►B

DECISIONE (PESC) 2021/1026 DEL CONSIGLIO

del 21 giugno 2021

a sostegno del programma di cibersicurezza e ciberresilienza e di garanzia di sicurezza delle informazioni dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nell'ambito dell'attuazione della strategia dell'UE contro la proliferazione delle armi di distruzione di massa

(GU L 224 del 24.6.2021, pag. 24)

Modificata da:

		Gazzetta ufficiale		
		n.	pag.	data
►M1	Decisione (PESC) 2023/1515 del Consiglio del 20 luglio 2023	L 184	37	21.7.2023

▼B

DECISIONE (PESC) 2021/1026 DEL CONSIGLIO

del 21 giugno 2021

a sostegno del programma di cibersicurezza e ciberresilienza e di garanzia di sicurezza delle informazioni dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nell'ambito dell'attuazione della strategia dell'UE contro la proliferazione delle armi di distruzione di massa

Articolo 1

1. Al fine di dare applicazione immediata e pratica ad alcuni elementi della strategia dell'UE, l'Unione sostiene un progetto dell'OPCW con gli obiettivi seguenti:

— aggiornare le infrastrutture TIC in linea con il quadro istituzionale di continuità operativa dell'OPCW, ponendo un forte accento sulla resilienza; e

— garantire la governance in materia di accessi privilegiati nonché la gestione e la separazione fisiche, logiche e crittografiche delle informazioni per tutte le reti strategiche e delle missioni dell'OPCW.

2. Nel contesto del paragrafo 1, le attività svolte per il progetto dell'OPCW e sostenute dall'Unione, che sono conformi alle misure di cui al capitolo III previste dalla strategia dell'UE, sono le seguenti:

— porre in atto un contesto favorevole agli sforzi in corso in materia di cibersicurezza e ciberresilienza nell'ambito delle operazioni condotte dall'OPCW in diverse sedi;

— progettare una soluzione personalizzata per l'integrazione e la configurazione di sistemi in locale e basati su cloud con i sistemi TIC dell'OPCW e sviluppare soluzioni di gestione degli accessi privilegiati; e

— avviare e collaudare soluzioni di gestione degli accessi privilegiati.

3. Una descrizione dettagliata delle attività dell'OPCW sostenute dall'Unione, di cui al paragrafo 2, figura nell'allegato.

Articolo 2

1. L'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (AR) è responsabile dell'attuazione della presente decisione.

2. All'attuazione tecnica del progetto di cui all'articolo 1 provvede il segretariato tecnico dell'OPCW («segretariato tecnico»). Esso svolge tale compito sotto la responsabilità e il controllo dell'AR. A tal fine l'AR conclude gli accordi necessari con il segretariato tecnico.

▼B

Articolo 3

1. L'importo di riferimento finanziario per l'esecuzione del progetto di cui all'articolo 1 è pari a 2 151 823 EUR.

2. Le spese finanziate con l'importo di cui al paragrafo 1 sono gestite secondo le procedure e le norme applicabili al bilancio generale dell'Unione.

3. La Commissione vigila sulla corretta gestione delle spese di cui al paragrafo 2. A tal fine essa conclude il necessario accordo con il segretariato tecnico. Tale accordo stipula che il segretariato tecnico deve assicurare la visibilità del contributo dell'Unione, in funzione della sua entità, nonché specificare le misure atte a facilitare lo sviluppo di sinergie ed evitare la duplicazione delle attività.

4. La Commissione si adopera per concludere l'accordo di cui al paragrafo 3 non appena possibile a decorrere dall'entrata in vigore della presente decisione. Essa informa il Consiglio di ogni difficoltà in tale procedimento e della data di conclusione dell'accordo.

Articolo 4

L'AR riferisce al Consiglio in merito all'attuazione della presente decisione sulla scorta di rapporti periodici stilati dal segretariato tecnico. Sui rapporti dell'AR si basa la valutazione del Consiglio. La Commissione fornisce informazioni sugli aspetti finanziari del progetto di cui all'articolo 1.

Articolo 5

1. La presente decisione entra in vigore il giorno dell'adozione.

▼M1

2. La presente decisione cessa di produrre effetti il 30 agosto 2024.

▼B

ALLEGATO

DOCUMENTO DI PROGETTO

1. Contesto

L'OPCW è tenuta a mantenere un'infrastruttura che consenta la sovranità delle informazioni in modo commisurato alle classificazioni di accesso privilegiato, alle opportune routine di gestione e alle minacce esistenti, e che possa al contempo garantire la difesa da rischi emergenti. L'OPCW continua a essere costantemente esposta a rischi gravi ed emergenti connessi alla cibersicurezza e alla ciberresilienza. L'OPCW è bersaglio di attori motivati, altamente qualificati e dotati di risorse. Tali attori continuano a dirigere frequenti attacchi contro la riservatezza e l'integrità delle informazioni e delle infrastrutture dell'OPCW. È evidente che sono necessari investimenti essenziali nelle capacità tecniche, al fine di rispondere alle preoccupazioni messe in evidenza dai recenti attacchi informatici, dalle attuali considerazioni politiche e dalla crisi COVID-19, tenendo conto dei requisiti unici connessi alla natura del lavoro svolto dall'OPCW per adempiere al mandato della CWC.

