DECYZJA RADY (WPZiB) 2021/1026

z dnia 21 czerwca 2021 r.

w sprawie wsparcia Programu Organizacji ds. Zakazu Broni Chemicznej (OPCW) na rzecz cyberbezpieczeństwa, cyberodporności i zabezpieczania informacji, w ramach wprowadzania w życie strategii UE przeciw rozprzestrzenianiu broni masowego rażenia

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 28 ust. 1 i art. 31 ust. 1,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 12 grudnia 2003 r. Rada Europejska przyjęła strategię UE przeciw rozprzestrzenianiu broni masowego rażenia (zwaną dalej „strategią UE"), której rozdział III zawiera wykaz środków służących zwalczaniu takiego rozprzestrzeniania.

(2) W strategii UE podkreślono zasadniczą rolę Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów (CWC) oraz Organizacji ds. Zakazu Broni Chemicznej (OPCW) w tworzeniu świata wolnego od broni chemicznej. Cele strategii UE uzupełniają cele realizowane przez OPCW jako podmiot odpowiedzialny za wdrożenie CWC.

(3) W dniu 22 listopada 2004 r. Rada przyjęła wspólne działanie 2004/797/WPZiB ([1]) dotyczące wsparcia działań OPCW. Po jego wygaśnięciu przyjęte zostało wspólne działanie Rady 2005/913/WPZiB ([2]), a następnie wspólne działanie Rady 2007/185/WPZiB ([3]).

Po wspólnym działaniu 2007/185/WPZiB przyjęte zostały decyzje Rady: 2009/569/WPZiB ([4]), 2012/166/WPZiB ([5]), 2013/726/WPZiB ([6]), (WPZiB) 2015/259 ([7]), (WPZiB) 2017/2302 ([8]), (WPZiB) 2017/2303 ([9]) i (WPZiB) 2019/538 ([10]).

([1]) Wspólne działanie Rady 2004/797/WPZiB z dnia 22 listopada 2004 r. w sprawie wsparcia działań OPCW w ramach wprowadzania w życie strategii UE przeciwko rozprzestrzenianiu broni masowego rażenia (Dz.U. L 349 z 25.11.2004, s. 63).

([2]) Wspólne działanie Rady 2005/913/WPZiB z dnia 12 grudnia 2005 r. wspierające działania OPCW w ramach wprowadzania w życie strategii UE przeciwko rozpowszechnianiu broni masowego rażenia (Dz.U. L 331 z 17.12.2005, s. 34).

([3]) Wspólne działanie Rady 2007/185/WPZiB z dnia 19 marca 2007 r. w sprawie wsparcia działań OPCW w ramach wprowadzania w życie strategii UE przeciwko rozprzestrzenianiu broni masowego rażenia (Dz.U. L 85 z 27.3.2007, s. 10).

([4]) Decyzja Rady 2009/569/WPZiB z dnia 27 lipca 2009 r. w sprawie wsparcia działań OPCW w ramach wprowadzania w życie strategii UE przeciwko rozprzestrzenianiu broni masowego rażenia (Dz.U. L 197 z 29.7.2009, s. 96).

([5]) Decyzja Rady 2012/166/WPZiB z dnia 23 marca 2012 r. w sprawie wsparcia działań Organizacji ds. Zakazu Broni Chemicznej (OPCW) w ramach wprowadzania w życie strategii UE przeciwko rozprzestrzenianiu broni masowego rażenia (Dz.U. L 87 z 24.3.2012, s. 49).

([6]) Decyzja Rady 2013/726/WPZiB z dnia 9 grudnia 2013 r. w sprawie wsparcia rezolucji Rady Bezpieczeństwa ONZ nr 2118 (2013) i decyzji Rady Wykonawczej Organizacji ds. Zakazu Broni Chemicznej EC-M-33/Dec 1 w ramach wprowadzania w życie strategii UE przeciw rozprzestrzenianiu broni masowego rażenia (Dz.U. L 329 z 10.12.2013, s. 41).

([7]) Decyzja Rady (WPZiB) 2015/259 z dnia 17 lutego 2015 r. w sprawie wsparcia działań Organizacji ds. Zakazu Broni Chemicznej (OPCW) w ramach wprowadzania w życie strategii UE przeciwko rozprzestrzenianiu broni masowego rażenia (Dz.U. L 43 z 18.2.2015, s. 14).

