Uzasadnienie

1. Wstęp

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), zwana dalej „ustawą o KSC", tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. Ustawa o KSC jest implementacją 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 (Dz. Urz. UE. L 2016/1148 z 19.07.2016), zwanej dalej „dyrektywą NIS".

Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do ustawy o KSC. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa, zwany dalej „organem właściwym", który odpowiada za identyfikację i wyznaczanie operatorów usług kluczowych oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy o KSC w danym sektorze.

Obecnie, ani przedsiębiorcy telekomunikacyjni ani dostawcy usług zaufania nie są podmiotami krajowego systemu cyberbezpieczeństwa.

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego, zwanych dalej „CSIRT". Do zadań zespołów CSIRT należy m.in. klasyfikowanie incydentów jako krytyczne. Ustawa o KSC usankcjonowała istnienie trzech zespołów na poziomie krajowym – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, zwanym dalej „NASK–PIB") oraz CSIRT MON (prowadzonego przez Ministra Obrony Narodowej). Zespoły CSIRT współpracują ze sobą w ramach Zespołu do spraw incydentów krytycznych.

1.1. Sektorowe zespoły cyberbezpieczeństwa

Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za wsparcie obsługi incydentów u operatorów usług kluczowych w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko dwa takie zespoły, tj. CSIRT KNF (zespół dla sektora finansowego), funkcjonujący przy Komisji Nadzoru Finansowego[1)], oraz Centrum e-Zdrowie (w sektorze ochrony zdrowia).

1.2. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, zwany dalej „Pełnomocnikiem", jest odpowiedzialny za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu albo podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy zarówno analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa (dokonywana na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT), jak i nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

1.3. Kolegium do Spraw Cyberbezpieczeństwa

Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium", jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje sprawy planowane do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 110 ust. 2 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221). Przewodniczącym Kolegium jest Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych, Szef Kancelarii Prezesa Rady Ministrów, Szef Biura Bezpieczeństwa

[1)] https://www.knf.gov.pl/dla_rynku/CSIRT_KNF.

Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK–PIB. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów, w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa, może wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa.

1.4. Potrzeba i cele projektu ustawy

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 L 2022/2555 z 27.12.2022), zwana dalej „dyrektywą NIS 2", utworzyła nowe ramy systemu zapewnienia cyberbezpieczeństwa w Unii Europejskiej. Wprowadziła nowe zadania państw członkowskich w tym obszarze, rozszerzyła zakres podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa oraz zredefiniowała zadania organów Unii Europejskiej w tym obszarze. Ponadto rozszerzeniu uległ katalog sektorów objętych dyrektywą NIS 2 – obok sektorów energii, transportu, zdrowia, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę, infrastruktury cyfrowej, w dyrektywie NIS 2 dodano następujące sektory: ścieki, zarządzanie ICT, przestrzeń kosmiczną, pocztę, produkcję, produkcję i dystrybucję chemikaliów, produkcję i dystrybucję żywności. Dyrektywa NIS 2 zastąpiła dotychczasowy podział na operatorów usług kluczowych i dostawców usług cyfrowych określony w NIS, na podmioty kluczowe i podmioty ważne. Dyrektywa NIS 2 nakłada również szereg obowiązków na podmioty kluczowe i podmioty ważne. Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Zmiany te zostały wprowadzone w związku z szybko postępującą transformacją cyfrową i siecią wzajemnych połączeń w społeczeństwie, w tym w kontekście wymiany transgranicznej, sieci i systemy informatyczne stały się zasadniczym elementem codziennego życia. Zmiana ta doprowadziła do ewolucji krajobrazu cyberzagrożeń, przynosząc nowe wyzwania, które wymagają dostosowanych, skoordynowanych i innowacyjnych reakcji we wszystkich państwach członkowskich. Liczba, skala, zaawansowanie, częstotliwość oraz wpływ incydentów stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie incydenty mogą utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników oraz powodować poważne szkody dla gospodarki i społeczeństw.

Są one również efektem analizy funkcjonowania dyrektywy NIS, która dotychczas regulowała te zagadnienia. Uznano, że dotychczasowe środki w tym zakresie nie są adekwatne do obecnej skali wyzwań z jakimi można zetknąć się w cyberprzestrzeni. Projektowana ustawa określa mechanizmy skutecznej współpracy między odpowiedzialnymi organami w poszczególnych sektorach gospodarki, a także określa nowe obowiązki w zakresie cyberbezpieczeństwa, jak i środki ich egzekwowania.

Ustawa o KSC nie spełnia wymogów dyrektywy NIS 2, w związku z czym należy ją wdrożyć do porządku krajowego do dnia 17 października 2024 r. – termin wynika z dyrektywy.

Pojawianie się nowych cyberzagrożeń, jak również szybki wzrost katalogu usług publicznych dostępnych online, powodują, że instytucje publiczne, jak i podmioty prywatne odpowiedzialne za cyberbezpieczeństwo będą zmuszone poświęcać coraz więcej środków na zapewnienie cyberbezpieczeństwa. Zmieniająca się sytuacja międzynarodowa oraz konieczność dostarczenia usług dużej grupie nowych klientów sprawia, że niezbędne jest dalsze wzmacnianie podmiotów krajowego systemu cyberbezpieczeństwa. Tą sytuację uwidaczniają statystyki zespołu CSIRT NASK. W 2022 r. do zespołu CSIRT NASK zgłoszono ponad 39 000 incydentów cyberbezpieczeństwa, a w 2023 r. ponad 75 000 incydentów cyberbezpieczeństwa. Dyrektywa NIS 2 i przepisy ją implementujące są odpowiedzią na dynamicznie zmieniającą się sytuację w cyberprzestrzeni.

Zauważono również, że uprawnienia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa są niewystarczające w stosunku do zadań, które organ ten musi wypełniać. Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa brakuje skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa. W przeciwieństwie do innych

Pełnomocników Rządu, nie ma on uprawnień do żądania niezbędnych informacji od organów administracji rządowej, możliwości powoływania zespołów problemowych, czy zlecania badań. Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa brakuje również środka prawnego, który umożliwiłby wydawanie rekomendacji o charakterze technicznym (w tym zakresie – Narodowych Standardów Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią") i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa, w trakcie procesu zarządzania ryzykiem.

Jak wyżej wskazano, do tej pory zostały utworzone tylko dwa sektorowe zespoły cyberbezpieczeństwa – CSIRT KNF i CSIRT Centrum e-Zdrowie. W pozostałych sektorach gospodarki brakuje zespołów wspierających przedsiębiorców w reagowaniu na incydenty. Utworzenie tych zespołów przewiduje inwestycja C3.1.1 KPO Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo, planowana jest realizacja projektu pn. „Utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)". Celem nowelizacji ustawy o KSC jest wprowadzenie uwarunkowań prawnych skutecznego funkcjonowania CSIRT sektorowych.

Coraz większe znaczenie dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe są uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych generacji). Komisja Europejska wielokrotnie, m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie powyższego znajduje odzwierciedlenie w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanym jako 5G Toolbox[2)]. Zestawienie to obejmuje zarówno rozwiązania o charakterze strategicznym, technicznym, jak i o charakterze wspierającym. Celami 5G Toolbox są po pierwsze bezpieczeństwo sieci 5G, a po drugie uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox definiuje zestaw środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków, niezbędne do ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą podstawą Jednolitego

[2)] *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures,* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Rynku Cyfrowego UE. Wśród opisanych w 5G Toolbox środków strategicznych, technicznych i wspierających są środki o charakterze:

- strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym w zakresie oceny bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,
- technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – czego odzwierciedleniem są na gruncie prawa krajowego uprawnienia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego, CSIRT MON, CSIRT NASK, CSIRT GOV wynikające z art. 33 ustawy o KSC,
- wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa.

Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox w Polsce.

1.5 Zgodność projektu ustawy o KSC z celami strategicznymi Rady Ministrów

Projekt ustawy służy realizacji celów Strategii, jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt ustawy realizuje także cel szczegółowy Strategii odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto projekt ustawy realizuje cele Strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

1.6. Skutki gospodarcze

Celem projektowanych zmian jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Wprowadzane w projekcie ustawy rozwiązania zobowiązują m.in. przedsiębiorców w poszczególnych sektorach gospodarki do dbania o cyberbezpieczeństwo. Skutkiem projektowanych przepisów może być konieczność poniesienia dodatkowych kosztów związanych z dostosowaniem się poszczególnych podmiotów krajowego systemu cyberbezpieczeństwa do wymogów wynikających z ustawy o KSC. Należy zauważyć, że wielu przedsiębiorców już obecnie posiada systemy zarządzania bezpieczeństwem informacji. Dzięki dalszemu inwestowaniu przez podmiot we własne cyberbezpieczeństwo zyskuje on zaufanie podmiotów, którym świadczy usługi i potencjalnych kontrahentów.

Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom zwiększyć skuteczność działań podejmowanych przez przedsiębiorców w zakresie cyberbezpieczeństwa w ich działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.

1.7. Skutki społeczne

Nałożenie nowych obowiązków z zakresu cyberbezpieczeństwa na większą liczbę podmiotów przyczyni się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększy to pewność ciągłości usług. Polepszy się ochrona danych osobowych przetwarzanych przez podmioty ważne i podmioty kluczowe. Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego.

Powołanie CSIRT sektorowych pozwoli na utworzenie jednostek, dzięki którym usprawnione zostanie funkcjonowanie i zwiększona skuteczność systemu reagowania na incydenty. Ponadto, dzięki powołaniu CSIRT sektorowego, w każdym sektorze powstanie baza wiedzy o cyberzagrożeniach i podatnościach danego sektora. Funkcjonowanie CSIRT sektorowych wpłynie na skrócenie czasu obsługi incydentów w sektorze, które będą obsługiwane z uwzględnieniem szczególnych uwarunkowań danego sektora.

1.8. Skutki finansowe

Tworzenie nowych struktur w ramach krajowego systemu cyberbezpieczeństwa będzie wymagało dodatkowych nakładów finansowych. Jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są coraz częstsze i bardziej zaawansowane.

Szkody powstałe wskutek tych działań (np. zaszyfrowanie danych, wykradzenie danych, uniemożliwienie lub utrudnienie świadczenia usług publicznych) są bardzo poważne i często mają również istotny wymiar finansowy. Inwestycja w dostosowanie krajowego systemu cyberbezpieczeństwa do wyzwań wynikających z postępującej gwałtownie cyfryzacji pozwoli ograniczyć prawdopodobieństwo powstania tych szkód, a w przypadku ataków – znacząco zmniejszyć ich negatywne skutki. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Ze względu na odwołania w samej dyrektywie NIS 2 do 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 (Dz. Urz. UE L 2022/2557 z 27.12.2022), zwanej dalej „dyrektywą CER", oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 2022/2554 z 27.12.2022), zwanego dalej „rozporządzeniem DORA" – projekt ustawy będzie ulegał zmianom, głównie w obszarze siatki pojęciowej, mającym na celu dostosowanie projektu do regulacji transponujących rozporządzenie DORA[3)] oraz dyrektywę CER[4)].

2. Uzasadnienie poszczególnych przepisów

2.1. Zmiany w przepisach ogólnych

2.1.1. Definicje

Zmiany w zakresie definicji ustawowych wynikają ze zmian w siatce pojęciowej jakie wprowadziła dyrektywa NIS 2. W związku z tym konieczna była zmiana części definiowanych pojęć, usunięcie przestarzałych terminów oraz dodanie nowych. Wprowadzone zmiany zapewnią spójność siatki pojęciowej wykorzystywanej we wszystkich krajach Unii Europejskiej.

Z uwagi na uwzględnienie w projekcie ustawy kwestii obowiązków rejestrów nazw domen najwyższego poziomu oraz podmiotów świadczących usługi rejestracji nazw domen to zaszła konieczność wprowadzenia definicji abonenta nazwy domeny. Tworząc tą definicję odwzorowano stosunki prawne, jakie zachodzą przy rejestracji domeny. Abonentem jest więc podmiot (osoba fizyczna, osoba prawna, ułomna osoba prawna), który jest stroną umowy o utrzymywanie nazwy domeny (por. https://www.dns.pl/regulamin_nazw_domeny_pl) zawartej z rejestrem nazw domen najwyższego poziomu (TLD) za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen.

Wprowadzono definicję CSIRT sektorowego – jest to zespół reagowania na incydenty bezpieczeństwa komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora.

[3)] Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego (UC11) https://legislacja.rcl.gov.pl/projekt/12384252.

[4)] Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw https://legislacja.rcl.gov.pl/projekt/12386961.

Definicja adresu do doręczeń elektronicznych okazała się konieczna, ponieważ pojawia się w kilku przepisach projektu ustawy. Tworząc tą definicję odesłano do ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045).

Z uwagi na to, że dotychczasowe pojęcie „cyberbezpieczeństwa" zostaje zastąpione „bezpieczeństwem systemów informacyjnych", to odpowiednio dostosowuje się definicję incydentu – jest to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.

Definicja cyberbezpieczeństwa odnosi się do definicji zawartej w unijnym akcie o cyberbezpieczeństwie. Tak samo jest przy definicji cyberzagrożenia.

Zaszła potrzeba zdefiniowania szeregu rodzajów podmiotów, które funkcjonują w sektorze infrastruktury cyfrowej. Dostawca sieci dostarczania treści jest potocznie znany jako CDN – content delivery network provider. Nawiązując do dyrektywy NIS 2 wskazano, że jest to osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług, jednakże z wyłączeniem przedsiębiorców komunikacji elektronicznej. Wielu przedsiębiorców komunikacji elektronicznej tworzy własne CDN, stąd też uznano, że warto tutaj rozgraniczyć te definicje. Przedsiębiorcy komunikacji elektronicznej i świadczone przez nich usługi podlegają reżimowi ustawy – ich usługi CDN też będą podlegać pod reżim ustawy jako usługi komunikacji elektronicznej.

Dostawca internetowej platformy handlowej to osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która dostarcza internetową platformę handlową w rozumieniu art. 2 pkt 8 ustawy z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2023 r. poz. 2759 oraz z 2024 r. poz. 1222).

Z uwagi na treść dyrektywy NIS 2 zaszła konieczność uzupełnienia definicji incydentu poważnego. Wskazano, że jest to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny – a nie jak do tej pory świadczenia usługi kluczowej przez operatora usługi kluczowej. Ponadto incydentem poważnym będzie też taki, który powoduje straty finansowe dla podmiotu kluczowego i podmiotu ważnego albo wpływa na inne podmioty – osoby

fizyczne, osoby prawne i ułomne osoby prawne – w taki sposób, że wywołuje szkodę materialną albo niematerialną.

Zgodnie z dyrektywą NIS 2 dodano także definicję incydentu w cyberbezpieczeństwie na dużą skalę – jest to incydent, którego skutki przekraczają możliwości reagowania państwa lub ma poważny wpływ na inne państwo członkowskie. Zakres tego pojęcia może krzyżować się z definicją incydentu krytycznego, jednakże jest to celowe działanie.

Za dyrektywą NIS 2 dodano także definicje dostawcy sieci dostarczania treści, dostawcy usług chmurowych, dostawcy usług DNS, dostawcy usługi ośrodka przetwarzania danych, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy wyszukiwarki internetowej, platformy sieci usług społecznościowych, czy podmiotu świadczącego usługi rejestracji nazw domen.

Nowością jest definicja dostawcy – tutaj projekt ustawy odwołuje się do art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 765/2008 z 13.08.2008 r.), zwanego dalej „rozporządzeniem 765/2008". Zgodnie z rozporządzeniem 765/2008 dostawcą jest:

– producent – każda osoba fizyczna lub prawna, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i oferuje ten produkt pod własną nazwą lub znakiem towarowym,

– upoważniony przedstawiciel – osoba fizyczna lub prawna mająca siedzibę w Unii Europejskiej, posiadająca pisemne pełnomocnictwo od producenta do występowania w jego imieniu w zakresie określonych zadań w odniesieniu do obowiązków producentów wynikających z odpowiedniego prawodawstwa wspólnotowego,

– importer – każda osoba fizyczna lub prawna, mająca siedzibę w Unii Europejskiej, wprowadzająca na rynek wspólnotowy produkt z kraju trzeciego

lub

– dystrybutor – każda osoba fizyczna lub prawna w łańcuchu dostaw, inna niż producent lub importer, która udostępnia produkt na rynku.

Definicja jest wprowadzana w związku z przepisami dotyczącymi systemu zarządzania bezpieczeństwem informacji, a także przepisami odnoszącymi się do postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Uchyla się odrębne definicje incydentu istotnego i incydentu w podmiocie publicznym, ponieważ podmioty kluczowe i podmioty ważne będą zgłaszały incydenty klasyfikowane jako incydenty poważne.

Dyrektywa NIS 2 wyraźnie wskazuje na odpowiedzialność zarządu podmiotu kluczowego i podmiotu ważnego w realizacji obowiązków z zakresu cyberbezpieczeństwa. Dlatego konieczne jest wyraźne zdefiniowanie kto jest kierownikiem podmiotu kluczowego lub podmiotu ważnego w rozumieniu ustawy o KSC. Definicja odsyła więc do pojęcia kierownika jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598 oraz z 2024 r. poz. 619) kierującego podmiotem kluczowym lub podmiotem ważnym. Takie odesłanie zapewni spójność w systemie prawa – pojęcie kierownika jednostki jest znane i ugruntowane w orzecznictwie i doktrynie. Ponadto na gruncie ustawy z dnia z dnia 29 września 1994 r. o rachunkowości, kierownik jednostki odpowiada za szereg obowiązków dotyczących rachunkowości – podobna sytuacja będzie miała miejsce w przypadku cyberbezpieczeństwa.

Definicja organizacji badawczej odwołuje się do osoby prawnej albo ułomnej osoby prawnej prowadzącej działalność wskazaną w ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742, z późn. zm.[5)]), tj. badania aplikacyjne oraz prace rozwojowe.

Konieczna jest zmiana definicji podatności, która obecnie odwołuje się do pojęcia systemu informacyjnego. W projekcie ustawy będzie to właściwość produktu ICT lub usług ICT, które mogą być wykorzystane przez cyberzagrożenie, co zapewni zgodność z dyrektywą NIS 2.

W definicji platformy sieci usług społecznościowych wskazano, że jest to usługa świadczona drogą elektroniczną, która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń, co oddaje sens zawarty w dyrektywie NIS 2.

Wprowadza się definicję podmiotu publicznego – w tym zakresie odsyła się do załącznika do projektu ustawy do sektora podmiotów publicznych. Będą to podmioty, które do tej pory były traktowane przez ustawę o KSC jako podmioty publiczne.

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1088, 1234, 1672, 1872 i 2005 oraz z 2024 r. poz. 124, 227 i 1089.

Definicja potencjalnego zdarzenia dla cyberbezpieczeństwa jest konieczna, ponieważ pojęcie to występuje w dyrektywie NIS 2. Państwa członkowskie sprawozdają się z liczby zgłoszonych potencjalnych zdarzeń dla cyberbezpieczeństwa. Jest to więc zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Zgłaszanie takich zdarzeń do zespołów CSIRT jest nieobowiązkowe.

Prawo unijne przewiduje likwidację odrębnych obowiązków regulacyjnych z zakresu cyberbezpieczeństwa dla sektora telekomunikacji. Dostawcy podlegają takim samym wymogom z zakresu cyberbezpieczeństwa, jak inne podmioty kluczowe. Dlatego konieczne jest wprowadzenie definicji do ustawy o KSC. W projekcie ustawy wprowadza się pojęcie przedsiębiorcy komunikacji elektronicznej. Na ten zbiór składają się przedsiębiorcy telekomunikacyjni prowadzący działalność regulowaną oraz podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów – będą to podmioty świadczące swoje usługi za pośrednictwem internetu, które mogą konkurować z usługami telekomunikacyjnymi. Przykładami takich usług, oznaczanych jako OTT-1, są usługi komunikatorów internetowych czy poczty elektronicznej.

Definicje przedsiębiorcy telekomunikacyjnego, przedsiębiorcy komunikacji elektronicznej oraz usług komunikacji interpersonalnej niewykorzystującej numerów znajdują się w ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej.

Dotychczasową definicję systemu informacyjnego uzupełnia się o wskazanie, że może to być również urządzenie lub grupa połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych. W ten sposób projektodawca chce wyeliminować wątpliwości, co do tego czy systemy OT mieszczą się w ramach obecnej definicji systemu informacyjnego czy nie.

Uchyla się definicję usługi kluczowej, ponieważ na gruncie dyrektywy NIS 2 nie występuje to pojęcie. Zostało ono bowiem przeniesione do dyrektywy CER.

Dyrektywa NIS 2 powołuje się na pojęcie podmiotu krytycznego w rozumieniu dyrektywy CER, która definiuje to pojęcie w art. 2 pkt 1. W związku z tym należało zdefiniować to pojęcie również w projekcie ustawy. Dyrektywa CER wciąż nie została wdrożona do polskiego porządku prawnego. Toczy się proces legislacyjny projektu ustawy wdrażającej tę dyrektywę. Mając świadomość, że nie odwołuje się do przepisów aktów niedających się bezpośrednio stosować zrobiono to wyjątkowo. W sytuacji gdy będzie możliwość odwołania się

do przepisów transponujących dyrektywę CER to definicja ta zostanie niezwłocznie zmieniona.

Definicja zagrożenia cyberbezpieczeństwa stała się zbędna w związku z dodaniem definicji cyberzagrożenia, stąd należy ją usunąć.

Wprowadza się definicję poważnego cyberzagrożenia – jest to cyberzagrożenie, które może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych poprzez wywołanie szkody materialnej lub niematerialnej. Jest to więc kwalifikowana postać cyberzagrożenia – jego zaistnienie będzie powodowało obowiązek poinformowania o środkach, które mogą podjąć użytkownicy podmiotów kluczowych i podmiotów ważnych celem zabezpieczenia się przed jego skutkami.

Dyrektywa NIS 2 posługuje się pojęciem usług w szerokim znaczeniu – odnosi się ona także do podmiotów publicznych. W polskim systemie prawnym podmioty publiczne realizują zadania publiczne. Aby uniknąć wątpliwości w przepisach ogólnych wskazuje się wprost, że w przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot. Oczywiście zdarza się, że podmiot publiczny, np. instytucja gospodarki budżetowej, świadczy komercyjne usługi, które nie są zadaniami publicznymi. Jednakże dla celów ustawy o KSC to uogólnienie jest konieczne, w przeciwnym razie konieczne byłoby utrzymanie dotychczasowego pojęcia „incydentu w podmiocie publicznym" czy też wprowadzenia odrębnych progów dla incydentu związanego z zadaniami publicznymi.

2.1.2. Działania w ramach obsługi incydentów

Przepisy projektu ustawy przesądzają, że w ramach obsługi incydentu dotknięty nim podmiot może wykrywać źródło ataku oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów. Równocześnie te działania mogą prowadzić do ewentualnego naruszenia uprawnień innych podmiotów. Do tej pory istniały wątpliwości na ile takie działania mogą być podejmowane. W związku z tym konieczne jest wprowadzenie wyraźnej podstawy prawnej do takich działań.

2.2. Podmioty kluczowe i podmioty ważne

Dyrektywa NIS 2 odeszła od pojęć operatorów usług kluczowych i dostawców usług cyfrowych, które były podstawą krajowego systemu cyberbezpieczeństwa. Obecnie obowiązki

wynikające z dyrektywy NIS 2 kierowane są do podmiotów kluczowych oraz podmiotów ważnych.

W związku ze zmianą siatki pojęciowej wprowadzonej w dyrektywie NIS 2 konieczne było dostosowanie do niej przepisu określającego podmioty krajowego systemu cyberbezpieczeństwa.

Przepisy definiują też, które podmioty są podmiotami kluczowymi i podmiotami ważnymi oraz określa procedurę ich rejestracji.

Dyrektywa NIS 2 dotyczy przede wszystkim średnich przedsiębiorstw w rozumieniu zalecenia Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. Urz. UE L 124 z 20.5.2003, str. 36). Zalecenie Komisji (UE) jest aktem prawa miękkiego i zgodnie z zasadami techniki prawodawczej nie odwołuje się do tego rodzaju aktów. Dlatego ustawa o KSC odwołuje się do progów średniego przedsiębiorstwa określonych w załączniku I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 651/2014 z 26.06.2014 r.), zwane dalej „rozporządzeniem 651/2014/UE", które jest identyczne z zaleceniem Komisji (UE). W tym przypadku nie jest możliwe odwołanie do ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 266 i 1222), ponieważ jego przepisy nie odpowiadają ww. zaleceniu.

Podstawowa różnica między podmiotem kluczowym a podmiotem ważnym wyraża się w kwestiach nadzorczych. Wobec podmiotu kluczowego można prowadzić czynności nadzorcze *ex ante* i *ex post.* Wobec podmiotu ważnego czynności nadzorcze można prowadzić tylko *ex post.* Pozostałe obowiązki podmiotów kluczowych i podmiotów ważnych są identyczne z wyjątkiem kwestii obowiązkowych audytów.

Podmiotem kluczowym jest:

1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do projektu ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;
2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w rozporządzeniu 651/2014/UE;

3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy albo je przewyższa – intencją tutaj jest objęcie mniejszych zespołów typu CSIRT/SOC/CERT wymaganiami z zakresu Cyberbezpieczeństwa;
4) niezależnie od wielkości podmiotu:
   a) dostawca usług DNS,
   b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia nr 910/2014,
   c) podmiot krytyczny – w rozumieniu dyrektywy CER,
   d) podmiot publiczny,
   e) podmiot zidentyfikowany jako podmiot kluczowy przez organ właściwy do spraw cyberbezpieczeństwa,
   f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy w sektorze podmiotów publicznych,
   g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do projektu ustawy z nazwy albo poprzez określenie jego rodzaju – jest to konieczne doprecyzowanie ponieważ, nie wszystkie rodzaje podmiotów określonych w załączniku to przedsiębiorcy i wobec tego nie można do nich zastosować progów wielkościowych z rozporządzenia 651/2014,
   h) podmiot będący operatorem obiektu energetyki jądrowej, określonego w art. 2 pkt 2 ustawie z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2024 r. poz. 1410),
   i) rejestr nazw domen najwyższego poziomu (TLD).

Podmiotem ważnym jest:

1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 lub nr 2 do projektu ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE oraz która nie jest podmiotem kluczowym;
2) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;

3) przedsiębiorca komunikacji elektronicznej będący mikro-, lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 2 i 3 załącznika I do rozporządzenia 651/2014/UE;
4) podmiot zidentyfikowany jako podmiot ważny przez organ właściwy do spraw cyberbezpieczeństwa;
5) podmiot, będący inwestorem obiektu energetyki jądrowej określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy;
6) podmiot określony w załączniku nr 2 do projektu nazwą rodzajową, a który nie jest przedsiębiorcą.

Względem dyrektywy NIS 2 przesądzono już na poziomie ustawowym, że dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa (podmioty typu Security Operations Center, Computer Security Incident Response Team, Computer Emergency Response Team itp.) są podmiotami kluczowymi. Podmioty te świadczą usługi obsługi incydentów na rzecz innych podmiotów i powinny mieć obowiązki w zakresie zapewnienia własnego cyberbezpieczeństwa, ponieważ od tego tak naprawdę będzie zależeć cyberbezpieczeństwo ich usługobiorców. Z tego zakresu wyłączono mikroprzedsiębiorców.

W przypadku podmiotów publicznych wyłączono stosowanie progów małych i średnich przedsiębiorstw. Wszystkie podmioty publiczne będą traktowane jak podmioty kluczowe. Podmioty publiczne, nawet te małe, świadczą zadania publiczne na rzecz obywateli, dlatego bardzo istotne jest aby mógł być prowadzony wobec nich także nadzór *ex ante* z zakresu cyberbezpieczeństwa.

Z pewnością wystąpi zjawisko multisektorowości – podmioty prowadzą zróżnicowaną działalność, która obejmuje wiele sektorów, zarówno sektory ważne, jak i kluczowe. Aby uniknąć rozważań, czy podmiot jest podmiotem ważnym czy kluczowym uznano, że w przypadku gdy spełnia on kryteria podmiotu kluczowego i podmiotu ważnego to powinno się wyrównać do góry i traktować go jako podmiot kluczowy. Ułatwi to określenie statusu podmiotu.

Aby ułatwić podmiotom samoidentyfikację – i uniknąć obowiązku ciągłego sprawdzania przesłanek uznania za podmiot kluczowy czy podmiot ważny w przypadkach, gdy zależy to od wielkości podmiotu – wskazano, że przesłanki uznania za podmiot kluczowy, czy podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego. Czyli

taki podmiot musi raz w roku zbadać, czy jest podmiotem ważnym lub kluczowym. Oczywiście dotyczy to wyłącznie przedsiębiorców i to takich, których status podmiotu kluczowego, czy podmiotu ważnego zależy od ich wielkości.

W projektowanych przepisach wdrożono motyw 16 dyrektywy NIS 2. Zgodnie z unijnymi kryteriami przy badaniu statusu mikro-, małych i średnich przedsiębiorstw bierze się pod uwagę przedsiębiorstwa powiązane i przedsiębiorstwa partnerskie – ich przychody, sumę bilansową i liczbę pracowników dolicza się przy ustalaniu wielkości podmiotu. To mogłoby oznaczać, że dany podmiot staje się średnim przedsiębiorcą, wliczając jego przedsiębiorstwa powiązane i partnerskie – i jest wtedy podmiotem ważnym. Ale jego systemy informacyjne mogą mieć charakter niezależny od systemów podmiotów partnerskich i powiązanych. Nie ma więc powodów, aby uznawać ten podmiot za podmiot ważny.

Wśród podmiotów leczniczych mamy także podmioty niebędące przedsiębiorcami – np. jednostki budżetowe. Trudno wobec nich stosować kryteria wielkości przedsiębiorców. Jednocześnie należy tutaj wprowadzić kryterium wielkościowe i zwolnić z obowiązków małe podmioty lecznicze. Wprowadzono więc regułę, że podmiot leczniczy, który nie jest przedsiębiorcą:

1) jest podmiotem ważnym, jeżeli zatrudnia od 50 do 249 osób;

2) jest podmiotem kluczowym jeżeli zatrudnia co najmniej 250 osób.

Wprowadzono uprawnienie dla Ministra Obrony Narodowej do ustalenia, które jednostki jemu podległe lub przez niego nadzorowane będą podmiotami kluczowymi lub podmiotami ważnymi.

Takie ujęcie tej kwestii gwarantuje pełną zgodność z postanowieniami dyrektywy NIS 2. Szczególnie istotne jest odniesienie do spełniania wymogów dla średniego przedsiębiorstwa, w przypadku najbardziej szerokich kategorii przedsiębiorców. Takie rozwiązanie gwarantuje, że nakładane obowiązki będą proporcjonalne do możliwości podmiotów, na które zostaną nałożone.

Podmioty świadczące usługi niezbędne dla funkcjonowania współczesnego społeczeństwa informacyjnego mają charakter transgraniczny. Należało więc przesądzić, zgodnie z dyrektywą NIS 2, jurysdykcję państwa nad podmiotami świadczącymi te usługi.

Co do zasady podmiot kluczowy i podmiot ważny podlega obowiązkom wynikającym z ustawy, jeżeli posiada jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej.

Przedsiębiorca komunikacji elektronicznej podlega obowiązkom wynikającym z ustawy, jeżeli świadczy usługi na terytorium Rzeczypospolitej Polskiej. Jest to spójne z ustawą z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej.

Podmioty z sektora infrastruktury cyfrowej podlegają jurysdykcji polskiej, jeżeli na terytorium Rzeczypospolitej Polskiej ma siedzibę kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji w podmiocie albo realizowane są zadania związane z systemem zarządzania bezpieczeństwem informacji w podmiocie albo podmiot ma największą liczbę pracowników w odniesieniu do innych państw członkowskich Unii Europejskiej.

