2024/1366

24.5.2024

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2024/1366

z dnia 11 marca 2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 z dnia 5 czerwca 2019 r. w sprawie rynku wewnętrznego energii elektrycznej ([1]), w szczególności jego art. 59 ust. 2 lit. e),

a także mając na uwadze, co następuje:

(1) Zarządzanie ryzykiem w cyberprzestrzeni jest kluczowe dla utrzymania bezpieczeństwa dostaw energii elektrycznej i zapewnienia wysokiego poziomu cyberbezpieczeństwa w sektorze energii elektrycznej.

(2) Cyfryzacja i cyberbezpieczeństwo mają decydujące znaczenie dla świadczenia usług kluczowych, a zatem są istotne pod względem strategicznym dla krytycznej infrastruktury energetycznej.

(3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 ([2]) w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/941 ([3]) uzupełnia dyrektywę (UE) 2022/2555 poprzez zapewnienie, aby incydenty w cyberbezpieczeństwie w sektorze energii elektrycznej były odpowiednio identyfikowane jako ryzyko, a środki stosowane w odpowiedzi na nie były właściwie odzwierciedlone w planach gotowości na wypadek zagrożeń. Rozporządzenie (UE) 2019/943 uzupełnia dyrektywę (UE) 2022/2555 i rozporządzenie (UE) 2019/941 poprzez określenie przepisów szczegółowych dotyczących sektora energii elektrycznej na poziomie Unii. Ponadto niniejsze rozporządzenie delegowane uzupełnia przepisy dyrektywy (UE) 2022/2555 dotyczące sektora energii elektrycznej w każdym przypadku związanym z transgranicznymi przepływami energii elektrycznej.

(4) W kontekście wzajemnie powiązanych cyfrowych systemów elektroenergetycznych zapobieganie kryzysom elektroenergetycznym związanym z cyberatakami i zarządzanie nimi nie może być uznawane za zadanie wyłącznie krajowe. Należy w pełni rozwinąć wydajniejsze i mniej kosztowne środki w ramach współpracy regionalnej i unijnej. W związku z tym potrzebne są wspólne ramy zasad i lepiej skoordynowane procedury, aby zapewnić skuteczną transgraniczną współpracę państw członkowskich i innych podmiotów w duchu zwiększonej przejrzystości, zaufania i solidarności między państwami członkowskimi a właściwymi organami odpowiedzialnymi za energię elektryczną i cyberbezpieczeństwo.

(5) Zarządzanie ryzykiem w cyberprzestrzeni wchodzące w zakres niniejszego rozporządzenia wymaga strukturalnego procesu obejmującego między innymi identyfikację ryzyka dla transgranicznych przepływów energii elektrycznej wynikającego z cyberataków, powiązanych procesów i zakresów operacyjnych, odpowiednich mechanizmów kontroli i weryfikacji cyberbezpieczeństwa. Chociaż ramy czasowe całego procesu rozkładają się na lata, każdy z jego etapów powinien przyczynić się do osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w tym sektorze i ograniczenia ryzyka w zakresie cyberbezpieczeństwa. Wszyscy uczestnicy procesu powinni dołożyć wszelkich starań w celu jak najszybszego opracowania i uzgodnienia metod bez zbędnej zwłoki, a w każdym razie nie później niż w terminach określonych w niniejszym rozporządzeniu.

([1]) Dz.U. L 158 z 14.6.2019, s. 54.

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148(dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/941 z dnia 5 czerwca 2019 r. w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej i uchylające dyrektywę 2005/89/WE (Dz.U. L 158 z 14.6.2019, s. 1).

(6) Oceny ryzyka w cyberprzestrzeni na poziomie Unii, państw członkowskich, regionów i podmiotów w niniejszym rozporządzeniu mogą być ograniczone do ocen wynikających z cyberataków zdefiniowanych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554 ([4]), w związku z czym wyklucza się na przykład ataki fizyczne, klęski żywiołowe i wyłączenia spowodowane utratą jednostek lub zasobów ludzkich. Ogólnounijne i regionalne ryzyko związane z atakami fizycznymi lub klęskami żywiołowymi w dziedzinie energii elektrycznej jest już objęte innymi obowiązującymi przepisami Unii, w tym art. 5 rozporządzenia (UE) 2019/941, lub rozporządzeniem Komisji (UE) 2017/1485 ([5]) ustanawiającym wytyczne dotyczące pracy systemu przesyłowego energii elektrycznej. Podobnie dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 ([6]) w sprawie odporności podmiotów krytycznych ma na celu zmniejszenie podatności na zagrożenia i wzmocnienie fizycznej odporności podmiotów krytycznych oraz obejmuje wszystkie istotne czynniki ryzyka, naturalne i spowodowane przez człowieka, które mogą mieć wpływ na świadczenie usług kluczowych, w tym wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego, np. pandemie, oraz zagrożenia hybrydowe lub inne zagrożenia związane z konfliktem, w tym przestępstwa terrorystyczne, infiltrację przestępczą i sabotaż.

(7) Pojęcia „podmioty o dużym wpływie" i „podmioty o krytycznym wpływie" stosowane w niniejszym rozporządzeniu są istotne dla określenia zakresu podmiotów, które będą podlegać obowiązkom opisanym w niniejszym rozporządzeniu. Podejście oparte na analizie ryzyka przedstawione w poszczególnych przepisach ma na celu określenie procesów, aktywów pomocniczych i podmiotów je obsługujących, które mają wpływ na transgraniczne przepływy energii elektrycznej. W zależności od stopnia znaczenia ewentualnych cyberataków dla operacji transgranicznych przepływów energii elektrycznej, można je uznać za podmioty „o dużym wpływie" lub za podmioty „o krytycznym wpływie". W art. 3 dyrektywy (UE) 2022/2555 określono pojęcia podmiotów kluczowych i ważnych oraz kryteria identyfikacji podmiotów należących do tych kategorii. Chociaż wiele z nich zostanie uznanych i zidentyfikowanych jednocześnie jako podmioty „kluczowe" w rozumieniu art. 3 dyrektywy (UE) 2022/2555 oraz podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgodnie z art. 24 niniejszego rozporządzenia, kryteria określone w niniejszym rozporządzeniu odnoszą się wyłącznie do ich roli i znaczenia w procesach związanych z energią elektryczną mających wpływ na przepływy transgraniczne, bez uwzględnienia kryteriów określonych w art. 3 dyrektywy (UE) 2022/2555.

(8) Podmiotami objętymi zakresem niniejszego rozporządzenia, uznawanymi za podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgodnie z art. 24 niniejszego rozporządzenia i podlegającymi obowiązkom w nim określonym, są przede wszystkim te podmioty, które mają bezpośrednie znaczenia dla transgranicznych przepływów energii elektrycznej w UE.

(9) W niniejszym rozporządzeniu wykorzystano istniejące mechanizmy i instrumenty, ustanowione już w innych aktach prawnych, aby zapewnić skuteczność i uniknąć powielania działań w ramach osiągania celów.

(10) Stosując niniejsze rozporządzenie, państwa członkowskie, odpowiednie organy i operatorzy systemów powinni uwzględniać uzgodnione normy europejskie i specyfikacje techniczne europejskich organizacji normalizacyjnych oraz działać zgodnie z przepisami Unii dotyczącymi wprowadzania do obrotu lub oddawania do użytku produktów objętych tymi przepisami Unii.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).

([5]) Rozporządzenie Komisji (UE) 2017/1485 z dnia 2 sierpnia 2017 r. ustanawiające wytyczne dotyczące pracy systemu przesyłowego energii elektrycznej (Dz.U. L 220 z 25.8.2017, s. 1).

([6]) Dyrektywa 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.U. L 333 z 27.12.2022, s. 164).

(11) W celu ograniczenia ryzyka w zakresie cyberbezpieczeństwa konieczne jest ustanowienie zbioru szczegółowych przepisów regulujących działania odpowiednich zainteresowanych stron, których działalność dotyczy aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, i współpracę między tymi stronami, aby zapewnić bezpieczeństwo systemu. Te przepisy organizacyjne i techniczne powinny zapewniać skuteczne reagowanie na szczeblu operacyjnym na większość incydentów związanych z energią elektryczną, których podstawowe przyczyny leżą w dziedzinie cyberbezpieczeństwa. Konieczne jest określenie, co te odpowiednie zainteresowane strony powinny zrobić, aby zapobiec takim kryzysom, oraz jakie środki mogą zastosować w przypadkach, gdy same przepisy dotyczące pracy systemu już nie wystarczają. W związku z tym należy ustanowić wspólne ramy zasad dotyczących sposobów zapobiegania jednoczesnym kryzysom elektroenergetycznym, których podstawową przyczyną jest cyberbezpieczeństwo, przygotowania się na takie kryzysy i zarządzania nimi. Zwiększa to przejrzystość na etapie przygotowań oraz podczas jednoczesnego kryzysu elektroenergetycznego i zapewnia, by środki były stosowane w sposób skoordynowany i efektywny we współpracy z właściwymi organami ds. cyberbezpieczeństwa w państwach członkowskich. Państwa członkowskie i odpowiednie podmioty powinny być zobowiązane do współpracy na szczeblu regionalnym oraz, w stosownych przypadkach, współpracy dwustronnej, w duchu solidarności. Ta współpraca i przepisy mają na celu osiągnięcie lepszej gotowości na wypadek ryzyka w zakresie cyberbezpieczeństwa po niższych kosztach, również zgodnie z celami dyrektywy (UE) 2022/2555. Konieczne wydaje się również wzmocnienie wewnętrznego rynku energii elektrycznej poprzez zwiększenie zaufania we wszystkich państwach członkowskich, w szczególności ograniczenie ryzyka nadmiernego ograniczenia transgranicznych przepływów energii elektrycznej, a tym samym zmniejszenie ryzyka negatywnych skutków ubocznych dla sąsiadujących państw członkowskich.

(12) Bezpieczeństwo dostaw energii elektrycznej wymaga skutecznej współpracy pomiędzy państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz odpowiednimi zainteresowanymi stronami. Operatorzy systemów dystrybucyjnych i operatorzy systemów przesyłowych odgrywają kluczową rolę w zapewnianiu bezpiecznego, niezawodnego i wydajnego systemu elektroenergetycznego zgodnie z art. 31 i 40 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944 ([7]). Poszczególne organy regulacyjne i inne stosowne właściwe organy krajowe również odgrywają ważną rolę w zapewnianiu i monitorowaniu cyberbezpieczeństwa w dostawach energii elektrycznej w ramach zadań powierzonych im w dyrektywie (UE) 2019/944 i dyrektywie (UE) 2022/2555. Państwa członkowskie powinny wyznaczyć istniejący lub nowo powołany podmiot jako właściwy organ krajowy do celów wdrażania niniejszego rozporządzenia, aby zapewnić przejrzysty i sprzyjający włączeniu udział wszystkich zainteresowanych podmiotów, sprawne przygotowanie i właściwe wdrożenie, współpracę między poszczególnymi odpowiednimi zainteresowanymi stronami i właściwymi organami w dziedzinie energii elektrycznej i cyberbezpieczeństwa, a także ułatwić zapobieganie kryzysom elektroenergetycznym, których podstawową przyczyną jest cyberbezpieczeństwo, i ocenę *ex post* tych kryzysów, a także wymianę związanych z nimi informacji.

(13) W przypadku gdy podmiot o dużym wpływie lub podmiot o krytycznym wpływie świadczy usługi w więcej niż jednym państwie członkowskim lub ma siedzibę lub prowadzi działalność, lub ma przedstawiciela w państwie członkowskim, ale jego sieć i systemy informatyczne znajdują się w co najmniej jednym innym państwie członkowskim, te państwa członkowskie powinny zachęcać swoje stosowne właściwe organy do dołożenia wszelkich starań, aby współpracować ze sobą i w razie potrzeby udzielać sobie wzajemnej pomocy.

(14) Państwa członkowskie powinny zapewnić, aby właściwe organy posiadały niezbędne uprawnienia, w odniesieniu do podmiotów o dużym wpływie i podmiotów o krytycznym wpływie, służące propagowaniu zgodności z niniejszym rozporządzeniem. Uprawnienia te powinny umożliwiać właściwym organom przeprowadzanie kontroli na miejscu i nadzoru zdalnego. Może to obejmować wyrywkowe kontrole, przeprowadzanie regularnych audytów, ukierunkowane audyty bezpieczeństwa oparte na ocenach ryzyka lub dostępne informacje dotyczące ryzyka i skany bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka oraz wnioski o udzielenie informacji niezbędnych do oceny środków cyberbezpieczeństwa przyjętych przez podmiot. Wnioski te powinny dotyczyć udokumentowanej polityki cyberbezpieczeństwa, udzielenia dostępu do danych, dokumentów lub informacji koniecznych do wykonywania ich zadań nadzorczych, a także przedstawienia dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz.U. L 158 z 14.6.2019, s. 125).

(15) Aby uniknąć luk w obowiązkach lub powielania obowiązków dotyczących zarządzania ryzykiem w cyberprzestrzeni nałożonych na podmioty o dużym wpływie i podmioty o krytycznym wpływie, organy krajowe na podstawie dyrektywy (UE) 2022/2555 i właściwe organy na podstawie niniejszego rozporządzenia powinny współpracować przy wdrażaniu środków zarządzania ryzykiem w cyberbezpieczeństwie oraz przy nadzorowaniu przestrzegania tych środków na szczeblu krajowym. Spełnienie przez podmiot wymogów w zakresie zarządzania ryzykiem w cyberprzestrzeni określonych w niniejszym rozporządzeniu może zostać uznane przez właściwe organy na podstawie dyrektywy (UE) 2022/2555 za zapewnienie zgodności z odpowiednimi wymogami ustanowionymi w tej dyrektywie lub odwrotnie.

(16) Wspólne podejście do zapobiegania jednoczesnym kryzysom elektroenergetycznym i zarządzania nimi wymaga wspólnego zrozumienia przez państwa członkowskie, na czym polega równoczesny kryzys elektroenergetyczny i kiedy cyberatak jest jego ważnym czynnikiem. W szczególności należy ułatwić koordynację między państwami członkowskimi i odpowiednimi podmiotami w celu zaradzenia sytuacjom, w których ryzyko znacznego niedoboru energii elektrycznej lub braku możliwości dostarczenia jej odbiorcom już istnieje bądź jest nieuchronne, i to z powodu cyberataku.

(17) W motywie 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 ([8]) uznano kluczową rolę sieci i systemów informatycznych oraz sieci i usług łączności elektronicznej w zapewnieniu funkcjonowania gospodarki w kluczowych sektorach, takich jak energetyka, natomiast w motywie 44 wyjaśniono, że Agencja Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA") powinna współpracować z Agencją Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki („ACER").

(18) W rozporządzeniu (UE) 2019/943 operatorom systemów przesyłowych („OSP") i operatorom systemów dystrybucyjnych („OSD") powierzono konkretne obowiązki w zakresie cyberbezpieczeństwa. Ich europejskie stowarzyszenia, a mianowicie europejska sieć operatorów systemów przesyłowych energii elektrycznej („ENTSO energii elektrycznej") i europejska organizacja operatorów systemów dystrybucyjnych („organizacja OSD UE"), wspierają cyberbezpieczeństwo zgodnie z odpowiednio art. 30 i 55 tego rozporządzenia we współpracy z właściwymi organami i podmiotami objętymi regulacją.

(19) Wspólne podejście do zapobiegania jednoczesnym kryzysom elektroenergetycznym, których podstawową przyczyną jest cyberbezpieczeństwo, i zarządzania nimi wymaga również, aby wszystkie odpowiednie zainteresowane strony stosowały zharmonizowane metody i definicje w celu identyfikacji ryzyka związanego z cyberbezpieczeństwem dostaw energii elektrycznej. Wymaga to również możliwości skutecznego porównania swoich wyników oraz wyników swoich sąsiadów w tym zakresie. W związku z tym konieczne jest ustanowienie procesów oraz ról i obowiązków w celu opracowania i aktualizacji metod zarządzania ryzykiem, skali klasyfikacji incydentów i środków cyberbezpieczeństwa dostosowanych do ryzyka w cyberbezpieczeństwie mającego wpływ na transgraniczne przepływy energii elektrycznej.

(20) Państwa członkowskie za pośrednictwem właściwego organu wyznaczonego do celów niniejszego rozporządzenia są odpowiedzialne za identyfikację podmiotów, które spełniają kryteria kwalifikowania się jako podmioty o dużym wpływie i podmioty o krytycznym wpływie. Aby wyeliminować rozbieżności pod tym względem między państwami członkowskimi oraz zapewnić wszystkim podmiotom objętym regulacją pewność prawa w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie i do obowiązków dotyczących zgłaszania incydentów, należy ustanowić jednolite kryterium określające, które podmioty są objęte zakresem stosowania niniejszego rozporządzenia. Ten zestaw kryteriów należy określić i regularnie aktualizować w ramach procesu opracowywania i przyjmowania warunków i metod określonych w niniejszym rozporządzeniu.

(21) Przepisy niniejszego rozporządzenia powinny pozostawać bez uszczerbku dla prawa Unii ustanawiającego przepisy szczegółowe dotyczące certyfikacji produktów technologii informacyjno-komunikacyjnej („ICT"), usług ICT i procesów ICT, w szczególności bez uszczerbku dla rozporządzenia (UE) 2019/881 w odniesieniu do ram ustanowienia europejskich programów certyfikacji cyberbezpieczeństwa. W kontekście niniejszego rozporządzenia produkty ICT powinny obejmować również urządzenia techniczne i oprogramowanie umożliwiające bezpośrednią interakcję z siecią elektrotechniczną, w szczególności przemysłowe systemy sterowania, które mogą być wykorzystywane do przesyłu energii, dystrybucji i wytwarzania energii, a także do gromadzenia i przekazywania związanych z tym informacji. Przepisy te powinny zapewniać, aby produkty ICT, usługi ICT i procesy ICT, które mają być zamawiane, spełniały odpowiednie cele w zakresie bezpieczeństwa określone w art. 51 rozporządzenia (UE) 2019/881.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

(22) Niedawne cyberataki wskazują, że podmioty w coraz większym stopniu stają się celem ataków w łańcuchu dostaw. Takie ataki w łańcuchu dostaw nie tylko mają wpływ na poszczególne podmioty objęte zakresem stosowania, lecz także mogą wywołać efekt kaskadowy w postaci większych ataków na podmioty, do których są one podłączone w sieci elektroenergetycznej. W związku z tym dodano przepisy i zalecenia mające pomóc w łagodzeniu ryzyka w cyberprzestrzeni związanego z procesami dotyczącymi łańcucha dostaw, w szczególności zamówień publicznych, które mają wpływ na transgraniczne przepływy energii elektrycznej.

(23) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia w dostawie energii i szkody dla gospodarki oraz konsumentów, należy szybko identyfikować te podatności i eliminować je w celu ograniczenia ryzyka. Aby ułatwić skuteczne wdrożenie niniejszego rozporządzenia, odpowiednie podmioty i właściwe organy powinny współpracować w zakresie prowadzenia ćwiczeń i testów, które uznaje się za odpowiednie do tego celu, w tym wymiany informacji na temat cyberzagrożeń, cyberataków, podatności, narzędzi i metod, taktyki, technik i procedur, gotowości w zakresie zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa i innych ćwiczeń. Ponieważ technologia stale się rozwija, a cyfryzacja sektora energii elektrycznej postępuje szybko, wdrażanie przyjętych przepisów nie powinno szkodzić innowacjom i nie powinno stanowić bariery w dostępie do rynku energii elektrycznej i późniejszego stosowania innowacyjnych rozwiązań, które przyczyniają się do efektywności i zrównoważonego charakteru systemu elektroenergetycznego.

(24) Informacje gromadzone na potrzeby monitorowania wdrażania niniejszego rozporządzenia powinny być racjonalnie ograniczone zgodnie z zasadą ograniczonego dostępu. Zainteresowanym stronom należy wyznaczyć możliwe do zachowania i skuteczne terminy przekazywania takich informacji. Należy unikać podwójnego powiadamiania.

(25) Ochrona w zakresie cyberbezpieczeństwa nie kończy się na granicach Unii. Bezpieczny system wymaga zaangażowania sąsiadujących państw trzecich. Unia i jej państwa członkowskie powinny dążyć do wspierania sąsiadujących państw trzecich, których infrastruktura elektroenergetyczna jest podłączona do sieci europejskiej, w stosowaniu przepisów dotyczących cyberbezpieczeństwa analogicznych z przepisami określonymi w niniejszym rozporządzeniu.

(26) Aby poprawić koordynację bezpieczeństwa na wczesnym etapie, przetestować przyszłe wiążące warunki i metody, ENTSO energii elektrycznej, organizacja OSD UE i właściwe organy powinny rozpocząć opracowywanie niewiążących wytycznych niezwłocznie po wejściu w życie niniejszego rozporządzenia. Wytyczne te posłużą jako punkt odniesienia dla opracowania przyszłych warunków i metod. Jednocześnie właściwe organy powinny wskazać podmioty jako kandydatów do miana podmiotów o dużym wpływie i podmiotów o krytycznym wpływie, aby dobrowolnie rozpoczęły wypełnianie obowiązków.

(27) Niniejsze rozporządzenie zostało opracowane w ścisłej współpracy z ACER, ENISA, ENTSO energii elektrycznej, organizacją OSD UE i innymi zainteresowanymi podmiotami w celu przyjęcia skutecznych, zrównoważonych i proporcjonalnych przepisów w przejrzysty i partycypacyjny sposób.

(28) Niniejsze rozporządzenie uzupełnia i wzmacnia środki zarządzania kryzysowego ustanowione w unijnych ramach reagowania w sytuacji kryzysu cyberbezpieczeństwa określone w zaleceniu Komisji (UE) 2017/1584 ([9]). Cyberatak może ponadto spowodować kryzys elektroenergetyczny zdefiniowany w art. 2 pkt 9 rozporządzenia (UE) 2019/941, który ma wpływ na transgraniczne przepływy energii elektrycznej, przyczynić się do takiego kryzysu lub zbiec się z nim. Ten kryzys elektroenergetyczny może prowadzić do jednoczesnego kryzysu elektroenergetycznego zdefiniowanego w art. 2 pkt 10 rozporządzenia (UE) 2019/941. Taki incydent mógłby mieć wpływ również na inne sektory zależne od bezpieczeństwa dostaw energii elektrycznej. Jeżeli taki incydent przerodzi się w incydent w cyberbezpieczeństwie na dużą skalę w rozumieniu art. 16 dyrektywy (UE) 2022/2555 zastosowanie powinny mieć przepisy tego artykułu ustanawiające europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe"). W odniesieniu do zarządzania kryzysowego na szczeblu unijnym odpowiednie strony powinny opierać się na zintegrowanych uzgodnieniach UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych („uzgodnienia IPCR") na podstawie decyzji wykonawczej Rady (UE) 2018/1993 ([10]).

