UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 6ze. ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą" i określa minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań, o których mowa w ust. 1 pkt 2 ustawy, mając na uwadze potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury krytycznej i ujednolicenie rozwiązań w tym zakresie.

Celem projektowanego rozporządzenia jest zapewnienie jednolitego, minimalnego i weryfikowalnego poziomu wymagań w zakresie ochrony infrastruktury krytycznej, obejmującego środki organizacyjne i techniczne niezbędne do ograniczenia ryzyka zakłócenia jej funkcjonowania oraz do zapewnienia ciągłości realizacji jej funkcji. Rozporządzenie ustanawia minimalne wymagania o charakterze funkcjonalnym, co oznacza, że operatorzy infrastruktury krytycznej wdrażają wymagania w sposób zapewniający osiągnięcie celu ochrony infrastruktury krytycznej adekwatnie do wyników analizy zagrożeń w zakresie zakłócenia jej funkcjonowania infrastruktury krytycznej, w tym jej wzajemnych zależności i współzależności z innymi elementami infrastruktury krytycznej i infrastrukturą krytyczną w innych sektorach i podsektorach.

Potrzeba wydania rozporządzenia wynika z konieczności doprecyzowania, w zakresie przewidzianym w art. 6ze ust. 4 ustawy, minimalnego standardu postępowania operatorów infrastruktury krytycznej w obszarach, które łącznie determinują poziom odporności infrastruktury krytycznej, tj. bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, bezpieczeństwa prawnego oraz ciągłości działania. Dotychczasowe ujęcie ustawowe, choć określa ramy obowiązków operatorów infrastruktury krytycznej, nie przesądzało w sposób dostatecznie jednoznaczny o minimalnym poziomie rozwiązań i mechanizmów, jakie powinny zostać wdrożone. W konsekwencji prowadziło to do zróżnicowanej praktyki, rozbieżności interpretacyjnych oraz powstawania luk bezpieczeństwa w obszarach wymagających podejścia zintegrowanego. Projektowane rozporządzenie porządkuje i ujednolica praktykę wdrażania rozwiązań, o których mowa w ust. 1 pkt 2 ustawy, poprzez wskazanie minimalnych wymagań stanowiących punkt odniesienia dla projektowania, wdrażania, utrzymywania oraz doskonalenia środków ochrony infrastruktury krytycznej. Regulacja ma charakter systemowy i służy zapewnieniu spójności działań operatorów infrastruktury krytycznej w całym cyklu życia rozwiązań bezpieczeństwa, w szczególności w zakresie planowania, wdrażania, monitorowania, testowania oraz korygowania przyjętych środków, w oparciu o analizę zagrożeń i analizę ryzyka.

Dotychczasowy model funkcjonowania tzw. sześciu obszarów bezpieczeństwa infrastruktury krytycznej (bezpieczeństwo fizyczne, techniczne, osobowe, teleinformatyczne, prawne oraz ciągłość działania), opisywanych w Narodowym Programie Ochrony Infrastruktury Krytycznej, nie był oparty na wiążących, minimalnych wymaganiach o charakterze normatywnym. Wdrażanie rozwiązań w tym zakresie odbywało się w oparciu o Załącznik 1 do NPOIK – „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje".

System oparty na zaleceniach i rekomendacjach nie zapewniał jednolitego i weryfikowalnego poziomu bezpieczeństwa infrastruktury krytycznej. Brak twardych wymagań powodował, że standardy zawarte w Załączniku 1 do NPOIK nie uzyskały wystarczającego przełożenia na rynek zamówień usług oraz sprzętu niezbędnych do zapewnienia bezpieczeństwa i ochrony infrastruktury krytycznej. W praktyce rekomendacje niebędące źródłem prawa nie stanowiły punktu odniesienia dla warunków zamówień ani dla oceny jakości i zgodności dostarczanych rozwiązań. Projektowane rozporządzenie wprowadza minimalne wymagania o charakterze wiążącym, które porządkują dotychczasowy model oparty na rekomendacjach i nadaje mu wymiar normatywny. Regulacja nie zastępuje Załącznika 1 do NPOIK

(nadal może być stosowany jako zbiór dobrych praktyk), lecz stanowi jego komplementarne rozwinięcie w zakresie minimalnego, obligatoryjnego poziomu zabezpieczeń. Oznacza to przejście od modelu opartego wyłącznie na dobrych praktykach do modelu łączącego rekomendacje z jednoznacznie określonymi wymaganiami podlegającymi weryfikacji.

