

Dyrektywa CER – unijne wzmocnienie ochrony infrastruktury krytycznej

14 grudnia 2022 roku w Unii Europejskiej wraz z dyrektywą NIS 2 (w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii) przyjęta została dyrektywa NIS 2 (w sprawie odporności podmiotów krytycznych). Ma ona na celu zwiększenie odporności podmiotów o krytycznym znaczeniu, które świadczą usługi niezbędne dla podstawowych funkcji społecznych lub działalności gospodarczej na rynku wewnętrznym. W niniejszym opracowaniu przedstawione zostaną jej główne założenia.

Wprowadzenie

Podmioty krytyczne, jako dostawcy usług kluczowych, odgrywają nieodzowną rolę w utrzymaniu niezbędnych funkcji społecznych oraz działalności gospodarczej nie tylko w poszczególnych państwach, ale i w całej Unii Europejskiej.

Pierwsze uregulowania prawne kwestii ochrony infrastruktury krytycznej (IK) zawarte zostały w Dyrektywie Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. Koncentrowała się ona na sektorach energii i transportu.

Po ponad jedenastu latach obowiązywania dyrektywy dokonano jej oceny. W 2019 roku zauważono, że wprowadzone środki ochronne, związane wyłącznie z pojedynczymi składnikami infrastruktury, są niewystarczające, aby zapobiec wszystkim zakłóceniom.

Powody rewizji przepisów dotyczących ochrony infrastruktury krytycznej



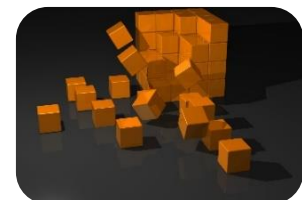
wzajemne powiązania sektorów wynikające z globalizacji i cyfryzacji



nowe zagrożenia i napięcia międzynarodowe



zwiększona częstotliwość występowania gwałtownych zjawisk pogodowych



fragmentacja rynku wewnętrznego w zakresie identyfikacji podmiotów krytycznych

Dyrektywa CER – timeline

Na podstawie przeprowadzonej w 2019 roku oceny dyrektywy 2008/114/WE, 16 grudnia 2020 roku Komisja Europejska przedstawiła nowy projekt aktu regulującego kwestie odporności podmiotów krytycznych. Wraz z nią zaprezentowano również wniosek dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE (NIS 2). Oba akty prawne wzajemnie się uzupełniają. Ich głównym celem jest wzmocnienie odporności UE na wszelkiego rodzaju zagrożenia, zarówno w wymiarze fizycznym, jak i cyfrowym.

Ostatecznie dyrektywa CER została zaakceptowana 14 grudnia 2022 roku i wraz z NIS 2 weszła w życie 16 stycznia 2023 roku. Państwa członkowskie zostały zobowiązane do transpozycji wymagań unijnych do prawa krajowego do 17 października 2024 roku.

Przedmiot i zakres stosowania

Dyrektywa CER reguluje przede wszystkim obowiązki państw członkowskich, do których należy przyjmowanie środków mających na celu zapewnienie niezakłóconego świadczenia usług kluczowych dla utrzymania niezbędnych funkcji społecznych lub niezbędnej działalności gospodarczej. W szczególności jest to identyfikowanie podmiotów krytycznych oraz wspieranie ich w wypełnianiu zadań. Oprócz tego CER wprowadza obowiązki dla podmiotów krytycznych, które służyć mają zwiększeniu ich odporności i zdolności do świadczenia usług.

W dokumencie znalazły się również uregulowania dotyczące nadzoru nad podmiotami krytycznymi i egzekwowania przepisów, a także środki mające na celu osiągnięcie wysokiego poziomu odporności tego rodzaju podmiotów. Dyrektywa obejmuje także przepisy w zakresie identyfikacji infrastruktury o szczególnym znaczeniu europejskim oraz misji doradczych. Reguluje również procedury dotyczące współpracy i sprawozdawczości.

Ponadto, w dokumencie przewidziano szereg wyłączeń stosowania dyrektywy.

