CYBERBEZPIECZEŃSTWO

– krajobraz regulacyjny przed implementacją dyrektywy NIS 2

RAPORT KANCELARII MARUTA WACHTA SPORZĄDZONY W RAMACH CALPE

CALPE
CENTRUM ANALIZ LEGISLACYJNYCH I POLITYKI EKONOMICZNEJ

MARUTA \

Szanowni Państwo,

w ostatnich latach obserwujemy wzrost zainteresowania kwestiami cyberbezpieczeństwa. Zwiększa się znaczenie usług cyfrowych w codziennych życiu i działalności przedsiębiorstw, rośnie liczba i skala zagrożeń w „cyfrowym świecie". Kluczowe staje się budowanie wspólnych standardów i schematów postępowania, a w konsekwencji – coraz większego znaczenia nabiera kwestia regulacji prawnych, które dotyczą cyberbezpieczeństwa.

Od czasu wdrożenia dyrektywy NIS minęły już ponad 3 lata. Obecnie obserwujemy wzmożoną aktywność legislacyjną unijnych organów. Za chwilę poznamy ostateczne brzmieniem dyrektywy NIS 2, która zastąpi w całości dyrektywę NIS. Równolegle pojawiają się propozycje uregulowania konkretnych kategorii podmiotów czy sektorów działalności. Przykładem może być rozporządzenie w sprawie operacyjnej odporności sektora finansowego (tzw. rozporządzenie DORA), a także nowa dyrektywa w sprawie odporności podmiotów krytycznych (tzw. dyrektywa CER).

Niezależnie od przepisów UE trwają prace nad znowelizowaniem polskiej ustawy o krajowym systemie cyberbezpieczeństwa. Pytanie tylko, czy to rzeczywiście dobry kierunek wobec nieuchronnej konieczności wdrożenia wymogów NIS 2. Może się okazać, że nowa wersja krajowych przepisów za chwilę będzie wymagać kolejnych zmian.

W raporcie próbujemy uporządkować i opisać regulacyjną rzeczywistość z perspektywy obowiązujących i planowanych regulacji. Najpierw omówimy przepisy, które obowiązują teraz, i wskażemy główne cechy polskiego systemu cyberbezpieczeństwa. Następnie skupimy się na tym, co czeka nas w niedalekiej przyszłości. Omówimy założenia nadchodzącej dyrektywy NIS 2 i odniesiemy się do prac legislacyjnych, które mają znowelizować ustawę KSC.

Ze względu na szeroki, przekrojowy charakter raport ten nie powinien być traktowany jako wyczerpujące opracowanie tematu, a jedynie jako wstęp do dalszej dyskusji.

Życzymy przyjemnej lektury!

Spis treści

WSTĘP Regulacyjny krajobraz cyberbezpieczeństwa w Polsce

RAMY PRAWNE polskiego systemu cyberbezpieczeństwa

Ramy prawne dotyczące cyberbezpieczeństwa w Polsce są w dużej mierze implementacją modelu przyjętego na poziomie Unii Europejskiej. Najważniejszy akt prawny w tym zakresie, czyli ustawa o Krajowym Systemie Cyberbezpieczeństwa (zwana dalej KSC), jest implementacją unijnej dyrektywy NIS. Obowiązuje też szereg rozporządzeń wydanych m.in. na podstawie upoważnień zawartych w KSC. Regulacyjny krajobraz cyberbezpieczeństwa jest więc dość złożony. Nie ma ogólnie obowiązującego aktu prawnego w obszarze cyberbezpieczeństwa, który dotyczyłby wszystkich podmiotów.

ⓘ Najważniejsze unijne akty prawne

- Dyrektywa (UE) 2016/1148 z dnia 6 lipca 2016 roku (Dyrektywa NIS)
- Rozporządzenie (UE) 2019/881 z dnia 17 kwietnia 2019 roku (Cybersecurity Act)
- Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r.
- Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 roku (RODO)
- Rozporządzenie (UE) 910/2014 z dnia 23 lipca 2014 roku (rozporządzenie eIDAS)

ⓘ Najważniejsze krajowe akty prawne

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym
- Ustawa z dnia 16 lipca 2004 roku - Prawo telekomunikacyjne
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji usług publicznych
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (implementacja dyrektywy 2000/31/CE)
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (UODO)
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (implementacja dyrektywy 2016/680/UE)

Polskie regulacje dotyczące cyberbezpieczeństwa pozostają pod dużym wpływem modelu przyjętego na poziomie unijnym. Model ten opiera się przede wszystkim na koordynacji działań i wymianie informacji między podmiotami krajowego systemu cyberbezpieczeństwa

MODEL oparty na koordynacji i wymianie informacji

Polska w zakresie cyberbezpieczeństwa na wzór regulacji UE przyjęła model oparty na koordynacji i wymianie informacji. Ten model zakłada, że niezbędne jest stworzenie warunków do efektywnej wymiany informacji między kluczowymi podmiotami, aby skutecznie zwalczać cyberprzestępczość.

Co do zasady przyjęty model jest pozytywnie oceniany. Pokazuje to m.in. raport ENISA dotyczący współpracy między zespołami reagowania na incydenty bezpieczeństwa komputerowego (ang. Computer Security Incident Response Team, w skrócie CSIRT). **Jak wskazano w raporcie ENISA za 2021 rok, współpraca między CSIRT-ami, policją i prokuraturą układa się w Polsce dobrze na tle innych państw europejskich.**

GŁÓWNE ZAŁOŻENIA MODELU PRZYJĘTEGO W POLSCE

- **Stworzenie warunków do szybkiej i efektywnej wymiany informacji** o incydentach, zwłaszcza między podmiotami o strategicznym znaczeniu dla państwa i gospodarki
- **Współpraca** zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), policji oraz prokuratury w reakcji na zagrożenia i ataki w cyberprzestrzeni
- **Dobrowolne dzielenie się wiedzą** o zagrożeniach cyberbezpieczeństwa, podatnościach i wykorzystywanych technologiach w ramach Krajowego systemu cyberbezpieczeństwa.

Współpraca pomiędzy trzema środowiskami [polskimi CSIRT-ami, policją i prokuraturą – przyp. aut. raportu] została oceniona przez rozmówców jako dobra, zwłaszcza, że te trzy środowiska mają różne role i obowiązki. Jak podkreślano podczas wywiadów, CSIRT NASK współpracuje na co dzień z Biurem do Walki z Cyberprzestępczością Komendy Głównej Policji. Podczas wywiadów wspominano, że gorąca linia CSIRT jest często wykorzystywana przez pracowników tego biura, co jest niezwykle przydatne (...).

Raport ENISA, s. 59

Podstawowe założenia KSC

KSC odnosi się do ograniczonego grona podmiotów. Są to operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC) i podmioty publiczne. Wraz z podmiotami wymienionymi w art. 4 KSC współtworzą oni krajowy system cyberbezpieczeństwa.

Podmioty objęte krajowym systemem cyberbezpieczeństwa
zgodnie z art. 4 KSC

* o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych
** w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej

Ramy prawne systemu cyberbezpieczeństwa są wynikiem implementacji przepisów przyjętych na poziomie UE. Co do zasady KSC odpowiada założeniom NIS

