NOWE REGULACJE DOTYCZĄCE INFRASTRUKTURY KRYTYCZNEJ

Sergiusz Parszowski

Unia Europejska wprowadza nowe regulacje w zakresie bezpieczeństwa infrastruktury krytycznej. Nadrzędnym ich celem jest zapewnienie niezakłóconego świadczenia usług kluczowych, to jest takich, które mają decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska. Sposobem na osiągnięcie tego ma być odporność podmiotów krytycznych, a więc ich zdolność do zapobiegania incydentowi, ochrony przed nim, odpowiedzi na niego, stawiania mu oporu, łagodzenia i absorbowania incydentu oraz adaptacji i odtworzenia po incydencie.

Dyrektywa CER

Właśnie zakończyły się prace legislacyjne nad Dyrektywą o odporności podmiotów krytycznych zwaną również Dyrektywą CER. Oficjalna nazwa przygotowanych przepisów prawa to „Dyrektywa Parlamentu Europejskiego i Rady *w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE*". Dotychczas sprawy infrastruktury krytycznej na poziomie Unii Europejskiej były regulowane przez „Dyrektywę 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*[1]" i to właśnie ona będzie uchylona.

Dyrektywa CER określa w szczególności:

- obowiązki państw członkowskich, w tym polegające na identyfikowaniu podmiotów krytycznych oraz wspieraniu podmiotów krytycznych;
- przepisy w zakresie identyfikacji podmiotów krytycznych o szczególnym znaczeniu europejskim;

[1] Dziennik Urzędowy Unii Europejskiej L 345/75

- obowiązki podmiotów krytycznych mające na celu zwiększenie ich odporności i zdolności do świadczenia usług;
- środki mające na celu osiągnięcie wysokiego poziomu odporności podmiotów krytycznych;
- przepisy dotyczące nadzoru nad podmiotami krytycznymi.

O tym, że nie są to wyłącznie kosmetyczne zmiany świadczy samo porównanie obszerności poszczególnych dokumentów. Dyrektywa z 2016 roku liczy jedynie 8 stron, Dyrektywa z 2022 roku liczy natomiast 103 strony.

Sektory krytyczne

Dyrektywa CER na nowo określa sektory, w ramach których wyznaczane będą podmioty krytyczne. W dotychczasowych przepisach przewidziano jedynie dwa sektory europejskiej infrastruktury krytycznej, tj. „energia" i „transport". W nowych regulacjach będzie już jedenaście takich obszarów:

- Energetyka (Energia elektryczna, Centralne ogrzewanie i chłodzenie, Ropa, Gaz, Wodór);
- Transport (powietrzny, kolejowy, wodny, lądowy);
- Bankowość;
- Infrastruktura rynków finansowych;
- Zdrowie;
- Woda pitna;
- Ścieki;
- Infrastruktura cyfrowa;
- Administracja publiczna;
- Przestrzeń kosmiczna;
- Wytwarzanie, przetwarzanie i dystrybucja żywności.

W ramach uzupełnienia należy podkreślić, że Dyrektywy CER nie stosuje się 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.

Ramy odporności dotyczące odporności

W ramach wdrażania postanowień Dyrektywy CER państwa członkowskie UE będą zobowiązane do przyjęcia, wprowadzenia lub przeprowadzenia szeregu środków i rozwiązań na rzecz odporności podmiotów krytycznych, w tym m.in.:

- Przyjąć strategię mającą na celu zwiększenie odporności podmiotów krytycznych zawierającą między innymi następujące elementy: cele strategiczne i priorytety; opis ról i obowiązków poszczególnych organów, podmiotów krytycznych i innych stron; opis środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, w tym opis oceny ryzyka; opis procesu, w ramach którego iden-

tyfikuje się podmioty krytyczne; opis procesu wspierania podmiotów krytycznych.