- Przede wszystkim, nie stosuje się jej do kwestii objętych dyrektywą (UE) 2022/2555 (NIS 2). Z uwagi na powiązanie między fizycznym bezpieczeństwem a cyberbezpieczeństwem podmiotów krytycznych te dwie dyrektywy powinny być wdrażane w sposób skoordynowany i wykluczający wzajemne nakładanie się obowiązków na poszczególne podmioty.
- Z obowiązków określonych w CER zwolnione zostały podmioty z trzech sektorów: bankowego, infrastruktury rynków finansowych oraz infrastruktury cyfrowej. Wiąże się to z istniejącymi już sektorowymi uregulowaniami unijnymi, wprowadzającymi szczegółowe obowiązki dla tych podmiotów. Nie wyklucza to jednak identyfikowania poszczególnych podmiotów z tych sektorów jako podmioty krytyczne.
- Co więcej, przepisy tej dyrektywy nie mają również zastosowania, jeżeli w przepisach sektorowych aktów prawa Unii nałożono na podmioty krytyczne obowiązek zastosowania środków zwiększających ich odporność i jeżeli wymogi te są uznawane przez państwa członkowskie za co najmniej równoważne odpowiadającym im obowiązkom przewidzianym w CER.
- Nie stosuje się również tej dyrektywy do podmiotów administracji publicznej, które prowadzą swoją działalność w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym w zakresie prowadzenia postępowań przygotowawczych oraz wykrywania i ścigania przestępstw.

Jeżeli chodzi o zakres przedmiotowy, to w celu wzmocnienia odporności infrastruktury krytycznej został on znacznie poszerzony, w stosunku do dotychczasowych uregulowań. Do tej pory przepisami unijnej dyrektywy objęte były tylko podmioty krytyczne w sektorach energii i transportu. Jak uznała Komisja Europejska, nie było to wystarczające, by w pełni chronić usługi kluczowe dla funkcjonowania rynku wewnętrznego UE i państw członkowskich. Dlatego też w załączniku do CER wymieniono jedenaście sektorów, w ramach których będą wyznaczane podmioty krytyczne.

Sektory i podsektory krytyczne według załącznika I CER



Krajowe ramy odporności podmiotów krytycznych

W obliczu coraz bardziej złożonego krajobrazu ryzyka nowe przepisy mają na celu wzmocnienie odporności infrastruktury krytycznej na szereg zagrożeń, w tym zagrożenia naturalne, ataki terrorystyczne, zagrożenia wewnętrzne czy sabotaż. Odporność zdefiniowana tu została jako zdolność podmiotu krytycznego do zapobiegania incydentowi, ochrony przed nim, odpowiedzi na niego, stawiania mu oporu, łagodzenia i absorbowania incydentu oraz adaptacji i odtworzenia po incydencie.

Dyrektywą CER ustanowione zostały krajowe ramy dotyczące odporności podmiotów krytycznych. W ich skład wchodzi przede wszystkim strategia w zakresie odporności podmiotów krytycznych, ocena ryzyka przeprowadzana przez państwa członkowskie oraz mechanizm identyfikacji podmiotów krytycznych.

Strategia odporności podmiotów krytycznych

Każde państwo zobowiązane zostało do przyjęcia strategii odporności w terminie do 17 stycznia 2026 roku, a następnie aktualizowania jej co najmniej raz na cztery lata.

W dokumencie mają być określone cele strategiczne i środki polityczne służące osiągnięciu i utrzymaniu wysokiego poziomu odporności po stronie podmiotów krytycznych. W dyrektywie znalazły się również elementy obowiązkowe strategii, m.in. takie jak: opis ról i obowiązków poszczególnych stron, opis procesu identyfikacji podmiotów krytycznych oraz ich wspierania przez państwo, a także ramy polityczne umożliwiające koordynację między właściwymi organami na podstawie dyrektywy CER oraz NIS 2 na potrzeby wymiany informacji.

Ocena ryzyka państwa członkowskiego

Oprócz przyjęcia strategii, państwa zostały także zobowiązane do przeprowadzenia w tym samym terminie oceny ryzyka (również aktualizowanej następnie co najmniej raz na cztery lata).