W odniesieniu do podmiotów krytycznych rozporządzenie jest wykonaniem obowiązku zawartego w art. 13 ust. 1 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 333 z 27.12.2022 r., który to artykuł stanowi, że „państwa członkowskie zapewniają, aby podmioty krytyczne wprowadzały odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne". Zgodnie z tym zapisem w projektowanym rozporządzeniu położono nacisk zarówno na rozwiązania techniczne, rozwiązania zapewniające odpowiedni poziom bezpieczeństwa, jak i na rozwiązania organizacyjne.

I. Część regulacji dotycząca bezpieczeństwa fizycznego została ukształtowana w sposób bardziej szczegółowy i rozbudowany w porównaniu z innymi obszarami bezpieczeństwa. Wynika to z następujących przesłanek:

1) Systemowa rola operatorów infrastruktury krytycznej w zapewnianiu ciągłości działania usług kluczowych – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 ustanawia ramy zapewnienia odporności podmiotów krytycznych, w tym obowiązek wdrażania adekwatnych środków technicznych i organizacyjnych służących zapobieganiu incydentom, ochronie przed nimi oraz zapewnieniu ciągłości świadczenia usług kluczowych. W polskiej implementacji podmioty krytyczne są wyłaniane spośród operatorów infrastruktury krytycznej. Ponadto podmioty krytyczne mogą wskazać infrastrukturę innych podmiotów (kooperantów, usługodawców itp.) jako infrastrukturę krytyczną. W efekcie operatorzy infrastruktury krytycznej stanowią element systemu zapewniającego ciągłość działania usług kluczowych, a ich zdolność do ochrony fizycznych komponentów infrastruktury ma bezpośredni wpływ na poziom odporności podmiotów krytycznych. W konsekwencji szczegółowe uregulowanie minimalnych wymagań w zakresie bezpieczeństwa fizycznego operatorów infrastruktury krytycznej pozostaje spójne z celami dyrektywy i zapewnia komplementarność rozwiązań krajowych względem unijnych ram odporności.

2) Materialny charakter infrastruktury krytycznej – zasadnicza część infrastruktury krytycznej posiada komponent fizyczny (obiekty, instalacje, urządzenia, linie przesyłowe, węzły energetyczne, obiekty morskie), który stanowi bezpośredni przedmiot potencjalnych działań sabotażowych, terrorystycznych lub przestępczych. Uszkodzenie lub zniszczenie elementu fizycznego może skutkować natychmiastowym i nieodwracalnym zakłóceniem realizacji funkcji infrastruktury krytycznej i negatywnie wpływać na zależności i współzależności z innymi sektorami i podsektorami infrastruktury krytycznej.

3) Pierwotność ochrony fizycznej względem innych warstw bezpieczeństwa – bezpieczeństwo fizyczne stanowi warstwę bazową dla bezpieczeństwa technicznego i cyberbezpieczeństwa, gdyż brak właściwego zabezpieczenia fizycznego może umożliwić bezpośrednią ingerencję w systemy techniczne i teleinformatyczne, niezależnie od poziomu ich zabezpieczenia cyfrowego.

4) Wysokie zróżnicowanie praktyki w zakresie ochrony fizycznej – analiza praktyki funkcjonowania operatorów infrastruktury krytycznej wskazuje na znaczne różnice w zakresie strefowania obszarów i obiektów, integracji systemów zabezpieczeń technicznych, organizacji bezpośredniej ochrony fizycznej, systemów transmisji alarmów oraz funkcjonowania Alarmowych Centrów Odbiorczych. W szczególności w obszarze systemów zabezpieczeń technicznych operator infrastruktury krytycznej nie dysponował jednoznacznie określonym mechanizmem regulacyjnym pozwalającym na ocenę czy

system został wykonany zgodnie z zamówieniem, projektem oraz właściwymi Polskimi Normami.