Podstawowe POJĘCIA

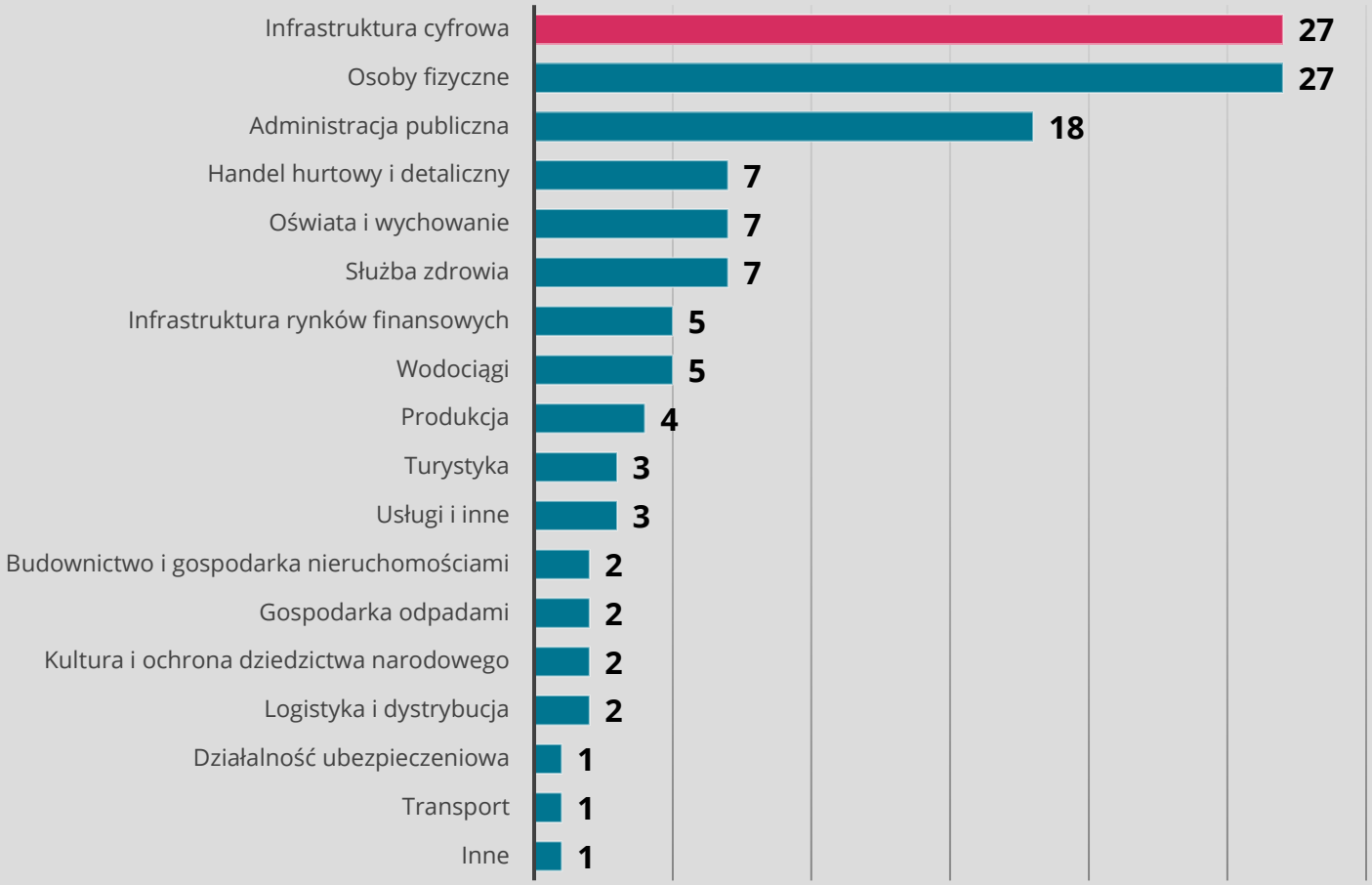
Cyberbezpieczeństwo w KSC rozumiane jest jako odporność systemów informatycznych na działania zagrażające poufności, integralności, dostępności i autentyczności przetwarzanych danych lub powiązanych usług oferowanych przez te systemy. Kluczowe dla KSC jest też pojęcie incydentu, przez który rozumie się **każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo**.

W KSC kładzie się szczególny nacisk na ochronę przed incydentami poważnymi, tzn. takimi, które zagrażają poważnym obniżeniem jakości lub przerwaniem ciągłości świadczenia usług kluczowych. Wykaz usług kluczowych jest dość szeroki i zawiera różne usługi dotyczące wydobywania kopalin, energii elektrycznej, ciepła, ropy naftowej, gazu, dostaw i usług dla sektora energii, substancji promieniotwórczych, transportu lotniczego, kolejowego, wodnego oraz drogowego, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej. **W obecnym brzmieniu KSC wyróżnia trzy usługi cyfrowe: internetową platformę handlową, usługę przetwarzania w chmurze oraz wyszukiwarkę internetową**.

OBOWIĄZKI i wymiana informacji

KSC nakłada na operatorów usług kluczowych, dostawców usług cyfrowych (z wyjątkiem mikro- i małych przedsiębiorców) oraz wskazane w ustawie podmioty publiczne szereg obowiązków w zakresie zarządzania bezpieczeństwem, zgłaszania i klasyfikacji incydentów, audytów i wewnętrznej organizacji

Liczba incydentów ransomware zarejestrowanych przez CERT Polska w podziale na sektory



Źródło: Raport roczny z działalności CERT Polska za 2021 r.
https://cert.pl/uploads/docs/Raport_CP_2021.pdf

Aby podmioty, które są częścią krajowego systemu cyberbezpieczeństwa, mogły skutecznie wymieniać informacje, zgodnie z KSC tworzy się **system IT wspierający ich pracę**. Za pośrednictwem tego systemu podmioty objęte krajowym systemem cyberbezpieczeństwa – w tym operatorzy usług kluczowych oraz dostawcy usług cyfrowych – mogą m.in. zgłaszać i obsługiwać incydenty oraz przekazywać sobie ostrzeżenia o zagrożeniach dla cyberbezpieczeństwa.

Aby zapewnić spójność i skuteczną koordynację polityki cyberbezpieczeństwa na poziomie krajowym i unijnym, KSC utworzyła trzy podmioty: **Kolegium do Spraw Cyberbezpieczeństwa, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Pojedynczy Punkt Kontaktowy**. Podmioty te mają w KSC z góry przypisane zakresy obowiązków.

Warto zauważyć, że incydent w rozumieniu KSC może być jednocześnie naruszeniem innej ustawy odnoszącej się do cyberbezpieczeństwa, na przykład naruszeniem ochrony danych osobowych w rozumieniu RODO. Wymagania wynikające z różnych regulacji stosowane są zwykle niezależnie.

OBOWIĄZKI OPERATORA USŁUGI KLUCZOWEJ
(terminy biegną od momentu, gdy dany podmiot zostanie uznany za operatora usługi kluczowej)

w ciągu 3 miesięcy

- szacuje ryzyko dla swoich usług kluczowych
- zarządza incydentami
- wyznacza osobę do kontaktu z właściwym CSIRT i właściwym organem ds. cyberbezpieczeństwa
- prowadzi działania edukacyjne wobec użytkowników
- obsługuje incydenty we własnych systemach
- zgłasza incydenty poważne
- usuwa wskazywane podatności

w ciągu 6 miesięcy

- wdraża odpowiedne środki techniczne i organizacyjne adekwatne do oszacowanego ryzyka
- zbiera informacje o zagrożeniach i podatnościach
- stosuje środki zapobiegające incydentom i ograniczające ich wpływ na bezpieczeństwo systemu informacyjnego
- stosuje wymaganą dokumentację

w ciągu 12 miesięcy

- przygotowuje pierwszy audyt w rozumieniu ustawy
- przekazuje sprawozdanie z audytu wskazanym w ustawie podmiotom

Źródło: Krajowy system cyberbezpieczeństwa - Cyfryzacja KPRM - Portal Gov.pl (www.gov.pl)

Organy odpowiedzialne – PODEJŚCIE SEKTOROWE

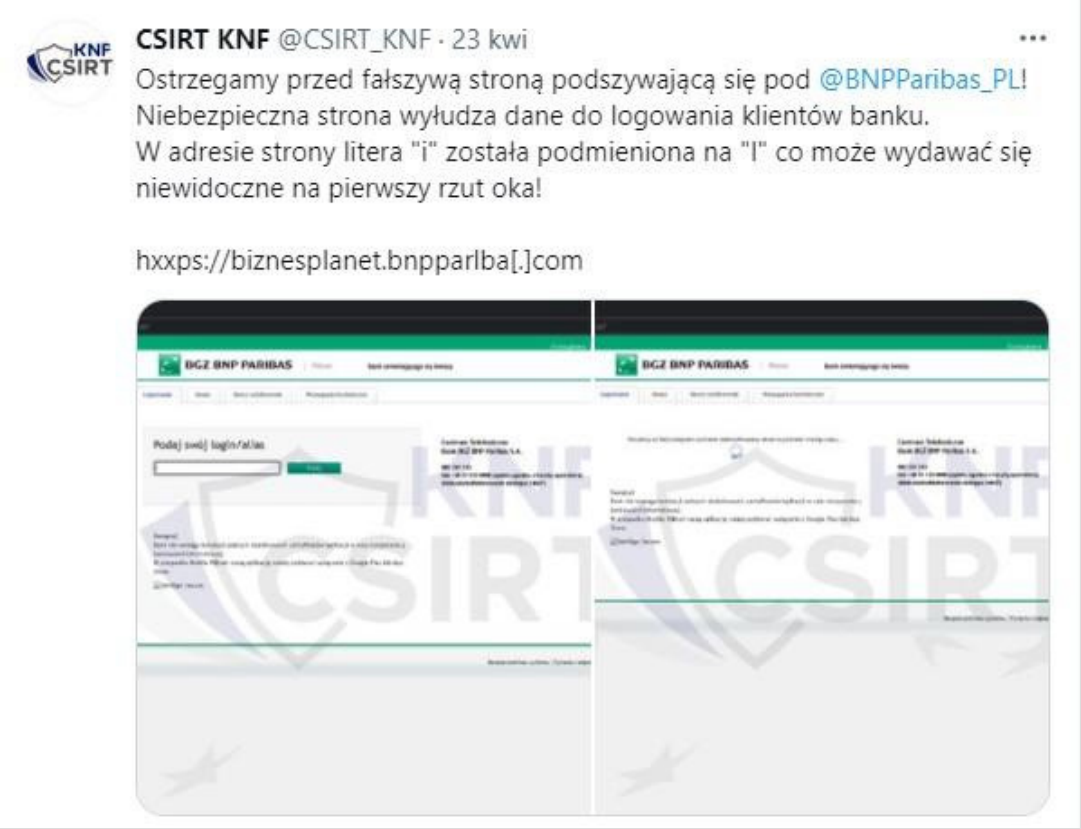
W polskim systemie cyberbezpieczeństwa przyjęto podejście sektorowe – nie utworzono, tak jak w kilku państwach UE, centralnego organu publicznego odpowiedzialnego za cyberbezpieczeństwo. Zamiast tego KSC wskazuje kilka organów odpowiedzialnych za ten obszar. Najczęściej jest to **minister lub centralny organ nadzorujący dany sektor** (np. dla sektora energetycznego – minister właściwy ds. polityki energetycznej, dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego itp.). Do głównych zadań tych organów należy:

- bieżąca analiza, które podmioty z danego sektora powinny być zakwalifikowane jako operatorzy usług kluczowych,
- monitorowanie zgodności operatorów usług kluczowych i dostawców usług cyfrowych w danym sektorze z wymogami KSC,
- audytowanie tych podmiotów i zawiadamianie ich o ewentualnej konieczności usunięcia podatności, które mogą prowadzić do wystąpienia incydentu.

