

Bruksela, 20 kwietnia 2023 r.
(OR. en)

8512/23

Międzyinstytucjonalny numer
referencyjny:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	19 kwietnia 2023 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2023) 209 final
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY ustanawiającego środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty

Delegacje otrzymują w załączeniu dokument COM(2023) 209 final.

Załącznik: COM(2023) 209 final



KOMISJA
EUROPEJSKA

Strasburg, dnia 18.4.2023 r.
COM(2023) 209 final

2023/0109 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

**ustanawiające środki mające na celu zwiększenie solidarności i zdolności w Unii
w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów
w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia
i incydenty**

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejsze uzasadnienie towarzyszy wnioskowi dotyczącemu aktu w sprawie cybersolidarności. Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich zyskały podstawowe znaczenie we wszystkich sektorach działalności gospodarczej, gdyż administracje publiczne, przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej. Ta większa absorpcja technologii cyfrowych zwiększa narażenie na incydenty w cyberbezpieczeństwie i ich potencjalne skutki. Jednocześnie państwa członkowskie są narażone na coraz większe ryzyko w cyberprzestrzeni i ogólnie złożony krajobraz zagrożeń, w tym również wyraźne ryzyko szybkiego rozprzestrzeniania się incydentów w cyberbezpieczeństwie z jednego państwa członkowskiego na inne.

Ponadto cyberoperacje coraz częściej stanowią element strategii hybrydowych i wojennych, oddziałując w istotny sposób na cel. W szczególności rosyjską napaść na Ukrainę poprzedziła i nadal jej towarzyszy strategia wrogich cyberoperacji, co ma przełomowe znaczenie w kontekście postrzegania i oceny zbiorowej gotowości UE do zarządzania kryzysowego w zakresie cyberbezpieczeństwa oraz stanowi wezwanie do podjęcia pilnych działań. Zagrożenie możliwym incydem na dużą skalę powodującym poważne zakłócenie i uszkodzenie infrastruktur krytycznych wymaga podwyższonej gotowości na wszystkich szczeblach unijnego ekosystemu cyberbezpieczeństwa. To zagrożenie wykracza poza rosyjską napaść na Ukrainę i obejmuje ciągłe cyberzagrożenia ze strony podmiotów państwowych i niepaństwowych, które prawdopodobnie będą się utrzymywać, biorąc pod uwagę wielość podmiotów powiązanych z organami państwowymi oraz ze środowiskami przestępczymi i hakywistycznymi, które mają swój udział w generowaniu obecnych napięć geopolitycznych. W ostatnich latach nastąpił drastyczny wzrost liczby cyberataków, w tym ataków na łańcuchy dostaw, które to ataki mają na celu cyberszpiegostwo, instalację oprogramowania szantażującego lub wywołanie zakłóceń. W 2020 r. skutki ataku na łańcuch dostaw firmy SolarWinds dotknęły ponad 18 000 organizacji na całym świecie, w tym agencje rządowe i duże przedsiębiorstwa. Poważne incydenty w cyberbezpieczeństwie mogą być zbyt gwałtowne, aby jedno państwo członkowskie lub kilka państw członkowskich, których to dotyczy, mogły poradzić sobie z nimi samodzielnie. Z tego powodu konieczna jest większa solidarność na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie.

Jeżeli chodzi o wykrywanie cyberzagrożeń i cyberincydentów, należy pilnie zintensyfikować wymianę informacji i poprawić nasz zbiorowy potencjał, aby zdecydowanie skrócić czas potrzebny na wykrycie cyberzagrożeń, zanim spowodują szkody i koszty na dużą skalę¹.

¹ Jak wynika ze sprawozdania Ponemon Institute i IBM Security, w 2022 r. średni czas identyfikacji naruszenia wynosił 207 dni, przy czym na jego wyeliminowanie potrzeba było kolejnych 70 dni.

Chociaż wiele zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie ma potencjalnie transgraniczny wymiar z uwagi na wzajemne połączenie infrastruktury cyfrowych, wymiana istotnych informacji między państwami członkowskimi pozostaje ograniczona. W rozwiązywaniu tego problemu ma pomóc budowa sieci transgranicznych centrów monitorowania bezpieczeństwa (SOC) w celu zwiększenia zdolności w zakresie wykrywania i reagowania.

Jeżeli chodzi o gotowość i reagowanie na incydenty w cyberbezpieczeństwie, obecnie wsparcie na szczeblu unijnym i solidarność między państwami członkowskimi są ograniczone. W konkluzjach z października 2021 r. Rada podkreśliła potrzebę wyeliminowania tych luk, wzywając Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego².

Niniejsze rozporządzenie wdraża również przyjętą w grudniu 2020 r.³ unijną strategię cyberbezpieczeństwa, w której zapowiedziano utworzenie europejskiej tarczy cyberbezpieczeństwa, wzmacniającej zdolności w zakresie wykrywania cyberzagrożeń i wymiany informacji w Unii Europejskiej za pośrednictwem federacji krajowych i transgranicznych SOC.

Niniejsze rozporządzenie opiera się na pierwszych działaniach opracowanych już w ramach zamkniętej współpracy z głównymi zainteresowanymi stronami i wspieranych ze środków programu „Cyfrowa Europa”. W szczególności, w odniesieniu do SOC, w programie prac w zakresie cyberbezpieczeństwa na lata 2021–2022 w ramach programu „Cyfrowa Europa” zawarto zaproszenie do wyrażenia zainteresowania udziałem we wspólnych zamówieniach na narzędzia i infrastruktury niezbędne do utworzenia transgranicznych SOC oraz zaproszenie do składania wniosków o dotacje w celu umożliwienia budowania zdolności SOC obsługujących organizacje publiczne i prywatne. Jeżeli chodzi o gotowość i reagowanie na incydenty, Komisja ustanowiła krótkoterminowy program wspierania państw członkowskich, przyznając Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dodatkowe środki finansowe, aby w trybie natychmiastowym zwiększyć gotowość i zdolność do reagowania na poważne cyberincydenty. Oba działania przygotowano w ścisłej koordynacji z państwami członkowskimi. W niniejszym rozporządzeniu odniesiono się do niedociągnięć w tych działaniach i uwzględniono wnioski z ich realizacji.

Niniejszy wniosek stanowi również realizację zobowiązania podjętego zgodnie ze wspólnym komunikatem w sprawie cyberobrony⁴ przyjętym w dniu 10 listopada, dotyczącego przygotowania wniosku w sprawie inicjatywy na rzecz cybersolidarności UE o następujących

Jednocześnie w 2022 r. koszty incydentów powodujących naruszenie ochrony danych, które trwały ponad 200 dni, wyniosły średnio 4,86 mln EUR, w porównaniu z 3,74 mln EUR w przypadku naruszeń trwających krócej niż 200 dni („Cost of a data breach 2022”, <https://www.ibm.com/reports/data-breach>).

² Konkluzje Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni zatwierdzone przez Radę na posiedzeniu w dniu 23 maja 2022 r. (9364/22).

³ Wspólny komunikat do Parlamentu Europejskiego i Rady: Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN(2020) 18 final.

⁴ Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.

celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania, stopniowe tworzenie na szczeblu UE rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców oraz wspieranie przeprowadzania testów w podmiotach krytycznych.

W tym kontekście Komisja przedkłada niniejszy akt w sprawie cybersolidarności w celu zwiększenia solidarności na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie, realizując następujące cele szczegółowe:

- wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie, a tym samym wniesienie wkładu w europejską suwerenność technologiczną w dziedzinie cyberbezpieczeństwa;
- zwiększenie gotowości krytycznych podmiotów w całej UE oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu wsparcia w reagowaniu na incydenty państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;
- zwiększenie odporności Unii i przyczynianie się do skutecznej reakcji dzięki przeglądowi i ocenie poważnych incydentów lub incydentów na dużą skalę, w tym wyciągnięciu wniosków i w stosownych przypadkach wydaniu zaleceń.

Realizacja tych celów odbywać się będzie za pośrednictwem następujących funduszy/instrumentów:

- wprowadzenie ogólnoeuropejskiej infrastruktury SOC (europejskiej tarczy cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej;
- stworzenie mechanizmu cyberkryzysowego, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków. Wsparcie w reagowaniu na incydenty udostępnia się również europejskim instytucjom, organom, urzędom i agencjom Unii;
- ustanowienie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę.

Europejska tarcza cyberbezpieczeństwa oraz mechanizm cyberkryzysowy będą objęte wsparciem ze środków programu „Cyfrowa Europa”, który niniejszy instrument ustawodawczy zmieni w celu wprowadzenia wyżej wymienionych działań, zapewnienia wsparcia finansowego na ich rozwój oraz doprecyzowania warunków korzystania ze wsparcia finansowego.

•**Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Ramy unijne obejmują szereg przepisów, które już obowiązują lub które zaproponowano na szczeblu UE, mających na celu zmniejszenie podatności, zwiększenie odporności podmiotów krytycznych na ryzyko w cyberprzestrzeni oraz wsparcie skoordynowanego zarządzania incydentami i kryzysami w cyberbezpieczeństwie na dużą skalę, w szczególności dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS 2)⁵, akt o cyberbezpieczeństwie⁶, dyrektywę dotyczącą ataków na systemy informatyczne⁷ oraz zalecenie Komisji (UE) 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę⁸.

Działania proponowane w akcie w sprawie cybersolidarności obejmują orientację sytuacyjną, wymianę informacji oraz wsparcie w zakresie gotowości i reagowania na incydenty w cyberbezpieczeństwie. Działania te są spójne z celami ram regulacyjnych obowiązujących na poziomie Unii, w szczególności celami dyrektywy (UE) 2022/2555 („dyrektywy NIS 2”), i wspierają realizację tych celów. Akt w sprawie cybersolidarności będzie opierał się przede wszystkim na istniejących ramach współpracy operacyjnej w zakresie cyberbezpieczeństwa oraz ramach zarządzania kryzysowego i będzie wspierał te ramy, w szczególności europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONE) i sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

Platformy transgranicznych SOC powinny stanowić nową zdolność, która jest uzupełnieniem sieci CSIRT, przez gromadzenie danych na temat zagrożeń cyberbezpieczeństwa od podmiotów publicznych i prywatnych oraz wymianę takich danych, zwiększenie wartości takich danych dzięki analizie eksperckiej i najnowocześniejszym narzędziom oraz wkład w rozwój zdolności i suwerenności technologicznej Unii.

Niniejszy wniosek jest również spójny z zaleceniem Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej⁹, w którym wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami

⁵ 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).

⁶ 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).

⁷ Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

⁸ Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020, COM(2022) 454 final.

⁹ Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (Tekst mający znaczenie dla EOG) (2023/C 20/01).

w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.

- **Spójność z innymi politykami Unii**

Wniosek jest spójny z innymi mechanizmami i protokołami kryzysowymi, w tym ze zintegrowanymi uzgodnieniami UE dotyczącymi reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR). Akt w sprawie cybersolidarności uzupełni te ramy i protokoły zarządzania kryzysowego, zapewniając specjalne wsparcie w zakresie gotowości i reagowania na incydenty w cyberbezpieczeństwie. Wniosek będzie również spójny z działaniami zewnętrznymi UE podejmowanymi w odpowiedzi na incydenty na dużą skalę w ramach wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB), w tym dzięki unijnemu zestawowi narzędzi dla dyplomacji cyfrowej. Wniosek uzupełni działania realizowane w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej lub w sytuacjach określonych w art. 222 Traktatu o funkcjonowaniu Unii Europejskiej.

Uzupełnia również ustanowiony w grudniu 2013 r. i dopełniony nowymi przepisami przyjętymi w maju 2021 r.¹⁰ Unijny Mechanizm Ochrony Ludności (UMOL)¹¹, który wzmacnia filary UCPM w zakresie zapobiegania, gotowości i reagowania oraz daje UE dodatkowe zdolności reagowania na nowe zagrożenia w Europie i na świecie, a także zwiększa rezerwę resEU.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Podstawą prawną niniejszego wniosku jest art. 173 ust. 3 i art. 322 ust. 1 lit. a) Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Art. 173 TFUE stanowi, że Unia i państwa członkowskie czuwają nad zapewnieniem warunków niezbędnych dla konkurencyjności przemysłu Unii. Celem niniejszego rozporządzenia jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Europie oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. W szczególności rozporządzenie ma na celu zwiększenie odporności obywateli, przedsiębiorstw i podmiotów działających w sektorach krytycznych i wysoce krytycznych na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze.

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/836 z dnia 20 maja 2021 r. zmieniające decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności (Tekst mający znaczenie dla EOG).

¹¹ Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Tekst mający znaczenie dla EOG).

Podstawą wniosku jest również art. 322 ust. 1 lit. a) TFUE, ponieważ zawiera on szczegółowe przepisy dotyczące przenoszenia środków, stanowiące odstępstwo od zasady jednoroczności określonej w rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 („rozporządzenie finansowe”)¹². Aby zapewnić należyte zarządzanie finansami i biorąc pod uwagę nieprzewidywalny, wyjątkowy i specyficzny charakter krajobrazu cyberbezpieczeństwa i zagrożeń cyberbezpieczeństwa, mechanizm cyberkryzysowy powinien obejmować pewien stopień elastyczności w zakresie zarządzania budżetem, a w szczególności dzięki umożliwieniu automatycznego przeniesienia na następny rok budżetowy niewykorzystanych środków na zobowiązania i środków na płatności przeznaczonych na działania służące realizacji celów określonych w rozporządzeniu. Ponieważ ten nowy przepis dotyczy zagadnień związanych z rozporządzeniem finansowym, kwestię tę należy uregulować w kontekście toczących się negocjacji w sprawie przekształcenia rozporządzenia finansowego.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Wyraźnie transgraniczny charakter zagrożeń cyberbezpieczeństwa i rosnąca liczba zagrożeń i incydentów, których skutki uboczne są odczuwalne w innych krajach oraz dotyczą inne sektory i produkty, oznaczają, że państwa członkowskie nie są w stanie skutecznie osiągnąć celów niniejszego wniosku samodzielnie i konieczne są wspólne działania oraz solidarność na szczeblu unijnym.

Doświadczenie w zwalczaniu cyberzagrożeń wynikające z wojny w Ukrainie oraz główne wnioski wyciągnięte z działań w zakresie cyberbezpieczeństwa zrealizowanych w ramach prezydencji francuskiej (EU CyCLES) pokazały, że osiągnięcie solidarności na szczeblu unijnym wymaga opracowania konkretnych mechanizmów wzajemnego wsparcia, w szczególności ustanowienia współpracy z sektorem prywatnym. W związku z tym w konkluzjach Rady z dnia 23 maja 2022 r. o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni wezwano Komisję do przedstawienia wniosku w sprawie nowego Funduszu Reagowania Cyberkryzysowego.

Wsparcie i działania na szczeblu unijnym służące skuteczniejszemu wykrywaniu zagrożeń cyberbezpieczeństwa oraz zwiększeniu gotowości i zdolności reagowania zapewniają wartość dodaną, ponieważ pozwalają uniknąć powielania podejmowanych działań w Unii i w państwach członkowskich. Może to przyczynić się do lepszego wykorzystania istniejących zasobów oraz do poprawy koordynacji oraz wymiany informacji na temat zdobytych doświadczeń. W ramach mechanizmu cyberkryzysowego przewidziano również wsparcie państw trzecich stowarzyszonych w ramach programu „Cyfrowa Europa” z unijnej rezerwy cyberbezpieczeństwa.

Wsparcie udzielane w ramach różnych inicjatyw, które zostaną ustanowione i sfinansowane na poziomie Unii, będzie uzupełnieniem a nie powieleniem krajowych zdolności w zakresie

¹² Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii (Dz.U. L 193 z 30.7.2018, s. 1).

wykrywania cyberzagrożeń i cyberincydentów, orientacji sytuacyjnej oraz gotowości i reagowania na cyberzagrożenia i cyberincydenty.