W szczególności powinna ona brać pod uwagę:

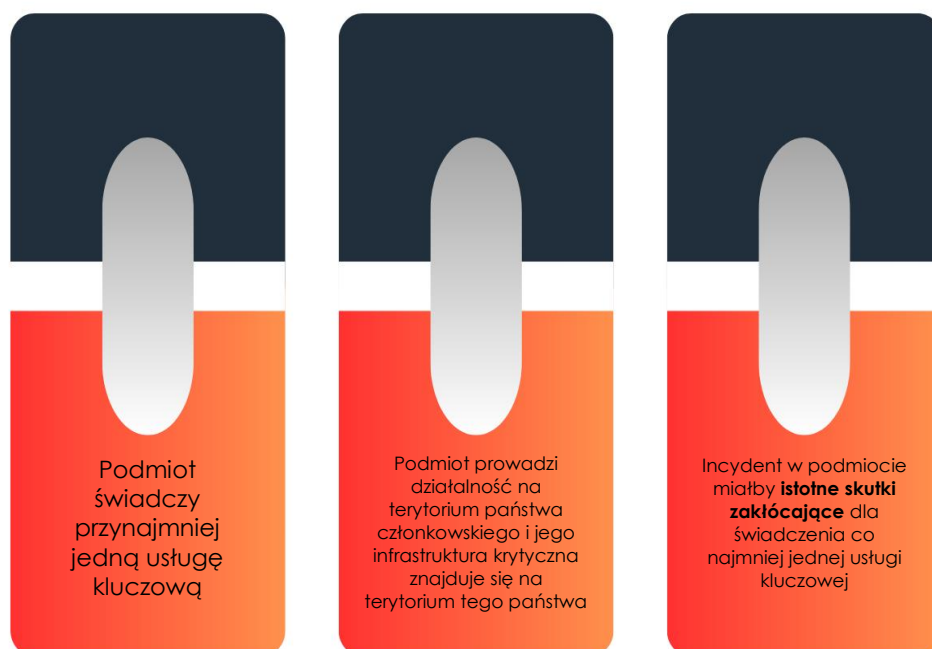
- ogólną ocenę ryzyka przeprowadzoną na podstawie Decyzji PE w sprawie Unijnego Mechanizmu Ochrony Ludności;
- inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów prawnych Unii;
- istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku oraz wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć na inne sektory;
- wszelkie informacje na temat incydentów zgłoszonych w podmiotach należących do sektorów określonych dyrektywą.

Ocena ryzyka państwa członkowskiego wykorzystywana jest następnie przez organy właściwe do celów identyfikacji podmiotów krytycznych i udzielania im pomocy we wprowadzaniu środków zgodnie z dyrektywą.

Identyfikowanie podmiotów krytycznych

Ostatnim elementem krajowych ram odporności jest mechanizm identyfikowania podmiotów krytycznych. W ciągu pół roku po przyjęciu strategii i przeprowadzeniu oceny ryzyka państwa członkowskiego, tj. do 17 lipca 2026 roku, państwa mają obowiązek wyznaczyć podmioty krytyczne w sektorach określonych w załączniku.

W dyrektywie zawarte zostały kryteria, które muszą być spełnione łącznie, aby dany podmiot mógł zostać uznany za krytyczny dla funkcjonowania danego sektora (lub państwa). Są one następujące:



Kategoria „istotności skutku zakłócającego” została również opisana w dyrektywie. Decyzję, czy ewentualny incydent w konkretnym podmiocie miałby charakter istotny, podejmuje się na podstawie sześciu kryteriów, opisanych na schemacie obok.