(29) Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji państw członkowskich w zakresie przedsięwzięcia środków niezbędnych do zapewnienia ochrony podstawowych interesów ich bezpieczeństwa, do ochrony polityki i bezpieczeństwa publicznego oraz do umożliwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw zgodnie z prawem Unii. Zgodnie z art. 346 TFUE żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa.

([9]) Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

([10]) Decyzja wykonawcza Rady (UE) 2018/1993 z dnia 11 grudnia 2018 r. w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (Dz.U. L 320 z 17.12.2018, s. 28).

(30) Mimo iż niniejsze rozporządzenie ma zasadniczo zastosowanie do podmiotów prowadzących działalność w zakresie wytwarzania energii elektrycznej w elektrowniach jądrowych, niektóre rodzaje takiej działalności mogą być powiązane z bezpieczeństwem narodowym.

(31) Do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia zastosowanie powinny mieć unijne przepisy dotyczące ochrony danych oraz unijne przepisy dotyczące prywatności. W szczególności niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([11]), dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady ([12]) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([13]). Niniejsze rozporządzenie nie powinno zatem wpływać między innymi na zadania i uprawnienia organów właściwych do spraw monitorowania zgodności z obowiązującymi unijnymi przepisami dotyczącymi ochrony danych i unijnymi przepisami dotyczącymi ochrony prywatności.

(32) Biorąc pod uwagę znaczenie współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa, właściwe organy odpowiedzialne za wykonywanie zadań powierzonych im na mocy niniejszego rozporządzenia i wyznaczone przez państwa członkowskie powinny mieć możliwość uczestnictwa w międzynarodowych sieciach współpracy. W związku z tym do celów wykonywania swoich zadań właściwe organy powinny mieć możliwość wymiany informacji, w tym danych osobowych, z właściwymi organami państw trzecich, pod warunkiem że spełnione są warunki określone w unijnych przepisach dotyczących ochrony danych odnoszące się do przekazywania danych osobowych do państw trzecich, między innymi warunki określone w art. 49 rozporządzenia (UE) 2016/679.

(33) Przetwarzanie danych osobowych, w zakresie, w jakim jest to konieczne i proporcjonalne do zapewnienia bezpieczeństwa aktywów przez podmioty o dużym wpływie lub podmioty o krytycznym wpływie można uznać za zgodne z prawem na podstawie tego, że takie przetwarzanie jest zgodne z obowiązkiem prawnym, któremu podlega administrator, zgodnie z wymogami art. 6 ust. 1 lit. c) i art. 6 ust. 3 rozporządzenia (UE) 2016/679. Przetwarzanie danych osobowych może być również konieczne ze względu na uzasadnione interesy podmiotów o dużym wpływie lub podmiotów o krytycznym wpływie, a także dostawców technologii i usług w zakresie bezpieczeństwa działających w imieniu tych podmiotów, zgodnie z art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679, w tym w przypadku gdy takie przetwarzanie jest niezbędne w związku z mechanizmami wymiany informacji o cyberbezpieczeństwie lub do dobrowolnego zgłaszania odpowiednich informacji zgodnie z niniejszym rozporządzeniem. Środki związane z zapobieganiem cyberatakom, ich wykrywaniem i identyfikacją, ograniczaniem ich zasięgu i ich analizowaniem oraz reagowaniem na nie, środki zwiększające świadomość konkretnych cyberzagrożeń, wymianę informacji w kontekście usuwania oraz skoordynowanego ujawniania podatności, dobrowolną wymianę informacji na temat tych cyberataków, a także na temat cyberzagrożeń i podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, ostrzeżeń dotyczących cyberbezpieczeństwa i narzędzi konfiguracji mogą wymagać przetwarzania pewnych kategorii danych osobowych, takich jak adresy IP, ujednolicone formaty adresowania zasobów (URL), nazwy domen, adresy poczty elektronicznej oraz znaczniki czasu, w przypadku gdy ujawniane są w nich dane osobowe. Przetwarzanie danych osobowych przez właściwe organy, pojedyncze punkty kontaktowe i CSIRT może stanowić obowiązek prawny lub może zostać uznane za niezbędne do wykonania zadania w interesie publicznym lub sprawowania władzy publicznej powierzonej administratorowi na podstawie art. 6 ust. 1 lit. c) lub e) i art. 6 ust. 3 rozporządzenia (UE) 2016/679 lub do realizacji uzasadnionego interesu podmiotów o dużym wpływie lub podmiotów o krytycznym wpływie, o którym mowa w art. 6 ust. 1 lit. f) tego rozporządzenia. Ponadto w prawie krajowym można ustanowić przepisy umożliwiające właściwym organom, pojedynczym punktom kontaktowym i CSIRT – w zakresie, w jakim jest to konieczne i proporcjonalne do zapewnienia bezpieczeństwa sieci i systemów informatycznych podmiotów o dużym wpływie lub podmiotów o krytycznym wpływie – przetwarzanie szczególnych kategorii danych osobowych zgodnie z art. 9 rozporządzenia (UE) 2016/679, w szczególności poprzez ustanowienie odpowiednich i konkretnych środków ochrony praw podstawowych i interesów osób fizycznych, w tym ograniczeń technicznych w zakresie ponownego wykorzystywania takich danych oraz stosowania najnowocześniejszych środków bezpieczeństwa i ochrony prywatności, takich jak pseudonimizacja lub szyfrowanie, jeżeli anonimizacja może mieć znaczący wpływ na zamierzony cel.

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([12]) Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

([13]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

(34) W wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych w wyniku cyberataków. W tym kontekście właściwe organy powinny współpracować oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii z organami, o których mowa w rozporządzeniu (UE) 2016/679 i dyrektywie 2002/58/WE.

(35) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych; swoją opinię wydał on w dniu 17 listopada 2023 r.,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się kodeks sieci określający zasady sektorowe dotyczące aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, w tym zasady dotyczące wspólnych wymogów minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego.

Artykuł 2

Zakres

1. Niniejsze rozporządzenie ma zastosowanie do aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej w ramach działalności następujących podmiotów, jeżeli zostały one zidentyfikowane jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgodnie z art. 24:

a) przedsiębiorstw energetycznych zdefiniowanych w art. 2 pkt 57 dyrektywy (UE) 2019/944;

b) wyznaczonych operatorów rynku energii elektrycznej („NEMO") zdefiniowanych w art. 2 pkt 8 rozporządzenia (UE) 2019/943;

c) zorganizowanych platform obrotu lub „rynków zorganizowanych" zdefiniowanych w art. 2 pkt 4 rozporządzenia wykonawczego Komisji (UE) nr 1348/2014 ([14]), które organizują transakcje dotyczące produktów istotnych dla transgranicznych przepływów energii elektrycznej;

d) kluczowych dostawców usług ICT, o których mowa w art. 3 pkt 9 niniejszego rozporządzenia;

e) ENTSO energii elektrycznej ustanowionej na podstawie art. 28 rozporządzenia (UE) 2019/943;

f) organizacji OSD UE ustanowionej na podstawie art. 52 rozporządzenia (UE) 2019/943;

g) podmiotów odpowiedzialnych za bilansowanie zdefiniowanych w art. 2 pkt 14 rozporządzenia (UE) 2019/943;

h) operatorów punktów ładowania zdefiniowanych w załączniku I do dyrektywy (UE) 2022/2555;

i) regionalnych centrów koordynacyjnych ustanowionych na podstawie art. 35 rozporządzenia (UE) 2019/943;

j) dostawców usług zarządzanych w zakresie bezpieczeństwa zdefiniowanych w art. 6 pkt 40 dyrektywy (UE) 2022/2555;

k) wszelkich innych podmiotów lub osób trzecich, którym przekazano lub powierzono obowiązki na podstawie niniejszego rozporządzenia.

2. Za wykonywanie zadań powierzonych w niniejszym rozporządzeniu odpowiedzialne są następujące organy w ramach ich obecnych mandatów:

a) Agencja Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki („ACER") ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/942 ([15]);

b) właściwe organy krajowe odpowiedzialne za wykonywanie zadań powierzonych im na podstawie niniejszego rozporządzenia i wyznaczone przez państwa członkowskie na podstawie art. 4 lub „właściwe organy";

c) krajowe organy regulacyjne wyznaczone przez każde państwo członkowskie zgodnie z art. 57 ust. 1 dyrektywy (UE) 2019/944;

([14]) Rozporządzenie wykonawcze Komisji (UE) nr 1348/2014 z dnia 17 grudnia 2014 r. w sprawie przekazywania danych wdrażające art. 8 ust. 2 i 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1227/2011 w sprawie integralności i przejrzystości hurtowego rynku energii (Dz.U. L 363 z 18.12.2014, s. 121).

([15]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/942 z dnia 5 czerwca 2019 r. ustanawiające Agencję Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki (Dz.U. L 158 z 14.6.2019, s. 22).

d) właściwe organy ds. gotowości na wypadek zagrożeń ustanowione na podstawie art. 3 rozporządzenia (UE) 2019/941;

e) zespoły reagowania na incydenty bezpieczeństwa komputerowego („CSIRT") wyznaczone lub ustanowione na podstawie art. 10 dyrektywy (UE) 2022/2555;

f) właściwe organy odpowiedzialne za cyberbezpieczeństwo wyznaczone lub ustanowione na podstawie art. 8 dyrektywy (UE) 2022/2555;

g) Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ustanowiona na podstawie rozporządzenia (UE) 2019/881;

h) wszelkie inne organy lub osoby trzecie, którym przekazano lub powierzono obowiązki na podstawie art. 4 ust. 3.

3. Niniejsze rozporządzenie ma również zastosowanie do wszystkich podmiotów, które nie mają siedziby w Unii, ale świadczą usługi na rzecz podmiotów w Unii, pod warunkiem że zostały one zidentyfikowane przez właściwe organy jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgodnie z art. 24 ust. 2.

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla spoczywającego na państwach członkowskich obowiązku ochrony bezpieczeństwa narodowego oraz dla ich uprawnień do zabezpieczania innych podstawowych funkcji państwa, w tym zapewniania integralności terytorialnej państwa i utrzymywania porządku publicznego.

5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla odpowiedzialności państw członkowskich za zagwarantowanie bezpieczeństwa narodowego w odniesieniu do działań związanych z wytwarzaniem energii elektrycznej z elektrowni jądrowych, w tym działań w ramach łańcucha wartości sektora jądrowego, zgodnie z Traktatami.

6. Podmioty, właściwe organy, pojedyncze punkty kontaktowe na poziomie podmiotu i CSIRT przetwarzają dane osobowe w zakresie niezbędnym do celów niniejszego rozporządzenia i zgodnie z rozporządzeniem (UE) 2016/679, w szczególności takie przetwarzanie odbywa się na podstawie jego art. 6.

Artykuł 3

Definicje

Stosuje się następujące definicje:

1) „aktywa" oznaczają wszelkie informacje, oprogramowanie lub sprzęt w sieci i systemach informatycznych, materialne lub niematerialne, które mają wartość dla osoby fizycznej, organizacji lub rządu;

2) „właściwy organ ds. gotowości na wypadek zagrożeń" oznacza właściwy organ wyznaczony zgodnie z art. 3 rozporządzenia (UE) 2019/941;

3) „zespół reagowania na incydenty bezpieczeństwa komputerowego" oznacza zespół odpowiedzialny za postępowanie w przypadku wystąpienia ryzyka i incydentów zgodnie z art. 10 dyrektywy (UE) 2022/2555;

4) „aktywa o krytycznym wpływie" oznaczają aktywa, które są niezbędne do przeprowadzenia procesu o krytycznym wpływie;

5) „podmiot o krytycznym wpływie" oznacza podmiot, który przeprowadza proces o krytycznym wpływie i który został zidentyfikowany przez właściwe organy zgodnie z art. 24;

6) „obszar o krytycznym wpływie" oznacza obszar określony przez podmiot, o którym mowa w art. 2 ust. 1, obejmujący wszystkie aktywa o krytycznym wpływie i na którym można kontrolować dostęp do tych aktywów i który określa zakres stosowania zaawansowanych kontroli cyberbezpieczeństwa;

7) „proces o krytycznym wpływie" oznacza proces biznesowy przeprowadzany przez podmiot, w przypadku którego wskaźniki wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej przekraczają próg krytycznego wpływu;

8) „próg krytycznego wpływu" oznacza wartości wskaźników wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej, o których mowa w art. 19 ust. 3 lit. b), powyżej których cyberatak na proces biznesowy spowoduje krytyczne zakłócenie transgranicznych przepływów energii elektrycznej;

9) „kluczowy dostawca usług ICT" oznacza podmiot świadczący usługę ICT lub realizujący proces ICT, które są niezbędne do przeprowadzenia procesu o krytycznym wpływie lub procesu o dużym wpływie dla aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej i które, jeśli zostaną zagrożone, mogą spowodować cyberatak o znaczeniu przekraczającym próg krytycznego wpływu lub próg dużego wpływu;

10) „transgraniczny przepływ energii elektrycznej" oznacza przepływ transgraniczny zdefiniowany w art. 2 pkt 3 rozporządzenia (UE) 2019/943;

11) „cyberatak" oznacza incydent zdefiniowany w art. 3 pkt 14 rozporządzenia (UE) 2022/2554;

12) „cyberbezpieczeństwo" oznacza cyberbezpieczeństwo zdefiniowane w art. 2 pkt 1 rozporządzenia (UE) 2019/881;

13) „kontrola cyberbezpieczeństwa” oznacza działania lub procedury przeprowadzane w celu uniknięcia i wykrywania ryzyka w cyberbezpieczeństwie, przeciwdziałania mu lub minimalizowania go;

14) „incydent w cyberbezpieczeństwie” oznacza incydent zdefiniowany w art. 6 pkt 6 dyrektywy (UE) 2022/2555;

15) „system zarządzania cyberbezpieczeństwem” oznacza politykę, procedury, wytyczne oraz powiązane zasoby i działania, zarządzane łącznie przez podmiot, służące ochronie jego zasobów informacyjnych przed cyberzagrożeniami poprzez systematyczne ustanawianie, wdrażanie, obsługę, monitorowanie, przeglądy, utrzymywanie i poprawę bezpieczeństwa sieci i systemów informatycznych organizacji;

16) „centrum operacyjne cyberbezpieczeństwa” oznacza specjalne centrum, w którym zespół techniczny składający się z co najmniej jednego eksperta, korzystający z systemów informatycznych w zakresie cyberbezpieczeństwa, wykonuje zadania związane z bezpieczeństwem (usługi centrum operacyjnego cyberbezpieczeństwa), takie jak postępowanie w przypadku cyberataków i błędów konfiguracji bezpieczeństwa, monitorowanie bezpieczeństwa, analiza dzienników i wykrywanie cyberataków;

17) „cyberzagrożenie” oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

18) „zarządzanie podatnościami wpływającymi na cyberbezpieczeństwo” oznacza praktykę identyfikowania i eliminowania podatności;

19) „podmiot” oznacza podmiot zdefiniowany w art. 6 pkt 38 dyrektywy (UE) 2022/2555;

20) „wczesne ostrzeżenie” oznacza informacje niezbędne do wskazania, czy istnieje podejrzenie, że poważny incydent jest spowodowany czynami niezgodnymi z prawem lub popełnionymi w złym zamiarze, oraz czy może on mieć skutki transgraniczne;

21) „wskaźnik wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej” („ECII”) oznacza wskaźnik lub skalę klasyfikacji, która klasyfikuje potencjalne konsekwencje cyberataków dla procesów biznesowych związanych z transgranicznymi przepływami energii elektrycznej;

22) „europejski program certyfikacji cyberbezpieczeństwa” oznacza program zdefiniowany w art. 2 pkt 9 rozporządzenia (UE) 2019/881;

23) „podmiot o dużym wpływie” oznacza podmiot, który przeprowadza proces o dużym wpływie i który został zidentyfikowany przez właściwe organy zgodnie z art. 24;

24) „proces o dużym wpływie” oznacza proces biznesowy przeprowadzany przez podmiot, w przypadku którego wskaźniki wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej przekraczają próg dużego wpływu;

25) „aktywa o dużym wpływie” oznaczają aktywa, które są niezbędne do przeprowadzenia procesu o dużym wpływie;

26) „próg dużego wpływu” oznacza wartości wskaźników wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej, o których mowa w art. 19 ust. 3 lit. b), powyżej których skuteczny cyberatak na proces spowoduje duże zakłócenie transgranicznych przepływów energii elektrycznej;

27) „obszar o dużym wpływie” oznacza obszar określony przez dowolny podmiot wymieniony w art. 2 ust. 1, obejmujący wszystkie aktywa o dużym wpływie, na którym można kontrolować dostęp do tych aktywów i który określa zakres stosowania minimalnych kontroli cyberbezpieczeństwa;

28) „produkt ICT” oznacza produkt ICT zdefiniowany w art. 2 pkt 12 rozporządzenia (UE) 2019/881;

29) „usługa ICT” oznacza usługę ICT zdefiniowaną w art. 2 pkt 13 rozporządzenia (UE) 2019/881;

30) „proces ICT” oznacza proces ICT zdefiniowany w art. 2 pkt 14 rozporządzenia (UE) 2019/881;

31) „dotychczasowy system” oznacza dotychczasowy system ICT zdefiniowany w art. 3 pkt 3 rozporządzenia (UE) 2022/2554;

32) „krajowy pojedynczy punkt kontaktowy” oznacza pojedynczy punkt kontaktowy wyznaczony lub ustanowiony przez każde państwo członkowskie na podstawie art. 8 ust. 3 dyrektywy (UE) 2022/2555;

33) „organy ds. zarządzania kryzysowego w cyberbezpieczeństwie w ramach NIS” oznaczają organy wyznaczone lub ustanowione na podstawie art. 9 ust. 1 dyrektywy (UE) 2022/2555;

34) „inicjator” oznacza podmiot inicjujący wymianę informacji, udostępnienie informacji lub przechowywanie informacji;

35) „specyfikacje zamówień publicznych” oznaczają specyfikacje określone przez podmioty na potrzeby zamówień na nowe lub zaktualizowane produkty ICT, procesy ICT lub usługi ICT;

36) „przedstawiciel” oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub miejsce prowadzenia działalności w Unii, wyraźnie wyznaczoną do występowania w imieniu podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie niemającego miejsca prowadzenia działalności w Unii, ale świadczącego usługi na rzecz podmiotów w Unii, do której właściwy organ krajowy lub CSIRT może się zwrócić zamiast do samego podmiotu o dużym lub krytycznym wpływie w związku z obowiązkami tego podmiotu przewidzianymi w niniejszym rozporządzeniu;

37) „ryzyko” oznacza ryzyko zgodnie z definicją w art. 6 pkt 9 dyrektywy (UE) 2022/2555;

38) „macierz wpływu ryzyka” oznacza matrycę wykorzystywaną podczas oceny ryzyka do określenia wynikającego z niej poziomu wpływu ryzyka dla każdego ocenianego rodzaju ryzyka;

39) „jednoczesny kryzys elektroenergetyczny” oznacza kryzys elektroenergetyczny zdefiniowany w art. 2 pkt 10 rozporządzenia (UE) 2019/941;

40) „pojedynczy punkt kontaktowy na poziomie podmiotu” oznacza pojedynczy punkt kontaktowy na poziomie podmiotu wyznaczony zgodnie z art. 38 ust. 1 lit. c);

41) „zainteresowana strona” oznacza każdą stronę, która jest zainteresowana powodzeniem i bieżącym funkcjonowaniem organizacji lub procesu, taką jak pracownicy, dyrektorzy, udziałowcy, organy regulacyjne, stowarzyszenia, dostawcy i klienci;

42) „norma” oznacza normę zdefiniowaną w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([16]);

43) „region pracy systemu” oznacza regiony pracy systemu określone w załączniku I do decyzji ACER 05-2022 w sprawie określenia regionów pracy systemu, ustanowione zgodnie z art. 36 rozporządzenia (UE) 2019/943;

44) „operator systemu” oznacza „operatora systemu dystrybucyjnego” (OSD) i „operatora systemu przesyłowego” (OSP) zdefiniowanego w art. 2 pkt 29 i art. 2 pkt 35 dyrektywy (UE) 2019/944;

45) „ogólnounijny proces o krytycznym wpływie” oznacza dowolny proces w sektorze energii elektrycznej, potencjalnie obejmujący więcej niż jeden podmiot, w przypadku którego ewentualny wpływ cyberataku można uznać za krytyczny podczas przeprowadzania ogólnounijnej oceny ryzyka w cyberprzestrzeni;

46) „ogólnounijny proces o dużym wpływie” oznacza dowolny proces w sektorze energii elektrycznej, potencjalnie obejmujący więcej niż jeden podmiot, w przypadku którego ewentualne wpływ cyberataku można uznać za duży podczas przeprowadzania ogólnounijnej oceny ryzyka w cyberprzestrzeni;

47) „nienaprawiona aktywnie wykorzystywana podatność” oznacza podatność, która nie została jeszcze ujawniona publicznie i naprawiona i w odniesieniu do której istnieją wiarygodne dowody na to, że podmiot wykonał złośliwy kod w systemie bez zgody właściciela systemu;

48) „podatność” oznacza podatność zdefiniowaną w art. 6 pkt 15 dyrektywy (UE) 2022/2555.

Artykuł 4

Właściwy organ

1. Najwcześniej jak to możliwe i nie później niż do dnia 13 grudnia 2024 r. każde państwo członkowskie wyznacza krajowy organ rządowy lub regulacyjny odpowiedzialny za wykonywanie zadań powierzonych mu na mocy niniejszego rozporządzenia („właściwy organ”). Do czasu powierzenia właściwemu organowi zadań wynikających z niniejszego rozporządzenia zadania właściwego organu zgodnie z niniejszym rozporządzeniem wykonuje organ regulacyjny wyznaczony przez każde państwo członkowskie na podstawie art. 57 ust. 1 dyrektywy (UE) 2019/944.

2. Państwa członkowskie niezwłocznie powiadamiają Komisję, ACER, ENISA, grupę współpracy NIS ustanowioną na podstawie art. 14 dyrektywy (UE) 2022/2555 oraz Grupę Koordynacyjną ds. Energii Elektrycznej ustanowioną na mocy art. 1 decyzji Komisji z dnia 15 listopada 2012 r. ([17]) oraz przekazują im nazwę i dane kontaktowe swojego właściwego organu wyznaczonego zgodnie z ust. 1 niniejszego artykułu oraz informują o wszelkich późniejszych zmianach w tym względzie.

([16]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

([17]) Decyzja Komisji z dnia 15 listopada 2012 r. ustanawiająca Grupę Koordynacyjną ds. Energii Elektrycznej (2012/C 353/02) (Dz.U. C 353 z 17.11.2012, s. 2).