- **Proporcjonalność**

Działania nie wykraczałyby poza to, co jest konieczne do osiągnięcia ogólnych i szczegółowych celów rozporządzenia. Działania w ramach niniejszego rozporządzenia nie wpływają na odpowiedzialność państw członkowskich za bezpieczeństwo narodowe, bezpieczeństwo publiczne oraz za zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, ich wykrywanie i ściganie. Nie wpływają one również na zobowiązania prawne podmiotów działających w sektorach krytycznych i wysoce krytycznych dotyczące przyjęcia środków w zakresie cyberbezpieczeństwa zgodnie z dyrektywą NIS 2.

Działania objęte niniejszym rozporządzeniem są uzupełnieniem takich starań i środków, wspierając tworzenie infrastruktur służących lepszemu wykrywaniu i analizowaniu zagrożeń oraz zapewniając wsparcie dla działań w zakresie gotowości i reagowania w przypadku poważnych incydentów lub incydentów na dużą skalę.

- **Wybór instrumentu**

Wnioskowi nadaje się formę rozporządzenia Parlamentu Europejskiego i Rady. Jest to najodpowiedniejszy instrument prawny, ponieważ wyłącznie rozporządzenie – ze względu na fakt, że jego przepisy mają bezpośrednie zastosowanie – może zapewnić niezbędny stopień jednolitości potrzebny do tego, aby europejska tarcza cyberbezpieczeństwa i mechanizm cyberkryzysowy mogły powstać i funkcjonować, zapewniając wsparcie z programu „Cyfrowa Europa” na ich utworzenie, a także jasne warunki wykorzystania i przyznawania tego wsparcia.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

Działania w ramach niniejszego rozporządzenia będą wspierane ze środków programu „Cyfrowa Europa”, co było przedmiotem szerszych konsultacji. Ponadto będą opierać się na pierwszych działaniach, które opracowano w ścisłej współpracy z głównymi zainteresowanymi stronami. Jeżeli chodzi o SOC, Komisja opracowała, w ścisłej współpracy z państwami członkowskimi w ramach Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), dokument koncepcyjny na temat rozwoju platform transgranicznych SOC oraz zaproszenie do wyrażenia zainteresowania. W tym kontekście przeprowadzono badanie zdolności krajowych SOC oraz omówiono wspólne podejścia i wymogi techniczne w ramach technicznej grupy roboczej ECCC, w skład której wchodzi przedstawiciele państw członkowskich. Ponadto wymieniono poglądy z przedstawicielami

przemysłu, w szczególności za pośrednictwem grupy ekspertów ds. SOC utworzonej przez ENISA i Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO).

Po drugie, jeżeli chodzi o gotowość i reagowanie na incydenty, Komisja ustanowiła krótkoterminowy program wspierania państw członkowskich, przyznając ENISA dodatkowe środki finansowe z programu „Cyfrowa Europa”, aby w trybie natychmiastowym zwiększyć gotowość i zdolność do reagowania na poważne cyberincydenty. Informacje zwrotne od państw członkowskich i przemysłu, zebrane podczas realizacji tego krótkoterminowego programu, już teraz dostarczają cennych spostrzeżeń, które wykorzystano przy przygotowywaniu proponowanego rozporządzenia w celu wyeliminowania stwierdzonych niedociągnięć. Był to pierwszy krok zgodny z konkluzjami Rady o pozycji w kwestiach cyberprzestrzeni, w których zwrócono się do Komisji o przedstawienie wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego.

Ponadto w dniu 16 lutego 2023 r. odbyły się warsztaty z udziałem ekspertów z państw członkowskich dotyczące mechanizmu cyberkryzysowego, zorganizowane na podstawie dokumentu otwierającego debatę. W warsztatach udział wzięły wszystkie państwa członkowskie, a jedenaście państw członkowskich przekazało dodatkowe uwagi na piśmie.

- **Ocena skutków**

Z uwagi na pilny charakter wniosku nie przeprowadzono oceny skutków. Działania przewidziane w niniejszym rozporządzeniu będą wspierane w ramach programu „Cyfrowa Europa” i są zgodne z działaniami określonymi w rozporządzeniu w sprawie programu „Cyfrowa Europa”, które było przedmiotem specjalnej oceny skutków. Niniejsze rozporządzenie nie pociągnie za sobą żadnych znaczących skutków administracyjnych ani środowiskowych, które by wykraczały poza skutki już uwzględnione w ocenie skutków rozporządzenia w sprawie programu „Cyfrowa Europa”.

Ponadto rozporządzenie to opiera się na pierwszych działaniach opracowanych w ramach zamkniętej współpracy z głównymi zainteresowanymi stronami, jak określono powyżej, i stanowi odpowiedź na apel państw członkowskich do Komisji o przedstawienie wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego do końca trzeciego kwartału 2022 r.

W szczególności w odniesieniu do orientacji sytuacyjnej i wykrywania w ramach europejskiej tarczy cyberbezpieczeństwa w programie prac w zakresie cyberbezpieczeństwa na lata 2021–2022 w ramach programu „Cyfrowa Europa” zawarto zaproszenie do wyrażenia zainteresowania udziałem we wspólnych zamówieniach na narzędzia i infrastruktury niezbędne do utworzenia transgranicznych SOC oraz zaproszenie do składania wniosków o udzielenie dotacji w celu umożliwienia budowania zdolności SOC obsługujących organizacje publiczne i prywatne.

W obszarze gotowości i reagowania na incydenty, jak wspomniano powyżej, Komisja ustanowiła krótkoterminowy program wspierania państw członkowskich w ramach programu „Cyfrowa Europa”, który wdraża ENISA. Usługi objęte programem będą dotyczyć działań

w zakresie gotowości, np. przeprowadzania w podmiotach krytycznych testów penetracyjnych pozwalających zidentyfikować podatności. Program służy również zwiększeniu możliwości udzielania pomocy państwom członkowskim w przypadku poważnego incydentu wpływającego na podmioty krytyczne. Realizacja tego krótkoterminowego programu przez ENISA jest w toku i już dostarczyła istotnych spostrzeżeń, które wzięto pod uwagę przy przygotowywaniu niniejszego rozporządzenia.

- **Prawa podstawowe**

Dzięki przyczynieniu się do poprawy bezpieczeństwa informacji cyfrowych niniejszy wniosek przyczyni się do ochrony prawa do wolności i bezpieczeństwa osobistego zgodnie z art. 6 Karty praw podstawowych Unii Europejskiej oraz prawa do poszanowania życia prywatnego i rodzinnego zgodnie z art. 7 Karty praw podstawowych Unii Europejskiej. Dzięki ochronie przedsiębiorstw przed szkodliwymi gospodarczo cyberatakami niniejszy wniosek przyczyni się również do ochrony wolności prowadzenia działalności gospodarczej zgodnie z art. 16 Karty praw podstawowych Unii Europejskiej oraz prawa własności zgodnie z art. 17 Karty praw podstawowych Unii Europejskiej. Ponadto dzięki ochronie integralności infrastruktury krytycznej w obliczu cyberataków wniosek przyczyni się do ochrony prawa do opieki zdrowotnej zgodnie z art. 35 Karty praw podstawowych Unii Europejskiej oraz prawa do dostępu do usług świadczonych w ogólnym interesie gospodarczym zgodnie z art. 36 Karty praw podstawowych Unii Europejskiej.

4. WPLYW NA BUDŻET

Działania w ramach niniejszego rozporządzenia będą wspierane ze środków w ramach celu strategicznego „Cyberbezpieczeństwo” programu „Cyfrowa Europa”.

Całkowity budżet obejmuje zwiększenie środków o 100 mln EUR, które w niniejszym rozporządzeniu proponuje się przesunąć z innych celów strategicznych programu „Cyfrowa Europa”. Dzięki temu nowa całkowita kwota dostępna na działania w ramach celu „Cyberbezpieczeństwo” programu „Cyfrowa Europa” wyniesie 842,8 mln EUR.

Część z dodatkowych 100 mln EUR posłuży zwiększeniu budżetu, którym zarządza ECCC, przeznaczonego na realizację działań dotyczących SOC i gotowości w ramach ich programów prac. Ponadto dodatkowe środki finansowe posłużą wsparciu ustanowienia unijnej rezerwy cyberbezpieczeństwa.

Stanowią one uzupełnienie budżetu przewidzianego już na podobne działania w programie prac dotyczącym głównego programu „Cyfrowa Europa” i celu „Cyberbezpieczeństwo” na lata 2023–2027, co mogłoby zwiększyć łączną kwotę na lata 2023–2027 do 551 mln, podczas gdy 115 mln rozdysponowano już w formie projektów pilotażowych na lata 2021–2022. Z uwzględnieniem wkładów państw członkowskich budżet całkowity może wynieść maksymalnie 1,109 mld EUR.

Przegląd odnośnych kosztów znajduje się w „Ocenie skutków finansowych regulacji” towarzyszącej niniejszemu wnioskowi.

5. ELEMENTY FAKULTATYWNE

• Plany wdrożenia i monitorowanie, ocena i sprawozdania

Komisja będzie monitorować wdrażanie i stosowanie tych nowych przepisów oraz zgodność z nimi w celu oceny ich skuteczności. Komisja przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia przed upływem czterech lat od daty rozpoczęcia jego stosowania.

• Szczegółowe objaśnienia poszczególnych przepisów wniosku

Cele ogólne, przegląd i definicje (rozdział I)

W rozdziale I określa się cele rozporządzenia, a mianowicie: zwiększenie solidarności na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie, a w szczególności wzmocnienie wspólnego unijnego wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie, zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz zwiększenie odporności Unii dzięki przeglądowi i ocenie poważnych incydentów lub incydentów na dużą skalę. W rozdziale tym określa się również działania, za pomocą których cele te zostaną osiągnięte: wprowadzenie europejskiej tarczy cyberbezpieczeństwa, stworzenie mechanizmu cyberkryzysowego oraz ustanowienie mechanizmu przeglądu incydentów w cyberbezpieczeństwie. Przedstawia się w nim również definicje stosowane w całym instrumencie.

Europejska tarcza cyberbezpieczeństwa (rozdział II)

W rozdziale II ustanawia się europejską tarczę cyberbezpieczeństwa oraz określa się jej różne elementy i warunki uczestnictwa. Po pierwsze, sformułowano w nim ogólny cel europejskiej tarczy cyberbezpieczeństwa, którym jest rozwijanie zaawansowanych zdolności w Unii w zakresie wykrywania cyberzagrożeń i cyberincydentów w Unii oraz analizowania i przetwarzania danych na ich temat, a także szczegółowe cele operacyjne. Przewidziano w nim, że finansowanie unijne przeznaczone na europejską tarczę cyberbezpieczeństwa będzie wdrażane zgodnie z rozporządzeniem w sprawie programu „Cyfrowa Europa”.

Ponadto w rozdziale tym opisano rodzaj podmiotów, które tworzą europejską tarczę cyberbezpieczeństwa. W skład tarczy wchodzi wszystkie krajowe centra monitorowania bezpieczeństwa („krajowe SOC”) oraz transgraniczne centra monitorowania bezpieczeństwa („transgraniczne SOC”). Każde uczestniczące państwo członkowskie wyznacza krajowy SOC. Pełni on funkcję punktu odniesienia i punktu dostępu dla innych organizacji

publicznych i prywatnych na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. W następstwie zaproszenia do wyrażenia zainteresowania ECCC może wybrać krajowy SOC do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury oraz przyznać mu dotację na obsługę tych narzędzi i infrastruktury. Jeżeli krajowy SOC korzysta ze wsparcia unijnego, zobowiązuje się do złożenia w ciągu dwóch lat wniosku o uczestnictwo w transgranicznym SOC.

Transgraniczne SOC składają się z konsorcjum złożonego z co najmniej trzech państw członkowskich, reprezentowanych przez krajowe SOC, zobowiązujących się do współpracy w celu koordynowania swoich działań w zakresie wykrywania cyberataków i monitorowania zagrożeń. W następstwie wstępnego zaproszenia do wyrażenia zainteresowania ECCC może wybrać konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury oraz przyznać mu dotację na obsługę tych narzędzi i infrastruktur. Członkowie konsorcjum przyjmującego zawierają pisemną umowę konsorcjum określającą ich wewnętrzne ustalenia. Ponadto w rozdziale tym szczegółowo opisano wymogi dotyczące wymiany informacji między uczestnikami transgranicznego SOC oraz wymiany informacji między transgranicznym SOC a innymi transgranicznymi SOC, a także z odpowiednimi podmiotami UE. Krajowe SOC uczestniczące w transgranicznym SOC udostępniają sobie nawzajem istotne informacje dotyczące cyberzagrożeń oraz informacje szczegółowe, w tym zobowiązują się do udostępniania znacznej ilości danych, a warunki tego udostępniania należy określić w umowie konsorcjum. Transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą. Transgraniczne SOC powinny również zawrzeć z innymi transgranicznymi SOC umowy o współpracy określające zasady wymiany informacji. W przypadku gdy transgraniczne SOC uzyskają informacje dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, przekazują istotne informacje EU-CyCLONe, sieci CSIRT i Komisji, biorąc pod uwagę ich odpowiednie role w zarządzaniu kryzysowym zgodnie z dyrektywą (UE) 2022/2555. Rozdział II kończy się określeniem warunków w zakresie bezpieczeństwa w odniesieniu do uczestnictwa w europejskiej tarczy cyberbezpieczeństwa.

Mechanizm cyberkryzysowy (rozdział III)

W rozdziale III ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na poważne zagrożenia cyberbezpieczeństwa oraz, działając w duchu solidarności, przygotować się na krótkoterminowe skutki poważnych incydentów lub sytuacji kryzysowych w cyberbezpieczeństwie oraz incydentów lub sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę i łagodzić ich skutki. Działania służące wdrażaniu mechanizmu cyberkryzysowego są wspierane ze środków programu „Cyfrowa Europa”. Mechanizm ten przewiduje działania mające na celu wspieranie gotowości, w tym skoordynowane testowanie podmiotów działających w sektorach wysoce krytycznych, reagowanie na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowe usuwanie ich skutków lub łagodzenie skutków poważnych cyberzagrożeń, jak również działania w zakresie wzajemnej pomocy.

Działania w zakresie gotowości w ramach mechanizmu cyberkryzysowego obejmują skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych. Komisja, po konsultacji z ENISA i grupą współpracy NIS, powinna regularnie określać odpowiednie sektory lub podsektory spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555, z których podmioty mogą podlegać skoordynowanemu testowaniu gotowości na szczeblu UE.

Na potrzeby wdrożenia proponowanych działań w zakresie reagowania na incydenty w niniejszym rozporządzeniu ustanawia się unijną rezerwę cyberbezpieczeństwa, składającą się z usług reagowania na incydenty świadczonych przez zaufanych dostawców wybranych zgodnie z kryteriami określonymi w niniejszym rozporządzeniu. Do użytkowników usług z unijnej rezerwy cyberbezpieczeństwa należą organy państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie, CSIRT oraz instytucje, organy i jednostki organizacyjne Unii. Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa i może powierzyć ENISA, w całości lub w części, obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią.

Aby otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, użytkownicy powinni stosować własne środki łagodzące skutki incydentu będącego przedmiotem wniosku o wsparcie. Wnioski o wsparcie z unijnej rezerwy cyberbezpieczeństwa powinny zawierać niezbędne istotne informacje na temat incydentu oraz środków już zastosowanych przez użytkowników. W rozdziale tym opisano również warunki wdrażania, w tym ocenę wniosków dotyczących unijnej rezerwy cyberbezpieczeństwa.

W rozporządzeniu przewiduje się również zasady udzielania zamówień i kryteria kwalifikacji w odniesieniu do zaufanych dostawców unijnej rezerwy cyberbezpieczeństwa.

Państwa trzecie mogą wystąpić z wnioskiem o wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli przewidują to układy o stowarzyszeniu zawarte w związku z uczestnictwem tych państw w programie „Cyfrowa Europa”. W rozdziale tym opisano dalsze warunki i zasady takiego uczestnictwa.