Na poziomie krajowym działają również **trzy zespoły reagowania na incydenty bezpieczeństwa komputerowego: CSIRT MON, CSIRT NASK i CSIRT GOV**. Mają one zarządzać ryzykiem w obszarze cyberbezpieczeństwa i je ograniczać. Dodatkowo CSIRT KNF odpowiada za ten obszar w sektorze bankowym.

Szczegółowe obowiązki i zasady współpracy **CSIRT-ów wskazuje rozdział 6 KSC. CSIRT-y są kluczowymi podmiotami dla operacyjnej skuteczności krajowego systemu cyberbezpieczeństwa** – to do ich kompetencji należy np. współpraca z organami ścigania i wymiaru sprawiedliwości, a także bieżąca analiza zagrożeń. Podział obowiązków między CSIRT-ami nie jest intuicyjny. Ustawa wskazuje, z którym z nich powinny się kontaktować określone podmioty.

Przykładowe ostrzeżenie opublikowane przez CSIRT KNF



Źródło: CSIRT KNF - Komisja Nadzoru Finansowego

Źródło: Operatorzy Usług Kluczowych - Cyfryzacja KPRM

Jedynym funkcjonującym obecnie CSIRT-em sektorowym jest **CSIRT KNF dedykowany dla sektora finansowego**. Chociaż bezpieczeństwo danych nie jest głównym ani jedynym przedmiotem zainteresowania Komisji Nadzoru Finansowego, podejmuje ona istotne działania w tym zakresie. Prowadzi własny zespół reagowania na incydenty na potrzeby krajowego systemu cyberbezpieczeństwa.

Dla cyberbezpieczeństwa ważny jest również **Urząd Komunikacji Elektronicznej (UKE)**, który pełni m.in. funkcję organu nadzorczego w sektorze telekomunikacyjnym i ma szerokie uprawnienia do monitorowania, czy przedsiębiorcy telekomunikacyjni przestrzegają przepisów prawa. Przedsiębiorcy ci mają obowiązek w ciągu 24 godzin powiadomić Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci czy usług, które w istotny sposób wpływa na ich funkcjonowanie. Warto zauważyć, że procedura zgłaszania tego typu incydentów różni się nieco od procedury przewidzianej w KSC. To jednak jedyny taki wyjątek w polskim porządku prawnym.

NA CZYM OPIERA SIĘ POLSKIE CYBERBEZPIECZEŃSTWO

To zasadniczo implementacja **modelu przyjętego na poziomie Unii Europejskiej**

Stworzenie **warunków do efektywnej wymiany informacji** między kluczowymi podmiotami uznano za niezbędne dla skutecznego zwalczania cyberprzestępczości

Podejście sektorowe oznacza, że nie ma centralnego organu ds. cyberbezpieczeństwa – obowiązki podzielono między istniejącymi organami

Nowelizacja KSC
Kluczowe założenia

NIEKOŃCZĄCE SIĘ prace nad nowelizacją KSC

We wrześniu 2020 r. Minister Cyfryzacji przedstawił projekt nowelizacji KSC. Prace nad nim trwają już prawie dwa lata, a projekt podlegał zasadniczym zmianom. **Wbrew dobrym praktykom i postanowieniom Regulaminu pracy Rady Ministrów nie wszystkie zmiany wprowadzane w ramach prac nad nowelizacją KSC poddano konsultacjom społecznym**. Zmiany proponowane w nowelizacji KSC zdecydowanie wykraczają poza „drobne legislacyjne poprawki" i dotyczą obowiązków uczestników krajowego systemu cyberbezpieczeństwa.

ⓘ Nowelizacja KSC przewiduje m.in.

- wprowadzenie **krajowego systemu certyfikacji cyberbezpieczeństwa** opartego na unijnym rozporządzeniu Cybersecurity Act
- powołanie **sektorowych zespołów CSIRT**, które wspierałyby operatorów usług kluczowych w obsłudze incydentów
- wprowadzenie nowych instrumentów prawnych związanych z **reagowaniem na incydent krytyczny** (ostrzeżenie i postanowienie zabezpieczające)

Prace nad nowelizacją KSC trwają od dłuższego czasu. Kolejne wersje projektu budzą liczne kontrowersje. Co istotne, wątpliwości budzi też zakres i sposób prowadzenia konsultacji społecznych

KONTROWERSYJNA ZMIANA związana z dostawcami wysokiego ryzyka

Jedna z najszerzej dyskutowanych zmian dotyczy wprowadzenia mechanizmu, który pozwala uznać dowolnego dostawcę za dostawcę wysokiego ryzyka, gdy postępowanie wykaże, że stwarza on wysokie zagrożenie dla bezpieczeństwa państwa. W konsekwencji operatorzy usług kluczowych, dostawcy usług cyfrowych, duża część przedsiębiorców telekomunikacyjnych czy jednostki publiczne i samorządowe będą musiały wycofać z użytku produkty, usługi lub procesy ICT wskazane w decyzji. Projekt nowelizacji KSC przewiduje siedmio- lub pięcioletni okres na ich wycofanie. Od dnia opublikowania decyzji nie będzie można też wprowadzać do użytku nowych rozwiązań tego typu. Konsekwencje uznania dostawcy za dostawcę wysokiego ryzyka będą zatem dotykały także szeregu innych podmiotów, a nie tylko samego dostawcy.

Uchwalenie przepisów w proponowanym brzmieniu znacząco zwiększy zakres obowiązków wszystkich podmiotów, o których mowa powyżej. Będą musiały na bieżąco monitorować informacje o wydanych decyzjach i utrzymywać ciągłą gotowość, aby niezwłocznie reagować. Będą musiały modyfikować postępowania zakupowe, monitorować wykorzystywane rozwiązania i być gotowe do zmiany każdego z nich. Tylko samych podmiotów publicznych jest w Polsce kilka tysięcy, więc potencjalne skutki tych zmian będą bardzo istotne.

CO W NOWELIZACJI KSC ZASŁUGUJE NA POCHWAŁĘ

- **Wprowadzenie systemu certyfikacji** – jeśli zostanie podtrzymane występujące w projekcie rozwiązanie, że proces certyfikacji kończy się wydaniem decyzji administracyjnej
- **Możliwość powoływania ISAC oraz SOC** – wszystkie działania, które mają przyśpieszyć wymianę informacji o cyberzagrożeniach i incydentach, to zmiany w dobrym kierunku
- **Dopracowanie nowego projektu pod względem legislacyjnym** w porównaniu z wersją z września 2020 r. – jednak nadal zawiera on szereg istotnych wad merytorycznych, nawet o charakterze konstytucyjnym

Aktualności dotyczące prac nad nowelizacją KSC

7 września 2020 r.

Publikacja pierwszej wersji projektu

Projekt skierowany do uzgodnień i konsultacji publicznych.

15 marca 2022 r.

Publikacja nowej wersji projektu

Opublikowany projekt istotnie różnił się od poprzedniej wersji. Pomimo tego, nie zarządzono ponownych konsultacji publicznych

3 października 2022 r.

Najnowsza, ósma już wersja projektu ustawy

Pomimo zmian w projekcie nie zarządzono konsultacji publicznych. Projekt skierowano do ponownego zaopiniowania przez Komitet ds. Bezpieczeństwa Narodowego i Spraw Obronnych

Mechanizm związany z uznaniem danego dostawcy za dostawcę wysokiego ryzyka może zostać uznany za niezgodny z prawem UE, Konstytucją, a także podstawowymi zasadami postępowania administracyjnego

NOWE PODMIOTY w krajowym systemie cyberbezpieczeństwa

Inne ważne zmiany to propozycje, aby **poszerzyć katalog podmiotów tworzących krajowy system cyberbezpieczeństwa o ISAC (ang.** *Information Sharing and Analysis Center***) oraz SOC (ang.** *Security Operations Center***)**. ISAC, czyli centra analizy i wymiany informacji, są formą partnerstwa publiczno-prywatnego i mają umożliwić szybki przepływ informacji między operatorami usług kluczowych a organami odpowiedzialnymi za cyberbezpieczeństwo. Tworzone są zwykle dla określonych sektorów gospodarki, takich jak energetyka czy finanse. SOC to zespoły pełniące funkcję centrów bezpieczeństwa tworzone przez podmioty prywatne.