- Przeprowadzenia oceny ryzyka, która to następnie posłuży do identyfikacji podmiotów krytycznych. Oceny ryzyka państw członkowskich muszą uwzględniać istotne czynniki ryzyka, naturalne i spowodowane przez człowieka, w tym zagrożenia mające charakter międzysektorowy i transgraniczny, wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego i zagrożenia hybrydowe lub inne zagrożenia związane z konfliktem, w tym przestępstwa terrorystyczne.
- Dokonać identyfikacji podmiotów krytycznych dla sektorów i podsektorów określonych w załączniku do Dyrektywy CER. W procesie tym uwzględniane będą wyniki oceny ryzyka oraz postanowienia strategii. Za podmioty krytyczne uznawane będą podmioty świadczące co najmniej jedną usługę kluczową i w przypadku których incydent miałby istotne skutki zakłócające dla świadczenia tejże usługi kluczowej lub usługi kluczowej świadczonej przez inny podmiot.
- Wyznaczenie lub ustanowienie co najmniej jednego organu odpowiedzialnego za prawidłowe stosowanie i egzekwowanie na poziomie krajowym przepisów określonych w niniejszej dyrektywie. Jednocześnie każde państwo członkowskie będzie musiało wyznaczyć lub ustanowić jeden pojedynczy punkt kontaktowy, który będzie wykonywać funkcję łącznikową w celu zapewnienia współpracy z pojedynczymi punktami kontaktowymi innych państw członkowskich i z Grupą ds. Odporności Podmiotów Krytycznych.
- Zapewnienie wsparcia państw członkowskich na rzecz podmiotów krytycznych. Wsparcie to może obejmować opracowywanie materiałów zawierających wytyczne oraz metodyk, pomoc w organizacji ćwiczeń mających na celu sprawdzenie odporności tych podmiotów oraz zapewnianie doradztwa i szkoleń dla personelu podmiotów krytycznych. Możliwe będzie przekazywanie podmiotom krytycznym przez państwa członkowskie także zasobów finansowych.

Wszystkie państwa członkowskie będą musiały przyjąć takie przepisy prawa, by zapewnić krajowym organom uprawnienia i środki umożliwiające:

- przeprowadzanie kontroli na miejscu w zakresie infrastruktury krytycznej oraz budynków i terenów wykorzystywanych przez podmiot krytyczny do świadczenia usług kluczowych, oraz prowadzenie zdalnego nadzoru nad środkami stosowanymi przez podmioty krytyczne;

- przeprowadzanie lub zlecanie audytów dotyczących podmiotów krytycznych.

Właściwe organy, po przeprowadzeniu działań nadzorczych i stwierdzeniu naruszeń, będą mogły nakazać podmiotom krytycznym podjęcie koniecznych i proporcjonalnych działań w celu ich wyeliminowania lub nałożyć sankcje, które zgodnie z wymaganiami Dyrektywy CER muszą być skuteczne, proporcjonalne i odstraszające.

Odporność podmiotów krytycznych

Obowiązek ochrony infrastruktury niezbędnej do utrzymania usług kluczowych będzie należał do podmiotów krytycznych. Dyrektywa wymienia szereg działań, do przeprowadzenia których będą one zobowiązane, m.in.:

- Przeprowadzenie oceny ryzyka obejmującej wszystkie istotne naturalne i spowodowane przez człowieka czynniki ryzyka mogące prowadzić do incydentu, w tym czynniki ryzyka o charakterze międzysektorowym lub transgranicznym, wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego i zagrożenia hybrydowe oraz inne zagrożenia związane z konfliktem.
- Zapobieganie incydentom, z należytym uwzględnieniem środków zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu.
- Zapewnienie odpowiedniej fizycznej ochrony ich budynków i terenów oraz infrastruktury krytycznej, z należytym uwzględnieniem na przykład zainstalowania ogrodzeń, budowy barier, narzędzi i procedur monitorowania terenu podlegającego ochronie, sprzętu do wykrywania i kontroli dostępu.
- Odpowiedzi na incydenty, stawiania im oporu i łagodzenia ich skutków, z należytym uwzględnieniem wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych.
- Odtworzenie po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej.
- Zapewnienie odpowiedniego zarządzania bezpieczeństwem pracowników, z należytym uwzględnieniem środków takich jak ustanowienie kategorii personelu wykonującego funkcje krytyczne, ustanowienie praw dostępu do budynków i terenów, infrastruktury krytycznej i informacji szczególnie chronionych, ustanowienie procedur sprawdzenia przeszłości, wyznaczenie kategorii osób podlegających takim procedurom sprawdzenia przeszłości

oraz określenie odpowiednich wymogów szkoleniowych i kwalifikacji.
- Zwiększanie świadomości odpowiedniego personelu na temat środków z należytym uwzględnieniem szkoleń, materiałów informacyjnych i ćwiczeń.

Wymienione powyżej środki będą musiały być opisane przez podmioty krytyczne w planie zwiększania odporności lub innym równoważnym dokumencie.