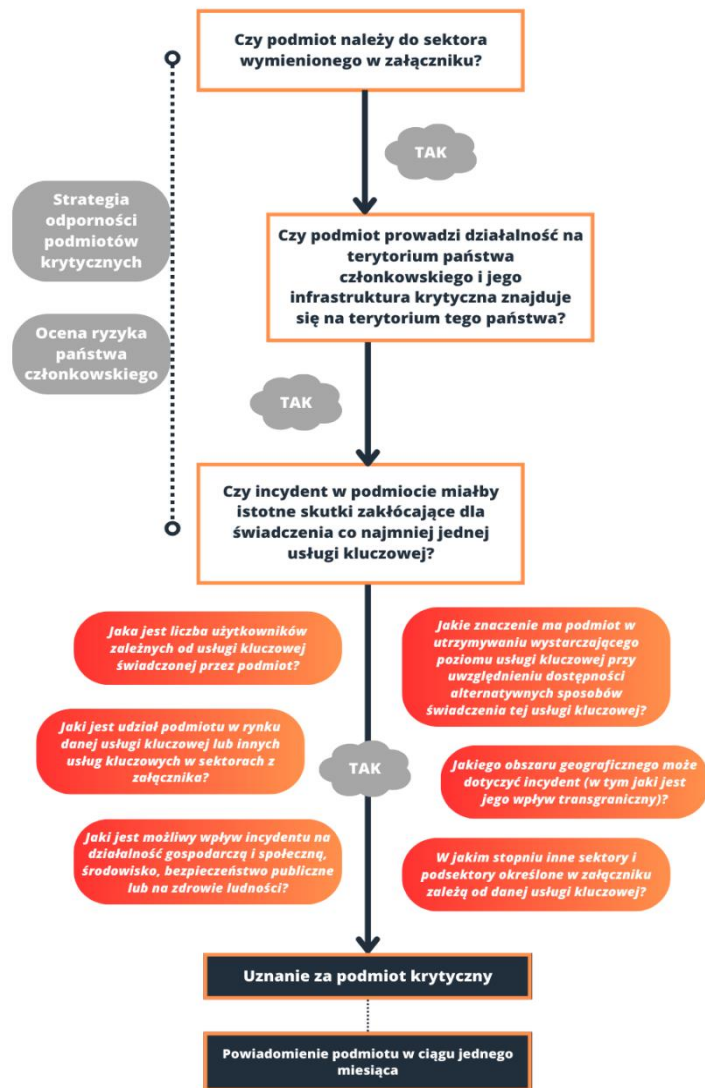
Identyfikując podmioty krytyczne państwo musi wziąć pod uwagę wyniki przeprowadzonej wcześniej oceny ryzyka państwa członkowskiego oraz przyjętą strategię ochrony infrastruktury krytycznej.

W przypadku zidentyfikowania danego podmiotu jako krytyczny na podstawie wymienionych kryteriów, państwo musi go o tym poinformować w ciągu miesiąca od zidentyfikowania.

Podmiot wyznaczony jako krytyczny zobowiązany jest wykonywać obowiązki określone dyrektywą CER po 10 miesiącach od daty powiadomienia.

Państwo ma również obowiązek prowadzenia wykazu podmiotów krytycznych, który aktualizowany ma być co najmniej co cztery lata, a w stosownych przypadkach – częściej.

Schemat wyznaczania podmiotów krytycznych



Organy właściwe i pojedynczy punkt kontaktowy

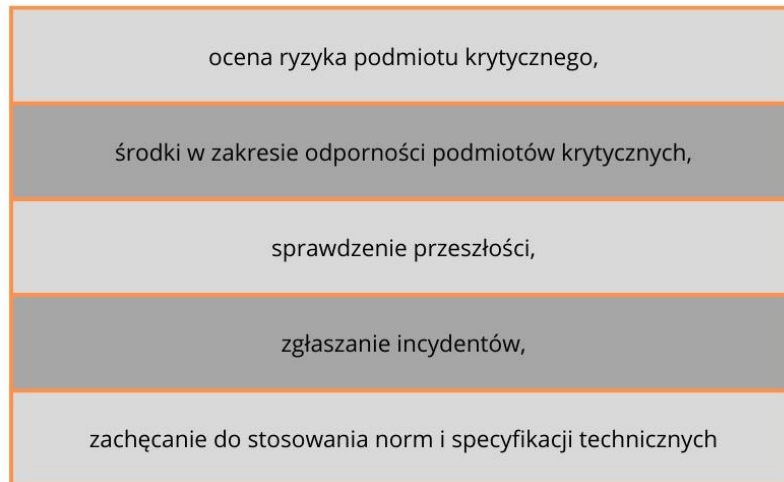
Dyrektywa CER wprowadza obowiązek wyznaczenia przez państwo co najmniej jednego organu właściwego, który odpowiedzialny jest za prawidłowe stosowanie i egzekwowanie przepisów. Co do zasady, w przypadku sektora bankowego oraz sektora infrastruktury rynku finansowego rolę tę pełnią organy właściwe wyznaczone na podstawie rozporządzenia DORA, a dla sektora infrastruktury cyfrowej – te określone na podstawie dyrektywy NIS 2.

Państwa muszą także wyznaczyć pojedynczy punkt kontaktowy, którego celem jest zapewnienie współpracy transgranicznej z pojedynczymi punktami kontaktowymi innych państw członkowskich oraz z Grupą ds. Odporności Podmiotów Krytycznych.

