszywając się pod banki, portale aukcyjne, dostawców energii, usługi pocztowe czy podmioty świadczące usługi kurierskie. Domeny wykorzystywane w atakach rejestrowane są z podaniem fikcyjnych danych, pochodzących z wycieków lub jawnych rejestrów przedsiębiorców.

Projekt dyrektywy NIS 2 jest wynikiem przeglądu stosowania obecnie obowiązującej dyrektywy NIS i ma być częścią szerszego pakietu obejmującego także odrębne regulacje dla instytucji finansowych (ang. Regulation on Digital Operational Resilience for the financial Sector -"DORA") oraz wspomnianej Resilience of Critical Entities Directive**.** Można powiedzieć, że w obecnym stanie prawnym doszło do rozbieżności między państwami członkowskimi w zakresie będącym przedmiotem regulacji przewidzianych w NIS oraz, że jednym z efektów tej sytuacji jest brak restrykcji w stosunku do podmiotów objętych regulacją, co wpływa negatywnie na poziom cyberbezpieczeństwa. Decyzja o rewizji dotychczasowej dyrektywy wydaje się słuszna. Nowa dyrektywa po jej implementacji ma szansę stać się dyrektywą minimalnej harmonizacji, co nie zamyka państwom członkowskim drogi do przyjmowania dalej idących rozwiązań, zapewniających jeszcze wyższy poziom cyberbezpieczeństwa (na co wskazuje art. 3 projektu). Projekt zakłada powstanie grupy współpracy (art. 12) i sieci CSIRTów (art. 13), a także EU – CyCLONe (European Cyber Crises Liaison Organisation Network) w celu koordynacji cyberincydentów dużej skali i kryzysów (art. 14), co jest kluczowe ze względu na często transgraniczny charakter skutków takich zdarzeń. W kontekście budowy sieci 5G, choć nie wyłącznie, istotne jest wprowadzenie zapisów o skoordynowanej ocenie ryzyk łańcucha dostaw (art. 19, a także pkt 47 motywów) i certyfikacji (art. 21). Istotnym elementem dyrektywy są także rozwiązania dotyczące standaryzacji (art. 22) i wymiany informacji (art. 26). Niewątpliwie obszar tych rozwiązań będzie elementem wpływającym na działania rynkowe. Co prawda Komisja zadecyduje, jakie kategorie podmiotów kluczowych (a status ten mogą posiadać podmioty publiczne, jak i prywatne, realizujące zadania publiczne lub zadania własne) będą miały obowiązek uzyskać certyfikat, jednak nowe obowiązki wynikające z dyrektywy NIS 2 będą wymagały zaangażowania różnych podmiotów w obszarach, które nie były dotychczas objęte taką regulacją. Cyfryzacja i informatyzacja życia gospodarczego spowodowały, że wciąż pojawiają się nowe dziedziny, w których cyberbezpieczeństwo ma kluczowe znaczenie. Stąd także nowe obowiązki dla nowej grupy - podmiotów ważnych (ang. important entities). Należy tu podkreślić, że nie zawsze interes ogólny, publiczny idzie w parze z interesem indywidualnym, gospodarczym. Niezależnie od wielkości, przedsiębiorca zajmujący się świadczeniem usług komunikacji elektronicznej będzie podlegał przepisom wynikającym z dyrektywy NIS 2. Dyrektywa przewiduje także wysokie kary finansowe dla podmiotów nie realizujących obowiązków we właściwy sposób. Kary te mają wynosić do 10 000 000 EUR lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa, w zależności od tego, która kwota

jest wyższa. Poziom tych kar może być szczególnie dotkliwy dla mniejszych przedsiębiorców, którzy dopiero wchodzą do systemu cyberbezpieczeństwa. Być może potrzebna byłaby tu odpowiednia gradacja kar. W kontekście tych zapisów trzeba wskazać, że nowe postanowienia dyrektywy NIS 2 zmierzają do osiągniecia głównego celu regulacji unijnych w tym obszarze, czyli szeroko rozumianej współpracy międzysektorowej na rzecz cyberbezpieczeństwa. Działania państw członkowskich i ich władz publicznych na rzecz cyberbezpieczeństwa, w warunkach wspólnego i jednolitego rynku cyfrowego, muszą wspierać wszyscy jego uczestnicy. To jest obowiązek także przedsiębiorców telekomunikacyjnych i wszelkich innych podmiotów, których funkcjonowanie może wpływać lub już wpływa na zakres cyberbezpieczeństwa. Bez tej współpracy i koordynacji działań nie możemy mówić o bezpiecznej cyberprzestrzeni.

Problematyczne pod względem rozwiązań dotyczących rynku telekomunikacyjnego jest to, że nowelizacja dyrektywy NIS 2 może stwarzać pole do kolizji z przepisami wynikającymi z innych przepisów, m.in. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej**,** gdzie zagadnienia bezpieczeństwa sieci oraz usług telekomunikacyjnych zostały także ustalone, a w praktyce wymogi są realizowane od wielu lat. Jednak należy zaznaczyć, że czymś innym są obowiązki wynikające z regulacji rynku telekomunikacyjnego, a czymś innym obowiązki związane z tworzeniem spójnego i skoordynowanego systemu cyberbezpieczeństwa w systemie administracyjnym państwa. Należy podkreślić, że nowe zadania związane z cyberbezpieczeństwem mogą stać się przyczyną wzrostu kosztów prowadzenia przez zobowiązane podmioty działalności, co w sposób oczywisty może stanowić argument do podniesienia cen usług dla użytkowników końcowych.

Niezależnie od powyższych wątpliwości, z całą pewnością nowa regulacja może służyć zwiększeniu odporności na cyberataki, wspierać systemowo cyberbezpieczeństwo, jeżeli zostanie skutecznie implementowana przez państwa członkowskie.

Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone w trybie obiegowym. Projekt uchwały nr 10 został przesłany członkom Rady 3 lutego 2021 r. z terminem głosowania do dnia 8 lutego 2021 r. W głosowaniu wzięło udział 14 członków Rady, z czego oddano:

- 14 głosów „za" przyjęciem uchwały,
- 0 głosów „przeciw" oraz
- 0 głosów „wstrzymuję się".

Uchwała nr 10 Rady do Spraw Cyfryzacji została przyjęta 8 lutego 2021 roku w głosowaniu jawnym w trybie obiegowym zwykłą większością głosów.

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Izabela	Albrycht	za
2.	Katarzyna	Chałubińska-Jentkiewicz	za
3.	Jan	Czajkowski	za
4.	Krzysztof	Dyki	za
5.	Paweł	Gora	za
6.	Agnieszka	Gryszczyńska	za
7.	Michał	Kanownik	za
8.	Janusz	Kosiński	za
9.	Anna Beata	Kwiatkowska	za
10.	Dariusz	Milka	za
11.	Józef	Orzeł	za
12.	Wiesław	Paluszyński	za
13.	Rafał	Rodziewicz	za
14.	Włodzimierz	Schmidt	za

Przewodniczący Rady
Józef Orzeł
/-podpisano elektronicznie/