ROZHODNUTIE RADY (SZBP) 2021/1026

z 21. júna 2021

na podporu programu Organizácie pre zákaz chemických zbraní (OPCW) v oblasti kybernetickej bezpečnosti a odolnosti a informačnej bezpečnosti v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o Európskej únii, a najmä na jej článok 28 ods. 1 a článok 31 ods. 1,

so zreteľom na návrh vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Európska rada 12. decembra 2003 prijala stratégiu EÚ proti šíreniu zbraní hromadného ničenia (ďalej len „stratégia EÚ“), ktorá v kapitole III obsahuje zoznam opatrení zameraných na boj proti šíreniu takýchto zbraní.

(2) V stratégii EÚ sa zdôrazňuje kľúčová úloha Dohovoru o zákaze vývoja, výroby, hromadenia a použitia chemických zbraní a o ich zničení (ďalej len „CWC“) a Organizácie pre zákaz chemických zbraní (ďalej len „OPCW“) pri vytváraní sveta bez chemických zbraní. Cieľmi stratégie EÚ sa dopĺňajú ciele, ktoré sleduje OPCW v kontexte svojej zodpovednosti za vykonávanie CWC.

(3) Rada 22. novembra 2004 prijala jednotnú akciu 2004/797/SZBP ([1]) o podpore činností OPCW. Na uvedenú jednotnú akciu po uplynutí jej účinnosti nadviazala jednotná akcia Rady 2005/913/SZBP ([2]), na ktorú následne nadviazala jednotná akcia Rady 2007/185/SZBP ([3]).

Na jednotnú akciu 2007/185/SZBP nadviazali rozhodnutia Rady 2009/569/SZBP ([4]), 2012/166/SZBP ([5]), 2013/726/SZBP ([6]), (SZBP) 2015/259 ([7]), (SZBP) 2017/2302 ([8]), (SZBP) 2017/2303 ([9]) a (SZBP) 2019/538 ([10]).

([1]) Jednotná akcia Rady 2004/797/SZBP z 22. novembra 2004 o podpore činností OPCW v rámci vykonávania Stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 349, 25.11.2004, s. 63).

([2]) Jednotná akcia Rady 2005/913/SZBP z 12. decembra 2005 o podpore činností OPCW v rámci vykonávania Stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 331, 17.12.2005, s. 34).

([3]) Jednotná akcia Rady 2007/185/SZBP z 19. marca 2007 o podpore činností OPCW v rámci vykonávania Stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 85, 27.3.2007, s. 10).

([4]) Rozhodnutie Rady 2009/569/SZBP z 27. júla 2009 o podpore činností OPCW v rámci vykonávania Stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 197, 29.7.2009, s. 96).

([5]) Rozhodnutie Rady 2012/166/SZBP z 23. marca 2012 o podpore činností Organizácie pre zákaz chemických zbraní (OPCW) v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 87, 24.3.2012, s. 49).

([6]) Rozhodnutie Rady 2013/726/SZBP z 9. decembra 2013 na podporu rezolúcie BR OSN 2118 (2013) a rozhodnutia výkonnej rady OPCW č. EC-M-33/DEC.1 v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 329, 10.12.2013, s. 41).

([7]) Rozhodnutie Rady (SZBP) 2015/259 zo 17. februára 2015 na podporu činností Organizácie pre zákaz chemických zbraní (OPCW) v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 43, 18.2.2015, s. 14).

([8]) Rozhodnutie Rady (SZBP) 2017/2302 z 12. decembra 2017 na podporu činností OPCW na pomoc pri sanačných operáciách v bývalom sklade chemických zbraní v Líbyi v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 329, 13.12.2017, s. 49).

([9]) Rozhodnutie Rady (SZBP) 2017/2303 z 12. decembra 2017 na podporu ďalšieho vykonávania rezolúcie Bezpečnostnej rady OSN č. 2118 (2013) a rozhodnutia výkonnej rady OPCW EC-M-33/DEC.1 o likvidácii sýrskych chemických zbraní v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 329, 13.12.2017, s. 55).