([8]) Decyzja Rady (WPZiB) 2017/2302 z dnia 12 grudnia 2017 r. w sprawie wsparcia działań OPCW z myślą o udzieleniu pomocy w oczyszczaniu dawnego składu broni chemicznej w Libii w ramach wprowadzania w życie strategii UE przeciw rozprzestrzenianiu broni masowego rażenia (Dz.U. L 329 z 13.12.2017, s. 49).

([9]) Decyzja Rady (WPZiB) 2017/2303 z dnia 12 grudnia 2017 r. w sprawie wsparcia stałego wykonywania rezolucji Rady Bezpieczeństwa ONZ nr 2118 (2013) oraz decyzji Rady Wykonawczej OPCW EC-M-33/DEC.1 dotyczącej zniszczenia broni chemicznej należącej do Syrii, w ramach wprowadzania w życie strategii UE przeciw rozprzestrzenianiu broni masowego rażenia (Dz.U. L 329 z13.12.2017, s. 55).

([10]) Decyzja Rady (WPZiB) 2019/538 z dnia 1 kwietnia 2019 r. w sprawie wsparcia działań Organizacji ds. Zakazu Broni Chemicznej (OPCW) w ramach wprowadzania w życie strategii UE przeciw rozprzestrzenianiu broni masowego rażenia (Dz.U. L 93 z 2.4.2019, s. 3).

(4) Kontynuowanie tak intensywnej i ukierunkowanej pomocy Unii na rzecz OPCW jest niezbędne w kontekście aktywnego wdrażania rozdziału III strategii UE.

(5) Konieczne jest dalsze wsparcie Unii dla Programu OPCW na rzecz cyberbezpieczeństwa, cyberodporności i zabezpieczania informacji, który ma na celu zwiększenie zdolności OPCW do zachowania odpowiedniego poziomu cyberbezpieczeństwa i cyberodporności w odpowiedzi na obecne i pojawiające się wyzwania związane z cyberbezpieczeństwem,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. W celu natychmiastowego i praktycznego zastosowania niektórych elementów strategii UE Unia wspiera projekt OPCW, mając na uwadze następujące cele:

— modernizacja infrastruktury ICT zgodnie z ramami instytucjonalnej ciągłości działania OPCW, ze szczególnym naciskiem na odporność, oraz

— zapewnienie zarządzania uprzywilejowanym dostępem, a także zapewnienie fizycznego, logicznego i kryptograficznego zarządzania informacją oraz jej rozdzielenia w przypadku wszystkich wykorzystywanych przez OPCW sieci strategicznych i sieci misji.

2. W kontekście ust. 1 Unia wspiera następujące działania w ramach projektu OPCW, które są zgodne ze środkami określonymi w rozdziale III strategii UE:

— uruchomienie środowiska sprzyjającego prowadzonym w sposób ciągły wysiłkom na rzecz cyberbezpieczeństwa i cyberodporności w ramach operacji OPCW prowadzonych w wielu miejscach,

— zaprojektowanie spersonalizowanych rozwiązań na potrzeby lokalnej i prowadzonej w chmurze integracji i konfiguracji systemów z wykorzystywanymi przez OPCW systemami ICT oraz rozwiązaniami w zakresie zarządzania uprzywilejowanym dostępem, oraz

— inicjowanie i testowanie rozwiązań w zakresie zarządzania uprzywilejowanym dostępem.

3. Szczegółowy opis działań OPCW wspieranych przez Unię, o których mowa w ust. 2, przedstawiono w załączniku.

Artykuł 2

1. Za wykonanie niniejszej decyzji odpowiada Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (WP).

2. Techniczną realizacją projektu, o którym mowa w art. 1, zajmuje się Sekretariat Techniczny OPCW (zwany dalej „Sekretariatem Technicznym"). Sekretariat Techniczny wykonuje to zadanie pod kierownictwem i kontrolą WP. W tym celu WP dokonuje niezbędnych uzgodnień z Sekretariatem Technicznym.

Artykuł 3

1. Finansowa kwota odniesienia na realizację projektu, o którym mowa w art. 1, wynosi 2 151 823 EUR.

2. Wydatkami finansowanymi z kwoty określonej w ust. 1 zarządza się zgodnie z procedurami i zasadami mającymi zastosowanie do budżetu ogólnego Unii.

3. Komisja nadzoruje właściwe zarządzanie wydatkami, o których mowa w ust. 2. W tym celu zawiera niezbędną umowę z Sekretariatem Technicznym. Umowa ta musi przewidywać, że Sekretariat Techniczny ma zapewnić wyeksponowanie wkładu Unii, stosownie do jego wielkości, oraz określić środki, które mają ułatwić rozwijanie synergii i unikanie powielania działań.