Mechanizm przeglądu incydentów w cyberbezpieczeństwie (rozdział IV)

Na wniosek Komisji, EU-CyCLONe lub sieci CSIRT ENISA powinna dokonać przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Przegląd i ocenę ENISA powinna przekazać sieci CSIRT, EU-CyCLONe i Komisji w formie sprawozdania z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań. W przypadku gdy incydent dotyczy państwa trzeciego, Komisja powinna udostępnić sprawozdanie wysokiemu przedstawicielowi. Sprawozdanie powinno obejmować zdobyte doświadczenia i w stosownych przypadkach zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.

Przepisy końcowe (rozdział V)

Rozdział V zawiera zmiany rozporządzenia w sprawie programu „Cyfrowa Europa” oraz zobowiązanie Komisji do przedkładania Parlamentowi Europejskiemu i Radzie regularnych sprawozdań z oceny i przeglądu rozporządzenia. Komisja jest uprawniona do przyjmowania aktów wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 21, w celu: określenia warunków interoperacyjności między transgranicznymi SOC; określenia ustaleń proceduralnych dotyczących wymiany informacji między transgranicznymi SOC a podmiotami unijnymi na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę; określenia wymogów technicznych w celu zapewnienia wysokiego poziomu bezpieczeństwa danych i bezpieczeństwa fizycznego infrastruktury oraz ochrony interesów Unii w zakresie bezpieczeństwa przy wymianie informacji z podmiotami, które nie są organami publicznymi państw członkowskich; określenia rodzaju i liczby usług reagowania wymaganych do celów unijnej rezerwy cyberbezpieczeństwa; oraz doprecyzowania szczegółowych ustaleń dotyczących przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa.

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

**ustanawiające środki mające na celu zwiększenie solidarności i zdolności w Unii
w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów
w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia
i incydenty**

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 173 ust. 3 i art. 322 ust. 1 lit. a),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Trybunału Obrachunkowego¹,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego²,

uwzględniając opinię Komitetu Regionów³,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

- (1) Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich stały się kwestią o zasadniczym znaczeniu we wszystkich sektorach działalności gospodarczej, gdyż administracje publiczne, przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej.
- (2) Rosną skala, częstotliwość i wpływ incydentów w cyberbezpieczeństwie, w tym ataków na łańcuchy dostaw, które to ataki mają na celu cyberszpiegostwo, instalację oprogramowania szantażującego lub wywołanie zakłóceń. Stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Z uwagi na szybko zmieniający się krajobraz zagrożeń zagrożenie możliwymi incydentami na dużą skalę powodującymi poważne zakłócenie lub uszkodzenie infrastruktur krytycznych wymaga podwyższonej gotowości na wszystkich szczeblach unijnych ram cyberbezpieczeństwa. To zagrożenie wykracza poza rosyjską napaść na Ukrainę i prawdopodobnie będzie się utrzymywać, biorąc pod uwagę wielość podmiotów powiązanych z organami państwowymi, ze środowiskami przestępczymi i haktywistycznymi, które mają swój udział w generowaniu obecnych napięć geopolitycznych. Takie incydenty mogą utrudniać świadczenie usług publicznych i prowadzenie działalności gospodarczej, w tym w sektorach krytycznych lub wysoce krytycznych, powodować znaczne straty finansowe, podważać zaufanie

¹ Dz.U. C [...] z [...], s. [...].

² Dz.U. C [...] z [...], s. [...].

³ Dz.U. C [...] z [...], s. [...].

użytkowników, powodować poważne szkody dla gospodarki Unii, a nawet mieć konsekwencje zagrażające zdrowiu lub życiu. Ponadto incydenty w cyberbezpieczeństwie są nieprzewidywalne, ponieważ często pojawiają się i ewoluują w bardzo krótkim czasie, nie są ograniczone do konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach.

- (3) Konieczne jest wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. Jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy⁴, konieczne jest zwiększenie odporności obywateli, przedsiębiorstw i podmiotów obsługujących infrastrukturę krytyczną na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. W związku z tym potrzebne są inwestycje w infrastruktury i usługi, które będą wspierać szybsze wykrywanie zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz reagowanie na nie, a państwa członkowskie potrzebują pomocy w lepszym przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę i w reagowaniu na nie. Unia powinna również zwiększyć swoje zdolności w tych obszarach, w szczególności w zakresie gromadzenia i analizy danych dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.
- (4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności i zwiększenia odporności infrastruktur i podmiotów krytycznych na ryzyko w cyberprzestrzeni, w szczególności dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555⁵, zalecenie Komisji (UE) 2017/1584⁶, dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE⁷ oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881⁸. Ponadto w zaleceniu Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia pilnych i skutecznych środków oraz do lojalnej, efektywnej, solidarnej i skoordynowanej współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, jak również z zainteresowanymi podmiotami w celu wzmocnienia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.
- (5) Coraz większe ryzyko w cyberprzestrzeni i ogólnie złożony krajobraz zagrożeń, w tym również wyraźne ryzyko szybkiego rozprzestrzeniania się incydentów w cyberbezpieczeństwie z jednego państwa członkowskiego na inne oraz z państwa

⁴ <https://futureu.europa.eu/pl/>

⁵ 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 (Dz.U. L 333 z 27.12.2022).

⁶ 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).

⁷ Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

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).

trzeciego na Unię, wymagają większej solidarności na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie. W konkluzjach Rady o pozycji UE w kwestiach cyberprzestrzeni⁹ państwa członkowskie wezwały również Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego.

- (6) We wspólnym komunikacie „Polityka UE w zakresie cyberobrony”¹⁰, przyjętym w dniu 10 listopada 2022 r., zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa („SOC”), wspieranie stopniowego tworzenia na szczeblu UE rezerwy na potrzeby cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka.
- (7) Koniecznie należy poprawić wykrywanie cyberzagrożeń i cyberincydentów oraz orientację sytuacyjną w tym zakresie w całej Unii, jak również zwiększyć solidarność dzięki poprawie gotowości i zdolności państw członkowskich i Unii do reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę. Dlatego należy wprowadzić ogólnoeuropejską infrastrukturę SOC (europejską tarczę cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej; należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków; należy ustanowić mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów lub incydentów na dużą skalę. Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).
- (8) Aby osiągnąć te cele, należy również w niektórych obszarach zmienić rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694¹¹. W szczególności niniejszym rozporządzeniem należy zmienić rozporządzenie (UE) 2021/694 przez dodanie nowych celów operacyjnych związanych z europejską tarczą cyberbezpieczeństwa i mechanizmem cyberkryzysowym w ramach celu szczegółowego nr 3 programu „Cyfrowa Europa”, który to cel obejmuje zagwarantowanie odporności, integralności i wiarygodności jednolitego rynku cyfrowego, zwiększenie zdolności w zakresie monitorowania cyberataków i cyberzagrożeń oraz reagowania na nie, a także wzmocnienie współpracy transgranicznej w dziedzinie cyberbezpieczeństwa. Jako uzupełnienie tych zmian należy ustanowić szczegółowe warunki, na jakich można przyznawać wsparcie finansowe na te działania, i określić mechanizmy zarządzania i koordynacji niezbędne do osiągnięcia zamierzonych celów. Inne zmiany

⁹ Konkluzje Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni zatwierdzone przez Radę na posiedzeniu w dniu 23 maja 2022 r. (9364/22).

¹⁰ Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony”, JOIN(2022) 49 final.

¹¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa” oraz uchylające decyzję (UE) 2015/2240 (Dz.U. L 166 z 11.5.2021, s. 1).

rozporządzenia (UE) 2021/694 powinny obejmować opisy proponowanych działań w ramach nowych celów operacyjnych, jak również mierzalne wskaźniki umożliwiające monitorowanie realizacji tych nowych celów operacyjnych.

- (9) Finansowanie działań na podstawie niniejszego rozporządzenia należy przewidzieć w rozporządzeniu (UE) 2021/694, które powinno pozostać właściwym aktem podstawowym dla tych działań objętych celem szczegółowym nr 3 programu „Cyfrowa Europa”. Szczegółowe warunki uczestnictwa dotyczące każdego działania zostaną określone w odpowiednich programach prac zgodnie z mającym zastosowanie przepisem rozporządzenia (UE) 2021/694.
- (10) Do niniejszego rozporządzenia zastosowanie mają horyzontalne zasady finansowe przyjęte przez Parlament Europejski i Radę na podstawie art. 322 TFUE. Zasady te są ustanowione w rozporządzeniu finansowym i określają w szczególności procedurę uchwalania i wykonywania budżetu Unii oraz przewidują kontrole odpowiedzialności podmiotów upoważnionych do działań finansowych. Zasady przyjęte na podstawie art. 322 TFUE obejmują również ogólny system warunkowości służący ochronie budżetu Unii ustanowiony w rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) 2020/2092.
- (11) Do celów należytego zarządzania finansami należy ustanowić przepisy szczegółowe dotyczące przenoszenia niewykorzystanych środków na zobowiązania i środków na płatności. Z poszanowaniem zasady, że budżet Unii jest ustalany corocznie, w niniejszym rozporządzeniu należy – ze względu na nieprzewidywalny, wyjątkowy i specyficzny charakter krajobrazu cyberbezpieczeństwa – przewidzieć – obok możliwości określonych w rozporządzeniu finansowym – możliwość przenoszenia niewykorzystanych środków, a tym samym maksymalnie zwiększyć zdolność mechanizmu cyberkryzysowego do wspierania państw członkowskich w skutecznym zwalczaniu cyberzagrożeń.
- (12) Aby skuteczniej zapobiegać cyberzagrożeniom i cyberincydentom, oceniać je i reagować na nie, należy zdobyć bardziej kompleksową wiedzę na temat zagrożeń dla aktywów i infrastruktur krytycznych na terytorium Unii, w tym na temat ich rozmieszczenia geograficznego, wzajemnych połączeń i potencjalnych skutków w przypadku cyberataków mających wpływ na te infrastruktury. Należy wprowadzić wielkoskalową unijną infrastrukturę SOC („europejską tarczę cyberbezpieczeństwa”), składającą się z kilku interoperacyjnych platform transgranicznych, z których każda zrzesza kilka krajowych SOC. Infrastruktura ta powinna służyć krajowym i unijnym interesom i potrzebom w zakresie cyberbezpieczeństwa, wykorzystując najnowocześniejszą technologię zaawansowanego gromadzenia danych i narzędzia analityki, zwiększając zdolności w zakresie wykrywania cyberataków i zarządzania nimi oraz zapewniając orientację sytuacyjną w czasie rzeczywistym. Infrastruktura ta powinna służyć lepszemu wykrywaniu zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie, a tym samym uzupełniać i wspierać unijne podmioty i sieci odpowiedzialne za zarządzanie kryzysowe w Unii, w szczególności europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe”), zdefiniowaną w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555¹².

¹² 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

- (13) Każde państwo członkowskie powinno wyznaczyć na szczeblu krajowym podmiot publiczny, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w tym państwie członkowskim. Te krajowe SOC powinny pełnić funkcję punktu odniesienia i punktu dostępu na szczeblu krajowym do celów uczestnictwa w europejskiej tarczy cyberbezpieczeństwa oraz powinny zapewniać, aby informacje o cyberzagrożeniach uzyskiwane od podmiotów publicznych i prywatnych skutecznie i sprawnie wymieniano i gromadzono na szczeblu krajowym.
- (14) W ramach europejskiej tarczy cyberbezpieczeństwa należy ustanowić szereg transgranicznych centrów monitorowania bezpieczeństwa („transgraniczne SOC”). Powinny one zrzeszać krajowe SOC z co najmniej trzech państw członkowskich, tak aby można było w pełni osiągnąć korzyści płynące z transgranicznego wykrywania zagrożeń, wymiany informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych SOC powinno być zwiększanie zdolności w zakresie analizy i wykrywania zagrożeń cyberbezpieczeństwa oraz zapobiegania im, wspieranie generowania wysokiej jakości danych wywiadowczych dotyczących zagrożeń cyberbezpieczeństwa, w szczególności w drodze wymiany danych z różnych źródeł publicznych lub prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami i ich wspólne używanie oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń oraz zapobiegania im w zaufanym otoczeniu. Powinny one zapewnić nowe dodatkowe zdolności, opierając się na istniejących SOC, zespołach reagowania na incydenty bezpieczeństwa komputerowego („CSIRT”) i innych odpowiednich podmiotach oraz uzupełniając je.
- (15) Na szczeblu krajowym monitorowanie, wykrywanie i analizę cyberzagrożeń zazwyczaj zapewniają SOC funkcjonujące w podmiotach publicznych i prywatnych w połączeniu z CSIRT. Ponadto CSIRT wymieniają informacje w kontekście sieci CSIRT zgodnie z dyrektywą (UE) 2022/2555. Transgraniczne SOC powinny stanowić nową zdolność, która jest uzupełnieniem sieci CSIRT, przez gromadzenie danych na temat zagrożeń cyberbezpieczeństwa od podmiotów publicznych i prywatnych oraz wymienianie takich danych, zwiększanie wartości takich danych dzięki analizie eksperckiej oraz wspólnie nabytym infrastrukturom i najnowocześniejszym narzędziom oraz poprzez wkład w rozwój zdolności i suwerenności technologicznej Unii.
- (16) Transgraniczne SOC powinny działać jako centralny punkt, który umożliwia szerokie gromadzenie odpowiednich danych, w tym danych wywiadowczych na temat cyberzagrożeń, oraz pozwala na rozpowszechnianie informacji o zagrożeniach wśród dużej i zróżnicowanej grupy podmiotów (np. zespołów reagowania na incydenty komputerowe („CERT”), CSIRT, ośrodków wymiany i analizy informacji („ISAC”), operatorów infrastruktury krytycznej). Informacje wymieniane między uczestnikami transgranicznego SOC mogłyby obejmować dane z sieci i czujników, dane wywiadowcze o zagrożeniach, oznaki naruszenia integralności oraz informacje kontekstowe na temat incydentów, zagrożeń i podatności. Ponadto transgraniczne SOC powinny również zawierać umowy o współpracy z innymi transgranicznymi SOC.
- (17) Wspólna orientacja sytuacyjna wśród właściwych organów jest niezbędnym warunkiem gotowości i koordynacji w całej Unii w odniesieniu do poważnych

rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) ([Dz.U. L 333 z 27.12.2022, s. 80](#)).

incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę. Dyrektywą (UE) 2022/2555 ustanowiono EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. W zaleceniu (UE) 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę uwzględniono rolę wszystkich odpowiednich podmiotów. W dyrektywie (UE) 2022/2555 przypomniano również o odpowiedzialności Komisji w ramach Unijnego Mechanizmu Ochrony Ludności („UMOL”) ustanowionego decyzją Parlamentu Europejskiego i Rady 1313/2013/UE oraz o spoczywającej na niej odpowiedzialności za przedstawianie sprawozdań analitycznych dotyczących uzgodnień na potrzeby mechanizmu reagowania na szczeblu politycznym w sytuacjach kryzysowych („IPCR”) na podstawie decyzji wykonawczej (UE) 2018/1993. W związku z tym w sytuacjach, w których transgraniczne SOC uzyskują informacje dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, powinny przekazywać istotne informacje EU-CyCLONe, sieci CSIRT i Komisji. W szczególności, w zależności od sytuacji, przekazywane informacje mogą obejmować informacje techniczne, informacje na temat charakteru i motywów sprawcy lub potencjalnego sprawcy ataku oraz informacje nietechniczne wyższego szczebla na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę. W tym kontekście należy zwrócić należytą uwagę na zasadę ograniczonego dostępu oraz potencjalnie poufny charakter wymienianych informacji.