Przepisy ustawy o KSC nakładają na przedsiębiorców spoza Unii Europejskiej działających na jej terenie obowiązek wyznaczenia przedstawiciela. W sprawach dotyczących cyberbezpieczeństwa instytucje krajowego systemu cyberbezpieczeństwa, takie jak zespoły CSIRT, będą mogły kontaktować się z tymi przedstawicielami w sprawach obowiązków spoczywających na tych podmiotach. Gwarantuje to, że w systemie zostaną ujęte wszystkie podmioty operujące na terenie UE.

2.3. Uchylenie wykazu usług kluczowych

Uchyla się podstawę prawną do wydania rozporządzenia Rady Ministrów w sprawie wykazu usług kluczowych. Dyrektywa NIS 2 nakazuje podmiotom kluczowym i podmiotom ważnym wdrożyć środki zarządzania ryzykiem dotyczące usług świadczonych przez te podmioty, a nie jednej konkretnej usługi.

Usługi kluczowe występują w przypadku dyrektywy CER – ich wykaz został ustalony w rozporządzeniu delegowanym Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych (Dz. Urz. UE L 2023/2450 z 30.10.2023). Tym bardziej prawodawca krajowy nie może precyzować usług kluczowych w rozporządzeniu.

2.4. Wykaz podmiotów kluczowych i podmiotów ważnych

Bardzo duża liczba podmiotów podlegająca obowiązkom z dyrektywy NIS 2 stanowi wyzwanie dla organów nadzorujących wykonywanie obowiązków z zakresu cyberbezpieczeństwa – czyli organów właściwych do spraw cyberbezpieczeństwa. Podstawowa trudność to ich prawidłowe zidentyfikowanie. Do tej pory operatorzy usług kluczowych byli wyznaczani w drodze decyzji administracyjnej organu właściwego do spraw cyberbezpieczeństwa. Duży problem stanowiła natomiast identyfikacja dostawców usług

cyfrowych w rozumieniu dyrektywy NIS 1 – nie byli oni identyfikowani w drodze decyzji administracyjnej, a obecne kody Polskiej Klasyfikacji Działalności nie identyfikowały dokładnie działalności podmiotów świadczących usługi przetwarzania w chmurze, wyszukiwarek internetowych oraz internetowych platform handlowych. Ponadto zgodnie z dyrektywą NIS 2 państwa członkowskie Unii Europejskiej mają obowiązek przekazać liczbę podmiotów w poszczególnych sektorach zidentyfikowanych w danym państwie. Po raz pierwszy państwo członkowskie musi tego dokonać do dnia 17 kwietnia 2025 r. W przypadku zaś sektora infrastruktury cyfrowej państwa członkowskie mają obowiązek podać konkretne podmioty świadczące usługi. Niezbędny jest więc mechanizm umożliwiający sprawną identyfikację podmiotów kluczowych i podmiotów ważnych.

Aby ułatwić identyfikację podmiotów kluczowych i podmiotów ważnych wprowadzono obowiązek samorejestracji tych podmiotów. Rejestracja będzie dokonywała się w wykazie podmiotów kluczowych i podmiotów ważnych, który będzie prowadzony przez ministra właściwego do spraw informatyzacji. Regulacja ta zastąpi dotychczasowe przepisy o wykazie operatorów usług kluczowych.

Podmioty spełniające wymogi dla podmiotów kluczowych i podmiotów ważnych będą obowiązane do zarejestrowania się w tym rejestrze w terminie 2 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy albo podmiot ważny. Wykaz będzie zawierał wszystkie informacje niezbędne do skutecznego nadzoru nad tymi podmiotami. Przede wszystkim będą to dane identyfikujące podmiot – nazwa (firma) podmiotu, sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub nr 2 do projektu ustawy, siedzibę i adres do korespondencji, adres do doręczeń elektronicznych, jeżeli został nadany, adres poczty elektronicznej, numer identyfikacji podatkowej, numer REGON oraz numer we właściwym rejestrze działalności regulowanej.

Oprócz samych danych identyfikujących będą w nim zawarte informacje takie jak:

1) zakres adresów IP wykorzystywanych przez podmiot;
2) zakres nazw domen wykorzystywanych przez ten podmiot;
3) dane co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej (w przypadku mikro i małych przedsiębiorców – jednej osoby);
4) numer telefonu przyporządkowany do wykonywanej działalności;

5) deklarację podmiotu czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy;

6) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot wykonuje działalność wraz z określeniem wykonywanej działalności;

7) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie bezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11 projektu ustawy wraz z danymi tego podmiotu.

Tego rodzaju informacje są niezbędne CSIRT poziomu krajowego, CSIRT sektorowym i innym organom krajowego systemu cyberbezpieczeństwa do prawidłowego wykonywania ich ustawowych zadań. Umieszczenie ich w jednym rejestrze zapewni łatwy dostęp do nich upoważnionym organom. Dane co najmniej osób kontaktowych umożliwią szybką komunikację między zespołem CSIRT a danym podmiotem w przypadku incydentu poważnego lub w sytuacji poinformowania podmiotu o istotnej podatności czy też znaczącym cyberzagrożeniu. Deklaracja podmiotu o statusie mikro-, małego lub średniego przedsiębiorcy umożliwi ustalenie statusu podmiotu – czy jest podmiotem ważnym czy podmiotem kluczowym.

Informacja o wykonywaniu działalności w innych państwach członkowskich Unii Europejskiej pozwoli określić np. czy incydent zgłoszony przez podmiot może mieć charakter transgraniczny. Ponadto będzie to przydatna informacja, jeżeli konieczna będzie współpraca organów nadzorczych z innych państw członkowskich Unii Europejskiej. Zasadne jest też, żeby podmioty wpisane do wykazu informowały o dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, z którym zawarły umowę na realizację zadań z zakresu cyberbezpieczeństwa. W przypadku trwającego incydentu poważnego istotne jest dla CSIRT sektorowych lub CSIRT poziomu krajowego kto faktycznie zajmuje się obsługą incydentu w danym podmiocie. Umożliwi to szybszą komunikację między zespołami. Warto podkreślić, że dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa może być także jednostka utworzona przez np. ministra kierującego danym działem administracji rządowej i świadcząca usługi reagowania na incydenty dla podmiotów podległych ministrowi i nadzorowanych przez tego ministra.

Organ właściwy do spraw cyberbezpieczeństwa powinien także wiedzieć, czy podmiot kluczowy albo podmiot ważny zawarł porozumienie w sprawie wymiany informacji o zdarzeniach z zakresu cyberbezpieczeństwa (w praktyce to będą porozumienia w sprawie

sektorowych inicjatyw ISAC). Bardzo istotna jest informacja czy podmiot jest podmiotem krytycznym w rozumieniu dyrektywy CER i podlega obowiązkom z dyrektywy CER.

Zdecydowana większość informacji w wykazie będzie pochodziła od samego podmiotu kluczowego, czy podmiotu ważnego – zostanie to zawarte we wniosku o wpis do wykazu. Natomiast część informacji będzie uzupełniana z urzędu przez ministra właściwego do spraw informatyzacji. Dotyczy to wskazania organu właściwego do spraw cyberbezpieczeństwa, właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego oraz tytułu prawnego wpisania do wykazu. Te dane są do ustalenia przez ministra w oparciu o przekazane dane z wniosku o wpis do wykazu.

Wskazano zakres danych, których dotyczy wniosek o wpis do wykazu – są to wszystkie dane z wyjątkiem tych, które minister właściwy do spraw informatyzacji jest w stanie ustalić z urzędu. Wniosek o zmianę wpisu w wykazie będzie zawierał wskazanie danych zmienianych.

Równocześnie wiele z tych danych będzie wrażliwych a ich podanie do publicznej wiadomości mogłoby negatywnie wpłynąć na bezpieczeństwo tych podmiotów i na ich chronione prawem interesy. Z tego względu do wykazu nie będą miały zastosowanie przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) i ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

W przypadkach, w których jest to możliwe, minister właściwy do spraw informatyzacji sam dokona rejestracji podmiotów z grup, które w całości znajdą się w wykazie, np. przedsiębiorców telekomunikacyjnych, podmiotów krytycznych, dostawców usług zaufania, czy podmiotów publicznych wykorzystując dane, które są już gromadzone w innych rejestrach publicznych. Celem projektodawcy jest wykorzystywanie informacji, które administracja publiczna już posiada oraz na unikaniu nakładania zbędnych obowiązków na podmioty prywatne.

Wykaz będzie prowadzony w systemie teleinformatycznym S46, a wnioski do niego będą miały formę elektroniczną, co pozwoli na jego efektywną obsługę. We wniosku powinny znaleźć się wszystkie informacje, które są wymagane w rejestrze. Wnioski mają zawierać również oświadczenia o świadomości odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2024 r. poz. 17 i 1228), zwanej dalej „Kodeks karny”. Powinno to zapewnić aktualność danych w rejestrze. Spod tej odpowiedzialności zwolnione są punkty wniosku dotyczące

wykorzystywanych adresów IP oraz domen. Adresy IP i domeny mogą ulegać bardzo szybkim zmianom, a także może ich być bardzo wiele. Z tego względu nie byłoby zasadne karanie za błędne podanie tych informacji.

Wpis do wykazu będzie dokonywał się automatycznie z chwilą złożenia poprawnego podpisanego wniosku przez podmiot kluczowy i podmiot ważny. Organy właściwe do spraw cyberbezpieczeństwa będą mogły weryfikować czy podmioty wpisane do wykazu rzeczywiście spełniają odpowiednie kryteria podmiotów kluczowych i podmiotów ważnych.

Po dokonaniu wpisu podmioty będą musiały podłączyć się do systemu S46 w zakresie funkcjonalności umożliwiających szacowanie ryzyka i zgłaszanie incydentów. Jest to system już obecnie funkcjonujący, wspierający wymianę informacji między podmiotami krajowego systemu cyberbezpieczeństwa. Docelowo w ramach tego systemu będzie przechodziła cała komunikacja w sprawach cyberbezpieczeństwa. System ten będzie zawierał również narzędzia, które pomogą tym podmiotom m.in. w przygotowaniu oceny ryzyka. Te rozwiązania usprawnią komunikację w ramach krajowego systemu cyberbezpieczeństwa i pozwolą skutecznie wspierać jego podmioty w realizacji ich obowiązków.

Przewiduje się obowiązkową elektronizację wniosków o wpis, zmianę wpisu w wykazie albo o wykreślenie z wykazu. Będą one musiały być opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Wnioski będą składane za pomocą systemu S46.

Dane z wykazu minister będzie udostępniał CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, organowi właściwemu do spraw cyberbezpieczeństwa w zakresie nadzorowanego sektora lub podsektora, a także podmiotowi kluczowemu lub podmiotowi ważnemu w zakresie go dotyczącym. Ponadto o dostęp do tych danych będą mogły wnioskować inne organy państwa takie jak np. policja, prokuratura i sądy.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł również z urzędu wpisać dany podmiot do wykazu podmiotów kluczowych i podmiotów ważnych jeśli na podstawie danych zawartych w rejestrach publicznych oraz w innych dostępnych źródłach informacji stwierdzi on, że dany podmiot spełnia kryteria podmiotu kluczowego lub podmiotu ważnego. To rozwiązanie gwarantuje, że nawet jeśli dany podmiot nie będzie chciał się wpisać do wykazu będzie możliwe włączenie go do rejestru. Czynność wpisania nie będzie miała charakteru decyzji administracyjnej, z uwagi na potencjalną liczbę podmiotów objętych

obowiązkiem wpisu do wykazu – szacunkowo ponad 10 000. Jeżeli część z tych podmiotów nie wpisze się dobrowolnie do wykazu, to konieczne będzie wydawanie wielu decyzji administracyjnych, co będzie bardzo dużym obciążeniem dla organów właściwych do spraw cyberbezpieczeństwa. Z tego powodu lepsza jest formuła innej czynności z zakresu administracji publicznej. Podmiot będzie mógł zaskarżyć taką czynność do sądu administracyjnego, co gwarantuje mu skuteczną możliwość ochrony jego praw.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł weryfikować dane zawarte w wykazie i w razie potrzeby wzywać podmiot do ich zmiany pod rygorem nałożenia administracyjnej kary pieniężnej.

Podmiot będzie mógł złożyć wniosek o wykreślenie z wykazu, jeżeli przestanie spełniać wymogi dla podmiotu kluczowego i podmiotu ważnego, ale będzie to weryfikowane przez organ właściwy do spraw cyberbezpieczeństwa.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł z urzędu wykreślić podmiot z wykazu podmiotów kluczowych i podmiotów ważnych jeżeli:

1) podmiot wpisany do wykazu nie jest podmiotem kluczowym albo podmiotem ważnym albo
2) podmiot wpisany do wykazu utracił status podmiotu kluczowego albo podmiotu ważnego po wpisie do wykazu.

Pozwoli to na utrzymanie aktualności tego wykazu.

W szczególnie uzasadnionych przypadkach gdy dany podmiot nie spełnia wymogów uznania za podmiot kluczowy lub podmiot ważny, ale:

1) jako jedyny świadczy usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
2) zakłócenie świadczenia usługi przez niego spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności,
3) zakłócenie świadczenia usługi przez niego spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
4) świadczenie przez niego usług ma istotne znaczenie na poziomie krajowym lub województwa lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub nr 2 do projektu ustawy

– to w drodze decyzji administracyjnej organu właściwego będzie możliwe uznanie go za podmiot kluczowy lub podmiot ważny. Możliwość ta wynika z przepisów samej dyrektywy NIS 2. Przepis ten ma zagwarantować, że w krajowym systemie cyberbezpieczeństwa znajdą się wszystkie podmioty prowadzące szczególnie istotną dla państwa i społeczeństwa działalność. Jak wykazały doświadczenia pandemii w wielu przypadkach zaprzestanie działalności przez stosunkowo mały podmiot może mieć bardzo szerokie skutki dla innej działalności, np. w sektorze energetyki czy przemyśle. Tego rodzaju podmioty muszą znaleźć się w krajowym systemie cyberbezpieczeństwa.

O uznaniu takiego podmiotu za podmiot kluczowy lub podmiot ważny rozstrzyga decyzja administracyjna. W ramach tej procedury podmiot będzie miał możliwość ochrony swoich spraw, przedstawiania dowodów oraz podważania rozstrzygnięć organów.

Przewidziano także możliwość, aby można było uznać państwową osobę prawną za podmiot kluczowy.

2.5. Obowiązki podmiotów kluczowych i podmiotów ważnych

2.5.1. System zarządzania bezpieczeństwem informacji

Artykuł 21 dyrektywy NIS 2 nakazuje podmiotom kluczowym i podmiotom ważnym wprowadzenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

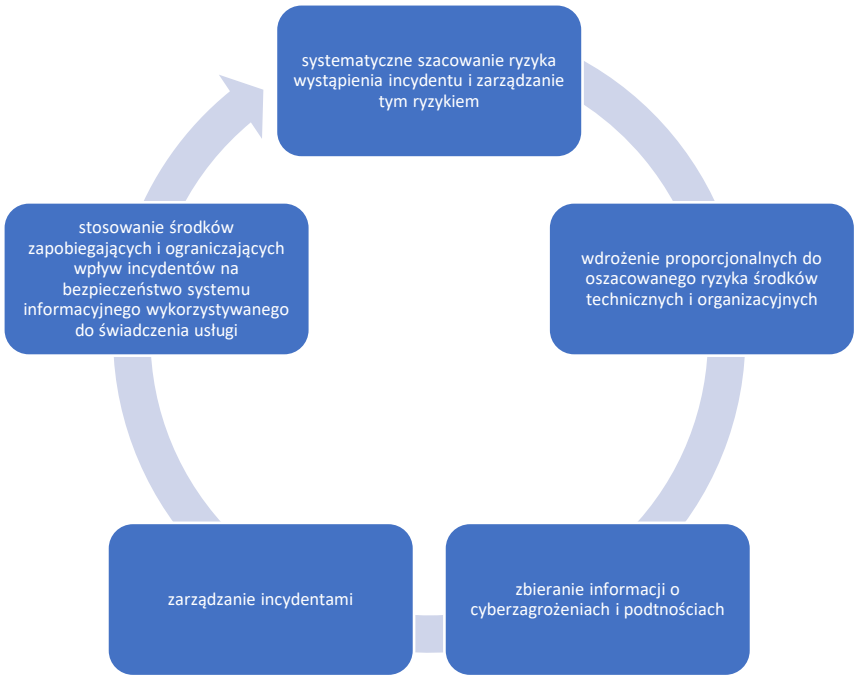
Dyrektywa NIS 2 odeszła od wdrażania środków zapewniających bezpieczeństwo systemów informacyjnych tylko w zakresie świadczonych usług kluczowych. Podmiot ma dbać o bezpieczeństwo wszystkich swoich systemów wykorzystywanych do prowadzenia swojej działalności. Zauważyć bowiem należy, że podmioty gospodarcze choć działają dla zysku, to nie działają w próżni – ich działalność ma istotny wpływ na świadczenie usług przez inne podmioty, a także ma wpływ na funkcjonowanie konsumentów. Od zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych przedsiębiorstw energetycznych zależy funkcjonowanie przedsiębiorców telekomunikacyjnych, przewoźników kolejowych, dostawców usług chmurowych, serwerowni, czy wreszcie konsumentów. Podmioty dostarczające wodę pitną i odprowadzające ścieki używają systemów automatyki

przemysłowej – tutaj incydent mógłby poważnie wpłynąć na zdrowie publiczne. Przykłady wzajemnego oddziaływania podmiotów współczesnej gospodarki można mnożyć. Wszystkie te podmioty używają systemów informacyjnych do świadczenia usług. Incydenty w jednym sektorze mogą spowodować poważne straty materialne oraz istotnie wpłynąć na funkcjonowanie społeczeństwa. Dlatego ważne jest nałożenie obowiązków z zakresu cyberbezpieczeństwa na podmioty kluczowe i podmioty ważne, aby przeciwdziałać negatywnemu wpływowi incydentów na funkcjonowanie społeczeństwa i gospodarki.

Dyrektywa NIS 2 mówi o wprowadzeniu środków zarządzania ryzykiem. Jednym z możliwych sposobów implementacji tych przepisów jest nałożenie obowiązków wdrożenia systemu zarządzania bezpieczeństwem informacji. Tak jest w chwili obecnej – operatorzy usług kluczowych mają obowiązek wdrożyć system zarządzania bezpieczeństwem informacji na podstawie aktualnego brzmienia art. 8 ustawy o KSC . Z kolei podmioty publiczne mają także obowiązek wdrożyć system zarządzania bezpieczeństwem informacji na podstawie § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773). Z tego powodu zdecydowano się wdrożyć art. 21 dyrektywy NIS 2 przez ewolucję obecnego art. 8 ustawy o KSC. Podmioty kluczowe i podmioty ważne będą więc obowiązane wdrożyć system zarządzania bezpieczeństwem informacji, obejmujący elementy wskazane w dyrektywie NIS 2. Takie podejście ułatwi dostosowanie się do regulacji podmiotom, które już obecnie są obowiązane na podstawie przepisów prawa posiadać wdrożony taki system – albo zrobiły to dobrowolnie. Podkreślić przy tym należy, że projekt nie wymaga uzyskania certyfikacji zgodności systemu zarządzania bezpieczeństwem informacji z jedną z norm technicznych. Wystarczające jest wdrożenie tego systemu zgodnie z ustawą o KSC oraz odpowiednie udokumentowanie tego faktu.

Zgodnie z nowym brzmieniem system zarządzania bezpieczeństwem informacji i ciągłości działania będzie wdrożony w systemach informacyjnych wykorzystywanych w procesach wpływających na świadczenie usług przez podmiot kluczowy lub podmiot ważny. Dzięki takiemu brzmieniu z jednej strony zachowamy brzmienie dyrektywy NIS 2, a z drugiej środki zarządzania ryzykiem będą wdrożone rzeczywiście w tych systemach, które służą świadczeniu usług.

Wdrażając art. 21 dyrektywy NIS 2 zachowano dotychczasową systematykę art. 8 ustawy o KSC.



Rysunek 1. System zarządzania bezpieczeństwem informacji w projekcie nowelizacji ustawy o KSC

Podstawowym obowiązkiem podmiotów kluczowych i podmiotów ważnych będzie wdrożenie systemu zarządzania bezpieczeństwem informacji obejmującego:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem – należy regularnie szacować ryzyko (identyfikować, analizować, oceniać), a następnie podejmować decyzję o podejściu do tego ryzyka;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia[6)], wielkość podmiotu[7)], prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze[8)], w szczególności:
   a) polityki szacowania ryzyka[9)] oraz bezpieczeństwa systemu informacyjnego[10)], w tym polityki tematyczne[11)],
   b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego[12)],
   c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu[13)],
   d) bezpieczeństwo zasobów ludzkich[14)],

---

6) Każda organizacja ma ograniczone zasoby, dlatego wybrane środki powinny być także adekwatne do jej możliwości finansowych.
7) Inne są możliwości organizacyjne i finansowe dużych przedsiębiorstw, a inne średnich przedsiębiorstw i nie można tych możliwości porównywać.
8) Należy więc bardzo dobrze ustalić kontekst danej organizacji, jej charakterystykę, świadczone usługi, posiadane systemy, otoczenie regulacyjne, wymogi podmiotów trzecich.
9) Polityka szacowania ryzyka powinna opisać proces szacowania ryzyka w danej organizacji.
10) Należy ustanowić politykę bezpieczeństwa systemu informacyjnego wskazującą podejście podmiotu do zarządzania bezpieczeństwem informacji wraz z przypisaniem ról w tym procesie. Polityka ta powinna być adekwatna do danego podmiotu, wskazać cele bezpieczeństwa systemu informacyjnego, zobowiązanie do ciągłego rozwoju jak również przewidywać jej przegląd. Polityka powinna być zakomunikowana osobom zatrudnionym w podmiocie.
11) Polityki tematyczne – przykładowo są to *topic specific policies* o których mowa w normie ISO 27001. Założeniem tego przepisu jest to, aby tam gdzie to konieczne organizacja opracowała polityki tematyczne. Przykładowo, jeśli przyczyni się to do lepszej ochrony to organizacja może wprowadzić politykę bezpieczeństwa urządzeń mobilinych.
12) Należy opracować i wdrożyć procedury zarządzania konfiguracją, zmianami w systemie, testowanie systemu.
13) Podmiot kluczowy/podmiot ważny powinien monitorować dostęp fizyczny do elementów systemu informacyjnego, zapobiegać cyberzagrożeniom mającym charakter fizyczny, zapobiegać utracie, uszkodzeniu urządzeń wspierających funkcjonowaniu systemu informacyjnego (np. urządzenia elektryczne).
14) Należy dbać o zrozumienie wymogów bezpieczeństwa wśród personelu. Personel o szczególnym dostępie do aktywów powinien w szczególny sposób wykonywać swoje zadania w. Pamiętać należy o personelu zewnętrznego dostawcy – należy wprowadzić odpowiednie postanowienia umowne dotyczące bezpieczeństwa oraz zachowaniu w poufności informacji. W procesie rekrutacji należy prowadzić weryfikację kandydatów (np. poprzez OSINT czy poprzez wymóg dostarczenia referencji czy zaświadczeń – przy czym należy pamiętać o wymogach RODO i poinformować kandydatów w ogłoszeniu, że takie czynności będą dokonywane i że wymagana jest ich zgoda); ponadto należy wprowadzić wewnętrzne reguły dyscyplinarne, jeśli nie wynikają z przepisów prawa powszechnie obowiązującego, dotyczące przypadków naruszenia obowiązków personelu w obszarze Cyberbezpieczeństwa, wraz z możliwością wypowiedzenia umowy;

e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym[15)],

f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych, oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków (katastrofa),

g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym[16)],

h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych[17)],

i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,

j) podstawowe zasady cyberhigieny,

w postanowieniach umownych z personelem należy zawrzeć zapisy dotyczące zachowania w poufności informacji związanych z organizacją także po zakończeniu umowy.

15) Należy wprowadzić politykę łańcucha dostaw obejmującą relację z bezpośrednimi dostawcami. W polityce należy wskazać kryteria wyboru dostawców. W umowach z dostawcami należy zawierać postanowienia dotyczące Cyberbezpieczeństwa m. in. obowiązek zachowania informacji w poufności, obowiązek zgłaszania incydentów do podmiotu, informowanie o podatnościach, wymogi dotyczące personelu podmiotu (np. co do certyfikacji osób) itd. Pamiętać przy tym należy, że duzi dostawcy sprzętu lub oprogramowania często mają wdrożoną certyfikację własnych systemów, osób lub produktów/usług z zakresu cyberbezpieczeństwa, co z jednej strony ułatwia zarządzanie bezpieczeństwem łańcuchów dostaw, z drugiej może potencjalnie utrudnić dodatkowe wymogi, zwłaszcza, jeżeli zamawiający jest zdecydowanie mniejszym podmiotem. Tutaj wchodzi więc zasada proporcjonalnych środków technicznych i organizacyjnych. Organizacja powinna mieć aktualny wykaz bezpośrednich dostawców z danymi kontaktowymi oraz wskazaniem jakie produkty ICT, usługi ICT czy procesy ICT dostarczają.

16) System informacyjny powinien być monitorowany ciągle – chodzi o to, aby zapewnić rozliczalność działań podejmowanych w systemie i analizować zaistniałe zdarzenia. Niekoniecznie trzeba w tym celu zatrudniać dodatkową osobę, można skorzystać z narzędzi open-source typu SIEM i ustawić adekwatne reguły. W szczególności należy monitorować zdarzenia, które mogą być przyczyną lub skutkiem incydentu. Monitorowanie dotyczy w szczególności ruchu z i do podmiotu, dostępu do systemu, kont z uprzywilejowanym dostępem, krytyczne pliki konfiguracyjne i kopii zapasowej, logi z narzędzi Cyberbezpieczeństwa (np. antywirusów, anti-spyware), zdarzenia środowiskowe, które mogą mieć wpływ na funkcjonowanie infrastruktury systemu (zalanie, pożar itd.)

17) Należy ustalić, które aktywności w SZBI podmiotu będą monitorowane, jakie będą wskaźniki (KPI), kiedy, w jakich interwałach będą monitorowane, kto będzie to robił, czy nastąpi ich ewaluacja oraz kto za to będzie odpowiedzialny.

k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania[18)],

l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,

m) zarządzanie aktywami[19)],

n) polityki kontroli dostępu[20)];

3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi[21)];

4) zarządzanie incydentami[22)];

5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:

a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,

b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,

c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,

d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

---

18) Polityki i procedury stosowania kryptografii obejmują m. in. jakie protokoły i algorytmy, rowiązania i praktyki są zatwierdzone do używania w podmiocie oraz kwestie zarządzanie kluczami.

19) Należy ustalić klasyfikację aktywów, polityki/procedury właściwego zarządzania aktywami, prowadzić inwentaryzację aktywów oraz dbać o zwrot aktywów po zakończeniu umowy z personelem.

20) Należy ustalić politykę kontroli dostępu wskazującą kto może uzyskać dostęp fizyczny i logiczny do zasobów. Należy zarządzać prawami dostępu i anulować dostęp dla osób, które już nie potrzebują dostępu do aktywów, w tym także personelu zewnętrznego dostawcy. Należy prowadzić rejestr udzielonych dostępów.

21) Zbieranie informacji o cyberzagrożeniach i podatnościach pozwala na rozwój własnego personelu, zwiększa dojrzałość organizacji, umożliwia prewencyjne usunięcie podatności w systemie lub zabezpieczenie się przed cyberzagrożeniem.

22) Warto opracować politykę zarządzania incydentami, wprowadzić narzędzie do zgłaszania incydentów wewnątrz podmiotu, wprowadzić procedurę obsługi incydentów.

Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym należy rozumieć w ten sposób, że podmiot powinien monitorować wszelkie zdarzenia, które zaistniały w systemie informacyjnym. Celem jest nie tylko zapewnienie rozliczalności, ale także umożliwienie odtworzenia co się stało w systemie informacyjnym w danym momencie.

Podmioty kluczowe oraz podmioty ważne będą obowiązane uwzględnić wyniki skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych przez Grupę Współpracy, o której mowa art. 22 dyrektywy NIS 2.

W zakresie reagowania na incydenty należy również zwrócić uwagę na kwestię ograniczenia ruchu sieciowego. Jest to jeden ze środków reagowania na incydenty. Polega on na zaatakowaniu ofiary z wielu miejsc jednocześnie. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu. Jest to jeden z najczęściej stosowanych typów ataku.

Ograniczenie ruchu sieciowego jest najskuteczniejszą metodą zablokowania takiego ataku. Równocześnie wiele podmiotów, w szczególności podmioty publiczne, wskazują, że zgodnie z przepisami muszą świadczyć usługi i nie powinny blokować do nich dostępu nikomu. W dotychczasowym stanie prawnym istniały wątpliwość czy obsługa incydentu i zapewnienia bezpieczeństwa swoim systemom upoważniają do zablokowania takiego ruchu.

Rada Ministrów będzie mogła ustalać, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji. Przepis ten pozwoli uwzględnić specyfikę poszczególnych sektorów i przedstawić rozwiązania dostosowane do tej specyfiki. Będzie to fakultatywne upoważnienie ustawowe.

Podkreślić należy, że zakłada się możliwość wydawania wielu rozporządzeń na podstawie dodawanego upoważnienia ustawowego. Projekt ustawy wdrażającej dyrektywę NIS 2 nakłada obowiązki na bardzo zróżnicowane podmioty w wielu sektorach gospodarki. W ramach

poszczególnych rodzajów działalności występuje także wiele podrodzajów. Przygotowanie jednego rozporządzenia obejmującego wszystkie te sektory byłoby zadaniem karkołomnym – wprowadzone regulacje musiałyby pozostać na bardzo wysokim poziomie ogólności, co poddawałoby w wątpliwość celowość uregulowania tej materii w rozporządzeniu. Alternatywa w postaci wprowadzenia kilkunastu przepisów upoważniających dla określenia minimalnych wymagań dla systemu zarządzania bezpieczeństwem informacji w poszczególnych sektorach nie wydaje się słuszna. Trudno byłoby w takim przypadku określić organ wydający rozporządzenie – wszakże nie wszystkie organy właściwe do spraw cyberbezpieczeństwa mają prawo do wydawania rozporządzeń. Dlatego zdecydowano się na wprowadzenie upoważnienia ustawowego dla Rady Ministrów.

W ramach rządowego procesu legislacyjnego wnioskodawcą projektu rozporządzenia dotyczącego określonej działalności powinien być organ właściwy do spraw cyberbezpieczeństwa nadzorujący daną działalność. Jeśli organ właściwy do spraw cyberbezpieczeństwa nie ma uprawnień do procedowania projektu rozporządzenia, to wnioskodawcą projektu powinien być minister nadzorujący dany organ.

Przepisy aktów podustawowych muszą być zgodne nie tylko z ustawą, na podstawie której zostały wydane, ale także z innymi ustawami. Wynika to z hierarchii systemu źródeł prawa. Przepisy art. 8 ustawy o KSC w wersji znowelizowanej będą nakładały obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji na podmioty publiczne. Te podmioty już obecnie mają taki obowiązek – wynika on z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Konieczna będzie nowelizacja tego rozporządzenia, aby uniknąć kolizji z przepisami art. 8 ustawy o KSC. Nie jest również wykluczone, że na podstawie art. 8a projektu ustawy zostanie wydane rozporządzenie precyzujące wymagania z zakresu cyberbezpieczeństwa dla podmiotów publicznych.

Komisja Europejska ma obowiązek wydania aktów wykonawczych do dyrektywy NIS 2 określających środki zarządzania ryzykiem dla części podmiotów z sektora infrastruktury cyfrowej. Dla pozostałych podmiotów Komisja może wydać takie akty. Dlatego w przepisie wskazano, że w ramach systemu zarządzania bezpieczeństwem informacji i ciągłości działania podmioty stosują środki określone w bezpośrednio stosowalnych aktach wykonawczych Komisji Europejskiej.