4. Komisja dąży do tego, aby umowa, o której mowa w ust. 3, została zawarta jak najszybciej po wejściu w życie niniejszej decyzji. Informuje Radę o wszelkich związanych z tym trudnościach oraz o dacie zawarcia umowy.

Artykuł 4

WP składa Radzie sprawozdania z wykonania niniejszej decyzji na podstawie regularnych sprawozdań przygotowywanych przez Sekretariat Techniczny. Na podstawie sprawozdań WP Rada dokonuje oceny. Komisja przekazuje informacje dotyczące finansowych aspektów projektu, o którym mowa w art. 1.

Artykuł 5

1. Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

2. Niniejsza decyzja wygasa 24 miesiące po dniu zawarcia umowy, o której mowa w art. 3 ust. 3. Niniejsza decyzja wygasa jednak sześć miesięcy po jej wejściu w życie, jeżeli umowa ta nie zostanie zawarta do tego czasu.

Sporządzono w Luksemburgu dnia 21 czerwca 2021 r.

W imieniu Rady
J. BORRELL FONTELLES
Przewodniczący

ZAŁĄCZNIK

DOKUMENT PROJEKTOWY

1. Kontekst

OPCW jest zobowiązana do utrzymywania infrastruktury, która umożliwia suwerenność informacyjną w sposób proporcjonalny do klasyfikacji uprzywilejowanego dostępu, odpowiednich procedur postępowania i istniejących zagrożeń, a jednocześnie pozwala na ochronę przed pojawiającymi się ryzykami. OPCW nadal stoi w obliczu poważnych i pojawiających się ryzyk cyberbezpieczeństwa i cyberodporności. OPCW jest celem zmotywowanych podmiotów dysponujących wysokimi umiejętnościami i zasobami. Podmioty te nadal często przypuszczają atak na poufność i integralność zasobów informacyjnych i infrastruktury OPCW. Oczywiste jest, że aby odpowiedzieć na problemy podkreślone przez niedawne cyberataki, bieżące względy polityczne i kryzys związany z COVID-19, a jednocześnie uwzględnić wyjątkowe wymogi wiążące się z charakterem prac OPCW nad realizacją mandatu CWC, niezbędne są znaczne inwestycje w zdolności techniczne.

W ramach specjalnego funduszu OPCW na rzecz cyberbezpieczeństwa, ciągłości działania i bezpieczeństwa infrastruktury fizycznej, OPCW opracowała Program na rzecz cyberbezpieczeństwa, cyberodporności i zabezpieczania informacji (zwany dalej „programem OPCW") obejmujący 47 działań będących odpowiedzią na wyzwania dotyczące cyberbezpieczeństwa, z którymi zetknięto się w ostatnim czasie. Program OPCW jest dostosowany do najlepszych praktyk propagowanych przez podmioty takie jak Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) lub wykorzystuje koncepcje związane z unijną dyrektywą o bezpieczeństwie sieci i systemów informatycznych (NIS) w zakresie telekomunikacji i obrony. Program OPCW obejmuje łącznie następujące obszary tematyczne: sieci niejawne i jawne; polityka i zarządzanie; wykrywanie i reagowanie; funkcjonowanie i utrzymanie; oraz telekomunikacja. Program OPCW ma przede wszystkim umożliwić OPCW zmniejszenie szans dysponujących znacznymi zasobami lub wspieranych przez państwa napastników na osiągnięcie ich celów, a także ograniczenie ryzyk, których źródłem są zagrożenia zewnętrzne i wewnętrzne, zarówno ze strony ludzi, jak i technologii. Wsparcie Unii ma postać projektu obejmującego trzy działania, które odpowiadają dwóm z 47 działań przewidzianych w programie OPCW.

2. Cel projektu

Ogólnym celem projektu jest zapewnienie, aby Sekretariat OPCW dysponował zdolnością do utrzymania odpowiedniego poziomu cyberbezpieczeństwa i cyberodporności w ramach przeciwdziałania powtarzającym się i nowym, dotyczącym obrony wyzwaniom w zakresie cyberbezpieczeństwa w siedzibie głównej OPCW i w obiektach pomocniczych, tak aby umożliwić OPCW realizację jej mandatu oraz skuteczne wdrażanie CWC.

