►B

ODLUKA VIJEĆA (ZVSP) 2021/1026

od 21. lipnja 2021.

o potpori Programu za kibersigurnost i kiberotpornost te sigurnost informacija Organizacije za zabranu kemijskog oružja (OPCW) u okviru provedbe Strategije EU-a za sprečavanje širenja oružja za masovno uništenje

(SL L 224, 24.6.2021., str. 24.)

Koju je izmijenila:

		Službeni list		
		br.	stranica	datum
►M1	Odluka Vijeća (ZVSP) 2023/1515 od 20. srpnja 2023.	L 184	37	21.7.2023.

▼B

ODLUKA VIJEĆA (ZVSP) 2021/1026

od 21. lipnja 2021.

o potpori Programu za kibersigurnost i kiberotpornost te sigurnost informacija Organizacije za zabranu kemijskog oružja (OPCW) u okviru provedbe Strategije EU-a za sprečavanje širenja oružja za masovno uništenje

Članak 1.

1. U svrhu neposredne i praktične primjene određenih elemenata Strategije EU-a, Unija podupire projekt OPCW-a sa sljedećim ciljevima:

— nadogradnja infrastrukture IKT-a u skladu s institucionalnim okvirom OPCW-a za kontinuitet poslovanja, s posebnim naglaskom na otpornosti; i

— osiguravanje upravljanja povlaštenim pristupom, kao i upravljanja fizičkim, logičkim i kriptografskim informacijama te njihovog odvajanja za sve strateške mreže i mreže misija OPCW-a.

2. U kontekstu stavka 1. Unija podupire sljedeće aktivnosti projekta OPCW-a koje su usklađene s mjerama utvrđenima u poglavlju III. strategije EU-a:

— operacionalizaciju povoljnog okruženja za napore koji se trenutačno ulažu u kibersigurnost i kiberotpornost u okviru operacija OPCW-a na više lokacija;

— razvoj prilagođenih rješenja za integraciju i konfiguraciju sustava, lokalnih i u oblaku, sa sustavima IKT-a OPCW-a i rješenjima za upravljanje povlaštenim pristupom (*Privileged Access Management*/PAM); i

— pokretanje i testiranje rješenjâ za PAM.

3. Detaljan opis aktivnosti OPCW-a koje podupire Unija navedenih u stavku 2. utvrđen je u Prilogu.

Članak 2.

1. Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku („VP”) odgovoran je za provedbu ove Odluke.

2. Tehnička provedba projekta iz članka 1. povjerena je Tehničkom tajništvu OPCW-a („Tehničko tajništvo”). Ono tu zadaću provodi pod odgovornošću i nadzorom VP-a. U tu svrhu VP sklapa potrebne dogovore s Tehničkim tajništvom.

▼B

Članak 3.

1. Financijski referentni iznos za provedbu projekta iz članka 1. iznosi 2 151 823 EUR.

2. Rashodima koji se financiraju iz iznosa navedenog u stavku 1. upravlja se u skladu s postupcima i pravilima koji se primjenjuju na opći proračun Unije.

3. Komisija nadzire ispravnost upravljanja rashodima iz stavka 2. U tu svrhu Komisija sklapa potrebni sporazum s Tehničkim tajništvom. Tim sporazumom utvrđuje se da Tehničko tajništvo mora osigurati vidljivost doprinosa Unije koja je razmjerna njegovoj veličini te odrediti mjere kojima se olakšava razvoj sinergija i izbjegava udvostručavanje aktivnosti.

4. Komisija nastoji sklopiti sporazum iz stavka 3. u najkraćem mogućem roku nakon stupanja na snagu ove Odluke. Komisija obavješćuje Vijeće o eventualnim poteškoćama u tom procesu i o datumu sklapanja sporazuma.

Članak 4.

VP izvješćuje Vijeće o provedbi ove Odluke na temelju redovitih izvješća koje priprema Tehničko tajništvo. Izvješća VP-a osnova su za evaluaciju koju provodi Vijeće. Komisija pruža informacije o financijskim aspektima projekta iz članka 1.

Članak 5.

1. Ova Odluka stupa na snagu na dan donošenja.

▼M1

2. Ova Odluka prestaje važiti 30. kolovoza 2024.

▼B

PRILOG

PROJEKTNI DOKUMENT

1. Kontekst

OPCW je dužan održavati infrastrukturu koja omogućuje informacijsku suverenost razmjerno klasifikacijama povlaštenog pristupa, odgovarajućim postupcima upravljanja i postojećim prijetnjama, dok istodobno održava sposobnost obrane od novih rizika. OPCW se i dalje neprekidno suočava s ozbiljnim i novim rizicima u vezi s kibersigurnosti i kiberotpornosti. OPCW je meta visokokvalificiranih, dobro opremljenih i motiviranih aktera. Ti akteri nastavljaju često napadati povjerljivost i integritet informacija i infrastrukture OPCW-a. Kako bi se odgovorilo na zabrinutost koju su izazvali nedavni kibernapadi, aktualna politička zbivanja i kriza uzrokovana bolešću COVID-19 te uzimajući u obzir jedinstvene zahtjeve koji proizlaze iz prirode rada OPCW-a u ispunjavanju mandata Konvencije o zabrani razvijanja, proizvodnje, gomilanja i korištenja kemijskog oružja i o njegovu uništenju (CWC), jasno je da su potrebna bitna ulaganja u tehničke sposobnosti.