Wskazano również, że podmioty kluczowe z podsektora energii elektrycznej stosują, w ramach systemu zarządzania bezpieczeństwem informacji i ciągłości działania środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

2.5.2. Zadania kierownictwa

Dyrektywa NIS 2 wprowadziła obowiązek wskazania roli kierownictwa poszczególnych podmiotów w zakresie zapewnienia ich cyberbezpieczeństwa. Kierownik podmiotu kluczowego lub podmiotu ważnego z mocy ustawy ponosi odpowiedzialność za wykonywanie obowiązków podmiotu w zakresie cyberbezpieczeństwa. Jeżeli kierownikiem jest organ wieloosobowy to odpowiedzialność ponoszą wszyscy członkowie tego organu. Odpowiedzialność kierownika podmiotu następuje także wtedy gdy niektóre z obowiązków zostały powierzone innej osobie za jej zgodą. Celem tych rozwiązań jest to, aby kierownictwo podmiotu poważnie podchodziło do zapewnienia cyberbezpieczeństwa podmiotu, ponieważ obecnie bez bezpiecznych systemów informacyjnych nie jest możliwe sprawne świadczenie usług innym podmiotom i konsumentom.

Wskazano zadania kierownika podmiotu kluczowego lub podmiotu ważnego:

1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie – co oznacza, że kierownik odpowiada za system zarządzania bezpieczeństwem informacji i jego rozwój zgodnie z cyklem Deminga;
2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa – mając na uwadze, że cyberbezpieczeństwo wymaga nakładów i nie powinny one być pomijane w budżetach podmiotów kluczowych i podmiotów ważnych;
3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie;
4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie. System zarządzania bezpieczeństwem informacji wymaga, aby każdy pracownik organizacji

miał przypisaną role i zadania do wykonania celem zachowania bezpieczeństwa informacji;

5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.

Osoby kierujące podmiotami kluczowymi i podmiotami ważnymi muszą również raz na rok przejść szkolenie z zakresu wykonywania zadań z zakresu cyberbezpieczeństwa. Dotyczy to zadań związanych z opracowaniem systemu zarządzania bezpieczeństwem informacji, zgłaszania incydentów, dokumentowania SZBI. Gwarantuje to, że będą posiadać aktualną wiedzę merytoryczną potrzebną do podejmowania decyzji w tym obszarze.

2.5.3. Niekaralność personelu

Ważną gwarancją prawidłowego wykonywania zadań z zakresu cyberbezpieczeństwa jest wskazanie, że zadań tych nie mogą wykonywać osoby skazane za przestępstwa przeciwko ochronie informacji[23)]. Daje to odpowiednią gwarancję, że zadania te będą wykonywały osoby dające rękojmię ich prawidłowej realizacji. Ograniczono się przy tym do przestępstw przeciwko ochronie informacji, ponieważ są one związane tematycznie z cyberbezpieczeństwem.

Osoba musi przedstawić zaświadczenie o niekaralności za ww. przestępstwa. Zaświadczenia w tym zakresie będą weryfikowane przez ich kierowników podmiotów kluczowych i podmiotów ważnych. Po otrzymaniu zaświadczenia kierownik dopuści taką osobę do realizacji zadań związanych z systemem zarządzania bezpieczeństwem informacji oraz zgłaszaniem incydentów. Weryfikacja personelu przed przydzieleniem zadań z zakresu cyberbezpieczeństwa jest przewidywana przez normy techniczne, np. normę ISO 27001, a zatem nie jest to zupełna nowość. Podkreślić należy, że mogą tutaj wystąpić stosunek pracy, a także inne stosunki zatrudnienia, np. umowa zlecenia. Jest to istotne w kontekście przetwarzania danych osobowych, jako że dotyczy to danych o karalności w rozumieniu art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

[23)] Czyli przestępstwa określone w rozdziale XXXIII Kodeksu karnego – art. 265 (ujawnienie informacji niejawnych), art. 266 (ujawnienie informacji służbowych), art. 267 (nielegalne uzyskanie informacji), art. 268 (niszczenie informacji), art. 268a (niszczenie danych w systemach), art. 269 (sabotaż komputerowy), art. 269a (zakłócanie sieci i systemów), art. 269b (bezprawne wykorzystanie programów i danych).

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.), zwanego dalej „RODO”. Tak jak wyżej wspomniano, weryfikacja niekaralności personelu przed wykonywaniem zadań z zakresu cyberbezpieczeństwa jest zasadna. Osoby, które dopuściły się czynów zabronionych przeciwko ochronie informacji nie dają należytej rękojmi prawidłowego wykonywania zadań z zakresu Cyberbezpieczeństwa. W interesie samego podmiotu kluczowego i podmiotu ważnego jest zatrudnienie wiarygodnego personelu. Ponadto sama dyrektywa NIS 2 wspomina o konieczności wdrożenia środków z zakresu bezpieczeństwa zasobów ludzkich. Stąd weryfikacja niekaralności personelu jest konieczna. Informacje o niekaralności będą przechowywane w dokumentacji pracowniczej albo w dokumentacji związanej z daną umową w przypadku innych stosunków zatrudnienia. Oczywiście, zgodnie z RODO, takie informacje będą musiały być należycie chronione. Wprowadza się również uprawnienie podmiotu kluczowego i podmiotu ważnego do wezwania osoby do ponownego przedstawienia zaświadczenia o niekaralności za przestępstwa przeciwko ochronie informacji, jeżeli podmiot poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji. Podejrzenie to musi być uzasadnione, w jakimś mierze uprawdopodobnione. Przy czym sam anonim czy zgłoszenie od sygnalisty może być niewystarczające w tej mierze, ponieważ złośliwość ludzka nie zna granic i takie zgłoszenie może być po prostu aktem szkalującym inną osobę. Również uzasadnionym działaniem podmiotu kluczowego i podmiotu ważnego nie będzie cykliczne wzywanie danej osoby do przedstawienia zaświadczenia o niekaralności.

Koszt uzyskania zaświadczenia z Krajowego Rejestru Karnego wynosi 20 zł w wersji elektronicznej, także zdaniem wnioskodawcy nie jest to wygórowana kwota.

Wprowadzono wyjątek od obowiązku przedstawiania zaświadczenia o niekaralności – jest to sytuacja gdy dana osoba posiada ważne poświadczenie bezpieczeństwa upoważniające w zakresie dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej. Taka osoba została zweryfikowana w postępowaniu sprawdzającym, dlatego nie ma potrzeby dodatkowej weryfikacji jej niekaralności.

2.5.4. Obowiązki informacyjne dostawców usług zarządzanych z zakresu cyberbezpieczeństwa

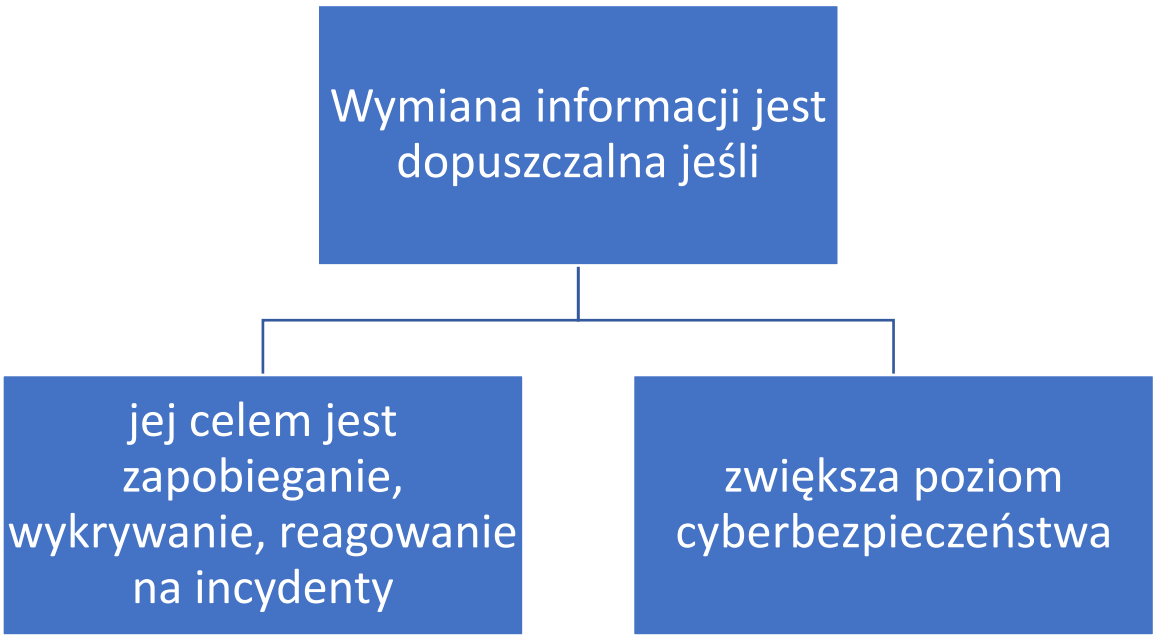
Nawiązując do powszechnej międzynarodowej praktyki (publikowanie informacji na podstawie wzoru zawartego w pkt. 3.3 dokumentu RFC 2350[24)]), nakłada się dla dostawców usług zarządzanych z zakresu cyberbezpieczeństwa obowiązek udostępniania na stronie internetowej podstawowych informacji o swojej działalności. W celu zrealizowania tego obowiązku wystarczy zamieścić krótki plik tekstowy na stronie internetowej dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa.

2.5.5. Dobrowolna wymiana informacji z zakresu cyberbezpieczeństwa

Przepisy projektu ustawy tworzą ramy do dobrowolnej wymiany informacji z zakresu cyberbezpieczeństwa pomiędzy podmiotami kluczowymi i podmiotami ważnymi. Jest to niezwykle istotne gdyż przekazanie informacji o zagrożeniach i atakach może pozwolić innym podmiotom zabezpieczyć swoje systemy i uchronić się przed zagrożeniem.

Dopuszczalna wymiana informacji o	cyberzagrożeniach	wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób
	potencjalnych zdarzeniach dla cyberbezpieczeństwa	zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych jednak nie wystąpiło lub, któremu udało się zapobiec
	podatnościach	właściwości produktu ICT lub usługi ICT, która mogą być wykorzystane przez cyberzagrożenie
	technikach	w tym kontekście - szczegółowy opis zachowania "actor" w kontekście jego taktyki - por. NIST-SP-800-150
	procedurach	drobiazgowy opis działania aktora w kontekście jego techniki - por. NIST-SP-800-150
	oznakach naruszenia integralności systemu informacyjnego	ang. indicators of compromise - mogą to być artefakty lub zdarzenia wskazujące na naruszenie integralności systemu - por. NIST-SP-800-150
	wrogich taktykach	generalny opis działania actora - por. NIST-SP-800-150
	grup przestępczych	grupy sponsorowane przez obce państwa działające agresywnie w cyberprzestrzeni grupy typu Private Sector Offensive Actors typowe grupy cyberprzestępców hacktywiści
	ostrzeżeniach dotyczących cyberbezpieczeństwa	porady, biuletyny, informacje o podatnościach, exploitach itd. przykładowo alerty amerykańskiej agencji CISA
	zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa	informacje o ustawieniu i skonfigurowaniu narzędzi służących automatycznemu zbieraniu, wymianie analizie i wykorzystaniu informacji o cyberzagrożeniach

24) https://datatracker.ietf.org/doc/html/rfc2350 .
Jako przykłady praktyki można wskazać:
https://www.knf.gov.pl/knf/pl/komponenty/img/RFC2350.pdf
https://www.csirt.gov.sk/csirt-sk-description-document-according-to-rfc-2350.html
https://www.ncsc.gov.ie/pdfs/RFC2350%20NCSC-IE.txt.



Komunikacja w tych sprawach ma odbywać się w systemie S46, który będzie dedykowanym kanałem komunikacji do kwestii cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa mogą również zawierać porozumienia dotyczące wzajemnej wymiany informacji. Takie porozumienia mogą stać się podstawą do wymiany informacji w danym sektorze i pozwolą usprawnić przepływ informacji tak aby informacje docierały do podmiotów, które tego najbardziej potrzebują. Porozumienia mogą być zawierane również przez organizacje społeczne zrzeszające podmioty kluczowe i podmioty ważne – przykładowo izby gospodarcze. Należy podkreślić, że przepis ten umieszcza w ramach ustawy również już funkcjonujące porozumienia, np. ISAC-Kolej. Nie zdecydowano się przy tym na nadanie osobowości prawnej inicjatywom typu ISAC tudzież nadania im statusu ułomnej osoby prawnej. W polskiej praktyce kilka istniejących tego typu inicjatyw ma charakter luźnych porozumień. Postanowiono więc nie zmieniać tego stanu rzeczy. Wprowadzenie formy prawnej ISAC jako (ułomnej) osoby prawnej powodowałoby dodatkowe obowiązki po stronie ISAC np. obowiązek prowadzenia uproszczonej rachunkowości. Wprowadzono przy tym przepis względnie obowiązujący, zgodnie z którym koszt wykonania porozumień o wymianie informacji ponoszą w równych częściach strony porozumienia, chyba, że postanowią one inaczej. Przykładowo może zaistnieć z pozoru banalna kwestia – kto ma zapłacić za utrzymanie strony internetowej ISAC.

2.5.6. Kolizja przepisów ustawy i rozporządzenia DORA

W zakresie sektora bankowego i infrastruktura rynków finansowych ustawa wskazuje, że pierwszeństwo przed nią mają przepisy rozporządzenia DORA. Ma to wyeliminować wątpliwości wynikające z funkcjonowania w tym obszarze, tych dwóch aktów prawnych. Dyrektywa NIS 2 w artykule 4 wskazuje na pierwszeństwo sektorowych aktów unijnych z zakresu Cyberbezpieczeństwa w zakresie środków zarządzania ryzykiem oraz zgłaszania incydentów. Komunikat Komisji – Wytyczne Komisji dotyczące stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) 2023/C 328/02 (Dz.Urz. UE C 328 z 18.9.2023, str. 2) wskazuje, że rozporządzenie DORA jest takim aktem w zakresie podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych. Zgodnie z proponowanym art. 8i pierwszeństwo nad ustawą o KSC mają regulacje DORA, z tym że do podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych stosuje się przepisy art. 3a (czynności dopuszczalne w ramach obsługi incydentów), art. 5 ust. 1–3 (kryteria podmiotu kluczowego i podmiotu ważnego), art. 5a ust. 1 (zasada, że podmiot kluczowy/podmiot ważny podlega obowiązkom ustawy, jeśli ma na terenie RP jednostkę organizacyjną), art. 7–7m (przepisy o wykazie podmiotów kluczowych i podmiotów ważnych), art. 8 ust. 1 pkt 1 (obowiązek prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu) i pkt 2 lit. j (obowiązek stosowania podstawowych zasad cyberhigieny), art. 8h (dopuszczalność wymiany informacji), art. 9 (obowiązki w zakresie wyznaczenia osób kontaktowych), art. 11 ust. 1 pkt 5 i 6 (współdziałanie z CSIRT podczas zgłoszenia incydentów), art. 13 (dobrowolne przekazywanie informacji do CSIRT), art. 15 (audyty), art. 16 (stosowanie obowiązków po raz pierwszy), art. 26a ust. 2–4 (zgłoszenia podatności w ramach skoordynowanego ujawniania podatności), art. 32 (uprawnienie CSIRT do wykonywania niezbędnych działań technicznych), art. 33 ust. 5, 7 oraz 8 (rekomendacje Pełnomocnika), art. 36a, art. 36b (ocena bezpieczeństwa), art. 37 (wyłączenie ustawy z dnia 6 września 2021 r. o dostępie do informacji publicznej przy informacjach o podatnościach, incydentach i cyberzagrożeniach), art. 43 (uprawnienie organu do żądania informacji), art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i oraz ust. 4–6 (obowiązek korzystania z S46), art. 67a (rekomendacje Pełnomocnika), art. 67c, art. 67d oraz, art. 67g, art. 67h oraz art. 67i (postępowanie w sprawie uznania za dostawcę wysokiego ryzyka oraz polecenie zabezpieczające).

2.5.7. Obowiązki podmiotów kluczowych w zakresie kontaktów z innymi podmiotami i użytkownikami

Podmioty kluczowe i podmioty ważne muszą również wyznaczyć dwie osoby do kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa. To rozwiązanie wynika z dotychczasowych doświadczeń w ramach krajowego systemu cyberbezpieczeństwa. Dotychczasowy obowiązek wyznaczenia jednej osoby do kontaktu sprawiał, że w przypadku gdy osoba ta przebywała na zwolnieniu lekarskim lub z innych powodów była nieobecna w pracy, zespoły CSIRT miały trudności ze skontaktowaniem się z podmiotami, w których wystąpił incydent. Dwie osoby mają zagwarantować, że zawsze będzie można nawiązać kontakt. Podmiot będący mikroprzedsiębiorcą lub małym przedsiębiorcą wyznaczy jedną osobę, ponieważ obowiązek wyznaczenia dwóch osób mógłby być zbyt dużym obciążeniem.

Podmioty te mają również obowiązek zapewniania użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami. Użytkownicy muszą posiadać aktualne informacje, aby być w stanie chronić się przed zagrożeniami.

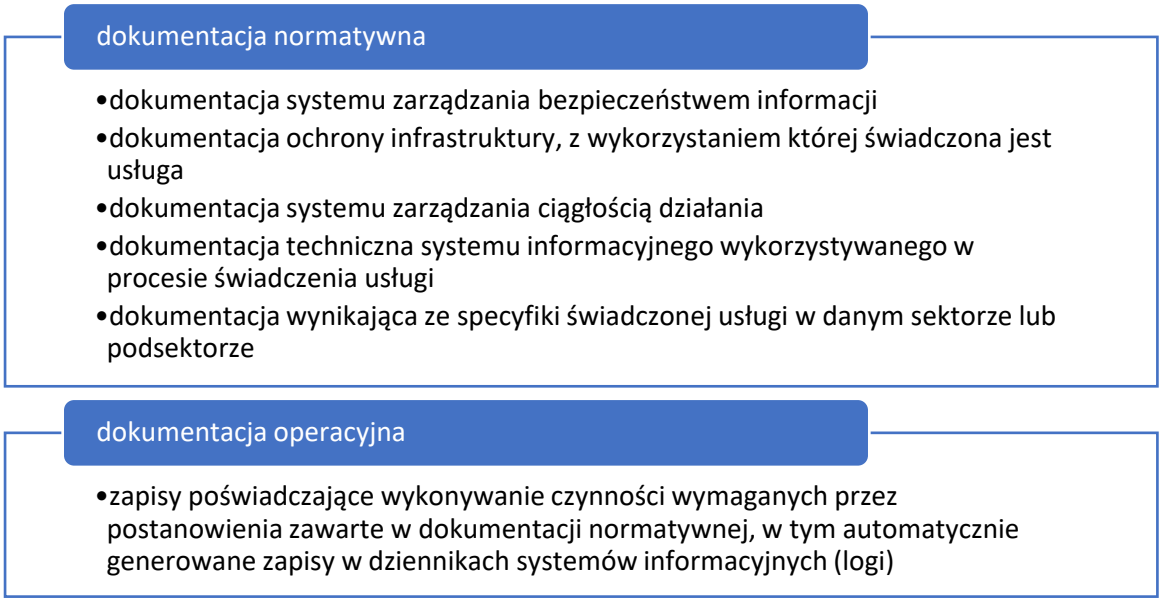
Każdy podmiot kluczowy oraz podmiot ważny powinien zapewnić możliwość zgłaszania przez swoich użytkowników cyberzagrożeń, podatności czy incydentu związanego z usługą świadczoną przez podmiot. Forma zgłoszenia należy już do podmiotu – czy to będzie odrębny adres poczty elektronicznej, czat na stronie internetowej, adres do doręczeń elektronicznych w przypadku podmiotów zobowiązanych do stosowania ustawy o doręczeniach elektronicznych.

2.5.8. Dokumentacja SZBI

Przepisy projektu ustawy precyzują również kwestię dokumentacji jaką musza przechowywać podmioty kluczowe i podmioty ważne. W tym zakresie przeniesiono dotychczasowe przepisy rozporządzenia i nadano im rangę ustawową. Dokumentacja dotyczy bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Prowadzona będzie w postaci elektronicznej lub papierowej.

Zakres dokumentacji podzielono na 2 części. Dokumentacja normatywna to ta część dokumentacji, która opisuje świadczoną usługę, systemy, infrastrukturę oraz funkcjonowanie bezpieczeństwa informacji w podmiocie. Dokumentacja operacyjna potwierdza wykonywanie czynności opisanych w dokumentacji normatywnej.

Rysunek 2 Dokumentacja w nowelizacji ustawy o KSC



Rysunek 3 Zakres przedmiotowy dokumentacji ochrony infrastruktury

Dokumentacja ochrony infrastruktury obejmuje:	charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa
	ocenę aktualnego stanu ochrony infrastruktury
	szacowanie ryzyka dla obiektów infrastruktury
	plan postępowania z ryzykiem
	opis zabezpieczeń technicznych obiektów infrastruktury
	zasady organizacji i wykonywania ochrony fizycznej infrastruktury
	dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995), chroniącej infrastrukturę

Podkreślić należy, że przepis wskazuje zakres przedmiotowy dokumentacji. Może powstać z tego jeden dokument albo kilka. To należy już do decyzji podmiotu kluczowego i podmiotu ważnego. Istotne jest, aby zakres dokumentacji został zachowany.

Ważne jest, aby podmiot dbał o bezpieczeństwo dokumentacji. Należy zapewnić dostępność dokumentacji dla uprawnionych osób (zasada need to know) w zakresie niezbędnym do realizacji zadań. Ograniczy to ryzyko ujawnienia informacji z dokumentacji osobom nieuprawnionym. Podmiot powinien także chronić dokumenty pod kątem fizycznym – ochrona przed uszkodzeniem (uszkodzenie papieru czy dysku), zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności. Pamiętać także należy o oznaczaniu kolejnych wersji dokumentów – ułatwi to identyfikację zmian i odnalezienie aktualnej wersji.

2.6. Zgłaszanie incydentów

Dyrektywa NIS 2 wprowadziła nowe rozwiązania w zakresie zgłaszania incydentów poważnych. Zgodnie z proponowanymi rozwiązaniami incydenty poważne zgłaszane będą do CSIRT sektorowego. Wskazanie CSIRT sektorowego jako podmiotu przyjmującego zgłoszenie o incydencie związane jest z zadaniami jakie CSIRT ten będzie realizował, tj. oprócz reagowania na incydenty, współpraca z podmiotami kluczowymi i ważnymi z danego sektora, dzięki temu CSIRT sektorowy będzie znał specyfikę danego sektora co umożliwi skuteczną obsługę incydentów. Zgłoszenie wczesnego ostrzeżenia i zgłoszenie incydentu poważnego będzie dokonywane za pośrednictwem systemu S46, takie rozwiązanie spowoduje, iż informacja o tych zgłoszeniach będzie dostępna dla pozostałych CSIRT, w tym również CSIRT poziomu krajowego. W pierwszej kolejności podmiot kluczowy i podmiot ważny zobowiązany będzie do zgłoszenia wczesnego ostrzeżenia o incydencie poważnym niezwłocznie nie później niż w ciągu 24 godzin od momentu wykrycia incydentu poważnego. Zgłoszenie wczesnego ostrzeżenia może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o dodatkowe wsparcie techniczne przy obsłudze incydentu. Jeżeli incydent poważny wyczerpuje znamiona przestępstwa CSIRT sektorowy przekazuje informacje o sposobie zgłoszenia tego faktu organom ścigania. CSIRT sektorowy zobowiązany będzie w terminie 24 godzin udzielić wsparcia zgodnie z treścią wniosku.

Wczesne ostrzeżenie zawiera m.in. dane podmiotu zgłaszającego, w tym dane kontaktowe do osób uprawnionych do składania wyjaśnień oraz informacje o momencie wystąpienia incydentu poważnego.

Natomiast w ciągu 72 godzin podmiot kluczowy i podmiot ważny zgłasza incydent poważny wraz z dodatkowymi informacjami o tym incydencie, m.in. opis wpływu incydentu na świadczone usługi, opis przyczyn incydentu, a także informacje o podjętych dzianiach.

W trakcie obsługi incydentu poważnego podmiot zgłaszający incydent, na wniosek CSIRT sektorowego, przekazują sprawozdanie okresowe z obsługi tego incydentu. Natomiast sprawozdanie końcowe z obsługi incydentu poważnego przekazywane będzie nie później niż w ciągu miesiąca od dnia zgłoszenia incydentu. Jeżeli jednak obsługa incydentu poważnego nie zakończyła się w terminie miesiąca podmiot zgłaszający incydent poważny przesyła sprawozdanie z postępu obsługi incydentu, a sprawozdanie końcowe w terminie miesiąca od zakończenia obsługi tego incydentu.

Progi uznania incydentu za incydent poważny zostaną określone w drodze rozporządzenia przez Radę Ministrów. Przy czym w tym rozporządzeniu nie będą określone progi incydentów dla podmiotów, dla których progi te ustaliła Komisja Europejska w bezpośrednio stosowalnym akcie wykonawczym wydanym na podstawie art. 23 ust. 11 dyrektywy NIS 2. Prawo krajowe nie może wkraczać w kwestie uregulowane bezpośrednio stosowalnym akcie prawa unijnego.

Obecny art. 13 ustawy o KSC umożliwia dobrowolne zgłaszanie do zespołów CSIRT poziomu krajowego jak również CSIRT sektorowego informacji o incydentach nie podlegających obowiązkowemu zgłoszeniu, o cyberzagrożeniach, wynikach szacowania ryzyka, podatnościach, potencjalnych zdarzeniach dla Cyberbezpieczeństwa czy wykorzystywanych technologiach[25)]. Przepis ten dostosowano do innych zmian, rozszerzając te uprawnienie na wszystkie podmioty kluczowe i podmioty ważne. Dodatkowo wskazano, że zgłoszenia te są dokonywane za pomocą systemu S46. Jest to ważny przepis ponieważ umożliwia dzielenie się informacjami z zespołami CSIRT, które mogą przeanalizować je i wyciągnąć wnioski, które pozwolą na lepsze wspieranie podmiotów kluczowych i podmiotów ważnych. Przykładowo informacje o podatnościach pozwolą na opracowanie sposobów ich mitygacji. Zapewniono przy tym możliwość ochrony informacji prawnie chronionych – w tym celu podmiot kluczowy i podmiot ważny ma obowiązek oznaczyć tego rodzaju informacje.

Tak jak przy obecnej treści ustawy o KSC przepisy będą od tej pory wskazywać, że podmiot kluczowy lub podmiot ważny realizuje zadania za pomocą wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo (np. komórka organizacyjna w danym podmiocie, niezależnie od jej nazwy, ale zajmująca się cyberbezpieczeństwem) lub zawiera umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa. Kluczowy jest tutaj spójnik „lub” – chodzi o możliwość outsourcingu tylko niektórych zadań. Decyzja o wyborze modelu

[25)] Technologie należy rozumieć szeroko, jako produkty, usługi, procesy ICT.

realizacji zadań należy do podmiotu kluczowego lub podmiotu ważnego. Podkreślić jednak należy, że musi być ona rozsądna. Zadania z zakresu cyberbezpieczeństwa nie powinny być powierzane np. przeciążonemu działowi help-desk, ponieważ nie będą one realizowane efektywnie.

Traci moc rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. z 2019 r. poz. 2479), które było wydane na podstawie obecnego art. 14 ustawy o KSC. Przede wszystkim dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się pod rządami znowelizowanej ustawy dostawcami usług zarządzanych z zakresu cyberbezpieczeństwa i będą podlegali wymogom wdrożenia systemu zarządzania bezpieczeństwem informacji. Wprowadzanie odrębnych wymogów dla nich jest zbędne, wobec tego przepisy ww. rozporządzenia wymagają uchylenia.

2.7. Audyt

Podmioty kluczowe mają obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 3 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Musi on być przeprowadzony przez podmiot posiadający odpowiednią akredytację, dwóch audytorów legitymujących się odpowiednimi certyfikatami i doświadczeniem lub przez CSIRT sektorowy. Audyty na zgodność należy rozumieć jako przeprowadzane na zgodność z przepisami ustawy. Audyt, o którym mowa w projektowanym art. 15 ust. 1, może być audytem wewnętrznym lub zewnętrznym. Te przepisy są analogiczne do obecnych rozwiązań w tym zakresie i nie wprowadzają istotnych zmian.

Raportu z audytu musi być przekazany w postaci elektronicznej do organu właściwego do spraw cyberbezpieczeństwa w terminie 3 dni roboczych od otrzymania go od audytorów przez podmiot kluczowy. Jest to niezbędne, gdyż analiza raportów audytowych będzie jednym ze skuteczniejszych środków nadzorczych przy tak dużej liczbie podmiotów podlegających ustawie. Wskazać jednak należy, że przekazanie raportu w tym terminie odnosi się do kopii tego raportu i dokonywane jest drogą elektroniczną.

Ponadto wdrożono tutaj postanowienia dyrektywy NIS 2 i wskazano, że organ właściwy do spraw cyberbezpieczeństwa będzie mógł nakazać przeprowadzenie audytu doraźnego przez podmiot kluczowy lub podmiot ważny. Audyt ten jest audytem zewnętrznym. Będzie on mógł

zostać zlecony w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez podmiot kluczowy lub podmiot ważny. W decyzji nakazującej przeprowadzenie audytu doraźnego organ właściwy do spraw cyberbezpieczeństwa określi termin przekazania raportu z przeprowadzonego audytu i wskaże podmioty uprawnione do jego przeprowadzenia uwzględniając przepisy ustawy. Będzie mógł także określić zakres audytu. Brak określenia zakresu audytu równoważny jest z obowiązkiem przeprowadzenia audytu w pełnym zakresie.

Audyt systemu zarządzania bezpieczeństwem informacji musi być przeprowadzany przez audytorów obiektywnych, którzy nie będą stronniczy wobec podmiotu audytowanego. Dlatego wprowadza się regulację, zgodnie z którą audyt nie może być przeprowadzony przez osoby, które w podmiocie audytowanym przez rok przed rozpoczęciem audytu realizowały zadania z zakresu systemu zarządzania bezpieczeństwem informacji oraz zgłaszania i reagowania na incydenty lub realizuje je nadal.

Ponadto realizacja obowiązku co do zapewnienia przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi nie zwalnia administratora – wykonawcy obowiązków z ustawy o KSC – z obowiązków wynikających z RODO w zakresie realizacji zasady poufności i integralności i konieczności wdrożenia odpowiednich środków technicznych i organizacyjnych z uwzględnieniem analizy ryzyka.

2.8. Wdrożenie obowiązków przez podmioty kluczowe i podmioty ważne po raz pierwszy

Należało przesądzić od kiedy podmioty kluczowe i podmioty ważne będą miały obowiązek wdrożenia obowiązków wynikających z nowelizacji ustawy o KSC. Obecnie momentem, od którego liczą się terminy na wdrożenie obowiązków przez operatorów usług kluczowych, jest doręczenie decyzji o uznaniu za operatora usługi kluczowej. W projektowanych przepisach wskazano, że podmiot kluczowy i podmiot ważny realizuje swoje obowiązki w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. Audyt systemu będzie realizowany po raz pierwszy w terminie 24 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy.