3. Założenia

— modernizacja infrastruktury ICT zgodnie z ramami instytucjonalnej ciągłości działania OPCW, ze szczególnym naciskiem na odporność,

— zapewnienie zarządzania uprzywilejowanym dostępem, a także zapewnienie fizycznego, logicznego i kryptograficznego zarządzania informacją oraz jej rozdzieleniem w przypadku wszystkich sieci strategicznych i sieci misji.

4. Rezultaty

Oczekuje się, że projekt przyczyni się do następujących rezultatów:

— sprzęt i usługi ICT zapewniają solidną niezawodność systemu (redundancja hybrydowa/rozproszona geograficznie) oraz ułatwiają zwiększoną dostępność systemów i usług ICT na rzecz ciągłości działania,

— ograniczenie do minimum możliwości, aby pojedynczy czynnik lub pojedyncza osoba wywarli niekorzystny wpływ na poufność i integralność informacji lub systemów w ramach OPCW.

5. Działania

5.1. Działanie 1 – uruchomienie środowiska sprzyjającego prowadzonym w sposób ciągły wysiłkom na rzecz cyberbezpieczeństwa i cyberodporności w ramach operacji OPCW prowadzonych w wielu miejscach

Działanie to ma zapewnić warunki sprzyjające sprawnemu wdrożeniu planowania OPCW w zakresie ciągłości działania w odniesieniu do cyberbezpieczeństwa i cyberodporności. Cel ten zostanie zrealizowany poprzez zajęcie się modernizacją infrastruktury – zmianą architektury lub archiwizacją na rzecz ciągłości działania OPCW w ramach operacji prowadzonych w wielu miejscach. Celem jest również ułatwianie i wspieranie uwzględniania zarządzania uprzywilejowanym dostępem w procesach planowania ciągłości działania oraz procesach reagowania.

5.2. Działanie 2 – zaprojektowanie spersonalizowanego rozwiązania na potrzeby lokalnej i prowadzonej w chmurze integracji i konfiguracji systemów z wykorzystywanymi przez OPCW systemami ICT oraz rozwiązaniami w zakresie zarządzania uprzywilejowanym dostępem

Działanie to koncentruje się na przełożeniu sprzyjającego środowiska na spersonalizowane projektowanie w zakresie lokalnej i prowadzonej w chmurze integracji i konfiguracji systemów z wykorzystywanymi przez OPCW systemami ICT oraz rozwiązaniami w zakresie zarządzania uprzywilejowanym dostępem. Ma to zwiększyć efektywność infrastruktury systemów ICT oraz doprowadzić do zaprojektowania zintegrowanego systemu zarządzania uprzywilejowanym dostępem na potrzeby aktywów strategicznych, który może odstraszać, wykrywać i jest zgodny z odnośnymi możliwościami aktywnego poszukiwania zagrożeń.

5.3. Działanie 3 – inicjowanie i testowanie rozwiązań w zakresie zarządzania uprzywilejowanym dostępem

Działanie to opiera się na wdrożonej infrastrukturze oraz rozwiązaniach w zakresie zarządzania uprzywilejowanym dostępem, opracowanych w celu przejścia w ramach integracji i konfiguracji od teorii do praktyki. Systemy muszą zostać przyporządkowane, muszą zostać określone w nich profile i muszą zostać wbudowane w istniejące systemy, z uwzględnieniem powiązanych czynników politycznych i ludzkich. Po tym jak gruntowne testy zweryfikują i zapewnią stabilność systemu (wszystkie nowe systemy mają mieć silne mechanizmy uwierzytelniania użytkowników i urządzeń, odpowiednią klasyfikację i ochronę informacji oraz zaawansowane zapobieganie utracie danych) na etapie wdrażania i następnie na dalszych etapach, Sekretariat OPCW będzie mógł identyfikować i w miarę możliwości usuwać luki.

6. Czas trwania

Szacuje się, że całkowity okres w ramach którego za pośrednictwem niniejszego projektu ponosi się wydatki i finalizuje działania wynosi 24 miesiące.

7. Beneficjenci

Beneficjentami projektu będą: personel Sekretariatu Technicznego OPCW, organy decydujące o polityce, organy pomocnicze oraz interesariusze CWC, w tym państwa-strony.

8. Wyeksponowanie działań UE

OPCW podejmuje wszelkie niezbędne środki, biorąc pod uwagę uzasadnione względy bezpieczeństwa, aby upublicznić fakt, że projekt ten został sfinansowany przez Unię.