Zmiany dotyczą też zespołów reagowania, przewidują bowiem rozbudowanie zadań CSIRT GOV, CSIRT MON i CSIRT NASK, a także wzmocnienie roli sektorowych CSIRT. **Ponadto planuje się dalsze ujednolicenie krajowego systemu cyberbezpieczeństwa i włączenie do niego przedsiębiorców komunikacji elektronicznej**.

Pierwotnie nowelizacja KSC zawierała także zapisy dotyczące spółki Polskie 5G oraz Funduszu celowego na rzecz strategicznej sieci bezpieczeństwa. Choć te postanowienia uważane były za kluczowe w kontekście rozwoju sieci łączności 5G i jako takie były przedstawiane jako jeden z najważniejszych elementów nowelizacji KSC, zostały one usunięte z najnowszej wersji projektu nowelizacji KSC. W tym świetle tym bardziej wydaje się, że nie ma potrzeby, aby procedować nowelizację KSC w pośpiechu i w oderwaniu od wdrożenia NIS 2.

KOLEJNE ZMIANY W PROJEKCIE KSC

Istotnie zmieniona wersja projektu pojawiła się na stronie RCL 25 marca 2022 r.

- **Do krajowego systemu cyberbezpieczeństwa włączono przedsiębiorców komunikacji elektronicznej**, niezależnie od ich wielkości i tego, czy mogą być zakwalifikowani jako operatorzy usług kluczowych lub dostawcy usług cyfrowych.
- **Uprawniono CSIRT-y do przeprowadzenia oceny bezpieczeństwa systemów cyberbezpieczeństwa** wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.
- **Zmodyfikowano nieznacznie** rozwiązania dotyczące (i) uznania danego dostawcy za dostawcę wysokiego ryzyka oraz (ii) wydawania poleceń zabezpieczających w przypadku wystąpienia incydentu krytycznego.
- **Podzielono SOC** na wewnętrzne (utworzone w ramach struktury operatora usługi kluczowej) i zewnętrzne (zewnętrzne podmioty świadczące usługi SOC na rzecz operatora usługi kluczowej).

PODSUMOWANIE

Nowelizacja KSC jest żywo dyskutowana, nie tylko ze względu na jej istotne konsekwencje gospodarcze dla wielu podmiotów. Wątpliwości budzi zgodność z Konstytucją i prawem UE pewnych zawartych w niej mechanizmów prawnych.

JAKIE GŁÓWNE ZMIANY MOŻE WPROWADZIĆ NOWELIZACJA KSC

Szeroko komentowany mechanizm **uznania dowolnego dostawcy za dostawcę wysokiego ryzyka**

Poszerzenie krajowego systemu cyberbezpieczeństwa o ISAC oraz SOC

Wprowadzenie krajowego systemu **certyfikacji cyberbezpieczeństwa**

Poszerzenie krajowego systemu cyberbezpieczeństwa o **przedsiębiorców komunikacji elektronicznej**

NIS 2 Kluczowe założenia

DLACZEGO TERAZ? Przyczyny rozpoczęcia prac nad NIS 2

Cyfryzacja co do zasady pozytywnie wpływa na efektywność i funkcjonowanie przedsiębiorstw. Przeniesienie większości procesów biznesowych do „świata cyfrowego" wiąże się jednak z istotnymi zagrożeniami, które wynikają z błędów, awarii, niedostępności usług, wycieków danych czy rosnącej cyberprzestępczości. Dodatkowo brak wspólnego standardu i sposobu postępowania spowodował praktyczne problemy z jednolitym wdrożeniem wymogów NIS w państwach członkowskich. Pojawiły się wątpliwości, czy założenia i instrumenty przewidziane w tej dyrektywie wystarczą, aby zbudować i utrzymać odpowiedni poziom cyberbezpieczeństwa w całej UE.

W grudniu 2020 r. opublikowano projekt nowej dyrektywy dotyczącej cyberbezpieczeństwa – NIS 2. To element unijnego pakietu na rzecz zapewniania cyberbezpieczeństwa. Po wejściu w życie NIS 2 , co jest planowane na listopad 2022 roku, dyrektywa ta zastąpi obecnie obowiązującą dyrektywę NIS w sprawie bezpieczeństwa sieci i systemów informatycznych.

Państwa członkowskie będą miały prawdopodobnie **21 miesięcy** na implementację przepisów NIS 2 do krajowych porządków prawnych, gdy dyrektywa ta wejdzie w życie. Jednak w naszej ocenie **prace nad implementacją powinny się jednak rozpocząć niezwłocznie po wejściu w życie dyrektywy** ze względu na zakres wprowadzanych zmian.

ⓘ Dyrektywa NIS

Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, nr 2016/1148)

- wdrożona w Polsce w postaci **ustawy o krajowym systemie cyberbezpieczeństwa**
- weszła w życie niecałe **5 lat temu**

Nowe przepisy mają **wyeliminować słabości NIS**, m.in.:

- zbyt duże różnice w implementacji przepisów w poszczególnych państwach członkowskich (np. brak jednolitych kryteriów wyznaczania operatorów usług kluczowych),
- problemy z właściwym nadzorem nad wypełnianiem obowiązków,

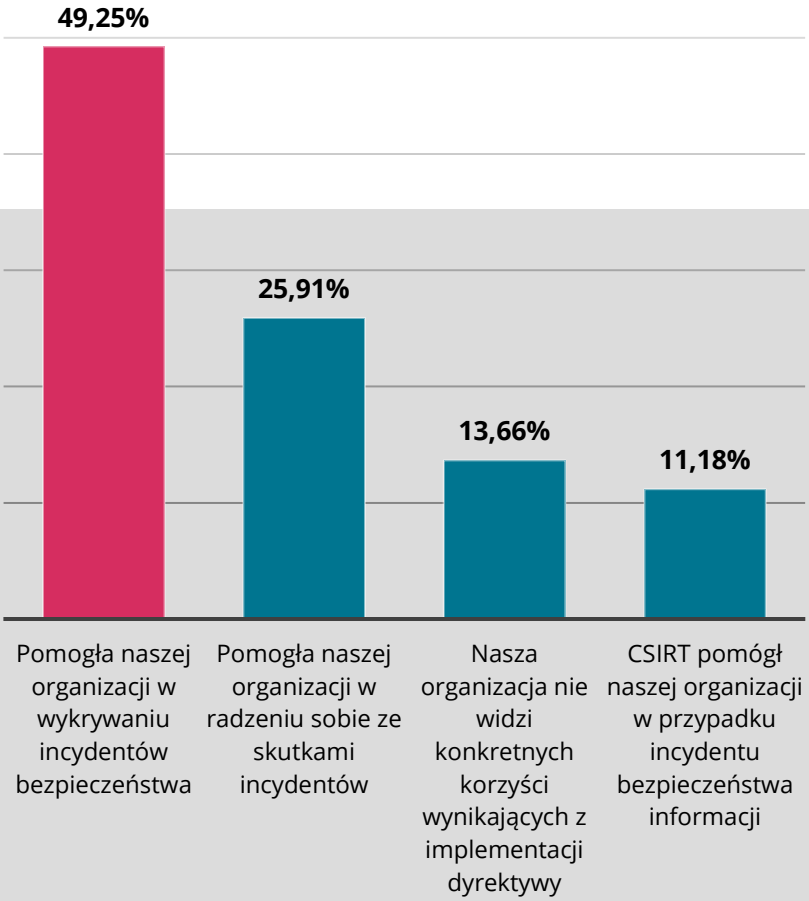
- brak efektywnej wymiany informacji między krajami członkowskimi,
- brak objęcia przepisami wszystkich podmiotów, które mają znaczenie dla systemów cyberbezpieczeństwa – unijny dostawca planuje istotne rozszerzenie podmiotowego zakresu regulacji.

Z uzasadnienia projektu dyrektywy NIS 2 wynika, że jej głównym celem jest doprowadzenie do większej harmonizacji przepisów dotyczących cyberbezpieczeństwa na terenie UE. Ma to zapobiec przyjmowaniu różnych standardów i wymogów przez państwa członkowskie. Uzasadnienie odnosi się też wprost do przyspieszenia transformacji cyfrowej wynikającej z pandemii COVID-19 oraz rosnącej liczby ataków cybernetycznych. Tym samym dyrektywę NIS 2 można postrzegać jako próbę **uaktualnienia i dostosowania wymogów regulacyjnych w zakresie cyberbezpieczeństwa do dynamicznie zmieniającej się rzeczywistości oraz zbudowania zbliżonego standardu w zakresie cyberbepieczeństwa w całej UE**.

KLUCZOWE ZMIANY: Rozszerzenie katalogu podmiotów

Podobnie jak NIS, również NIS 2 nakłada na państwa członkowskie obowiązek przyjęcia krajowej strategii cyberbezpieczeństwa, wyznaczenia właściwych organów krajowych, pojedynczych punktów kontaktowych i zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Jednocześnie **NIS 2 jest zdecydowanie bardziej szczegółowa i m.in. zaostrza wymogi w zakresie bezpieczeństwa dla przedsiębiorców. Wprowadza też bardziej rygorystyczne środki nadzoru ze strony organów na poziomie poszczególnych państw**.