3. Państwa członkowskie mogą zezwolić swojemu właściwemu organowi na przekazywanie zadań powierzonych mu w niniejszym rozporządzeniu innym organom krajowym, z wyjątkiem zadań wymienionych w art. 5. Każdy właściwy organ monitoruje stosowanie niniejszego rozporządzenia przez organy, którym przekazał zadania. Właściwy organ przekazuje Komisji, ACER, Grupie Koordynacyjnej ds. Energii Elektrycznej, ENISA oraz grupie współpracy NIS nazwę, dane kontaktowe, informacje o przydzielonych zadaniach oraz wszelkie późniejsze zmiany w tym względzie.

Artykuł 5

Współpraca między właściwymi organami i podmiotami na szczeblu krajowym

Właściwe organy koordynują i zapewniają odpowiednią współpracę między właściwymi organami odpowiedzialnymi za cyberbezpieczeństwo, organami ds. zarządzania kryzysowego w cyberbezpieczeństwie, krajowymi organami regulacyjnymi, właściwymi organami ds. gotowości na wypadek zagrożeń i CSIRT w celu wypełnienia stosownych obowiązków określonych w niniejszym rozporządzeniu. Właściwe organy koordynują również współpracę z wszystkimi innymi podmiotami lub organami określonymi przez każde państwo członkowskie, aby zapewnić skuteczne procedury i uniknąć powielania zadań i obowiązków. Właściwe organy muszą mieć możliwość polecenia odpowiednim krajowym organom regulacyjnym zwrócenia się do ACER o opinię zgodnie z art. 8 ust. 3.

Artykuł 6

Warunki lub metody, lub plany

1. OSP opracowują, we współpracy z organizacją OSD UE, propozycje dotyczące warunków lub metod zgodnie z ust. 2 lub planów zgodnie z ust. 3.

2. Poniższe warunki lub metody oraz wszelkie ich zmiany podlegają zatwierdzeniu przez wszystkie właściwe organy:

a) metody oceny ryzyka w cyberprzestrzeni zgodnie z art. 18 ust. 1;

b) kompleksowe sprawozdanie z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej zgodnie z art. 23;

c) minimalne i zaawansowane kontrole cyberbezpieczeństwa na podstawie art. 29, mapowanie kontroli cyberbezpieczeństwa w odniesieniu do energii elektrycznej względem norm na podstawie art. 34, w tym minimalne i zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw zgodnie z art. 33;

d) zalecenie dotyczące zamówień publicznych w dziedzinie cyberbezpieczeństwa zgodnie z art. 35;

e) metodyka określania skali klasyfikacji cyberataków zgodnie z art. 37 ust. 8.

3. Propozycje dotyczące regionalnych planów ograniczenia ryzyka w cyberprzestrzeni zgodnie z art. 22 podlegają zatwierdzeniu przez wszystkie właściwe organy regionu pracy systemu, którego to dotyczy.

4. Propozycje dotycząca ustanowienia warunków i metod wymienionych w ust. 2 lub planów, o których mowa w ust. 3, muszą obejmować proponowane ramy czasowe ich wdrożenia oraz opis ich przewidywanego wpływu na realizację celów określonych w niniejszym rozporządzeniu.

5. Organizacja OSD UE może przedstawić OSP, których to dotyczy, uzasadnioną opinię najpóźniej na trzy tygodnie przed upływem terminu przedłożenia właściwym organom propozycji dotyczącej ustanowienia warunków lub metod, lub planów. Przed przedłożeniem propozycji dotyczącej ustanowienia warunków lub metod, lub planów właściwym organom do zatwierdzenia OSP odpowiedzialni za propozycję uwzględniają uzasadnioną opinię organizacji OSD UE. Jeżeli opinia organizacji OSD UE nie zostanie uwzględniona, OSP muszą podać uzasadnienie.

6. Uczestniczący OSP ściśle ze sobą współpracują przy wspólnym opracowywaniu warunków, metod i planów. OSP, z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, regularnie informują właściwe organy i ACER o postępach w opracowywaniu warunków lub metod, lub planów.

Artykuł 7

Zasady głosowania w ramach OSP

1. Jeżeli OSP podejmujący decyzję w sprawie propozycji dotyczących ustanowienia warunków lub metod nie są w stanie osiągnąć porozumienia, podejmują oni decyzję kwalifikowaną większością głosów. Większość kwalifikowaną w przypadku takich propozycji oblicza się w następujący sposób:

a) OSP reprezentujących co najmniej 55 % państw członkowskich; oraz

b) OSP reprezentujących państwa członkowskie, których liczba mieszkańców stanowi co najmniej 65 % ludności Unii.

2. Przy podejmowaniu decyzji w sprawie propozycji dotyczących ustanowienia warunków lub metod wymienionych w art. 6 ust. 2 mniejszość blokująca musi obejmować OSP reprezentujących co najmniej cztery państwa członkowskie; w przypadku niespełnienia powyższego warunku uznaje się, że większość kwalifikowana została osiągnięta.

3. Jeżeli OSP regionu pracy systemu podejmujący decyzję w sprawie propozycji dotyczących ustanowienia planów wymienionych w art. 6 ust. 2 nie są w stanie osiągnąć porozumienia oraz jeżeli dany region pracy systemu obejmuje więcej niż pięć państw członkowskich, podejmują oni decyzję kwalifikowaną większością głosów. W przypadku propozycji wymienionych w art. 6 ust. 2 większość kwalifikowana oznacza następującą większość:

a) OSP reprezentujących co najmniej 72 % zainteresowanych państw członkowskich; oraz

b) OSP reprezentujących państwa członkowskie, na których terytorium zamieszkuje co najmniej 65 % ludności obszaru, którego to dotyczy.

4. Przy podejmowaniu decyzji w sprawie propozycji dotyczących ustanowienia planów mniejszość blokująca musi obejmować co najmniej minimalną liczbę OSP reprezentujących ponad 35 % ludności uczestniczących państw członkowskich, a także OSP reprezentujących co najmniej jedno dodatkowe zainteresowane państwo członkowskie; w przypadku niespełnienia powyższego warunku uznaje się, że większość kwalifikowana została osiągnięta.

5. W przypadku decyzji podejmowanych przez OSP w sprawie propozycji dotyczących ustanowienia warunków lub metod zgodnie z art. 6 ust. 2 każdemu państwu członkowskiemu przysługuje jeden głos. W przypadku występowania na terytorium danego państwa członkowskiego więcej niż jednego OSP państwo członkowskie rozdziela uprawnienia do głosowania wśród OSP.

6. Jeżeli OSP, we współpracy z organizacją OSD UE, nie przedstawią odpowiednim właściwym organom wstępnej lub zmienionej propozycji dotyczącej ustanowienia warunków lub metod lub planów w terminach określonych w niniejszym rozporządzeniu, przekazują odpowiednim właściwym organom i ACER stosowne projekty warunków lub metod, lub planów. Wyjaśniają one, co uniemożliwiło osiągnięcie porozumienia. Właściwe organy wspólnie podejmują odpowiednie kroki w celu przyjęcia wymaganych warunków lub metod, lub wymaganych planów. Można tego dokonać na przykład poprzez zwrócenie się o wprowadzenie zmian do projektów zgodnie z niniejszym ustępem, zmianę i uzupełnienie tych projektów lub, w przypadku gdy nie przedstawiono projektów, określenie i zatwierdzenie wymaganych warunków lub metod lub planów.

Artykuł 8

Przedkładanie propozycji właściwym organom

1. OSP przedkładają propozycje dotyczące ustanowienia warunków lub metod, lub planów odpowiednim właściwym organom do zatwierdzenia w stosownych terminach określonych w art. 18, 23, 29, 33, 34, 35 i 37. W wyjątkowych okolicznościach właściwe organy mogą wspólnie przedłużyć te terminy, w szczególności w przypadkach, w których termin nie może zostać dotrzymany z powodu okoliczności zewnętrznych w stosunku do sfery odpowiedzialności OSP lub organizacji OSD UE.

2. Propozycje dotyczące ustanowienia warunków, metod lub planów, o których mowa w ust. 1, są przedkładane ACER w celach informacyjnych w tym samym czasie, w którym są przedkładane właściwym organom.

3. Na wspólny wniosek krajowych organów regulacyjnych ACER wydaje opinię na temat propozycji dotyczącej ustanowienia warunków lub metod, lub planów w terminie sześciu miesięcy od otrzymania propozycji dotyczących ustanowienia warunków lub metod, lub planów oraz powiadamia o swojej opinii krajowe organy regulacyjne i właściwe organy. Krajowe organy regulacyjne, właściwe organy odpowiedzialne za cyberbezpieczeństwo i wszelkie inne organy wyznaczone jako właściwe organy koordynują swoje działania przed zwróceniem się do ACER o opinię. ACER może zawrzeć w takiej opinii zalecenia. ACER konsultuje się z ENISA przed wydaniem opinii w sprawie wniosków wymienionych w art. 6 ust. 2.

4. Właściwe organy prowadzą konsultację w swoim gronie, ściśle ze sobą współpracują i koordynują swe stanowiska w celu osiągnięcia porozumienia w sprawie proponowanych warunków, metod lub planów. Przed zatwierdzeniem warunków lub metod, lub też planów dokonują przeglądu i w razie potrzeby uzupełnienia propozycji, po konsultacji z ENTSO energii elektrycznej i organizacją OSD UE, w celu zapewnienia zgodności propozycji z niniejszym rozporządzeniem i przyczynienia się do wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii.

5. Właściwe organy podejmują decyzje w zakresie warunków lub metod, lub planów w terminie sześciu miesięcy od dnia otrzymania warunków lub metod, lub planów przez odpowiedni właściwy organ lub, w stosownych przypadkach, przez ostatni odpowiedni właściwy organ, którego to dotyczy.

6. W przypadku gdy ACER wyda opinię, odpowiednie właściwe organy uwzględniają taką opinię i podejmują swoje decyzje w terminie sześciu miesięcy od otrzymania opinii ACER.

7. W przypadku gdy właściwe organy wspólnie żądają zmiany proponowanych warunków lub metod, lub planów w celu ich zatwierdzenia, OSP opracowują, we współpracy z organizacją OSD UE, propozycję takiej zmiany warunków lub metod, lub planów. OSP przedkładają zmienioną propozycję do zatwierdzenia w terminie dwóch miesięcy od złożenia wniosku przez właściwe organy. Właściwe organy podejmują decyzję w sprawie zmienionych warunków lub metod, lub planów w terminie dwóch miesięcy od daty ich przedłożenia.

8. Jeżeli właściwe organy nie były w stanie osiągnąć porozumienia w terminie, o którym mowa w ust. 5 lub 7, informują o tym Komisję. Komisja może podjąć stosowne kroki w celu umożliwienia przyjęcia wymaganych warunków lub metod lub planów.

9. OSP, z pomocą ENTSO energii elektrycznej, oraz organizacja OSD UE publikują warunki lub metody, lub plany na swoich stronach internetowych po zatwierdzeniu przez odpowiednie właściwe organy, z wyjątkiem przypadków, w których takie informacje uznaje się za poufne zgodnie z art. 47.

10. Właściwe organy mogą wspólnie zwracać się do OSP i organizacji OSD UE o propozycje zmian zatwierdzonych warunków lub metod, lub zatwierdzonych planów oraz określić termin składania tych propozycji. OSP, we współpracy z organizacją OSD UE, mogą również przedstawiać właściwym organom propozycje zmian z własnej inicjatywy. Propozycje zmiany warunków lub metod lub zmian planów opracowuje się i zatwierdza zgodnie z procedurą określoną w niniejszym artykule.

11. Co najmniej raz na trzy lata po pierwszym przyjęciu odpowiednich warunków lub metod, lub odpowiednich przyjętych planów OSP we współpracy z organizacją OSD UE dokonują przeglądu skuteczności przyjętych warunków lub metod, lub przyjętych planów oraz bez zbędnej zwłoki przedstawiają wyniki przeglądu właściwym organom i ACER.

Artykuł 9

Konsultacje

1. OSP, z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, konsultują się z zainteresowanymi stronami, w tym ACER, ENISA i właściwym organem każdego państwa członkowskiego, w sprawie projektów propozycji dotyczących ustanowienia warunków lub metod wymienionych w art. 6 ust. 2 oraz planów, o których mowa w art. 6 ust. 3. Konsultacje te trwają co najmniej jeden miesiąc.

2. Propozycje dotyczące ustanowienia warunków lub metod wymienionych w art. 6 ust. 2 przedłożone przez OSP we współpracy z organizacją OSD UE są publikowane i przedkładane do konsultacji na szczeblu unijnym. Propozycje planów wymienionych w art. 6 ust. 3 przedłożone przez odpowiednie OSP we współpracy z organizacją OSD UE na szczeblu regionalnym są przedkładane do konsultacji przynajmniej na szczeblu regionalnym.

3. Przed przedłożeniem propozycji dotyczącej ustanowienia warunków lub metod, lub planów organowi regulacyjnemu do zatwierdzenia OSP, z pomocą ENTSO energii elektrycznej, oraz organizacja OSD UE odpowiedzialne za propozycję należycie uwzględniają uwagi zainteresowanych stron zgłoszone w ramach konsultacji przeprowadzonych zgodnie z ust. 1. We wszystkich przypadkach sporządza się i publikuje w sposób terminowy należyte uzasadnienie przyczyn uwzględnienia lub nieuwzględnienia uwag będących wynikiem konsultacji w złożonym dokumencie, przed przedstawieniem propozycji dotyczącej ustanowienia warunków lub metod lub jednocześnie z przedstawieniem takiej propozycji.

Artykuł 10

Zaangażowanie zainteresowanych stron

ACER, w ścisłej współpracy z ENTSO energii elektrycznej i organizacją OSD UE, organizuje zaangażowanie zainteresowanych stron, które obejmuje regularne spotkania z zainteresowanymi stronami w celu zidentyfikowania problemów i zaproponowania usprawnień w odniesieniu do wykonania niniejszego rozporządzenia.

Artykuł 11

Zwrot kosztów

1. Koszty ponoszone przez OSP i OSD podlegające regulacji taryf sieciowych oraz wynikające z obowiązków określonych w niniejszym rozporządzeniu, w tym koszty ponoszone przez ENTSO energii elektrycznej i organizację OSD UE, podlegają ocenie właściwego krajowego organu regulacyjnego każdego państwa członkowskiego.

2. Koszty uznane za uzasadnione, efektywne i proporcjonalne są zwracane za pośrednictwem taryf sieciowych lub innych odpowiednich mechanizmów określonych przez odpowiedni krajowy organ regulacyjny.

3. Na wniosek odpowiednich organów regulacyjnych OSP i OSD, o których mowa w ust. 1, przedstawiają – w odpowiednim terminie określonym przez krajowy organ regulacyjny – informacje niezbędne do ułatwienia oceny poniesionych kosztów.

Artykuł 12

Monitorowanie

1. ACER monitoruje wdrażanie niniejszego rozporządzenia zgodnie z art. 32 ust. 1 rozporządzenia (UE) 2019/943 i art. 4 ust. 2 rozporządzenia (UE) 2019/942. W ramach tego monitorowania ACER może współpracować z ENISA i zwracać się o wsparcie do ENTSO energii elektrycznej i organizacji OSD UE. ACER regularnie informuje Grupę Koordynacyjną ds. Energii Elektrycznej i grupę współpracy NIS o wdrażaniu niniejszego rozporządzenia.

2. ACER publikuje sprawozdanie co najmniej raz na trzy lata po wejściu w życie niniejszego rozporządzenia w celu:

a) dokonania przeglądu stanu wdrożenia mających zastosowanie środków zarządzania ryzykiem w cyberprzestrzeni w odniesieniu do podmiotów o dużym wpływie i podmiotów o krytycznym wpływie;

b) ustalenia, czy konieczne mogą być dodatkowe zasady dotyczące wspólnych wymogów minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego w celu uniknięcia ryzyka dla sektora energii elektrycznej; oraz

c) określenia obszarów wymagających poprawy w ramach zmiany niniejszego rozporządzenia lub określenia nieuwzględnionych obszarów i nowych priorytetów, które mogą pojawić się w wyniku rozwoju technologicznego.

3. Do dnia 13 czerwca 2025 r. ACER, we współpracy z ENISA i po konsultacji z ENTSO energii elektrycznej i organizacją OSD UE, może wydać wytyczne dotyczące istotnych informacji, które należy przekazać ACER do celów monitorowania, a także procesu i częstotliwości gromadzenia danych, w oparciu o wskaźniki skuteczności działania określone zgodnie z ust. 5.

4. Właściwe organy mogą mieć dostęp do odpowiednich informacji będących w posiadaniu ACER, zgromadzonych przez Agencję zgodnie z niniejszym artykułem.

5. ACER we współpracy z ENISA i przy wsparciu ze strony ENTSO energii elektrycznej i organizacji OSD UE wydaje niewiążące wskaźniki skuteczności działania na potrzeby oceny niezawodności działania, które są związane z aspektami cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

6. Podmioty wymienione w art. 2 ust. 1 niniejszego rozporządzenia przekazują ACER informacje, których ACER potrzebuje do realizacji zadań wymienionych w ust. 2.

Artykuł 13

Analiza porównawcza

1. Do dnia 13 czerwca 2025 r. ACER, we współpracy z ENISA, ustanowi niewiążące wytyczne dotyczące analizy porównawczej w zakresie cyberbezpieczeństwa. Wytyczne służą wyjaśnieniu krajowym organom regulacyjnym zasad analizy porównawczej wdrożonych kontroli cyberbezpieczeństwa zgodnie z ust. 2 niniejszego artykułu, z uwzględnieniem kosztów wdrożenia tych kontroli oraz skuteczności funkcji, jaką pełnią procesy, produkty, usługi, systemy i rozwiązania zastosowane do wdrożenia takich kontroli. Przy ustanawianiu niewiążących wytycznych dotyczących analizy porównawczej w zakresie cyberbezpieczeństwa ACER uwzględnia istniejące sprawozdania z analizy porównawczej. ACER przedkłada niewiążące wytyczne dotyczące analizy porównawczej w zakresie cyberbezpieczeństwa krajowym organom regulacyjnym w celach informacyjnych.

2. W terminie 12 miesięcy od ustanowienia wytycznych dotyczących analizy porównawczej zgodnie z ust. 1 krajowe organy regulacyjne przeprowadzają analizę porównawczą, aby ocenić, czy obecne inwestycje w cyberbezpieczeństwo:

a) przyczyniają się do ograniczenia ryzyka wpływającego na transgraniczne przepływy energii elektrycznej;

b) przynoszą pożądane wyniki i powodują zwiększenie wydajności na potrzeby rozwoju systemów elektroenergetycznych;

c) są skuteczne i zintegrowane z ogólnymi zamówieniami na aktywa i usługi.

3. Do celów tej analizy porównawczej krajowe organy regulacyjne mogą uwzględnić niewiążące wytyczne dotyczące analizy porównawczej w zakresie cyberbezpieczeństwa ustanowione przez ACER oraz oceniają w szczególności:

a) średnie związane z cyberbezpieczeństwem wydatki na ograniczanie ryzyka wpływającego na transgraniczne przepływy energii elektrycznej, zwłaszcza w odniesieniu do podmiotów o dużym wpływie i podmiotów o krytycznym wpływie;

b) we współpracy z ENTSO energii elektrycznej i organizacją OSD UE – średnie ceny usług, systemów i produktów w zakresie cyberbezpieczeństwa, które w znacznym stopniu przyczyniają się do poprawy i utrzymania środków zarządzania ryzykiem w cyberbezpieczeństwie w poszczególnych regionach pracy systemu;

c) występowanie i poziom porównywalności kosztów i funkcji usług, systemów i rozwiązań w zakresie cyberbezpieczeństwa odpowiednich do wdrożenia niniejszego rozporządzenia, z określeniem możliwych środków niezbędnych do zwiększenia efektywności wydatków, w szczególności tam, gdzie mogą być potrzebne inwestycje technologiczne w dziedzinie cyberbezpieczeństwa.

4. Wszelkie informacje związane z analizą porównawczą przygotowuje się i przetwarza zgodnie z wymogami dotyczącymi klasyfikacji danych określonymi w niniejszym rozporządzeniu, minimalnymi kontrolami cyberbezpieczeństwa oraz sprawozdaniem z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej. Analizy porównawczej, o której mowa w ust. 2 i 3, nie podaje się do wiadomości publicznej.

5. Bez uszczerbku dla wymogów poufności zawartych w art. 47 oraz dla potrzeby ochrony bezpieczeństwa podmiotów podlegających przepisom niniejszego rozporządzenia analizę porównawczą, o której mowa w ust. 2 i 3 niniejszego artykułu, udostępnia się wszystkim krajowym organom regulacyjnym, wszystkim właściwym organom, ACER, ENISA i Komisji.

Artykuł 14

Umowy z OSP spoza Unii

1. W terminie 18 miesięcy od wejścia w życie niniejszego rozporządzenia OSP z regionu pracy systemu sąsiadującego z państwem trzecim podejmują starania w celu zawarcia z OSP z sąsiedniego państwa trzeciego umów zgodnych z odpowiednimi przepisami prawa Unii i określających podstawę współpracy w zakresie ochrony cyberbezpieczeństwa i ustaleń dotyczących współpracy w dziedzinie cyberbezpieczeństwa z tymi OSP.

2. OSP informują właściwy organ o umowach zawartych zgodnie z ust. 1.

Artykuł 15

Przedstawiciele prawni

1. Podmioty, które nie mają siedziby w Unii, ale świadczą usługi na rzecz podmiotów w Unii i zostały zgłoszone jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgodnie z art. 24 ust. 6, w terminie trzech miesięcy od powiadomienia wyznaczają na piśmie przedstawiciela w Unii i odpowiednio informują właściwy organ powiadamiający.

2. Przedstawiciel ten zostaje upoważniony, by mógł się do niego zwracać dowolny właściwy organ lub CSIRT w Unii – oprócz lub zamiast do podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie – w sprawie obowiązków takiego podmiotu wynikających z niniejszego rozporządzenia. Podmiot o dużym wpływie lub podmiot o krytycznym wpływie przekazuje swojemu przedstawicielowi prawnemu niezbędne uprawnienia i wystarczające zasoby, aby zagwarantować jego skuteczną i terminową współpracę z odpowiednimi właściwymi organami lub CSIRT.

3. Przedstawiciel musi posiadać jednostkę organizacyjną w jednym z państw członkowskich, w których dany podmiot świadczy usługi. Uznaje się, że podmiot podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną. Podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgłaszają właściwemu organowi w państwie członkowskim, w którym ich przedstawiciel prawny ma miejsce zamieszkania lub siedzibę, imię i nazwisko lub nazwę, adres pocztowy, adres e-mail oraz numer telefonu tego przedstawiciela prawnego.

4. Wyznaczony przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu niewypełniania obowiązków wynikających z niniejszego rozporządzenia bez uszczerbku dla odpowiedzialności samego podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie i kroków prawnych, które mogą zostać przeciwko niemu podjęte.

5. W przypadku braku przedstawiciela w Unii wyznaczonego na podstawie niniejszego artykułu każde państwo członkowskie, w którym dany podmiot świadczy usługi, może podjąć wobec tego podmiotu działania prawne w związku z niewykonaniem obowiązków wynikających z niniejszego rozporządzenia.