Odporność podmiotów krytycznych

Jednym z głównych celów dyrektywy CER jest podniesienie odporności podmiotów krytycznych na wszelkiego rodzaju zagrożenia. Mają być one w stanie zwiększyć swoje zdolności do zapobiegania incydom mogącym zakłócić świadczenie usług kluczowych, ochrony przed takimi incydentami i odpowiedzi na nie, stawiania im oporu, łagodzenia

i absorbowania ich oraz adaptacji i odtworzenia po takich incydentach. Dlatego też w dyrektywie cały rozdział poświęcony został mechanizmowi wzmacniania odporności podmiotów krytycznych. W jego ramach mieści się:



Ocena ryzyka podmiotu krytycznego

Na podstawie dyrektywy CER podmioty, które zostały zidentyfikowane jako krytyczne, w terminie dziewięciu miesięcy po otrzymaniu powiadomienia mają obowiązek przeprowadzić ocenę ryzyka. Kolejne oceny powinny być dokonywane w razie potrzeby, co najmniej co cztery lata.

Aby holistycznie spojrzeć na ryzyko, oceny takie mają obejmować wszystkie istotne naturalne i spowodowane przez człowieka czynniki ryzyka mogące prowadzić do incydentu, w tym czynniki o charakterze międzysektorowym lub transgranicznym, wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego, zagrożenia hybrydowe czy inne zagrożenia związane z konfliktami międzynarodowymi, w tym przestępstwa terrorystyczne.

Podmiot musi również uwzględnić w swojej ocenie ryzyka stopień zależności innych sektorów (określonych w załączniku do CER) od świadczonej przez siebie usługi kluczowej. Należy także wziąć pod uwagę, w jakim stopniu dany podmiot krytyczny jest zależny od usług kluczowych świadczonych przez inne podmioty krytyczne.

Zgłaszanie incydentów

Podmioty krytyczne zostały również zobowiązane do zgłaszania organom właściwym incydentów, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych. Zgłoszenie wstępne powinno być dokonane nie później niż 24 godziny od chwili uzyskania wiedzy o zaistnieniu incydentu. Następnie, konieczne jest przedłożenie szczegółowego sprawozdania na ten temat, w terminie nie dłuższym niż jeden miesiąc od zaistnienia incydentu.

W dyrektywie zostały określone parametry, które muszą być uwzględniane przez podmiot w celu określenia wagi zakłócenia. W przypadku gdy incydent ma lub może mieć znaczący wpływ na ciągłość świadczenia usług kluczowych na rzecz co najmniej sześciu państw członkowskich, konieczne jest powiadomienie Komisji Europejskiej przez organ właściwy.

Pozostałe środki w zakresie odporności podmiotów krytycznych

W oparciu o informacje dostarczone w ramach oceny ryzyka państwa członkowskiego oraz wyników oceny ryzyka podmiotu krytycznego, podmioty te muszą wprowadzić **odpowiednie i proporcjonalne środki, które mają zapewnić im odporność** na wszelkiego rodzaju incydenty.



Wśród nich muszą znaleźć się takie, które mają na celu:

- zapobieganie incydentom, w tym środki zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu;
- zapewnienie odpowiedniej fizycznej ochrony budynków i terenów oraz infrastruktury krytycznej,
- odpowiedź na incydenty, stawianie im oporu i łagodzenie ich skutków, w tym procedury i protokoły zarządzania ryzykiem i zarządzania kryzysowego, a także procedury ostrzegawcze,
- odtworzenie po incydentach, w tym środki na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw,
- zapewnienie odpowiedniego zarządzania bezpieczeństwem pracowników,
- zwiększanie świadomości odpowiedniego personelu na temat środków wzmacniania odporności.

Środki te muszą być opisane w planie zwiększania odporności podmiotu krytycznego bądź w równoważnych dokumentach.

Państwa mają obowiązek **wspierać podmioty krytyczne w zwiększaniu ich odporności**. Obejmuje to m.in. opracowywanie materiałów zawierających wytyczne oraz metodyk, pomoc w organizacji ćwiczeń mających na celu sprawdzenie odporności tych podmiotów, czy zapewnianie doradztwa i szkoleń dla personelu podmiotów krytycznych. Jeżeli jest to konieczne i uzasadnione celami interesu publicznego, państwa mogą również przekazywać zasoby finansowe podmiotom krytycznym.

