►B

A TANÁCS (KKBP) 2021/1026 HATÁROZATA

(2021. június 21.)

a Vegyifegyver-tilalmi Szervezet (OPCW) kiberbiztonságra és -rezilienciára és információvédelemre vonatkozó programjának a tömegpusztító fegyverek elterjedése elleni uniós stratégia végrehajtásának keretében történő támogatásáról

(HL L 224., 2021.6.24., 24. o.)

Módosította:

		Hivatalos Lap		
		Szám	Oldal	Dátum
►M1	A Tanács (KKBP) 2023/1515 határozata (2023. július 20.)	L 184	37	2023.7.21.

▼B

A TANÁCS (KKBP) 2021/1026 HATÁROZATA

(2021. június 21.)

a Vegyifegyver-tilalmi Szervezet (OPCW) kiberbiztonságra és -rezilienciára és információvédelemre vonatkozó programjának a tömegpusztító fegyverek elterjedése elleni uniós stratégia végrehajtásának keretében történő támogatásáról

1. cikk

(1) Az uniós stratégia bizonyos elemeinek azonnali és gyakorlati alkalmazása céljából az Unió támogatja az OPCW egyik, a következő célkitűzésekre irányuló projektjét:

— az IKT-infrastruktúra fejlesztése az OPCW intézményi üzletmenet-folytonossági keretével összhangban, nyomatékos hangsúlyt helyezve a rezilienciára, és

— a kiemelt hozzáférés kezelésének, valamint a fizikai, logikai és kriptográfiai információkezelésnek és -szétválasztásnak a biztosítása az OPCW valamennyi stratégiai és műveleti hálózatának esetében.

(2) Az (1) bekezdéssel összefüggésben az OPCW projektjének az Unió által támogatott, az uniós stratégia III. fejezetében meghatározott intézkedéseknek megfelelő tevékenységei a következők:

— támogató környezet működőképessé tétele a több helyszínen folytatott OPCW-műveletek keretében a kiberbiztonságra és -rezilienciára irányuló, folyamatban lévő erőfeszítések számára,

— az OPCW IKT-rendszerekkel való helyben telepített és felhőalapú rendszerintegrációra és -konfigurálásra irányuló testreszabott megoldások, valamint a kiemelt hozzáférés kezelésére irányuló megoldások megtervezése, és

— a kiemelt hozzáférés kezelésére irányuló megoldások bevezetése és tesztelése.

(3) Az OPCW-nek az Unió által támogatott, a (2) bekezdésben említett tevékenységeinek részletes leírását a Melléklet határozza meg.

2. cikk

(1) E határozat végrehajtásáért az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: a főképviselő) felel.

(2) Az 1. cikkben említett projekt technikai végrehajtását az OPCW Technikai Titkársága (a továbbiakban: a Technikai Titkárság) végzi. Az említett feladatot a főképviselő felügyelete alatt és ellenőrzése mellett látja el. A főképviselő e célból megköti a szükséges megállapodásokat a Technikai Titkársággal.

▼B

3. cikk

(1) Az 1. cikkben említett projekt végrehajtására szolgáló pénzügyi referenciaösszeg 2 151 823 EUR.

(2) Az (1) bekezdésben meghatározott összeggel finanszírozott kiadásokat az Unió általános költségvetésére alkalmazandó eljárásoknak és szabályoknak megfelelően kell kezelni.

(3) A (2) bekezdésben említett kiadások megfelelő kezelését a Bizottság felügyeli. E célból megköti a szükséges megállapodást a Technikai Titkársággal. E megállapodásnak rendelkeznie kell arról, hogy a Technikai Titkárságnak biztosítania kell az uniós hozzájárulás láthatóságát, arányosan annak mértékével, valamint meg kell határoznia a szinergiák kialakításának elősegítésére és a tevékenységek közötti átfedések elkerülésére irányuló intézkedéseket.

(4) A Bizottság törekszik arra, hogy a (3) bekezdésben említett megállapodást e határozat hatálybalépését követően mielőbb megkösse. Tájékoztatja a Tanácsot az ezen eljárás során felmerülő bármely nehézségről és a megállapodás megkötésének dátumáról.