2.9. Zadania i obowiązki rejestrów nazw domen najwyższego poziomu oraz zadania i obowiązki podmiotów świadczących usługi rejestracji nazw domen

Projekt ustawy nakłada szczególne obwiązki na rejestr nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen w zakresie gromadzenia i zachowywania z należytą starannością danych dotyczących rejestracji nazw domen. Podmioty te mają wprowadzić polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych rejestracji domen zawierały dokładne i kompletne dane. Jest to szczególnie istotne gdyż informacje o domenach mogą być szczególnie istotne przy wykrywaniu źródeł cyberataków oraz niebezpiecznego ruchu sieciowego. Polityki w tym zakresie muszą też być podane do publicznej wiadomości co gwarantuje transparentność tego procesu. Dane z rejestru będą również udostępniane na wniosek:

1) sądu – w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia lub w postępowaniu cywilnym;

2) prokuratora – w celu przeprowadzenia dowodu w postępowaniu karnym lub postępowaniu w sprawach o wykroczenia;

3) Policji oraz innych upoważnionych organów w postępowaniu karnym i postępowaniu w sprawach o wykroczenia, w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia.

Pozwoli to na zwiększenie skuteczności walki z przestępczością w internecie, a w szczególności ze stronami internetowymi służącymi podszywaniu się pod inne podmioty.

2.10. Uchylenie rozdziału o obowiązkach dostawcach usług cyfrowych i podmiotów publicznych

Ze względu na zmiany w strukturze krajowego systemu cyberbezpieczeństwa uchyla się rozdziały 4 i 5 ustawy o KSC dotyczące obowiązków dostawców usług cyfrowych i podmiotów publicznych. Te podmioty, zgodnie z dyrektywą NIS 2, staną się podmiotami kluczowymi i podmiotami ważnymi, w związku z czym nie jest zasadne utrzymywanie dla nich osobnych regulacji.

2.11. Uwspólnienie zadań z zakresu Cyberbezpieczeństwa w podmiotach publicznych

Przepisy projektu ustawy umożliwiają ministrowi kierującemu działem administracji publicznej, kierownikowi urzędu centralnego, wojewodzie oraz jednostce samorządu

terytorialnego wyznaczenie jednostki, która będzie realizowała zadania z zakresu cyberbezpieczeństwa w pozostałych jednostkach podległych danemu organowi. Rozwiązanie to ma być elastyczne i z jednej strony zapewnić, że nawet najmniejsze jednostki budżetowe będą w krajowym systemie cyberbezpieczeństwa, z drugiej strony, że obowiązki te będą realizowane przez wyspecjalizowany podmiot działający na rzecz wielu podmiotów publicznych.

2.12. Zadania zespołów CSIRT

2.12.1. Zadania CSIRT

Zadania CSIRT zostały rozszerzone i doprecyzowane w dyrektywie NIS 2 co znalazło odzwierciedlenie w ich nowym katalogu. Należy podkreślić, że część z tych zadań, np. przetwarzanie danych kryminalistycznych, było już realizowane przez zespoły CSIRT na podstawie obecnych przepisów. Projektowane przepisy pozwolą uporządkować te zadania i zwiększyć spójność krajowego systemu cyberbezpieczeństwa.

W związku z nową rolą CSIRT sektorowych wskazano, że udzielając wsparcia podmiotom krajowego systemu cyberbezpieczeństwa informuje o tym odpowiedni CSIRT sektorowy. Pozwoli to uniknąć dublowania działań przez te podmioty.

Projektowane przepisy dają też możliwość Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa zlecenia udzielenia wsparcia przez CSIRT poziomu krajowego innemu podmiotowi krajowego systemu cyberbezpieczeństwa. W przypadku CSIRT GOV i CSIRT MON na takie zlecenie muszą wyrazić zgodę organy prowadzące taki CSIRT. To uprawnienie pozwoli Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa skutecznie reagować na zagrożenia i szybko zapewnić niezbędne wsparcie podmiotom dotkniętym incydentami. Przepisy dopuszczają wyrażenie zgody na udzielenie zgody ustnie oraz z wykorzystaniem środków porozumiewania się na odległość. Jest to konieczne, aby reakcja była odpowiednio szybka w sytuacji incydentu.

2.12.2. Ujawnianie podatności

CSIRT NASK będzie realizował zadania w zakresie skoordynowanego ujawniania podatności w Unii Europejskiej. W tym zakresie będzie on przyjmował zgłoszenia o wystąpieniu podatności, a następnie kontaktował się z producentami lub dostawcami danych produktów i usług w celu ustalenia sposobu i harmonogramu likwidacji podatności. Należy podkreślić, że CSIRT nie będzie posiadał kompetencji władczych w tym zakresie, w związku

z czym eliminacja podatności i jej sposób pozostaną w gestii właściciela danego produktu lub usługi. Równocześnie przepisy ustawy pozwalają CSIRT wydać ostrzeżenie lub zwrócić się do Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa o wydanie rekomendacji dotyczących niekorzystania z określonego sprzętu. W związku z tym, posiada on narzędzia, którymi może wpływać na te podmioty. Pozwoli to zwiększyć bezpieczeństwo produktów ICT i usług ICT dostępnych dla konsumentów.

W ramach tych zadań informacje o podatnościach będą przesyłane do Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji, zwanej dalej „ENISA", tak aby chronić konsumentów w całej Unii Europejskiej.

2.12.3. Działania w zakresie obsługi incydentu

Przepisy projektu ustawy doprecyzowują działania zespołów CSIRT w zakresie koordynacji obsługi incydentu. W trakcie koordynacji obsługi incydentu poważnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV mogą wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem, aby w wyznaczonym terminie usunął podatności lub o udzielenie informacji niezbędnych do koordynacji tego procesu. Daje to gwarancje, że zespoły CSIRT będą w stanie szybko wprowadzić środki naprawcze przy obsłudze incydentu. Jest to szczególnie istotne w przypadku incydentów, które mają skutki dla wielu podmiotów, gdzie współpraca podmiotu dotkniętego incydentem jest szczególnie istotna. Dzięki pozyskiwanym informacjom zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe będą również w stanie skutecznie informować inne podmioty o wykrytych podatnościach, zwiększając ich bezpieczeństwo.

2.12.4. Badanie produktów ICT

Doprecyzowano kwestie związane z prowadzeniem badań przez zespół CSIRT. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, nie będą związane postanowieniami umów licencyjnych badanych urządzeń i oprogramowania, które ograniczają możliwość przeprowadzenia badania.

Wskazane wyżej uprawnienia zespołu prowadzącego badanie są konieczne do zapewnienia ochrony bezpieczeństwa państwa. Niektóre postanowienia umów licencyjnych mogłyby uniemożliwić realizację tego zadania. Zespół CSIRT prowadzący badanie nie powinien być ograniczony licencją twórcy złośliwego oprogramowania, którego wykorzystanie zagraża bezpieczeństwu państwa, w tym np. bezpieczeństwu infrastruktury krytycznej. W zakresie badania sprzętu lub oprogramowania należy zwrócić uwagę,

że standardowe umowy licencyjne nie przewidują możliwości dokonywania badania sprzętu pod kątem jego bezpieczeństwa ani też testowania konkretnych rozwiązań zastosowanych w danym produkcie. Konieczność uzyskania zgody właściciela licencji na takie działania często jest niemożliwa do uzyskania w drodze umowy zawieranej na ogólnych zasadach. Producenci nie mają bowiem interesu w umożliwianiu podmiotom zewnętrznym takich działań. Równocześnie rosnąca liczba cyberzagrożeń oraz zależność kluczowych usług od systemów teleinformatycznych sprawia, że konieczne jest, by administracja publiczna dysponowała narzędziem, które pozwoli jej przeprowadzić takie badanie. Brak tych przepisów mógłby prowadzić do powstania sytuacji, w której CSIRT poziomu krajowego musiałby uzyskać zgodę dostawcy potencjalnie niebezpiecznego sprzętu na przeprowadzenie jego badania, nawet w wypadku gdyby powstało uzasadnione podejrzenie, że dany produkt może być wykorzystany do wywołania incydentu. W związku z powyższym, przepisy te są niezbędne dla zapewnienia bezpieczeństwa podmiotom krajowego systemu cyberbezpieczeństwa.

Celem regulacji jest umożliwienie zespołom CSIRT poziomu krajowego skuteczne badanie produktów ICT i usług ICT pod kątem zagrożeń dla bezpieczeństwa narodowego.

Zaproponowana regulacja jest w stanie doprowadzić do realizacji tego celu – wprowadza bowiem licencję ustawową na badanie tych produktów i usług. Ta licencja ustawowa jest niezbędna do ochrony bezpieczeństwa państwa – wykorzystywanie produktów ICT i usług ICT zawierających podatności umożliwiające np. zaprzestanie działania systemów automatyki przemysłowej elektrowni, uniemożliwienie dostaw paliw czy znaczne zwiększenie chloru w zakładzie wodociągowych grozi zagrożeniem dla funkcjonowania państwa i jego obywateli. Proponowane rozwiązania są proporcjonalne – korzyści dla państwa i obywateli z identyfikacji niebezpiecznych produktów i usług przewyższają obciążenia dla producentów oprogramowania. Licencja jest powiązana tylko z badaniem, o którym mowa w projektowanym art. 33 ustawy o KSC. Licencja nie może służyć np. uzyskaniu oprogramowania do bieżącej działalności zespołów CSIRT. Stąd też należy uznać, że przepisy te spełniają wymóg testu proporcjonalności.

Wprowadza się także uprawnienie dla CSIRT MON, CSIRT NASK i CSIRT GOV zażądania od dostawcy badanego produktu ICT, usługi ICT lub procesu ICT dokumentacji, co pozwoli na skuteczne przeprowadzenie badania. Doświadczenia z dotychczasowych badań wykazały niechęć do przekazywania informacji przez producentów sprzętu lub oprogramowania, co utrudniało przeprowadzenie badania.

2.13. Zespół Incydentów Krytycznych

Projekt ustawy zakłada, że prowadzenie Zespołu przejmie od Dyrektora Rządowego Centrum Bezpieczeństwa Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa. Dotychczasowa praktyka prac Zespołu pokazała, że takie rozwiązanie będzie bardziej efektywne.

2.14. Ocena bezpieczeństwa

Wprowadza się możliwość przeprowadzania przez CSIRT GOV, CSIRT MON, CSIRT NASK i CSIRT sektorowe, oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. Przepisy tego rozdziału były wzorowane na art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812 i 1222)[26)], zwanej dalej „ustawą o ABW i AW". Wprowadzono jednak kilka istotnych zmian w stosunku do pierwowzoru. Przede wszystkim wyłącza się stosowanie tego przepisu do ocen bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy o ABW i AW. Bez tego wyłączenia powstałyby dwie podstawy prawne do przeprowadzania ocen bezpieczeństwa wobec podmiotów krajowego systemu cyberbezpieczeństwa, które są jednocześnie operatorami infrastruktury krytycznej. Nie jest to sytuacja pożądana.

Ponadto wyłącza się stosowanie rozdziału 6b do systemów teleinformatycznych akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222). Są to systemy służące przetwarzaniu informacji niejawnych i tutaj pierwszeństwo powinny mieć przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Wprowadzono jasne określenie właściwości CSIRT poziomu krajowego do przeprowadzania ocen bezpieczeństwa – nawiązuje ono do ogólnej właściwości zespołów CSIRT określonej w art. 26 ust. 5–7. CSIRT sektorowe będą mogły przeprowadzać ocenę bezpieczeństwa wobec operatorów usług kluczowych w danym sektorze.

[26)] Podsumowanie ocen bezpieczeństwa wykonywanych przez Agencję Bezpieczeństwa Wewnętrznego znajduje się w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* str. 43–52 https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/977,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2021-roku.html.

Wprowadza się również regułę, że przeprowadzanie oceny bezpieczeństwa powinno być uzgodnione z właściwym CSIRT poziomu krajowego. Jest to po to, aby w tym samym czasie nie były prowadzone oceny bezpieczeństwa przez kilka zespołów. Jednocześnie wprowadza się obowiązek poinformowania odpowiednio organu właściwego do spraw cyberbezpieczeństwa czy Prezesa Urzędu Komunikacji Elektronicznej o zamiarze wykonania oceny bezpieczeństwa.

Ocena bezpieczeństwa będzie mogła być przeprowadzona wyłącznie za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w postaci pisemnej lub elektronicznej pod rygorem nieważności. Jest to duża różnica względem art. 32a ustawy o ABW i AW, zgodnie z którym Szef ABW decyduje o włączeniu systemu teleinformatycznego operatora infrastruktury krytycznej do rocznego planu przeprowadzania ocen bezpieczeństwa. Jednakże dyrektywa NIS 2 przewiduje także przeprowadzanie *security scans* wobec podmiotu kluczowego lub podmiotu ważnego. Dlatego wprowadza się możliwość przeprowadzenia oceny bezpieczeństwa na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

Celem oceny bezpieczeństwa jest pomoc w identyfikacji podatności. Ma ona charakter prewencyjny. Jednakże prowadzenie tej oceny nie może zaszkodzić systemowi informacyjnemu, a szerzej podmiotowi, który korzysta z tego systemu i świadczy usługi dla swoich klientów. Dlatego wprowadza się zasadę, zgodnie z którą czynności przeprowadzane w ramach oceny bezpieczeństwa powinny w jak najmniejszym stopniu zakłócać funkcjonowanie tego systemu lub ograniczać jego dostępność (dodawany art. 36b ust. 2). Tym bardziej nie jest dopuszczalne, aby działania te doprowadziły do nieodwracalnego zniszczenia danych w systemie poddanym ocenie. Przepis ten ma stanowić ogólną zasadę dla osób przeprowadzających ocenę bezpieczeństwa i stanowi gwarancję dla podmiotu krajowego systemu cyberbezpieczeństwa, wobec którego prowadzona jest ocena bezpieczeństwa.

Po uzyskaniu zgody od podmiotu krajowego systemu cyberbezpieczeństwa albo po otrzymaniu zlecenia od organu właściwego do spraw cyberbezpieczeństwa, CSIRT przeprowadzający ocenę bezpieczeństwa będzie obowiązany uzgodnić tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa (art. 36e ust. 3).

Zespół CSIRT przeprowadzający ocenę bezpieczeństwa otrzyma dwa ważne uprawnienia, które są niezbędne do skutecznego przeprowadzenia takiej oceny (dodawany art. 36b ust. 4 i 5).

Po pierwsze, będzie uprawniony do wytworzenia lub pozyskania urządzeń lub oprogramowania przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4[27], art. 267 § 3[28], art. 268a[29] § 1 albo § 2 w związku z § 1, art. 269 § 1[30] lub 2 albo art. 269a[31] Kodeksu karnego, aby móc sprawdzić, czy oceniany system jest podatny na tego rodzaju oprogramowanie.

Po drugie, używając ww. urządzeń lub programów zespół CSIRT będzie uprawniony do dostępu do informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Będzie mógł uzyskać dostęp do całości lub części ocenianego systemu. Wprowadza się przy tym kontratyp, zgodnie z którym osoba wykonująca te czynności nie popełnia przestępstwa, o którym mowa w art. 267 § 1 Kodeksu karnego.

Bez tego rodzaju szczególnych uprawnień zespół CSIRT nie będzie w stanie zidentyfikować podatności, które mogą być wykorzystane przez przestępców komputerowych do zaatakowania podmiotu krajowego systemu cyberbezpieczeństwa.

Aby zapewnić gwarancje dla podmiotu, u którego jest przeprowadzana ocena ,wprowadza się przepis, na mocy którego informacje uzyskane w wyniku oceny stanowią tajemnicę prawnie chronioną. Zespół CSIRT nie będzie mógł wykorzystać ich do realizacji innych zadań ustawowych. Informacje te będą podlegały niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

---

[7] Przestępstwo polegające na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach w ramach którego sprawca zakłóca, uniemożliwia lub w inny sposób wpływaj na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych.

[28] Przestępstwo w którym sprawca w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

[29] Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

[30] Przestępstwo w którym sprawca niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

[31] Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej.

Końcowym etapem oceny bezpieczeństwa będzie sporządzenie przez CSIRT raportu, który będzie zawierał podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Raport będzie przekazany do podmiotu, którego system był poddany ocenie bezpieczeństwa. Dzięki temu podmiot będzie mógł przeanalizować np. jak jego personel, odpowiedzialny za bezpieczeństwo systemu, zachowywał się podczas oceny bezpieczeństwa, czy procedury bezpieczeństwa zadziałały prawidłowo, a także czy i jakie podatności zostały wykryte podczas oceny bezpieczeństwa.

W wyniku prowadzonej przez zespół CSIRT oceny bezpieczeństwa może zostać zidentyfikowana podatność, która może występować w innych systemach informacyjnych, które np. wykorzystują to samo oprogramowanie zawierające podatność. W takiej sytuacji zasadne jest, aby zespół CSIRT był obowiązany poinformować o tym:

1) ministra właściwego do spraw informatyzacji – z uwagi na to, że minister jest właściwy w sprawach systemów i sieci teleinformatycznych administracji publicznej[32)];
2) Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa – z uwagi na to, że do zadań Pełnomocnika należy ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, a także może on przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie (art. 63 ustawy o KSC).

Dodano także upoważnienie ustawowe dla Rady Ministrów do określenia, w drodze rozporządzenia, sposobu niszczenia materiałów zawierające informacje, które zespół CSIRT uzyskał w trakcie przeprowadzania oceny bezpieczeństwa, a także tryb działania komisji jak i wzór protokołu. Przy wydaniu rozporządzenia powinien być wzięty pod uwagę rodzaj materiałów podlegających zniszczeniu. W szczególności chodzi tutaj o tajemnice prawnie chronione.

[32)] Art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. 2024 r. poz. 1370).

2.15. Zasady udostępniania informacji i przetwarzania danych osobowych

2.15.1. Zmiany w zakresie przepisów o przetwarzaniu danych osobowych

Obecne przepisy o przetwarzaniu danych osobowych dostosowano do zmian wprowadzonych w pozostałej części ustawy. Przyznano uprawnienia zespołom CSIRT sektorowym do przetwarzania danych osobowych co jest konieczne do realizacji ich zadań.

Dodano wyłączenie stosowania ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów. Wskazać należy, że zgłoszenie incydentu może zawierać wrażliwe dane dotyczące kluczowych dla państwa podmiotów gospodarczych, takich właśnie jak podmioty kluczowe i podmioty ważne. Udostępnienie informacji o tym, że u konkretnego operatora usługi kluczowej, np. elektrociepłowni, szpitalu czy kopalni, wystąpiły podatności w systemach informacyjnych czy incydenty poważne, może zachęcić przestępców lub podmioty nieprzychylne Państwu do dokonania cyberataku na te podmioty. Z tego też powodu projektodawca uważa, że znajdzie zastosowanie artykuł 1 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 2019/1024 z 26.06.2019) ze względu na konieczność ochrony bezpieczeństwa narodowego.

Incydenty mogą być związane z różnego rodzajami danymi, w tym z danymi osobowymi. Jako przykład można wskazać zdarzenie, w którym dzienniki połączeń konsumentów zostały wykradzione lub numery telefonów użytkowników końcowych oraz numery IMSI zostały upublicznione. Atak na sieć, z której korzysta podmiot świadczący usługi OTT może spowodować utratę poufności i dostęp do wiadomości o użytkownikach, np. komunikatorów internetowych. Z kolei wskutek ataku mogłaby zostać zaszyfrowana baza abonentów przedsiębiorcy komunikacji elektronicznej, wskutek czego tymczasowo niemożliwe lub utrudnione może być świadczenie usług komunikacji elektronicznej.

Aby skutecznie zareagować na tego rodzaju zdarzenia, zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe muszą otrzymać niezbędne dane m.in. po to, aby dokonać czynności z zakresu informatyki śledczej. Niezbędne będzie przekazanie dzienników zdarzeń (logów), które mogą zawierać informacje kto, kiedy, jakiej czynności dokonał. Innym przykładem będzie przekazanie zaszyfrowanej bazy danych abonentów. Wśród tych danych

często będą znajdować się dane osobowe, jak wskazano wyżej. Może być też tak, że w skład tych danych będą znajdować się informacje umożliwiające identyfikację osób, które przyczyniły się do powstania incydentu. W tej sytuacji niezbędne jest zapewnienie możliwości przetwarzania przez ww. zespoły CSIRT danych osobowych. Zespoły CSIRT będą przetwarzać dane osobowe pozyskane dopiero przy zaistnieniu szczególnego rodzaju zdarzenia, jakim będzie incydent poważny.

Wprowadza się jeszcze dodatkowy przepis regulujący zasady usuwania danych osobowych pozyskanych przez ministra właściwego do spraw informatyzacji, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, Dyrektora Rządowego Centrum Bezpieczeństwa, Prezesa UKE w związku z wykonywaniem zadań wynikających z ustawy o KSC. Przepis wypełnia lukę prawną, która obecnie występuje w ustawie o KSC.

2.15.2. Przetwarzanie danych przez CSIRT NASK w celu tworzenia usługi online (art. 26c i zmiany w art. 39)

Wycieki danych na przestrzeni lat stają się coraz powszechniejsze co często wiąże się z poważnymi konsekwencjami takimi jak utrata prywatności, kradzież tożsamości, czy negatywnymi skutkami finansowymi. Z tego względu, dla zapewnienia bardziej efektywnej ochrony użytkowników i w celu minimalizacji ryzyka powstania szkód materialnych i niematerialnych związanych z nieuprawnionym upublicznieniem danych osobowych w sieci internet, CSIRT NASK będzie tworzył i udostępniał usługę online umożliwiającą sprawdzenie przez osobę fizyczną, czy jej dane osobowe nie zostały ujawnione w sieci Internet w sposób nieuprawniony, na skutek incydentu lub cyberzagrożenia.

Projektowane przepisy art. 26c i art. 39 ustawy o KSC określają wyraźne podstawy do gromadzenia i przetwarzania danych pozyskanych w związku z incydentami i cyberzagrożeniami. Tym samym CSIRT NASK może gromadzić i przetwarzać dane pozyskane m.in. przy obsłudze incydentów lub przy prowadzeniu czynności operacyjnych i wykorzystywać je do świadczenia usługi online, o której mowa w przepisach. Projektowany art. 26c ust. 2 ustawy o KSC wskazuje ponadto zakres danych, które mogą być przetwarzane przy realizacji tej usługi. Katalog ten wydaje się być szeroki, natomiast CSIRT NASK na podstawie przepisów odrębnych zobowiązany jest do minimalizacji przetwarzanych danych, co będzie miało miejsce także przy realizacji usługi online. Szeroki zakres wynika przede wszystkim z technicznych uwarunkowań profilu zaufanego, a dokładniej węzła krajowego, w którym przetwarzane są wszystkie te dane i przekazywane w momencie

logowania użytkownika. CSIRT NASK musi być zatem uprawniony do przetwarzania danych, które uzyska w momencie logowania się przez użytkownika.

Jednocześnie nie sposób przewidzieć zakresu danych, jakie zostaną upublicznione w sposób nieuprawniony w sieci internet. Katalog możliwych do gromadzenia i przetwarzania danych musi zatem być na tyle szeroki, aby umożliwiać prawidłowe funkcjonowanie usługi online, pozwalające na realizację założonego w ustawie celu.

Realizacja usługi online przez CSIRT NASK przy pomocy gromadzonych przez ten podmiot danych oznacza, że CSIRT NASK będzie administratorem danych zgromadzonych i przetwarzanych w tej usłudze. Usługa ta – co wynika z przepisów odrębnych – musi być zgodna z RODO oraz z minimalnymi wymaganiami dla systemów teleinformatycznych wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Wszelkie techniczne aspekty tworzenia i udostępniania usługi online, o której mowa w art. 26c ust. 1 zostaną opracowane w dokumentacji technicznej.

Zgromadzone dane będą przez CSIRT NASK anonimizowane w terminie 5 lat od dnia ich zgromadzenia co pozostaje w zgodzie z terminem na anonimizację danych pozyskanych do realizacji pozostałych zadań wynikających z ustawy. Termin ten jest adekwatny z punktu widzenia realizacji samej usługi – użytkownik musi mieć możliwość sprawdzenia historycznych wycieków, których skutki mogą być widoczne po kilku latach. Nie można wykluczyć sytuacji, że użytkownik skorzysta z funkcjonalności usługi nie od razu po wycieku, a dopiero po roku, 2 czy nawet 5 latach.

W związku z tym, że zadanie to będzie ustawowym zadaniem CSIRT NASK, finansowane będzie przez ministra właściwego do spraw informatyzacji na zasadzie dotacji podmiotowej.

2.15.3. Ocena wzajemna

CISRT MON, NASK NASK, CSIRT GOV, CSIRT sektorowe oraz organy właściwe do spraw cyberbezpieczeństwa będą mogły również uczestniczyć w ocenie wzajemnej organów z państw członkowskich Unii Europejskiej. Jest to proces, w ramach którego podmioty z poszczególnych państw członkowskich Unii Europejskiej badają nawzajem funkcjonowanie swoich zespołów CSIRT oraz procedur postępowania w przypadku wystąpienia incydentu. Metodyka przeprowadzania tych ocen zostanie ustalona przez państwa członkowskie Unii Europejskiej przy współudziale Komisji Europejskiej oraz ENISA. Udział

w ocenie wzajemnej jest dobrowolny i każdy z podmiotów mogących wziąć w nim udział będzie mógł zadecydować czy chce brać w nim udział.

Aby umożliwić realizację tych procesów niezbędne jest również stworzenie podstawy prawnej do przekazywania informacji ekspertom biorącym udział w tym procesie, tak aby mogli zapoznać się ze szczegółami spraw jakimi zajmowały się zespoły CSIRT.

Udział w tym procesie pozwoli krajowym ekspertom zapoznać się z metodami postępowania wypracowanymi w innych krajach, a następnie wykorzystać je w ramach swojej pracy. Udział w ocenie wzajemnej pozwoli również wykorzystać wiedzę ekspertów z innych krajów do usprawnienia funkcjonowania krajowych instytucji zajmujących się cyberbezpieczeństwem.

2.16. Zmiany w obszarze organów właściwych do spraw cyberbezpieczeństwa

W przepisach o właściwości organów właściwych do spraw cyberbezpieczeństwa pozostawiono właściwość dotychczasowych organów właściwych do spraw cyberbezpieczeństwa. Uzupełniono ją w przypadku nowych sektorów.

Nowe organy właściwe do spraw cyberbezpieczeństwa dla sektorów kluczowych:

1) dla sektora podsektora komunikacji elektronicznej – Prezes Urzędu Komunikacji Elektronicznej;
2) dla sektora ścieków – minister właściwy do spraw gospodarki wodnej;
3) dla sektora zarządzania usług ICT – minister właściwy do spraw informatyzacji;
4) dla sektora przestrzeni kosmicznej – minister właściwy do spraw gospodarki;
5) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw zdrowia;
6) dla sektora produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;
7) dla sektora produkcji, z wyłączeniem podsektora produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw gospodarki;
8) dla podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw zdrowia.

Organami właściwymi do spraw cyberbezpieczeństwa dla podmiotów ważnych są:

1) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;
2) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu;
3) dla sektora dostawców usług cyfrowych – minister właściwy do spraw informatyzacji;
4) dla sektora badań naukowych – minister właściwy do spraw nauki.

Przypisując właściwość organów właściwych do spraw cyberbezpieczeństwa kierowano się właściwością wynikającą z ustawy o działach administracji rządowej albo ustawami regulującymi poszczególne sektory gospodarki.

W przypadku sektora administracji publicznej organami właściwymi do spraw cyberbezpieczeństwa będą:

1) w zakresie właściwości CSIRT GOV – Szef Agencji Bezpieczeństwa Wewnętrznego;
2) w zakresie podmiotów zgłaszających incydenty do CSIRT NASK – minister właściwy do spraw informatyzacji, przy czym zadania nadzorcze z wyjątkiem wydawania decyzji administracyjnych będą mogły być powierzone CSIRT NASK;
3) w zakresie podmiotów zgłaszających incydenty do CSIRT MON – Minister Obrony Narodowej.

Podział ten jest konieczny z uwagi na bardzo dużą liczbę podmiotów publicznych.

Katalog zadań organów właściwych do spraw cyberbezpieczeństwa został uzupełniony zgodnie z innymi przepisami ustawy. Dodatkowo dodaje się także uprawnienie do odpytywania podmiotów, np. przedsiębiorców, o przekazanie informacji umożliwiających stwierdzenie, czy są one podmiotami kluczowymi czy podmiotami ważnymi. To uprawnienie jest konieczne, aby zapewnić skuteczność ustawy.

2.17. CSIRT sektorowe

Wprowadza się obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał podmioty kluczowe i podmioty ważne tego sektora w obszarze reagowania na incydenty.

Do obligatoryjnych zadań CSIRT sektorowego będzie należało przyjmowanie zgłoszeń o incydentach oraz reagowanie na incydenty. Dotychczas sektorowe zespoły cyberbezpieczeństwa miały za zadanie przyjmować zgłoszenia o incydentach poważnych i reagować na nie. Zmiana ta pozwoli CSIRT sektorowemu uzyskiwać więcej zgłoszeń o incydentach, dzięki czemu zespół będzie mógł szybciej zdobywać doświadczenie i wiedzę

w ciągle zmieniającej się sytuacji w cyberprzestrzeni. Przełoży się to na skuteczną pomoc dla podmiotów kluczowych i podmiotów ważnych zmagających się z incydentami. Podkreślić przy tym należy, że nadal podmioty kluczowe i podmioty ważne będą prawnie obowiązani zgłaszać tylko incydenty poważne do CSIRT sektorowego. Dobrowolnie będą mogli zgłosić każdy incydent, nawet ten który nie spełnia progów incydentu poważnego.

Innymi zadaniami CSIRT sektorowego będzie:

1) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;
2) współpraca z podmiotami kluczowymi i podmiotami ważnymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
3) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów; przepis podkreśla nadrzędną rolę zespołów CSIRT poziomu krajowego;
4) współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.

Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze, a także będą mogły, w uzgodnieniu z operatorem usługi kluczowej, wspierać go w wykonywaniu jego obowiązków określonych w ustawie o KSC. Będą one również uprawnione do przeprowadzania, w określonych sytuacjach, testów bezpieczeństwa. Katalog zadań CSIRT sektorowego jest katalogiem otwartym, mając na względzie, że CSIRT sektorowy powinien być dostosowany do sektora, do podmiotów, które wspiera. Zależnie od oceny organu właściwego do spraw cyberbezpieczeństwa ustawowe zadania CSIRT sektorowego mogłyby być uzupełnione o inne np. o wsparcie operatorów usług kluczowych w zakresie zarządzania ciągłością działania, czy o zadania związane z proaktywnym przeciwdziałaniem incydentom, tworzeniem oprogramowania bezpieczeństwa, czy monitoring technologii[33)]. Otwartość katalogu jest

[33)] Por. Martijn van der Heide, *Establishing a CSIRT*, str. 25. https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf

spowodowana także tym, że nie ma CSIRT, który zapewniałby wszystkie usługi zawarte w metodykach[34)], dlatego niezbędna jest tutaj zdrowa elastyczność. Projekt zakłada, że część zadań CSIRT sektorowego może być ustalona w akcie tworzącym CSIRT (np. w statucie jednostki budżetowej działającej jako CSIRT). Oczywiście te fakultatywne zadania nie mogą prowadzić do nałożenia pozaustawowych obowiązków na operatorów usług kluczowych. Organ właściwy do spraw cyberbezpieczeństwa ustanawiając te zadania powinien się kierować uznanymi metodykami tworzenia takich zespołów oraz koniecznością zapewnienia jak najlepszego wsparcia operatorom usług kluczowych.

CSIRT sektorowy będzie niezwłocznie (maksymalnie w ciągu 8 godzin) przekazywał zgłoszenie o incydencie poważnym do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV. Takie rozwiązanie gwarantuje, że zespoły CSIRT poziomu krajowego będą posiadały aktualną wiedzę o występowaniu incydentów w systemie.

Dzięki wprowadzonym zmianom podmiotom kluczowym i podmiotom ważnym zostanie zapewnione najlepsze możliwe wsparcie przy obsłudze incydentów. Ponadto nowy system zgłaszania incydentów zmniejsza obciążenia administracyjne ciążące na operatorach usług kluczowych.