6. Wyznaczenie przedstawiciela prawnego na terytorium Unii zgodnie z ust. 1 nie jest równoznaczne z posiadaniem siedziby w Unii.

Artykuł 16

Współpraca między ENTSO energii elektrycznej a organizacją OSD UE

1. ENTSO energii elektrycznej i organizacja OSD UE współpracują w ramach przeprowadzania ocen ryzyka w cyberprzestrzeni zgodnie z art. 19 i art. 21, w szczególności jeżeli chodzi o następujące zadania:

a) opracowanie metodyk oceny ryzyka w cyberprzestrzeni zgodnie z art. 18 ust. 1;

b) opracowanie kompleksowego sprawozdania z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej zgodnie z art. 23;

c) opracowanie wspólnych ram cyberbezpieczeństwa w odniesieniu do energii elektrycznej zgodnie z rozdziałem III;

d) opracowanie zalecenia dotyczącego zamówień publicznych w dziedzinie cyberbezpieczeństwa zgodnie z art. 35;

e) opracowanie metodyki określania skali klasyfikacji cyberataków zgodnie z art. 37 ust. 8;

f) opracowanie tymczasowego wskaźnika wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej („ECII") zgodnie z art. 48 ust. 1 lit. a);

g) opracowanie skonsolidowanego wstępnego wykazu podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 48 ust. 3;

h) opracowanie skonsolidowanego wstępnego wykazu ogólnounijnych procesów o dużym wpływie i procesów o krytycznym wpływie zgodnie z art. 48 ust. 4;

i) opracowanie wstępnego wykazu europejskich i międzynarodowych norm i kontroli zgodnie z art. 48 ust. 6;

j) przeprowadzenie ogólnounijnej oceny ryzyka w cyberprzestrzeni zgodnie z art. 19;

k) przeprowadzenie regionalnych ocen ryzyka w cyberprzestrzeni zgodnie z art. 21;

l) określenie regionalnych planów ograniczenia ryzyka w cyberprzestrzeni zgodnie z art. 22;

m) opracowanie wytycznych dotyczących europejskich programów certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT zgodnie z art. 36;

n) opracowanie wytycznych dotyczących wykonania niniejszego rozporządzenia w porozumieniu z ACER i ENISA.

2. Współpraca między ENTSO energii elektrycznej a organizacją OSD UE może odbywać się w ramach grupy roboczej ds. ryzyka w cyberprzestrzeni.

3. ENTSO energii elektrycznej i organizacja OSD UE regularnie informują ACER, ENISA, grupę współpracy NIS oraz Grupę Koordynacyjną ds. Energii Elektrycznej o postępach w realizacji ogólnounijnych i regionalnych ocen ryzyka w cyberprzestrzeni zgodnie z art. 19 i 21.

Artykuł 17

Współpraca między ACER a właściwymi organami

ACER we współpracy z każdym właściwym organem:

1) monitoruje wdrażanie środków zarządzania ryzykiem w cyberprzestrzeni zgodnie z art. 12 ust. 2 lit. a) oraz obowiązki sprawozdawcze zgodnie z art. 27 i art. 39; oraz

2) monitoruje proces przyjmowania i wdrażanie warunków, metod lub planów zgodnie z art. 6 ust. 2 i 3. Współpraca między ACER, ENISA i każdym właściwym organem może odbywać się w ramach podmiotu monitorującego ryzyko w cyberprzestrzeni.

ROZDZIAŁ II

OCENA RYZYKA I IDENTYFIKACJA ODPOWIEDNICH RODZAJÓW RYZYKA W CYBERPRZESTRZENI

Artykuł 18

Metody oceny ryzyka w cyberprzestrzeni

1. Do dnia 13 marca 2025 r. OSP, z pomocą ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i po konsultacji z grupą współpracy NIS, przedkładają propozycję metod oceny ryzyka w cyberprzestrzeni na szczeblu unijnym, regionalnym i na szczeblu państw członkowskich.

2. Metody oceny ryzyka w cyberprzestrzeni na szczeblu unijnym, regionalnym i na szczeblu państw członkowskich obejmują:

a) wykaz cyberzagrożeń, które należy uwzględnić, obejmujący co najmniej następujące zagrożenia dla łańcucha dostaw:

   (i) poważna i nieoczekiwana korupcja łańcucha dostaw;

   (ii) brak dostępności produktów ICT, usług ICT lub procesów ICT z łańcucha dostaw;

(iii) cyberataki inicjowane przez podmioty w łańcuchu dostaw;

(iv) wycieki informacji szczególnie chronionych w łańcuchu dostaw, w tym śledzenie łańcucha dostaw;

(v) wprowadzanie luk lub backdoorów do produktów ICT, usług ICT lub procesów ICT za pośrednictwem podmiotów łańcucha dostaw;

b) kryteria oceny wpływu ryzyka w cyberbezpieczeństwie jako wysokiego lub krytycznego z zastosowaniem określonych progów w zakresie konsekwencji i prawdopodobieństwa;

c) podejście do analizy ryzyka w cyberbezpieczeństwie wynikającego z dotychczasowych systemów, kaskadowych skutków cyberataków oraz charakteru systemów obsługujących sieć w czasie rzeczywistym;

d) podejście do analizy ryzyka w cyberbezpieczeństwie wynikającego z zależności od jednego dostawcy produktów ICT, usług ICT lub procesów ICT.

3. W ramach metody oceny ryzyka w cyberprzestrzeni na szczeblu unijnym, regionalnym i na szczeblu państw członkowskich dokonuje się oceny ryzyka w cyberprzestrzeni przy użyciu tej samej macierzy wpływu ryzyka. Macierz wpływu ryzyka:

a) służy do pomiaru skutków cyberataków w oparciu o następujące kryteria:

(i) czas braku dostaw energii elektrycznej;

(ii) ograniczenie wytwarzania energii elektrycznej;

(iii) utrata mocy w ramach rezerwy pierwotnej utrzymania częstotliwości;

(iv) utrata mocy do przywrócenia działania sieci elektroenergetycznej bez polegania na zewnętrznej sieci przesyłowej po całkowitym lub częściowym wyłączeniu (zwanego również „rozruchem autonomicznym");

(v) przewidywany czas wyłączenia dostaw energii elektrycznej wpływającego na odbiorców w połączeniu ze skalą wyłączenia pod względem liczby odbiorców oraz

(vi) wszelkie inne kryteria ilościowe lub jakościowe, które w racjonalny sposób mogłyby służyć jako wskaźnik wpływu cyberataku na transgraniczne przepływy energii elektrycznej;

b) służy do pomiaru prawdopodobieństwa wystąpienia incydentu jako częstotliwość cyberataków rocznie.

4. Metodyki oceny ryzyka w cyberprzestrzeni na poziomie Unii opisują, w jaki sposób zostaną określone wartości ECII dla progu dużego wpływu i progu krytycznego wpływu. ECII umożliwia podmiotom oszacowanie za pomocą kryteriów, o których mowa w ust. 2 lit. b), wpływu ryzyka na ich proces biznesowy podczas ocen wpływu na działalność, które przeprowadzają zgodnie z art. 26 ust. 4 lit. c) pkt (i).

5. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE, informuje Grupę Koordynacyjną ds. Energii Elektrycznej o propozycjach dotyczących metod oceny ryzyka w cyberprzestrzeni opracowanych zgodnie z ust. 1.

Artykuł 19

Ogólnounijna ocena ryzyka w cyberprzestrzeni

1. W terminie 9 miesięcy od zatwierdzenia metodyk oceny ryzyka w cyberprzestrzeni zgodnie z art. 8, a następnie co trzy lata ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i w porozumieniu z grupą współpracy NIS, bez uszczerbku dla art. 22 dyrektywy (UE) 2022/2555, przeprowadza ogólnounijną ocenę ryzyka w cyberprzestrzeni i sporządza projekt ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni. W tym celu będą one korzystać z metod opracowanych na podstawie art. 18 i zatwierdzonych na podstawie art. 8 w celu identyfikacji, analizy i oceny ewentualnych konsekwencji cyberataków mających wpływ na bezpieczeństwo pracy systemu elektroenergetycznego i zakłócających transgraniczne przepływy energii elektrycznej. W ogólnounijnej ocenie ryzyka w cyberprzestrzeni nie uwzględnia się kwestii szkody prawnej, szkody finansowej ani nadszarpnięcia reputacji spowodowanych cyberatakami.

2. W ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni uwzględnia się następujące elementy:

a) ogólnounijne procesy o dużym wpływie i ogólnounijne procesy o krytycznym wpływie;

b) macierz wpływu ryzyka, którą podmioty i właściwe organy stosują do oceny ryzyka w cyberprzestrzeni zidentyfikowanego w ocenie ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego przeprowadzonej na podstawie art. 20 oraz w ocenie ryzyka w cyberprzestrzeni na poziomie podmiotu zgodnie z art. 26 ust. 2 lit. b).

3. W odniesieniu do ogólnounijnych procesów o dużym wpływie i ogólnounijnych procesów o krytycznym wpływie ogólnounijne sprawozdanie z oceny ryzyka w cyberprzestrzeni zawiera:

a) ocenę możliwych konsekwencji cyberataku z wykorzystaniem wskaźników określonych w metodyce oceny ryzyka w cyberprzestrzeni opracowanej na podstawie art. 18 ust. 2, 3 i 4 i zatwierdzonej na podstawie art. 8;

b) ECII oraz progi dużego i krytycznego wpływu, które właściwe organy stosują zgodnie z art. 24 ust. 1 i 2 w celu zidentyfikowania podmiotów o dużym wpływie i podmiotów o krytycznym wpływie uczestniczących w ogólnounijnych procesach o dużym wpływie oraz w ogólnounijnych procesach o krytycznym wpływie.

4. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE, przedkłada ACER projekt ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni wraz z wynikami ogólnounijnej oceny ryzyka w cyberprzestrzeni. ACER wydaje opinię na temat projektu sprawozdania w terminie trzech miesięcy od jego otrzymania. ENTSO energii elektrycznej i organizacja OSD UE uwzględniają w jak największym stopniu opinię ACER przy przygotowaniu ostatecznej wersji tego sprawozdania.

5. W ciągu trzech miesięcy od otrzymania opinii ACER ENTSO energii elektrycznej, we współpracy z organizacją OSD UE, przedstawia ACER, Komisji, ENISA i właściwym organom wersję ostateczną ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni.

Artykuł 20

Ocena ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego

1. Każdy właściwy organ przeprowadza ocenę ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego w odniesieniu do wszystkich podmiotów o dużym wpływie i podmiotów o krytycznym wpływie w swoim państwie członkowskim, stosując metodyki opracowane zgodnie z art. 18 i zatwierdzone zgodnie z art. 8. Ocena ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego obejmuje identyfikację i analizę ryzyka cyberataków mających wpływ na bezpieczeństwo pracy systemu elektroenergetycznego i zakłócających transgraniczne przepływy energii elektrycznej. W ocenie ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego nie uwzględnia się kwestii szkody prawnej, szkody finansowej ani nadszarpnięcia reputacji spowodowanych cyberatakami.

2. W terminie 21 miesięcy od powiadomienia podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 24 ust. 6 i co trzy lata od tej daty oraz po konsultacji z właściwym organem odpowiedzialnym za cyberbezpieczeństwo w obszarze energii elektrycznej każdy właściwy organ, wspierany przez CSIRT, przekazuje ENTSO energii elektrycznej i organizacji OSD UE sprawozdanie z oceny ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego, zawierające następujące informacje dotyczące każdego procesu biznesowego o dużym wpływie i procesu biznesowego o krytycznym wpływie:

a) stan wdrożenia minimalnych i zaawansowanych kontroli cyberbezpieczeństwa na podstawie art. 29;

b) wykaz wszystkich cyberataków zgłoszonych w ciągu ostatnich trzech lat na podstawie art. 38 ust. 3;

c) streszczenie informacji na temat cyberzagrożeń zgłoszonych w ciągu poprzednich trzech lat zgodnie z art. 38 ust. 6;

d) w odniesieniu do każdego ogólnounijnego procesu o dużym wpływie lub procesu o krytycznym wpływie – oszacowanie ryzyka naruszenia poufności, integralności i dostępności informacji i istotnych aktywów;

e) w stosownych przypadkach wykaz dodatkowych podmiotów określonych jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie zgodnie z art. 24 ust. 1, 2, 3 i 5.

3. W sprawozdaniu z oceny ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego uwzględnia się plan gotowości na wypadek zagrożeń państwa członkowskiego sporządzony na podstawie art. 10 rozporządzenia (UE) 2019/941.

4. Informacje zawarte w sprawozdaniu z oceny ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego na podstawie ust. 2 lit. a)–d) nie mogą być powiązane z konkretnymi podmiotami lub aktywami. Sprawozdanie z oceny ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego musi również zawierać ocenę ryzyka dotyczącą czasowych odstępstw przyznanych przez właściwe organy państw członkowskich na podstawie art. 30.

5. ENTSO energii elektrycznej i organizacja OSD UE mogą zwrócić się do właściwych organów o dodatkowe informacje w odniesieniu do zadań określonych w ust. 2 lit. a) i c).

6. Właściwe organy zapewniają, aby przekazywane przez nie informacje były dokładne i prawidłowe.

Artykuł 21

Regionalne oceny ryzyka w cyberprzestrzeni

1. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i w porozumieniu z odpowiednim regionalnym centrum koordynacyjnym, przeprowadza regionalną ocenę ryzyka w cyberprzestrzeni w odniesieniu do każdego regionu pracy systemu, wykorzystując metody opracowane na podstawie art. 19 i zatwierdzone na podstawie art. 8 w celu identyfikacji, analizy i oceny ryzyka cyberataków mających wpływ na bezpieczeństwo pracy systemu elektroenergetycznego i zakłócających transgraniczne przepływy energii elektrycznej. W regionalnych ocenach ryzyka w cyberprzestrzeni nie uwzględnia się kwestii szkody prawnej, szkody finansowej ani nadszarpnięcia reputacji spowodowanych cyberatakami.

2. W terminie 30 miesięcy od powiadomienia podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 24 ust. 6, a następnie co trzy lata ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i w porozumieniu z grupą współpracy NIS, sporządza regionalne sprawozdanie z oceny ryzyka w cyberprzestrzeni w odniesieniu do każdego regionu pracy systemu.

3. W regionalnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni uwzględnia się istotne informacje zawarte w ogólnounijnych sprawozdaniach z oceny ryzyka w cyberprzestrzeni oraz w sprawozdaniach z ocen ryzyka w zakresie cyberprzestrzeni na poziomie państw członkowskich.

4. W regionalnej ocenie ryzyka w cyberprzestrzeni uwzględnia się regionalne scenariusze kryzysu elektroenergetycznego związane z cyberbezpieczeństwem ustalone zgodnie z art. 6 rozporządzenia (UE) 2019/941.

Artykuł 22

Regionalne plany ograniczenia ryzyka w cyberprzestrzeni

1. W terminie 36 miesięcy od powiadomienia podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 24 ust. 6 i nie później niż do dnia 13 czerwca 2031 r., a następnie co trzy lata, OSP, przy wsparciu ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i w porozumieniu z regionalnymi centrami koordynacyjnymi i grupą współpracy NIS, opracowują regionalny plan ograniczenia ryzyka w cyberprzestrzeni w odniesieniu do każdego regionu pracy systemu.

2. Regionalne plany ograniczenia ryzyka w cyberprzestrzeni obejmują:

a) minimalne i zaawansowane kontrole cyberbezpieczeństwa, które podmioty o dużym wpływie i podmioty o krytycznym wpływie stosują w danym regionie pracy systemu;

b) ryzyko w cyberprzestrzeni w regionach pracy systemu pozostałe po zastosowaniu mechanizmów kontroli, o których mowa w lit. a).

3. ENTSO energii elektrycznej przedkłada regionalne plany ograniczania ryzyka odpowiednim operatorom systemów przesyłowych, właściwym organom oraz Grupie Koordynacyjnej ds. Energii Elektrycznej. Grupa Koordynacyjna ds. Energii Elektrycznej może zalecić wprowadzenie zmian.

4. OSP, przy wsparciu ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i w porozumieniu z grupą współpracy NIS, aktualizują regionalne plany ograniczenia ryzyka co trzy lata, chyba że okoliczności wymagają częstszych aktualizacji.

Artykuł 23

Kompleksowe sprawozdanie z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej

1. W terminie 40 miesięcy od powiadomienia podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 24 ust. 6, a następnie co trzy lata OSP, przy wsparciu ENTSO energii elektrycznej, we współpracy z organizacją OSD UE i w porozumieniu z grupą współpracy NIS, przedkładają Grupie Koordynacyjnej ds. Energii Elektrycznej sprawozdanie z wyniku oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej („kompleksowe sprawozdanie z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej").

2. Kompleksowe sprawozdanie z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej opiera się na ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni, sprawozdaniach z oceny ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego i na regionalnych sprawozdaniach z oceny ryzyka w cyberprzestrzeni i obejmuje następujące informacje:

a) wykaz ogólnounijnych procesów o dużym wpływie i procesów o krytycznym wpływie wskazanych w ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 2 lit. a), w tym oszacowanie prawdopodobieństwa i wpływu ryzyka w cyberprzestrzeni ocenionego w regionalnych sprawozdaniach z oceny ryzyka w cyberprzestrzeni zgodnie z art. 21 ust. 2 i art. 19 ust. 3 lit. a);

b) bieżące cyberzagrożenia, ze szczególnym uwzględnieniem pojawiających się zagrożeń i pojawiającego się ryzyka dla systemu elektroenergetycznego;

c) informacje o cyberatakach na poziomie Unii, które miały miejsce w poprzednim okresie, zapewniające krytyczny przegląd tego, w jaki sposób takie cyberataki mogły mieć wpływ na transgraniczne przepływy energii elektrycznej;

d) ogólny stan wdrożenia środków w zakresie cyberbezpieczeństwa;

e) stan wdrożenia przepływów informacji zgodnie z art. 37 i 38;

f) wykaz informacji lub szczególne kryteria klasyfikacji informacji na podstawie art. 46;

g) zidentyfikowane i wyraźnie wskazane czynniki ryzyka, które mogą wynikać z zarządzania łańcuchem dostaw w sposób niezabezpieczony;

h) wyniki regionalnych i międzyregionalnych ćwiczeń w dziedzinie cyberbezpieczeństwa organizowanych na podstawie art. 44 i suma zebranych dzięki nim doświadczeń;

i) analiza rozwoju sytuacji w zakresie ogólnego transgranicznego ryzyka w cyberprzestrzeni w sektorze energii elektrycznej od czasu ostatnich regionalnych ocen ryzyka w cyberprzestrzeni;

j) wszelkie pozostałe informacje, które mogą być przydatne do określenia możliwych usprawnień niniejszego rozporządzenia lub potrzeby zmiany niniejszego rozporządzenia bądź któregokolwiek z jego narzędzi; oraz

k) zagregowane i zanonimizowane informacje na temat odstępstw przyznanych na podstawie art. 30 ust. 3.

3. Podmioty wymienione w art. 2 ust. 1 mogą wnieść wkład w opracowanie kompleksowego sprawozdania z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej, z poszanowaniem poufności informacji zgodnie z art. 47. OSP, przy wsparciu ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, konsultują się z tymi podmiotami od wczesnego etapu.

4. Kompleksowe sprawozdanie z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej podlega przepisom dotyczącym ochrony wymiany informacji zgodnie z art. 46. Bez uszczerbku dla art. 10 ust. 4 i art. 47 ust. 4 ENTSO energii elektrycznej i organizacja OSD UE udostępniają publiczną wersję tego sprawozdania, która nie zawiera informacji, które mogą wyrządzić szkodę podmiotom wymienionym w art. 2 ust. 1. Publiczną wersję tego sprawozdania udostępnia się wyłącznie za zgodą grupy współpracy NIS oraz Grupy Koordynacyjnej ds. Energii Elektrycznej. ENTSO energii elektrycznej, w koordynacji z organizacją OSD UE, odpowiada za sporządzenie i udostępnienie publicznej wersji sprawozdania.

Artykuł 24

Identyfikacja podmiotów o dużym wpływie i podmiotów o krytycznym wpływie

1. Każdy właściwy organ identyfikuje, za pomocą ECII oraz progów dużego wpływu i progów krytycznego wpływu zawartych w ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 3 lit. b), podmioty o dużym wpływie i podmioty o krytycznym wpływie w jego państwie członkowskim, które są zaangażowane w ogólnounijne procesy o dużym wpływie i procesy o krytycznym wpływie. Właściwe organy mogą zażądać informacji od podmiotu w ich państwie członkowskim w celu określenia wartości ECII w odniesieniu do tego podmiotu. Jeżeli ustalony ECII podmiotu przekracza próg dużego wpływu lub próg krytycznego wpływu, zidentyfikowany w ten sposób podmiot zostaje wymieniony w sprawozdaniu z oceny ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego, o którym mowa w art. 20 ust. 2.

2. Każdy właściwy organ identyfikuje, za pomocą ECII oraz progów dużego wpływu i progów krytycznego wpływu zawartych w ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 3 lit. b), podmioty o dużym wpływie i podmioty o krytycznym wpływie, które nie mają siedziby w Unii, w zakresie, w jakim są aktywne w UE. Właściwy organ może zażądać informacji od podmiotu, który nie ma siedziby w Unii, w celu określenia wartości ECII w odniesieniu do tego podmiotu.

3. Każdy właściwy organ może wskazać dodatkowe podmioty w swoim państwie członkowskim jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie, jeżeli spełnione są następujące kryteria:

a) podmiot jest częścią grupy podmiotów, w przypadku której istnieje znaczne ryzyko, że cyberatak wpłynie na nie jednocześnie;

b) zagregowany ECII grupy podmiotów przekracza próg dużego wpływu lub próg krytycznego wpływu.

4. Jeżeli właściwy organ zidentyfikuje dodatkowe podmioty zgodnie z ust. 3, wszystkie procesy w tych podmiotach, w przypadku których zagregowany ECII grupy przekracza próg dużego wpływu, uznaje się za procesy o dużym wpływie, a wszystkie procesy w tych podmiotach, w przypadku których zagregowany ECII grupy przekracza progi krytycznego wpływu, uznaje się za procesy o krytycznym wpływie.

5. Jeżeli właściwy organ zidentyfikuje podmioty, o których mowa w ust. 3 lit. a), w więcej niż jednym państwie członkowskim, informuje o tym pozostałe właściwe organy, ENTSO energii elektrycznej i organizację OSD UE. ENTSO energii elektrycznej we współpracy z organizacją OSD UE, w oparciu o informacje otrzymane od wszystkich właściwych organów, przekazuje właściwym organom analizę agregacji podmiotów działających w więcej niż jednym państwie członkowskim, które mogą być źródłem rozproszonego zakłócenia w transgranicznych przepływach energii elektrycznej i w związku z tym taka sytuacja może skutkować cyberatakiem. Jeżeli grupa podmiotów w szeregu państw członkowskich zostanie zidentyfikowana jako agregacja, w przypadku której ECII przekracza próg dużego wpływu lub próg krytycznego wpływu wszystkie zainteresowane właściwe organy identyfikują te podmioty w takiej grupie, na podstawie zagregowanego ECII grupy podmiotów, jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie dla danego państwa członkowskiego i zamieszcza się te zidentyfikowane podmioty w ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni.