4. cikk

A főképviselő a Technikai Titkárság által készített rendszeres jelentések alapján beszámol a Tanácsnak e határozat végrehajtásáról. A főképviselő jelentései képezik a Tanács által végzett értékelés alapját. A Bizottság tájékoztatást nyújt az 1. cikkben említett projekt pénzügyi vonatkozásairól.

5. cikk

(1) Ez a határozat az elfogadásának napján lép hatályba.

▼M1

(2) Ez a határozat 2024. augusztus 30-án hatályát veszti.

▼B

MELLÉKLET

PROJEKTDOKUMENTUM

1. Háttér

Az OPCW-nek olyan infrastruktúrát kell fenntartania, amely lehetővé teszi az információs szuverenitást a kiemelt hozzáférés osztályozásával, a megfelelő kezelési gyakorlatokkal és a fennálló fenyegetésekkel arányos módon, ugyanakkor továbbra is képes az újonnan felmerülő kockázatokkal szembeni védelemre. Az OPCW továbbra is rendszeresen súlyos és felmerülő kockázatokkal szembesül a kiberbiztonság és a kiberreziliencia terén. Az OPCW magasan képzett és jelentős erőforrásokkal rendelkező, rendkívül motivált szereplők célpontja. Az OPCW információs és infrastrukturális eszközeinek titkossága és integritása továbbra is ki van téve e szereplők gyakori támadásainak. Ahhoz, hogy reagálni lehessen azokra az aggályokra, amelyeket a közelmúltbeli kibertámadások, jelenlegi politikai megfontolások és a Covid19-válság okoztak, valamint figyelembe véve azon egyedülálló követelményeket, amelyek az OPCW által a vegyifegyver-tilalmi egyezmény (CWC) megbízatásának teljesítése érdekében végzett munka jellegéből fakadnak, egyértelmű, hogy a technikai képességek terén jelentős beruházásokra van szükség.

Az OPCW-nek a kiberbiztonságra, az üzletmenet-folytonosságra és a fizikai infrastruktúra biztonságára irányuló különleges alapja keretében az OPCW kialakította a kiberbiztonságra és -rezilienciára és az információvédelemre vonatkozó programját (OPCW-program), amely 47 tevékenységet foglal magában a közelmúltban tapasztalt kiberbiztonsági kihívások kezelésére. Az OPCW-program összhangban áll azokkal a bevált gyakorlatokkal, amelyeket olyan szervezetek mozdítanak elő, mint például az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), illetve a telekommunikáció és a védelem területén a hálózati és információs rendszerek biztonságáról szóló európai irányelvhez kapcsolódó koncepciókat alkalmaz. Összességében az OPCW-program a következő tematikus területekre terjed ki: minősített és nem minősített hálózatok; stratégia és irányítás; felderítés és reagálás; működés és karbantartás; és telekommunikáció. Az OPCW-programot alapvetően úgy alakították ki, hogy az OPCW képes legyen csökkenteni a megfelelő forrásokkal rendelkező és/vagy államilag szponzorált elkövetők számára a céljaik eléréséhez nyitva álló lehetőségeket, valamint mérsékelni mind emberi, mind technikai szempontból a külső és a belső fenyegetésből eredő kockázatokat. Az uniós támogatás egy három tevékenységből álló projekt formájában valósul meg, amely az OPCW-program 47 tevékenysége közül kettőnek felel meg.

2. A projekt célja

A projekt általános célja annak biztosítása, hogy az OPCW Titkársága kapacitással rendelkezzen a megfelelő szintű kiberbiztonság és -reziliencia fenntartására az ismétlődő és felmerülő, a kiberbiztonsági védelemmel kapcsolatos kihívások kezelése terén az OPCW központjában és a kapcsolódó létesítményekben, lehetővé téve az OPCW megbízatásának teljesítését és a CWC eredményes végrehajtását.

3. Célkitűzések

— Az IKT-infrastruktúra fejlesztése az OPCW intézményi üzletmenet-folytonossági keretével összhangban, nyomatékos hangsúlyt helyezve a rezilienciára;

— A kiemelt hozzáférés kezelésének, valamint a fizikai, logikai és kriptográfiai információkezelésnek és -szétválasztásnak a biztosítása valamennyi stratégiai és műveleti hálózat esetében.