Należy przy tym wskazać na doświadczenia płynące z funkcjonowania CSIRT KNF – jedynego obecnie sektorowego zespołu cyberbezpieczeństwa. W 2021 r. CSIRT KNF przekazał podmiotom rynku finansowego 22 ostrzeżenia o zagrożeniach cyberbezpieczeństwa wraz z sugerowanymi działaniami mitygującymi te zagrożenia. Zespół ten systematycznie monitoruje kampanie złośliwego oprogramowania ukierunkowane na instytucje i klientów polskiego rynku finansowego. Prowadzi działalność edukacyjną poprzez szkolenia dla podmiotów nadzorowanych, publikowanie artykułów w prasie czy w mediach społecznościowych[35)]. Niezależnie od tego zespół ten wspiera 20 operatorów usług kluczowych w sektorze bankowości i infrastrukturze rynków finansowych w obsłudze incydentów poważnych. W 2021 r. w tym sektorze doszło do 30 incydentów poważnych[36)], a od dnia 1 stycznia do dnia 8 grudnia 2022 r. do 21 incydentów poważnych[37)]. Dzięki istnieniu wyspecjalizowanego dla tego sektora zespołu CSIRT podmioty rynku finansowego mogły

---

[34)] *Ibidem.*

[35)] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku, str. 151–154. https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf.

[36)] Źródło https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska/resource/35639/table.

[37)] Źródło https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska/resource/43252/table.

liczyć na szybką i konkretną pomoc przy incydentach poważnych związanych ze świadczeniem usług bankowości elektronicznej.

Opierając się na tych doświadczeniach projektodawca jest zdania, że powołanie analogicznych zespołów w innych sektorach gospodarki pozytywnie wpłynie na zdolności operatorów usług kluczowych w zakresie cyberbezpieczeństwa.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł powierzyć realizację zadań CSIRT sektorowego jednostkom podległym lub nadzorowanym[38)] albo organowi przez niego nadzorowanemu.

Przykładowo zadania CSIRT sektorowego będą mogły być powierzone jednostce budżetowej podległej danemu organowi właściwemu do spraw cyberbezpieczeństwa. Finansowanie CSIRT sektorowego odbędzie się co do zasady z budżetu państwa – jednostka budżetowa będąca CSIRT sektorowym powinna być ustanowiona dysponentem[39)] środków budżetu państwa drugiego lub trzeciego stopnia z części budżetowej, której dysponentem jest organ właściwy do spraw cyberbezpieczeństwa. Do decyzji organu właściwego do spraw cyberbezpieczeństwa należeć będzie czy zadania CSIRT sektorowego zostaną powierzone istniejącej jednostce budżetowej czy też zostanie w tym celu utworzona nowa jednostka budżetowa zgodnie z art. 12 lub 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, z późn. zm.[40)]).

Projekt przewiduje możliwość powierzenia zadań także jednostce nadzorowanej przez organ właściwy do spraw cyberbezpieczeństwa. W szczególności CSIRT sektorowy mógłby zostać utworzony w państwowym instytucie badawczym. Zgodnie z art. 22 pkt 2 lit b ustawy z 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534), do zadań państwowego instytutu badawczego należy wykonywanie m.in. zadań szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonanie jest niezbędne dla zapewnienia obronności i bezpieczeństwa publicznego, które dotyczą monitoringu i zapobiegania skutkom zjawisk i wydarzeń mogących stwarzać zagrożenie publiczne. Niewątpliwie zapobieganie i reagowanie na incydenty poważne stanowi materię bezpieczeństwa publicznego. Z tego

[38)] Należy przy tym podkreślić, że chodzi tutaj o jednostki organizacyjne, o których mowa w art. 33 ust. 1d ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. 2022 r. poz. 1188 oraz z 2024 r. poz. 1195, 1234 i 1641).

[39)] Zgodnie z rozporządzeniem Ministra Finansów z dnia 15 stycznia 2014 r. w sprawie szczegółowego sposobu wykonywania budżetu państwa (Dz. U. z 2021 r. poz. 259 oraz z 2022 r. poz. 2846).

[40)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1273, 1407, 1429, 1641, 1693 i 1872 oraz z 2024 r. poz. 858 i 1089.

powodu zasadne jest powierzenie zadań CSIRT sektorowego państwowemu instytutowi badawczemu.
Jednostka której powierzono zadania CSIRT sektorowego będzie mogła otrzymać na ten cel dotację celową. Chodzi oczywiście o jednostki, które nie są jednostkami budżetowymi.

Przewiduje się także możliwość powierzenia zadania CSIRT sektorowego państwowej osobie prawnej – chodzi o możliwość wykorzystania już istniejących zasobów w podmiotach, które są kontrolowane przez Skarb Państwa.

Wprowadza się także możliwość porozumienia się organów właściwych ds. cyberbezpieczeństwa i wyznaczenia wspólnego CSIRT sektorowego dla kilku sektorów. Organ właściwy będzie mógł także, alternatywnie, porozumieć się z organami prowadzącymi CSIRT MON, CSIRT NASK, CSIRT GOV i powierzyć im realizację zadań CSIRT sektorowego. Przewidziano także sytuację, gdy minister jest organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów, ponieważ kieruje kilkoma działami administracji rządowej. Będzie mógł wtedy wydać decyzję o wyznaczeniu jednego CSIRT sektorowego dla wszystkich nadzorowanych podmiotów – a następcy prawni ministra będą mogli zawrzeć porozumienie, w którym zdecydują jaka jednostka dalej będzie pełniła funkcje CSIRT sektorowego dla nadzorowanych przez nich sektorów. Tego rodzaju przepisy zapewnią elastyczność i efektywne wykorzystanie zasobów przy powoływaniu zespołów CSIRT sektorowych. Komunikaty o tych porozumieniach będą publikowane w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa oraz w Biuletynie Informacji Publicznej Pełnomocnika.

Jednostka organizacyjna, której organ właściwy do spraw Cyberbezpieczeństwa powierzył rolę CSIRT sektorowego stanie się oczywiście administratorem danych osobowych przetwarzanych w ramach obsługi incydentów.

Organy właściwe do spraw cyberbezpieczeństwa będą raz w roku, do dnia 31 stycznia, przedkładać Pełnomocnikowi Rządu do Spaw Cyberbezpieczeństwa sprawozdania z funkcjonowania CSIRT sektorowych, które zapewni niezbędne informacje do prowadzenia oceny funkcjonowania krajowego systemu cyberbezpieczeństwa zgodnie z art. 62 ust. 1 pkt 1 ustawy o KSC.

2.18. Kompetencje ministra właściwego do spraw informatyzacji

2.18.1. Kompetencje ministra

Zmiany w zakresie kompetencji ministra właściwego do spraw informatyzacji wynikają ze zmian w zakresie struktury krajowego systemu cyberbezpieczeństwa i nowych definicji oraz dostosowują je do tych zmian. Wskazano, że minister ten będzie prowadził wykaz podmiotów kluczowych i podmiotów ważnych. Nowym zadaniem ministra właściwego do spraw informatyzacji, wynikającym z dyrektywy NIS 2, będzie przygotowanie i monitorowanie wykonania Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę i monitorowania jego wykonania. Minister właściwy do spraw informatyzacji będzie pełnił rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym. Pozwoli to zbliżyć reżim krajowego systemu cyberbezpieczeństwa oraz zarządzania kryzysowego zapewniając przepływ niezbędnych informacji i synergię działań.

2.18.2. System S46

System S46 zostanie dostosowany do tego, aby stać się głównym środkiem komunikacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa. W związku z koniecznością dodania do tego systemu bardzo dużej liczby podmiotów zrezygnowano z zawierania porozumienia o dołączeniu do systemu. Ponadto dołączenie do systemu nie będzie już wymagało zakupu specjalnych urządzeń, ale będzie odbywało się za pomocą rozwiązań chmurowych. Podmioty kluczowe i podmioty ważne obowiązane są zapewnić zgodność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi podłączenia do systemu, o którym mowa w ust. 1, w terminie 3 miesięcy od ich udostępnienia. Podmioty te będą więc miały odpowiedni czas na dostosowanie swoich systemów.

W systemie tym będzie prowadzony również wykaz podmiotów kluczowych i podmiotów ważnych. Oprócz tego system będzie wspierał wykonywanie zadań nadzorczych organów właściwych do spraw cyberbezpieczeństwa – np. będzie mógł ułatwić analizę sprawozdań audytowych poprzez zastosowanie sztucznej inteligencji.

Obowiązki z zakresu cyberbezpieczeństwa oraz ochrona danych osobowych często wzajemnie się przenikają. W obydwu przypadkach należy wdrożyć proporcjonalne środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych. Bardzo często incydent w rozumieniu ustawy o KSC stanowi jednocześnie naruszenie ochrony danych osobowych.

Przepisy prawa przewidują także obowiązek notyfikacji tych zdarzeń. W przypadku incydentów cyberbezpieczeństwa podmioty krajowego systemu cyberbezpieczeństwa zgłaszają incydenty do jednego z zespołów CSIRT poziomu krajowego, a w przypadku naruszeń – do Prezesa Urzędu Ochrony Danych Osobowych.

Mnogość obowiązków informacyjnych może utrudnić ich realizację. Tymczasem art. 67 pkt 2 oraz 3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, nakazuje przy projektowaniu aktów normatywnych dążenie do ograniczenia obowiązków informacyjnych oraz umożliwienie ich realizacji w postaci elektronicznej.

Z tego powodu wprowadza się możliwość zgłaszania naruszeń ochrony danych osobowych za pomocą systemu S46. Takie rozwiązanie z pewnością ułatwi zgłaszanie zdarzeń, będących zarówno incydentami jak i naruszeniami ochrony danych osobowych.

2.18.3. Pojedynczy punkt kontaktowy

Przepisy ustawy o KSC w zakresie pojedynczego punktu kontaktowego zostały dostosowane do nowej struktury pojęciowej oraz do zmian jakie zostały wprowadzone w tym wśród instytucji unijnych. Zapewni to sprawną i efektywną wymianę informacji w obszarze cyberbezpieczeństwa. Pojedynczy punkt kontaktowy będzie przekazywał Agencji Unii Europejskiej do Spraw Cyberbezpieczeństwa dane o podmiotach z sektorów infrastruktury cyfrowej, zarządzania ICT i dostawców usług cyfrowych, a także Komisji Europejskiej oraz Grupie Współpracy informacje o podmiotach znajdujących się w wykazie podmiotów kluczowych i podmiotów ważnych.

2.19. Zadania Ministra Obrony Narodowej

Katalog zadań Ministra Obrony Narodowej został dostosowany do nowej struktury krajowego systemu cyberbezpieczeństwa. Nowe zadania w zakresie cyberbezpieczeństwa będą obejmować:

1) kierowanie, za pośrednictwem CSIRT MON, działaniami związanymi z obsługą incydentów, a także koordynowanie działań CSIRT NASK i CSIRT GOV w czasie stanu wojennego oraz w czasie wojny;
2) ocenę cyberzagrożeń w każdym ze stanów gotowości obronnej państwa oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;
3) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów

administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego i w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia;

4) koordynację działania organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie dotyczącej obrony Państwa oraz Sił Zbrojnych Rzeczpospolitej Polskiej.

Zadania te podkreślają kluczową role Ministra Obrony Narodowej w przypadku wprowadzenia stanu wojennego oraz przy przygotowywaniu rozwiązań związanych z obroną państwa. Ponadto przepisy powierzają Ministrowi Obrony Narodowej zadania związane z zarządzaniem kryzysowym w cyberbezpieczeństwie w zakresie w jakim dotyczy to obrony państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej. Takie rozwiązanie gwarantuje, że w zakresie Sił Zbrojnych i obrony państwa Minister Obrony Narodowej będzie miał kluczową rolę.

Ponadto, w drodze decyzji niepodlegającej ogłoszeniu, zostaną wydzielone z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi. To rozwiązanie ma zapewnić, że w przypadku wprowadzenia stanu wojennego lub podobnej sytuacji, Minister Obrony Narodowej wciąż będzie dysponował personelem i zasobami niezbędnymi do realizacji ustawowych zadań.

2.20. Nadzór i środki egzekwowania przepisów

2.20.1. Organy nadzoru, środki nadzoru i egzekwowania przepisów

Zmiany art. 53 ustawy o KSC wynikają przede wszystkim z obowiązku implementacji postanowień art. 31 i 32 dyrektywy NIS 2.

Nadzór sprawować będą organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków. Wskazać należy, że może dojść do sytuacji zbiegu nadzoru kiedy podmiot kluczowy lub podmiot ważny będzie tym podmiotem w kilku sektorach, dla których różny jest organ nadzorczy. W takiej sytuacji nadzór nad tym podmiotem sprawuje kilka organów właściwych do spraw cyberbezpieczeństwa jednak wyłącznie we właściwym dla tego organu sektorze. Tym samym organ nadzorczy właściwy dla danego sektora uprawniony jest do stosowania środków nadzorczych tylko w zakresie obejmującym sektor, który został mu przypisany. W pozostałym zakresie (dotyczącym innego sektora) nie wykonuje środków

nadzorczych, gdyż robi to inny organ właściwy. W sytuacji zbiegu nadzoru oraz niemożliwości rozdzielenia właściwości rozwiązaniem będzie stworzenie przez organy właściwe do spraw cyberbezpieczeństwa wspólnych metodyk nadzoru, w których zostaną określone te kwestie. Ponadto możliwe będzie wspólne prowadzenie nadzoru, w tym kontroli, a także wyznaczenie organu wiodącego w tym zakresie. Organy właściwe do spraw cyberbezpieczeństwa obowiązane będą do informowania się wzajemnie o zamiarze wszczęcia kontroli, co pozwoli na sprawne i efektywne zarządzanie nadzorem bez ryzyka podwójnej kontroli i zbiegu kompetencji.

Określone zostały również środki nadzoru, a więc uprawnienia organu nadzoru w stosunku do podmiotów kluczowych i podmiotów ważnych. Do takich środków nadzoru należą m.in. kontrole prowadzone na miejscu lub zdalnie, występowanie z wnioskami o udzielenie informacji, dostępu do danych, dokumentów i informacji. Organ właściwy do spraw cyberbezpieczeństwa będzie mógł zobowiązać podmiot w drodze decyzji do przeprowadzenia audytu bezpieczeństwa. Takie zobowiązanie znajdzie zastosowanie gdy wystąpi poważny incydent lub sytuacja naruszenia przepisów ustawy. Realizacja uprawnień nadzorczych będzie mogła przyjąć postać zlecenia CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu dokonania oceny bezpieczeństwa w podmiocie.

W sytuacji uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy niniejszej ustawy, organ właściwy do spraw cyberbezpieczeństwa będzie kierował pismo z ostrzeżeniem, w którym wskaże te działania lub zaniechania oraz czynności, jakie należy podjąć w celu zapobiegnięcia lub zaprzestania przepisów ustawy. Przez uzasadnione podejrzenie należy rozumieć wszelkie wiarygodne informacje, które organ uzyskał. W szczególności dowody, wskazówki, informacje podane przez inne organy właściwe i pozostałe podmioty krajowego systemu cyberbezpieczeństwa, obywateli, media lub z innych źródeł. Mogą być to informacje dostępne publicznie lub mogą one wynikać z innych działań prowadzonych przez właściwe organy podczas wykonywania ich zadań, w tym w ramach czynności operacyjnych.

Organ właściwy do spraw cyberbezpieczeństwa zyska uprawnienie do nakazania podmiotom podjęcia określonych czynności dotyczących obsługi incydentu, a także nakazania w drodze decyzji administracyjnej zaprzestania naruszania przepisów ustawy, zapewnienia zgodności środków zarządzania ryzykiem w cyberbezpieczeństwie czy wdrożenia w określonym terminie zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego. Może także wyznaczyć na określony czas (nie dłuższy jednak niż miesiąc), spośród osób zatrudnionych

w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3 ustawy o KSC. Organ właściwy do spraw cyberbezpieczeństwa będzie musiał wskazać ściśle określone zadania, które urzędnik powinien realizować w tym czasie. W przypadku nakazu dotyczącego podjęcia określonych czynności dotyczących obsługi incydentu zdecydowano się wyłączyć decyzję administracyjną. Incydent wymaga podejmowania zdecydowanych i szybkich działań, aby zapobiec lub zminimalizować negatywne skutki. Nakaz podjęcia określonych czynności powinien być zatem wydany w jak najkrótszym czasie i mieć jak najprostszą formę, która zapewni maksymalną efektywność w sytuacji wystąpienia incydent.

Postępowanie prowadzone w powyższym zakresie jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługiwać będzie skarga do sądu administracyjnego. Również w przypadku nakazu, o którym mowa w projektowanym art. 53 ust. 5 pkt 1 ustawy o KSC, który jest inną czynnością z zakresu administracji publicznej, podmiotowi przysługuje skarga do sądu administracyjnego. Wskazać nadto należy, że oznacza to, że w przypadku wniesienia skargi do sądu administracyjnego, właściwe zastosowanie znajdą przepisy dotyczące postępowania sądowoadministracyjnego. Tym samym podmiotom będzie przysługiwało uprawnienie, o którym mowa w art. 61 ust 2 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2024 r. poz. 935), tzn. możliwe będzie wstrzymanie wykonania decyzji lub czynności z zakresu administracji publicznej do czasu rozpatrzenia sprawy przez sąd.

Projekt ustawy przewiduje ponadto dalej idące uprawnienia organu nadzoru w sytuacji, w której dany podmiot nie zastosował się w określonym terminie, do postanowień decyzji administracyjnej. Przed realizacją tych uprawnień oraz przed wydaniem decyzji administracyjnej organ zobowiązany jest poinformować podmiot o wstępnych ustaleniach wraz ze szczegółowym uzasadnieniem, a podmiot ten uprawniony jest do przedstawienia stanowiska w sprawie niezwłocznie, nie później niż w terminie 7 dni od poinformowania o wstępnych ustaleniach. Określono także zamknięty katalog wyjątków od obowiązku informowania o wstępnych ustaleniach. Środków, o których mowa w projektowanym art. 53 ust. 9 ustawy o KSC, nie stosuje się do czasu rozstrzygnięcia sprawy przez sąd, jeśli podmiot kluczowy wniósł skargę do sądu administracyjnego. Środków tych nie stosuje się także do podmiotów publicznych.

W projektowanym art. 53e ustawy o KSC wskazano procedurę związaną z realizacją środków nadzorczych określonych w projektowanym art. 53 ust. 9 ustawy o KSC. Przepis ten reguluje

sposób postępowania organu właściwego do spraw cyberbezpieczeństwa, organu lub sądu, do którego organ właściwy do spraw cyberbezpieczeństwa zwrócił się z wnioskiem oraz uprawnienia podmiotu kluczowego i organu właściwego do spraw cyberbezpieczeństwa zmierzające do przywrócenia stanu sprzed zastosowania środków, o których mowa we wspomnianym przepisie. W zakresie nieuregulowanym zastosowanie mają przepisy odrębne, właściwe dla danego rodzaju koncesji, zezwolenia, czy rodzaju działalności gospodarczej.

Organ nie wybiera środka egzekwowania przepisów czy środka nadzoru na zasadzie dobrowolności. Z tego względu proponuje się, aby organ właściwy do spraw cyberbezpieczeństwa, dokonując wyboru określonego środka, brał pod uwagę m.in. wagę naruszenia i znaczenie naruszonych przepisów, czas trwania naruszenia, istotne wcześniejsze naruszenia, spowodowane szkody majątkowe i niemajątkowe, umyślny lub nieumyślny charakter czynu, środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć, stopień współpracy podmiotu z organami właściwymi do spraw cyberbezpieczeństwa.

Wskazać również należy, że podmioty kluczowe objęte są kompleksowym systemem nadzoru ex ante (prewencyjnym) i ex post (następczym), a podmioty ważne uproszczonym systemem nadzoru – ex post – co wynika przede wszystkim z odmiennej roli jaką pełnią w systemie cyberbezpieczeństwa. Oznacza to zatem, że podmioty kluczowe podlegają nadzorowi prewencyjnemu i następczemu aby zapewnić, że podmioty kluczowe i świadczone przez nich usługi spełniają wymogi określone w niniejszej ustawie. W przypadku podmiotów ważnych nadzór został zawężony do nadzoru następczego, w oparciu o podejście reaktywne. Może być on uruchamiany w przypadku podejrzenia, że zachodzi możliwość naruszenia przepisów niniejszej ustawy. Jak wskazano wyżej, takie podejrzenie może być wynikiem uzyskania przez organ właściwy do spraw cyberbezpieczeństwa dowodów, wskazówek, informacji podanych przez inne organy właściwe, pozostałe podmioty krajowego systemu cyberbezpieczeństwa, obywateli, media lub inne źródła. Mogą być to informacje dostępne publicznie lub mogą one wynikać z innych działań prowadzonych przez właściwe organy podczas wykonywania ich zadań, w tym w ramach czynności operacyjnych. Podkreślić należy, że przepisy nadzorcze i egzekwowania przepisów odnoszące się do podmiotów kluczowych mają zastosowanie również do podmiotów ważnych, ale z tym zastrzeżeniem, że stosuje się do nich tylko te środki, które mogą być zastosowane ex post. Oznacza to, że organ właściwy do spraw cyberbezpieczeństwa wykonując swoje uprawnienia wobec podmiotów ważnych będzie

musiał podjąć adekwatne środki uwzględniając, że mogą mieć one wyłącznie charakter następczy.

W dodawanym w ustawie o KSC art. 53d określono ponadto uprawnienia jakie przysługują urzędnikowi monitorującemu w ramach nadzoru realizacji przez podmiot kluczowy obowiązków określonych w rozdziale 3 ustawy o KSC. Zaproponowany zakres uprawnień pozwoli na skuteczne wykonywanie przez niego zadań, a informacje pozyskane w toku monitorowania będą mogły stanowić podstawę do podjęcia przez organ właściwy do spraw cyberbezpieczeństwa innych, koniecznych środków nadzoru, w tym wszcząć kontrolę doraźną. Do nadzorowania przez urzędnika monitorującego wykonywania przez podmiot kluczowy obowiązków stosuje się odpowiednio art. 58 ustawy o KSC. Jednocześnie wskazać należy, że realizując swoje obowiązki urzędnik monitorujący obowiązany jest do poszanowania tajemnicy prawnie chronionej na podstawie odrębnych przepisów. Przykładowo dostęp do informacji niejawnych będzie zależny od tego czy wyznaczony urzędnik posiada dostęp do informacji klauzulowanych. Jeśli nie posiada takiego dostępu, to nie będzie on mógł zapoznawać się z takimi dokumentami. Organ właściwy do spraw cyberbezpieczeństwa powinien zatem wyznaczać urzędnika monitorującego według zarówno swojego zaplecza kadrowego jak i potrzeb nadzorczych.

Urzędnik monitorujący w zakresie przetwarzania przez niego danych osobowych będzie związany przepisami RODO jako osoba realizująca zadania w imieniu i na rzecz administratora.

Za uniemożliwianie bądź utrudnianie urzędnikowi monitorującemu realizacji jego zadań bądź uprawnień, przewidzianych w projektowanym art. 53d ust. 1 ustawy o KSC, podmiot kluczowy będzie podlegał karze pieniężnej. Przez uniemożliwianie lub utrudnianie należy rozumieć w szczególności niewydanie urzędnikowi monitorującemu przepustki.

Ze względu na zróżnicowanie w zakresie prowadzenia nadzoru nad podmiotami kluczowymi i podmiotami ważnymi, przepisy dotyczące nadzoru nad podmiotami kluczowymi stosuje się odpowiednio do nadzoru nad podmiotami ważnymi.

Zmiany wprowadzane w art. 53 ustawy o KSC i w dodawanym w tej ustawie art. 53d w jasny sposób określają zarówno organy nadzoru, ich uprawnienia nadzorcze i zmierzające do egzekwowania przepisów w stosunku do podmiotów kluczowych i podmiotów ważnych, co przekładać się będzie na wysoki poziom bezpieczeństwa usług.

2.20.2. Metodyki nadzoru i hierarchia priorytetów zadań nadzorczych

Przepisy określające możliwość tworzenia metodyk nadzoru oraz ustanawiania hierarchii priorytetów w odniesieniu do zadań nadzorczych mają na celu zapewnienie skutecznego nadzoru w zakresie stosowania przepisów ustawy przez podmioty kluczowe i podmioty ważne.

Celem utworzenia metodyk nadzoru jest dostosowanie metod nadzoru do określonego sektora oraz podmiotu nadzorowanego co pozwoli na usystematyzowanie i ujednolicenie sposobu przeprowadzania nadzoru, lepsze wykorzystanie dostępnych zasobów i zwiększenie efektywności działań nadzorczych. Metodyki nadzoru powinny w szczególności określać zakres nadzoru, a więc m.in. rodzaje czynności nadzorczych, sposób przeprowadzania nadzoru obejmujący np. etapy nadzoru, stosowane narzędzia i techniki oraz kryteria oceny, które pozwolą na wyprowadzenie odpowiednich wniosków w zakresie tego, czy dany podmiot prawidłowo realizuje nałożone na niego obowiązki. Należy mieć na uwadze, że każdy organ właściwy do spraw cyberbezpieczeństwa będzie określał adekwatne dla swojego sektora zakres nadzoru, sposób jego przeprowadzenia i kryteria oceny. Z tego względu nie zdecydowano się na precyzyjne wskazanie w przepisie co należy rozumieć jako zakres, sposób oraz kryteria. Metodyka nadzoru powinna być dobrana w taki sposób, aby zapewnić skuteczność oraz zgodność z przepisami prawa, a także właściwą i pełną realizację zarówno obowiązków nałożonych na podmioty nadzorowane jak i zadań organów sprawujących nadzór. Dodatkowo organy nadzoru mogą określać inne elementy w metodykach nadzoru jeśli uznają to za stosowne. Metodyki nadzoru będą także rozwiązaniem problemu wielosektorowości danego podmiotu to znaczy sytuacji, w której dany podmiot kluczowy lub podmiot ważny jest nadzorowany przez różne organy właściwe do spraw cyberbezpieczeństwa. W sytuacji braku możliwości rozdzielenia działań nadzorczych z uwagi na niemożliwość wyodrębnienia sektorów, sporządzenie przez organy właściwe do spraw cyberbezpieczeństwa wspólnych metodyk nadzoru pozwoli na porozumienie organów właściwych do spraw cyberbezpieczeństwa, np. co do zakresu sprawowanego przez nich nadzoru i pozwoli uniknąć sporów kompetencyjnych. Metodyki nadzoru można uznać w tym przypadku za porozumienia pomiędzy organami właściwymi do spraw cyberbezpieczeństwa.

Ponadto ustanowienie hierarchii priorytetów w odniesieniu do zadań nadzorczych, które oparte będzie na analizie ryzyka przeprowadzanej przez organ właściwy do spraw cyberbezpieczeństwa, pozwoli na dobór efektywnej formy nadzoru dostosowanej do sytuacji nadzorowanego podmiotu. W celu zapewnienia maksymalnej efektywności w sytuacji,

w której organy zdecydują się wprowadzić metodykę nadzoru zobowiązane będą do jej przeglądu i oceny co 2 lata.

W celu przeprowadzenia analizy ryzyka organ właściwy do spraw cyberbezpieczeństwa będzie mógł skorzystać z kompetencji określonej w projektowanym art. 53c ust. 1 ustawy o KSC.

2.20.3. Obowiązek przekazywania danych, informacji i dokumentów

W celu zagwarantowania prawidłowego realizowania kompetencji nadzorczych, a tym samym podjęcia adekwatnych i efektywnych działań, wprowadza się w ustawie o KSC art. 53c, który nakłada na podmioty kluczowe i podmioty ważne obowiązek dostarczenia organom właściwym do spraw cyberbezpieczeństwa na ich żądanie wszelkich danych, informacji i dokumentów niezbędnych do wykonywania przez te organy ich uprawnień i obowiązków określonych w ustawie.

Określono również elementy jakie żądanie organu właściwego do spraw cyberbezpieczeństwa powinno zawierać. Istotnym obwarowaniem jest również określenie, iż żądanie powinno być proporcjonalne do celu jakiemu ma służyć. Oznacza to, że nie jest możliwe żądanie udostępnienia takich informacji, dokumentów czy danych, które nie są konieczne, adekwatne i proporcjonalne do wykonywania przez organ jego obowiązków i uprawnień.

2.20.4. Czynności kontrolne

W toku przeglądu przepisów ustawy o KSC oraz na podstawie doświadczeń z przeprowadzonych na podstawie tych przepisów czynności kontrolnych, zidentyfikowano problemy znacznie utrudniające prawidłowe realizowanie tych czynności. Z tego względu zdecydowano się na wprowadzenie zmian w art. 54 i art. 58 ustawy o KSC.

Zmiany w art. 54 ustawy o KSC mają charakter dostosowujący i są konsekwencją zmian poczynionych w pozostałych przepisach. Mając jednak na uwadze fakt, że w przypadku kontroli na podstawie art. 54 ustawy o KSC, nie będą miały zastosowania art. 54 i art. 55 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, konieczne stało się określenie maksymalnego czasu trwania kontroli w podmiocie. Zdecydowano się na przyjęcie maksymalnie 48 dniowego czasu trwania, który to termin wynika z doświadczeń organów właściwych do spraw cyberbezpieczeństwa prowadzących czynności kontrolne na podstawie obecnie obowiązujących przepisów. Niekiedy określone w ustawie z dnia 6 marca 2018 r.– Prawo przedsiębiorców terminy nie były adekwatne do zakresu kontroli sprawowanej przez organy właściwe i uniemożliwiały prawidłowe i skuteczne realizowanie uprawnień.

W nowym brzmieniu art. 58 ustawy o KSC wskazano wyraźnie, że kontrolowany w przypadku zastrzeżeń co do ustaleń zawartych w protokole kontroli ma prawo odmówić jego podpisania, a także złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu protokołu kontroli do podpisu. Nie tylko podkreślono zatem uprawnienie kontrolowanego do odmowy podpisania protokołu ale i postanowiono, że pisemne zastrzeżenia powinny być umotywowane.

Obowiązek analizy zastrzeżeń przekazano na kierownika komórki do spraw kontroli jednocześnie zdejmując ten obowiązek z osoby prowadzącej czynności kontrolne. Kierownik komórki do spraw kontroli po analizie odrzuca zastrzeżenia i informuje o tym fakcie podmiot kontrolowany albo uwzględnia zastrzeżenia w całości lub w części lub je oddala. Kierownik komórki obowiązany jest również do sporządzenia stanowiska wobec złożonych zastrzeżeń. W tym miejscu należy wskazać, że kierownik komórki do spraw kontroli nie oznacza, że organ właściwy do spraw cyberbezpieczeństwa obowiązany jest posiadać specjalnie wyodrębnioną komórkę do spraw kontroli. Przez komórkę do spraw kontroli należy rozumieć komórkę organizacyjną, która w ramach swoich zadań zajmuje się kontrolą. Kontrola może być zatem jednym z wielu zadań realizowanych w tej komórce.

Osoba prowadząca czynności kontrole w razie potrzeby podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki do spraw kontroli zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu.

Zmiana procedury w przypadku zastrzeżeń do protokołu w zaproponowanym brzmieniu pozwoli na zapewnienie większej efektywności i obiektywności.

Zgodnie z NIS 2 wprowadzono także regulację dotyczącą współpracy nadzorczej organów właściwych do spraw cyberbezpieczeństwa z organami innych państw członkowskich Unii Europejskiej. Współpraca ta dotyczy nadzoru nad podmiotami, które świadczą usługi na terytorium Rzeczypospolitej Polskiej, ale ich siedziba znajduje się w innym państwie – albo sytuacji odwrotnej.

Dodano także przepisy o informowaniu Prezesa Urzędu Ochrony Danych Osobowych o podejrzeniu nadużycia ochrony danych osobowych.