Co istotne, NIS 2 w projektowanym brzmieniu **odchodzi od podziału podmiotów podlegających dyrektywnie na operatorów usług kluczowych i dostawców usług kluczowych**. W miejsce tego podziału, zakładając podobne wymagania względem wszystkich podmiotów, które prowadzą działalność określoną w załącznikach do dyrektywy, klasyfikujących się jako podmioty **niezbędne** (*essential entities*) lub istotne (*important entities*) i czyniąc



Ocena wpływu implementacji dyrektywy NIS

Głównym
celem NIS 2 jest
doprowadzenie do
większej harmonizacji
przepisów
dotyczących
cyberbezpieczeństwa
na terenie UE.
Ma to zapobiec
przyjmowaniu
różnych standardów
i wymogów przez państwa
członkowskie

wyjątek jedynie dla małych i mikro- przedsiębiorców (wyjątek ten jednak nie dotyczy wszystkich przypadków). Określenie wprost w załącznikach do dyrektywy, które podmioty jej podlegają, ma zapewnić jednolitą implementację przepisów dyrektywy w państwach członkowskich. Jak się wydaje, organy unijne wyciągnęły lekcję z pozostawienia w tym zakresie większej swobody ustawodawcom krajowym na etapie projektowania przepisów NIS, co doprowadziło do znacznego zróżnicowania choćby w zakresie wyznaczenia operatorów usług kluczowych.

Największą zmianą jest niewątpliwie **istotne rozszerzenie kategorii podmiotów objętych zakresem dyrektywy**. Za podmioty niezbędne dla zapewnienia cyberbezpieczeństwa (odpowiednik operatorów usług kluczowych w NIS) oprócz podmiotów z sektora energetycznego, transportowego, bankowego, finansowego, czy zdrowotnego uznano m.in.:

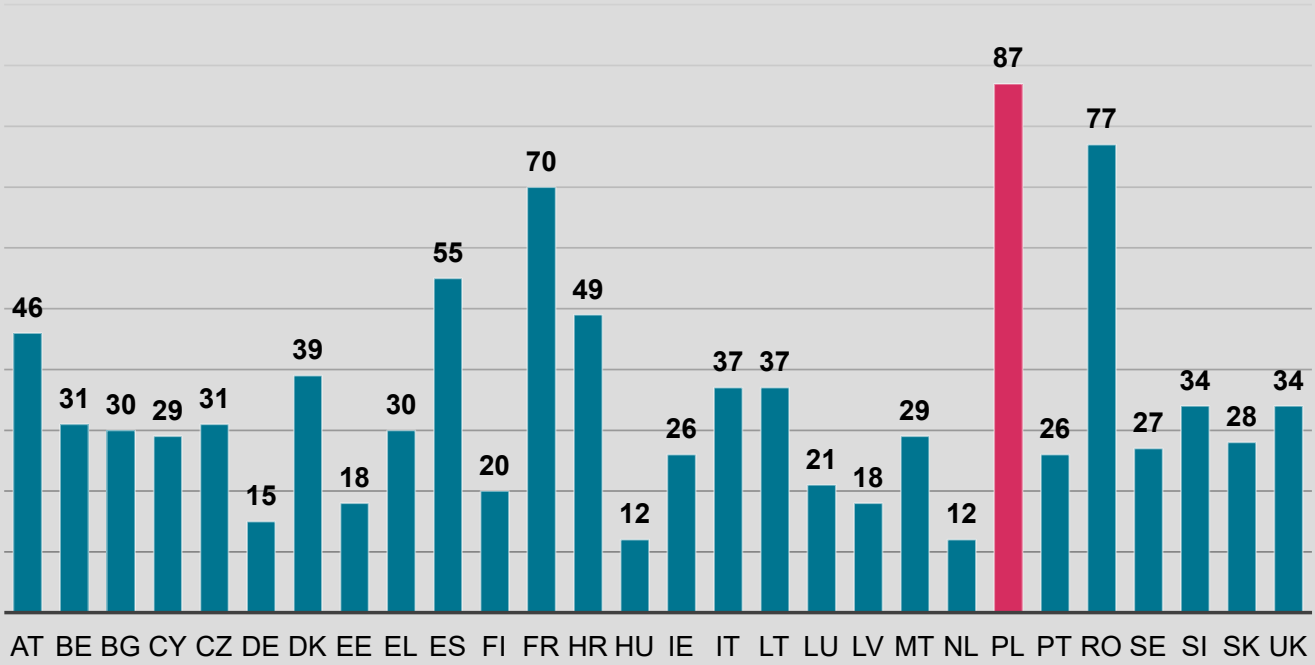
- dostawców usług przetwarzania w chmurze obliczeniowej (cloud computing service providers);
- dostawców usług centrów danych (data centre service providers);
- dostawców usług CDN (content delivery network providers);
- dostawców usług zaufania;
- dostawców publicznych sieci łączności elektronicznej oraz usług łączności elektronicznej;
- jednostki centralnej administracji rządowej.

Dodatkowo poszerzono krąg adresatów regulacji – dodano kategorię podmiotów istotnych (a więc podmiotów, których usługi są postrzegane jako mniej krytyczne z punktu widzenia cyberbezpieczeństwa), m.in.:

- operatorów usług pocztowych i dostawców usług kurierskich,
- podmioty zajmujące się produkcją, przetwarzaniem lub dystrybucją żywności,
- podmioty produkujące komputery, wyroby elektroniczne czy urządzenia elektryczne;
- dostawców wyszukiwarek internetowych i internetowych platform handlowych (w NIS przypisanych do kategorii dostawców usług cyfrowych).

Tym samym NIS 2 stanie się regulacją o bardzo szerokim zakresie zastosowania, nakładającą specyficzne obowiązki na szeroki krąg podmiotów.

Ogólna liczba usług kluczowych zidentyfikowanych przez państwa członkowskie



Źródło: Sprawozdanie Komisji Parlamentu Europejskiego i Rady oceniające spójność podejść przyjętych przez Państwa członkowskie w procesie identyfikacji operatorów usług kluczowych zgodnie z art. 23 ust. 1 dyrektywy (UE) 2016/1148 w sprawie bezpieczeństwa sieci i informacji

Jak się wydaje, organy unijne wyciągnęły lekcję z pozostawienia większej swobody ustawodawcom krajowym na etapie projektowania przepisów NIS, co doprowadziło do znacznego zróżnicowania – choćby w wyznaczaniu operatorów usług kluczowych

Poglądowe przykłady podejść wybranych przez państwa członkowskie w ramach identyfikacji usług kluczowych w podsektorze transportu kolejowego

FINLANDIA	FRANCJA	IRLANDIA	POLSKA
Zarządzanie infrastrukturą państwową	Utrzymanie infrastruktury	Zarządcy infrastruktury	(luki w zakresie spójności)
(luki w zakresie spójności)	Utrzymanie taboru kolejowego	(luki w zakresie spójności)	(luki w zakresie spójności)
Usługi zarządzania ruchem	Kontrola ruchu kolejowego i zarządzanie ruchem kolejowym	(luki w zakresie spójności)	Przygotowywanie rozkładów jazdy pociągów
(luki w zakresie spójności)	Przewóz towarów i materiałów niebezpiecznych	Przedsiębiorstwa kolejowe	Transport kolejowy towarów
(luki w zakresie spójności)	Przewóz pasażerów		Transport kolejowy pasażerów
(luki w zakresie spójności)	Metro, tramwaje i inne przewozy lekkimi pojazdami szynowymi (w tym koleje podziemne)		(luki w zakresie spójności)
(luki w zakresie spójności)	Przewozy kolejowe	(luki w zakresie spójności)	(luki w zakresie spójności)

Źródło: Sprawozdanie Komisji Parlamentu Europejskiego i Rady oceniające spójność podejść przyjętych przez Państwa członkowskie w procesie identyfikacji operatorów usług kluczowych zgodnie z art. 23 ust. 1 dyrektywy (UE) 2016/1148 w sprawie bezpieczeństwa sieci i informacji

KRYTERIUM KWALIFIKACJI: Wielkość podmiotu

Projekt NIS 2 wprowadza również jasne kryterium kwalifikacji związane z wielkością danego podmiotu (*size cup*). **Wszystkie średnie i duże przedsiębiorstwa będą podlegać nowym przepisom, o ile ich działalność może zostać przypisania do jednej z ww. kategorii.** Mikro- i małe przedsiębiorstwa w rozumieniu zalecenia Komisji 2003/361/WE będą wyłączone z zakresu dyrektywy, z wyjątkiem sytuacji, gdy:

- świadczą usługi określonego rodzaju (np. usługi zaufania czy usługi łączności elektronicznej);
- posiadają szczególny status (np. są podmiotami publicznymi lub jedynymi dostawcami usług określonego rodzaju w danym państwie członkowskim);
- zakłócenia w działaniu usług świadczonych przez te podmioty mogłyby mieć istotny skutek np. dla bezpieczeństwa publicznego czy zdrowia publicznego.

W takich przypadkach obowiązki wynikające z dyrektywy NIS 2 będą miały zastosowanie nawet do nich, o ile mogą zostać zakwalifikowane jako podmioty niezbędne lub istotne.