U okviru Posebnog fonda OPCW-a za kibersigurnost, kontinuitet poslovanja i sigurnost fizičke infrastrukture OPCW je izradio svoj Program za kibersigurnost i kiberotpornost te sigurnost informacija (Program OPCW-a) koji obuhvaća 47 aktivnosti za rješavanje izazova u području kibersigurnosti koji su se nedavno pojavili. Program OPCW-a usklađen je s najboljom praksom koju promiču subjekti kao što je Agencija Europske unije za kibersigurnost (ENISA) ili upotrebljava koncepte povezane s Direktivom EU-a o sigurnosti mrežnih i informacijskih sustava (NIS) u području telekomunikacija i u području obrane. Općenito, Program OPCW-a obuhvaća sljedeća tematska područja: klasificirane i neklasificirane mreže; politika i upravljanje; otkrivanje i odgovor; operacije i održavanje; i telekomunikacije. Program OPCW-a u osnovi je koncipiran tako da je OPCW u stanju omesti napadače koji su dobro opremljeni ili ih sponzorira država u postizanju njihovih ciljeva, te ublažiti rizike povezane s vanjskim i unutarnjim prijetnjama iz ljudske i tehničke perspektive. Potpora Unije strukturirana je kao projekt koji se sastoji triju aktivnosti koji odgovara dvjema od 47 aktivnosti Programa OPCW-a.

2. Svrha projekta

Opća je svrha projekta osigurati da Tajništvo OPCW-a ima kapacitet za održavanje odgovarajuće razine kibersigurnosti i kiberotpornosti u rješavanju izazova u obrani kibersigurnosti koji se ponavljaju i pojavljuju, u sjedištu OPCW-a i u pomoćnim objektima, kako bi se omogućilo ispunjavanje mandata OPCW-a i djelotvorna provedba CWC-a.

3. Ciljevi

— nadogradnja infrastrukture IKT-a u skladu s institucionalnim okvirom kontinuiteta poslovanja OPCW-a s posebnim naglaskom na otpornosti;

— osiguravanje upravljanja povlaštenim pristupom, kao i upravljanja fizičkim, logičkim i kriptografskim informacijama te njihovog odvajanja za sve strateške mreže i mreže misija.

▼B

4. Rezultati

Očekivani rezultati projekta jesu sljedeći:

— opremom i uslugama IKT-a osigurava se robusna pouzdanost sustava (hibridna/geografska zalihost) i omogućuje povećana dostupnost sustava i usluga IKT-a kojima se podupire kontinuitet poslovanja;

— minimiziranje sposobnosti svakog čimbenika ili svake osobe da negativno utječe na povjerljivost i integritet informacija ili sustava unutar OPCW-a.

5. Aktivnosti

5.1 Aktivnost 1. – operacionalizacija povoljnog okruženja za napore koji se trenutačno ulažu u kibersigurnost i kiberotpornost u okviru operacija OPCW-a na više lokacija

Ovom aktivnošću nastoji se osigurati povoljno okruženje za nesmetano uvođenje planiranja kontinuiteta poslovanja OPCW-a u vezi s kibersigurnosti i kiberotpornosti. To će se postići nadogradnjom infrastrukture – reorganizacijom i/ili arhiviranjem radi kontinuiteta poslovanja OPCW-a u okviru operacija na više lokacija. Usto je potrebno dodatno olakšati i omogućiti integraciju upravljanja povlaštenim pristupom u postupke planiranja kontinuiteta poslovanja i odgovora.

5.2 Aktivnost 2. – razvoj prilagođenog rješenja za integraciju i konfiguraciju sustavâ, lokalnu i u oblaku, sa sustavima IKT-a u OPCW-u i rješenjima za upravljanje povlaštenim pristupom (*Privileged Access Management*/PAM)

Ova je aktivnost usmjerena na pretvaranje povoljnog okruženja u prilagođeni dizajn za integraciju i konfiguraciju sustavâ, lokalnu i u oblaku, sa sustavima IKT-a u OPCW-u i rješenjima za PAM. Očekuje se da će se time povećati učinkovitost infrastrukture sustava IKT-a i dovesti do razvoja integriranog sustava za PAM za kritičnu imovinu koji može odvraćati i otkrivati te raspolaže odgovarajućim sposobnostima traženja prijetnji.

5.3 Aktivnost 3. – Pokretanje i testiranje rješenjâ za PAM

Ova aktivnost temelji se na uvedenoj infrastrukturi i rješenjima za PAM koja su razvijena kako bi se integracija i konfiguracija provele iz teorije u praksu. Sustavi se moraju mapirati, profilirati i ugraditi u postojeće sustave te pritom treba uzeti u obzir povezane političke i ljudske čimbenike. Potom će se temeljitim testiranjem provjeriti i osigurati robusnost sustava (svi novi sustavi imaju strogu autentikaciju za korisnike i uređaje, odgovarajuću klasifikaciju i zaštitu informacija te napredno sprečavanje gubitka podataka) u provedbi i tijekom vremena, čime će se Tajništvu OPCW-a omogućiti da prepozna i ukloni nedostatke u mjeri u kojoj je to moguće.

6. Trajanje

Ukupno trajanje izvođenja i zaključenja provedbe koja se financira u okviru ovog projekta procjenjuje se na 24 mjeseca.

7. Korisnici

Korisnici projekta bit će osoblje Tehničkog tajništva OPCW-a, tijela za oblikovanje politika, pomoćna tijela i dionici CWC-a, uključujući države stranke.

8. Vidljivost EU-a

OPCW poduzima sve odgovarajuće mjere, u okviru razumnih sigurnosnih pitanja, kako bi istaknuo činjenicu da je ovaj projekt financirala Unija.