- (18) Podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny zapewnić wysoki poziom interoperacyjności między sobą, w tym w stosownych przypadkach w odniesieniu do formatów danych, taksonomii, narzędzi przetwarzania i analizy danych oraz bezpiecznych kanałów komunikacji, minimalnego poziomu bezpieczeństwa warstwy aplikacji, tablicy wskaźników orientacji sytuacyjnej oraz samych wskaźników. Przy przyjmowaniu wspólnej taksonomii i opracowywaniu wzoru sprawozdań sytuacyjnych na potrzeby opisywania technicznej przyczyny i skutków incydentów w cyberbezpieczeństwie należy uwzględnić trwające prace nad zgłaszaniem incydentów w kontekście wdrażania dyrektywy (UE) 2022/2555.
- (19) Aby umożliwić prowadzoną na dużą skalę wymianę danych na temat zagrożeń cyberbezpieczeństwa pochodzących z różnych źródeł w zaufanym środowisku, podmioty uczestniczące w europejskiej tarczy cyberbezpieczeństwa powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastruktury. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów i terminowe ostrzeganie organów i odpowiednich podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii sztucznej inteligencji i analityki danych.
- (20) Dzięki gromadzeniu i udostępnianiu danych oraz ich wymianie europejska tarcza cyberbezpieczeństwa powinna zwiększyć suwerenność technologiczną Unii. Łączenie wyselekcjonowanych danych wysokiej jakości powinno również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. Należy to ułatwiać przez połączenie europejskiej tarczy cyberbezpieczeństwa

z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną rozporządzeniem Rady (UE) 2021/1173¹³.

- (21) Chociaż europejska tarcza cyberbezpieczeństwa jest projektem cywilnym, społeczność zajmująca się cyberobroną mogłaby skorzystać na poprawie cywilnych zdolności w zakresie wykrywania i orientacji sytuacyjnej do celów ochrony infrastruktury krytycznej. Transgraniczne SOC, przy wsparciu Komisji i Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) oraz we współpracy z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa („wysoki przedstawiciel”), powinny stopniowo opracowywać specjalne protokoły i standardy, aby umożliwić współpracę ze społecznością zajmującą się cyberobroną, w tym warunki weryfikacji i bezpieczeństwa. Rozwojowi europejskiej tarczy cyberbezpieczeństwa powinna towarzyszyć refleksja umożliwiająca przyszłą współpracę z sieciami i platformami odpowiedzialnymi za wymianę informacji w społeczności zajmującej się cyberobroną, w ścisłej współpracy z wysokim przedstawicielem.
- (22) Wymiana informacji między uczestnikami europejskiej tarczy cyberbezpieczeństwa powinna być zgodna z obowiązującymi wymogami prawnymi, w szczególności z unijnymi i krajowymi przepisami o ochronie danych, a także z unijnymi regułami konkurencji regulującymi wymianę informacji. Odbiorca informacji powinien wdrożyć – o ile konieczne jest przetwarzanie danych osobowych – środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą, oraz zniszczyć dane, gdy tylko przestaną one być niezbędne do określonego celu, i poinformować organ udostępniający dane o ich zniszczeniu.
- (23) Bez uszczerbku dla art. 346 TFUE wymiana informacji, które zgodnie z przepisami unijnymi lub krajowymi mają status informacji poufnych, powinna być ograniczona do tego, co jest istotne i proporcjonalne do celów tej wymiany. Podczas wymiany takich informacji należy zachować poufność informacji oraz chronić bezpieczeństwo i interesy handlowe danych podmiotów, z pełnym poszanowaniem tajemnic handlowych i tajemnic przedsiębiorstwa.
- (24) W związku z rosnącym ryzykiem i rosnącą liczbą cyberincydentów mających wpływ na państwa członkowskie konieczne jest ustanowienie instrumentu wsparcia kryzysowego, aby poprawić odporność Unii na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz uzupełnić działania państw członkowskich wsparciem finansowym w sytuacjach nadzwyczajnych na potrzeby gotowości, reagowania i natychmiastowego przywrócenia funkcjonowania usług kluczowych. Instrument ten powinien umożliwiać szybkie wdrażanie pomocy w określonych okolicznościach i na jasnych warunkach oraz uważne monitorowanie i wnikliwą ocenę sposobu wykorzystania zasobów. O ile podstawowa odpowiedzialność za zapobieganie incydom i kryzysom w cyberbezpieczeństwie spoczywa na państwach członkowskich, mechanizm cyberkryzysowy propaguje solidarność między państwami członkowskimi zgodnie z art. 3 ust. 3 Traktatu o Unii Europejskiej („Traktat UE”).
- (25) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia

¹³ Rozporządzenie Rady (UE) 2021/1173 z dnia 13 lipca 2021 r. w sprawie ustanowienia Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali i uchylające rozporządzenie (UE) 2018/1488 ([Dz.U. L 256 z 19.7.2021, s. 3](#)).

w przypadku reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania ich skutków, takie jak: usługi świadczone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA”) zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 Traktatu UE, zespoły szybkiego reagowania na cyberincydenty w ramach PESCO¹⁴ i zespoły szybkiego reagowania na zagrożenia hybrydowe. W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w całej Unii i w państwach trzecich.

- (26) Instrument ten pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na szczeblu Unii, w szczególności UMOL¹⁵, IPCR¹⁶, i dyrektywy (UE) 2022/2555. Może on wносить wkład w działania realizowane w kontekście art. 42 ust. 7 Traktatu UE lub w sytuacjach określonych w art. 222 TFUE lub uzupełniać takie działania. Stosowanie tego instrumentu powinno być również skoordynowane, w stosownych przypadkach, z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej.
- (27) Wsparcie udzielane na podstawie niniejszego rozporządzenia powinno wspomagać i uzupełniać działania podejmowane przez państwa członkowskie na szczeblu krajowym. W tym celu należy zapewnić ścisłą współpracę i konsultacje między Komisją a zainteresowanym państwem członkowskim. Wnosząc o wsparcie w ramach mechanizmu cyberkryzysowego, państwo członkowskie powinno przedstawić odpowiednie informacje uzasadniające potrzebę wsparcia.
- (28) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskie do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie i do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, jak również do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien

¹⁴ Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich.

¹⁵ Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

¹⁶ Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) i zgodnie z zaleceniem Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

zapewniać pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych.

- (29) Aby propagować spójne podejście i zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach wysoce krytycznych określonych zgodnie z dyrektywą (UE) 2022/2555. W tym celu Komisja, przy wsparciu ENISA i we współpracy z grupą współpracy NIS ustanowioną na mocy dyrektywy (UE) 2022/2555, powinna regularnie określać odpowiednie sektory lub podsektory, które mogą kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie na szczeblu Unii. Sektory lub podsektory należy wybierać z załącznika I do dyrektywy (UE) 2022/2555 („sektory kluczowe”). Skoordynowane testowanie powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które mają przeprowadzić Komisja, wysoki przedstawiciel i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturami łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), skoordynowane oceny ryzyka, które mają zostać przeprowadzone na podstawie art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554¹⁷. Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.
- (30) Ponadto w ramach mechanizmu cyberkryzysowego należy oferować wsparcie innych działań w zakresie gotowości i wsparcie gotowości w innych sektorach, nieobjętych skoordynowanym testowaniem podmiotów działających w sektorach wysoce krytycznych. Działania te mogą obejmować różnego rodzaju krajowe działania związane z gotowością.
- (31) Mechanizm cyberkryzysowy powinien również zapewniać wsparcie działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia natychmiastowego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych. W stosownych przypadkach powinien on uzupełniać UMOL, aby zapewnić kompleksowe podejście do reagowania na skutki incydentów w cyberbezpieczeństwie dla obywateli.

¹⁷ 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.

- (32) Mechanizm cyberkryzysowy powinien wspierać pomoc udzielaną przez państwa członkowskie państwu członkowskiemu dotkniętemu poważnym incydem w cyberbezpieczeństwie lub incydem w cyberbezpieczeństwie na dużą skalę, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 15 dyrektywy (UE) 2022/2555. Udzielające pomocy państwa członkowskie powinny mieć możliwość składania wniosków o pokrycie kosztów związanych z wysyłaniem zespołów ekspertów w ramach wzajemnej pomocy. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.
- (33) Należy stopniowo tworzyć rezerwę cyberbezpieczeństwa na szczeblu Unii, składającą się z usług oferowanych przez prywatnych dostawców usług zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i natychmiastowe usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę. Unijna rezerwa cyberbezpieczeństwa powinna zapewniać dostępność i gotowość usług. Usługi z unijnej rezerwy cyberbezpieczeństwa powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom działającym w sektorach krytycznych lub wysoce krytycznych jako uzupełnienie działań tych organów na szczeblu krajowym. Wnioskując o wsparcie z unijnej rezerwy cyberbezpieczeństwa, państwa członkowskie powinny wskazać wsparcie udzielone na szczeblu krajowym podmiotowi dotkniętemu incydem, które należy uwzględnić przy ocenie wniosku państwa członkowskiego. Usługi z unijnej rezerwy cyberbezpieczeństwa mogą również służyć zapewnieniu wsparcia instytucjom, organom i jednostkom organizacyjnym Unii na podobnych warunkach.
- (34) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście unijnej rezerwy cyberbezpieczeństwa konieczne jest ustanowienie zestawu minimalnych kryteriów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich i podmiotów działających w sektorach krytycznych lub wysoce krytycznych.
- (35) Aby wesprzeć tworzenie unijnej rezerwy cyberbezpieczeństwa, Komisja mogłaby rozważyć zwrócenie się do ENISA o przygotowanie propozycji programu certyfikacji na podstawie rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa w obszarach objętych mechanizmem cyberkryzysowym.
- (36) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii i umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, EU-CyCLONe, sieć CSIRT lub Komisja powinny mieć możliwość zwrócenia się do ENISA o dokonanie przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we współpracy z odpowiednimi zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, państwami członkowskimi, Komisją i innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi UE. Jeżeli chodzi o sektor prywatny, ENISA opracowuje kanały wymiany informacji z wyspecjalizowanymi dostawcami, w tym z dostawcami i sprzedawcami rozwiązań zarządzanych w zakresie bezpieczeństwa, aby realizować misję ENISA polegającą na osiągnięciu wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. Sprawozdanie z przeglądu

konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy dostarczyć EU-CyCLONe, sieci CSIRT i Komisji i powinno ono stanowić wkład w ich prace. W przypadku gdy incydent dotyczy państwa trzeciego, Komisja udostępni sprawozdanie również wysokiemu przedstawicielowi.

- (37) Biorąc pod uwagę nieprzewidywalny charakter ataków na cyberbezpieczeństwo oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa” mogą otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli jest to przewidziane w odpowiednim układzie o stowarzyszeniu z tym programem. Unia powinna wspierać finansowanie dla stowarzyszonych państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów. Warunki określone w niniejszym rozporządzeniu w odniesieniu do unijnej rezerwy cyberbezpieczeństwa i zaufanych dostawców powinny mieć zastosowanie do udzielania wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa”.
- (38) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze do określenia warunków interoperacyjności między transgranicznymi SOC; określenia ustaleń proceduralnych dotyczących wymiany informacji między transgranicznymi SOC a podmiotami unijnymi na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę; ustanowienia wymogów technicznych zapewniających bezpieczeństwo europejskiej tarczy cyberbezpieczeństwa; określenia rodzaju i liczby usług reagowania wymaganych do celów unijnej rezerwy cyberbezpieczeństwa; oraz doprecyzowania szczegółowych ustaleń dotyczących przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011.
- (39) Cel niniejszego rozporządzenia można lepiej osiągnąć na poziomie Unii niż państw członkowskich. W związku z tym Unia może podjąć działania zgodnie z zasadami pomocniczości i proporcjonalności określonymi w art. 5 Traktatu o Unii Europejskiej. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Rozdział I

CELE OGÓLNE, PRZEDMIOT I DEFINICJE

Artykuł 1

Przedmiot i cele

1. Niniejszym rozporządzeniem ustanawia się środki mające na celu zwiększenie zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty, w szczególności przez następujące działania:

- a) wprowadzenie ogólnoeuropejskiej infrastruktury centrów monitorowania bezpieczeństwa („europejska tarcza cyberbezpieczeństwa”) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej;
- b) stworzenie mechanizmu cyberkryzysowego, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków;
- c) ustanowienie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny poważnych incydentów lub incydentów na dużą skalę.

2. Celem niniejszego rozporządzenia jest zwiększenie solidarności na szczeblu unijnym przez następujące cele szczegółowe:

- a) wzmocnienie wspólnego unijnego wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie, co umożliwi wzmocnienie konkurencyjnej pozycji sektorów przemysłu i usług w Unii w całej gospodarce cyfrowej oraz wniesienie wkładu w suwerenność technologiczną Unii w dziedzinie cyberbezpieczeństwa;
- b) zwiększenie gotowości podmiotów działających w sektorach krytycznych i wysoce krytycznych w całej Unii oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;
- c) zwiększenie odporności Unii i przyczynianie się do skutecznej reakcji poprzez przegląd i ocenę poważnych incydentów lub incydentów na dużą skalę, w tym wyciąganie wniosków i w stosownych przypadkach wydawanie zaleceń.

3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla głównej odpowiedzialności państw członkowskich za bezpieczeństwo narodowe, bezpieczeństwo publiczne oraz za zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, ich wykrywanie i ściganie.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) **„transgraniczne centrum monitorowania bezpieczeństwa” („transgraniczny SOC”)** oznacza wielokrajową platformę, która łączy w skoordynowanej strukturze sieciowej krajowe SOC z co najmniej trzech państw członkowskich tworzących konsorcjum przyjmujące i która ma zapobiegać cyberzagrożeniom i cyberincydentom oraz wspierać generowanie wysokiej jakości danych wywiadowczych, w szczególności w drodze wymiany danych z różnych źródeł publicznych i prywatnych, a także przez dzielenie się najnowocześniejszymi narzędziami oraz wspólnie rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń i incydentów oraz zapobiegania im i ochrony przed nimi w zaufanym otoczeniu;
- 2) **„podmiot publiczny”** oznacza podmiot prawa publicznego zdefiniowany w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE¹⁸;
- 3) **„konsorcjum przyjmujące”** oznacza konsorcjum składające się z państw uczestniczących, reprezentowanych przez krajowe SOC, które zgodziły się utworzyć narzędzia i infrastrukturę na potrzeby transgranicznego SOC i jego funkcjonowania oraz wnieść wkład w nabycie tych narzędzi i infrastruktury;
- 4) **„podmiot”** oznacza podmiot zdefiniowany w art. 6 pkt 38 dyrektywy (UE) 2022/2555;
- 5) **„podmioty działające w sektorach krytycznych lub wysoce krytycznych”** oznaczają rodzaje podmiotów wymienione w załączniku I i załączniku II do dyrektywy (UE) 2022/2555;
- 6) **„cyberzagrożenie”** oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;
- 7) **„poważny incydent w cyberbezpieczeństwie”** oznacza incydent w cyberbezpieczeństwie spełniający kryteria określone w art. 23 ust. 3 dyrektywy (UE) 2022/2555;
- 8) **„incydent w cyberbezpieczeństwie na dużą skalę”** oznacza incydent zdefiniowany w art. 6 pkt 7 dyrektywy (UE) 2022/2555;
- 9) **„gotowość”** oznacza stan przygotowania i zdolności do zapewnienia skutecznego szybkiego reagowania na poważny incydent w cyberbezpieczeństwie lub incydent w cyberbezpieczeństwie na dużą skalę, który to stan jest osiągnięty w wyniku podjętych uprzednio działań w zakresie oceny ryzyka i monitorowania;
- 10) **„reakcja”** oznacza działanie w przypadku poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę,

¹⁸ 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).

w trakcie takiego incydentu lub po nim w celu zaradzenia jego natychmiastowym i krótkoterminowym negatywnym skutkom;

- 11) „**zaufani dostawcy**” oznaczają dostawców usług zarządzanych w zakresie bezpieczeństwa zdefiniowanych w art. 6 pkt 40 dyrektywy (UE) 2022/2555, wybranych zgodnie z art. 16 niniejszego rozporządzenia.

Rozdział II

EUROPEJSKA TARCZA CYBERBEZPIECZEŃSTWA

Artykuł 3

Ustanowienie europejskiej tarczy cyberbezpieczeństwa

1. W celu rozwijania zaawansowanych zdolności w Unii w zakresie wykrywania, analizowania i przetwarzania danych dotyczących cyberzagrożeń i cyberincydentów w Unii ustanawia się wzajemnie połączoną ogólnoeuropejską infrastrukturę centrów monitorowania bezpieczeństwa („europejska tarcza cyberbezpieczeństwa”). W jej skład wchodzi wszystkie krajowe centra monitorowania bezpieczeństwa („krajowe SOC”) oraz transgraniczne centra monitorowania bezpieczeństwa („transgraniczne SOC”).