6. Każdy właściwy organ w terminie dziewięciu miesięcy od otrzymania od ENTSO energii elektrycznej i organizacji OSD UE powiadomienia o ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 5, a w każdym razie nie później niż do dnia 13 czerwca 2028 r., powiadamia podmioty znajdujące się w wykazie o tym, że zostały zidentyfikowane jako podmioty o dużym wpływie lub podmioty o krytycznym wpływie w jego państwie członkowskim.

7. Jeżeli dostawca usług zostanie zgłoszony właściwemu organowi jako kluczowy dostawca usług ICT zgodnie z art. 27 lit. c), właściwy organ powiadamia o tym właściwe organy państw członkowskich, na których terytorium znajduje się siedziba lub przedstawiciel tego dostawcy. Ten ostatni właściwy organ powiadamia dostawcę usług o tym, że został on zidentyfikowany jako kluczowy dostawca usług.

Artykuł 25

Krajowe systemy weryfikacji

1. Właściwe organy mogą utworzyć krajowy system weryfikacji w celu sprawdzenia, czy podmioty o krytycznym wpływie zidentyfikowane zgodnie z art. 24 ust. 1 wdrożyły krajowe ramy prawne zawarte w macierzy mapowania, o której mowa w art. 34. Krajowy system weryfikacji może opierać się na inspekcji przeprowadzanej przez właściwy organ, niezależnych audytach bezpieczeństwa lub wzajemnych ocenach przeprowadzanych przez podmioty o krytycznym wpływie w tym samym państwie członkowskim nadzorowane przez właściwy organ.

2. Jeżeli właściwy organ podejmie decyzję o utworzeniu krajowego systemu weryfikacji, organ ten zapewnia prowadzenie weryfikacji zgodnie z następującymi wymogami:

a) każda strona przeprowadzająca wzajemną ocenę, audyt lub inspekcję musi być niezależna od weryfikowanego podmiotu o krytycznym wpływie i nie może znajdować się w sytuacji konfliktu interesów;

b) personel przeprowadzający wzajemną ocenę, audyt lub inspekcję posiada możliwą do wykazania wiedzę na temat następujących zagadnień:

   (i) cyberbezpieczeństwo w sektorze energii elektrycznej;

   (ii) systemy zarządzania cyberbezpieczeństwem;

   (iii) zasady audytu;

   (iv) oceny ryzyka w cyberprzestrzeni;

   (v) wspólne ramy cyberbezpieczeństwa w odniesieniu do energii elektrycznej;

   (vi) krajowe ramy prawne i regulacyjne oraz normy europejskie i międzynarodowe objęte zakresem weryfikacji;

   (vii) procesy o krytycznym wpływie wchodzące w zakres weryfikacji;

c) strona przeprowadzająca wzajemną ocenę, audyt lub inspekcję musi otrzymać wystarczająco dużo czasu na wykonanie tych działań;

d) strona przeprowadzająca wzajemną ocenę, audyt lub inspekcję podejmuje odpowiednie środki w celu ochrony informacji, które gromadzi podczas weryfikacji, zgodnie z ich poziomem poufności; oraz

e) wzajemne oceny, audyty lub inspekcje przeprowadza się co najmniej raz w roku i odbywają się one w pełnym zakresie weryfikacji co najmniej raz na trzy lata.

3. Jeżeli właściwy organ podejmie decyzję o utworzeniu krajowego systemu weryfikacji, co roku informuje ACER o częstotliwości przeprowadzania inspekcji w ramach tego systemu.

Artykuł 26

Zarządzanie ryzykiem w cyberprzestrzeni na poziomie podmiotu

1. Każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie zidentyfikowany przez właściwe organy na podstawie art. 24 ust. 1 wykonuje czynności w zakresie zarządzania ryzykiem w cyberprzestrzeni w odniesieniu do wszystkich swoich aktywów w swoim obszarze o dużym wpływie i obszarze o krytycznym wpływie. Każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie co trzy lata wykonuje czynności w zakresie zarządzania ryzykiem obejmujące etapy, o których mowa w ust. 2.

2. Każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie opiera swoje zarządzanie ryzykiem w cyberprzestrzeni na podejściu ukierunkowanym na ochronę jego sieci i systemów informatycznych, które obejmuje następujące etapy:

a) ustalenie kontekstu;

b) ocena ryzyka w cyberprzestrzeni na poziomie podmiotu;

c) zaradzenie ryzyku w cyberprzestrzeni;

d) akceptacja ryzyka w cyberprzestrzeni.

3. Na etapie ustalania kontekstu każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie:

a) określa zakres oceny ryzyka w cyberprzestrzeni, w tym procesy o dużym wpływie i procesy o krytycznym wpływie określone przez ENTSO energii elektrycznej i organizację OSD UE oraz inne procesy, które mogą być celem cyberataków, o dużym wpływie lub krytycznym wpływie na transgraniczne przepływy energii elektrycznej; oraz

b) określa kryteria oceny ryzyka i akceptacji ryzyka zgodnie z macierzą wpływu ryzyka, które podmioty i właściwe organy stosują do oceny ryzyka w cyberprzestrzeni i w ramach metodyk oceny ryzyka w cyberprzestrzeni na poziomie Unii, na szczeblu regionalnym i na poziomie państw członkowskich, opracowanych przez ENTSO energii elektrycznej i organizację OSD UE zgodnie z art. 19 ust. 2.

4. Na etapie oceny ryzyka w cyberprzestrzeni każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie:

a) identyfikuje ryzyko w cyberprzestrzeni, biorąc pod uwagę:

(i) wszystkie aktywa wykorzystywane w ogólnounijnych procesach o dużym wpływie i procesach o krytycznym wpływie wraz z oceną ewentualnego wpływu na transgraniczne przepływy energii elektrycznej, jeżeli aktywa te są zagrożone;

(ii) możliwe cyberzagrożenia z uwzględnieniem cyberzagrożeń zidentyfikowanych w najnowszym kompleksowym sprawozdaniu z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej. o którym mowa w art. 23, oraz zagrożenia dla łańcucha dostaw;

(iii) podatności, w tym podatności dotychczasowych systemów;

(iv) możliwe scenariusze cyberataków, w tym cyberataków mających wpływ na bezpieczeństwo pracy systemu elektroenergetycznego i zakłócających transgraniczne przepływy energii elektrycznej;

(v) odpowiednie oceny ryzyka przeprowadzane na poziomie Unii, w tym skoordynowane oceny ryzyka krytycznych łańcuchów dostaw zgodnie z art. 22 dyrektywy (UE) 2022/2555, oraz

(vi) wdrożone kontrole;

b) analizuje prawdopodobieństwo i konsekwencje ryzyka w cyberprzestrzeni określonego w lit. a) oraz określa poziom ryzyka w cyberprzestrzeni przy użyciu macierzy wpływu ryzyka stosowanej do oceny ryzyka w cyberprzestrzeni w ramach metodyk oceny ryzyka w cyberprzestrzeni na szczeblu unijnym, regionalnym i na szczeblu państw członkowskich, opracowanych przez OSP, przy wsparciu ENTSO energii elektrycznej i we współpracy z organizacją OSD UE zgodnie z art. 19 ust. 2;

c) klasyfikuje aktywa zgodnie z możliwymi konsekwencjami naruszenia cyberbezpieczeństwa i określa obszar o dużym wpływie i obszar o krytycznym wpływie, stosując następujące etapy:

(i) przeprowadza, w odniesieniu do wszystkich procesów objętych oceną ryzyka w cyberprzestrzeni, ocenę skutków dla działalności z wykorzystaniem ECII;

(ii) klasyfikuje proces jako proces o dużym wpływie lub proces o krytycznym wpływie, jeżeli jego ECII przekracza, odpowiednio, próg dużego wpływu lub próg krytycznego wpływu;

(iii) określa wszystkie aktywa o dużym wpływie i aktywa o krytycznym wpływie jako aktywa potrzebne do, odpowiednio, procesów o dużym wpływie i procesów o krytycznym wpływie;

(iv) określa obszary o dużym wpływie i obszary o krytycznym wpływie obejmujące, odpowiednio, wszystkie aktywa o dużym wpływie i aktywa o krytycznym wpływie, tak aby można było kontrolować dostęp do tych obszarów;

d) ocenia czynniki ryzyka w cyberbezpieczeństwie, nadając im priorytet za pomocą kryteriów oceny ryzyka i kryteriów akceptacji ryzyka, o których mowa w ust. 3 lit. b).

5. Na etapie zaradzenia ryzyku w cyberprzestrzeni każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie sporządza plan ograniczania ryzyka na poziomie podmiotu, wybierając warianty zaradzenia ryzyku odpowiednie do zarządzania ryzykiem i identyfikacji pozostałego ryzyka.

6. Na etapie akceptacji ryzyka w cyberprzestrzeni każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie podejmuje decyzję, czy zaakceptować ryzyko rezydualne, na podstawie kryteriów akceptacji ryzyka ustanowionych w ust. 3 lit. b).

7. Każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie rejestruje aktywa zidentyfikowane w ust. 1 w wykazie aktywów. Ten wykaz aktywów nie stanowi części sprawozdania z oceny ryzyka.

8. Podczas kontroli właściwy organ może przeprowadzić inspekcję aktywów znajdujących się w wykazie.

Artykuł 27

Sprawozdawczość w zakresie oceny ryzyka na poziomie podmiotu

Każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie przedkłada właściwemu organowi, w terminie 12 miesięcy od powiadomienia podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 24 ust. 6 i co trzy lata od tej daty, sprawozdanie zawierające następujące informacje:

1) wykaz kontroli wybranych na potrzeby planu ograniczania ryzyka na poziomie podmiotu zgodnie z art. 26 ust. 5 wraz z aktualnym stanem wdrożenia każdej kontroli;

2) w odniesieniu do każdego ogólnounijnego procesu o dużym wpływie lub procesu o krytycznym wpływie – oszacowanie ryzyka naruszenia poufności, integralności i dostępności informacji i istotnych aktywów. Oszacowanie tego ryzyka podaje się zgodnie z macierzą wpływu ryzyka w art. 19 ust. 2;

3) wykaz kluczowych dostawców usług ICT w odniesieniu do ich procesów o krytycznym wpływie.

ROZDZIAŁ III

WSPÓLNE RAMY CYBERBEZPIECZEŃSTWA W ODNIESIENIU DO ENERGII ELEKTRYCZNEJ

Artykuł 28

Skład, funkcjonowanie i przegląd wspólnych ram cyberbezpieczeństwa w odniesieniu do energii elektrycznej

1. Wspólne ramy cyberbezpieczeństwa w odniesieniu do energii elektrycznej składają się z następujących kontroli i systemów zarządzania cyberbezpieczeństwem:

a) minimalne kontrole cyberbezpieczeństwa opracowane zgodnie z art. 29;

b) zaawansowane kontrole cyberbezpieczeństwa opracowane zgodnie z art. 29;

c) matryca mapowania opracowana zgodnie z art. 34, pokazująca mapę kontroli, o których mowa w lit. a) i b), w oparciu o wybrane normy europejskie i międzynarodowe oraz krajowe ramy prawne lub regulacyjne;

d) system zarządzania cyberbezpieczeństwem ustanowiony zgodnie z art. 32.

2. Wszystkie podmioty o dużym wpływie stosują minimalne kontrole cyberbezpieczeństwa zgodnie z ust. 1 lit. a) w obszarze o dużym wpływie.

3. Wszystkie podmioty o krytycznym wpływie stosują zaawansowane kontrole cyberbezpieczeństwa zgodnie z ust. 1 lit. b) w obszarze o krytycznym wpływie.

4. W terminie siedmiu miesięcy od przedłożenia pierwszego projektu ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 4 wspólne ramy cyberbezpieczeństwa w odniesieniu do energii elektrycznej, o których mowa w ust. 1, uzupełnia się minimalnymi i zaawansowanymi kontrolami cyberbezpieczeństwa w łańcuchu dostaw opracowanymi na podstawie art. 33.

Artykuł 29

Minimalne i zaawansowane kontrole cyberbezpieczeństwa

1. W terminie siedmiu miesięcy od przedłożenia pierwszego projektu ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 4 OSP z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE opracowują wniosek dotyczący minimalnych i zaawansowanych kontroli cyberbezpieczeństwa.

2. W terminie sześciu miesięcy od sporządzenia każdego regionalnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 21 ust. 2 OSP z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE przedstawiają właściwemu organowi zmianę minimalnych i zaawansowanych kontroli cyberbezpieczeństwa. Wniosek zostanie sporządzony zgodnie z art. 8 ust. 10 i będzie uwzględniał ryzyko zidentyfikowane w regionalnej ocenie ryzyka.

3. Minimalne i zaawansowane kontrole cyberbezpieczeństwa muszą być możliwe do zweryfikowania przez uczestnictwo w krajowym systemie weryfikacji zgodnie z procedurą określoną w art. 31 lub przez poddanie się niezależnym audytom bezpieczeństwa przeprowadzanym przez osobę trzecią zgodnie z wymogami wymienionymi w art. 25 ust. 2.

4. Pierwotne minimalne i zaawansowane kontrole cyberbezpieczeństwa opracowane zgodnie z ust. 1 opierają się na ryzyku zidentyfikowanym w ogólnounijnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni, o którym mowa w art. 19 ust. 5. Zmienione minimalne i zaawansowane kontrole cyberbezpieczeństwa opracowane zgodnie z ust. 2 opierają się na regionalnym sprawozdaniu z oceny ryzyka w cyberprzestrzeni, o którym mowa w art. 21 ust. 2.

5. Minimalne kontrole cyberbezpieczeństwa obejmują kontrole mające na celu ochronę informacji wymienianych na podstawie art. 46.

6. W terminie 12 miesięcy od zatwierdzenia minimalnych i zaawansowanych kontroli cyberbezpieczeństwa zgodnie z art. 8 ust. 5 lub po każdej aktualizacji zgodnie z art. 8 ust. 10 podmioty wymienione w art. 2 ust. 1 i zidentyfikowane jako podmioty o krytycznym wpływie i podmioty o dużym wpływie zgodnie z art. 24, podczas opracowywania planu ograniczania ryzyka na poziomie podmiotu zgodnie z art. 26 ust. 5, stosują minimalne kontrole cyberbezpieczeństwa w obszarze o dużym wpływie i zaawansowane kontrole cyberbezpieczeństwa w obszarze o krytycznym wpływie.

Artykuł 30

Odstępstwa od minimalnych i zaawansowanych kontroli cyberbezpieczeństwa

1. Podmioty wymienione w art. 2 ust. 1 mogą zwrócić się do odpowiedniego właściwego organu o przyznanie odstępstwa od obowiązku stosowania minimalnych i zaawansowanych kontroli cyberbezpieczeństwa, o których mowa w art. 29 ust. 6. Właściwy organ może przyznać takie odstępstwo z jednego z następujących powodów:

a) w wyjątkowych okolicznościach, jeżeli podmiot jest w stanie wykazać, że koszty wdrożenia odpowiednich kontroli cyberbezpieczeństwa znacznie przewyższają korzyści. ACER i ENTSO energii elektrycznej we współpracy z organizacją OSD UE mogą wspólnie opracować wytyczne dotyczące szacowania kosztów kontroli cyberbezpieczeństwa, aby pomóc podmiotom;

b) jeżeli podmiot przedstawia plan zaradzenia ryzyku na poziomie podmiotu, który ogranicza ryzyko w cyberbezpieczeństwie za pomocą alternatywnych kontroli do poziomu akceptowalnego zgodnie z kryteriami akceptacji ryzyka, o których mowa w art. 26 ust. 3 lit. b).

2. W terminie trzech miesięcy od otrzymania wniosku, o którym mowa w ust. 1, każdy właściwy organ podejmuje decyzję o przyznaniu odstępstwa od minimalnych i zaawansowanych kontroli cyberbezpieczeństwa. Odstępstwa od minimalnych lub zaawansowanych kontroli cyberbezpieczeństwa przyznaje się na okres maksymalnie trzech lat, z możliwością przedłużenia.

3. Zagregowane i zanonimizowane informacje dotyczące przyznanych odstępstw zamieszcza się w załączniku do kompleksowego sprawozdania z oceny ryzyka w cyberprzestrzeni w odniesieniu do transgranicznych przepływów energii elektrycznej, o którym mowa w art. 23. ENTSO energii elektrycznej i organizacja OSD UE wspólnie aktualizują ten wykaz w stosownych przypadkach.

Artykuł 31

Weryfikacja wspólnych ram cyberbezpieczeństwa w odniesieniu do energii elektrycznej

1. Nie później niż w terminie 24 miesięcy po przyjęciu kontroli, o których mowa w art. 28 ust. 1 lit. a), b) i c), oraz ustanowieniu systemu zarządzania cyberbezpieczeństwem, o którym mowa w lit. d) tego artykułu, każdy podmiot o krytycznym wpływie zidentyfikowany zgodnie z art. 24 ust. 1 musi być w stanie wykazać na wniosek właściwego organu zgodność z systemem zarządzania cyberbezpieczeństwem oraz minimalnymi lub zaawansowanymi kontrolami cyberbezpieczeństwa.

2. Każdy podmiot o krytycznym wpływie wypełnia obowiązek, o którym mowa w ust. 1, przez poddanie się niezależnym audytom bezpieczeństwa przeprowadzanym przez osobę trzecią zgodnie z wymogami wymienionymi w art. 25 ust. 2 lub przez uczestniczenie w krajowym systemie weryfikacji zgodnie z art. 25 ust. 1.

3. Weryfikacja zgodności podmiotu o krytycznym wpływie z systemem zarządzania cyberbezpieczeństwem oraz minimalnymi lub zaawansowanymi kontrolami cyberbezpieczeństwa obejmuje wszystkie aktywa w obszarze o krytycznym wpływie podmiotu o krytycznym wpływie.

4. Weryfikację zgodności podmiotu o krytycznym wpływie z systemem zarządzania cyberbezpieczeństwem oraz minimalnymi lub zaawansowanymi kontrolami cyberbezpieczeństwa powtarza się regularnie w terminie najpóźniej 36 miesięcy po zakończeniu pierwszej weryfikacji, a następnie co trzy lata.

5. Każdy podmiot o krytycznym wpływie określony zgodnie z art. 24 wykazuje swoją zgodność z wymogiem stosowania kontroli, o których mowa w art. 28 ust. 1 lit. a), b) i c), oraz ustanowienia systemu zarządzania cyberbezpieczeństwem, o którym mowa w lit. d) tego artykułu, przez złożenie właściwemu organowi sprawozdania w sprawie wyniku weryfikacji zgodności.

Artykuł 32

System zarządzania cyberbezpieczeństwem

1. Każdy podmiot o dużym wpływie lub podmiot o krytycznym wpływie w terminie 24 miesięcy od powiadomienia przez właściwy organ, że został zidentyfikowany jako podmiot o dużym wpływie lub podmiot o krytycznym wpływie zgodnie z art. 24 ust. 6, ustanawia system zarządzania cyberbezpieczeństwem, a następnie co trzy lata dokonuje jego przeglądu w celu:

a) określenia zakresu systemu zarządzania cyberbezpieczeństwem z uwzględnieniem interfejsów i zależności od innych podmiotów;

b) zapewnienia, aby cała kadra kierownicza najwyższego szczebla była informowana o odpowiednich obowiązkach prawnych i aktywnie przyczyniała się do wdrażania systemu zarządzania cyberbezpieczeństwem przez terminowe podejmowanie decyzji i szybkie reagowanie;

c) zapewnienia dostępności zasobów koniecznych w systemie zarządzania cyberbezpieczeństwem;

d) ustanowienia polityki cyberbezpieczeństwa, która jest dokumentowana i przekazywana w ramach podmiotu i do osób, których dotyczy ryzyko dla bezpieczeństwa;

e) przydzielenia obowiązków dotyczących ról istotnych dla cyberbezpieczeństwa i informowania o nich;

f) zarządzania ryzykiem w cyberprzestrzeni na poziomie podmiotu zgodnie z definicją zawartą w art. 26;

g) określenia i zapewnienia zasobów niezbędnych do wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania cyberbezpieczeństwem, z uwzględnieniem niezbędnych kompetencji i wiedzy z zakresu zasobów cyberbezpieczeństwa;

h) określenia komunikacji wewnętrznej i zewnętrznej istotnej z punktu widzenia cyberbezpieczeństwa;

i) tworzenia, aktualizowania i kontrolowania udokumentowanych informacji związanych z systemem zarządzania cyberbezpieczeństwem;

j) oceny wydajności i skuteczności systemu zarządzania cyberbezpieczeństwem;

k) prowadzenia audytów wewnętrznych w planowanych odstępach czasu, tak aby zapewnić skuteczne wdrożenie i utrzymanie systemu zarządzania cyberbezpieczeństwem;

l) przeglądu wdrażania systemu zarządzania cyberbezpieczeństwem w planowanych odstępach czasu; oraz kontrolowania i korygowania niezgodności zasobów i działań z politykami, procedurami i wytycznymi w systemie zarządzania cyberbezpieczeństwem.

2. Zakres systemu zarządzania cyberbezpieczeństwem obejmuje wszystkie aktywa w obszarze o dużym wpływie i obszarze o krytycznym wpływie podmiotu o dużym wpływie i podmiotu o krytycznym wpływie.

3. Właściwe organy, bez narzucania czy propagowania korzystania z określonego rodzaju technologii, zachęcają do stosowania europejskich lub międzynarodowych norm i specyfikacji związanych z systemami zarządzania i mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych.

Artykuł 33

Minimalne i zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw

1. W terminie siedmiu miesięcy od przedłożenia pierwszego projektu ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 4 OSP z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE opracowują wniosek dotyczący minimalnych i zaawansowanych kontroli cyberbezpieczeństwa w łańcuchu dostaw, które ograniczają ryzyko w łańcuchach dostaw zidentyfikowane w ogólnounijnych ocenach ryzyka w cyberprzestrzeni, jako uzupełnienie minimalnych i zaawansowanych kontroli cyberbezpieczeństwa opracowanych zgodnie z art. 29. Minimalne i zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw opracowuje się wraz z minimalnymi i zaawansowanymi kontrolami cyberbezpieczeństwa zgodnie z art. 29. Minimalne i zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw obejmują cały cykl życia wszystkich produktów ICT, usług ICT i procesów ICT w obszarze o dużym wpływie lub obszarze o krytycznym wpływie podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie. Przy opracowywaniu wniosku dotyczącego minimalnych i zaawansowanych kontroli cyberbezpieczeństwa w łańcuchu dostaw prowadzi się konsultacje z grupą współpracy NIS.