Sektory objęte NIS 2

Źródło: Agreement reached on new EU Network Information Security Directive

OBOWIĄZKI PODMIOTÓW niezbędnych i istotnych

Istotną zmianą względem aktualnych regulacji jest to, że **NIS 2 ustanawia podobne obowiązki dla wszystkich objętych nią podmiotów niezależnie od tego, czy są przypisane do kategorii podmiotów niezbędnych, czy do istotnych**. Podstawowym obowiązkiem pozostaje podjęcie odpowiednich i proporcjonalnych środków operacyjnych, technicznych i organizacyjnych, aby zarządzać ryzykami, na jakie są narażone sieci i systemy informatyczne, które te podmioty wykorzystują do świadczenia usług. Zgodnie z dotychczasowym podejściem środki powinny być dobrane adekwatnie do poziomu ryzyka wystąpienia incydentu bezpieczeństwa (risk basek approach). NIS 2 doprecyzowuje minimalne wymogi w tym zakresie, do których należą:

- prowadzenie analizy ryzyka;
- zapewnienie bieżącej obsługi incydentów;
- opracowanie planu ciągłości działania;
- opracowanie odpowiednich polityk i procedur w zakresie testowania i przeprowadzania audytów zabezpieczeń;
- korzystanie z kryptografii i szyfrowania.

Katalog środków, o których mowa powyżej, powinien zostać określony w sposób odpowiedni i przede wszystkim **proporcjonalny do poziomu ryzyka**. NIS 2 kładzie na tę zasadę szczególny nacisk i wskazuje, że państwa członkowskie powinny wziąć pod uwagę takie czynniki jak poziom ekspozycji na ryzyko, wielkość danego podmiotu czy prawdopodobieństwo wystąpienia incydentu. Co więcej, NIS 2 wskazuje konieczność uwzględnienia obowiązujących standardów i – czego nie sposób pominąć – kosztów ich potencjalnego wdrożenia (art. 18 NIS 2).

Zgodnie z NIS 2 państwa członkowskie powinny kierować się zasadą proporcjonalności. Zapewnienie wysokiego poziomu bezpieczeństwa jest oczywiście kluczowe, ale trzeba też wziąć pod uwagę ewentualne nadmierne koszty wdrożenia nowych obowiązków. Środki powinny być adekwatne i odpowiadające poziomowi ryzyka

To samo zostało podkreślone w odniesieniu do środków związanych z zachowaniem **bezpieczeństwa łańcucha dostaw** (w zakresie produktów i usług ICT). Przy określaniu „odpowiednich" wymogów w tym zakresie państwa członkowskie powinny kierować się szeregiem czynników, przede wszystkim o charakterze technicznym (overall quality of products and cybersecurity practices of suppliers and service providers). Dodatkowo mają obowiązek uwzględnić wyniki skoordynowanej oceny ryzyka krytycznych łańcuchów dostaw przeprowadzanej na poziomie UE, o której mowa w art. 19 NIS 2 (koordynacja w tym zakresie to zupełnie nowy element wprowadzany przez NIS 2).

Tego rodzaju ocenę przeprowadzać będą przedstawiciele państw członkowskich, we współdziałaniu z Komisją Europejską i ENISA m.in. w odniesieniu do krytycznych usług i produktów ICT oraz – co szczególnie istotne – na podstawie technicznych czynników ryzyka. Celem jest budowanie spójnego podejścia na poziomie poszczególnych państw członkowskich, tym razem w zakresie dostawców ICT oraz oceny ryzyka związanego z korzystaniem z ich usług i produktów.

Wyeksponowano rolę i **odpowiedzialność osób zarządzających** (management bodies), które mają być bezpośrednio odpowiedzialne za nadzór i aktywne zarządzanie ryzykiem w zakresie cyberbezpieczeństwa. NIS 2 wprost wskazuje na możliwość pociągnięcia osób zarządzających do odpowiedzialności za brak wypełnienia obowiązków w tym zakresie. Jak się wydaje, ma to zwiększyć „efektywność" egzekwowania

> NIS 2 ma istotnie szerszy zakres podmiotowy niż NIS – obejmie m.in. administrację publiczną, sektor żywności, ścieki, przemysł, zarzadzanie odpadami i przestrzeń kosmiczną.

PROCEDURA RAPORTOWANIA INCYDENTÓW BEZPIECZEŃSTWA

- **Wstępne zgłoszenie incydentu** w ciągu 24 godzin. Właściwy organ lub CSIRT powinien odpowiedzieć na nie również w ciągu 24 godzin, wskazując wstępną ocenę incydentu.
- **Przedstawienie informacji o statusie incydentu** na żądanie CSIRT lub właściwego organu.
- **Przedstawienie szczegółowego raportu** w ciągu miesiąca od zgłoszenia incydentu. Raport powinien zawierać co najmniej opis incydentu, jego przyczynę i środki powzięte w celu złagodzenia jego skutków.

Zgodnie z NIS 2 ocena ryzyka m.in. usług i produktów ICT wykonywana będzie na szczeblu UE i przy udziale przedstawicieli poszczególnych państw członkowskich. Takie rozwiązanie pozwala na koordynację działań oraz – co szczególnie istotne – budowanie jednolitych standardów w zakresie cyberbezpieczeństwa w całej UE

obowiązków związanych z cyberbezpieczeństwem. Projektowane przepisy wprost odnoszą się również do **obowiązkowych szkoleń i podnoszenia świadomości w zakresie zarządzania ryzykiem w obszarze cyberbezpieczeństwa**.

RAPORTOWANIE incydentów bezpieczeństwa

Zmiany dotyczą również zasad raportowania incydentów bezpieczeństwa. Obowiązek ten istniał już wcześniej, ale w projekcie NIS 2 został szczegółowo doprecyzowany (zarówno od strony proceduralnej, jak i od strony skutków niedochowania obowiązków w tym zakresie). Obowiązek raportowania do CSIRT lub innego kompetentnego organu będą miały wszystkie podmioty niezbędne i istotne. Dotyczy to nie tylko informacji o incydentach bezpieczeństwa, które mają wpływ na świadczenie usług przez te podmioty, ale również informacji o wszystkich zidentyfikowanych zagrożeniach, które mogą doprowadzić do wystąpienia istotnego incydentu bezpieczeństwa.

ŚRODKI nadzorcze I KARY administracyjne

Brak zastosowania się do nowych obowiązków może mieć istotne konsekwencje dla podmiotów niezbędnych i podmiotów istotnych, z karami administracyjnymi włącznie. Planowana wysokość kar wydaje się istotnym „czynnikiem mobilizującym". Zgodnie z NIS 2 właściwe organy państw członkowskich mają mieć możliwość nałożenia administracyjnych kar pieniężnych, których wartość nie może przekroczyć **10 mln euro** lub kwoty stanowiącej wartość **2% rocznego obrotu danego podmiotu (zależnie od tego, która suma jest wyższa)**. To jakościowa zmiana w stosunku do dyrektywy NIS.

Projekt NIS 2, choć kierunkowo zgodny z założeniami NIS, stanowi istotną zmianę jakościową. Przede wszystkim jest dużo bardziej szczegółowy, aby budować jednolity standard cyberbezpieczeństwa w całej UE

NIS 2 istotnie zmieni regulacyjny krajobraz cyberbezpieczeństwa. Kluczowe jest, aby w pracach nad jej implementacją uniknąć pośpiechu. Istotnym elementem będzie też przeprowadzenie szerokich konsultacji społecznych

NIS 2 szczegółowo odnosi się również do środków nadzorczych, które państwa członkowskie będą miały obowiązek wdrożyć, aby budować efektywność zarządzania cyberbezpieczeństwem. Środki te obejmują m.in.:

- możliwość kierowania ostrzeżeń, wiążących instrukcji i poleceń;
- nałożenie obowiązku poinformowania osób zagrożonych wystąpieniem incydentu bezpieczeństwa o związanym z tym ryzyku;
- zobowiązanie danego podmiotu, aby podał do publicznej wiadomości informację o niedopełnieniu obowiązków przewidzianych dyrektywą.

W przypadku podmiotów niezbędnych, jeśli zastosowane środki nie doprowadzą do przestrzegania obowiązków przez dany podmiot, właściwy organ krajowy może dodatkowo:

- cofnąć lub zawiesić zezwolenie na prowadzenie określonego rodzaju działalności – co może mieć szczególne znaczenie dla podmiotów działających na rynkach regulowanych, np. dla branży finansowej, telekomunikacyjnej czy energetycznej;
- zakazać sprawowania funkcji kierowniczych w danym podmiocie osobie odpowiedzialnej za naruszenie obowiązków wynikających z dyrektywy.

Z tej perspektywy niewątpliwie kluczowym etapem będzie implementacja przepisów do krajowych porządków prawnych. Pośpiech lub próba budowania wyłącznie „literalnej" zgodności z wymogami może wypaczać ich sens i utrudniać osiągniecie założonych celów. Dodatkowo obowiązkami objęto znacznie szerszy krąg podmiotów, w tym (w określonych sytuacjach) mikro- i małe przedsiębiorstwa. To kolejny argument za tym, aby prac nad implementacją nie zostawiać na ostatnią chwilę.