([10]) Rozhodnutie Rady (SZBP) 2019/538 z 1. apríla 2019 na podporu činností Organizácie pre zákaz chemických zbraní (OPCW) v rámci vykonávania stratégie EÚ proti šíreniu zbraní hromadného ničenia (Ú. v. EÚ L 93, 2.4.2019, s. 3).

(4) Pokračovanie v takejto intenzívnej a cielenej pomoci organizácii OPCW zo strany Únie je potrebné v súvislosti s aktívnym vykonávaním kapitoly III stratégie EÚ.

(5) Je potrebná ďalšia podpora zo strany Únie pre program OPCW v oblasti kybernetickej bezpečnosti a odolnosti a informačnej bezpečnosti, ktorého cieľom je posilniť schopnosť OPCW udržiavať primeranú úroveň kybernetickej bezpečnosti a odolnosti pri riešení súčasných a vznikajúcich výziev súvisiacich s kybernetickou bezpečnosťou,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Únia na účely okamžitého a praktického uplatňovania niektorých častí stratégie EÚ podporuje projekt OPCW s týmito cieľmi:

— modernizácia infraštruktúry IKT v súlade s inštitucionálnym rámcom OPCW na zabezpečenie kontinuity činností s výrazným dôrazom na odolnosť, a

— zabezpečenie správy privilegovaného prístupu, ako aj riadenia a oddelenia fyzických, logických a kryptografických informácií pre všetky strategické siete a siete misií OPCW.

2. Za činnosti v rámci projektu OPCW, ktoré patria medzi činnosti podporované Úniou a sú v súlade s opatreniami stanovenými v kapitole III stratégie EÚ, sa v súvislosti s odsekom 1 považujú:

— sprevádzkovanie prostredia priaznivého pre úsilie vynakladané v oblasti kybernetickej bezpečnosti a odolnosti v rámci operácií OPCW na viacerých miestach,

— navrhnutie prispôsobeného riešenia pre integráciu a konfiguráciu lokálnych a cloudových systémov so systémami IKT OPCW a s riešeniami riadenia privilegovaného prístupu (PAM), a

— iniciácia a testovanie riešení PAM.

3. Podrobný opis činností OPCW podporovaných Úniou uvedených v odseku 2 sa uvádza v prílohe.

Článok 2

1. Za vykonávanie tohto rozhodnutia zodpovedá vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „VP“).

2. Technické vykonávanie projektu uvedeného v článku 1 zabezpečuje technický sekretariát OPCW (ďalej len „technický sekretariát“). Túto úlohu vykonáva pod vedením a kontrolou VP. VP uzavrie na tento účel s technickým sekretariátom potrebné dohody.

Článok 3

1. Referenčná suma na vykonávanie projektu uvedeného v článku 1 je 2 151 823 EUR.

2. Výdavky financované zo sumy stanovenej v odseku 1 sa spravujú v súlade s postupmi a pravidlami, ktoré sa vzťahujú na všeobecný rozpočet Únie.

3. Komisia dohliada na riadne spravovanie výdavkov uvedených v odseku 2. Na tento účel uzavrie s technickým sekretariátom potrebnú dohodu o financovaní. Na základe uvedenej dohody technický sekretariát zabezpečí viditeľnosť príspevku Únie úmernú jeho výške a stanoví opatrenia na podporu vytvárania synergií a predchádzanie zdvojeniu činností.

4. Komisia vyvinie úsilie, aby sa dohoda uvedená v odseku 3 uzavrela čo najskôr po nadobudnutí účinnosti tohto rozhodnutia. Informuje Radu o všetkých ťažkostiach, ktoré v tomto procese vzniknú, ako aj o dátume uzavretia dohody.