Wprowadza się także instytucję kontroli doraźnej (projektowany art. 59c ustawy o KSC), która jest jednym ze środków nadzorczych. Kontrola doraźna może zostać wszczęta w przypadkach uzasadnionych charakterem sprawy lub pilnością przeprowadzenia czynności kontrolnych. Wskazano przykładowe sytuacje, w których wszczęcie jest możliwe – będzie to m.in. kontrola

wszczynana w razie potrzeby sprawdzenia informacji uzyskanej od urzędnika monitorującego, że podmiot kluczowy może naruszać przepisy ustawy. Kontrola ta jest z reguły szybsza i prostsza, w związku z tym wyłącza się w stosunku do niej niektóre czynności, które mają miejsce przy kontroli przeprowadzanej na zasadach ogólnych. Istotne jest jednak to, że w stosunku do kontroli doraźnej nie zachodzi wyłączenie co do terminów jej przeprowadzania. Tym samym kontrola doraźna nie może być dłuższa niż wynika to bezpośrednio z przepisów odrębnych, właściwych dla podmiotu kontrolowanego.

2.21. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Nowe przepisy przewidują, że Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa może być minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Takie rozwiązanie zapewni stabilność w zakresie obsługi tego Pełnomocnika oraz jego odpowiednią rangę. Należy podkreślić, że minister właściwy do spraw informatyzacji nadzoruje Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, w której zlokalizowany jest CSIRT NASK. Dzięki temu Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa ma łatwy dostęp do dodatkowej wiedzy eksperckiej i kompetencji z zakresu cyberbezpieczeństwa.

Dotychczasowa praktyka pokazała, że takie rozwiązanie jest korzystne gdyż zapewnia pełnomocnikowi dodatkowe informacje i zasoby niezbędne do realizacji jego zadań. Przepisy te zapewnią również stabilizację funduszy Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, wskazując z której części budżetowej jest finansowany.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie również mógł zlecać przeprowadzanie badań i ekspertyz oraz tworzyć zespoły robocze. Te kompetencje zapewnią mu dodatkowe narzędzia do realizacji jego zadań. Wprowadzono również regulację, że inne organy państwa mają obowiązek udzielania wsparcia Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa, tak aby w sytuacji gdy dane zagadnienie dotyczy ich właściwości otrzymał on niezbędne wsparcie.

Przy Pełnomocniku Rządu do Spraw Cyberbezpieczeństwa zostanie utworzone Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”, będące organem pomocniczym w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa. W jego skład będą wchodzili przedstawiciele najważniejszych instytucji rządowych zapewniających cyberbezpieczeństwo w kraju. Do zadań PCOC należeć będzie:

1) wymiana informacji na temat cyberzagrożeń, incydentów i podatności na poziomie krajowym;
2) wymiana informacji o wynikach szacowania ryzyka związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami;
3) wymiana informacji o przeprowadzanych badaniach, o których mowa w art. 33 ust. 1 ustawy o KSC;
4) jednomyślne wyznaczanie roli CSIRT w przypadku incydentów, których obsługa wymaga działań kilku zespołów CSIRT, z wyjątkiem przypadków incydentów krytycznych;
5) wymiana informacji dotyczących sytuacji kryzysowych w cyberprzestrzeni;
6) przygotowywanie bieżących informacji na temat sytuacji w cyberprzestrzeni dla Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

Dotychczasowa inicjatywa spotkań koordynujących cyberbezpieczeństwo w Polsce będzie unormowana na poziomie ustawowym. Formuła ta sprawdza się przy intensywnej sytuacji w cyberprzestrzeni.

Dodatkowo Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa umożliwia się wydanie zarządzenia określającego sposób działania PCOC. Zdaniem projektodawcy wydanie aktu prawa wewnętrznego w tym zakresie jest możliwe, mając na względzie, że PCOC będzie działał przy Pełnomocniku Rządu do Spraw Cyberbezpieczeństwa i na jego rzecz, a Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa przewodniczy PCOC. Podobna sytuacja ma miejsce przy Rządowym Zespole Zarządzania Kryzysowego – tryb działania jest określany w zarządzeniu Prezesa Rady Ministrów, który przewodniczy temu zespołowi.

2.22. Kolegium do Spraw Cyberbezpieczeństwa

Zmiana ustawy poszerza skład Kolegium do Spraw Cyberbezpieczeństwa, zakres jego zadań i precyzuje pewne kwestie związane z jego funkcjonowaniem.

W projektowanej ustawie zostały określone nowe rodzaje analiz jakie będą mogły być zlecane CSIRT MON, CSIRT NASK lub CSIRT GOV. Będą to analizy dotyczące wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1 ustawy o KSC oraz analizy dotyczące trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT. Analizy te będą wykonywane na wniosek Przewodniczącego

Kolegium do Spraw Cyberbezpieczeństwa i będą mogły posłużyć jako dowód w ramach postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka.

Rozszerzono katalog zadań Kolegium do Spraw Cyberbezpieczeństwa m.in. o wyrażanie opinii o decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie także wyrażało opinię w sprawie wyznaczenia Operatora strategicznej sieci bezpieczeństwa.

Proponuje się rozszerzenie składu Kolegium do Spraw Cyberbezpieczeństwa – nowym członkiem będzie minister właściwy do spraw energii, z uwagi na to, że sektor energii jest jednym z największych sektorów.

W posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa będą mogli także uczestniczyć:

1) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca;
2) Przewodniczący Komisji Nadzoru Finansowego;
3) Prokurator Generalny albo jego zastępca;
4) Szef Agencji Wywiadu albo jego zastępca;
5) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca;
6) Szef Służby Wywiadu Wojskowego albo jego zastępca.

Ponadto umożliwiono, aby pozostali szefowie służb (wymienieni w znowelizowanym art. 66 ust. 4 ustawy o KSC) mogli także desygnować na posiedzenia Kolegium swoich zastępców.

W ślad za odpowiednimi zmianami w innych przepisach, uzupełniono katalog kompetencji przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa o możliwość:

1) wnioskowania o przeprowadzenie badania produktu ICT, usługi ICT lub procesu ICT;
2) zlecenia zespołom CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty kluczowe i podmioty ważne oraz największych przedsiębiorców telekomunikacyjnych;
3) zlecenia CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu i oprogramowani sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2 ustawy o KSC;
4) wnioskowania o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka.

Ustawa o KSC nie przewiduje sytuacji nieobecności sekretarza Kolegium do Spraw Cyberbezpieczeństwa na przykład spowodowanej czasowymi problemami zdrowotnymi. Aby zapewnić ciągłość obsługi Kolegium do Spraw Cyberbezpieczeństwa proponuje się wprowadzenie instytucji zastępcy sekretarza Kolegium. Sekretarz Kolegium do Spraw Cyberbezpieczeństwa jest powoływany przez Przewodniczącego Kolegium – czyli Prezesa Rady Ministrów. Aby nie nakładać nadmiernych obowiązków na Prezesa Rady Ministrów zastosowano zasadę pomocniczości – zastępcę sekretarza Kolegium do Spraw Cyberbezpieczeństwa będzie powoływał jak również odwoływał sekretarz Kolegium. Będzie to też oznaczało, że sekretarz Kolegium do Spraw Cyberbezpieczeństwa odpowiada przed Przewodniczącym Kolegium za wybór danej osoby na zastępcę. Kryteria wyboru zastępcy Sekretarza będą takie same, jak dla Sekretarza – zastępca będzie musiał spełniać wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne".

W przepisie wskazano jasno, że zastępca sekretarza Kolegium wykonuje obowiązki sekretarza w razie nieobecności tego ostatniego, w szczególności zastępuje go na posiedzeniu Kolegium do Spraw Cyberbezpieczeństwa.

2.23. Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

2.23.1. Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

Nowe przepisy umożliwią wydawanie przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększenia bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Ten dokument będzie publikowany na stronie podmiotowej Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w Biuletynie Informacji Publicznej. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, a także inne zbiory dobrych praktyk. Podkreślić należy, że rekomendacje będą formalnie niewiążące, jednak podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić je w ramach procesu zarządzania ryzykiem. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Dzięki rekomendacjom uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne do oszacowanego ryzyka zabezpieczenia.

2.23.2. Dostawca Wysokiego Ryzyka

Zawarty w rozdziale I Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. poz. 483, z 2001 r. poz. 319, z 2006 r. poz. 1471 oraz z 2009 r. poz. 946) art. 20 stanowi o ustroju gospodarczym Rzeczypospolitej Polskiej. Opiera się on między innymi na wolności prowadzenia działalności gospodarczej, która polega na możliwości: podejmowania działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji Rzeczypospolitej Polskiej dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków Trybunał zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym[41)]. Państwo może więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości[42)]. Z kolei w innym orzeczeniu Trybunał zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłaby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego, a także prawno-międzynarodowym zobowiązaniom państwa[43)]. W tym kontekście należy wskazać, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady Ministrów jest zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji Rzeczypospolitej Polskiej).

Opierając się na powyższych przesłankach, projektodawca proponuje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka, będą musiały być wycofane z tych

41) Wyrok Trybunału Konstytucyjnego z dnia 8 kwietnia 1998 r., sygn. K 10/97.

42) Ibidem.

43) Wyrok Trybunału Konstytucyjnego z dnia 10 października 2001 r., sygn. K 28/01.

podmiotów. Rozwiązanie to ma na celu zapewnienie ochrony ważnego interesu państwowego w postaci bezpieczeństwa państwa.

Obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W szczególności dotyczy to kluczowych przedsiębiorców telekomunikacyjnych, którzy będą świadczyć usługi w oparciu o mobilne sieci 5G[44)]. Sieć 5G będzie oferowała możliwość przetwarzania znacznie większej liczby danych oraz wyższe prędkości przekazywania danych w porównaniu do dotychczasowej sieci 3G oraz 4G. Dzięki sieci 5G możliwe będzie podłączenie znacznie większej liczby urządzeń Internetu Rzeczy niż do tej pory. Umożliwi to znacznie większe możliwości przekazywania danych pomiędzy obywatelami oraz wpłynie pozytywnie na rozwój gospodarki.

Wdrożenie sieci 5G wiąże się z ryzykami, szczególnie tymi związanymi z bezpieczeństwem. Dzięki tym sieciom będzie możliwe świadczenie wielu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i realizacji podstawowych funkcji społecznych i gospodarczych – takich jak energetyka, transport, bankowość i opieka zdrowotna oraz systemy sterowania produkcją. Potencjalny cyberatak mógłby doprowadzić do naruszenia dostępności danej usługi na niespotykaną dotąd skalę. Możliwy byłby atak na sieć 5G, który doprowadziłby do przejęcia kontroli nad infrastrukturą krytyczną jak np. sieci energetyczne. Przejęcie kontroli nad siecią 5G mogłoby doprowadzić do naruszenia poufności ogromnej liczby przesyłanych danych. Skutki takich incydentów byłyby bardzo poważne.

Kwestia bezpieczeństwa sieci 5G została podjęta na poziomie unijnym. W motywie 3 i 4 zaleceń Komisji (UE) 2019/534 wskazano, że:

„(3) Z powodu uzależnienia wielu usług o krytycznym znaczeniu od sieci 5G konsekwencje systemowych i rozległych zakłóceń byłyby szczególnie poważne. W rezultacie

[44)] Jako sieci 5G Komisja Europejska zdefiniowała: *zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności ruchomej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń. Mogą one obejmować elementy dotychczasowych sieci wykorzystujących technologię łączności ruchomej i bezprzewodowej poprzednich generacji, takich jak 4G lub 3G. Sieci 5G należy rozumieć jako obejmujące wszystkie istotne części sieci*. Pkt II.2.a Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz. Urz. UE L 88 z 29.3.2019, s. 42.).

zapewnienie cyberbezpieczeństwa sieci 5G jest kwestią o strategicznym znaczeniu dla Unii w czasie, gdy cyberataki przybierają na sile i są coraz bardziej wyrafinowane.

(4) Ponadnarodowy charakter infrastruktury stanowiącej podstawę ekosystemu cyfrowego, która charakteryzuje się siecią wzajemnych powiązań, jak również transgraniczny charakter zagrożeń oznaczają, że wszelkie istotne luki bezpieczeństwa lub cyberincydenty dotyczące sieci 5G występujące w jednym państwie członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G.".

Komisja zaleciła, aby państwa członkowskie przeprowadziły krajową ocenę ryzyka bezpieczeństwa sieci 5G, zgodnie z rekomendacjami Komisji. Ponadto Komisja zaleciła, aby w oparciu o krajową ocenę ryzyka państwa członkowskie powinny:

1) zaktualizować wymogi w zakresie bezpieczeństwa oraz metody zarządzania ryzykiem stosowane w odniesieniu do sieci 5G;

2) zaktualizować odpowiednie obowiązki nakładane na przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej zgodnie z art. 13a i art. 13b dyrektywy 2002/21/WE;

3) obwarować ogólne zezwolenia warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem oraz uzyskać od przedsiębiorstw uczestniczących w przyszłych postępowaniach o udzielenie praw użytkowania częstotliwości radiowych w pasmach 5G zobowiązanie do przestrzegania wymogów w zakresie bezpieczeństwa sieci na podstawie dyrektywy 2002/20/WE;

4) stosować inne środki zapobiegawcze mające na celu ograniczenie potencjalnych zagrożeń dla cyberbezpieczeństwa.

Środki te powinny obejmować obowiązki nakładane na dostawców oraz operatorów celem zapewnienia bezpieczeństwa sieci 5G.

W wyniku powyższych zaleceń powstała unijna skoordynowana ocena ryzyka cyberbezpieczeństwa sieci 5G[45)] oraz Unijny zestaw środków dla cyberbezpieczeństwa sieci

[45)] Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049, zwana dalej Unijną oceną cyberbezpieczeństwa sieci 5G".

5G – tzw. Toolbox 5G[46)]. W dokumentach tych wskazano na ryzyka związane z sieciami 5G w tym także tymi związanymi z dostawcami sprzętu i oprogramowania dla tej sieci.

Jedno ze wskazanych ryzyk dotyczy dostawców, którzy znajdują się pod wpływem państw prowadzących agresywne działania w cyberprzestrzeni. Takie państwo może wpływać na dostawcę, aby wykorzystał ukryte podatności w sprzęcie lub oprogramowaniu dostarczonemu innemu państwu, aby uzyskać dostęp do wrażliwych danych przesyłanych przez ten sprzęt czy też wpływać na dostępność usług świadczonych poprzez ten sprzęt. Dostawca taki będzie działał na rzecz interesów państwa, pod którego wpływem znajduje się. Prawdopodobieństwo zaistnienia tej sytuacji zależy od stopnia, w jakim dostawca ma dostęp do sieci, w szczególności jej krytycznych funkcji[47)].

Natomiast ryzyka dotyczą również aspektów technicznych, np. tego czy dostawca jest w stanie zapewnić bezpieczeństwo swoich produktów, jak reaguje na incydenty związane z tymi produktami, jak zarządza podatnościami własnych produktów. Niska jakość sprzętu i oprogramowania dostarczanego przez dostawcę, w tym ukryte podatności, może umożliwić cyberatak na sieć dokonywany przez agresywne państwa w cyberprzestrzeni, grupy *Advanced Persistent Threat* czy grupy przestępcze[48)].

Z wyżej wskazanych dokumentów wynika więc, że mogą istnieć dostawcy sprzętu lub oprogramowania, którzy poprzez dostarczany sprzęt lub oprogramowanie mogą zagrażać państwom członkowskim UE, w tym także Polsce. Przyjęło się określać takich dostawców jako „dostawców wysokiego ryzyka" (high risk vendors).

Toolbox 5G wskazuje środki strategiczne, które będą w stanie zmitygować ryzyka wskazane w Unijnej ocenie cyberbezpieczeństwa sieci 5G. Przede wszystkim Toolbox 5G zaleca środki strategiczne:

1) SM01 – wzmocnienie roli władz krajowych – środek ten polega m.in. na wyposażeniu władz krajowych w kompetencje do zakazu, ograniczenia lub wprowadzenia wymagań odnośnie produktów dla sieci 5G, biorąc pod uwagę m.in. bezpieczeństwo krytycznych (critical and sensitive) części sieci 5G, ryzyka związane z wpływem państw trzecich na łańcuchy dostaw 5G czy ryzyka dla bezpieczeństwa narodowego;

[46)] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[47)] Unijna ocena cyberbezpieczeństwa sieci 5G str. 22, przypis 14 i 15, str. 27; Toolbox str. 43 i 44.
[48)] Unijna ocena cyberbezpieczeństwa sieci 5G pkt 2.51, Toolbox 5G str. 43.

2) SM03 – ocena ryzyka dostawców – przeprowadzenie rygorystycznej oceny ryzyka dostawców, a następnie wprowadzenie niezbędnych wyłączeń w krytycznych zasobach.

W swoim komunikacie z 29 stycznia 2020 Komisja Europejska potwierdziła, że „państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w zestawie narzędzi”[49)].

Biorąc pod uwagę powyższe stanowisko unijne zasadne jest wprowadzenie procedury umożliwiającej zbadanie ryzyk związanych z danym dostawcą sprzętu lub oprogramowania. W przypadku, gdyby ryzyka dla bezpieczeństwa państwa okazały się zbyt wysokie, taki dostawca powinien być uznany za stwarzający wysokie ryzyko.

W przepisach nowelizacji została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postępowanie to będzie prowadzone w celu ochrony ważnych interesów państwowych w postaci bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Tak jak wyżej wspomniano kwestia cyberbezpieczeństwa sieci 5G jest kwestią strategiczną dla Unii Europejskiej z uwagi na współzależności pomiędzy sieciami telekomunikacyjnymi państw członkowskich Unii Europejskiej. Ze względu na potencjalne szkody, które może przynieść zakłócenie funkcjonowania tych sieci jest to również materia dotycząca bezpieczeństwa państwa. Jednakże przepis nie zamyka się wyłącznie do sieci 5G. Postępowaniu będzie mógł być poddany dostawca produktów, usług i procesów ICT nie tylko dla sieci 5G, ale również dla innych systemów informacyjnych – jeżeli będzie spełniona przesłanka zapewnienia ochrony bezpieczeństwa państwa.

Dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT[50)]. Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor.

[49)] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ

[50)] Dla przypomnienia: produktem ICT jest element lub grupę elementów systemu informacyjnego, usługą ICT jest usługa polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych, procesem ICT jest zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT.
Zauważyć przy tym należy, że definicja systemu informacyjnego obejmuje także sieć telekomunikacyjną - por.

Dzięki temu postępowaniem będą mogły być objęte wszystkie podmioty kluczowe w łańcuchu dostaw. Postępowanie nie będzie dotyczyło wszystkich produktów ICT, usług ICT i procesów ICT pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez podmioty kluczowe i podmioty ważne z wyłączeniem podsektora komunikacji elektronicznej lub przedsiębiorców komunikacji elektronicznej, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych.

Podmioty te są szczególnie ważne dla zapewnienia bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu lub oprogramowania w trakcie świadczenia usług na rzecz państwa i obywateli.

Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą miały zastosowanie przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572), zwanej dalej „Kpa". Dzięki temu dostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach strony, z odmiennościami wynikających ze szczególnych regulacji wynikających z przepisów nowelizacji. W postępowaniu nie będą stosowane następujące przepisy Kpa:

1) art. 28 – projekt wprowadza wyjątek, że w tym szczególnym postępowaniu stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka;
2) art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;
3) art. 51 – wyłącza się przepis, który zawęża osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;
4) art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;
5) art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu;

Wyłączenie tych przepisów Kpa jest niezbędne ze względu na szczególny charakter tego postępowania, które ma na celu zapewnienie bezpieczeństwa narodowego.

W celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na

Sejm RP VIII kadencji, druk nr 2505, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, uzasadnienie str. 18-19. https://sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2505.

względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania.

Wyłączenie art. 28 Kpa jest konieczne, ponieważ postępowanie jest wszczynane z urzędu przez ministra albo na wniosek przewodniczącego Kolegium – co za tym idzie stroną jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Podobne rozwiązanie znajduje się w art. 88 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2024 r. poz. 594).

Z kolei wyłączenie art. 31 Kpa wynika ze szczególnego związku tego postępowania z kwestiami bezpieczeństwa narodowego.

Ze względu na ogólnopolski zasięg decyzji jaka ma zostać wydana w tym postępowaniu został wyłączony art. 51 Kpa.

Kwestia metryki sprawy przy tego typu postępowaniu jest złożona. Obowiązkowo w ramach postepowania o uznaniu dostawcy za dostawcę wysokiego ryzyka będą przeprowadzane szerokie analizy podmiotu, którego dotyczy postępowanie oraz jego produktów. Ujawnienie nazwisk osób, które przeprowadzały te analizy mogłoby narazić ich na działania ze strony podmiotów zainteresowanych konkretnym wynikiem sprawy. Ponadto wiele z tych osób to funkcjonariusze, których tożsamość, ze względu na wykonywane zadania, musi być chroniona. Z powyższych względów wyłączony został art. 66a Kpa.

W związku z wrażliwym charakterem informacji, jakie będą wykorzystywane w ramach tego postępowania, konieczne jest wyłączenie udziału strony z przeprowadzanych dowodów.

Jednocześnie umożliwiono przystąpienie do postępowania na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej. Będą to tacy przedsiębiorcy komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2023 r. poz. 1251, 1429 i 1672 oraz z 2024 r. poz. 834, 858 i 1243). Aby przystąpić do postępowania taki przedsiębiorca będzie obowiązany złożyć stosowny wniosek. Zmiana odpowiada na postulaty strony społecznej, jednocześnie zapewniając sprawny przebieg postępowania.

Umożliwia się wypowiedzenie się w toku postępowania izbom gospodarczym. Będą one mogły przedstawić stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Minister właściwy do spraw informatyzacji, przed wydaniem decyzji, udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej raport ze złożonych stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach. Rozwiązanie to zapewnia z jednej strony możliwość wypowiedzenia się reprezentantów przedsiębiorców w sprawie tego postępowania, a z drugiej strony nie spowoduje to przewlekłości postępowania.

Minister właściwy do spraw informatyzacji stanowisko zajmuje w drodze decyzji administracyjnej, co umożliwi dostawcy ewentualne złożenie skargi do wojewódzkiego sądu administracyjnego.

W przypadku, gdy dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) zawiadomienie o wszczęciu postępowania publikowane jest na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Publikacja ma skutek doręczenia po upływie 14 dni od dnia jej dokonania. Przepis ten stanowi szczególną regulację w stosunku do zasad doręczeń określonych w Kpa.

Zawiadomienie o wszczęciu postępowania wobec dostawcy, który ma siedzibę na terytorium Unii Europejskiej, Konfederacji Szwajcarskiej czy państwa członkowskiego EFTA będzie doręczane na zasadach ogólnych wynikających z Kpa. Natomiast po otrzymaniu potwierdzenia doręczenia informacja o tym będzie publikowana na stronie Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, aby uprawnieni przedsiębiorcy telekomunikacyjni mogli złożyć wniosek o dopuszczenie do postępowania na prawach strony.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego do spraw informatyzacji lub na wniosek Przewodniczącego Kolegium Spraw Cyberbezpieczeństwa. Minister właściwy do spraw informatyzacji jest odpowiedzialny za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym, stąd też zasadne jest, aby to on prowadził tego rodzaju postępowanie. Przed wydaniem decyzji minister właściwy do spraw informatyzacji będzie obowiązany zwrócić się

do Kolegium do Spraw Cyberbezpieczeństwa o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium do Spraw Cyberbezpieczeństwa będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra. Termin od dnia wystąpienia o opinię do dnia otrzymania opinii nie będzie wliczał się do terminu załatwienia sprawy.

Wskazano elementy analizy, która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G[51)].

Celem opinii Kolegium do Spraw Cyberbezpieczeństwa jest kompleksowa analiza działalności dostawcy sprzętu lub oprogramowania. Mając na uwadze, że w skład Kolegium do Spraw Cyberbezpieczeństwa wchodzą ministrowie kluczowi dla bezpieczeństwa państwa a także szefowie służb specjalnych, będą w stanie pozyskać niezbędne informacje do oceny dostawcy od swoich jednostek podległych lub nadzorowanych.

Zasadne jest, aby opinia obejmowała kwestie zagrożeń, które stwarza dostawca. Nie są to jednak zwykłe zagrożenia, lecz takie, które wpływają na bezpieczeństwo narodowe. Przepis dalej precyzuje, że chodzi o zagrożenia w wymiarze ekonomicznym, wywiadowczym oraz terrorystycznym[52)]. Ponadto konieczna będzie analiza zagrożeń, które stwarza dostawca dla zobowiązań sojuszniczych (np. w ramach NATO czy innych umów międzynarodowych) a także europejskich. Niewątpliwie zobowiązaniem europejskim jest zapewnienie na poziomie unijnym wysokiego poziomu bezpieczeństwa systemów informacyjnych (co wynika z dyrektywy NIS 2).

Kolejnym aspektem opinii powinna być analiza prawdopodobieństwa, z jakim dostawca znajduje się pod wpływem państwa. Ta część opinii skupia się na powiązaniach dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej oraz NATO. Wpływ ten może obejmować prawodawstwo danego państwa, które reguluje stosunki między państwem a dostawcą (np. w zakresie swobody działalności gospodarczej czy bezpieczeństwa przetwarzanych danych). Co istotne Kolegium do Spraw Cyberbezpieczeństwa powinno pochylić się także nad praktyką stosowania tych przepisów, aby sprawdzić, jak one

[51)] Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

[52)] Np. cyberterroryzm w postaci ataków na infrastrukturę krytyczną państwa.

funkcjonują, np. czy gwarancje zawarte w tych przepisach rzeczywiście są respektowane przez dane państwo.

Z uwagi na to, że współcześnie coraz więcej danych osobowych jest przesyłanych poza Unię Europejską ważna jest także kwestia ochrony danych osobowych w danym państwie i kwestia faktycznego stosowania tych przepisów.

Opinia będzie także zawierała analizę struktury własnościowej dostawcy sprzętu lub oprogramowania – w celu ustalenia kto faktycznie sprawuje kontrolę własnościową nad dostawcą. Finalnie powinny być sprawdzone możliwości wpływu danego państwa na dostawcę.

Opinia będzie dotyczyła otoczenia regulacyjnego dostawcy, faktycznego stosowania prawa, struktury własnościowej oraz faktycznego wpływu państwa na dostawcę. Po dokonaniu analiz uzyskany zostanie całościowy obraz relacji między dostawcą a państwem.

Rozporządzeniem wykonawczym Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonującym rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 2020/1125 z 30.07.2020) Unia Europejska wskazała podmioty, które dokonują cyberataków na Unię lub jej państwa członkowskie. Wskazane jest, aby opinia Kolegium do Spraw Cyberbezpieczeństwa dotyczyła również tego, jakie są relacje pomiędzy tymi podmiotami a dostawcą sprzętu lub oprogramowania.

Jak już wyżej wskazano ryzyka dotyczą również aspektów technicznych produktów ICT, usług ICT i procesów ICT dostarczanych przez dostawcę. Dlatego do technicznych aspektów opinii należy analiza:

1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

2) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w art. 67b ust. 1 ustawy o KSC, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

3) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4 ustawy o KSC, dotyczących sprzętu lub oprogramowania danego dostawcy.

Jest to związane z potencjalnymi ryzykami, które wiążą się z niską jakością sprzętu lub oprogramowania. Jak wyżej wspomniano podatności mogą być wykorzystane do cyberataków przez państwa, grupy APT czy grupy przestępcze – dlatego warto zbadać jakość produktów dostarczanych przez dostawcę.

Realizując postulaty strony społecznej dodano wymóg, aby prowadząc opinię Kolegium do Spraw Cyberbezpieczeństwa uwzględniło także certyfikaty produktów, usług i procesów ICT dostarczanych przez dostawcę oraz wyniki analiz łańcuchów dostaw, które przeprowadziły zespoły CSIRT poziomu krajowego.

Określono procedurę sporządzania opinii Kolegium do Spraw Cyberbezpieczeństwa. Opinia zostanie przygotowana przez zespół opiniujący w skład, którego wchodzą przedstawiciele członków Kolegium do Spraw Cyberbezpieczeństwa. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. Przewodniczący Kolegium do Spraw Cyberbezpieczeństwa będzie miał kompetencję do rozstrzygnięcia ewentualnego negatywnego sporu co do zakresu tej właściwości poprzez wskazanie właściwego członka zespołu opiniującego. Wprowadzono obowiązek przeprowadzenia analiz łańcuchów dostaw, zanim zostanie sporządzona opinia Kolegium do Spraw Cyberbezpieczeństwa w sprawie dostawcy.

Po przeprowadzeniu postępowania minister właściwy do spraw informatyzacji wyda decyzję uznającą dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. Nie chodzi więc o zwykłe zagrożenie, tylko o jego kwalifikowaną postać. Decyzja będzie zawierać wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka – ponieważ one też stwarzają zagrożenie.

Dzięki prawnemu zidentyfikowaniu dostawcy wysokiego ryzyka będzie możliwe wprowadzenie dodatkowych środków mitygujących zagrożenie, jakie stwarza sprzęt lub oprogramowanie dostarczane przez dostawcę wysokiego ryzyka. Ze względu na charakter sprawy – stwierdzenie poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi – decyzja ta będzie podlegała

natychmiastowej wykonalności. Wskazać należy, że zastosowane w przepisie przesłanki w żaden sposób nie odnoszą się do pochodzenia dostawcy. Za dostawcę wysokiego ryzyka może być uznany zarówno podmiot zagraniczny jak również podmiot działający na terytorium Rzeczypospolitej Polskiej. Wszyscy przedsiębiorcy są obowiązani do działania w sposób niezagrażający bezpieczeństwu państwa polskiego.

Jeżeli w trakcie postępowania zostanie stwierdzone, że dostawca nie stanowi poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, to zgodnie z zasadami ogólnymi Kpa zostanie wydana decyzja o umorzeniu postępowania.

Aby podmioty obowiązane do wycofania sprzętu mogły zastosować się do obowiązków wynikających z wydania tej decyzji administracyjnej, minister właściwy do spraw informatyzacji opublikuje ją w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski", na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Od decyzji w sprawie uznania za dostawcę wysokiego ryzyka nie będzie przysługiwał wniosek o ponowne rozpatrzenie sprawy. Prawa strony postępowania będą zagwarantowane poprzez możliwość złożenia skargi do sądu administracyjnego.

Następstwem prawnego zidentyfikowania dostawcy wysokiego ryzyka powinno być zmitygowanie ryzyka, które on stwarza. Wprowadza się więc niezbędne wymogi bezpieczeństwa dla podmiotów kluczowych i podmiotów ważnych w związku z wykorzystywaniem sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka.

Podmioty kluczowe i podmioty ważne nie będą mogły wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów ICT, usług ICT lub procesów ICT, jak i używanych. Celem jest, aby nie wprowadzać kolejnych produktów ICT, usług ICT lub procesów ICT, żeby nie zwiększać już i tak wysokiego ryzyka związanego z nimi.

Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji. Chodzi tutaj o sytuację, w której w chwili wydania decyzji o uznaniu za

dostawcę wysokiego ryzyka dany podmiot już używa lub korzysta z produktów ICT, usług ICT lub procesów ICT uwzględnionych w decyzji o uznaniu za dostawcę wysokiego ryzyka. Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów ICT, usług ICT lub procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.

Natomiast najwięksi przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT wskazanych w decyzji i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy, będą musieli wycofać je w ciągu 4 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3 do ustawy.

Jednocześnie wprowadzono przepis umożliwiający użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją w sprawie uznania za dostawcę wysokiego ryzyka, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji. Będzie to możliwe wyłącznie, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. Te same przepisy zostały zastosowane do podmiotów publicznych, które już zakupiły określony sprzęt w drodze zamówienia publicznego. Jest to niezbędne rozwiązanie zarówno dla zapewnienia ciągłości świadczenia usług jak również ochrony dyscypliny finansów publicznych.