Działania służące wdrażaniu europejskiej tarczy cyberbezpieczeństwa wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3.

2. Europejska tarcza cyberbezpieczeństwa:

- a) gromadzi i udostępnia dane na temat cyberzagrożeń i cyberincydentów z różnych źródeł za pośrednictwem transgranicznych SOC;
- b) generuje wysokiej jakości i użyteczne operacyjnie informacje i dane wywiadowcze dotyczące cyberzagrożeń, wykorzystując najnowocześniejsze narzędzia, w szczególności sztuczną inteligencję i technologie analityki danych;
- c) przyczynia się do lepszej ochrony przed cyberzagroženiami i lepszego reagowania na nie;
- d) przyczynia się do szybszego wykrywania cyberzagrożeń i zapewniania orientacji sytuacyjnej w całej Unii;
- e) udostępnia usługi i działania na rzecz społeczności zajmującej się cyberbezpieczeństwem w Unii, w tym przyczynia się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych.

Jest ona rozwijana we współpracy z ogólnoeuropejską infrastrukturą obliczeń wielkiej skali ustanowioną na podstawie rozporządzenia (UE) 2021/1173.

Krajowe centra monitorowania bezpieczeństwa

1. Aby uczestniczyć w europejskiej tarczy cyberbezpieczeństwa, każde państwo członkowskie wyznacza co najmniej jeden krajowy SOC. Krajowy SOC jest podmiotem publicznym.

Ma on zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na szczeblu krajowym w celu gromadzenia i analizowania informacji dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz wnoszenia wkładu w transgraniczny SOC. Jest on wyposażony w najnowocześniejsze technologie wykrywania, agregowania i analizy danych istotnych dla zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.

2. W następstwie zaproszenia do wyrażenia zainteresowania Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa („ECCC”) wybiera krajowe SOC do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać wybranym krajowym SOC dotacje na finansowanie funkcjonowania tych narzędzi i infrastruktur. Wkład finansowy Unii pokrywa do 50 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa państwo członkowskie. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i krajowy SOC zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.

3. Krajowy SOC wybrany na podstawie ust. 2 zobowiązuje się do złożenia wniosku o uczestnictwo w transgranicznym SOC w ciągu dwóch lat od dnia nabycia narzędzi i infrastruktur lub od dnia otrzymania finansowania w formie dotacji, w zależności od tego, która z tych dat przypada wcześniej. Jeżeli do tego czasu krajowy SOC nie zostanie uczestnikiem transgranicznego SOC, nie kwalifikuje się do dodatkowego wsparcia Unii na mocy niniejszego rozporządzenia.

Transgraniczne centra monitorowania bezpieczeństwa

1. Konsorcjum przyjmujące, które składa się z co najmniej trzech państw członkowskich, reprezentowanych przez krajowe SOC, zobowiązujących się do współpracy w celu koordynowania swoich działań w zakresie wykrywania cyberataków i monitorowania zagrożeń, kwalifikuje się do uczestnictwa w działaniach mających na celu ustanowienie transgranicznego SOC.

2. W następstwie zaproszenia do wyrażenia zainteresowania ECCC wybiera konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia i infrastruktury. ECCC może przyznać konsorcjum przyjmującemu dotację na finansowanie funkcjonowania tych narzędzi i infrastruktur. Wkład finansowy Unii pokrywa do 75 % kosztów nabycia narzędzi i infrastruktur oraz do 50 % kosztów operacyjnych, a pozostałe koszty pokrywa konsorcjum przyjmujące. Przed rozpoczęciem procedury nabycia narzędzi i infrastruktur ECCC i konsorcjum przyjmujące zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi i infrastruktur.

3. Członkowie konsorcjum przyjmującego zawierają pisemną umowę konsorcjum określającą ich wewnętrzne ustalenia dotyczące wykonania umowy o przyjęciu i użytkowaniu.

4. Transgraniczny SOC jest reprezentowany do celów prawnych przez krajowy SOC pełniący funkcję koordynującego SOC lub przez konsorcjum przyjmujące, jeżeli ma ono osobowość prawną. Koordynujący SOC odpowiada za zgodność z wymogami umowy o przyjęciu i użytkowaniu oraz niniejszego rozporządzenia.

Artykuł 6

Współpraca i wymiana informacji w ramach transgranicznych SOC i między nimi

1. Członkowie konsorcjum przyjmującego wymieniają się istotnymi informacjami w ramach transgranicznego SOC, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami specyficznymi dla konkretnych agresorów, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi cyberbezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:

- a) ma na celu zapobieganie incydom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydentach lub łagodzenie ich skutków;
- b) zwiększa poziom cyberbezpieczeństwa, zwłaszcza przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się cyberzagrożeń, wspieranie różnorodnych zdolności do obrony przed nimi, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub wspieranie badań nad zagrożeniami prowadzonych w ramach współpracy między podmiotami publicznymi i prywatnymi.

2. Pisemna umowa konsorcjum, o której mowa w art. 5 ust. 3, określa:

- a) zobowiązanie do udostępniania znacznej ilości danych, o których mowa w ust. 1, oraz warunki wymiany tych informacji;
- b) ramy zarządzania zachęcające wszystkich uczestników do wymiany informacji;
- c) cele dotyczące wkładu w rozwój zaawansowanych narzędzi sztucznej inteligencji i analityki danych.

3. Aby wspierać wymianę informacji między transgranicznymi SOC, transgraniczne SOC zapewniają wysoki poziom interoperacyjności między sobą. Aby ułatwić interoperacyjność między transgranicznymi SOC, Komisja może w drodze aktów wykonawczych, po konsultacji z ECCC, określić warunki tej interoperacyjności. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.

4. Transgraniczne SOC zawierają między sobą umowy o współpracy określające zasady wymiany informacji między platformami transgranicznymi.

Artykuł 7

Współpraca i wymiana informacji z podmiotami unijnymi

1. W przypadku gdy transgraniczne SOC uzyskają informacje na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, bez zbędnej zwłoki przekazują istotne informacje EU-CyCLONe, sieci CSIRT i Komisji, biorąc pod uwagę ich odpowiednie role w zarządzaniu kryzysowym zgodnie z dyrektywą (UE) 2022/2555.
2. Komisja może w drodze aktów wykonawczych określić ustalenia proceduralne dotyczące wymiany informacji przewidzianej w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia.

Artykuł 8

Bezpieczeństwo

1. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają wysoki poziom bezpieczeństwa danych i bezpieczeństwa fizycznego infrastruktury europejskiej tarczy cyberbezpieczeństwa oraz zapewniają, aby infrastruktura ta była odpowiednio zarządzana i kontrolowana w taki sposób, aby chronić ją przed zagrożeniami oraz zapewnić bezpieczeństwo jej i systemów, w tym bezpieczeństwo danych wymienianych za pośrednictwem tej infrastruktury.
2. Państwa członkowskie uczestniczące w europejskiej tarczy cyberbezpieczeństwa zapewniają, aby wymiana informacji w ramach europejskiej tarczy cyberbezpieczeństwa z podmiotami, które nie są podmiotami publicznymi państw członkowskich, nie wpływała negatywnie na interesy Unii w zakresie bezpieczeństwa.
3. Komisja może przyjąć akty wykonawcze określające wymagania techniczne dla państw członkowskich w celu wypełnienia ich obowiązku wynikającego z ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2 niniejszego rozporządzenia. Przyjmując te akty, Komisja, wspierana przez wysokiego przedstawiciela, uwzględnia odpowiednie normy bezpieczeństwa na poziomie obronnym, aby ułatwić współpracę z podmiotami wojskowymi.

Rozdział III

MECHANIZM CYBERKRYZYSOWY

Artykuł 9

Ustanowienie mechanizmu cyberkryzysowego

1. Ustanawia się mechanizm cyberkryzysowy, aby zwiększyć odporność Unii na poważne zagrożenia cyberbezpieczeństwa oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę i łagodzić je w duchu solidarności („mechanizm”).

2. Działania służące wdrażaniu mechanizmu cyberkryzysowego wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3.

Artykuł 10

Rodzaje działań

1. W ramach mechanizmu wspiera się następujące rodzaje działań:

- a) działania w zakresie gotowości, w tym skoordynowane testowanie gotowości podmiotów działających w sektorach wysoce krytycznych w całej Unii;
- b) działania w zakresie reagowania wspierające reagowanie na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowe usuwanie ich skutków, realizowane przez zaufanych dostawców uczestniczących w unijnej rezerwie cyberbezpieczeństwa ustanowionej na mocy art. 12;
- c) działania w zakresie wzajemnej pomocy polegające na udzielaniu pomocy przez organy krajowe jednego państwa członkowskiego innemu państwu członkowskiemu, w szczególności zgodnie z art. 11 ust. 3 lit. f) dyrektywy (UE) 2022/2555.

Artykuł 11

Skoordynowane testowanie gotowości podmiotów

1. Do celów wspierania w całej Unii skoordynowanego testowania gotowości podmiotów, o których mowa w art. 10 ust. 1 lit. a), Komisja, po konsultacji z grupą współpracy NIS i ENISA, określa odnośne sektory lub podsektory spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555, z których podmioty mogą podlegać skoordynowanemu testowaniu gotowości, z uwzględnieniem istniejących i planowanych skoordynowanych ocen ryzyka i testów odporności na szczeblu Unii.

2. Grupa współpracy NIS we współpracy z Komisją, ENISA i wysokim przedstawicielem opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania.

Artykuł 12

Ustanowienie unijnej rezerwy cyberbezpieczeństwa

1. Ustanawia się unijną rezerwę cyberbezpieczeństwa, aby pomóc użytkownikom, o których mowa w ust. 3, w reagowaniu lub w udzielaniu wsparcia w reagowaniu na poważne incydenty

w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz w natychmiastowym usuwaniu skutków takich incydentów.

2. Unijna rezerwa cyberbezpieczeństwa składa się z usług reagowania na incydenty świadczonych przez zaufanych dostawców wybranych zgodnie z kryteriami określonymi w art. 16. Rezerwa obejmuje wcześniej zadeklarowane usługi. Usługi te muszą być możliwe do wprowadzenia we wszystkich państwach członkowskich.

3. Użytkownikami usług z unijnej rezerwy cyberbezpieczeństwa są:

a) organy państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie i CSIRT, o których mowa odpowiednio w art. 9 ust. 1 i 2 oraz w art. 10 dyrektywy (UE) 2022/2555;

b) instytucje, organy i jednostki organizacyjne Unii.

4. Użytkownicy, o których mowa w ust. 3 lit. a), korzystają z usług z unijnej rezerwy cyberbezpieczeństwa, aby reagować lub wspierać reagowanie na poważne incydenty lub incydenty na dużą skalę mające wpływ na podmioty działające w sektorach krytycznych lub wysoce krytycznych oraz aby natychmiast usuwać skutki takich incydentów.

5. Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa. Komisja decyduje o priorytetach i rozwoju unijnej rezerwy cyberbezpieczeństwa zgodnie z wymogami użytkowników, o których mowa w ust. 3, i nadzoruje jej wdrażanie oraz zapewnia komplementarność, spójność, synergię i powiązania z innymi działaniami wspierającymi prowadzonymi na podstawie niniejszego rozporządzenia, a także z innymi działaniami i programami unijnymi.

6. Komisja może powierzyć ENISA obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, w całości lub w części, w drodze umów o przyznanie wkładu.

7. Aby wesprzeć Komisję w tworzeniu unijnej rezerwy cyberbezpieczeństwa, ENISA przygotowuje zestawienie potrzebnych usług, po konsultacji z państwami członkowskimi i Komisją. ENISA przygotowuje podobne zestawienie, po konsultacji z Komisją, w celu określenia potrzeb państw trzecich kwalifikujących się do wsparcia z unijnej rezerwy cyberbezpieczeństwa zgodnie z art. 17. W stosownych przypadkach Komisja konsultuje się z wysokim przedstawicielem.

8. Komisja może w drodze aktów wykonawczych określić rodzaje i liczbę usług reagowania wymaganych na potrzeby unijnej rezerwy cyberbezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.

Artykuł 13

Wnioski o wsparcie z unijnej rezerwy cyberbezpieczeństwa

1. Użytkownicy, o których mowa w art. 12 ust. 3, mogą składać wnioski o usługi z unijnej rezerwy cyberbezpieczeństwa w celu wsparcia reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego usuwania skutków takich incydentów.

2. Aby otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, użytkownicy, o których mowa w art. 12 ust. 3, stosują środki łagodzące skutki incyduentu będącego przedmiotem wniosku o wsparcie, które to środki obejmują zapewnienie bezpośredniej pomocy technicznej i innych zasobów, aby wspomóc reagowanie na incydent, oraz działania służące natychmiastowemu usunięciu skutków incyduentu.

3. Wnioski o wsparcie składane przez użytkowników, o których mowa w art. 12 ust. 3 lit. a) niniejszego rozporządzenia, przekazuje się Komisji i ENISA za pośrednictwem pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego przez państwo członkowskie zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555.

4. Państwa członkowskie informują sieć CSIRT i w stosownych przypadkach EU-CyCLONe o swoich wnioskach o wsparcie w reagowaniu na incydenty i w natychmiastowym usuwaniu skutków incydentów na podstawie niniejszego artykułu.

5. Wnioski o wsparcie w reagowaniu na incydenty i w natychmiastowym usuwaniu skutków incydentów zawierają:

- a) odpowiednie informacje na temat podmiotu, na który incydent ma wpływ, i potencjalnych skutków incydentu oraz planowanego wykorzystania wsparcia, którego dotyczy wniosek, w tym wskazanie szacowanych potrzeb;
- b) informacje o środkach zastosowanych w celu złagodzenia skutków incydentu będącego przedmiotem wniosku o wsparcie, o których to środkach mowa w ust. 2;
- c) informacje na temat innych form wsparcia dostępnych dla podmiotu, na który incydent ma wpływ, w tym obowiązujących ustaleń umownych dotyczących usług w zakresie reagowania na incydenty i natychmiastowego usuwania skutków incydentów, a także umów ubezpieczenia potencjalnie obejmujących taki rodzaj incydentu.

6. ENISA, we współpracy z Komisją i grupą współpracy NIS, opracowuje wzór ułatwiający składanie wniosków o wsparcie z unijnej rezerwy cyberbezpieczeństwa.

7. Komisja może w drodze aktów wykonawczych doprecyzować szczegółowe ustalenia dotyczące przyznawania usług wsparcia z unijnej rezerwy cyberbezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 21 ust. 2.

Artykuł 14

Wdrożenie wsparcia z unijnej rezerwy cyberbezpieczeństwa

1. Wnioski o wsparcie z unijnej rezerwy cyberbezpieczeństwa są oceniane przez Komisję przy wsparciu ze strony ENISA lub zgodnie z ustaleniami zawartymi w umowach o przyznanie wkładu na podstawie art. 12 ust. 6, a odpowiedź jest niezwłocznie przekazywana użytkownikom, o których mowa w art. 12 ust. 3.

2. Aby ustalić hierarchię ważności wniosków w przypadku istnienia równocześnie wielu wniosków, w stosownych przypadkach uwzględnia się następujące kryteria:

- a) dotkliwość incydentu w cyberbezpieczeństwie;
- b) rodzaj podmiotu, na który incydent ma wpływ, przy czym jako ważniejsze traktuje się incydenty mające wpływ na podmioty kluczowe zdefiniowane w art. 3 ust. 1 dyrektywy (UE) 2022/2555;
- c) potencjalne skutki dla państw członkowskich lub użytkowników, na których incydent ma wpływ;
- d) potencjalny transgraniczny charakter incydentu i ryzyko rozprzestrzenienia się incydentu na inne państwa członkowskie lub na innych użytkowników;

- e) środki zastosowane przez użytkownika w celu wsparcia reagowania oraz działania służące natychmiastowemu usunięciu skutków incydentu, o których to środkach i działaniach mowa w art. 13 ust. 2 i art. 13 ust. 5 lit. b).
3. Usługi z unijnej rezerwy cyberbezpieczeństwa są świadczone zgodnie z konkretnymi umowami między dostawcą usług a użytkownikiem, któremu udziela się wsparcia w ramach unijnej rezerwy cyberbezpieczeństwa. Umowy te zawierają warunki dotyczące odpowiedzialności.
4. Umowy, o których mowa w ust. 3, mogą opierać się na wzorach przygotowanych przez ENISA po konsultacji z państwami członkowskimi.
5. Komisja i ENISA nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania unijnej rezerwy cyberbezpieczeństwa.
6. W terminie jednego miesiąca od zakończenia działania wspierającego użytkownicy przekazują Komisji i ENISA sprawozdanie podsumowujące na temat świadczonej usługi, osiągniętych wyników i zdobytych doświadczeń. Jeżeli użytkownik pochodzi z państwa trzeciego, jak określono w art. 17, sprawozdanie to udostępnia się wysokiemu przedstawicielowi.
7. Komisja regularnie składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia.