Článok 4

VP podáva Rade správu o vykonávaní tohto rozhodnutia na základe pravidelných správ, ktoré vypracúva technický sekretariát. Správy VP tvoria základ pre hodnotenie, ktoré vykoná Rada. Komisia poskytuje informácie o finančných aspektoch projektu uvedeného v článku 1.

Článok 5

1. Toto rozhodnutie nadobúda účinnosť dňom jeho prijatia.

2. Účinnosť tohto rozhodnutia uplynie 24 mesiacov po uzavretí dohody uvedenej v článku 3 ods. 3 Ak sa však uvedená dohoda neuzavrie do šiestich mesiacov po nadobudnutí účinnosti rozhodnutia, účinnosť rozhodnutia sa po uplynutí tejto lehoty skončí.

V Luxemburgu 21. júna 2021

Za Radu
predseda
J. BORRELL FONTELLES

PRÍLOHA

PROJEKTOVÝ DOKUMENT

1. Kontext

Od OPCW sa vyžaduje, aby udržiavala infraštruktúru, ktorá umožňuje informačnú suverenitu spôsobom, ktorý zodpovedá klasifikáciám privilegovaného prístupu, primeraným postupom zaobchádzania a existujúcim hrozbám, a ktorá je zároveň naďalej schopná zabezpečovať ochranu pred vznikajúcimi rizikami. OPCW naďalej neustále čelí vážnym a vznikajúcim rizikám v súvislosti s kybernetickou bezpečnosťou a kybernetickou odolnosťou. OPCW je cieľom aktérov, ktorých zručnosti sú na vysokej úrovni, ktorí na to majú zdroje a ktorí sú motivovaní. Títo aktéri naďalej často útočia na dôvernosť a integritu informácií a zložky infraštruktúry OPCW. S cieľom reagovať na obavy, ktoré znásobili nedávne kybernetické útoky, súčasné politické úvahy a kríza spôsobená ochorením COVID-19, a vzhľadom na jedinečné požiadavky, ktoré predstavuje povaha práce OPCW na plnenie mandátu CWC, je jasné, že sú potrebné zásadné investície do technických spôsobilostí.

V rámci osobitného fondu OPCW pre kybernetickú bezpečnosť, kontinuitu činností a bezpečnosť fyzickej infraštruktúry OPCW vypracovala svoj program kybernetickej bezpečnosti a odolnosti a informačnej bezpečnosti (ďalej len „program OPCW“) so 47 činnosťami na riešenie výziev v oblasti kybernetickej bezpečnosti, ktoré sa v poslednom čase vyskytli. Program OPCW je zosúladený s najlepšími postupmi, ktoré podporujú subjekty, ako je Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA), alebo používa koncepcie súvisiace s európskou smernicou o bezpečnosti sietí a informačných systémov (NIS) týkajúce sa telekomunikácií a obrany. Program OPCW zahŕňa celkovo tieto tematické oblasti: siete využívané pre utajované skutočnosti a siete bez utajovaných skutočností; politika a riadenie; detekcia a reakcia; prevádzka a údržba; a telekomunikácie. Program OPCW je v zásade navrhnutý tak, aby OPCW umožnil obmedziť príležitosti pre útočníkov s dostatočnými zdrojmi a/alebo štátom sponzorovaných útočníkov na dosiahnutie ich cieľov a zmiernil riziká vyplývajúce tak z vonkajších, ako aj vnútorných hrozieb z ľudského aj technického hľadiska. Podpora Únie je štruktúrovaná ako projekt troch činností, ktoré zodpovedajú dvom zo 47 činností programu OPCW.

2. Účel projektu

Celkovým účelom projektu je zabezpečiť, aby mal sekretariát OPCW kapacitu na zachovanie primeranej úrovne kybernetickej bezpečnosti a odolnosti pri riešení opakujúcich sa a vznikajúcich výziev v oblasti obrany v súvislosti s kybernetickou bezpečnosťou v ústrediach a pomocných zariadeniach OPCW s cieľom umožniť plnenie mandátu OPCW a účinné vykonávanie CWC.