Wyżej zaproponowana interwencja prawodawcy jest konieczna ze względu na istotność dla bezpieczeństwa państwa usług świadczonych przez podmioty obowiązane do wycofania sprzętu lub oprogramowania. Podmioty te mogą być związane wieloletnimi umowami z dostawcą wysokiego ryzyka na dostarczanie sprzętu lub oprogramowania czy świadczenie usług serwisowych. Bez prawnego obowiązku stopniowego wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka podmioty te nie wycofają sprzętu lub oprogramowanie m. in. z uwagi na ryzyko odpowiedzialności kontraktowej wobec dostawcy. W konsekwencji ryzyko związane ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka nie zostanie skutecznie zmitygowane.

Podkreślić należy, że jest to wyjątek od podstawowej reguły zakazu wprowadzania do użytkowania i obowiązku wycofania ww. sprzętu lub oprogramowania w ciągu 5–7 lat. Wyjątek ten nie może być interpretowany rozszerzająco.

Wyjaśnienia wymaga termin użytkowania użyty w tym przepisie. Nie należy go utożsamiać z użytkowaniem z Kodeksu cywilnego, które jest ograniczonym prawem rzeczowym. Użytkowanie w rozumieniu projektowanego art. 66b ustawy o KSC oznacza każdy przypadek używania czy korzystania z produktu ICT, usługi ICT lub procesu ICT do świadczenia usług przez dany podmiot.

Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Raport BEREC wskazuje, że w przypadku sprzętu 5G wykorzystywanego w radiowej sieci dostępowej (RAN) cykl życia urządzenia wynosi w większości przypadków od 5 do 10 lat[53)].

Proponowane rozwiązania mają wpływ na swobodę działalności gospodarczej podmiotów zobowiązanych do wycofania sprzętu – wpływają bowiem na wolność podejmowania decyzji gospodarczych. Mają także wpływ na wykonywanie niektórych atrybutów prawa własności, tj. prawa do używania produktów. Wskazać należy, że przepisy te mają na celu mitygację ryzyk związanych ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka. Tak jak wyżej wspomniano korzystanie z takiego sprzętu mogłoby doprowadzić do poważnych ryzyk naruszenia poufności danych oraz naruszenia dostępności usługi. Co za tym idzie doprowadziłoby to do poważnego utrudnienia funkcjonowania obywateli - współczesnego społeczeństwa informacyjnego, a także do ryzyka przejęcia kontroli nad infrastrukturą krytyczną państwa. Wycofanie sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka jest zatem konieczne do zapewnienia funkcjonowania demokratycznego państwa prawnego.

Proponowane rozwiązania nie naruszają istoty swobody prowadzenia działalności gospodarczej. Ogranicza się wykorzystywanie przez przedsiębiorców konkretnego sprzętu lub

[53)] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-secure-5g-networks str. 24.

oprogramowania do świadczenia usług – w pozostałym zakresie przedsiębiorcy będą mogli swobodnie podejmować decyzje biznesowe. Przepisy te nie naruszają również istoty prawa własności. Tak jak wyżej wskazano nie ma mechanizmu natychmiastowego wycofania sprzętu lub oprogramowania – przez czas wycofywania z użytkowania podmioty te będą mogły w pełni wykonywać prawo własności. Ponadto w czasie wycofywania będzie można wprowadzić dotychczas posiadany sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka, aby dokonać niezbędnych napraw usterek czy awarii, aby zapewnić ciągłość świadczenia usługi – pokazuje to, że istota prawa własności nie została naruszona. Należy również zaznaczyć, że sprzęt lub oprogramowanie, które pochodzą od dostawcy wysokiego ryzyka i tak podlegałby stopniowej wymianie ze względu na zużycie czy postęp technologiczny. Zatem proponowane rozwiązanie wpisuje się w mechanizm stopniowej wymiany sprzętu.

Proponowane rozwiązanie wpłynie na swobodę prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka. Należy jednak podkreślić, że będzie to związane z poważnym zagrożeniem dla państwa, które stwarza ten dostawca. Jednakże istota prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka nie zostanie naruszona. Taki dostawca nadal będzie mógł prowadzić działalność gospodarczą.

Podkreślić należy, że wartością konstytucyjną, która w tej sytuacji powinna być bardziej chroniona od swobody prowadzenia działalności gospodarczej czy prawa własności jest bezpieczeństwo państwa. Państwo powinno odpowiednio zaadresować problem dostawcy wysokiego ryzyka, który może, dzięki podatnościom w sprzęcie lub oprogramowaniu, które dostarczył, doprowadzić do ataku na infrastrukturę krytyczną państwa (np. inteligentne sieci energetyczne, sieci telekomunikacyjne), zakłócać funkcjonowanie organów państwa (np. poprzez ataki man in the middle, kradzież danych), czy zakłócić działanie kluczowych dla społeczeństwa usług (np. poprzez atak na systemy i urządzenia szpitalne, bez których znacznie utrudnione jest wykonywanie operacji ratujących życie). Może to się odbyć poprzez celowo zaprojektowane ukryte podatności lub również ukryte podatności powstałe w wyniku aktualizacji oprogramowania dostarczonego przez dostawcę wysokiego ryzyka. Wykorzystanie podatności w infrastrukturze telekomunikacyjnej, której elementy dostarczył taki dostawca, mogłoby utrudnić lub uniemożliwić funkcjonowanie usług komunikacji elektronicznej na danym obszarze.

Demokratyczne państwo prawne nie może być bezbronne i musi zawczasu identyfikować poważne zagrożenia dla jego funkcjonowania oraz skutecznie je mitygować. Ryzyka

stwarzanego przez dostawcę wysokiego ryzyka (który działa pod wpływem obcych służb wywiadowczych lub grup przestępczych) oraz jego sprzęt lub oprogramowanie nie da się inaczej zmitygować, jak tylko poprzez stopniowe wycofanie takiego sprzętu. Podmioty korzystające z tych produktów ICT, usług ICT lub procesów ICT nie będą w stanie zidentyfikować ukrytych podatności, poprzez które dostawca wysokiego ryzyka będzie mógł dokonywać ataków. W związku z tym nie jest możliwe zmitygowanie ryzyka stwarzanego przez dostawcę wysokiego ryzyka poprzez wprowadzenie dodatkowych środków bezpieczeństwa, innych niż wycofanie sprzętu lub oprogramowania, ponieważ będą one nieskuteczne wobec ukrytych podatności pozwalających np. nagle wyłączyć sprzęt czy zakłócić telekomunikację między podmiotami.

Warto podkreślić, że postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będzie postępowaniem administracyjnym, a zatem dostawca będzie mógł przedstawić swoje racje w postępowaniu zanim zostanie uznany za dostawcę wysokiego ryzyka. Decyzja będzie mogła być zaskarżona do sądu administracyjnego, co zapewnia dostawcy możliwość obrony swoich praw. Dostawca będzie mógł być uznany za dostawcę wysokiego ryzyka, jeżeli będzie spełniał szczególnego rodzaju przesłanki, tj. będzie stwarzał poważne zagrożenie dla obronności, bezpieczeństwa państwa.

Podsumowując, zanim dostawca zostanie uznany za dostawcę wysokiego ryzyka jego sprawa zostanie wszechstronnie wyjaśniona – nastąpi to poprzez opinię Kolegium do Spraw Cyberbezpieczeństwa oraz czynności przeprowadzone przez ministra właściwego do spraw informatyzacji. Dostawca będzie mógł przedstawić swoje stanowisko, a w przypadku uznania za dostawcę wysokiego ryzyka – kwestionować to przed sądem administracyjnym.

Organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Przepis wzmocni kompetencje organów i zapewni im możliwość monitorowania procesu wycofywania produktów ICT, usług ICT i procesów ICT.

Wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze lex specialis do ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. 2023 r. poz. 1634, 1705 i 1860), zwanej dalej „PPSA". Jest on wzorowany na art. 38 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, która dotyczy rozpoznania skargi na decyzję o odmowie wydania

poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpoznawał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego[54)]. Przepis stanowi niezbędne odstąpienie od zasady ustności i jawności, jednakże strona będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym.

Rozwiązanie to jest konieczne dla zapewnienia bezpieczeństwa demokratycznego państwa prawnego – ujawnienie informacji niejawnych wykorzystanych w postępowaniu o uznaniu za dostawcę wysokiego ryzyka mogłoby narazić Rzeczpospolitą Polską na niepowetowane szkody. Nie została naruszona istota prawa do sądu, ponieważ w zakresie w jakim uzasadnienie nie zawiera informacji niejawnych (uzasadnienie prawne, kwestia wykładni, ustalenia organu niepodlegające utajnieniu) zostanie doręczone skarżącemu, dzięki czemu będzie mógł złożyć skargę kasacyjną. Rozwiązanie jest też proporcjonalne sensu stricto, bowiem sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Na poparcie tego rozwiązania warto tutaj odwołać się do wyroku Naczelnego Sądu Administracyjnego z 8 marca 2017 r. sygn. akt I OSK 1312/15: „strona skarżąca – z istoty sprawy mająca ograniczony dostęp do szeregu informacji z nią związanych – powinna móc działać w zaufaniu, że zasadniczo pełny dostęp do informacji posiada sąd, do którego zwraca się ona o kontrolę działania organu administracji publicznej, i że tę kontrolę sąd ten dokona w sposób niezależny i niezawisły w oparciu o pełną wiedzę wynikającą z ustaleń organu, w tym także niejawnych”.

Minister właściwy do spraw informatyzacji będzie prowadził w Biuletynie Informacji Publicznej wykaz decyzji o uznaniu za dostawcę wysokiego ryzyka w podziale na produkty,

[54)] Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14.

usługi i procesy w nich wskazane. Ułatwi to dostęp do informacji o niebezpiecznych produktach ICT, usługach ICT i procesach ICT.

2.23.2.1. Polecenie zabezpieczające

Przepisy nowelizacji ustawy o KSC wprowadzają regulację dotyczącą polecenia zabezpieczającego, które będzie mogło być wydane przez ministra właściwego do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego, w celu skoordynowania efektywnej reakcji na ten incydent. Incydent krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie – po przeprowadzeniu należytej oceny – może być uznany przez CSIRT poziomu krajowego za incydent krytyczny.

Obecnie państwo nie dysponuje środkami prawnymi, które umożliwiałyby skuteczną reakcję na incydent krytyczny. Oczywiście za obsługę incydentu krytycznego odpowiada jeden z zespołów CSIRT poziomu krajowego, który będzie współpracował z podmiotem, u którego wystąpił incydent krytyczny. Podkreślić jednak należy, że cyberataki mogą nie dotyczyć jednego podmiotu, a skutki takich ataków mogą się rozszerzać na inne podmioty w bardzo szybkim czasie. Zespoły CSIRT mogą nie nadążyć w obsłudze takiego incydentu krytycznego, który dotyczy wielu podmiotów. Jako przykład można podać sytuację, gdy cały świat zmagał się z podatnością Log4Shell. Była to krytyczna podatność, która mogła być wykorzystywana przez grupy advanced persistent threat[55)]. Innym przykładem są ataki na wiele podmiotów administracji rządowej na Ukrainie.

Dlatego istnieje ważny interes publiczny w tym, aby państwo mogło nakazać, w niezbędnym i proporcjonalnym zakresie, przedsiębiorcom świadczącym istotne usługi dla społeczeństwa informacyjnego, zachowanie, które uchroni m.in. systemy informacyjne, sieci telekomunikacyjne wielu podmiotów przed skutkami incydentu krytycznego. Takim instrumentem będzie właśnie polecenie zabezpieczające.

[55)] https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/

Przed wydaniem polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa, Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny.

Natomiast minister właściwy do spraw informatyzacji będzie mógł wydać w drodze decyzji administracyjnej polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. W poleceniu zabezpieczającym zawarte będzie wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Katalog tych zachowań został wskazany w projektowanym art. 67g ust. 10 ustawy o KSC. Może to być m.in. nakaz zastosowania określonej poprawki bezpieczeństwa, nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zakaz korzystania z określonego sprzętu lub oprogramowania. Jednocześnie należy wskazać, że zakaz korzystania z konkretnych usług i oprogramowania będzie dotyczył wyłącznie rozwiązań mających związek z trwającym incydentem krytycznym.

Polecenie zabezpieczające będzie miało charakter decyzji generalnej, a więc będzie skierowane w konkretnej sprawie do podmiotów ustalonych rodzajowo. Przemawia za tym fakt, że niemożliwe jest zidentyfikowanie ile dokładnie podmiotów mogłoby być dotkniętymi incydentem krytycznym.

Decyzje generalne są znane w prawie administracyjnym państw UE[56)], jak również w doktrynie i praktyce w polskim prawie sprzed 1997 r. Decyzja generalna to jeden z rodzajów aktu administracyjnego, a zatem akt stosowania prawa, a nie jego stanowienia (np. rozporządzenia czy ustawy)[57)]. Ma charakter generalno-konkretny, czyli wymagają poczynienia ustaleń faktycznych i przyporządkowania (podciągnięcia) stanu faktycznego pod daną normę. Odróżnia je to od aktów normatywnych, które wiążą co do zasady wszystkich[58)].

---

56) Przykładem mogą być: Niemcy, Grecja, Hiszpania i Portugalia oraz – jako przedstawiciel EOG – Norwegia.

57) Zbigniew Kmieciak (red.), *Raport Zespołu Eksperckiego z prac w latach 2012-2016 – Reforma prawa o postępowaniu administracyjnym*, Warszawa 2017.

58) E. Szewczyk, M. Szewczyk, *Między indywidualnym aktem administracyjnym a aktem normatywnym,* Warszawa 2014.

Nie jest to nowa forma stanowienia prawa, a raczej specyficzny rodzaj aktu administracyjnego, działający obok, a nie zamiast decyzji administracyjnej. Decyzja administracja charakteryzuje się tzw. podwójną konkretnością (konkretny adresat i konkretna sprawa), natomiast akty normatywne są podwójnie ogólne (generalnie określony adresat i abstrakcyjnie opisana sprawa). Akty generalne charakteryzują się natomiast ogólnie określonym adresatem i konkretnie określoną sprawą.

Decyzje generalne, mimo braku sformalizowanych zasad procedowania, są stosowane w polskim prawie. Przykładem mogą być niektóre uchwały Komisji Nadzoru Finansowego (dawny art. 71 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2023 r. poz. 2488)), Wykaz Produktów Leczniczych Dopuszczonych do Obrotu na terytorium Rzeczypospolitej Polskiej (art. 4 ust. 1 pkt 1 lit. j ustawy z dnia 18 marca 2011 r. o Urzędzie Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych (Dz. U. z 2023 r. poz. 1223), czy też rozstrzygnięcia Głównego Inspektora Sanitarnego (art. 27 ust. 1 i 2 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz. U. 2024 r. poz. 416).

Do postępowania nie będą miały zastosowania przepisy art. 10, art. 34, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 Kpa, a inne przepisy Kpa będą stosowane odpowiednio. Wyłączenia ww. przepisów są konieczne ponieważ w przypadku decyzji generalnych niemożliwe są do zidentyfikowania wszystkie strony postępowania. Wyłączenia w projekcie nawiązują do poglądów doktryny[59)].

W przypadku polecenia zabezpieczającego wyłączone wprost zostaną następujące przepisy Kpa odnoszące się do udziału strony w postępowaniu:

1) art. 10 – w przypadku decyzji generalnej, gdzie strona jest ustalona rodzajowo nie jest możliwe zapewnienie czynnego udziału wszystkim pomiotom, na których ten akt ma wpływ – ich prawa są chronione przez możliwość zaskarżenia decyzji do sądu administracyjnego;

2) art. 34 – z uwagi na to, że strona co do zasady nie będzie brała czynnego udziału w postępowaniu należy wyłączyć obowiązek organu dot. wystąpienia do sądu z wnioskiem o wyznaczenie przedstawiciela dla osoby nieobecnej lub niezdolnej do czynności prawnych;

[59)] Rozdział 7.4 E. Szewczyk, M. Szewczyk, *Generalny akt administracyjny: między indywidualnym aktem administracyjnym a aktem normatywnym*, Wolters Kluwer 2014.

3) art. 79 – z uwagi na rodzajowe określenie strony (a także potencjalną liczbę podmiotów, np. ok. 4000 przedsiębiorców telekomunikacyjnych) nie jest możliwe zawiadamianie ich o miejscu i terminie przeprowadzenia dowodu na siedem dni przed terminem; tym bardziej nie będzie to możliwe w przypadku polecenia zabezpieczającego, gdzie istotny będzie czas reakcji na trwający incydent krytyczny;

4) art. 81 – z uwagi na rodzajowe określenie strony należy wyłączyć przepis o domniemaniu udowodnienia danego faktu, jeżeli strona miała możność wypowiedzenia się co do przeprowadzonych dowodów;

5) art. 81a – z uwagi na rodzajowe określenie strony należy wyłączyć przepis o zasadzie rozstrzygania wątpliwości faktycznych na korzyść strony;

6) art. 107 § 1 pkt 3 – wyłącza się przepis o wskazaniu strony w treści decyzji administracyjnej; w zamian w poleceniu zabezpieczającym będzie określony rodzaj podmiotów, do których skierowane będzie polecenie;

7) art. 145 § 1 pkt 4 – wyłącza się przepis o możliwości wznowienia postępowania, jeżeli strona nie brała z własnej winy udziału w postępowaniu – w przypadku decyzji generalnych, gdzie strona jest ustalona rodzajowo nie jest możliwe zapewnienie czynnego udziału wszystkim pomiotom, na których ten akt ma wpływ, stąd należy wyłączyć ten przepis, aby nie powstała podstawa do wzruszania tego aktu;

8) art. 156 § 1 pkt 4 – wyłącza się przepis o obowiązku stwierdzenia nieważności decyzji która została skierowana do osoby niebędącej stroną w sprawie - strona w przypadku decyzji generalnej jest określona rodzajowo.

Zawiadomienia w sprawie będą doręczane poprzez publiczne obwieszczenie na stronie podmiotowej ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej. Samo polecenie zabezpieczające będzie ogłoszone w dzienniku urzędowym ministra właściwego do spraw informatyzacji oraz na stronie podmiotowej ministra w Biuletynie Informacji Publicznej lub na stronie internetowej urzędu obsługującego ministra.

Wskazane w poleceniu zabezpieczającym określone zachowanie ma być adekwatne do sytuacji – minister nie będzie mógł więc arbitralnie wskazać zachowania, tylko wybrać takie, które w świetle analizy, będzie proporcjonalne do sytuacji wywołanej incydentem krytycznym.

Ze względu na fakt, że w dodawanym w ustawie o KSC art. 67g wprowadzona została decyzja generalna skierowana do bliżej nieokreślonego kręgu podmiotów, konieczne było wprowadzanie również kwestii precyzujących niektóre aspekty postępowania sądowo administracyjnego. Ze względu na specyfikę tej decyzji zdecydowano się wyraźnie wskazać, że sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia. Ma to ułatwić stosowanie tych przepisów oraz zapobiec powstaniu wątpliwości w zakresie postępowania ze skargami na decyzję stanowiącą polecenie zabezpieczające.

Rygor natychmiastowej wykonalności polecenia zabezpieczającego jest jedyną rzeczą, która zapewni skuteczne działanie tego środka prawnego i szybkie podjęcie działań ograniczających skutki incydentu krytycznego. Przykłady cyberataków m.in. związane z oprogramowaniem firmy SolarWinds, czy wykorzystujących niewykryte wcześniej podatności w programie Microsoft Exchange Server, dobitnie pokazują jak kluczowa w reagowaniu na takie ataki jest szybkość podjęcia działań mitygujących ryzyka i ograniczających skutki ataku. Jak krytyczne jest dokonywanie natychmiastowych aktualizacji oprogramowania pokazuje właśnie przykład podatności w przypadku produktu firmy Microsoft. Podatności, nie naprawione w porę natychmiast wykorzystali cyberprzestępcy, którzy mieli możliwość m.in. czytania wewnętrznej korespondencji mailowej.

Wyłączone zostały przepisy o ponownym rozpatrzeniu sprawy przez organ. Decyzja ta będzie oparta na specjalistycznej analizie opracowanej w warunkach wystąpienia incydentu krytycznego. Nie jest zasadne ponowne angażowanie osób w przeprowadzenie takiej analizy, w przypadku gdy wystąpiła znaczna szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Priorytetem w takiej sytuacji musi być podjęcie odpowiednich działań naprawczych. Prawa strony są odpowiednio chronione poprzez instytucję skargi do sądu administracyjnego.

Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata, a wygasa z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji lub po upływie czasu, na które zostało wydane.

Wprowadzenie do polskiego porządku prawnego polecenia zabezpieczającego jest konieczne dla zapewnienia bezpieczeństwa narodowego, ponieważ cyberataki są coraz

częstsze i coraz bardziej niebezpieczne. Należy podkreślić, że są one dokonywane zarówno przez zwykłych przestępców jak i sprawców powiązanych z określonymi państwami, którzy dysponują znaczną wiedzą i zasobami. Państwo zawczasu musi mieć odpowiednie prawne środki reakcji na incydenty krytyczne, aby bronić swojego społeczeństwa i gospodarki przed skutkami tych incydentów. Polecenie zabezpieczające będzie skutecznym środkiem przeciwdziałania incydentom krytycznym. Będzie miało charakter proporcjonalny do cyberzagrożenia. Wpłynie ono wyłącznie w niezbędnym zakresie na swobodę działalności gospodarczej, aby uchronić kluczowe podmioty przed skutkami incydentu krytycznego, który jak wspomniano wyżej, w bardzo poważny sposób zagraża obywatelom, gospodarce czy szerzej bezpieczeństwu narodowemu. Katalog zachowań możliwych do nałożenia w drodze polecenia zabezpieczającego zostanie ustawowo ograniczony. Ponadto minister będzie zobligowany wybrać zachowanie adekwatne do cyberzagrożenia, jakie stwarza incydent krytyczny. Dlatego projektodawca jest zdania, że nie narusza ono istoty swobody działalności gospodarczej, a także jest ono proporcjonalne sensu stricto.

Z uwagi na konstytucyjną niezależność Narodowego Banku Polskiego nie będą do niego stosowały się przepisy dotyczące wycofania produktów ICT, usług ICT lub procesów ICT pochodzących od dostawcy wysokiego ryzyka. Minister właściwy do spraw informatyzacji będzie informował Prezesa Narodowego Banku Polskiego o wydaniu decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka. Prezes Narodowego Banku Polskiego zdecyduje zatem czy wycofa produkty ICT, usługi ICT oraz procesy ICT wskazane w decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka.

Dodano opcjonalną możliwość przekazania zadań zespołów CSIRT, określonych w art. 26 ustawy o KSC, Ministrowi Obrony Narodowej. Decyzję w tej sprawie podejmie Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium do Spraw Cyberbezpieczeństwa oraz w uzgodnieniu z Ministrem Obrony Narodowej. W decyzji zostaną określone m.in. zakres, czas powierzenia zadań, a także fakultatywnie szczegóły współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV. Zadania te będą realizowane przez Ministra Obrony Narodowej za pomocą jego jednostek podległych lub przez niego nadzorowanych. Komunikat o powierzeniu realizacji zadań będzie ogłaszany w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Ponadto celem poinformowania podmiotów krajowego systemu cyberbezpieczeństwa informacja o komunikacie będzie udostępniana na stronach internetowych CSIRT MON, CSIRT NASK, CSIRT GOV lub w Biuletynie

Informacji Publicznej na stronie podmiotowej Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

2.24. Przepisy o karach pieniężnych

Zmiany poczynione w przepisach z zakresu kar pieniężnych obejmują dostosowanie katalogu kar w związku z nowymi obowiązkami jakim podlegają podmioty kluczowe lub podmioty ważne. Przewidziano także możliwość nałożenia kary na podmiot, który nie wyznaczył osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami kluczowymi i podmiotami ważnymi lub na podmiot, który nie zapewnia użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczenia się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami. Możliwość wymierzenia kary aktualizuje się wtedy, gdy przemawia za tym waga i znaczenie naruszonych przepisów. Doprecyzowano również, że karze pieniężnej podlegają podmioty kluczowe lub podmioty ważne także wtedy, gdy ich działanie lub zaniechanie ma charakter jednorazowy. Taki przepis pozwoli wyeliminować wątpliwości co do tego, czy np. niewykonywanie obowiązku musi mieć charakter ciągły lub powtarzalny, żeby wypełniało to znamiona czynu, za który nałożona może zostać kara pieniężna.

Dążąc do zapewnienia, że kary określone w ustawie będą skuteczne, proporcjonalne i odstraszające, określono minimalną wysokość kary na poziomie 20 000 zł w przypadku podmiotów kluczowych oraz 15 000 zł w przypadku podmiotów ważnych. Co do zasady jednak kara nie może przekroczyć 10 000 000 euro wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. W przypadku kar nakładanych na podmioty ważne jej wysokość nie może przekroczyć 7 000 000 euro wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez ten podmiot z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Zastosowanie ma kara wyższa. Określenie granic wymiaru kary pieniężnej w powyższy sposób pozwala na miarkowanie represji, włącznie z jej ograniczaniem do minimum w uzasadnionych przypadkach. Tak szeroki zakres kar umożliwi indywidualne i adekwatne – zarówno surowe jak i łagodne – karanie podmiotów, które dopuszczają się naruszeń.

Przewidziano także sytuację, w której okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo podmiot w ogóle nie osiągnął przychodu. W takiej sytuacji podstawą wymiaru kary w przypadku podmiotów kluczowych jest równowartość kwoty 500 000 euro, wyrażona w złotych i ustalana przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązujący w dniu wydania decyzji o wymierzeniu kary. W przypadku podmiotów ważnych jest to równowartość kwoty 250 000 euro.

Określając wymiar kary niezwykle istotną rolę odgrywają przychody osiągnięte przez podmiot z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Zdecydowano się na przyjęcie kategorii roku obrotowego z tego względu, że kara nakładana w powiązaniu z tym przychodem w większym stopniu uwzględnia sytuację majątkową podmiotu istniejącą w chwili wydania decyzji o nałożeniu kary. Zapewniono w ten sposób również zgodność z brzmieniem dyrektywy NIS 2.

W sytuacji, w której zidentyfikowane zostanie, że podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, a przy tym powoduje bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi lub zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług, organ właściwy nakłada karę w wysokości do 100 000 000 zł. Zwiększenie wymiaru kary w stosunku do obecnie obowiązujących przepisów wynika z nadrzędnego celu kar pieniężnych jaki określa implementowana dyrektywa NIS 2, a także z wagi tego naruszenia, które może mieć poważne skutki – również z punktu widzenia obecnej sytuacji międzynarodowej. Należy bowiem mieć na uwadze fakt, że przez długi czas, tj. od dnia 21 lutego 2022 r. utrzymywany był trzeci stopień alarmowy CRP (CHARLIE-CRP), co świadczy o wysokim stopniu zagrożenia bezpieczeństwa narodowego związanego z zagrożeniami w cyberprzestrzeni. Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu. Aktualnie od dnia 1 marca 2024 r. do dnia 31 maja 2024 r. na całym terytorium Rzeczypospolitej Polskiej obowiązuje drugi stopień alarmowy CRP (BRAVO-CRP), który może być wprowadzony w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym w cyberprzestrzeni, jednak konkretny cel ataku nie został zidentyfikowany. Z tego względu każde naruszenie przepisów, które spełnia powyżej wskazane przesłanki, może wiązać się z poważnymi konsekwencjami dla państwa i jego obywateli, a tym samym powinno być obarczone odpowiednio wysoką sankcją, która

będzie spełniać funkcję zarówno prewencyjną jak i represyjną. Oznacza to, że kara pieniężna ma odstraszać od kolejnych naruszeń i w związku z tym być odpowiednio dolegliwa. Jednocześnie należy wskazać, że w związku z zakazem podwójnego karania za te same naruszenia, organ właściwy do spraw cyberbezpieczeństwa może nałożyć wyłącznie jedną karę pieniężną. Oznacza to, że jeśli naruszenie wypełni znamiona określone w art. 73 ust. 5 ustawy o KSC, to organ właściwy do spraw cyberbezpieczeństwa powinien nałożyć wyłącznie karę za to naruszenie, nie wymierzając już kary przewidzianej na zasadach ogólnych.

Za niewykonywanie obowiązków określonych w ustawie karze pieniężnej może podlegać także kierownik podmiotu kluczowego lub podmiotu ważnego. Co więcej, kara może zostać nałożona na kierownika podmiotu niezależnie od tego czy została nałożona na podmiot kluczowy lub podmiot ważny. Proponuje się, żeby kara mogła być wymierzona w kwocie nie większej niż 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. Wymierzając karę organ właściwy do spraw cyberbezpieczeństwa powinien kierować się w szczególności możliwościami finansowymi kierownika podmiotu.

Kary pieniężne nakładane są przez organ właściwy do spraw cyberbezpieczeństwa w drodze decyzji. Decyzja ta co do zasady nie jest natychmiastowo wykonalna z wyjątkiem sytuacji, w której wymaga tego ochrona bezpieczeństwa lub porządku publicznego. Może mieć to miejsce w szczególności gdy organ właściwy do spraw cyberbezpieczeństwa, po analizie naruszenia na podstawie kryteriów określonych w projektowanym art. 53 ust. 12 ustawy o KSC, uzna, że naruszenie to ma charakter na tyle poważny, że decyzja o wymierzeniu kary zasługuje na nadanie klauzuli natychmiastowej wykonalności. Kolejnym przykładem, w którym przesłanki bezpieczeństwa lub porządku publicznego mogą zostać zrealizowane, to okresowe kary pieniężne. Można bowiem wyobrazić sobie sytuację, w której brak podjęcia czynności określonych przez organ właściwy do spraw cyberbezpieczeństwa w decyzji będzie wiązał się z istotnym zagrożeniem dla bezpieczeństwa lub porządku publicznego, które należy oceniać sytuacyjnie pod względem wewnętrznym jak i zewnętrznym. Podkreślić należy, że dążąc do zapewnienia bezpieczeństwa lub porządku publicznego działania podejmowane przez organ nie mogą polegać wyłącznie na zwalczaniu zagrożeń, które już się zrealizowały, ale wymaga to podejmowania działań prospektywnych. W takiej sytuacji nadrzędną wartością będzie zapewnienie skuteczności wymierzonych kar co w pełni zagwarantuje nałożenie klauzuli natychmiastowej wykonalności na decyzję w przedmiocie wymierzenia okresowej kary pieniężnej.

Wpływy z tytułu kar pieniężnych stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667 oraz z 2024 r. poz. 834 i 1222).

Organ właściwy do spraw cyberbezpieczeństwa ustalając wysokość kary i wydając decyzję o wymierzeniu kary pieniężnej zobowiązany jest do uwzględniania kryteriów określonych w projektowanym art. 53 ust. 12 ustawy o KSC oraz wysokości przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, możliwości finansowych podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowych kierownika podmiotu. Z tego powodu konieczne jest, aby podmiot kluczowy lub podmiot ważny, na żądanie organu właściwego do spraw cyberbezpieczeństwa, przekazał wszelkie niezbędne do wymierzenia kary dane. Chcąc jednocześnie zapobiec sytuacji, w której organ nie będzie mógł wymierzyć kary z powodu braku wykonania polecenia przez podmiot, organ ten będzie uprawniony do ustalenia podstawy wymiaru kary pieniężnej w sposób szacunkowy. W tym celu może skorzystać z ogólnodostępnych danych oraz wziąć pod uwagę specyfikę działalności podmiotu i jego wielkość. W przypadku podmiotów kluczowych lub podmiotów ważnych będących podmiotami publicznymi ich możliwości finansowe ustala się przede wszystkim biorąc pod uwagę środki finansowe w części budżetowej przeznaczonej dla danego podmiotu.

Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, o której mowa w art. 73 lub dodawanym art. 73a ustawy o KSC, w sytuacji, w której waga i znaczenie naruszonych przepisów jest znikome, a podmiot albo kierownik podmiotu zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

Istotną zmianą jest wprowadzenie możliwości nakładania na podmiot okresowej kary pieniężnej. Będzie to możliwe w sytuacji, w której podmiot opóźnia się z wykonaniem czynności określonych w decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8 ustawy o KSC. Za każdy dzień opóźnienia organ właściwy do spraw cyberbezpieczeństwa będzie mógł nałożyć karę pieniężną w wysokości od 500 zł do 100 000 zł. Należy zwrócić uwagę, że okresowa kara pieniężna różni się od kary nakładanej w artykułach poprzedzających tym, że karane nie jest samo naruszenie przepisów ustawy, a zwłoka w wykonaniu czynności zleconych przez organ, często w związku z tym naruszeniem. Okresowa kara pieniężna ma stanowić zatem narzędzie do efektywnego egzekwowania stosowania przepisów ustawy i wykonywania nałożonych na podmioty obowiązków.

Kara pieniężna jest także, zgodnie z wdrażaną dyrektywą NIS 2, środkiem nadzorczym, który może być stosowany niezależnie, a więc równolegle, do innych środków nadzorczych. Nałożenie kary pieniężnej na podmiot kluczowy lub podmiot ważny nie oznacza zatem, że organ właściwy do spraw cyberbezpieczeństwa nie może podjąć innych działań o charakterze nadzoru czy kontroli.

Doprecyzowano także, że w zakresie nieuregulowanym w rozdziale stanowiącym o karach stosuje się odpowiednio przepisy działu IVa Kpa.

2.25. Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej

Wprowadzono zmiany w przepisach dotyczących Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej. Zakres Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej został rozszerzony i uszczegółowiony, tak aby obejmował wszystkie kwestie kluczowe dla zapewnienia cyberbezpieczeństwa. Zmiana ta pozwoli zaadresować w tym dokumencie nowe istotne zagadnienia takie jak bezpieczeństwo łańcucha dostaw. Zmiana ta pozwoli też na uspójnienie dokumentów w poszczególnych państwach członkowskich.

Ponadto dodany został przepis pozwalający ministrowi właściwemu do spraw informatyzacji, będącemu organem odpowiedzialnym za realizacje Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej, uzyskiwać informacji o realizacji strategii od innych podmiotów zaangażowanych w jej realizację. Pozwoli to ministrowi na uzyskanie bieżących informacji o realizowanych zadaniach i na ewentualne podjęcie dodatkowych działań w danym obszarze. Wskazano również, że zespoły CSIRT poziomu krajowego, CSIRT sektorowe i organy właściwe do spraw cyberbezpieczeństwa będą corocznie informować ministra o postępach we wdrażaniu strategii.

Pozwoli to na skuteczniejszą realizację zadań z zakresu cyberbezpieczeństwa oraz bieżącą ocenę stanu realizacji Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej.

Równocześnie ze Strategią Cyberbezpieczeństwa Rzeczpospolitej Polskiej będzie przygotowany plan działań do Strategii, który będzie stanowił jej załącznik i operacjonalizował jej zapisy, w tym uwzględniał koszty realizacji i źródła finansowania działań.

2.26. Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

Zgodnie z dyrektywą NIS 2 przyjęte zostały przepisy wprowadzające Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwany

dalej „Krajowym Planem”. Będzie to dokument strategiczny określający rolę organów, środki i procedury w przypadku wystąpienia sytuacji kryzysowej związanej z cyberbezpieczeństwem. Dokument ten ma posłużyć koordynacji działań z zakresu zapewniania cyberbezpieczeństwa i zarządzania kryzysowego w celu maksymalizacji ich efektywności.

Dokument ten będzie przyjmowany w drodze uchwały Rady Ministrów, a przygotowywany przez ministra właściwego do spraw informatyzacji. Dużą rolę w jego przygotowaniu będzie odgrywać również Rządowe Centrum Bezpieczeństwa gwarantując jego spójność z dokumentami z zakresu zarządzania kryzysowego.

Podobnie jak w przypadku Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej, minister będzie mógł zwracać się o informacje dotyczące realizacji Krajowego Planu do organów w nim wskazanych. Pozwoli mu to na bieżąco monitorować postępy we wdrażaniu Krajowego Planu i podejmować działania w razie wystąpienia nieprawidłowości.

2.27. Zmiany w podstawowych ustawach

Wprowadzone zmiany w zakresie podmiotów i funkcjonowania krajowego systemu cyberbezpieczeństwa wymagają również wprowadzenia zmian w szeregu innych ustaw. W szczególności nowelizacji wymagają poniższe ustawy.

Zmiany w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125) dotyczą wprowadzenia tam pojęcia usługi przetwarzania w chmurze, ponieważ obecna treść tej ustawy odwołuje się do obecnego załącznika nr 2 ustawy o KSC – a ten przepis jest zmieniany.

Zmiany w ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2024 r. poz. 497, 863 i 1243) umożliwią organom właściwym do spraw cyberbezpieczeństwa uzyskiwanie informacji o rocznej liczbie pracowników lub rocznej liczbie ubezpieczonych – co pozwoli na ustalenie wielkości przedsiębiorcy, a co za tym idzie statusu podmiotu kluczowego lub podmiotu ważnego.

Zmiany w ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2023 r. poz. 2383 i 2760 oraz 2024 r. poz. 879) dotyczą umożliwienia organom podatkowym przekazywania informacji organom właściwy do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Dane te są niezbędne do realizacji ustawowych zadań tych podmiotów,

a w szczególności do oceny czy dany podmiot spełnia przesłanki bycia podmiotem kluczowym lub ważnym oraz co do jego znaczenia w danym sektorze gospodarki.

Zmiany w ustawie z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz. U. z 2024 r. poz. 1194) pozwolą ministrowi właściwemu do spraw gospodarki powierzenie realizacji zadań CSIRT sektorowego dla sektorów produkcji, produkcji chemikaliów i przestrzeni kosmicznej Urzędowi Dozoru Technicznego, zwanego dalej „UDT". Aby UDT mógł realizować zadania CSIRT sektorowego konieczna jest zmiana art. 37 ustawy o dozorze technicznym określającego zakres działania UDT. Zmiana dotyczy dopisania do katalogu zadań UDT wykonywanie zadań określonych w przepisach ustawy o KSC. Projekt jako źródło finansowania utworzenia i utrzymania CSIRT wskazuje istniejący w UDT fundusz rezerwowy. Takie rozwiązanie jest neutralne dla budżetu państwa, zgodnie bowiem z art. 35 ustawy z dnia 21 grudnia 2000 r. o dozorze technicznym Skarb Państwa nie odpowiada za zobowiązania UDT. Taka konstrukcja przepisów odciąży zgodnie z założeniami OSR budżet Państwa w ciągu 10 lat na kwotę 100 mln. Projekt przewiduje również alternatywną opcję finansowania CSIRT przez UDT. Pojawia się możliwość tworzenia lub przystępowania do spółek prawa handlowego oraz posiadania, obejmowania lub nabywania akcji lub udziałów w spółkach przez państwową osobę prawną jaką jest Urząd Dozoru Technicznego. Pozwoli to na długofalowe finansowanie działalności podmiotu np. w przypadku wyczerpania środków funduszu rezerwowego.

Zmiany w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 422 i 1222). Wprowadzono przepisy, które umożliwią administracji skorzystanie z informacji, które już zgromadziła a także uchylono przepisy z których wynikały dotychczasowe obowiązki z zakresu cyberbezpieczeństwa dla dostawców usług zaufania – te obowiązki będą teraz wynikały ze znowelizowanej ustawy o KSC. Wynika to też z faktu, że dyrektywa NIS 2 uchyliła art. 19 EIDAS dotyczący wymogów bezpieczeństwa dla dostawców usług zaufania.

Zmiana w ustawie z dnia 6 marca 2018 r. – Prawo przedsiębiorców służy zapewnieniu spójności przepisów prawa i wskazaniu, że kontrole z ustawy o KSC mają specyficzny charakter. Dotyczą one tylko jednego aspektu działalności przedsiębiorcy czyli zapewniania cyberbezpieczeństwa. Przepisy te odnoszą się do podmiotów prowadzących działalność o szczególnym charakterze, która jest niezbędna dla prawidłowego funkcjonowania państwa i społeczeństwa. Wprowadzenie zmiany do powyższej ustawy jest również konieczne w związku z możliwością zajścia zbiegu nadzoru w sytuacji, w której podmiot kluczowy lub

podmiot ważny jest tym podmiotem równocześnie w kilku sektorach nadzorowanych przez różne organy właściwe do spraw cyberbezpieczeństwa. Należy zatem zapewnić skuteczność, szybkość i prawidłowość realizowanych środków nadzorczych, w szczególności kontroli. Podmiot kluczowy lub podmiot ważny może naruszać przepisy ustawy w różny sposób w kilku sektorach. Brak powyższej zmiany skutkowałby, że co najmniej jeden z organów właściwych do spraw cyberbezpieczeństwa sprawujących nadzór nad podmiotem kluczowym lub podmiotem ważnym nie mógłby realizować swoich obowiązków i kompetencji. W przypadku cyberbezpieczeństwa istotny jest czas, a czynności kontrolne powinny być realizowane bez żadnych przeszkód. Wskazać jednocześnie należy, że zmiany wprowadzane do ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców mają różny charakter – przepisy dotyczące kontroli na zasadach ogólnych będą wyłączone zarówno spod przepisów określających terminy kontroli u przedsiębiorców jak i przepisu zakazującego równoczesnej kontroli przez więcej niż jeden podmiot kontrolujący. W przypadku kontroli doraźnej wyłącza się jedynie zakaz równoczesnej kontroli, z tych samych powodów co powyżej. Terminy będą musiały być jednak takie jak wskazuje ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców, gdyż kontrola doraźna jest uproszczoną formą kontroli, a w zakresie nieuregulowanym stosuje się w przypadku podmiotów będących przedsiębiorcami przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

Wprowadza się również zmianę w art. 226 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320). Artykuł ten reguluje sytuacje, w których zamawiający odrzuca ofertę złożoną w ramach postępowania o zamówienie publiczne. Kolejną przesłanką odrzucenia oferty będzie sytuacja, gdy oferta obejmuje produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w projektowanym art. 66a ust. 13 ustawy o KSC oraz usługę ICT lub proces ICT, określone w tej decyzji.

Zmiany w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667 oraz z 2024 r. poz. 834 i 1222) dotyczą:

1) wprowadzenia zasady, że dotacja z budżetu państwa dla Funduszu Cyberbezpieczeństwa ma charakter bezzwrotny – chodzi o to, aby niewykorzystane w danym roku środki na świadczenie teleinformatyczne, pochodzące z dotacji mogły pozostać w Funduszu na kolejny rok;

2) dostosowania treści art. 5 ustawy i wskazanie, że świadczenie teleinformatyczne przysługuje pracownikom zatrudnionym w zespołach CSIRT sektorowych;
3) wskazanie, że świadczenie teleinformatyczne będzie przysługiwać również osobom realizującym zadania w zakresie zapewnienia cyberbezpieczeństwa w Urzędzie Ochrony Danych Osobowych oraz w jednostkach Krajowej Administracji Skarbowej;
4) uregulowania przychodu z kar pieniężnych, o których mowa w art. 101 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, które staną się jednym z przychodów Funduszu Cyberbezpieczeństwa.

Zmiany te wpłyną na przychody Funduszu Cyberbezpieczeństwa co pozwoli na zwiększenie wsparcia udzielanego organom administracji na zapewnienie cyberbezpieczeństwa ich systemów informacyjnych.

2.28. Przepisy przejściowe, dostosowujące i końcowe

Projekt ustawy wskazuje, że postępowania karnoadministracyjne oraz kontrole wszczęte i niezakończone przed dniem wejścia w życie ustawy zostaną ukończone na podstawie przepisów dotychczasowych. Gwarantuje to, że podmioty, których te postępowania dotyczą nie zostaną zaskoczone nowymi zasadami i pozwoli zakończyć te postępowania w odpowiednim terminie. Dotychczasowe przepisy mają zastosowanie również do rozpoczętej obsługi incydentu, ponieważ w przypadku wystąpienia incydentu istotne jest postępowanie zgodnie z ustalonymi procedurami. Projektowane przepisy dotyczące obsługi incydentu wprowadziły szereg nowych obowiązków nałożonych na podmiot m.in. obowiązek sporządzenia raportu końcowego, dlatego też zdecydowano by trwające incydenty zostały obsłużone na dotychczasowych zasadach. Pozwoli to uniknąć sytuacji, w której podmioty musiałyby zmieniać swoje wewnętrzne procedury przy jednoczesnym zwalczaniu skutków incydentu, co w znacznym stopniu mogłoby utrudnić prawidłową obsługę incydentu. Zachowane w mocy zostały rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, dotyczących stosowania urządzeń informatycznych lub oprogramowania, co wynika z zastosowania nowych przepisów do badań rozpoczętych i niezakończonych na podstawie obecnie obowiązującego art. 33 ust. 1 ustawy o KSC.

Minister właściwy do spraw informatyzacji uruchomi rejestr podmiotów kluczowych i podmiotów ważnych w ciągu miesiąca od dnia wejścia w życie ustawy. Rejestr będzie prowadzony elektronicznie w związku z czym taki termin gwarantuje czas niezbędny na jego uruchomienie i odpowiednie zabezpieczenie. Minister właściwy do spraw informatyzacji

w komunikacje ogłoszonym w dzienniku urzędowym ministra właściwego do spraw informatyzacji określi termin złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych przez podmioty kluczowe i podmioty ważne oraz rozpoczęcia korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ustawy o KSC.

W przepisach przejściowych rozstrzygnięto, że podmioty mające obecnie status operatorów usług kluczowych w momencie wejścia w życie ustawy zostaną również automatycznie wpisane na listę podmiotów kluczowych. Jest to niezbędne dla zapewnienia ciągłości realizowanych przez nie zadań m.in. obsługi incydentów. Dzięki takiemu rozwiązaniu podmioty te nie będą również musiały przeprowadzać wewnętrznych analiz i dokonywać samoidentyfikacji co oszczędzi im czas. Należy podkreślić, że obecne przepisy dużo węziej definiują operatorów usług kluczowych niż wynika to definicji podmiotów kluczowych. W związku z czym nie ma wątpliwości, że podmioty te spełniają przesłanki dla podmiotów kluczowych.

Przepisy przewidują, że do czasu wdrożenia przez ministra właściwego do spraw informatyzacji rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej doręczenie pism na elektroniczną skrzynkę podawczą w ePUAP, w ramach usługi udostępnianej w ePUAP, jest równoważne w skutkach prawnych z doręczeniem przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego. To rozwiązanie pozwoli na realizację zadań i obowiązków określonych w ustawie nawet w przypadku gdyby do czasu jej wejścia w życie ww. rozwiązania w zakresie doręczenia elektronicznego nie zostały uruchomione.

W zakresie podmiotów świadczących usługi rejestracji nazw domen został zastosowany termin 6-miesięczny na dostosowanie baz danych oraz wdrożenie odpowiednich polityk i procedur. Nowe regulacje dotyczące tych podmiotów znacząco wpływają na ich działalność w związku z czym konieczne jest zapewnienie im odpowiedniego czasu na wprowadzenie niezbędnych rozwiązań technicznych.

Przepisy regulują przekazanie przez ministra właściwego do spraw informatyzacji danych dotyczących ilości podmiotów kluczowych i podmiotów ważnych i przepisów na podstawie których je zidentyfikowano w terminie do dnia 17 kwietnia 2025 r. do Komisji Europejskiej oraz Grupy Współpracy. Obowiązek ten wynika bezpośrednio z art. 3 ust. 5 dyrektywy NIS 2. Wykonanie tych przepisów pozwoli Komisji skutecznie oszacować liczbę podmiotów

kluczowych i ważnych w całej Unii a następnie podejmować kolejne działania mające na celu zwiększenie ich cyberbezpieczeństwa. Minister przekaże też Komisji informacje dotyczące wyznaczenie krajowego organu do spraw zarządzania kryzysowego w cyberbezpieczeństwie. Do tych działań jesteśmy bezpośrednio zobligowani przepisami dyrektywy NIS 2.

Przepisy przewidują też rozszerzenie możliwości badania produktów przez zespoły CSIRT. Badaniu bezpieczeństwa nie mogą stać na drodze standardowe postanowienia licencji, które zakazują takich działań. Z tego względu w przepisach przejściowych dotyczących umów już obowiązujących konieczne były przesądzenie, że takie klauzule umowne utracą moc. Nie może być sytuacji by umowa cywilnoprawna uniemożliwiała organom państwa skuteczne działania w zakresie bezpieczeństwa.

W ramach zmian w funkcjonowaniu systemu S46 przewidziana jest rezygnacja z zawierania osobnych porozumień z przystępującymi obecnie podmiotami. Równocześnie w ramach tego systemu przyłączono już pewną liczbę podmiotów a ich prawa i obowiązki uregulowano w porozumieniach. W takim przypadku, dla zapewnienia efektywnej realizacji zadań zasadnym jest utrzymanie tych porozumień w mocy.

Dla zapewnienia ciągłości działań Kolegium do Spraw Cyberbezpieczeństwa konieczne jest utrzymanie w mocy rozporządzenia wydanego na podstawie art. 66 ust. 9 ustawy o KSC.

W dotychczasowym stanie prawnym CSIRT MON, CSIRT NASK i CSIRT GOV mogły zawierać porozumienia przekazujące określone podmioty do właściwości CSIRT innego niż ten wskazany w ustawie. W związku ze zmianami w zakresie struktury podmiotowej krajowego systemu cyberbezpieczeństwa konieczne jest przesądzenie o sytuacji tych porozumień. Zawarte w ustawie rozwiązanie zapewniają podmiotom czas na dostosowanie tych porozumień do zmian w przepisach.

Organy właściwe do spraw cyberbezpieczeństwa będą miały 18 miesięcy na utworzenie CSIRT sektorowych. Termin ten ma pozwolić na utworzenie nowych podmiotów, skompletowanie niezbędnej kadry oraz zapewnienie im zasobów do działań. Utworzenie CSIRT sektorowego podlega ogłoszeniu, w drodze komunikatu, w dzienniku urzędowym danego organu właściwego oraz na stronie internetowej m.in. Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Takie rozwiązanie pozwoli na precyzyjne określenie momentu od kiedy podmioty obowiązane będą miały realizować obowiązki do CSIRT sektorowych. Do tego czasu obowiązki te będą realizowane w stosunku do dotychczasowo właściwych CSIRT poziomu krajowego.

Przepisy określają też jakie informacje zostaną zamieszczone w sprawozdaniu z działania CSIRT sektorowego w roku, w którym został on utworzony. W tym okresie podstawową kwestią będzie zapewnienie takiemu podmiotowi wszystkich narzędzi i zasobów niezbędnych do realizacji jego działań. Może on w tym okresie nie zrealizować swoich standardowych zadań. Z tego względu sprawozdanie to będzie zawierało kwestie związane z jego utworzeniem.

Powołane już sektorowe zespoły cyberbezpieczeństwa staną się z chwilą wejścia w życie projektu ustawy CSIRT sektorowymi. Przepis ten pozwoli zapewnić pełną ciągłość ich działań.

Projekt ustawy dodaje nowe zdania, które do tej pory nie były planowane w budżecie państwa, stąd też w projekcie zostały dodane przepisy określające zwiększenie limitów wydatków w poszczególnych częściach budżetowych, a w przypadku ich przekroczenia nakazujące wprowadzenie mechanizmu korygującego. Wpływ projektowanej ustawy na sektor finansów publicznych został szczegółowo określony w Ocenie Skutków Regulacji.

2.29. Załączniki

Załącznik nr 1 do projektu ustawy określa sektory, i w ich obrębie, podsektory w ramach których działają podmioty kluczowe. Są to obszary, które zostały uznane za szczególnie istotne dla prawidłowego funkcjonowania państwa takie jak energetyka, transport, bankowość czy dostarczanie wody pitnej. Wystąpienie przerw w działaniu usług kluczowych podmiotów w tych sektorach będzie miało natychmiastowy i znaczny wpływ na całe funkcjonowanie społeczeństwa na określonym obszarze i z tego powodu to właśnie je uznano za szczególnie istotne. Załącznik nr 1 do projektu ustawy oparty jest na załączniku I do dyrektywy NIS 2, rozszerza jednak jego zakres o działalność w zakresie wydobywania kopalin, energii jądrowej oraz podmiotów publicznych.

Działalność w zakresie wydobycia kopalin to działalność, która również posiada bardzo istotny wpływ na funkcjonowanie innych podmiotów, zwłaszcza innych podmiotów z sektora energii i dlatego powinna być objęta tymi samymi regułami co przedsiębiorstwa wytwarzające i przesyłające prąd. Należy również podkreślić, że podmioty z tego sektora są obecnie objęte postanowieniami ustawy o krajowym systemie cyberbezpieczeństwa i mają już obecnie obowiązki z tego wynikające.

Ze względu zarówno na:

1) znaczną doniosłość świadczonych usług (pozyskiwanie surowca, wytwarzanie paliwa, wykorzystanie paliwa do generacji elektryczności, ciepła oraz potencjalnie wodoru, postępowanie ze zużytym paliwem oraz innymi odpadami radioaktywnymi),
2) bezpieczeństwo jądrowe oraz ochronę radiologiczną

– zasadnym jest, aby operatorzy obiektów energetyki jądrowej zostali uznani za podmioty kluczowe – niezależnie od przewyższania wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Wdrażana dyrektywa NIS 2 oparta jest na zasadzie minimalnej harmonizacji (art. 5 dyrektywy). Wobec czego zasadnym jest przyjęcie szerszego niż przewidziany w dyrektywie katalogu podmiotów objętych regulacjami ustawy o KSC.

Mając na uwadze:

1) rozwój energetyki jądrowej w Polsce – zarówno programu rządowego jak i inicjatyw prywatnych;
2) znaczenie podmiotów z jądrowego cyklu paliwowego (od wydobycia rudy, poprzez wzbogacanie izotopowe, wytworzenie paliwa jądrowego, jego wykorzystanie, postępowanie z wypalonym paliwem jądrowym i odpadami radioaktywnymi) dla świadczenia usług wytwarzania energii, ciepła, a potencjalnie również wodoru;
3) znaczenie paliwa jądrowego dla funkcjonowania elektrowni jądrowych – generacji elektryczności, ciepła i wodoru;
4) ryzyka związane z paliwem jądrowym na każdym etapie postępowania z nim

zasadnym jest poszerzenie katalogu podmiotów kluczowych o operatorów obiektów wskazanych w art. 2 ust. 2 ww. ustawy, tj. operatorów:

a) zakładu do wydobywania rud uranu i toru ze złóż i do ich wstępnego przetwarzania,

b) zakładu wzbogacania izotopowego,

c) zakładu wytwarzania paliwa jądrowego,

d) elektrowni jądrowej,

e) zakładu przerobu wypalonego paliwa jądrowego,

f) przechowalnika wypalonego paliwa jądrowego,

g) obiektu do przechowywania odpadów promieniotwórczych,

h) składowisko odpadów promieniotwórczych.

2.29.1. Podmioty zaangażowane w proces wytwarzania paliwa.

Zakłady wskazane w lit. a-c są zaangażowane w wytwarzanie paliwa jądrowego do reaktorów jądrowych. Tym samym w zakresie energetyki jądrowej ich rola jest analogiczna do podmiotów, które odpowiadają za pozyskanie takich surowców jak węgiel, gaz czy ropa. Tak jak węgiel, gaz czy ropa stanowią nośniki energii pierwotnej (paliwa) do dalszego wykorzystania, podobną rolę pełni paliwo jądrowe dla reaktorów. Skoro więc za podmioty kluczowe uznaje się podmioty odpowiedzialne za pozyskanie węgla, gazu i ropy, a także przesył czy dystrybucję, również podmioty zaangażowane w cykl wytwarzania paliwa jądrowego powinny zostać objęte wymogami z zakresu cyberbezpieczeństwa.

2.29.2. Wykorzystanie paliwa – elektrownia jądrowa.

Operator elektrowni jądrowej powinien zostać uznany za podmiot kluczowy niezależnie od kwestii z przewyższania wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Za „oderwaniem" operatora elektrowni jądrowej od kwestii wielkość przedsiębiorstwa przemawia nie tylko kwestia zapewnienia ciągłości pracy, ale również bezpieczeństwa jądrowego i ochrony radiologicznej,

Stąd ujmowanie operatorów elektrowni jądrowych jako objętych regulacją ustawy o zmianie ustawy o ksc w ramach przedsiębiorstw energetycznych posiadających koncesje na wytwarzanie energii elektrycznej lub ciepła (załącznik nr 1 w zw. z projektowanym art. 5 ust. 1 pkt 1 ustawy o KSC, sektor energia) jest niewystarczające, gdyż wiąże kwestie objęcia tą kategorią z przewyższaniem wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Pomiędzy osiągnięciem przez elektrownię jądrową zdolności operacyjnej, a uzyskaniem koncesji na wytwarzanie energii elektrycznej lub ciepła może wystąpić „luka" czasowa, która spowoduje okres ekspozycji na cyberzagrożenia – w tym wykorzystanie podatności przez zagrożenia, które aktywują się zarówno przed jak i po uzyskaniu koncesji. Moment identyfikacji powinien więc być wcześniejszy, o czym niżej.

2.29.3 Wypalone paliwo jądrowe i odpady radioaktywne.

Operatorzy obiektów jądrowych wymienionych w powyżej w lit. e-h są z kolei zaangażowani w postępowanie z wypalonym paliwem jądrowym oraz odpadami radioaktywnymi. Ich rola w tym zakresie jest więc analogiczna do roli podmiotów zaangażowanych w gospodarkę odpadami, które znalazły się w załączniku jako podmioty kluczowe. Podmioty wymienione powyżej w lit. e-h nie wydają się jednak objęte załącznikiem. Załącznik nawiązuje do ustawy z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, 1688, 1852 i 2029), której nie stosuje się do odpadów promieniotwórczych (art. 2 pkt 4 ustawy z dnia 14 grudnia 2012 r. o odpadach). Dodatkowo załącznik co do zasady wiąże status podmiotu kluczowego z przewyższaniem wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

Składowisko odpadów promieniotwórczych – w chwili obecnej w Polsce funkcjonuje tylko jedno składowisko odpadów promieniotwórczych, prowadzone przez Zakład Unieszkodliwiania Odpadów Promieniotwórczych (ZUOP) – jednostkę nadzorowaną przez ministra właściwego do spraw energii, a po wejściu w życie uchwalonej przez Sejm ustawy o zmianie, będzie nadzorowany przez ministra do spraw gospodarki surowcami energetycznymi. W związku z rozwojem energetyki jądrowej konieczne będzie powstanie dalszych składowisk odpadów promieniotwórczych – zarówno powierzchniowych jak i głębokich. Obecnie nie wiadomo w jakiej formie prawnej będą funkcjonowały, ani czy ich operatorzy będą podlegali nadzorowi ze strony określonego ministra. Stąd zasadne jest uznanie operatora składowiska odpadów promieniotwórczych za podmiot kluczowy. Takie rozwiązanie zapewni odpowiedni poziom ogólności przepisów i ich elastyczność w przypadku, gdyby operatorzy nowych składowisk nie byli objęci kategorią jednostek nadzorowanych.

Ze względu na znaczną doniosłość świadczonych usług jak i kwestie związane z bezpieczeństwem jądrowym oraz ochroną radiologiczną zasadnym jest, aby operatorzy obiektów energetyki jądrowej zostali uznani za podmioty kluczowe – niezależnie od przewyższania wymogów dla średniego przedsiębiorstwa określonych w art. 2 ust. 1 załącznika I do rozporządzeniem 651/2014/UE (projektowany art. 5 ust. 1 pkt 1 ustawy o KSC).

2.29.4 Moment uzyskania statusu podmiotu kluczowego.

W odniesieniu do podmiotów paliwowego cyklu jądrowego moment uzyskania statusu podmiotu kluczowego mógłby zostać powiązany z uzyskaniem określonego zezwolenia,

o którym mowa w art. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2024 r. poz. 1277), np. zezwolenia na eksploatację – art. 4 ust. 1 pkt odpowiednio 2 lub 3 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe.

W odniesieniu do operatora elektrowni jądrowej moment uzyskania statusu podmiotu kluczowego mógłby stanowić połączenie art. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (zezwolenie na eksploatację) z art. 32 ustawy z dnia 10 kwietnia 2017 r. – Prawo energetyczne (Dz. U. z 2024 r. poz. 266, 834 i 859) – koncesje, w zależności od tego, które zostałoby uzyskane jako pierwsze.

W przypadku zakładu do wydobywania rud uranu i toru ze złóż i ich wstępnego przetwarzania moment uzyskania statusu podmiotu kluczowego mógłby stanowić połączenie art. 4 ustawy z dnia 29 listopada 2000 r. – Prawo atomowo (zezwolenie na eksploatację) z art. 22 ustawy z dnia 9 czerwca 2011 r. – Prawa geologicznego i górniczego (Dz. U. z 2024 r. poz. 1290) (koncesje na wydobywanie kopalin) – w zależności od tego, które zostałoby uzyskane jako pierwsze.

W ramach załącznika nr 1 do projektu ustawy uwzględniono także obecne rodzaje podmiotów, które mogą być uznane za operatorów usług kluczowych. Przykładowo dotyczy to przedsiębiorców, którzy prowadzą aptekę ogólnodostępną – ten rodzaj podmiotu nie wynika z dyrektywy NIS 2, jednakże w polskiej transpozycji dyrektywy NIS1 został on uznany za operatora usług kluczowych.

Załącznik nr 2 do projektu ustawy określa sektory, i w ich obrębie podsektory, dotyczące podmiotów ważnych. Należą do nich m.in. produkcja, przetwarzanie i dystrybucja żywności, gospodarowanie odpadami czy usługi pocztowe, produkcja, wytwarzanie i dystrybucja chemikaliów, produkcja, przetwarzanie i dystrybucja żywności i produkcja ogółem. Wszystkie z tych rodzajów działalności są istotne dla prawidłowego funkcjonowania społeczeństwa, ale równocześnie ich zakłócenie nie powoduje skutków w tak krótkiej perspektywie czasowej jak w przypadku podmiotów kluczowych. Tabela ta jest w całości oparta na załączniku II do dyrektywy NIS 2.

Załącznik nr 3 do projektu ustawy określa funkcje krytyczne. Jest on oparty na rozwiązaniach z innych państw europejskich, zwłaszcza francuskiej liście funkcji krytycznych. Załącznik ten wskazuje funkcje których narażenie szczególnie zagroziłoby systemowi czy sieci w ramach której funkcjonują. Produkty, usługi lub procesy pochodzące od dostawcy wysokiego ryzyka

muszą być wycofane w pierwszej kolejności co odzwierciedla krótszy termin na wykonanie tego obowiązku.

3. Pozostałe informacje

Projektowana ustawa wejdzie w życie po upływie 1 miesiąca od dnia jej ogłoszenia. Taki termin gwarantuje, że wszystkie podmioty, których dotyczą projektowane przepisy, będą miały czas na zapoznanie się z nimi. Termin ten jest też konieczny z uwagi na konieczność wdrożenia dyrektywy NIS 2 do dnia 17 października 2024 r. Zauważyć przy tym należy, że ustawa przewiduje 6 miesięczny okres dostosowawczy dla podmiotów kluczowych i podmiotów ważnych. Takie rozwiązanie zapewni wdrożenie dyrektywy w terminie, a z drugiej strony pozwoli podmiotom przygotować się do jej wdrożenia.

Projekt ustawy nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

Projekt ustawy zostanie przesłany do Europejskiego Banku Centralnego, w celu uzyskania opinii, natomiast nie podlega przedstawieniu innym właściwym organom i instytucjom Unii Europejskiej, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806) został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.