Artykuł 15

Koordinacja z mechanizmami zarządzania kryzysowego

1. W przypadkach gdy poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę wynikają z klęsk lub katastrof zdefiniowanych w decyzji nr 1313/2013/UE¹⁹ lub skutkują takimi klęskami lub katastrofami, wsparcie udzielane na podstawie niniejszego rozporządzenia na potrzeby reagowania na takie incydenty uzupełnia działania podejmowane na podstawie decyzji nr 1313/2013/UE i pozostaje bez uszczerbku dla tej decyzji.
2. W przypadku wystąpienia transgranicznego incydentu w cyberbezpieczeństwie na dużą skalę, w którym uruchamiane są zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), wsparcie udzielane na podstawie niniejszego rozporządzenia na potrzeby reagowania na taki incydent odbywa się zgodnie z odpowiednimi protokołami i procedurami w ramach IPCR.
3. W porozumieniu z wysokim przedstawicielem wsparcie w ramach mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty. Może ono również uzupełniać pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu lub wносить wkład w taką pomoc w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej.
4. Wsparcie w ramach mechanizmu cyberkryzysowego może stanowić część wspólnej reakcji Unii i państw członkowskich w sytuacjach, o których mowa w art. 222 Traktatu o funkcjonowaniu Unii Europejskiej.

¹⁹ Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

Artykuł 16

Zaufani dostawcy

1. W postępowaniach o udzielenie zamówienia do celów utworzenia unijnej rezerwy cyberbezpieczeństwa instytucja zamawiająca działa zgodnie z zasadami określonymi w rozporządzeniu (UE, Euratom) 2018/1046 oraz zgodnie z następującymi zasadami:

- a) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa obejmowała usługi, które mogą być wprowadzone we wszystkich państwach członkowskich, z uwzględnieniem w szczególności krajowych wymogów dotyczących świadczenia takich usług, w tym certyfikacji lub akredytacji;
- b) zapewnienie ochrony podstawowych interesów Unii i jej państw członkowskich w zakresie bezpieczeństwa;
- c) zapewnienie, aby unijna rezerwa cyberbezpieczeństwa wносиła unijną wartość dodaną przez wkład w osiągnięcie celów określonych w art. 3 rozporządzenia (UE) 2021/694, w tym promowanie rozwoju umiejętności w dziedzinie cyberbezpieczeństwa w UE.

2. Przy zamawianiu usług na potrzeby unijnej rezerwy cyberbezpieczeństwa instytucja zamawiająca uwzględnia w dokumentach zamówienia następujące kryteria kwalifikacji:

- a) dostawca musi wykazać, że jego personel charakteryzuje się najwyższym stopniem uczciwości zawodowej, niezależności, odpowiedzialności i kompetencji technicznych niezbędnych do wykonywania działań w danej dziedzinie oraz zapewnia trwałość/ciągłość wiedzy fachowej, a także wymagane zasoby techniczne;
- b) dostawca, jego jednostki zależne i podwykonawcy muszą dysponować ramami chroniącymi informacje szczególnie chronione dotyczące usług, a w szczególności dowody, ustalenia i sprawozdania, oraz zgodnymi z unijnymi przepisami bezpieczeństwa dotyczącymi ochrony informacji niejawnych UE;
- c) dostawca musi dostarczyć wystarczające dowody na to, że jego struktura zarządzania jest przejrzysta, nie zagraża jego bezstronności i jakości świadczonych przez niego usług ani nie powoduje konfliktów interesów;
- d) dostawca musi posiadać odpowiednie poświadczenie bezpieczeństwa, przynajmniej w odniesieniu do personelu mającego wprowadzać usługi;
- e) dostawca musi dysponować odpowiednim poziomem bezpieczeństwa swoich systemów informatycznych;
- f) dostawca musi być wyposażony w sprzęt i oprogramowanie techniczne niezbędne do obsługi żądanej usługi;
- g) dostawca musi być w stanie wykazać, że ma doświadczenie w świadczeniu podobnych usług odpowiednim organom krajowym lub podmiotom działającym w sektorach krytycznych lub wysoce krytycznych;
- h) dostawca musi być w stanie zapewnić usługę w krótkim terminie w państwach członkowskich, w których może świadczyć tę usługę;
- i) dostawca musi być w stanie zapewnić usługę w języku lokalnym państw członkowskich, w których może świadczyć tę usługę;

- j) po wprowadzeniu unijnego programu certyfikacji usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem.

Artykuł 17

Wsparcie dla państw trzecich

1. Państwa trzecie mogą wystąpić z wnioskiem o wsparcie z unijnej rezerwy cyberbezpieczeństwa, jeżeli przewidują to układy o stowarzyszeniu zawarte w związku z uczestnictwem tych państw w programie „Cyfrowa Europa”.
2. Wsparcie z unijnej rezerwy cyberbezpieczeństwa musi być zgodne z niniejszym rozporządzeniem i z wszelkimi szczegółowymi warunkami określonymi w układach o stowarzyszeniu, o których mowa w ust. 1.
3. Do użytkowników ze stowarzyszonych państw trzecich kwalifikujących się do otrzymania usług z unijnej rezerwy cyberbezpieczeństwa należą właściwe organy, takie jak CSIRT i organy ds. zarządzania kryzysowego w cyberbezpieczeństwie.
4. Każde państwo trzecie kwalifikujące się do wsparcia z unijnej rezerwy cyberbezpieczeństwa wyznacza organ, który będzie pełnił funkcję pojedynczego punktu kontaktowego do celów niniejszego rozporządzenia.
5. Przed otrzymaniem jakiegokolwiek wsparcia z unijnej rezerwy cyberbezpieczeństwa państwa trzecie przekazują Komisji i wysokiemu przedstawicielowi informacje na temat swoich zdolności w zakresie cyberodporności i zarządzania ryzykiem, w tym co najmniej informacje na temat środków krajowych wprowadzonych w celu przygotowania się na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, a także informacje na temat odpowiedzialnych podmiotów krajowych, w tym CSIRT lub równoważnych podmiotów, ich zdolności i przydzielonych im zasobów. W przypadku gdy w przepisach art. 13 i 14 niniejszego rozporządzenia mowa jest o państwach członkowskich, przepisy te mają zastosowanie do państw trzecich określonych w ust. 1.
6. Komisja koordynuje z wysokim przedstawicielem działania dotyczące otrzymanych wniosków i wdrażania wsparcia przyznanego państwom trzecim z unijnej rezerwy cyberbezpieczeństwa.

Rozdział IV

MECHANIZM PRZEGLĄDU INCYDENTÓW W CYBERBEZPIECZEŃSTWIE

Artykuł 18

Mechanizm przeglądu incydentów w cyberbezpieczeństwie

1. Na wniosek Komisji, EU-CyCLONe lub sieci CSIRT ENISA dokonuje przeglądu i oceny zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA przekazuje sieci CSIRT, EU-CyCLONe i Komisji sprawozdanie z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań,

w szczególności w świetle zadań określonych w art. 15 i 16 dyrektywy (UE) 2022/2555. W stosownych przypadkach Komisja udostępnia sprawozdanie to wysokiemu przedstawicielowi.

2. W celu przygotowania sprawozdania z przeglądu incydentu, o którym to sprawozdaniu mowa w ust. 1, ENISA współpracuje ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym przedstawicielami państw członkowskich, Komisji, innych odpowiednich instytucji, organów i jednostek organizacyjnych UE, dostawców usług zarządzanych w zakresie bezpieczeństwa i użytkowników usług w zakresie cyberbezpieczeństwa. W stosownych przypadkach ENISA współpracuje również z podmiotami, na które poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę mają wpływ. Na potrzeby przeglądu ENISA może również konsultować się z innymi rodzajami zainteresowanych stron. Przedstawiciele, z którymi przeprowadza się konsultacje, ujawniają wszelkie potencjalne konflikty interesów.

3. Sprawozdanie obejmuje przegląd i analizę konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę, w tym głównych przyczyn, podatności i zdobytych doświadczeń. Informacje poufne chronione są w sprawozdaniu zgodnie z prawem unijnym lub krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych.

4. W stosownych przypadkach sprawozdanie zawiera zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni.

5. W miarę możliwości wersję sprawozdania udostępnia się publicznie. Wersja ta zawiera wyłącznie informacje publiczne.

Rozdział V

PRZEPISY KOŃCOWE

Artykuł 19

Zmiany w rozporządzeniu (UE) 2021/694

W rozporządzeniu (UE) 2021/694 wprowadza się następujące zmiany:

1) w art. 6 wprowadza się następujące zmiany:

a) w ust. 1 wprowadza się następujące zmiany:

1) dodaje się lit. aa) w brzmieniu:

„aa) wspieraniu rozwoju europejskiej tarczy cyberbezpieczeństwa, w tym rozwijaniu, wprowadzaniu i eksploatacji platform krajowych i transgranicznych SOC, które wnoszą wkład w orientację sytuacyjną w Unii oraz w zwiększanie unijnych zdolności wywiadowczych w zakresie cyberzagrożeń;”;

2) dodaje się lit. g) w brzmieniu:

„g) utworzeniu i obsłudze mechanizmu cyberkryzysowego w celu wspierania państw członkowskich w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i reagowaniu na nie, stanowiącego uzupełnienie krajowych zasobów i zdolności oraz innych form wsparcia dostępnych na szczeblu Unii, w tym utworzeniu unijnej rezerwy cyberbezpieczeństwa.”;

a) ust. 2 otrzymuje brzmienie:

„2. Działania w ramach celu szczegółowego nr 3 będą realizowane przede wszystkim za pośrednictwem Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieci krajowych ośrodków koordynacji zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887²⁰, z wyjątkiem działań służących wdrażaniu unijnej rezerwy cyberbezpieczeństwa, które będą realizowane przez Komisję i ENISA.”;

2) w art. 9 wprowadza się następujące zmiany:

a) ust. 2 lit. b), c) i d) otrzymują brzmienie:

„b) 1 776 956 000 EUR na cel szczegółowy nr 2 – »Sztuczna inteligencja«;

c) 1 629 566 000 EUR na cel szczegółowy nr 3 – »Cyberbezpieczeństwo i zaufanie«;

d) 482 347 000 EUR na cel szczegółowy nr 4 – »Zaawansowane umiejętności cyfrowe«;”;

b) dodaje się ust. 8 w brzmieniu:

„8. Na zasadzie odstępstwa od art. 12 ust. 4 rozporządzenia (UE, Euratom) 2018/1046 niewykorzystane środki na zobowiązania i środki na płatności przeznaczone na działania służące osiągnięciu celów określonych w art. 6 ust. 1 lit. g) niniejszego rozporządzenia są automatycznie przenoszone i mogą być przeznaczane na zobowiązania i płatności realizowane do dnia 31 grudnia następnego roku budżetowego.”;

3) art. 14 ust. 2 otrzymuje brzmienie:

„2. Program może zapewniać finansowanie w dowolnej formie przewidzianej w rozporządzeniu finansowym, w tym w szczególności poprzez zamówienia stanowiące podstawową formę lub poprzez dotacje i nagrody.

W przypadku gdy osiągnięcie celu działania wymaga zamówienia innowacyjnych towarów i usług, dotacje można przyznać tylko beneficjentom będącym instytucjami

²⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji (Dz.U. L 202 z 8.6.2021, s. 1).

zamawiającymi lub podmiotami zamawiającymi zdefiniowanymi w dyrektywach Parlamentu Europejskiego i Rady 2014/24/UE ²⁷ i 2014/25/UE ²⁸.

W przypadku gdy do osiągnięcia celów działania niezbędne jest dostarczenie innowacyjnych towarów lub usług, które nie są jeszcze powszechnie dostępne na rynku, instytucja zamawiająca lub podmiot zamawiający mogą zezwolić na udzielenie więcej niż jednego zamówienia w ramach tego samego postępowania o udzielenie zamówienia.

Z powodów należycie uzasadnionych względami bezpieczeństwa publicznego instytucja zamawiająca lub podmiot zamawiający mogą wymagać, aby miejsce wykonania zamówienia znajdowało się na terytorium Unii.

Realizując postępowania o udzielenie zamówienia na potrzeby unijnej rezerwy cyberbezpieczeństwa ustanowionej na mocy art. 12 rozporządzenia (UE) 2023/XX, Komisja i ENISA mogą działać jako centralna jednostka zakupująca w celu udzielania zamówień w imieniu lub na rzecz państw trzecich stowarzyszonych z Programem zgodnie z art. 10. Komisja i ENISA mogą również działać jako hurtownik, kupując, przechowując i odsprzedażając lub przekazując jako darowiznę towary i usługi, w tym przedmioty najmu, tym państwom trzecim. Na zasadzie odstępstwa od art. 169 ust. 3 rozporządzenia (UE) XXX/XXXX [wersja przekształcona rozporządzenia finansowego] wniosek jednego państwa trzeciego wystarcza, aby upoważnić Komisję lub ENISA do działania.

Realizując postępowania o udzielenie zamówienia na potrzeby unijnej rezerwy cyberbezpieczeństwa ustanowionej na mocy art. 12 rozporządzenia (UE) 2023/XX, Komisja i ENISA mogą działać jako centralna jednostka zakupująca w celu udzielania zamówień w imieniu lub na rzecz instytucji, organów i jednostek organizacyjnych Unii. Komisja i ENISA mogą również działać jako hurtownik, kupując, przechowując i odsprzedażając lub przekazując jako darowiznę towary i usługi, w tym przedmioty najmu, instytucjom, organom i jednostkom organizacyjnym Unii. Na zasadzie odstępstwa od art. 169 ust. 3 rozporządzenia (UE) XXX/XXXX [wersja przekształcona rozporządzenia finansowego] wniosek jednej instytucji, jednego organu lub jednej jednostki organizacyjnej Unii wystarcza, aby upoważnić Komisję lub ENISA do działania.

Program może również zapewniać finansowanie w formie instrumentów finansowych w operacjach łączonych.”;

4) dodaje się art. 16a w brzmieniu:

„W przypadku działań służących wdrażaniu europejskiej tarczy cyberbezpieczeństwa ustanowionej na mocy art. 3 rozporządzenia (UE) 2023/XX przepisami mającymi zastosowanie są przepisy określone w art. 4 i 5 rozporządzenia (UE) 2023/XX. W przypadku konfliktu między przepisami niniejszego rozporządzenia a przepisami art. 4 i 5 rozporządzenia (UE) 2023/XX te ostatnie mają pierwszeństwo i mają zastosowanie do tych konkretnych działań.”;

5) art. 19 otrzymuje brzmienie:

„Dotacje w ramach Programu przyznaje się i zarządza się nimi zgodnie z tytułem VIII rozporządzenia finansowego i mogą one pokrywać do 100 % kosztów kwalifikowalnych, bez uszczerbku dla zasady współfinansowania ustanowionej w art. 190 rozporządzenia finansowego. Takie dotacje przyznaje się i zarządza się nimi w sposób określony dla poszczególnych celów.

Wsparcie w formie dotacji może przyznawać bezpośrednio ECCC bez zaproszenia do składania wniosków krajowym SOC, o których mowa w art. 4 rozporządzenia XXXX, oraz konsorcjum przyjmującemu, o którym mowa w art. 5 rozporządzenia XXXX, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia finansowego.