▼B

4. Eredmények

A várt eredmények, amelyekhez a projekt hozzájárul a következők:

— Az IKT-berendezések és -szolgáltatások által garantált stabil rendszermegbízhatóság (hibrid/földrajzi redundancia), valamint az IKT-rendszerek és -szolgáltatások fokozott rendelkezésre állásának elősegítése az üzletmenet-folytonosság támogatása érdekében;

— Bármely tényező vagy személy arra irányuló képességeinek minimálisra csökkentése, hogy negatív hatást gyakoroljon az információk vagy rendszerek titkosságára és integritására az OPCW-n belül.

5. Tevékenységek

5.1. 1. tevékenység – Támogató környezet működőképessé tétele a több helyszínen folytatott OPCW-műveletek keretében a kiberbiztonságra és -rezilienciára irányuló, folyamatban lévő erőfeszítésekhez

E tevékenység célja, hogy támogató környezetet biztosítson az OPCW kiberbiztonsággal és -rezilienciával kapcsolatos üzletmenet-folytonossági tervezésének zökkenőmentes megvalósításához. Ezt infrastruktúra-fejlesztések – az architektúra átalakítása és/vagy archiválás – révén kell elérni az OPCW üzletmenet-folytonosságának garantálása érdekében a több helyszínen folytatott műveletek esetében. További cél, hogy még inkább megkönnyítések és lehetővé tegyék a kiemelt hozzáférés kezelésének integrálását az üzletmenet-folytonossági tervezésre és a reagálásra vonatkozó folyamatokba.

5.2. 2. tevékenység – Az OPCW IKT-rendszerekkel való helyben telepített és felhőalapú rendszerintegrációra és -konfigurálásra irányuló testreszabott megoldások, valamint a kiemelt hozzáférés kezelésére irányuló megoldások megtervezése

E tevékenység arra fókuszál, hogy ezt a támogató környezetet a helyben telepített és felhőalapú rendszereknek az OPCW IKT-rendszereibe való integrálására és konfigurálására vonatkozó testreszabott megoldássá alakítsák, valamint a kiemelt hozzáférés kezelésére vonatkozó megoldásokat alakítsanak ki. Ez várhatóan növeli az IKT-rendszerek infrastruktúrájának hatékonyságát, és a kritikus eszközök tekintetében a kiemelt hozzáférés kezelésére vonatkozó, olyan integrált rendszer kialakítását eredményezi, amely lehetővé teszi az elrettentést és az észlelést, és összhangban áll arányos, fenyegetésvadászatra irányuló képességekkel.

5.3. 3. tevékenység – A kiemelt hozzáférés kezelésére irányuló megoldások bevezetése és tesztelése

Ez a tevékenység a már megvalósított infrastruktúrára, valamint az integrációt és a konfigurációt az elméletből a gyakorlatba átültetni hivatott, a kiemelt hozzáférés kezelésére vonatkozó megoldásokra épül. Ehhez el kell végezni a rendszerek feltérképezését, profiljuk meghatározását, és be kell ágyazni őket a meglévő rendszerekbe, mindeközben figyelembe véve a kapcsolódó stratégiai és emberi tényezőket. Ezt követően részletes teszteléssel ellenőrizni és biztosítani kell a rendszer megbízható működését a bevezetésekor és azt követően (valamennyi új rendszer szigorú hitelesítést garantál a felhasználók és az eszközök tekintetében, biztosítja az információk megfelelő minősítését és védelmét, valamint az adatvesztés megelőzését szolgáló fejlett rendszer meglétét), ami lehetővé teszi az OPCW Titkársága számára, hogy a lehető legnagyobb mértékben azonosítsa és orvosolja a hiányosságokat.

6. Időtartam

Az e projekten keresztül finanszírozott végrehajtás teljes becsült időtartama a megkezdéstől a lezárásig várhatóan 24 hónap.

7. Kedvezményezettek

A projekt kedvezményezettjei az OPCW Technikai Titkárságának személyzete, a döntéshozatalért felelős szervek, a kisegítő testületek és a CWC végrehajtásában érdekelt felek lesznek, beleértve a részes államokat is.

8. Az Unió láthatósága

Az OPCW észszerű biztonsági megfontolások mellett minden megfelelő intézkedést megtesz annak közismertté tétele érdekében, hogy e projektet az Unió finanszírozta.