DLACZEGO NA NIS 2 WARTO ZWRÓCIĆ UWAGĘ JUŻ TERAZ?

NIS 2 istotnie rozszerza krąg podmiotów włączonych w system cyberbezpieczeństwa. Wymogi dotyczyć będą m.in. operatorów usług pocztowych, dostawców usług kurierskich czy podmiotów zajmujących się produkcją, przetwarzaniem lub dystrybucją żywności.

NIS 2 odchodzi od zasadniczego podziału na operatorów usług kluczowych (OES) oraz dostawców usług cyfrowych (DSP). Jednolite wymogi dotyczyć będą wszystkich podmiotów prowadzących działalność określoną w załączniku do dyrektywy (podmiotów niezbędnych lub istotnych).

NIS 2 przewiduje istotne kary finansowe. Kara za naruszenie podstawowych obowiązków wynikających z Dyrektywy w wysokości do 10.000.000 EUR lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa. To niewątpliwie kluczowa zmiana względem obecnego poziomu kar.

NIS 2 opiera się na tzw. *risk basek approach*. W praktyce oznacza, to, że efektywne wdrożenie wymogów dyrektywy wymagać będzie przeprowadzenia analizy ryzyka i zarządzania ryzykiem cyberbezpieczeństwa, a nie tylko przyjęcia procedur „do szuflady".

Szacuje się, że firmy objęte NIS 2 będą musiały zwiększyć wydatki na obszar cyberbezpieczeństwa maks. o 22%. Firmy już objęte NIS poniosą wydatki większe o 12%. Wydatki te powinny się jednak zwrócić ze względu na niższe koszty związane z incydentami*

11,3 mld €

to szacowane obniżenie kosztów incydentów cybernetycznych dzięki NIS 2*

* Źródło: „Agreement reached on new EU Network Information Security (NIS) Directive"

NIS 2 A NOWELIZACJA KSC

Spójne czy rozbieżne cele i koncepcje?

RÓWNOLEGŁE PRACE nad dwoma ważnymi aktami

Obecnie procedowane są dwa akty prawne, które będą miały doniosłe znaczenie dla polskich regulacji w zakresie cyberbezpieczeństwa:

- na poziomie krajowym – nowelizacja KSC, której przewidywana data uchwalenia nie jest znana,
- na poziomie unijnym – dyrektywa NIS 2, która jest już na końcowym etapie procesu legislacyjnego i może zostać uchwalona nawet na przełomie października i listopada br.

Postanowienia NIS 2 trzeba będzie wdrożyć do krajowego porządku prawnego w ciągu 21 miesięcy po jej uchwaleniu. Prawdopodobnie zatem **dwa rozbudowane projekty nowelizujące ustawę o KSC będą procedowane równolegle lub zostaną uchwalone w niedługim odstępie czasowym**. Warto zastanowić się, na ile te dwa akty prawne są ze sobą spójne.

NIESPÓJNOŚCI i ich konsekwencje dla podmiotów na rynku

Jednym z pierwszych elementów, które zwracają uwagę, jest niejednolita siatka pojęciowa. Nowelizacja KSC wprowadza na przykład nowe definicje incydentów, jeszcze bardziej je różnicując, a NIS 2 idzie raczej w przeciwnym kierunku. **Wskazane jest zapewnienie jednolitej terminologii, co w praktyce najłatwiej osiągnąć przez połączenie nowelizacji KSC z projektem ustawy wdrażającej NIS 2**. Dzięki temu już na etapie legislacyjnym będzie można wyeliminować wszystkie niespójności.

> Nowelizacja KSC nie odnosi się w żaden sposób do wielu rozwiązań projektowanych w NIS 2. Przepisy trzeba będzie ponownie zmienić w związku z implementacją tej dyrektywy.

Inna siatka pojęciowa przekłada się na inny zakres podmiotowy nowelizacji KSC oraz NIS 2. Aby uprościć system, NIS 2 wyróżnia wyłącznie dwie kategorie podmiotów (podmioty niezbędne oraz istotne) i przewidzianych dla nich obowiązków. Nowelizacja KSC różnicuje obowiązki dużo bardziej szczegółowo. To

Dwa rozbudowane projekty nowelizujące ustawę o KSC będą procedowane równolegle lub zostaną uchwalone w niedługim odstępie czasowym. Przepisy KSC trzeba będzie ponownie zmienić w związku z implementacją NIS 2

Najważniejsze różnice między nowelizacją KSC a NIS 2

NA CZYM POLEGA RÓŻNICA?	KOMENTARZ	POTENCJALNY SKUTEK
Brak spójności w wymogach wobec CSiRT	Nowelizacja KSC nie odnosi się do obowiązku utworzenia sieci krajowych CSIRT-ów, który wynika z projektowanego art. 13 NIS 2	Niepotrzebne osłabienie krajowego systemu cyberbezpieczeństwa i uczynienie go nie w pełni kompatybilnym z systemami innych krajów UE
Brak uwzględnienia skoordynowanego podejścia przy wykluczeniu niektórych dostawców	Procedura oceny dostawcy wysokiego ryzyka w nowelizacji KSC nie zawiera odwołań do możliwości zastosowania unijnego, skoordynowanego podejścia, a także nie uwzględnia obowiązku stosowania wyłącznie odpowiednich i proporcjonalnych środków wynikającego z projektowanego art. 18 NIS 2	Dodatkowe ryzyka dla Polski związane z błędną lub niepełną oceną dostawcy oraz niekompatybilność z systemami innych krajów UE
Brak pełnego wdrożenia certyfikacji i standaryzacji	Nowelizacja KSC wprowadza własny reżim certyfikacji i standaryzacji, nie odnosząc się do europejskiego systemu certyfikacji, który na podstawie projektowanego art. 21 NIS 2 obejmie prawdopodobnie wiele sektorów	Dodatkowe ryzyka dla Polski związane z błędną lub niepełną oceną dostawcy oraz niekompatybilność z systemami innych krajów UE
Niekompatybilność systemu egzekwowania obowiązków	Nowelizacja KSC nie wdraża systemu kar przewidzianych w NIS 2 za nieprzestrzeganie obowiązków cyberbezpieczeństwa, m.in. w zakresie kar okresowych wynikających z projektowanego art. 31 ust. 5 NIS 2	System egzekwowania obowiązków niewystarczający, aby zapewnić przestrzeganie zasad cyberbezpieczeństwa
Brak spójnych zasad ustalania jurysdykcji	Nowelizacja KSC nie zawiera szczegółowych zasad spójnych m.in. z projektowanym art. 24 NIS 2 w zakresie określania jurysdykcji podmiotów podlegających pod system cyberbezpieczeństwa	Podmioty mogą twierdzić, że nie podlegają pod KSC, ponieważ nie da się zastosować do nich zasad określania jurysdykcji

Źródło: opracowanie własne

sprawia, że niektóre podmioty będą częścią krajowego systemu cyberbezpieczeństwa w rozumieniu NIS 2, ale już nie nowelizacji KSC. Chodzi m.in. o operatorów usług pocztowych, dostawców usług kurierskich czy podmiotów zajmujących się produkcją żywności. Już teraz można by zastanowić się nad tymi problemami i stworzyć rozwiązania systemowe, szczególnie że będą one dotyczyły nawet niektórych małych i mikroprzedsiębiorców.

Analizy i namysłu wart jest również **sposób informowania o incydentach**. To jedna z najważniejszych kwestii w całym reżimie KSC. Nowelizacja KSC w obecnym brzmieniu zmieni przepisy w tym obszarze w całkowitym oderwaniu od założeń dyrektywy NIS 2.

Nowelizacja KSC nie odnosi się zatem w żaden sposób do wielu rozwiązań projektowanych w NIS 2. Co prawda dyrektywa wciąż nie weszła w życie. Jednak trudno sobie wyobrazić, aby w oderwaniu od tych rozwiązań stworzyć dobre i stabilne przepisy. Jest to legislacyjny Mount Everest – osiągalny, ale warto mierzyć siły na zamiary.

Nowelizacja KSC i NIS 2 Z SZERSZEJ PERSPEKTYWY

Nowelizacja KSC nie implementuje unijnych przepisów, jest „krajową" inicjatywą zmiany KSC. Doprowadzi jednak do zmiany ustawy opartej na prawie unijnym. **Zmiana ta będzie polegać na wprowadzeniu treści sformułowanych wyłącznie przez polskiego ustawodawcę – w przeddzień uchwalenia dyrektywy NIS 2, którą Polska będzie zobowiązana wdrożyć w ciągu 21 miesięcy**. Co więcej, mowa o dyrektywie, której głównym celem jest harmonizowanie przepisów na poziomie państw członkowskich UE.

Wydaje się, że taki tryb procedowania prowadzi do chaosu legislacyjnego, którego można łatwo uniknąć, łącząc nowelizację KSC z implementacją NIS 2. **Uchwalona zostałaby jedna ustawa wdrażająca przepisy unijne i przepisy zaproponowane na poziomie krajowym**. W takim scenariuszu łatwiej uniknąć potencjalnych niezgodności między obecnym brzmieniem nowelizacji KSC i proponowanym brzmieniem NIS 2. Uczestnicy rynku musieliby podjąć się tylko jednego wdrożenia, zamiast wdrażać dwa różne (częściowo niezgodne) akty prawne w krótkim odstępie czasu.