Podmioty krytyczne będą zobowiązane również do zgłaszania wskazanemu organowi wszystkich incydentów, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych. Zgłoszenie wstępne, co do zasady będzie musiało być dokonane nie później niż 24 godziny od chwili uzyskania wiedzy o zaistnieniu incydentu. W stosownych przypadkach, w terminie nie dłuższym niż jeden miesiąc od zaistnienia incydentu, wymagane będzie również przełożenie szczegółowego sprawozdania.

Grupa ds. Odporności Podmiotów Krytycznych

Celem działania Grupy ds. Odporności Podmiotów Krytycznych będzie wspieranie Komisji, jak również ułatwianie współpracy między państwami członkowskimi oraz wymiany informacji na temat kwestii związanych z Dyrektywą CER. Będą ją tworzyć przedstawiciele państw członkowskich i Komisji. Zadaniami Grupy ds. Odporności Podmiotów Krytycznych będą między innymi:
- Wspieranie Komisji w pomocy państwom członkowskim w zwiększaniu ich zdolności do zapewniania odporności podmiotów krytycznych.
- Analizowanie strategii w celu określenia najlepszych praktyk w odniesieniu do tych strategii.
- Ułatwianie wymiany najlepszych praktyk w odniesieniu do identyfikacji podmiotów krytycznych przez państwa członkowskie.
- Wnoszenie wkładu w przygotowywanie dokumentów dotyczących odporności na poziomie Unii.
- Analizowanie sprawozdań podsumowujących z myślą o promowaniu wymiany najlepszych praktyk.
- Wymiana najlepszych praktyk dotyczących zgłaszania incydentów.
- Wymiana informacji i najlepszych praktyk dotyczących innowacji, badań i rozwoju w zakresie odporności podmiotów krytycznych.
- Wymiana informacji w sprawach dotyczących odporności podmiotów krytycznych z odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii.

Komisja będzie wspierać państwa członkowskie i podmioty krytyczne w wypełnianiu ich obowiązków. W tym celu będzie przygotowywać ogólnounijny przegląd transgranicznych i międzysektorowych czynników ryzyka, organizować misje doradcze oraz ułatwiać wymianę informacji między państwami członkowskimi i ekspertami w całej Unii. Dodatkowo będzie opracowywać najlepsze praktyki, materiały zawierające wytyczne i metodyki oraz organizować transgraniczne działania szkoleniowe i ćwiczenia w celu sprawdzania odporności podmiotów krytycznych.

Dyrektywa CER a Dyrektywa NIS2

Równolegle do prac nad Dyrektywą CER przygotowana była również *Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii* zwana Dyrektywą NIS2[2]. Z uwagi na fakt, że obie regulacje wpłyną na funkcjonowanie podobnej grupy podmiotów, zostały one ze sobą ściśle skorelowane, by prezentowały tożsame podejście.

Dyrektywy mają zostać skierowane do publikacji w grudniu 2022, zaś wejść w życie dwudziestego dnia po ich opublikowaniu w Dzienniku Urzędowym Unii Europejskiej. Możemy zatem oczekiwać, że już w połowie stycznia 2023 r. o wspomnianych dyrektywach nie będziemy już mówić jako o projektach, ale o obowiązującym prawie.

Nie oznacza to oczywiście, że powyższe regulacje będą stosowane bezpośrednio. W następnym etapie wszystkie Państwa członkowskie UE będą zobowiązane do wdrożenia poszczególnych postanowień dyrektywy do własnych systemów prawnych. Będą miały na to 21 miesięcy od wejścia w życie Dyrektywy CER. Natomiast wdrażanie najważniejszych jej postanowień zostało zaplanowane na 3 lata od wejścia nowych regulacji w życie. Z uwagi na powiązanie między fizycznym bezpieczeństwem a cyberbezpieczeństwem podmiotów krytycznych wdrażanie obu dyrektyw musi przebiegać w sposób skoordynowany.

Rekomendacje wdrożeniowe

Rada Europejska przygotowała także trzydziesto-stronicowy dokument zatytułowany „Zalecenie Rady (UE) w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej", który to jest zestawem rekomendacji do wdrażania Dyrektywy CER i zawiera szereg rozwiązań przejściowych mających na celu poprawę bezpieczeństwa infrastruktury krytycznej w ciągu najbliższych miesięcy. ■

Sergiusz Parszowski
Lider zespołu eksperckiego Instin.pl
Prezes think tanku ObserwatoriumBezpieczenstwa.pl

[2] Aktualnie obowiązuje Dyrektywa 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 (Dyrektywa NIS). Dyrektywa określana jest potocznie pierwszym europejskim prawem w zakresie cyberbezpieczeństwa.