Wsparcie w formie dotacji do celów mechanizmu cyberkryzysowego określonego w art. 10 rozporządzenia XXXX może przyznawać bezpośrednio ECCC państwom członkowskim bez zaproszenia do składania wniosków, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia finansowego.

W przypadku działań określonych w art. 10 ust. 1 lit. c) rozporządzenia 202X/XXXX ECCC informuje Komisję i ENISA o wnioskach państw członkowskich o udzielenie dotacji bezpośrednich bez zaproszenia do składania wniosków.

Do celów wsparcia wzajemnej pomocy w reagowaniu na poważny incydent w cyberbezpieczeństwie lub incydent w cyberbezpieczeństwie na dużą skalę, o której to wzajemnej pomocy mowa w art. 10 lit. c) rozporządzenia XXXX, oraz zgodnie z art. 193 ust. 2 akapit drugi lit. a) rozporządzenia finansowego w należycie uzasadnionych przypadkach koszty można uznać za kwalifikowalne, nawet jeżeli zostały poniesione przed przedłożeniem wniosku o udzielenie dotacji.”;

6) w załącznikach I i II wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

Artykuł 20

Ocena

Do dnia [cztery lata od daty rozpoczęcia stosowania niniejszego rozporządzenia] r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia.

Artykuł 21

Procedura komitetowa

1. Komisję wspomaga Komitet Koordynacyjny ds. Programu „Cyfrowa Europa” ustanowiony rozporządzeniem (UE) 2021/694. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 22

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 Strasburgu dnia r.

*W imieniu Parlamentu Europejskiego
Przewodnicząca*

*W imieniu Rady
Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

1.3. Wniosek/inicjatywa dotyczy:

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

1.4.2. Cel(e) szczegółowy(e)

1.4.3. Oczekiwane wyniki i wpływ

1.4.4. Wskaźniki dotyczące realizacji celów

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii” należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

1.7. Planowane metody wykonania budżetu

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

- 3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY**
- 3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ**
- 3.2. Szacunkowy wpływ finansowy wniosku na środki**
 - 3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne*
 - 3.2.2. Przewidywany produkt finansowany ze środków operacyjnych*
 - 3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne*
 - 3.2.3.1. Szacowane zapotrzebowanie na zasoby ludzkie*
 - 3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi*
 - 3.2.5. Udział osób trzecich w finansowaniu*
- 3.3. Szacunkowy wpływ na dochody**

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

Europa na miarę ery cyfrowej
Europejskie inwestycje strategiczne
Działanie: Kształtowanie cyfrowej przyszłości Europy.

1.3. Wniosek/inicjatywa dotyczy:

- ☒ nowego działania
- ☐ nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego³³
- ☐ przedłużenia bieżącego działania
- ☐ połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Akt w sprawie cybersolidarności zwiększy solidarność na szczeblu unijnym, aby skuteczniej wykrywać zagrożenia cyberbezpieczeństwa i incydenty w cyberbezpieczeństwie oraz lepiej przygotować się i reagować na nie. Jego celem jest:

- a) wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania cyberzagrożeń i cyberincydentów oraz poprawa orientacji sytuacyjnej w tej dziedzinie;
- b) zwiększenie gotowości krytycznych podmiotów w całej UE oraz pogłębienie solidarności dzięki rozwijaniu wspólnych zdolności w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty w cyberbezpieczeństwie na dużą skalę, między innymi dzięki udostępnieniu wsparcia w reagowaniu na incydenty państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa”;
- c) zwiększenie odporności Unii i przyczynianie się do skutecznej reakcji dzięki przeglądowi i ocenie poważnych incydentów lub incydentów na dużą skalę, w tym wyciągnięciu wniosków i w stosownych przypadkach wydaniu zaleceń.

³³

O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

1.4.2. Cel(e) szczegółowy(e)

Akt w sprawie cybersolidarności pozwoli osiągnąć ten zestaw celów przez:

- a) wprowadzenie ogólnoeuropejskiej infrastruktury centrów monitorowania bezpieczeństwa (europejskiej tarczy cyberbezpieczeństwa) w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej;
- b) stworzenie mechanizmu cyberkryzysowego, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków. Wsparcie w reagowaniu na incydenty udostępnia się również europejskim instytucjom, organom, urzędom i agencjom Unii.

Działania te będą objęte wsparciem ze środków programu „Cyfrowa Europa”, który niniejszy instrument ustawodawczy zmienia w celu wprowadzenia wyżej wymienionych działań, zapewnienia wsparcia finansowego na ich rozwój oraz doprecyzowania warunków korzystania ze wsparcia finansowego.

- c) ustanowienie europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny poważnych incydentów lub incydentów na dużą skalę.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Wniosek może przynieść znaczące korzyści dla poszczególnych zainteresowanych stron. Ustanowienie europejskiej tarczy cyberbezpieczeństwa poprawi zdolności państw członkowskich w zakresie wykrywania cyberzagrożeń. Mechanizm cyberkryzysowy uzupełni działania państw członkowskich dzięki wsparciu w sytuacjach nadzwyczajnych w zakresie gotowości, reagowania, natychmiastowego usuwania skutków lub przywrócenia funkcjonowania usług kluczowych.

Działania te wzmocnią konkurencyjną pozycję sektorów przemysłu i przedsiębiorstw w całej gospodarce cyfrowej w Europie oraz wsparcie ich transformacji cyfrowej przez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. W szczególności rozporządzenie ma na celu zwiększenie odporności obywateli, przedsiębiorstw i podmiotów działających w sektorach krytycznych lub wysoce krytycznych na rosnące zagrożenia cyberbezpieczeństwa, które mogą mieć niszczące skutki społeczne i gospodarcze. Cel ten zostanie osiągnięty dzięki inwestycjom w narzędzia, które będą wspierać szybsze wykrywanie zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz reagowanie na nie i pomogą państwom członkowskim w lepszym przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę i w reagowaniu na nie. Powinno to również przyczynić się do zwiększenia zdolności w Europie w tych obszarach, w szczególności w zakresie gromadzenia i analizy danych dotyczących zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

W celu promowania solidarności na szczeblu Unii można uwzględnić szereg wskaźników:

- 1) liczbę infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa nabytych w drodze wspólnych zamówień;
- 2) liczbę działań wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w ramach mechanizmu cyberkryzysowego.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Niniejsze rozporządzenie powinno mieć pełne zastosowanie wkrótce po jego przyjęciu, tj. dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii” należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Wyraźnie transgraniczny charakter zagrożeń cyberbezpieczeństwa w ujęciu ogólnym i rosnąca liczba zagrożeń i incydentów, których skutki uboczne są odczuwalne w innych krajach oraz dotyczą inne sektory i produkty, oznaczają, że państwa członkowskie nie są w stanie skutecznie osiągnąć celów niniejszego wniosku samodzielnie i konieczne są wspólne działania oraz solidarność na szczeblu unijnym. Doświadczenie w zwalczaniu cyberzagrożeń wynikające z wojny w Ukrainie oraz główne wnioski wyciągnięte z działań w zakresie cyberbezpieczeństwa zrealizowanych w ramach prezydencji francuskiej (EU CyCLES) pokazały, że osiągnięcie solidarności na szczeblu unijnym wymaga opracowania konkretnych mechanizmów wzajemnego wsparcia, w szczególności ustanowienia współpracy z sektorem prywatnym. W związku z tym w konkluzjach Rady z dnia 23 maja 2022 r. o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni wezwano Komisję do przedstawienia wniosku w sprawie nowego Funduszu Reagowania Cyberkryzysowego. Wsparcie i działania na szczeblu unijnym służące skuteczniejszemu wykrywaniu zagrożeń cyberbezpieczeństwa oraz zwiększeniu gotowości i zdolności reagowania zapewniają wartość dodaną, ponieważ pozwalają uniknąć powielania podejmowanych działań w Unii i w państwach członkowskich. Może to przyczynić się do lepszego wykorzystania istniejących zasobów oraz do poprawy koordynacji oraz wymiany informacji na temat zdobytych doświadczeń.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

W odniesieniu do orientacji sytuacyjnej i wykrywania w ramach europejskiej tarczy cyberbezpieczeństwa w programie prac w zakresie cyberbezpieczeństwa na lata 2021–2022 w ramach programu „Cyfrowa Europa” zawarto zaproszenie do wyrażenia zainteresowania wspólnymi zamówieniami na narzędzia i infrastrukturę niezbędne do utworzenia transgranicznych SOC oraz zaproszenie do składania wniosków o udzielenie dotacji w celu umożliwienia budowania zdolności SOC obsługujących organizacje publiczne i prywatne.

Jeżeli chodzi o gotowość i reagowanie na incydenty, Komisja ustanowiła krótkoterminowy program wspierania państw członkowskich, przyznając ENISA dodatkowe środki finansowe, aby w trybie natychmiastowym zwiększyć gotowość i zdolność do reagowania na poważne cyberincydenty. Usługi objęte programem będą dotyczyły działań w zakresie gotowości, np. przeprowadzania w podmiotach krytycznych testów penetracyjnych pozwalających zidentyfikować podatności. Program służy również zwiększeniu możliwości udzielania pomocy państwom członkowskim w przypadku poważnego incydentu wpływającego na podmioty krytyczne. Realizacja tego krótkoterminowego programu przez ENISA jest w toku i już dostarczyła istotnych cennych spostrzeżeń, które wzięto pod uwagę przy przygotowywaniu niniejszego rozporządzenia.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Akt w sprawie cybersolidarności będzie opierać się na działaniach wspieranych obecnie przez Unię i państwa członkowskie w celu poprawy orientacji sytuacyjnej i wykrywania cyberzagrożeń oraz reagowania na incydenty w cyberbezpieczeństwie na dużą skalę i transgraniczne incydenty w cyberbezpieczeństwie. Ponadto instrument ten jest spójny z innymi ramami zarządzania kryzysowego, w tym z IPCR, wspólną polityką bezpieczeństwa i obrony, w tym z ramami regulującymi zespoły szybkiego reagowania na cyberincydenty, oraz z pomocą udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu w kontekście art. 42 ust. 7 Traktatu o Unii Europejskiej. Nowy wniosek posłuży również uzupełnieniu i wsparciu struktur opracowanych zgodnie z innymi instrumentami dotyczącymi cyberbezpieczeństwa, takimi jak dyrektywa (UE) 2022/2555 (dyrektywa NIS 2) lub rozporządzenie (UE) 2019/881 (akt o cyberbezpieczeństwie).

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Zarządzanie obszarami działania przydzielonymi ENISA odpowiada jej obowiązującemu mandatowi i zadaniom ogólnym. Te obszary działania mogą wymagać określonych profili lub nowych zadań, ale mogą one zostać wchłonięte przez istniejące zasoby ENISA; rozwiązaniem może też być realokacja lub połączenie różnych zadań. Obecnie ENISA realizuje krótkoterminowy program, który Komisja ustanowiła w 2022 r., aby w trybie natychmiastowym zwiększyć gotowość i zdolność do reagowania na poważne cyberincydenty. Objęte nim usługi dają możliwość udzielania pomocy państwom członkowskim w przypadku poważnego incydentu wpływającego na podmioty krytyczne. Realizacja tego krótkoterminowego programu przez ENISA jest w toku i już dostarczyła istotnych cennych spostrzeżeń, które wzięto pod uwagę przy przygotowywaniu niniejszego rozporządzenia. Zasoby przydzielone na ten program krótkoterminowy można również wykorzystać w kontekście niniejszego rozporządzenia.

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

☒ Ograniczony czas trwania

- ☒ ze skutkiem od dnia przyjęcia wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zwiększenia solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty („akt w sprawie cybersolidarności”)
- ☒ Okres trwania wpływu finansowego: od 2023 r. do 2027 r. w odniesieniu do środków na zobowiązania oraz od 2023 r. do 2031 r. w odniesieniu do środków na płatności³⁴.

☐ Nieograniczony czas trwania

- Wprowadzenie w życie z okresem rozruchu od RRRR r. do RRRR r.,
- po którym następuje faza operacyjna.

1.7. Planowane metody wykonania budżetu³⁵

☒ Bezpośrednie zarządzanie przez Komisję

- ☒ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;
- ☐ przez agencje wykonawcze;

☐ Zarządzanie dzielone z państwami członkowskimi

☒ Zarządzanie pośrednie poprzez przekazanie zadań związanych z wykonaniem budżetu:

- ☐ państwom trzecim lub organom przez nie wyznaczonym;
- ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);
- ☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;
- ☒ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;
- ☐ organom prawa publicznego;
- ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile są im zapewnione odpowiednie gwarancje finansowe;
- ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego i zapewniono odpowiednie gwarancje finansowe;
- ☐ podmiotom lub osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

³⁴ Działania przewidziane w akcie powinny być wspierane ze środków przewidzianych w następnych wieloletnich ramach finansowych.

³⁵ Szczegóły dotyczące metod wykonania budżetu oraz odniesienia do rozporządzenia finansowego znajdują się na stronie BUDGpedia: <https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx>

- W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.

Uwagi

Działania związane z europejską tarczą cyberbezpieczeństwa będzie realizować ECCC. Dopóki ECCC nie będzie w stanie wykonywać własnego budżetu, Komisja Europejska będzie realizować działania w ramach zarządzania bezpośredniego w imieniu ECCC. ECCC może wybrać podmioty na podstawie zaproszeń do wyrażenia zainteresowania udziałem we wspólnych zamówieniach na narzędzia. ECCC może przyznawać dotacje na finansowanie funkcjonowania tych narzędzi.

Ponadto ECCC może przyznawać dotacje na działania w zakresie gotowości w ramach mechanizmu cyberkryzysowego.

Komisja ponosi ogólną odpowiedzialność za wdrażanie unijnej rezerwy cyberbezpieczeństwa. Komisja może powierzyć ENISA obsługę unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, w całości lub w części, w drodze umów o przyznanie wkładu. Działania powierzone ENISA na mocy niniejszego rozporządzenia są zgodne z jej obecnym mandatem. Działania te obejmują: (i) wspieranie grupy współpracy NIS w opracowywaniu działań w zakresie gotowości zgodnie z ocenami ryzyka; (ii) wspieranie Komisji w tworzeniu unijnej rezerwy cyberbezpieczeństwa i nadzorowaniu jej wdrażania, w tym w przyjmowaniu i rozpatrywaniu wniosków o wsparcie; (iii) opracowanie wzorów w celu ułatwienia składania wniosków o wsparcie i opracowanie konkretnych umów zawieranych między dostawcą usług a użytkownikiem, któremu udziela się wsparcia w ramach unijnej rezerwy cyberbezpieczeństwa; (iv) przegląd i ocenę zagrożeń, podatności i działań łagodzących w odniesieniu do konkretnych poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę oraz przygotowywanie sprawozdań na ten temat.

Szacuje się, że wszystkie te zadania będą wymagały około 7 EPC z istniejących zasobów ENISA, biorąc pod uwagę wiedzę fachową i prace przygotowawcze wykonywane obecnie przez ENISA w ramach pilotażu wsparcia w sytuacjach nadzwyczajnych na rzecz gotowości i reagowania na incydenty.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Komisja będzie monitorować wdrażanie i stosowanie tych nowych przepisów oraz zgodność z nimi w celu oceny ich skuteczności. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia do czterech lat od daty rozpoczęcia jego stosowania.

2.2. System zarządzania i kontroli

2.2.1. *Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli*

W rozporządzeniu wprowadza się ramy wdrażania finansowania unijnego w celu zwiększania odporności pod względem cyberbezpieczeństwa dzięki działaniom zwiększającym zdolności w zakresie wykrywania poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, reagowania na takie incydenty i usuwania ich skutków. Wdrażaniem rozporządzenia będą zarządzać działy DG CNECT odpowiedzialne za tę dziedzinę polityki.

Konieczne jest zapewnienie służbom Komisji odpowiednich zasobów, aby mogły sprostać tym nowym zadaniom. Szacuje się, że egzekwowanie nowego rozporządzenia będzie wymagało 6 EPC (3 AD i 3 CA) do realizacji następujących zadań:

- ustalenie działań w zakresie gotowości zgodnie z ocenami ryzyka;
- zapewnienie interoperacyjności między platformami transgranicznych SOC;
- opracowanie potencjalnych aktów wykonawczych (dwóch w odniesieniu do SOC i dwóch w odniesieniu do mechanizmu cyberkryzysowego);
- zarządzanie umowami o przyjęciu i użytkowaniu z SOC;
- ustanowienie unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, bezpośrednio lub na podstawie umowy o przyznanie wkładu zawartej z ENISA. W przypadku zawarcia z ENISA umowy o przyznanie wkładu zadania będą obejmowały opracowanie i nadzorowanie wykonania umowy o przyznanie wkładu w odniesieniu do zadań powierzonych ENISA;
- udział w grupach konsultacyjnych powołanych przez ENISA w celu dokonania przeglądu i oceny poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę oraz sporządzanie sprawozdań.

2.2.2. *Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia*

Stwierdzone ryzyko dla europejskiej tarczy cyberbezpieczeństwa polega na tym, że państwa członkowskie nie udostępniają wystarczającej ilości istotnych informacji na temat cyberzagrożeń ani w ramach platform transgranicznych SOC, ani między platformami transgranicznymi i innymi odpowiednimi podmiotami na szczeblu UE. Aby ograniczyć to ryzyko, przydział środków finansowych nastąpi po zaproszeniu do wyrażenia zainteresowania, w ramach którego państwa członkowskie zobowiążą

się do udostępnienia pewnej ilości informacji na szczeblu UE. Zobowiązanie to zostanie następnie sformalizowane w umowie o przyjęciu i użytkowaniu, która da ECCC uprawnienia do przeprowadzania audytów w celu zapewnienia, aby narzędzia i infrastruktury nabyte w drodze wspólnych zamówień były wykorzystywane zgodnie z umową. Zobowiązania do wysokiego poziomu wymiany informacji w ramach transgranicznych SOC zostaną sformalizowane w umowie konsorcjum.

Ryzyko stwierdzone dla mechanizmu cyberkryzysowego polega na tym, że użytkownicy uczestniczący w tym mechanizmie nie wprowadzają środków wystarczających do zapewnienia gotowości w obliczu cyberataków. Z tego powodu, aby móc otrzymać wsparcie z unijnej rezerwy cyberbezpieczeństwa, użytkownicy mają obowiązek wprowadzić takie środki w zakresie gotowości. Przy składaniu wniosków o wsparcie z unijnej rezerwy cyberbezpieczeństwa użytkownicy muszą wyjaśnić, jakie środki już zastosowano w celu zareagowania na incydent, co zostanie uwzględnione podczas oceny wniosków dotyczących unijnej rezerwy cyberbezpieczeństwa.

2.2.3. *Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)*

Z uwagi na fakt, że zasady dotyczące uczestnictwa w programie „Cyfrowa Europa” mające zastosowanie do wsparcia udzielanego na podstawie aktu w sprawie cybersolidarności są podobne do zasad, które Komisja stosuje w swoich programach prac, a beneficjenci mają podobny profil ryzyka do profilu ryzyka beneficjentów programów w trybie zarządzania bezpośredniego, można oczekiwać, że margines błędu będzie podobny do marginesu przewidzianego przez Komisję w odniesieniu do programu „Cyfrowa Europa”, tj. będzie zapewniał wystarczającą pewność, że ryzyko błędu w wieloletnim okresie wydatkowania mieści się w ujęciu rocznym w przedziale 2–5 %, przy czym ostatecznym celem jest osiągnięcie poziomu błędu rezydualnego jak najbliższego wartości 2 % w momencie zamknięcia programów wieloletnich po uwzględnieniu skutków finansowych wszystkich audytów, korekt i działań w zakresie odzyskiwania kwot.

2.3. **Środki zapobiegania nadużyciom finansowym i nieprawidłowościom**

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

W przypadku europejskiej tarczy cyberbezpieczeństwa ECCC będzie uprawnione do przeprowadzania – w drodze dostępu do informacji i kontroli na miejscu – audytu narzędzi i infrastruktury nabytych w drodze wspólnych zamówień, zgodnie z umową o przyjęciu i użytkowaniu zawieraną między konsorcjum przyjmującym a ECCC.

Dodatkowe potrzeby w zakresie środków niezbędnych do celów niniejszego rozporządzenia zostaną zaspokojone w ramach istniejących środków zapobiegania nadużyciom finansowym mających zastosowanie do instytucji, organów i jednostek organizacyjnych Unii.

3. SZACUNKOWY WPLYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn. ³⁶	państw EFTA ³⁷	krajów kandydujących i potencjalnych krajów kandydujących ³⁸	innych państw	pochodzący z pozostałych dochodów przeznaczonych na określony cel
1	02 04 01 10 – Program „Cyfrowa Europa” – Cyberbezpieczeństwo	Zróżn.	TAK	TAK	NIE	NIE
1	02 04 01 11 – Program „Cyfrowa Europa” – Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa	Zróżn.	TAK	TAK	NIE	NIE
1	02 04 03 – Program „Cyfrowa Europa” – Sztuczna inteligencja	Zróżn.	TAK	TAK	NIE	NIE
1	02 04 04 – Program „Cyfrowa Europa” – Umiejętności	Zróżn.	TAK	TAK	NIE	NIE
1	02 01 30 – Wydatki na wsparcie dotyczące programu „Cyfrowa Europa”	Niezróżn.	TAK	TAK	NIE	NIE

³⁶ Środki zróżnicowane/środki niezróżnicowane

³⁷ EFTA: Europejskie Stowarzyszenie Wolnego Handlu

³⁸ Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące.

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

- ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych
- ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	1 Jednolity rynek, innowacje i gospodarka cyfrowa
---	--------------	--

Wniosek nie zwiększy całkowitego poziomu zobowiązań w ramach programu „Cyfrowa Europa”. Wkład w tę inicjatywę polega bowiem na redystrybucji środków na zobowiązania wynikających z celów szczegółowych nr 2 i nr 4 w celu zwiększenia budżetu celu szczegółowego nr 3 i ECCC. Wszelki wzrost zobowiązań w ramach programu „Cyfrowa Europa” wynikający z przeglądu WRF można wykorzystać do celów tej inicjatywy.

DG CONNECT			Rok 2025	Rok 2026	Rok 2027	Rok 2028+	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			OGÓŁEM
○ Środki operacyjne										
Linia budżetowa ³⁹ 02.040110 (redystrybucja z 02.0403 i 02.0404)	Środki na zobowiązania	(1a)	15,000	15,000	6,000	p.m.				36,000
	Środki na płatności	(2a)	15,000	15,000	6,000					36,000
Linia budżetowa 02.040111.02 (redystrybucja z 02.0403 i 02.0404)	Środki na zobowiązania	(1b)	13,000	23,000	28,000	p.m.				64,000
	Środki na płatności	(2b)	8,450	18,200	25,250	12,100				64,000
Środki administracyjne finansowane ze środków przydzielonych na określone programy ⁴⁰										

³⁹ Zgodnie z oficjalną nomenklaturą budżetową.

Linia budżetowa 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450
OGÓŁEM środki dla DG CONNECT	Środki na zobowiązania	=1a+1b+3	28,150	38,150	34,150	p.m.				100,450
	Środki na płatności	=2a+2b+3	23,600	33,350	31,400	12,100				100,450

○ OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)	28,000	38,000	34,000	p.m.				100,000
	Środki na płatności	(5)	23,450	33,200	31,250	12,100				100,000
○ OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy		(6)	0,150	0,150	0,150	p.m.				0,450
OGÓŁEM środki na DZIAŁ 1 wieloletnich ram finansowych	Środki na zobowiązania	=4 + 6	28,150	38,150	34,150	p.m.				100,450
	Środki na płatności	=5 + 6	23,600	33,350	31,400	12,100				100,450

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu operacyjnego, należy powtórzyć powyższą część:

○ OGÓŁEM środki operacyjne (wszystkie działy operacyjne)	Środki na zobowiązania	(4)	28,000	38,000	34,000	p.m.				100,000
	Środki na płatności	(5)	23,450	33,200	31,250	12,100				100,000
OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy (wszystkie działy)		(6)	0,150	0,150	0,150					0,450

⁴⁰ Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

operacyjne)										
OGÓŁEM środki na DZIAŁY od 1 do 6 wieloletnich ram finansowych (kwota referencyjna)	Środki na zobowiązania	=4 + 6	28,150	38,150	34,150	p.m.				100,450
	Środki na płatności	=5 + 6	23,600	33,350	31,400	12,100				100,450

Dział wieloletnich ram finansowych	7	„Wydatki administracyjne”
---	----------	---------------------------

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznika 5 do decyzji Komisji w sprawie przepisów wewnętrznych dotyczących wykonania budżetu ogólnego Unii Europejskiej), przesyłanego do DECIDE w celu konsultacji między służbami.

w mln EUR (do trzech miejsc po przecinku)

		Rok 2025	Rok 2026	Rok 2027	Rok 2028+	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			OGÓŁEM
Dyrekcja Generalna: CONNECT									
○ Zasoby ludzkie		0,786	0,786	0,786	p.m.				2,358
○ Pozostałe wydatki administracyjne		0,035	0,035	0,035	p.m.				0,105
DG CONNECT OGÓŁEM	Środki	0,821	0,821	0,821					2,463

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	0,821	0,821	0,821					2,463
--	--	--------------	--------------	--------------	--	--	--	--	--------------

w mln EUR (do trzech miejsc po przecinku)

		Rok 2025	Rok 2026	Rok 2027	Rok 2028+	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			OGÓŁEM
OGÓŁEM środki na DZIAŁY od 1 do 7 wieloletnich ram finansowych	Środki na zobowiązania	28,971	38,971	34,971	p.m.				102,913
	Środki na płatności	24,421	34,171	32,221	12,100				102,913

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty ↓			Rok N		Rok N+1		Rok N+2		Rok N+3		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)						OGÓŁEM	
	PRODUKT																	
	Rodzaj ⁴¹	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1 ⁴²																		
- Produkt																		
- Produkt																		
- Produkt																		
Cel szczegółowy nr 1 – suma częściowa																		
CEL SZCZEGÓŁOWY nr 2																		
- Produkt																		
Cel szczegółowy nr 2 – suma częściowa																		
OGÓŁEM																		

⁴¹ Produkty odnoszą się do produktów i usług, które mają zostać zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

⁴² Zgodnie z opisem w pkt 1.4.2. „Cel(e) szczegółowy(e) ...”.

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

- ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych
- ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok 2025	Rok r 2026	Rok 2027	Rok N+3	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			OGÓŁEM
--	-------------	---------------	-------------	------------	---	--	--	--------

DZIAŁ 7 wieloletnich ram finansowych								
Zasoby ludzkie	0,786	0,786	0,786					2,358
Pozostałe wydatki administracyjne	0,035	0,035	0,035					0,105
Suma częściowa DZIAŁU 7 wieloletnich ram finansowych	0,821	0,821	0,821					2,463

Poza DZIAŁEM 7⁴³ wieloletnich ram finansowych								
Zasoby ludzkie								
Pozostałe wydatki o charakterze administracyjnym	0,150	0,150	0,150					0,450
Suma częściowa poza DZIAŁEM 7 wieloletnich ram finansowych	0,150	0,150	0,150					0,450

OGÓŁEM	0,971	0,971	0,971					2,913
---------------	--------------	--------------	--------------	--	--	--	--	--------------

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

⁴³ Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.3.1. Szacowane zapotrzebowanie na zasoby ludzkie

- ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.
- ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

	Rok 2025	Rok 2026	Rok 2027	Rok N+3	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
○ Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)							
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)	3	3	3				
20 01 02 03 (w delegaturach)							
01 01 01 01 (pośrednie badania naukowe)							
01 01 01 11 (bezpośrednie badania naukowe)							
Inna linia budżetowa (określić)							
○ Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC) ⁴⁴							
20 02 01 (CA, SNE, INT z globalnej koperty finansowej)	3	3	3				
20 02 03 (CA, LA, SNE, INT i JPD w delegaturach)							
XX 01 xx yy zz ⁴⁵	- w centrali						
	- w delegaturach						
01 01 01 02 (CA, SNE, INT – pośrednie badania naukowe)							
01 01 01 12 (CA, INT, SNE – bezpośrednie badania naukowe)							
Inna linia budżetowa (określić)							
OGÓŁEM	6	6	6				

XX oznacza odpowiedni obszar polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	- Ustalanie działań w zakresie gotowości zgodnie z ocenami ryzyka (art. 11) - Opracowywanie potencjalnych aktów wykonawczych (dwóch w odniesieniu do SOC i dwóch w odniesieniu do mechanizmu cyberkryzysowego) - Zarządzanie umowami o przyjęciu i użytkowaniu z SOC - Ustanowienie unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, bezpośrednio lub na podstawie umowy o przyznanie wkładu zawartej z ENISA.
Personel zewnętrzny	Pod nadzorem urzędnika: - Ustalanie działań w zakresie gotowości zgodnie z ocenami ryzyka (art. 11) - Opracowywanie potencjalnych aktów wykonawczych (dwóch w odniesieniu do SOC i dwóch w odniesieniu do mechanizmu cyberkryzysowego)

⁴⁴ CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JPD = młodszy specjalista w delegaturze.

⁴⁵ W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA”).

	- Zarządzanie umowami o przyjęciu i użytkowaniu z SOC - Ustanowienie unijnej rezerwy cyberbezpieczeństwa i zarządzanie nią, bezpośrednio lub na podstawie umowy o przyznaniu wkładu zawartej z ENISA.
--	--

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

- ☒ może zostać w pełni sfinansowany(a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF).

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając linie budżetowe, których ma ono dotyczyć, oraz podając odpowiednie kwoty. W przypadku znacznego przeprogramowania należy załączyć arkusz kalkulacyjny.

	23	24	25	26	27	ogółem
CS* nr 1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
CS nr 2 (początkowy)	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Na inicjatywę w zakresie CYBERBEZPIECZEŃSTWA			18 000 000	28 000 000	19 000 000	65 000 000
CS nr 2 (NOWY)	226 316 819	295 067 000	177 649 000	193 809 000	227 608 000	1 120 449 819
CS nr 3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
Z CS nr 2/CS nr 4			15 000 000	15 000 000	6 000 000	36 000 000
CS nr 3 (nowy)	24 361 553	35 596 172	18 638 000	18 638 000	17 175 000	114 408 725
ECCC (początkowy)	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
Z CS nr 2/CS nr 4			13 000 000	23 000 000	28 000 000	64 000 000
ECCC (nowy)	176 222 303	208 374 879	117 228 130	113 704 986	112 851 497	728 381 795
CS nr 4 (początkowy)	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Na inicjatywę w zakresie CYBERBEZPIECZEŃSTWA			10 000 000	10 000 000	15 000 000	35 000 000
CS nr 4 (NOWY)	66 902 708	64 892 032	46 577 977	60 477 245	57 107 201	295 957 163

* CS - cel szczegółowy

- ☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF.

Należy wyjaśnić, który wariant jest konieczny, określając działy i linie budżetowe, których ma dotyczyć, odpowiadające im kwoty oraz proponowane instrumenty, które należy zastosować.

- ☐ wymaga rewizji WRF.

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

- ☒ nie przewiduje współfinansowania ze strony osób trzecich
- ☐ przewiduje współfinansowanie ze strony osób trzecich szacowane zgodnie z poniższymi szacunkami:

środki w mln EUR (do trzech miejsc po przecinku)

	Rok N ⁴⁶	Rok N+1	Rok N+2	Rok N+3	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

⁴⁶ Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy. „N” należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021). Tak samo należy postąpić dla kolejnych lat.

3.3. Szacunkowy wpływ na dochody

- ☒ Wniosek/inicjatywa nie ma wpływu finansowego na dochody
- ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:
 - ☐ wpływ na zasoby własne
 - ☐ wpływ na dochody inne
 - Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków ☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy ⁴⁷						
		Rok N	Rok N+1	Rok N+2	Rok N+3	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł ...								

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

[...]

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

[...]

⁴⁷

W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.