Zasadność rezygnacji z uchwalania odrębnych ustaw dotyczących cyberbezpieczeństwa w przeddzień wejścia w życie dyrektywy NIS 2 jest widoczna na przykładzie innych państw członkowskich UE. Przykładowo w Czechach*, gdzie procedowano podobną ustawę do nowelizacji KSC, w której planowano wprowadzenie mechanizmu uznawania dostawców za dostawców wysokiego ryzyka, zrezygnowano z uchwalenia odrębnej ustawy w tym zakresie i skupiono się na przygotowaniach do wdrożenia NIS 2.

Alternatywą dla tego – w naszej ocenie najprostszego – rozwiązania jest procedowanie dwóch dużych nowelizacji KSC. Prawdopodobnie równoległe. To oczywiście możliwe, choć dużo bardziej skomplikowane dla uczestników krajowego systemu cyberbezpieczeństwa. **Ze względu na niespójności między nowelizacją KSC a przyszłą ustawą wdrażającą NIS 2, które są niemożliwe do uniknięcia przy takim trybie procedowania, zainteresowane podmioty będą musiały włożyć więcej wysiłku w zapewnienie zgodności regulacyjnej**. Co więcej, ich otoczenie prawne może ulegać dynamicznym zmianom, co na pewno nie jest pożądane w tak wrażliwym temacie jak cyberbezpieczeństwo.

NA CZYM POLEGA PROBLEM I JAK GO ROZWIĄZAĆ?

Rozbieżności między nowelizacją KSC i NIS 2 budzą wiele wątpliwości praktycznych

Nowelizacja KSC nie odnosi się do wielu rozwiązań projektowanych w NIS 2, więc będziemy musieli poradzić sobie z „podwójną" zmianą przepisów

Rozwiązaniem większości problemów mogłoby być **połączenie nowelizacji KSC z projektem wdrażającym NIS 2**

* https://osveta.nukib.cz/course/view.php?id=145

Przyjęcie nowelizacji KSC w obecnym kształcie oznacza m.in. wprowadzenie postępowania w zakresie dostawców wysokiego ryzyka, które jest specyficzne na tle innych państw członkowskich. Taka zmiana dziwi wobec zbliżającej się konieczności implementacji NIS 2

PODSUMOWANIE
Nowelizacja KSC czy implementacja NIS 2?

Dyskusje nad potrzebą nowelizacji KSC trwają już długo, a od publikacji projektu ustawy minęły dwa lata. Nie było jeszcze wtedy projektu NIS 2, ale przy kolejnych wersjach ustawy jego treść była już dobrze znana (choć trzeba przyznać, że także ulegała zmianom). Mimo to oba projekty różnią się istotnie w zakresie pojęć, obowiązków i ogólnego podejścia do zarządzania cyberbezpieczeństwem. To nie zarzut, a stwierdzenie faktu (niezależnie od merytorycznych i proceduralnych uwag do nowelizacji KSC).

ⓘ Kiedy to się skończy?

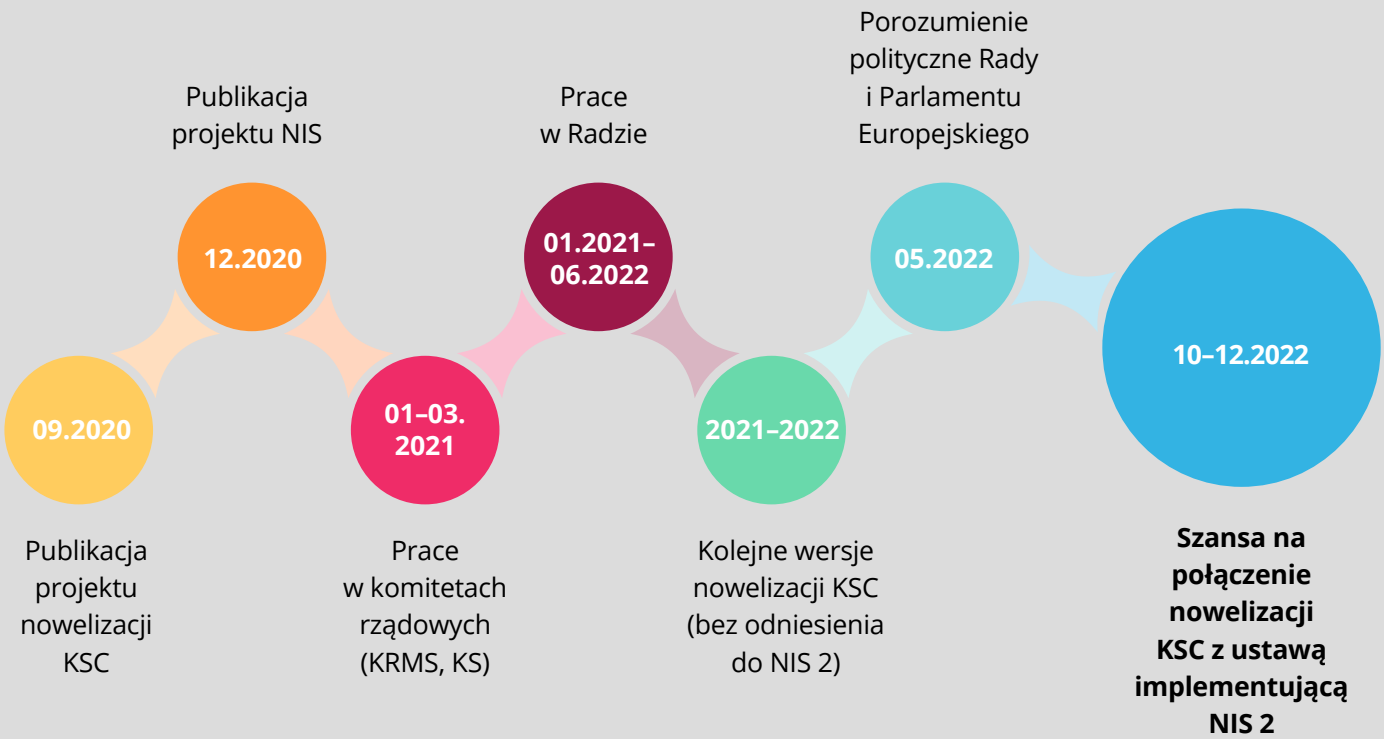
Czas przewidziany na wdrożenie NIS 2 do polskiego porządku prawnego to 21 miesięcy. Tymczasem prace nad nowelizacją KSC jeszcze się nie zakończyły, a trwają już ponad dwa lata. Przyjąć należy zatem, że wdrożenie NIS 2 również potrwa **co najmniej dwa lata**.

Najbardziej aktualna wersja nowelizacji KSC to już ósma propozycja, ale nadal nie mamy pewności, że będzie ostatnią. Projekt ten wywołuje ożywione dyskusje, zwłaszcza z uwagi na procedurę dotyczącą uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka i związane z tym skutki dla tysięcy podmiotów działających na rynku. Część wątpliwości ma charakter zasadniczy i dotyczy np. podstawowych reguł postępowania administracyjnego, zgodności z Konstytucją oraz prawem UE. **Równolegle perspektywa przyjęcia ostatecznej, obowiązującej wersji NIS 2 staje się coraz mniej odległa. Tym samym zbliża się również początek 21-miesięcznego okresu na implementację jej przepisów**.

W tym kontekście warto zatrzymać się na chwilę i zastanowić, czy kontynuowanie prac nad nowelizacją KSC w obecnym kształcie ma jeszcze sens. Czy nie warto jednak „przerzucić" wszystkich sił, aby przygotować się do implementacji NIS 2 i połączyć w jednym akcie wybrane, spójne z NIS 2 postanowienia nowelizacji KSC z przepisami wprost wdrażającymi tę dyrektywę. W naszej ocenie taki alternatywny scenariusz postępowania jest co najmniej wart rozważenia.

> NIS 2 istotnie zmieni regulacyjny krajobraz cyberbezpieczeństwa w UE. Warto już dziś zastanowić się nad optymalnym wdrożeniem jej przepisów.

Kalendarz prac nad projektami nowelizacji KSC i NIS 2



Dwa rozbudowane projekty nowelizujące ustawę o KSC będą procedowane równolegle lub zostaną uchwalone w niedługim odstępie czasowym. Przepisy KSC trzeba będzie ponownie zmienić w związku z implementacją NIS 2

Warto zastanowić się, czy kontynuowanie prac nad nowelizacją KSC w obecnym kształcie ma sens. Może lepiej połączyć w jednym akcie wybrane postanowienia nowelizacji KSC i wdrożenie NIS 2

RAPORT KANCELARII MARUTA WACHTA SPORZĄDZONY W RAMACH CALPE

CALPE

CENTRUM ANALIZ LEGISLACYJNYCH
I POLITYKI EKONOMICZNEJ

MARUTA