Interesującym mechanizmem, mającym wzmocnić odporność podmiotów krytycznych, jest umożliwienie **sprawdzania przeszłości osób, które pełnią newralgiczne role w podmiocie krytycznym** lub na jego rzecz, lub są upoważnione do posiadania bezpośredniego lub zdalnego dostępu do budynków i terenów podmiotu krytycznego, jego informacji lub systemów kontroli. Sprawdzenie to może również obejmować osoby, które są brane pod uwagę przy rekrutacji na określone stanowiska w podmiocie krytycznym.

Sprawdzanie przeszłości musi być proporcjonalne i ściśle ograniczone do tego, co jest konieczne. Przeprowadza się je wyłącznie w celu oceny potencjalnego ryzyka dla bezpieczeństwa danego podmiotu krytycznego.

Państwa członkowskie mogą zachęcać podmioty krytyczne, nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych dla środków w zakresie bezpieczeństwa i odporności mających zastosowanie do podmiotów krytycznych.

Podmioty krytyczne o szczególnym znaczeniu europejskim

Dyrektywa CER wprowadza szczególną kategorię podmiotów krytycznych – podmioty krytyczne o szczególnym znaczeniu europejskim.



Wyznaczanie podmiotów krytycznych o szczególnym znaczeniu europejskim odbywa się jednak po konsultacjach, w których bierze udział KE, właściwy organ państwa członkowskiego, właściwy organ innych zainteresowanych państw członkowskich oraz określony podmiot krytyczny. W ich trakcie każde państwo członkowskie informuje Komisję o tym, czy uważa, że usługi świadczone na jego rzecz przez podmiot krytyczny stanowią usługi kluczowe w rozumieniu dyrektywy. Dopiero po tym KE uznaje dany podmiot za mający szczególne znaczenie europejskie, co wiąże się z określonymi w dyrektywie obowiązkami.

Dyrektywa przewiduje również możliwość zorganizowania przez Komisję misji doradczej w celu oceny środków wprowadzonych przez dany podmiot krytyczny o szczególnym znaczeniu europejskim. Może być ona przeprowadzona z własnej inicjatywy KE lub na wniosek: (1) państwa członkowskiego, które zidentyfikowało podmiot krytyczny o szczególnym znaczeniu europejskim lub (2) co najmniej jednego państwa członkowskiego, na rzecz którego lub w którym świadczona jest usługa kluczowa.

Zamysłem prawodawcy unijnego w tym przypadku było przede wszystkim stworzenie mechanizmu wzajemnej oceny funkcjonowania danego podmiotu krytycznego i wywiązywania się przez niego z nałożonych dyrektywą obowiązków, której mogą dokonać państwa członkowskie, na rzecz których lub w których świadczona jest usługa kluczowa. Mogą one doradzać Komisji w kwestii tego, czy dany podmiot krytyczny o szczególnym znaczeniu europejskim wywiązuje się z obowiązków. Możliwe jest także udzielanie porad w zakresie tego, jakie środki można wprowadzić, aby zwiększyć odporność określonego podmiotu krytycznego.

Współpraca w zakresie infrastruktury krytycznej

Na podstawie przepisów dyrektywy CER ustanowiona została Grupa ds. Odporności Podmiotów Krytycznych, której głównym celem jest ułatwianie współpracy i wymiany informacji między państwami członkowskimi. Wspiera ona także Komisję w pomocy tym państwom w zwiększaniu ich zdolności do zapewniania odporności podmiotów krytycznych.

W celu zapewnienia komplementarności z przepisami nałożonymi dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii,

Grupa ds. Odporności Podmiotów Krytycznych spotyka się regularnie (co najmniej raz w roku) z Grupą Współpracy ustanowioną na podstawie dyrektywy NIS 2.

Nadzór, egzekwowanie przepisów i sankcje

Organy właściwe na podstawie dyrektywy CER otrzymały możliwość skorzystania z dwóch rodzajów **środków nadzoru**. Są to:



Zakresem kontroli objęta jest infrastruktura krytyczna¹ oraz budynki i tereny wykorzystywane przez podmiot krytyczny do świadczenia usług kluczowych. W tej grupie środków znalazło się także uprawnienie do prowadzenia zdalnego nadzoru nad środkami w zakresie odporności stosowanymi przez podmioty krytyczne.