Wprowadzenie obowiązku przeprowadzenia dokonania odbioru końcowego obejmującego minimalny zakres weryfikacji, a także możliwości zastąpienia odbioru oceną zgodności dokumentacji wykonawczej i certyfikacją zainstalowanego systemu zabezpieczeń technicznych w istotny sposób ogranicza ryzyko przyjęcia przez operatora infrastruktury krytycznej systemu wadliwego lub niespełniającego wymaganego poziomu zabezpieczenia. Proponowany mechanizm eliminuje dotychczasową lukę w systemie, zwiększa rzeczywisty poziom ochrony infrastruktury krytycznej oraz ogranicza ryzyko powstawania sporów prawnych, dodatkowych kosztów organizacyjnych i finansowych związanych z konieczności naprawy lub wymiany nieskutecznych rozwiązań.

5) Konsekwencje incydentów fizycznych – incydenty o charakterze fizycznym mogą powodować skutki o charakterze kaskadowym, w tym wtórne incydenty techniczne i cyberbezpieczeństwa, a także zagrożenie dla życia i zdrowia ludzi. Z tego względu projektodawca uznał za zasadne szczegółowe określenie minimalnych elementów systemu bezpieczeństwa fizycznego, przy zachowaniu zasady adekwatności do wyników analizy zagrożeń.

II. W zakresie bezpieczeństwa technicznego projektowane rozporządzenie określa minimalne wymagania dotyczące zapewnienia niezawodności, odporności i utrzymania zdolności operacyjnej obiektów, instalacji oraz urządzeń infrastruktury krytycznej. Bezpieczeństwo techniczne pozostaje w ścisłym związku z bezpieczeństwem fizycznym, cyberbezpieczeństwem oraz ciągłością działania, gdyż awarie technologiczne, błędy eksploatacyjne lub brak redundancji mogą prowadzić do zakłóceń o skutkach porównywalnych z incydentami o charakterze celowym. Ujednolicenie minimalnych wymagań w tym obszarze, adekwatnie do wyników analizy zagrożeń, ogranicza ryzyko strat materialnych i operacyjnych, wzmacnia odporność infrastruktury krytycznej na zakłócenia techniczne oraz sprzyja zapewnieniu ciągłości realizacji jej funkcji.

III. Projektowane rozporządzenie obejmuje minimalne wymagania w obszarze cyberbezpieczeństwa, w tym w zakresie przetwarzania i przechowywania informacji, systemów i sieci teleinformatycznych, systemów sterowania przemysłowego (OT) oraz przetwarzania danych w chmurze obliczeniowej. Jest to istotne z tego względu, że zakłócenia w cyberprzestrzeni mogą bezpośrednio powodować zakłócenia funkcjonowania infrastruktury krytycznej oraz wywoływać skutki kaskadowe w innych sektorach i podsektorach. Wymagania te odnoszą się do infrastruktury krytycznej jako zasobu materialnego i usługowego, a ich wdrażanie przez operatorów infrastruktury krytycznej odbywa się adekwatnie do wyników analizy zagrożeń.

Jednocześnie projektowane rozporządzenie zachowuje spójność systemową z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zmienionej ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, która wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (dyrektywa NIS 2). Ustawa ta ustanawia obowiązki podmiotów kluczowych i podmiotów ważnych, w szczególności obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji, prowadzenia systematycznego szacowania ryzyka, wdrażania adekwatnych środków technicznych i organizacyjnych, obsługi incydentów, utrzymywania planów ciągłości działania oraz zapewnienia audytu.

W praktyce część operatorów infrastruktury krytycznej (IK) będzie jednocześnie podmiotami kluczowymi w rozumieniu przepisów o krajowym systemie cyberbezpieczeństwa, a część – podmiotami objętymi wymaganiami kontraktowymi lub sektorowymi wynikającymi z funkcjonowania w łańcuchach dostaw usług kluczowych. Z tego względu minimalne

wymagania w rozporządzeniu pełnią funkcję komplementarną: wzmacniają poziom cyberbezpieczeństwa infrastruktury krytycznej, w tym w szczególności w warstwie OT, oraz ułatwiają operatorom infrastruktury krytycznej prawidłowe określanie wymagań wobec dostawców, usługodawców i podwykonawców w sposób ograniczający ryzyko zakłóceń.