2. Minimalne kontrole cyberbezpieczeństwa w łańcuchu dostaw obejmują kontrole podmiotów o dużym wpływie lub podmiotów o krytycznym wpływie, w których to kontrolach:

a) uwzględnia się zalecenia dotyczące zamówień publicznych na produkty ICT, usługi ICT i procesy ICT odnoszące się do specyfikacji cyberbezpieczeństwa, obejmujące co najmniej:

   (i) sprawdzanie przeszłości pracowników dostawcy uczestniczącego w łańcuchu dostaw i zajmującego się informacjami szczególnie chronionymi lub mającego dostęp do należących do podmiotu aktywów o dużym wpływie lub aktywów o krytycznym wpływie. Sprawdzanie przeszłości może obejmować weryfikację tożsamości i przeszłości personelu lub wykonawców podmiotu zgodnie z prawem i procedurami krajowymi oraz odpowiednim i mającym zastosowanie prawem Unii, w tym rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 i dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 ([18]). Sprawdzanie przeszłości musi być proporcjonalne i ściśle ograniczone do tego, co jest konieczne. Przeprowadza się je wyłącznie w celu oceny potencjalnego ryzyka dla bezpieczeństwa odnośnego podmiotu. Musi być ono proporcjonalne do wymogów biznesowych, klauzul tajności informacji, które mają być udostępniane, oraz postrzeganego ryzyka, a także może być przeprowadzane przez sam podmiot, przez przedsiębiorstwo zewnętrzne przeprowadzające kontrolę bezpieczeństwa lub w ramach rządowego poświadczenia;

   (ii) procesy bezpiecznego i kontrolowanego projektowania, opracowywania i wytwarzania produktów ICT, usług ICT i procesów ICT, promujące projektowanie i rozwój produktów ICT, usług ICT i procesów ICT, które obejmują odpowiednie środki techniczne w celu zapewnienia cyberbezpieczeństwa;

   (iii) projektowanie sieci i systemów informatycznych, w których urządzenia nie są zaufane, nawet jeśli znajdują się w bezpiecznym obszarze, wymagają weryfikacji wszystkich otrzymanych wniosków i opierają się na zasadzie „najniższych uprawnień";

   (iv) dostęp dostawcy do aktywów podmiotu;

([18]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, oraz w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

(v) zobowiązania umowne dostawcy do ochrony i ograniczenia dostępu do informacji szczególnie chronionych podmiotu;

(vi) podstawowe specyfikacje zamówień publicznych w dziedzinie cyberbezpieczeństwa dla podwykonawców dostawcy;

(vii) identyfikowalność stosowania specyfikacji cyberbezpieczeństwa od opracowania przez produkcję do dostarczenia produktów ICT, usług ICT lub procesów ICT;

(viii) wspieranie aktualizacji bezpieczeństwa przez cały cykl życia produktów ICT, usług ICT lub procesów ICT;

(ix) prawo do audytu cyberbezpieczeństwa w procesach projektowania, rozwoju i produkcji dostawcy; oraz

(x) ocenę profilu ryzyka dostawcy;

b) zobowiązuje się takie podmioty do uwzględniania zaleceń dotyczących udzielania zamówień, o których mowa w lit. a), przy zawieraniu umów z dostawcami, partnerami współpracującymi i innymi stronami w łańcuchu dostaw, obejmujących zwykłe dostawy produktów ICT, usług ICT i procesów ICT, a także zdarzenia i okoliczności niezwiązane z zamówieniami, takie jak rozwiązanie i przeniesienie umów w przypadku zaniedbania ze strony partnera umownego;

c) zobowiązuje się takie podmioty do uwzględniania wyników odpowiednich skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych zgodnie z art. 22 ust. 1 dyrektywy (UE) 2022/2555;

d) uwzględnia się kryteria wyboru dostawców, którzy mogą spełnić specyfikacje cyberbezpieczeństwa określone w lit. a) i którzy mają poziom cyberbezpieczeństwa odpowiedni do ryzyka w cyberbezpieczeństwie związanego z produktem ICT, usługą ICT lub procesami ICT, które dostawca dostarcza, i zawierania umów z takimi dostawcami;

e) uwzględnia się kryteria dywersyfikacji źródeł dostaw produktów ICT, usług ICT i procesów ICT oraz zmniejszenia ryzyka uzależnienia od jednego dostawcy;

f) uwzględnia się kryteria regularnego monitorowania, przeglądu lub audytu specyfikacji cyberbezpieczeństwa w odniesieniu do wewnętrznych procesów operacyjnych dostawców przez cały cykl życia każdego produktu ICT, każdej usługi ICT i każdego procesu ICT.

3. W odniesieniu do specyfikacji cyberbezpieczeństwa zawartych w zaleceniu dotyczącym zamówień publicznych w dziedzinie cyberbezpieczeństwa, o którym mowa w ust. 2 lit. a), podmioty o dużym wpływie lub podmioty o krytycznym wpływie stosują zasady udzielania zamówień publicznych zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2014/24/UE ([19]), zgodnie z art. 35 ust. 4, lub określają własne specyfikacje na podstawie wyników oceny ryzyka w cyberprzestrzeni na poziomie podmiotu.

4. Zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw obejmują kontrole podmiotów o krytycznym wpływie w celu sprawdzenia podczas udzielania zamówień publicznych, czy produkty ICT, usługi ICT i procesy ICT, które będą wykorzystywane jako aktywa o krytycznym wpływie, spełniają specyfikacje cyberbezpieczeństwa. Produkt ICT, usługę ICT lub proces ICT weryfikuje się za pomocą europejskiego programu certyfikacji cyberbezpieczeństwa, o którym mowa w art. 31, albo za pomocą działań weryfikacyjnych wybranych i zorganizowanych przez podmiot. Stopień szczegółowości i zakres działań weryfikacyjnych muszą być wystarczające do uzyskania pewności, że produkt ICT, usługa ICT lub proces ICT mogą zostać wykorzystane do ograniczenia ryzyka zidentyfikowanego w ocenie ryzyka na poziomie podmiotu. Podmiot o krytycznym wpływie dokumentuje działania podjęte w celu ograniczenia zidentyfikowanego ryzyka.

5. Minimalne i zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw stosuje się do zamówień publicznych odpowiednich produktów ICT, usług ICT i procesów ICT. Minimalne i zaawansowane kontrole cyberbezpieczeństwa w łańcuchu dostaw będą stosowane do procedur udzielania zamówień w podmiotach zidentyfikowanych jako podmioty o krytycznym wpływie i podmioty o dużym wpływie zgodnie z art. 24, które to procedury rozpoczynają się sześć miesięcy po przyjęciu lub aktualizacji minimalnych i zaawansowanych kontroli cyberbezpieczeństwa, o których mowa w art. 29.

([19]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

6. W terminie sześciu miesięcy od sporządzenia każdego regionalnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 21 ust. 2 OSP z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE przedstawiają właściwemu organowi zmianę minimalnych i zaawansowanych kontroli cyberbezpieczeństwa w łańcuchu dostaw. Wniosek zostanie sporządzony zgodnie z art. 8 ust. 10 i będzie uwzględniał ryzyko zidentyfikowane w regionalnej ocenie ryzyka.

Artykuł 34

Macierze mapowania do celów kontroli cyberbezpieczeństwa w odniesieniu do energii elektrycznej pod kątem norm

1. W terminie siedmiu miesięcy od przedłożenia pierwszego projektu ogólnounijnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 19 ust. 4 OSP z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE i w konsultacji z ENISA opracowują wniosek dotyczący macierzy do celów mapowania kontroli, o których mowa w art. 28 ust. 1 lit. a) i b), pod kątem norm europejskich i międzynarodowych, a także odpowiednich specyfikacji technicznych („matryca mapowania"). ENTSO energii elektrycznej i organizacja OSD UE dokumentują równoważność poszczególnych kontroli za pomocą kontroli określonych w art. 28 ust. 1 lit. a) i b).

2. Właściwe organy mogą zapewnić ENTSO energii elektrycznej i organizacji OSD UE mapy kontroli określonych w art. 28 ust. 1 lit. a) i b), z odniesieniem do powiązanych krajowych ram prawnych lub regulacyjnych, w tym odpowiednich norm krajowych państw członkowskich zgodnie z art. 25 dyrektywy (UE) 2022/2555. Jeżeli właściwy organ państwa członkowskiego przedstawi takie mapy, ENTSO energii elektrycznej i organizacja OSD UE włączają te mapy krajowe do macierzy mapowania.

3. W terminie sześciu miesięcy od sporządzenia każdego regionalnego sprawozdania z oceny ryzyka w cyberprzestrzeni zgodnie z art. 21 ust. 2 OSP z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE oraz w konsultacji z ENISA przedstawiają właściwemu organowi zmianę macierzy mapowania. Wniosek zostanie sporządzony zgodnie z art. 8 ust. 10 i będzie uwzględniał ryzyko zidentyfikowane w regionalnej ocenie ryzyka.

ROZDZIAŁ IV

ZALECENIA DOTYCZĄCE ZAMÓWIEŃ PUBLICZNYCH W DZIEDZINIE CYBERBEZPIECZEŃSTWA

Artykuł 35

Zalecenia dotyczące zamówień publicznych w dziedzinie cyberbezpieczeństwa

1. OSP, z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, opracowują w programie prac, który należy ustanowić i aktualizować za każdym razem, gdy przyjmowany jest regionalne sprawozdanie z oceny ryzyka w cyberprzestrzeni, zestawy niewiążących zaleceń dotyczących zamówień publicznych w dziedzinie cyberbezpieczeństwa, które podmioty o dużym wpływie i podmioty o krytycznym wpływie mogą wykorzystać jako podstawę przy zamówieniach na produkty ICT, usługi ICT i procesy ICT w obszarze o dużym wpływie i obszarze o krytycznym wpływie. Ten program prac obejmuje następujące elementy:

a) opis i klasyfikację rodzajów produktów ICT, usług ICT i procesów ICT wykorzystywanych przez podmioty o dużym wpływie i podmioty o krytycznym wpływie w obszarze o dużym wpływie i obszarze o krytycznym wpływie;

b) wykaz rodzajów produktów ICT, usług ICT i procesów ICT, w odniesieniu do których opracowuje się zestaw niewiążących zaleceń w dziedzinie cyberbezpieczeństwa na podstawie odpowiednich regionalnych sprawozdań z oceny ryzyka w cyberprzestrzeni i na podstawie priorytetów podmiotów o dużym wpływie i podmiotów o krytycznym wpływie.

2. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE, przedstawia ACER podsumowanie tego programu prac w terminie sześciu miesięcy od przyjęcia lub aktualizacji regionalnego sprawozdania z oceny ryzyka w cyberprzestrzeni.

3. OSP, z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, dąży do zapewnienia, aby niewiążące zalecenia dotyczące zamówień publicznych w dziedzinie cyberbezpieczeństwa opracowane na podstawie odpowiednich regionalnych ocen ryzyka w cyberprzestrzeni były podobne lub porównywalne w regionach pracy systemu. Zestawy zaleceń dotyczących zamówień publicznych w dziedzinie cyberbezpieczeństwa obejmują co najmniej specyfikacje, o których mowa w art. 33 ust. 2 lit. a). W miarę możliwości specyfikacje wybiera się spośród norm europejskich i międzynarodowych.

4. OSP, z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, zapewnia, aby zestawy zaleceń dotyczących zamówień publicznych w dziedzinie cyberbezpieczeństwa:

a) były zgodne z zasadami udzielania zamówień publicznych określonymi w dyrektywie 2014/24/UE; oraz

b) były zgodne z najnowszymi dostępnymi europejskimi programami certyfikacji cyberbezpieczeństwa odnoszącymi się do danego produktu ICT, danej usługi ICT lub danego procesu ICT oraz uwzględniały te systemy.

Artykuł 36

Wytyczne dotyczące wykorzystania europejskich programów certyfikacji cyberbezpieczeństwa na potrzeby zamówień publicznych w odniesieniu do produktów ICT, usług ICT i procesów ICT

1. Niewiążące zalecenia dotyczące zamówień publicznych w dziedzinie cyberbezpieczeństwa opracowane na podstawie art. 35 mogą obejmować wytyczne sektorowe dotyczące wykorzystania europejskich programów certyfikacji cyberbezpieczeństwa, jeżeli dostępny jest odpowiedni program dla danego rodzaju produktu ICT, usługi ICT lub procesu ICT wykorzystywanych przez podmioty o krytycznym wpływie, bez uszczerbku dla ram tworzenia europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z art. 46 rozporządzenia (UE) 2019/881.

2. OSP, z pomocą ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, ściśle współpracuje z ENISA w zakresie dostarczania sektorowych wytycznych uwzględnionych w niewiążących zaleceniach dotyczących zamówień publicznych w dziedzinie cyberbezpieczeństwa zgodnie z ust. 1.

ROZDZIAŁ V

PRZEPŁYWY INFORMACJI, CYBERATAKI I ZARZĄDZANIE KRYZYSOWE

Artykuł 37

Przepisy dotyczące wymiany informacji

1. Jeżeli właściwy organ otrzyma informacje dotyczące cyberataku podlegającego obowiązkowi zgłaszania, ten właściwy organ:

a) ocenia poziom poufności tych informacji oraz bez zbędnej zwłoki i nie później niż w ciągu 24 godzin od otrzymania informacji powiadamia dany podmiot o wynikach swojej oceny;

b) podejmuje próbę znalezienia jakiegokolwiek innego podobnego cyberataku w Unii zgłoszonego innym właściwym organom w celu skorelowania informacji otrzymanych w kontekście cyberataku podlegającego obowiązkowi zgłaszania z informacjami przekazanymi w kontekście innych cyberataków oraz rozbudowania istniejących informacji, a także wzmocnienia i koordynacji reagowania w zakresie cyberbezpieczeństwa;

c) odpowiada za usunięcie tajemnic handlowych i anonimizację informacji zgodnie z odpowiednimi przepisami krajowymi i unijnymi;

d) udostępnia te informacje krajowym pojedynczym punktom kontaktowym, CSIRT i wszystkim właściwym organom wyznaczonym zgodnie z art. 4 w innych państwach członkowskich bez zbędnej zwłoki i nie później niż w ciągu 24 godzin po powzięciu wiadomości o cyberataku podlegającym obowiązkowi zgłaszania oraz regularnie przekazują tym organom lub podmiotom zaktualizowane informacje;

e) rozpowszechnia informacje o cyberataku, po anonimizacji i usunięciu tajemnic handlowych zgodnie z ust. 1 lit. c) wśród podmiotów o krytycznym wpływie i podmiotów o dużym wpływie w swoim państwie członkowskim bez zbędnej zwłoki i nie później niż w ciągu 24 godzin po otrzymaniu informacji zgodnie z ust. 1 lit. a) oraz regularnie przekazuje zaktualizowane informacje umożliwiające tym podmiotom skuteczne zorganizowanie obrony;

f) może zwrócić się do podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie, który dokonuje zgłoszenia, o dalsze rozpowszechnianie w bezpieczny sposób informacji na temat cyberataku podlegającego obowiązkowi zgłaszania wśród innych podmiotów, których atak ten może dotyczyć, w celu umożliwienia orientacji sytuacyjnej w sektorze energii elektrycznej oraz zapobieżenia urzeczywistnieniu się ryzyka, które może się nasilić i przybrać formę transgranicznego incydentu w cyberbezpieczeństwie w sektorze energii elektrycznej;

g) udostępnia ENISA sprawozdanie podsumowujące, po anonimizacji i usunięciu tajemnic handlowych, z informacjami dotyczącymi cyberataku.

2. W przypadku gdy CSIRT dowiaduje się o nienaprawionej aktywnie wykorzystywanej podatności, CSIRT:

a) niezwłocznie informuje o niej ENISA za pośrednictwem odpowiedniego bezpiecznego kanału wymiany informacji, chyba że inne przepisy prawa Unii stanowią inaczej;

b) wspiera dany podmiot w uzyskaniu od producenta lub dostawcy skutecznego, skoordynowanego i szybkiego zarządzania nienaprawioną aktywnie wykorzystywaną podatnością lub skutecznych i wydajnych środków ograniczających ryzyko;

c) dzieli się dostępnymi informacjami ze sprzedawcą i zwraca się do producenta lub dostawcy, w miarę możliwości, o wskazanie wykazu CSIRT w państwach członkowskich, których dotyczy nienaprawiona aktywnie wykorzystywana podatność i które muszą zostać poinformowane;

d) dzieli się dostępnymi informacjami z CSIRT określonymi w poprzedniej literze, w oparciu o zasadę ograniczonego dostępu;

e) dzieli się strategiami i środkami łagodzącymi, o ile takie istnieją, w związku ze zgłoszoną nienaprawioną aktywnie wykorzystywaną podatnością.

3. W przypadku gdy właściwy organ dowiaduje się o nienaprawionej aktywnie wykorzystywanej podatności, ten właściwy organ:

a) dzieli się strategiami i środkami łagodzącymi, o ile takie istnieją, w związku ze zgłoszoną nienaprawioną aktywnie wykorzystywaną podatnością, w koordynacji z CSIRT w jego państwie członkowskim;

b) dzieli się informacjami z CSIRT w państwie członkowskim, w którym zgłoszono nienaprawioną aktywnie wykorzystywaną podatność.

4. Jeżeli właściwy organ poweźmie wiadomość o nienaprawionej podatności, co do której nie ma jeszcze dowodów na to, że jest ona aktywnie wykorzystywana, bez zbędnej zwłoki koordynuje swoje działania z CSIRT do celów skoordynowanego ujawniania podatności, jak określono w art. 12 ust. 1 dyrektywy (UE) 2022/2555.

5. Jeżeli CSIRT otrzyma informacje dotyczące cyberzagrożeń od co najmniej jednego podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie zgodnie z art. 38 ust. 6, bez zbędnej zwłoki i nie później niż cztery godziny po otrzymaniu informacji rozpowszechnia w swoim państwie członkowskim te informacje lub wszelkie inne informacje mające znaczenie dla zapobiegania ryzyku związanemu z podmiotami o krytycznym wpływie i podmiotami o dużym wpływie, reagowania na to ryzyko lub łagodzenia go, a także, w stosownych przypadkach, przekazuje te informacje wszystkim zainteresowanym CSIRT i swojemu krajowemu pojedynczemu punktowi kontaktowemu.

6. Jeżeli właściwy organ uzyska informacje dotyczące cyberzagrożeń od co najmniej jednego podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie, przekazuje te informacje CSIRT do celów ust. 5.

7. Właściwe organy mogą przekazać w całości lub w części obowiązki, o których mowa w ust. 3 i 4, dotyczące jednego lub większej liczby podmiotów o dużym wpływie lub podmiotów o krytycznym wpływie, które działają w więcej niż jednym państwie członkowskim, innemu właściwemu organowi w jednym z tych państw członkowskich, zgodnie z porozumieniem między zainteresowanymi właściwymi organami.

8. OSP, przy wsparciu ENTSO energii elektrycznej i we współpracy z organizacją OSD UE, opracowuje metodykę dotyczącą skali klasyfikacji cyberataków do dnia 13 czerwca 2025 r. OSP, przy udziale ENTSO energii elektrycznej i organizacji OSD UE, mogą zwrócić się do właściwych organów o skonsultowanie się z ENISA oraz do swoich właściwych organów odpowiedzialnych za cyberbezpieczeństwo o pomoc w opracowywaniu takiej skali klasyfikacji. Metodyka ta zapewnia klasyfikację wagi cyberataku według pięciu poziomów, przy czym dwa najwyższe poziomy to poziom „wysoki" i „krytyczny". Podstawą klasyfikacji jest ocena następujących parametrów:

a) potencjalny wpływ z uwzględnieniem narażonych aktywów i obszarów określonych zgodnie z art. 26 ust. 4 lit. c); oraz

b) dotkliwość cyberataku.

9. Do dnia 13 czerwca 2026 r. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE, przeprowadza studium wykonalności w celu oceny możliwości i kosztów finansowych niezbędnych do opracowania wspólnego narzędzia umożliwiającego wszystkim podmiotom wymianę informacji z właściwymi organami krajowymi.

10. W studium wykonalności uwzględnia się możliwość zastosowania takiego wspólnego narzędzia w celu:

a) wsparcia podmiotów o krytycznym wpływie i podmiotów o dużym wpływie w drodze zapewnienia na potrzeby operacji związanych z transgranicznymi przepływami energii elektrycznej odpowiednich informacji dotyczących bezpieczeństwa, takich jak zgłaszanie cyberataków w czasie zbliżonym do rzeczywistego, wczesne ostrzeżenia związane z kwestiami cyberbezpieczeństwa i nieujawnione podatności w urządzeniach używanych w systemie elektroenergetycznym;

b) utrzymywania tego narzędzia w odpowiednim i wysoce niezawodnym środowisku;

c) umożliwienia gromadzenia danych od podmiotów o krytycznym wpływie i podmiotów o dużym wpływie oraz ułatwianie usuwania informacji poufnych i anonimizacji danych oraz ich szybkiego rozpowszechniania wśród tych podmiotów.

11. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE:

a) zasięga opinii ENISA i grupy współpracy NIS, krajowych pojedynczych punktów kontaktowych oraz przedstawicieli głównych zainteresowanych stron przy przeprowadzaniu oceny wykonalności;

b) przedstawia wyniki studium wykonalności ACER i grupie współpracy NIS.

12. ENTSO energii elektrycznej, we współpracy z organizacją OSD UE może rozważać i ułatwiać realizację inicjatyw proponowanych przez podmioty o krytycznym wpływie i podmioty o dużym wpływie do celów oceny i testowania takich narzędzi wymiany informacji.

Artykuł 38

Rola podmiotów o dużym wpływie i podmiotów o krytycznym wpływie w odniesieniu do wymiany informacji

1. Każdy podmiot o dużym wpływie i podmiot o krytycznym wpływie:

a) ustala, w odniesieniu do wszystkich aktywów wchodzących w jego obszar cyberbezpieczeństwa określony zgodnie z art. 26 ust. 4 lit. c), co najmniej zdolności centrów operacyjnych cyberbezpieczeństwa w zakresie:

   (i) zapewnienia, aby odpowiednie sieci i systemy oraz aplikacje informatyczne generowały dzienniki bezpieczeństwa do celów monitorowania bezpieczeństwa, umożliwiające wykrywanie nieprawidłowości i gromadzenie informacji na temat cyberataków;

   (ii) monitorowania bezpieczeństwa, w tym wykrywania włamań i oceny podatności sieci i systemów informatycznych;

   (iii) prowadzenia analiz i, w razie potrzeby, podejmowania wszelkich działań wymaganych w ramach jego odpowiedzialności i zdolności do ochrony podmiotu;

   (iv) uczestniczenia w gromadzeniu i wymianie informacji opisanych w niniejszym artykule.

b) jest uprawniony do nabycia całości lub części tych zdolności zgodnie z lit. a) za pośrednictwem dostawców usług zarządzanych w zakresie bezpieczeństwa. Podmioty o krytycznym wpływie i podmioty o dużym wpływie pozostają odpowiedzialne za dostawców usług zarządzanych w zakresie bezpieczeństwa oraz prowadzą nadzór ich działań;

c) wyznaczają pojedynczy punkt kontaktowy na poziomie podmiotu do celów wymiany informacji.