3. Ciele

— Modernizácia infraštruktúry IKT v súlade s inštitucionálnym rámcom OPCW na zabezpečenie kontinuity činností s výrazným dôrazom na odolnosť;

— zabezpečenie správy privilegovaného prístupu, ako aj riadenia a oddelenia fyzických, logických a kryptografických informácií pre všetky strategické siete a siete misií.

4. Výsledky

K očakávaným výsledkom, ku ktorým projekt prispeje, patria:

— Zariadenia a služby IKT zabezpečia vysokú spoľahlivosť systému (hybridná/geografická redundancia) a uľahčia zvýšenú dostupnosť systémov a služieb IKT na podporu kontinuity činností;

— Minimalizácia schopností akéhokoľvek jednotlivého faktora alebo osoby nepriaznivo ovplyvniť dôvernosť a integritu informácií alebo systémov v rámci OPCW.

5. Činnosti

5.1. 1. činnosť – sprevádzkovanie prostredia priaznivého pre úsilie vynakladané v oblasti kybernetickej bezpečnosti a odolnosti v rámci operácií OPCW na viacerých miestach

Cieľom tejto činnosti je zabezpečiť priaznivé prostredie pre bezproblémové zavádzanie plánovania kontinuity činností OPCW v súvislosti s kybernetickou bezpečnosťou a odolnosťou. To sa dosiahne prostredníctvom modernizácie infraštruktúry – opätovným navrhnutím a/alebo archiváciou na účely kontinuity činností OPCW v rámci operácií na viacerých miestach. Rovnako je potrebné ďalej uľahčiť a umožniť integráciu správy privilegovaného prístupu do procesov plánovania kontinuity činností a reakcie na ne.

5.2. 2. činnosť – navrhnutie prispôsobeného riešenia pre integráciu a konfiguráciu lokálnych a cloudových systémov so systémami IKT v rámci OPCW a s riešeniami riadenia privilegovaného prístupu (PAM)

Táto činnosť sa zameria na premietnutie priaznivého prostredia do prispôsobeného návrhu na integráciu a konfiguráciu lokálnych a cloudových systémov so systémami IKT v rámci OPCW a s riešeniami PAM. Očakáva sa, že sa tým zvýši účinnosť infraštruktúry systémov IKT a povedie to k návrhu integrovaného systému PAM pre kritické aktíva, ktorý dokáže odrádzať a odhaľovať a bude v súlade s primeranými schopnosťami vyhľadávania hrozieb.

5.3. 3. činnosť – iniciácia a testovanie riešení PAM

Táto činnosť vychádza z realizovanej infraštruktúry a riešení PAM určených na to, aby integrácia a konfigurácia prešli od teórie k praxi. Systémy sa musia mapovať, profilovať a vkladať do existujúcich systémov, pričom sa musia zohľadniť súvisiace politické a ľudské faktory. Potom sa pri realizácii a v priebehu času dôkladným testovaním overí a zabezpečí spoľahlivosť systému (všetky nové systémy disponujú silnou autentifikáciou používateľov a zariadení, primeranou klasifikáciou a ochranou informácií a pokročilými systémami pre prevenciu straty údajov), čo umožní sekretariátu OPCW identifikovať a riešiť nedostatky v čo najväčšom rozsahu.

6. Trvanie

Očakáva sa, že celková odhadovaná dĺžka realizácie financovaná prostredníctvom tohto projektu bude predstavovať 24 mesiacov a v tomto termíne sa aj ukončí.

7. Príjemcovia

Príjemcami projektu budú zamestnanci technického sekretariátu OPCW, orgány zodpovedné za tvorbu politík, pomocné orgány a zainteresované strany CWC vrátane štátov, ktoré sú zmluvnými stranami dohovoru.

8. Zviditeľnenie EÚ

OPCW prijme v rámci primeraných aspektov bezpečnosti všetky vhodné opatrenia na propagáciu skutočnosti, že tento projekt financuje Únia.