IV. W zakresie bezpieczeństwa osobowego projektowane rozporządzenie określa minimalne wymagania dotyczące weryfikacji personelu, zarządzania uprawnieniami oraz organizacji szkoleń, adekwatnie do wyników analizy zagrożeń. Czynnik ludzki stanowi istotny element ryzyka zakłócenia funkcjonowania infrastruktury krytycznej, w szczególności w przypadku osób posiadających dostęp do obszarów chronionych, systemów technicznych i teleinformatycznych oraz informacji wrażliwych. Ujednolicenie minimalnych wymagań w tym zakresie ogranicza ryzyko nadużyć, błędów organizacyjnych oraz nieuprawnionego dostępu, a także zapewnia spójność działań operatorów infrastruktury krytycznej z systemowym podejściem do ochrony i odporności infrastruktury krytycznej.

V. W zakresie bezpieczeństwa prawnego projektowane rozporządzenie określa minimalne wymagania dotyczące zapewnienia zgodności procesów ochrony infrastruktury krytycznej z obowiązującymi przepisami prawa, zabezpieczenia tytułów prawnych do kluczowych zasobów oraz uwzględniania w umowach z dostawcami i usługodawcami postanowień ograniczających ryzyka mogące prowadzić do zakłócenia funkcjonowania infrastruktury krytycznej. Uregulowanie tego obszaru ma na celu ograniczenie ryzyk wynikających z niejednoznacznych relacji kontraktowych, uzależnienia od pojedynczych dostawców, zmian struktury właścicielskiej lub innych działań prawnych podmiotów zewnętrznych, które mogą oddziaływać na ciągłość i bezpieczeństwo infrastruktury krytycznej.

VI. W zakresie ciągłości działania projektowane rozporządzenie określa minimalne wymagania dotyczące planowania, wdrażania, testowania i doskonalenia działań zapewniających zdolność operatora infrastruktury krytycznej do utrzymania oraz odtworzenia realizacji funkcji infrastruktury krytycznej w przypadku wystąpienia zakłóceń. Wymagania te obejmują w szczególności zapewnienie spójnej dokumentacji, analizę wpływu na działania (BIA), określenie parametrów odtwarzania (RTO i RPO) oraz cykliczną weryfikację skuteczności przyjętych rozwiązań. Ujednolicenie minimalnych standardów w tym obszarze, adekwatnie do wyników analizy zagrożeń, wzmacnia odporność infrastruktury krytycznej, ogranicza ryzyko długotrwałych przerw w świadczeniu usług oraz zapewnia spójność działań operatorów w sytuacjach kryzysowych.

Koncepcja minimalnych wymagań była przedmiotem prezentacji i dyskusji w toku licznych wydarzeń branżowych i eksperckich, skierowanych do operatorów infrastruktury krytycznej oraz innych interesariuszy rynku. Proces ten umożliwił weryfikację proponowanych rozwiązań pod kątem ich wykonalności oraz adekwatności do realiów funkcjonowania operatorów infrastruktury krytycznej. Przykładowe wydarzenia, na których była omawiana koncepcja:

- ✓ X Krajowe Forum Ochrony Infrastruktury Krytycznej w dniach 5 października 2023 r.
- ✓ Seminarium „Podnoszenie Cyberodporności u operatorów IK" w dniach 13-14 maja 2024 r.,
- ✓ Ogólnopolski Szczyt Energetyczny w dniu 18 czerwca 2024 r.,
- ✓ VII Międzynarodowego Kongresu Naukowo-Technicznego „Safe Place" w dniu 27 listopada 2024 r.
- ✓ XI Krajowe Forum Ochrony Infrastruktury Krytycznej w dniach 3-4 grudnia 2024 r.
- ✓ Konferencja Defence24 DAYS w dniach 6-7 maja 2025 r.
- ✓ Kongres Sektorowej Rady ds. Kompetencji – Ochrona i Bezpieczeństwo Mienia i Osób w dniu 2 grudnia 2025 r.
- ✓ XII Krajowe Forum Ochrony Infrastruktury Krytycznej w dniach 3-4 grudnia 2025 r.

Projektowane rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia

Projekt rozporządzenia nie podlega notyfikacji zgodnie z przepisami dotyczącymi funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projekt rozporządzenia nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.