2. ENISA może wydawać niewiążące wytyczne dotyczące ustanowienia takich zdolności lub zlecania odnośnych usług dostawcom usług zarządzanych w zakresie bezpieczeństwa w charakterze podwykonawców w ramach zadania określonego w art. 6 ust. 2 rozporządzenia (UE) 2019/881.

3. Każdy podmiot o krytycznym wpływie i podmiot o dużym wpływie przekazuje swoim CSIRT i właściwemu organowi istotne informacje dotyczące cyberataków podlegających obowiązkowi zgłaszania bez zbędnej zwłoki i nie później niż w ciągu czterech godzin od uzyskania informacji, że dany incydent podlega obowiązkowi zgłaszania.

4. Informacje dotyczące cyberataku uznaje się za podlegające obowiązkowi zgłaszania, jeżeli podmiot, który padł ofiarą cyberataku, oceni jego dotkliwość w zakresie od „wysokiej" do „krytycznej" zgodnie z metodyką dotyczącą skali klasyfikacji cyberataków na podstawie art. 37 ust. 8. Pojedynczy punkt kontaktowy na poziomie podmiotu wyznaczony zgodnie z ust. 1 lit. c) powiadamia o klasyfikacji incydentu.

5. W przypadku gdy podmioty o krytycznym wpływie i podmioty o dużym wpływie zgłaszają do CSIRT istotne informacje dotyczące nienaprawionych aktywnie wykorzystywanych podatności, zespół ten może przekazać te informacje swojemu właściwemu organowi. Ze względu na poziom wrażliwości zgłaszanych informacji CSIRT może wstrzymać się z przekazaniem informacji lub przekazać je później z uzasadnionych względów związanych z cyberbezpieczeństwem.

6. Każdy podmiot o krytycznym wpływie i podmiot o dużym wpływie przekazuje bez zbędnej zwłoki swoim CSIRT wszelkie informacje dotyczące cyberzagrożenia podlegającego obowiązkowi zgłaszania, które może mieć skutki transgraniczne. Informacje dotyczące cyberzagrożenia uznaje się za podlegające obowiązkowi zgłaszania, jeżeli spełniony jest co najmniej jeden z następujących warunków:

a) zapewnia to istotne informacje dla innych podmiotów o krytycznym wpływie i podmiotów o dużym wpływie do celów zapobiegania wpływowi odnośnego ryzyka, wykrywania go, reagowania na niego lub łagodzenia go;

b) określone techniki, taktyki i procedury stosowane w kontekście ataku prowadzą do uzyskania takich informacji jak zagrożony adres URL lub adres IP, skróty lub wszelkie inne atrybuty przydatne do kontekstualizacji i skorelowania ataku;

c) cyberzagrożenie może zostać poddane dalszej ocenie i kontekstualizacji na podstawie dodatkowych informacji przekazywanych przez dostawców usług lub osoby trzecie niepodlegające niniejszemu rozporządzeniu.

7. Przy wymianie informacji na podstawie niniejszego artykułu każdy podmiot o krytycznym wpływie i podmiot o dużym wpływie wskazuje:

a) że informacje przedkładane są zgodnie z niniejszym rozporządzeniem;

b) czy informacje dotyczą:

(i) cyberataku podlegającego obowiązkowi zgłaszania, o którym mowa w ust. 3;

(ii) nienaprawionych aktywnie wykorzystywanych podatności nieujawnionych publicznie, o których mowa w ust. 4;

(iii) cyberzagrożenia podlegającego obowiązkowi zgłaszania, o którym mowa w ust. 5;

c) w przypadku cyberataku podlegającego obowiązkowi zgłaszania – poziom cyberataku zgodnie z metodyką dotyczącą skali klasyfikacji cyberataków, o której mowa w art. 37 ust. 8, oraz informacje będące podstawą tej klasyfikacji, w tym co najmniej dotkliwość cyberataku.

8. W przypadku gdy podmiot o krytycznym wpływie lub podmiot o dużym wpływie powiadamia o poważnym incydencie zgodnie z art. 23 dyrektywy (UE) 2022/2555, a zgłoszenie incydentu na podstawie tego artykułu zawiera istotne informacje wymagane na podstawie ust. 3 niniejszego artykułu, zgłoszenie dokonywane przez podmiot na podstawie art. 23 ust. 1 tej dyrektywy stanowi zgłoszenie informacji na podstawie ust. 3 niniejszego artykułu.

9. Każdy podmiot o krytycznym wpływie i podmiot o dużym wpływie dokonuje zgłoszeń do swojego właściwego organu lub CSIRT w drodze wyraźnego wskazania wyłącznie tych konkretnych informacji, które są udostępniane właściwemu organowi lub CSIRT w przypadkach, w których wymiana informacji mogłaby być źródłem cyberataku. Każdy podmiot o krytycznym wpływie i podmiot o dużym wpływie ma prawo przekazać właściwemu CSIRT nieopatrzoną klauzulą poufności wersję informacji.

Artykuł 39

Wykrywanie cyberataków i postępowanie z powiązanymi informacjami

1. Podmioty o krytycznym wpływie i podmioty o dużym wpływie rozwijają zdolności niezbędne do radzenia sobie z wykrytymi cyberatakami przy niezbędnym wsparciu ze strony odpowiedniego właściwego organu, ENTSO energii elektrycznej i organizacji OSD UE. CSIRT wyznaczony w odnośnym państwie członkowskim w ramach zadania przydzielonego CSIRT na mocy art. 11 ust. 5 lit. a) dyrektywy (UE) 2022/2555 może zapewniać wsparcie podmiotom o krytycznym wpływie i podmiotom o dużym wpływie. Podmioty o krytycznym wpływie i podmioty o dużym wpływie wdrażają skuteczne procesy w celu identyfikacji i klasyfikacji cyberataków, które będą lub mogą mieć wpływ na transgraniczne przepływy energii elektrycznej, oraz zminimalizowania ich wpływu i reagowania na nie.

2. Jeżeli cyberatak ma wpływ na transgraniczne przepływy energii elektrycznej pojedyncze punkty kontaktowe na poziomie podmiotu o krytycznym wpływie i podmiotu o dużym wpływie dotkniętego tym wpływem podejmują współpracę w celu prowadzenia wymiany informacji koordynowanej przez właściwy organ państwa członkowskiego, w którym cyberatak został po raz pierwszy zgłoszony.

3. Podmioty o krytycznym wpływie i podmioty o dużym wpływie:

a) zapewniają, aby ich własny pojedynczy punkt kontaktowy na poziomie podmiotu miał dostęp na zasadzie ograniczonego dostępu do informacji otrzymanych od krajowego pojedynczego punktu kontaktowego za pośrednictwem właściwego organu;

b) o ile nie dokonano tego już na podstawie art. 3 ust. 4 dyrektywy (UE) 2022/2555, przekazują właściwemu organowi państwa członkowskiego, w którym mają siedzibę, oraz krajowemu pojedynczemu punktowi kontaktowemu wykaz swoich pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa na poziomie podmiotu:

   (i) co do których ten właściwy organ i krajowy pojedynczy punkt kontaktowy mogą oczekiwać, że będą im one przekazywać informacje na temat cyberataków podlegających obowiązkowi zgłaszania;

   (ii) którym te właściwy organy i krajowe pojedyncze punkty kontaktowe będą w razie konieczności przykazywać informacje;

c) ustanawiają procedury zarządzania cyberatakami w odniesieniu do cyberataków, w tym role i obowiązki, zadania i działania służące reagowaniu, na podstawie możliwego do zaobserwowania rozwoju wypadków związanych z cyberatakiem w obszarach o krytycznym wpływie i obszarach o dużym wpływie;

d) testują ogólne procedury zarządzania cyberatakami co najmniej raz w roku w drodze zbadania co najmniej jednego scenariusza mającego bezpośredni lub pośredni wpływ na transgraniczne przepływy energii elektrycznej. Ten coroczny test może być przeprowadzany przez podmioty o krytycznym wpływie i podmioty o dużym wpływie podczas regularnych ćwiczeń, o których mowa w art. 43. Wszelkie bieżące działania służące reagowaniu na cyberataki, których skutki sklasyfikowane są co najmniej jako skutki o skali 2 zgodnie z metodyką dotyczącą skali klasyfikacji cyberataków, o której mowa w art. 37 ust. 8, oraz których podstawową przyczyną jest cyberbezpieczeństwo, mogą służyć jako coroczny test planu reagowania na cyberataki.

4. Państwa członkowskie mogą przekazać zadania, o których mowa w ust. 1, również regionalnym centrom koordynacyjnym zgodnie z art. 37 ust. 2 rozporządzenia (UE) 2019/943.

Artykuł 40

Zarządzanie w sytuacji kryzysowej

1. Jeżeli właściwy organ stwierdzi, że kryzys elektroenergetyczny jest związany z cyberatakiem, który ma wpływ na więcej niż jedno państwo członkowskie, właściwe organy z państw członkowskich dotkniętych kryzysem, właściwe organy odpowiedzialne za cyberbezpieczeństwo, właściwe organy ds. gotowości na wypadek zagrożeń oraz organy ds. zarządzania kryzysowego w cyberbezpieczeństwie w ramach NIS z państw członkowskich dotkniętych kryzysem tworzą wspólnie grupę koordynacyjną *ad hoc* ds. kryzysów transgranicznych.

2. Transgraniczna grupa koordynacyjna *ad hoc* ds. kryzysu:

a) koordynuje skuteczne pozyskanie i dalsze rozpowszechnianie wszelkich istotnych informacji dotyczących cyberbezpieczeństwa wśród podmiotów zaangażowanych w proces zarządzania kryzysowego;

b) organizuje komunikację między wszystkimi podmiotami dotkniętymi kryzysem a właściwymi organami, aby ograniczyć nakładanie się działań i zwiększyć skuteczność analiz i technicznych środków reagowania w celu zaradzenia jednoczesnym kryzysom elektroenergetycznym, których podstawową przyczyną jest cyberbezpieczeństwo;

c) zapewnia, we współpracy z właściwymi CSIRT, wymaganą wiedzę fachową, w tym doradztwo operacyjne w zakresie wdrażania ewentualnych środków ograniczających ryzyko, na rzecz podmiotów dotkniętych incydentem;

d) powiadamia Komisję i Grupę Koordynacyjną ds. Energii Elektrycznej o stanie incydentu i regularnie przekazuje im aktualne informacje na ten temat, zgodnie z zasadami ochrony określonymi w art. 46;

e) zasięga porady odpowiednich organów, agencji lub podmiotów, które mogą pomóc w łagodzeniu kryzysu elektroenergetycznego.

3. W przypadku gdy cyberatak kwalifikuje się lub oczekuje się, że będzie się kwalifikować jako incydent w cyberbezpieczeństwie na dużą skalę, grupa koordynacyjna *ad hoc* ds. kryzysów transgranicznych niezwłocznie informuje krajowe organy ds. zarządzania kryzysowego w cyberbezpieczeństwie zgodnie z art. 9 ust. 1 dyrektywy (UE) 2022/2555 w państwach członkowskich, których dotyczy incydent, a także Komisję i EU-CyCLONe. W takiej sytuacji grupa koordynacyjna *ad hoc* ds. kryzysów transgranicznych wspiera EU-CyCLONe w odniesieniu do kwestii specyficznych dla sektora.

4. Podmioty o krytycznym wpływie i podmioty o dużym wpływie rozwijają i utrzymują zdolności w zakresie wykrywania i łagodzenia kryzysów transgranicznych oraz opracowują i utrzymują wewnętrzne wytyczne i plany gotowości w tym zakresie, a ponadto posiadają personel biorący udział w wykrywaniu i łagodzeniu takich kryzysów. Podmiot o krytycznym wpływie lub podmiot o dużym wpływie, na który ma wpływ jednoczesny kryzys elektroenergetyczny, bada podstawową przyczynę takiego kryzysu we współpracy ze swoim właściwym organem w celu określenia zakresu, w jakim kryzys jest związany z cyberatakiem.

5. Państwa członkowskie mogą przekazać zadania określone w ust. 4 również regionalnym centrom koordynacyjnym zgodnie z art. 37 ust. 2 rozporządzenia (UE) 2019/943.

Artykuł 41

Plany zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie

1. W terminie 24 miesięcy od przekazania ACER ogólnounijnego sprawozdania z oceny ryzyka ACER opracowuje w ścisłej współpracy z ENISA, ENTSO energii elektrycznej, organizacją OSD UE, właściwymi organami odpowiedzialnymi za cyberbezpieczeństwo, właściwymi organami, właściwymi organami ds. gotowości na wypadek zagrożeń, oraz krajowymi organami ds. zarządzania kryzysowego w cyberbezpieczeństwie w ramach NIS oraz krajowymi organami regulacyjnymi plan zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie na szczeblu Unii dla sektora energii elektrycznej.

2. W terminie 12 miesięcy od opracowania przez ACER planu zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie na szczeblu Unii dla sektora energii elektrycznej zgodnie z ust. 1 każdy właściwy organ opracowuje krajowy plan zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej, uwzględniając plan zarządzania kryzysami w dziedzinie cyberbezpieczeństwa na szczeblu Unii oraz krajowy plan gotowości na wypadek zagrożeń ustanowiony zgodnie z art. 10 rozporządzenia (UE) 2019/941. Plan ten musi być spójny z planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę przyjętym na podstawie art. 9 ust. 4 dyrektywy (UE) 2022/2555. Właściwy organ koordynuje działania z podmiotami o krytycznym wpływie i podmiotami o dużym wpływie oraz z właściwym organem ds. gotowości na wypadek zagrożeń w swoim państwie członkowskim.

3. Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę wymagany na podstawie art. 9 ust. 4 dyrektywy (UE) 2022/2555 uznaje się za krajowy plan zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie na podstawie niniejszego artykułu, jeżeli zawiera on postanowienia dotyczące zarządzania kryzysami i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej.

4. Państwa członkowskie mogą przekazać zadania wymienione w ust. 1 i 2 również regionalnym centrom koordynacyjnym zgodnie z art. 37 ust. 2 rozporządzenia (UE) 2019/943.

5. Podmioty o krytycznym wpływie i podmioty o dużym wpływie zapewniają, że ich procesy związane z zarządzaniem kryzysami w dziedzinie cyberbezpieczeństwa:

a) przewidują zgodne procedury obsługi incydentów transgranicznych w dziedzinie cyberbezpieczeństwa zgodnie z definicją zawartą w art. 6 pkt 8 dyrektywy (UE) 2022/2555, formalnie włączone do ich planów zarządzania kryzysowego;

b) są częścią ogólnych działań w zakresie zarządzania kryzysowego.

6. W terminie 12 miesięcy od powiadomienia podmiotów o dużym wpływie i podmiotów o krytycznym wpływie zgodnie z art. 24 ust. 6, a następnie co trzy lata, podmioty o krytycznym wpływie i podmioty o dużym wpływie opracowują na poziomie podmiotu plan zarządzania kryzysowego dotyczący kryzysu związanego z cyberbezpieczeństwem, który to plan uwzględniają w swoich ogólnych planach zarządzania kryzysowego. Plan ten zawiera co najmniej następujące elementy:

a) zasady ogłoszenia kryzysu zgodnie z art. 14 ust. 2 i 3 rozporządzenia (UE) 2019/941;

b) jasne role i obowiązki w zakresie zarządzania kryzysowego, w tym rolę innych istotnych podmiotów o krytycznym wpływie i podmiotów o dużym wpływie;

c) aktualne dane kontaktowe, a także zasady komunikacji i wymiany informacji w sytuacji kryzysowej, w tym połączenie z CSIRT.

7. Środki zarządzania kryzysowego na podstawie art. 21 ust. 2 lit. c) dyrektywy (UE) 2022/2555 uznaje się za plan zarządzania kryzysowego na poziomie podmiotu dla sektora energii elektrycznej na podstawie niniejszego artykułu, jeżeli obejmuje on wszystkie wymogi wymienione w ust. 6.

8. Plany zarządzania kryzysowego testuje się podczas ćwiczeń w dziedzinie cyberbezpieczeństwa, o których mowa w art. 43, 44 i 45.

9. Podmioty o krytycznym wpływie i podmioty o dużym wpływie włączają swoje plany zarządzania kryzysowego na poziomie podmiotu do swoich planów ciągłości działania dotyczących procesów o krytycznym wpływie i procesów o dużym wpływie. Plany zarządzania kryzysowego na poziomie podmiotu obejmują:

a) procesy zależne od dostępności, integralności i niezawodności usług informatycznych;

b) wszystkie lokalizacje istotne dla ciągłości działania, w tym lokalizacje sprzętu i oprogramowania;

c) wszystkie wewnętrzne role i obowiązki związane z procesami ciągłości działania.

10. Podmioty o krytycznym wpływie i podmioty o dużym wpływie aktualizują swoje plany zarządzania kryzysowego na poziomie podmiotu co najmniej raz na trzy lata oraz w razie potrzeby.

11. ACER aktualizuje plan zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie na szczeblu Unii dla sektora energii elektrycznej, opracowany zgodnie z ust. 1, co najmniej raz na trzy lata oraz w razie potrzeby.

12. Każdy właściwy organ aktualizuje krajowy plan zarządzania kryzysami w dziedzinie cyberbezpieczeństwa i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej opracowany zgodnie z ust. 2 co najmniej raz na trzy lata i w razie potrzeby.

13. Podmioty o krytycznym wpływie i podmioty o dużym wpływie testują swoje plany ciągłości działania co najmniej raz na trzy lata lub po istotnych zmianach w procesach o krytycznym wpływie. Wyniki testów planu ciągłości działania są dokumentowane. Podmioty o krytycznym wpływie i podmioty o dużym wpływie mogą włączyć test swojego planu ciągłości działania do ćwiczeń w dziedzinie cyberbezpieczeństwa.

14. Podmioty o krytycznym wpływie i podmioty o dużym wpływie aktualizują swój plan ciągłości działania w razie potrzeby i co najmniej raz na trzy lata, z uwzględnieniem wyników testu.

15. Jeżeli w wyniku testu wykryte zostaną niedociągnięcia w planie ciągłości działania, podmiot o krytycznym wpływie i podmiot o dużym wpływie koryguje te niedociągnięcia w terminie 180 dni kalendarzowych od przeprowadzenia testu i przeprowadza nowy test w celu przedstawienia dowodów na to, że środki naprawcze są skuteczne.

16. Jeżeli podmiot o krytycznym wpływie lub podmiot o dużym wpływie nie jest w stanie usunąć niedociągnięć w terminie 180 dni kalendarzowych, przedstawia uzasadnienie w sprawozdaniu przekazywanym właściwemu organowi zgodnie z art. 27.

Artykuł 42

Zdolności wczesnego ostrzegania w zakresie cyberbezpieczeństwa w odniesieniu do sektora energii elektrycznej

1. Właściwe organy współpracują z ENISA w celu rozwijania zdolności wczesnego ostrzegania w zakresie cyberbezpieczeństwa w odniesieniu do energii elektrycznej (ECEAC) w ramach pomocy udzielanej państwom członkowskim zgodnie z art. 6 ust. 2 i 7 rozporządzenia (UE) 2019/881.

2. ECEAC umożliwiają ENISA, podczas wykonywania zadań wymienionych w art. 7 ust. 7 rozporządzenia (UE) 2019/881:

a) gromadzenie dobrowolnie udostępnianych informacji przekazywanych przez:

   (i) CSIRT, właściwe organy;

   (ii) podmioty wymienione w art. 2 niniejszego rozporządzenia;

   (iii) każdy inny podmiot, który chce dobrowolnie udostępniać istotne informacje;

b) ocenę i klasyfikację gromadzonych informacji;

c) ocenę informacji, do których ENISA ma dostęp, pod kątem określenia warunków ryzyka w cyberprzestrzeni oraz odpowiednich wskaźników dotyczących aspektów transgranicznych przepływów energii elektrycznej;

d) określenie warunków i wskaźników, które są często skorelowane z cyberatakami w sektorze energii elektrycznej;

e) określenie – w drodze oceny i identyfikacji czynników ryzyka – czy należy podjąć dalszą analizę i działania zapobiegawcze w drodze oceny i identyfikacji czynników ryzyka;

f) informowanie właściwych organów o stwierdzonych zagrożeniach i zalecanych działaniach zapobiegawczych właściwych dla zainteresowanych podmiotów;

g) informowanie wszystkich odpowiednich podmiotów wymienionych w art. 2 o wynikach oceny informacji zgodnie z niniejszym ustępem lit. b), c) i d);

h) okresowe uwzględnianie odpowiednich informacji w sprawozdaniu z orientacji sytuacyjnej, sporządzonym zgodnie z art. 7 ust. 6 rozporządzenia (UE) 2019/881;

i) w miarę możliwości wyprowadzanie, z zebranych informacji, odpowiednich danych wskazujących na potencjalne naruszenie bezpieczeństwa lub cyberatak („oznaki naruszenia integralności systemu").

3. CSIRT niezwłocznie przekazują informacje otrzymane od ENISA zainteresowanym podmiotom w ramach ich zadań określonych w art. 11 ust. 3 lit. b) dyrektywy (UE) 2022/2555.

4. ACER monitoruje skuteczność ECEAC. ENISA wspiera ACER, przekazując wszelkie niezbędne informacje zgodnie z art. 6 ust. 2 i art. 7 ust. 1 rozporządzenia (UE) 2019/881. Analiza tego działania w zakresie monitorowania stanowi część monitorowania zgodnie z art. 12 niniejszego rozporządzenia.

ROZDZIAŁ VI

RAMY ĆWICZEŃ W DZIEDZINIE CYBERBEZPIECZEŃSTWA W ODNIESIENIU DO ENERGII ELEKTRYCZNEJ

Artykuł 43

Ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie podmiotu i na poziomie państwa członkowskiego

1. Do dnia 31 grudnia roku następującego po powiadomieniu podmiotów o krytycznym wpływie, a następnie co trzy lata, każdy podmiot o krytycznym wpływie przeprowadza ćwiczenie w dziedzinie cyberbezpieczeństwa obejmujące co najmniej jeden scenariusz cyberataków mających bezpośredni lub pośredni wpływ na transgraniczne przepływy energii elektrycznej i związanych z ryzykiem zidentyfikowanym w ramach ocen ryzyka w cyberprzestrzeni na poziomie państwa członkowskiego i podmiotu zgodnie z art. 20 i art. 27.