Oprócz tego organy właściwe wyposażone zostały w **środki egzekwowania przepisów**. Należą do nich:

- zobowiązanie podmiotów zidentyfikowanych jako podmioty krytyczne do przekazania w rozsądnym terminie
 - informacji koniecznych do oceny, czy działania podjęte przez nie w celu zapewnienia ich odporności spełniają wymogi określone w dyrektywie,
 - dowodów potwierdzających skuteczne wdrożenie tych środków, w tym wyników audytu przeprowadzonego na koszt tego podmiotu przez wybranego przez niego niezależnego i wykwalifikowanego audytora,
- po przeprowadzeniu działań nadzorczych, nakaz podjęcia przez podmioty krytyczne koniecznych i proporcjonalnych działań w celu wyeliminowania wszelkiego stwierdzonego naruszenia dyrektywy w rozsądnym terminie ustalonym przez te organy oraz poinformowania tych organów o podjętych działaniach.

Środki nadzoru i egzekwowania prawa muszą być stosowane wyłącznie z zastrzeżeniem odpowiednich gwarancji prawnych. W szczególności wykonywanie tych uprawnień musi nastąpić w sposób obiektywny, przejrzysty i proporcjonalny oraz z należyтым zabezpieczeniem praw i prawnie uzasadnionych interesów podmiotów krytycznych, takich jak ochrona tajemnicy przedsiębiorstwa i tajemnicy handlowej, prawo do bycia wysłuchanym, prawo do obrony oraz prawo do skutecznego środka odwoławczego przed niezależnym sądem.

W dyrektywie znalazł się również zapis o możliwości nakładania przez państwa członkowskie sankcji, mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie dyrektywy CER. Ich rodzaj i wysokość ewentualnych kar administracyjnych

¹ Zgodnie z definicją zawartą w artykule 2 dyrektywy CER „infrastruktura krytyczna” oznacza składnik, obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci lub systemu, niezbędne do świadczenia usługi kluczowej.

pozostawiono w gestii poszczególnych państw. Prawodawca unijny ograniczył się wyłącznie do określenia, że przewidziane sankcje muszą być **skuteczne, proporcjonalne i odstraszające**.

Podsumowanie

- Dyrektywa CER **ma na celu zwiększenie odporności podmiotów o krytycznym znaczeniu**, które świadczą usługi niezbędne dla podstawowych funkcji społecznych lub działalności gospodarczej na rynku wewnętrznym.
- **Wraz z dyrektywą NIS 2 tworzą one komplementarne, zharmonizowane ramy prawne** w zakresie zapewniania ciągłości usług kluczowych dla państwa oraz odporności (fizycznej i w cyberprzestrzeni) podmiotów je świadczących.
- Dyrektywa CER **reguluje przede wszystkim obowiązki państw członkowskich** poprzez ustanowienie krajowych ram dotyczących odporności podmiotów krytycznych.
- W załączniku do dyrektywy wymieniono **jedenastie sektorów, w ramach których będą wyznaczane podmioty krytyczne**.
- W stosunku do wcześniejszych uregulowań dotyczących infrastruktury krytycznej **zmienił się sposób i mechanizm identyfikowania podmiotów krytycznych**. Wprowadzono trzy kryteria, które muszą być spełnione przez podmiot łącznie, a dodatkowo bierze się pod uwagę strategię państwa w zakresie odporności podmiotów krytycznych i ocenę ryzyka państwa członkowskiego.
- **Uznanie za podmiot krytyczny następuje w drodze decyzji administracyjnej**.
- CER wprowadza także **obowiązki dla podmiotów krytycznych**. Muszą one wprowadzić **odpowiednie i proporcjonalne środki techniczne, bezpieczeństwa i organizacyjne, które mają zapewnić im odporność** na wszelkiego rodzaju incydenty.
- Dyrektywa wprowadza także **możliwość sprawdzania przeszłości osób**, które pełnią niewrażliwe role w podmiocie krytycznym lub na jego rzecz, lub posiadają dostęp do jego budynków i terenów.
- Dyrektywa CER wprowadza szczególną kategorię podmiotów krytycznych – podmioty krytyczne o szczególnym znaczeniu europejskim.
- Organy właściwe na podstawie dyrektywy CER otrzymały możliwość skorzystania z dwóch rodzajów **środków nadzoru: przeprowadzania kontroli oraz przeprowadzania lub zlecenia audytów**. Wyposażone zostały również w środki egzekwowania przepisów.
- Dyrektywa przewiduje możliwość stosowania sankcji wobec podmiotów krytycznych, które naruszają obowiązki, ale ich rodzaj pozostawiono w gestii państw członkowskich.