Nel quadro del fondo speciale dell'OPCW per la cibersicurezza, la continuità operativa e la sicurezza delle infrastrutture fisiche, l'OPCW ha elaborato il proprio programma di cibersicurezza e ciberresilienza e di garanzia di sicurezza delle informazioni (programma dell'OPCW), che contempla 47 attività tese a rispondere alle sfide in materia di cibersicurezza emerse negli ultimi tempi. Il programma dell'OPCW è in linea con le buone prassi promosse da organismi quali l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) o fa ricorso a concetti di cui alla direttiva europea sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) per quanto riguarda le telecomunicazioni e la difesa. Nel complesso il programma dell'OPCW copre i seguenti settori tematici: reti classificate e non classificate; politica e governance; individuazione e risposta; operazioni e manutenzione; telecomunicazioni. Fondamentalmente il programma dell'OPCW è concepito per consentire all'OPCW di ridurre le possibilità che aggressori dotati di considerevoli risorse e/o sostenuti da Stati conseguano i loro obiettivi, come anche di ridurre i rischi provenienti da minacce sia esterne che interne da un punto di vista sia umano che tecnico. Il sostegno dell'Unione è strutturato come un progetto costituito da tre attività, che corrisponde a due delle 47 attività del programma dell'OPCW.

2. Finalità del progetto

La finalità generale del progetto è garantire che il segretariato dell'OPCW sia in grado di mantenere un opportuno livello di cibersicurezza e ciberresilienza nell'affrontare sfide ricorrenti ed emergenti in materia di difesa informatica presso la sede come anche le strutture ausiliarie dell'OPCW, così da garantire l'adempimento del mandato dell'OPCW e l'effettiva attuazione della CWC.

3. Obiettivi

— Aggiornare le infrastrutture TIC in linea con il quadro istituzionale di continuità operativa dell'OPCW, ponendo un forte accento sulla resilienza;

— garantire la governance in materia di accessi privilegiati nonché la gestione e la separazione fisiche, logiche e crittografiche delle informazioni per tutte le reti strategiche e delle missioni.

▼B

4. Risultati

Il progetto contribuisce ai seguenti risultati previsti:

— le apparecchiature e i servizi TIC garantiscono una solida affidabilità di sistema (ridondanza ibrida/geografica) e rendono possibile una maggiore disponibilità dei sistemi e servizi TIC a sostegno della continuità operativa;

— riduzione al minimo della capacità di un singolo fattore o individuo di incidere negativamente sulla riservatezza e sull'integrità delle informazioni o dei sistemi all'interno dell'OPCW.

5. Attività

5.1. Attività 1 – Porre in atto un contesto favorevole agli sforzi in corso in materia di cibersicurezza e ciberresilienza nell'ambito delle operazioni condotte dall'OPCW in diverse sedi

Questa attività mira ad assicurare un ambiente favorevole alla corretta attuazione dei piani per la continuità operativa dell'OPCW relativamente alla cibersicurezza e ciberresilienza. L'obiettivo sarà conseguito attraverso aggiornamenti delle infrastrutture – riorganizzazione dell'architettura e/o archiviazione per la continuità operativa dell'OPCW per quanto riguarda le operazioni condotte in diverse sedi. Si procederà inoltre ad agevolare ulteriormente e ad abilitare l'integrazione della governance in materia di accessi privilegiati nei processi di pianificazione e risposta in materia di continuità operativa.

5.2. Attività 2 – Progettare una soluzione personalizzata per l'integrazione e la configurazione di sistemi in locale e basati su cloud con i sistemi TIC dell'OPCW e sviluppare soluzioni di gestione degli accessi privilegiati

Questa attività è incentrata sulla trasformazione dell'ambiente favorevole in un design personalizzato per l'integrazione e la configurazione di sistemi in locale e basati su cloud con i sistemi TIC dell'OPCW e le soluzioni di gestione degli accessi privilegiati. Si prevede che ciò accresca l'efficienza delle infrastrutture dei sistemi TIC e porti alla progettazione di un sistema integrato di gestione degli accessi privilegiati per le risorse critiche in grado di assicurare la dissuasione e l'individuazione, in linea con commisurate capacità di ricerca delle minacce.

5.3. Attività 3 – Avviare e collaudare soluzioni di gestione degli accessi privilegiati

Questa attività si basa sulle infrastrutture realizzate e sulle soluzioni di gestione degli accessi privilegiati che dovrebbero portare l'integrazione e la configurazione dalla teoria alla pratica. È necessario procedere alla mappatura e profilazione dei sistemi, nonché alla loro integrazione nei sistemi esistenti, tenendo conto dei fattori politici e umani associati. In seguito, test approfonditi verificano e garantiscono la solidità del sistema (tutti i nuovi sistemi dispongono di un'autenticazione forte per utenti e dispositivi, di un'adeguata classificazione e protezione delle informazioni e di sistemi avanzati di prevenzione della perdita di dati) sia in fase di attuazione che a lungo termine; in questo modo il segretariato dell'OPCW potrà, nella misura del possibile, individuare eventuali lacune e porvi rimedio.

6. Durata

La durata totale prevista per l'attuazione finanziata da questo progetto non dovrebbe superare i 24 mesi.

7. Beneficiari

I beneficiari del progetto saranno il personale del segretariato tecnico dell'OPCW, gli organi decisionali, gli organi sussidiari e le parti interessate della CWC, compresi gli Stati parte.

8. Visibilità dell'UE

L'OPCW adotterà tutte le misure opportune, entro ragionevoli considerazioni di sicurezza, per pubblicizzare il fatto che il progetto è stato finanziato dall'Unione.