2. Na zasadzie odstępstwa od ust. 1 właściwy organ ds. gotowości na wypadek zagrożeń po konsultacji z właściwym organem i odpowiednim organem ds. zarządzania kryzysowego w cyberbezpieczeństwie wyznaczonymi lub ustanowionymi na podstawie art. 9 dyrektywy (UE) 2022/2555 może podjąć decyzję o zorganizowaniu ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie państwa członkowskiego, jak opisano w ust. 1, zamiast przeprowadzania ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie podmiotu. W tym względzie właściwy organ informuje:

a) wszystkie podmioty o krytycznym wpływie z danego państwa członkowskiego, krajowy organ regulacyjny, CSIRT oraz właściwy organ odpowiedzialny za cyberbezpieczeństwo najpóźniej do dnia 30 czerwca roku poprzedzającego przeprowadzenie ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie podmiotu;

b) każdy podmiot, który uczestniczy w ćwiczeniu w dziedzinie cyberbezpieczeństwa na szczeblu państwa członkowskiego, najpóźniej 6 miesięcy przed rozpoczęciem ćwiczenia.

3. Właściwy organ ds. gotowości na wypadek zagrożeń przy wsparciu technicznym jego CSIRT organizuje ćwiczenie w dziedzinie cyberbezpieczeństwa określone w ust. 2 na poziomie państwa członkowskiego niezależnie lub w kontekście innego ćwiczenia w dziedzinie cyberbezpieczeństwa w danym państwie członkowskim. Aby móc grupować te ćwiczenia, właściwy organ ds. gotowości na wypadek zagrożeń może odroczyć o jeden rok przeprowadzenie ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie państwa członkowskiego, o którym mowa w ust. 1.

4. Ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie podmiotu i na poziomie państw członkowskich muszą być spójne z krajowymi ramami zarządzania kryzysowego w cyberbezpieczeństwie zgodnie z art. 9 ust. 4 lit. d) dyrektywy (UE) 2022/2555.

5. Do dnia 31 grudnia 2026 r., a następnie co trzy lata ENTSO energii elektrycznej we współpracy z organizacją OSD UE udostępnia wzór scenariusza ćwiczeń na potrzeby przeprowadzania ćwiczeń w dziedzinie cyberbezpieczeństwa na poziomie podmiotu i państwa członkowskiego, o których mowa w ust. 1. We wzorze tym bierze się pod uwagę wyniki ostatnio przeprowadzonej oceny ryzyka w cyberprzestrzeni na poziomie podmiotu i państwa członkowskiego oraz uwzględnia się kluczowe kryteria powodzenia. ENTSO energii elektrycznej i organizacja OSD UE angażują ACER i ENISA w opracowywanie takiego wzoru.

Artykuł 44

Regionalne lub międzyregionalne ćwiczenia w dziedzinie cyberbezpieczeństwa

1. Do dnia 31 grudnia 2029 r., a następnie co trzy lata, w każdym regionie pracy systemu ENTSO energii elektrycznej we współpracy z organizacją OSD UE organizuje regionalne ćwiczenie w dziedzinie cyberbezpieczeństwa. Podmioty o krytycznym wpływie w danym regionie pracy systemu uczestniczą w regionalnym ćwiczeniu w dziedzinie cyberbezpieczeństwa. ENTSO energii elektrycznej we współpracy z organizacją OSD UE może zamiast regionalnego ćwiczenia w dziedzinie cyberbezpieczeństwa zorganizować międzyregionalne ćwiczenia w dziedzinie cyberbezpieczeństwa w więcej niż jednym regionie pracy systemu w tych samych ramach czasowych. W ćwiczeniu tym należy uwzględnić inne istniejące oceny ryzyka i scenariusze w zakresie cyberbezpieczeństwa i scenariusze opracowane na poziomie Unii.

2. ENISA wspiera ENTSO energii elektrycznej i organizację OSD UE w przygotowaniu i organizacji ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie regionalnym lub międzyregionalnym.

3. ENTSO energii elektrycznej w koordynacji z organizacją OSD UE informuje podmioty o krytycznym wpływie, które uczestniczą w regionalnym lub międzyregionalnym ćwiczeniu w dziedzinie cyberbezpieczeństwa, na sześć miesięcy przed jego przeprowadzeniem.

4. Organizator regularnego ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie unijnym zgodnie z art. 7 ust. 5 rozporządzenia (UE) 2019/881 lub jakiegokolwiek obowiązkowego ćwiczenia w dziedzinie cyberbezpieczeństwa związanego z sektorem energii elektrycznej w tym samym obszarze geograficznym może zaprosić do udziału ENTSO energii elektrycznej i organizację OSD UE. W takich przypadkach obowiązek określony w ust. 1 nie ma zastosowania, pod warunkiem że w tym samym działaniu uczestniczą wszystkie podmioty o krytycznym wpływie w danym regionie pracy systemu.

5. Jeżeli ENTSO energii elektrycznej i organizacja OSD UE uczestniczą w ćwiczeniu w dziedzinie cyberbezpieczeństwa, o którym mowa w ust. 4, mogą odroczyć o jeden rok przeprowadzenie regionalnego lub międzyregionalnego ćwiczenia w dziedzinie cyberbezpieczeństwa, o którym mowa w ust. 1.

6. Do dnia 31 grudnia 2027 r., a następnie co trzy lata ENTSO energii elektrycznej w koordynacji z organizacją OSD UE udostępnia wzór ćwiczeń na potrzeby przeprowadzania regionalnych i międzyregionalnych ćwiczeń w dziedzinie cyberbezpieczeństwa. We wzorze tym bierze się pod uwagę wyniki ostatnio przeprowadzonej oceny ryzyka w cyberprzestrzeni na poziomie regionalnym oraz uwzględnia się kluczowe kryteria powodzenia. ENTSO energii elektrycznej konsultuje się z Komisją oraz może zasięgać porady ACER, ENISA i Wspólnego Centrum Badawczego w kwestii organizacji i przeprowadzania regionalnych i międzyregionalnych ćwiczeń w dziedzinie cyberbezpieczeństwa.

Artykuł 45

Wyniki ćwiczeń w dziedzinie cyberbezpieczeństwa na poziomie podmiotu, państwa członkowskiego, regionalnym lub międzyregionalnym

1. Na wniosek podmiotu o krytycznym wpływie kluczowi dostawcy usług uczestniczą w ćwiczeniach w dziedzinie cyberbezpieczeństwa, o których mowa w art. 43 ust. 1 i 2 oraz w art. 44 ust. 1, jeżeli świadczą usługi na rzecz podmiotu o krytycznym wpływie w obszarze odpowiadającym zakresowi odpowiedniego ćwiczenia w dziedzinie cyberbezpieczeństwa.

2. Organizatorzy ćwiczeń w dziedzinie cyberbezpieczeństwa, o których mowa w art. 43 ust. 1 i 2 oraz w art. 44 ust. 1, za radą ENISA, jeżeli o to wniosą, i zgodnie z art. 7 ust. 5 rozporządzenia (UE) 2019/881, analizują i finalizują odpowiednie ćwiczenia w dziedzinie cyberbezpieczeństwa w drodze sprawozdania podsumowującego wnioski skierowanego do wszystkich uczestników. Sprawozdanie to obejmuje:

a) scenariusze ćwiczeń, sprawozdania ze spotkań, najważniejsze stanowiska, sukcesy i wnioski odnotowane na każdym szczeblu łańcucha wartości energii elektrycznej;

b) spełnienie kluczowych kryteriów powodzenia;

c) wykaz zaleceń dla podmiotów uczestniczących w odpowiednim ćwiczeniu w dziedzinie cyberbezpieczeństwa w celu skorygowania, dostosowania lub zmiany procesów, procedur, powiązanych modeli zarządzania oraz wszelkich istniejących zobowiązań umownych z kluczowymi dostawcami usług.

3. Na wniosek sieci CSIRT, grupy współpracy NIS lub EU-CyCLONe, organizatorzy ćwiczeń w dziedzinie cyberbezpieczeństwa, o których mowa w art. 43 ust. 1 i 2 oraz art. 44 ust. 1, udostępniają wyniki odpowiedniego ćwiczenia w dziedzinie cyberbezpieczeństwa. Organizatorzy udostępniają każdemu podmiotowi uczestniczącemu w ćwiczeniach informacje, o których mowa w ust. 2 lit. a) i b) niniejszego artykułu. Organizatorzy udostępniają wykaz zaleceń, o którym mowa w tym ustępie lit. c), wyłącznie podmiotom, do których odnoszą się te zalecenia.

4. Organizatorzy ćwiczeń w dziedzinie cyberbezpieczeństwa, o których mowa w art. 43 ust. 1 i 2 oraz art. 44 ust. 1, regularnie podejmują wraz z podmiotami uczestniczącymi w ćwiczeniach działania następcze w związku z wdrażaniem zaleceń zgodnie z ust. 2 lit. c) niniejszego artykułu.

ROZDZIAŁ VII

OCHRONA INFORMACJI

Artykuł 46

Zasady ochrony informacji podlegających wymianie

1. Podmioty wymienione w art. 2 ust. 1 zapewniają, aby informacje dostarczane, otrzymywane, wymieniane lub przekazywane na podstawie niniejszego rozporządzenia były dostępne wyłącznie na zasadzie ograniczonego dostępu i zgodnie z odpowiednimi przepisami Unii oraz przepisami krajowymi dotyczącymi bezpieczeństwa informacji.

2. Podmioty wymienione w art. 2 ust. 1 zapewniają, aby informacje dostarczane, otrzymywane, wymieniane lub przekazywane na podstawie niniejszego rozporządzenia były przetwarzane i monitorowane przez cały cykl życia tych informacji oraz aby informacje te można było udostępnić po zakończeniu ich cyklu życia dopiero wtedy, gdy zostaną zanonimizowane.

3. Podmioty wymienione w art. 2 ust. 1 zapewniają wprowadzenie wszelkich niezbędnych środków ochrony o charakterze organizacyjnym i technicznym w celu zabezpieczenia i ochrony poufności, integralności, dostępności i niezaprzeczalności informacji dostarczanych, otrzymywanych, wymienianych lub przekazywanych na podstawie niniejszego rozporządzenia, niezależnie od wykorzystanych środków. Środki ochrony powinny:

a) być proporcjonalne;

b) uwzględniać ryzyko w cyberprzestrzeni związane ze znanymi przeszłymi i pojawiającymi się zagrożeniami, którym takie informacje mogą podlegać w kontekście niniejszego rozporządzenia;

c) w miarę możliwości opierać się na krajowych, europejskich lub międzynarodowych normach i najlepszych praktykach;

d) być odpowiednio udokumentowane.

4. Podmioty wymienione w art. 2 ust. 1 zapewniają, aby każda osoba fizyczna, której przyznano dostęp do informacji dostarczanych, otrzymywanych, wymienianych lub przekazywanych na podstawie niniejszego rozporządzenia, była informowana o zasadach bezpieczeństwa mających zastosowanie na poziomie podmiotu oraz o środkach i procedurach mających znaczenie do celów ochrony informacji. Podmioty te zapewniają, aby zainteresowana osoba fizyczna uznała odpowiedzialność za ochronę informacji zgodnie z instrukcjami przekazanymi w ramach briefingu.

5. Podmioty wymienione w art. 2 ust. 1 zapewniają, aby dostęp do informacji dostarczanych, otrzymywanych, wymienianych lub przekazywanych na podstawie niniejszego rozporządzenia był ograniczony do osób fizycznych:

a) które są uprawnione do dostępu do tych informacji w oparciu o ich funkcje i był ograniczony do wykonywania powierzonych im zadań;

b) w odniesieniu do których podmiot był w stanie ocenić zasady etyki i uczciwości, a także w odniesieniu do których nie ma dowodów na negatywny wynik sprawdzenia przeszłości w celu oceny wiarygodności danej osoby fizycznej zgodnie z najlepszymi praktykami i standardowymi wymogami bezpieczeństwa stosowanymi przez podmiot oraz, w razie potrzeby, z krajowymi przepisami ustawowymi i wykonawczymi.

6. Przed przekazaniem informacji osobie trzeciej nieobjętej zakresem stosowania niniejszego rozporządzenia podmioty wymienione w art. 2 ust. 1 muszą uzyskać pisemną zgodę osoby fizycznej lub prawnej, która pierwotnie stworzyła lub przekazała te informacje.

7. Podmiot wymieniony w art. 2 ust. 1 może uznać, że informacje te muszą zostać udostępnione bez zapewnienia zgodności z ust. 1 i 4 niniejszego artykułu, aby zapobiec jednoczesnemu kryzysowi elektroenergetycznemu, którego podstawową przyczyną jest cyberbezpieczeństwo, lub jakimkolwiek kryzysom transgranicznym w Unii w innym sektorze. W takim przypadku podmiot ten:

a) zasięga opinii właściwego organu i zostaje przez ten organ upoważniony do dzielenia się takimi informacjami;

b) anonimizuje takie informacje, nie tracąc przy tym elementów niezbędnych, by poinformować opinię publiczną o nadchodzącym i poważnym zagrożeniu dla transgranicznych przepływów energii elektrycznej oraz o możliwych środkach łagodzących;

c) zabezpiecza tożsamość inicjatora i podmiotów, które przetwarzały takie informacje na podstawie niniejszego rozporządzenia.

8. Na zasadzie odstępstwa od ust. 6 niniejszego artykułu właściwe organy mogą przekazywać informacje dostarczone, otrzymane, wymienione lub przekazane na podstawie niniejszego rozporządzenia osobie trzeciej niewymienionej w art. 2 ust. 1 bez uprzedniej pisemnej zgody inicjatora informacji, ale informując go w jak najkrótszym czasie. Przed ujawnieniem jakichkolwiek informacji dostarczonych, otrzymanych, wymienionych lub przekazanych na podstawie niniejszego rozporządzenia osobie trzeciej niewymienionej w art. 2 ust. 1 zainteresowany właściwy organ w sposób uzasadniony zapewnia, aby dana osoba trzecia znała obowiązujące przepisy bezpieczeństwa, i uzyskuje wystarczającą pewność, że dana osoba trzecia może chronić otrzymane informacje zgodnie z ust. 1–5 niniejszego artykułu. Właściwy organ anonimizuje takie informacje, nie tracąc przy tym elementów niezbędnych, by poinformować opinię publiczną o bezpośrednim i poważnym zagrożeniu dla transgranicznych przepływów energii elektrycznej oraz o możliwych środkach łagodzących, a także chroni tożsamość inicjatora informacji. W takim przypadku osoba trzecia niewymieniona w art. 2 ust. 1 chroni otrzymane informacje zgodnie z przepisami obowiązującymi już na poziomie podmiotu lub, jeżeli nie jest to możliwe, zgodnie z przepisami i instrukcjami przekazanymi przez odpowiedni właściwy organ.

9. Niniejszy artykuł nie ma zastosowania do podmiotów niewymienionych w art. 2 ust. 1, które otrzymują informacje zgodnie z ust. 6 niniejszego artykułu. W takim przypadku stosuje się ust. 7 niniejszego artykułu lub właściwy organ może przekazać temu podmiotowi na piśmie przepisy, które będą miały zastosowanie w przypadku otrzymania informacji na podstawie niniejszego rozporządzenia.

Artykuł 47

Poufność informacji

1. Wszelkie informacje dostarczane, otrzymywane, wymieniane lub przekazywane na podstawie niniejszego rozporządzenia podlegają warunkom tajemnicy zawodowej określonym w ust. 2–5 niniejszego artykułu niniejszego rozporządzenia oraz wymogom określonym w art. 65 rozporządzenia (UE) 2019/943. Wszelkie informacje dostarczane, otrzymywane, wymieniane lub przekazywane między podmiotami wymienionymi w art. 2 niniejszego rozporządzenia do celów wdrożenia niniejszego rozporządzenia podlegają ochronie z uwzględnieniem poziomu poufności informacji zastosowanego przez inicjatora.

2. Do podmiotów wymienionych w art. 2 ma zastosowanie obowiązek zachowania tajemnicy zawodowej.

3. Właściwe organy odpowiedzialne za cyberbezpieczeństwo, krajowe organy regulacyjne, właściwe organy ds. gotowości na wypadek zagrożeń i CSIRT wymieniają się wszelkimi informacjami niezbędnymi do wykonywania ich zadań.

4. Wszelkie informacje otrzymywane, wymieniane lub przekazywane między podmiotami wymienionymi w art. 2 w ust. 1 do celów wdrożenia art. 23 są anonimizowane i agregowane.

5. Informacje, które każdy podmiot lub organ podlegający przepisom niniejszego rozporządzenia otrzymał w trakcie wykonywania swoich obowiązków, nie mogą zostać ujawnione żadnym innym podmiotom ani organom, bez uszczerbku dla przypadków objętych prawem krajowym, innymi przepisami niniejszego rozporządzenia bądź innymi mającymi zastosowanie przepisami Unii.

6. Bez uszczerbku dla przepisów krajowych lub unijnych organ, podmiot lub osoba fizyczna, które otrzymują informacje na podstawie niniejszego rozporządzenia, nie mogą wykorzystywać ich do żadnych innych celów niż wykonywanie swoich obowiązków wynikających z niniejszego rozporządzenia.

7. ACER, po konsultacji z ENISA, wszystkimi właściwymi organami, ENTSO energii elektrycznej i organizacją OSD UE do dnia 13 czerwca 2025 r. wydaje wytyczne dotyczące mechanizmów wymiany informacji dla wszystkich podmiotów wymienionych w art. 2 ust. 1, a w szczególności przewidywanych przepływów wymiany informacji, oraz dotyczące metod anonimizacji i agregowania informacji do celów wykonywania przepisów niniejszego artykułu.

8. Informacje, które są poufne zgodnie z przepisami unijnymi i krajowymi, wymienia się z Komisją i innymi właściwymi organami tylko wtedy, gdy taka wymiana jest niezbędna do stosowania niniejszego rozporządzenia. Informacje podlegające wymianie ograniczają się do tego, co jest niezbędne na potrzeby takiej wymiany i proporcjonalne do jej celów. W ramach wymiany informacji zachowuje się poufność tych informacji oraz chroni się bezpieczeństwo i interesy handlowe podmiotów o krytycznym wpływie lub podmiotów o dużym wpływie.

ROZDZIAŁ VIII

PRZEPISY KOŃCOWE

Artykuł 48

Przepisy przejściowe

1. Do czasu zatwierdzenia warunków lub metod, o których mowa w art. 6 ust. 2, lub planów, o których mowa w art. 6 ust. 3, ENTSO energii elektrycznej we współpracy z organizacją OSD UE opracowuje niewiążące wytyczne dotyczące następujących kwestii:

a) tymczasowego wskaźnika wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej (ECII) zgodnie z ust. 2 niniejszego artykułu;

b) wstępnego wykazu ogólnounijnych procesów o dużym wpływie i procesów o krytycznym wpływie zgodnie z ust. 4 niniejszego artykułu; oraz

c) wstępnego wykazu europejskich i międzynarodowych norm i kontroli wymaganych na mocy przepisów krajowych, mających znaczenie dla aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej zgodnie z ust. 6 niniejszego artykułu.

2. Do dnia 13 października 2024 r. ENTSO energii elektrycznej we współpracy z organizacją OSD UE opracowuje zalecenie dotyczące tymczasowego ECII. ENTSO energii elektrycznej we współpracy z organizacją OSD UE powiadamia właściwe organy o zalecanym tymczasowym ECII.

3. Cztery miesiące od otrzymania zalecanego tymczasowego wskaźnika wpływu na cyberbezpieczeństwo w odniesieniu do energii elektrycznej lub najpóźniej do dnia 13 lutego 2025 r. właściwe organy określają kandydatów na podmioty o dużym wpływie podmioty o krytycznym wpływie w ich państwie członkowskim na podstawie zalecanego ECII i opracowują wstępny wykaz podmiotów o dużym wpływie i podmiotów o krytycznym wpływie. Podmioty o dużym wpływie i podmioty o krytycznym wpływie wskazane w wstępnym wykazie mogą dobrowolnie wypełniać swoje obowiązki określone w niniejszym rozporządzeniu w oparciu o zasadę ostrożności. Do dnia 13 marca 2025 r. właściwe organy powiadamiają podmioty wskazane w wykazie tymczasowym o tym, że zostały one uznane za podmioty o dużym wpływie lub podmioty o krytycznym wpływie.

4. Do dnia 13 grudnia 2024 r. ENTSO energii elektrycznej we współpracy z organizacją OSD UE opracowuje wstępny wykaz ogólnounijnych procesów o dużym wpływie i procesów o krytycznym wpływie. Podmioty powiadomione zgodnie z ust. 3, które dobrowolnie podejmują decyzję o wypełnieniu swoich obowiązków określonych w niniejszym rozporządzeniu w oparciu o zasadę ostrożności, stosują wstępny wykaz procesów o dużym wpływie i procesów o krytycznym wpływie w celu określenia wstępnych obszarów o dużym wpływie i obszarów o krytycznym wpływie oraz ustalenia, które aktywa należy uwzględnić w pierwszej ocenie ryzyka w cyberprzestrzeni na poziomie podmiotu.

5. Do dnia 13 września 2024 r. każdy właściwy organ zgodnie z art. 4 ust. 1 przedstawia ENTSO energii elektrycznej i organizacji OSD UE wykaz swoich przepisów krajowych mających znaczenie dla aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

6. Do dnia 13 czerwca 2025 r. ENTSO energii elektrycznej we współpracy z organizacją OSD UE przygotowuje wstępny wykaz europejskich i międzynarodowych norm i kontroli wymaganych na mocy przepisów krajowych, mających znaczenie dla aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, z uwzględnieniem informacji przekazanych przez właściwe organy.

7. Wstępny wykaz europejskich i międzynarodowych norm i kontroli obejmuje:

a) normy europejskie i międzynarodowe oraz przepisy krajowe zawierające wytyczne dotyczące metodyk zarządzania ryzykiem w cyberprzestrzeni na poziomie podmiotu; oraz

b) kontrole cyberbezpieczeństwa równoważne kontrolom, które mają stanowić część minimalnych i zaawansowanych kontroli cyberbezpieczeństwa.

8. ENTSO energii elektrycznej i organizacja OSD UE uwzględniają opinie przedstawione przez ENISA i ACER przy finalizacji wstępnego wykazu norm. ENTSO energii elektrycznej i organizacja OSD UE publikują wstępny wykaz europejskich i międzynarodowych norm i kontroli na swoich stronach internetowych.

9. ENTSO energii elektrycznej i organizacja OSD UE konsultują się z ENISA i ACER w kwestii propozycji niewiążących wytycznych opracowanych zgodnie z ust. 1.

10. Do czasu opracowania minimalnych i zaawansowanych kontroli cyberbezpieczeństwa zgodnie z art. 29 i przyjęcia ich zgodnie z art. 8 wszystkie podmioty wymienione w art. 2 ust. 1 dążą do tego, by stopniowo coraz szerzej stosować niewiążące wytyczne opracowane zgodnie z ust. 1.

Artykuł 49

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 11 marca 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN