DECIZIA (PESC) 2021/1026 A CONSILIULUI

din 21 iunie 2021

privind sprijinul acordat Programului de securitate cibernetică și reziliență și asigurare a informațiilor al Organizației pentru Interzicerea Armelor Chimice (OIAC) în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 28 alineatul (1) și articolul 31 alineatul (1),

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 12 decembrie 2003, Consiliul European a adoptat Strategia UE împotriva proliferării armelor de distrugere în masă (denumită în continuare „strategia UE"), al cărei capitol III cuprinde o listă de măsuri de combatere a acestei proliferări.

(2) Strategia UE evidențiază rolul crucial al Convenției privind interzicerea dezvoltării, producerii, stocării și folosirii armelor chimice și distrugerea acestora (CWC) și al Organizației pentru Interzicerea Armelor Chimice (OIAC) în crearea unei lumi fără arme chimice. Obiectivele strategiei UE sunt complementare celor urmărite de OIAC, în contextul responsabilității acesteia de punere în aplicare a CWC.

(3) La 22 noiembrie 2004, Consiliul a adoptat Acțiunea comună 2004/797/PESC ([1]) privind sprijinul acordat activităților OIAC. Acțiunea comună respectivă a fost urmată, la expirarea sa, de Acțiunea comună 2005/913/PESC a Consiliului ([2]), aceasta din urmă fiind urmată, la rândul său, de Acțiunea comună 2007/185/PESC a Consiliului ([3]).

Acțiunea comună 2007/185/PESC a fost urmată de Deciziile 2009/569/PESC ([4]), 2012/166/PESC ([5]), 2013/726/PESC ([6]), (PESC) 2015/259 ([7]), (PESC) 2017/2302 ([8]), (PESC) 2017/2303 ([9]) și (PESC) 2019/538 ([10]) ale Consiliului.

([1]) Acțiunea comună 2004/797/PESC a Consiliului din 22 noiembrie 2004 privind sprijinul acordat activităților OIAC în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 349, 25.11.2004, p. 63).

([2]) Acțiunea comună 2005/913/PESC a Consiliului din 12 decembrie 2005 privind sprijinul acordat activităților OIAC în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 331, 17.12.2005, p. 34).

([3]) Acțiunea comună 2007/185/PESC a Consiliului din 19 martie 2007 privind sprijinul acordat activităților OIAC în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 85, 27.3.2007, p. 10).

([4]) Decizia 2009/569/PESC a Consiliului din 27 iulie 2009 privind sprijinul acordat activităților OIAC în cadrul punerii în aplicare a strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 197, 29.7.2009, p. 96).

([5]) Decizia 2012/166/PESC a Consiliului din 23 martie 2012 privind sprijinul acordat activităților Organizației pentru Interzicerea Armelor Chimice (OIAC) în cadrul punerii în aplicare a strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 87, 24.3.2012, p. 49).

([6]) Decizia 2013/726/PESC a Consiliului din 9 decembrie 2013 în sprijinul RCSONU 2118 (2013) și al EC-M-33/DEC.1 a Consiliului executiv al OIAC, în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 329, 10.12.2013, p. 41).

([7]) Decizia (PESC) 2015/259 a Consiliului din 17 februarie 2015 privind sprijinul acordat activităților Organizației pentru Interzicerea Armelor Chimice (OIAC) în cadrul punerii în aplicare a strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 43, 18.2.2015, p. 14).

([8]) Decizia (PESC) 2017/2302 a Consiliului din 12 decembrie 2017 în sprijinul activităților OIAC de asistență pentru operațiunile de curățare la fostul depozit de arme chimice din Libia în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 329, 13.12.2017, p. 49).

([9]) Decizia (PESC) 2017/2303 a Consiliului din 12 decembrie 2017 în sprijinul continuării punerii în aplicare a Rezoluției Consiliului de Securitate al ONU 2118 (2013) și a Deciziei EC-M-33/DEC.1 a Consiliului executiv al OIAC privind distrugerea armelor chimice siriene în cadrul punerii în aplicare a Strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 329, 13.12.2017, p. 55).

([10]) Decizia (PESC) 2019/538 a Consiliului din 1 aprilie 2019 privind sprijinul acordat activităților Organizației pentru Interzicerea Armelor Chimice (OIAC) în cadrul punerii în aplicare a strategiei UE împotriva proliferării armelor de distrugere în masă (JO L 93, 2.4.2019, p. 3).

(4) Continuarea unei asemenea asistențe intensive și specifice acordate de Uniune către OIAC este necesară în contextul punerii în aplicare în mod activ a capitolului III din strategia UE.

(5) Este necesar ca Uniunea să sprijine în continuare Programul de securitate cibernetică și reziliență și asigurare a informațiilor al OIAC, care vizează consolidarea capacității OIAC de a menține niveluri adecvate de securitate cibernetică și reziliență în abordarea provocărilor actuale și emergente legate de securitatea cibernetică,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

(1) În scopul aplicării imediate și concrete a anumitor elemente din strategia UE, Uniunea acordă sprijin unui proiect al OIAC cu următoarele obiective:

— modernizarea infrastructurii TIC în conformitate cu cadrul instituțional de continuitate a activității al OIAC, cu un accent puternic pe reziliență; și

— asigurarea guvernanței accesului privilegiat, precum și gestionarea și separarea fizice, logice și criptografice ale informațiilor pentru toate rețelele strategice și de misiune ale OIAC.

(2) În contextul alineatului (1), activitățile sprijinite de Uniune în cadrul proiectului OIAC, care corespund măsurilor prevăzute în capitolul III din strategia UE, sunt următoarele:

— operaționalizarea unui mediu propice pentru eforturile continue de securitate cibernetică și reziliență în cadrul operațiunilor OIAC cu amplasamente multiple;

— conceperea unor soluții personalizate pentru integrarea și configurarea sistemelor de la fața locului și a celor de tip cloud cu sistemele TIC ale OIAC și cu soluțiile de gestionare a accesului privilegiat (PAM); și

— inițierea și testarea soluțiilor de PAM.

(3) În anexă este prezentată o descriere detaliată a activităților OIAC sprijinite de Uniune menționate la alineatul (2).

Articolul 2

(1) Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate (ÎR) este responsabil de punerea în aplicare a prezentei decizii.

(2) Punerea în aplicare tehnică a proiectului menționat la articolul 1 este realizată de Secretariatul tehnic al OIAC (denumit în continuare „secretariatul tehnic"). Acesta îndeplinește sarcina respectivă sub responsabilitatea și controlul ÎR. În acest scop, ÎR încheie acordurile necesare cu secretariatul tehnic.

Articolul 3

(1) Valoarea de referință financiară pentru punerea în aplicare a proiectului menționat la articolul 1 este de 2 151 823 EUR.

(2) Cheltuielile finanțate din suma prevăzută la alineatul (1) sunt gestionate în conformitate cu procedurile și normele aplicabile bugetului general al Uniunii.

(3) Comisia supraveghează gestionarea corectă a cheltuielilor menționate la alineatul (2). În acest scop, aceasta încheie acordul necesar cu secretariatul tehnic. Acordul respectiv prevede obligația secretariatului tehnic de a asigura vizibilitatea contribuției Uniunii corespunzător cu dimensiunea acesteia și de a preciza măsurile de facilitare a dezvoltării unor sinergii și de evitare a suprapunerii activităților.

(4) Comisia depune eforturile necesare pentru a încheia acordul menționat la alineatul (3) cât mai curând posibil după intrarea în vigoare a prezentei decizii. Aceasta informează Consiliul cu privire la orice dificultate care intervine în cursul acestui proces și cu privire la data încheierii acordului.

Articolul 4

ÎR informează Consiliul cu privire la punerea în aplicare a prezentei decizii, pe baza unor rapoarte întocmite periodic de secretariatul tehnic. Aceste rapoarte stau la baza evaluării efectuate de Consiliu. Comisia furnizează informații cu privire la aspectele financiare ale proiectului menționat la articolul 1.

Articolul 5

(1) Prezenta decizie intră în vigoare la data adoptării.

(2) Prezenta decizie expiră după 24 de luni de la data încheierii acordului menționat la articolul 3 alineatul (3). Totuși, aceasta expiră după șase luni de la intrarea ei în vigoare în situația în care acordul respectiv nu a fost încheiat până la data respectivă.

Adoptată la Luxemburg, 21 iunie 2021.

Pentru Consiliu
Președintele
J. BORRELL FONTELLES

ANEXĂ

DOCUMENT DE PROIECT

1. Context

OIAC are obligația de a menține o infrastructură care permite suveranitatea informațiilor într-un mod proporțional cu clasificările accesului privilegiat, cu procedurile corespunzătoare de gestionare și cu amenințările existente, rămânând în același timp capabilă să protejeze împotriva riscurilor emergente. OIAC continuă să se confrunte în mod constant cu riscuri grave și emergente în legătură cu securitatea cibernetică și reziliența cibernetică. OIAC este ținta unor actori cu înaltă calificare, cu resurse și motivați. Aceștia continuă să atace frecvent confidențialitatea și integritatea activelor de infrastructură și de informații ale OIAC. Pentru a răspunde preocupărilor evidențiate de recentele atacuri cibernetice, de considerațiile politice actuale și de criza provocată de pandemia de COVID-19 și ținând seama de cerințele unice impuse de natura activității OIAC pentru îndeplinirea mandatului CWC, este clar că sunt necesare investiții esențiale în capacitățile tehnice.

În cadrul Fondului special al OIAC pentru securitate cibernetică, continuitatea activității și securitatea infrastructurii fizice, OIAC a conceput Programul său de securitate cibernetică și reziliență și asigurare a informațiilor (programul OIAC) cu 47 de activități de abordare a provocărilor în materie de securitate cibernetică care au fost întâmpinate în ultimii ani. Programul OIAC este aliniat la cele mai bune practici promovate de entități precum Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sau care utilizează concepte legate de Directiva europeană privind securitatea rețelelor și a sistemelor informatice (NIS) referitoare la telecomunicații și apărare. Colectiv, programul OIAC acoperă următoarele domenii tematice: rețele clasificate și neclasificate, politici și guvernanță, depistare și reacție, operațiuni și întreținere și telecomunicații. În esență, programul OIAC este conceput astfel încât să permită OIAC să diminueze oportunitățile pentru atacatorii care dispun de resurse suficiente și/sau sunt sponsorizați de stat pentru a își atinge obiectivele, precum și să atenueze riscurile generate atât de amenințările externe, cât și de cele interne, atât din perspectivă umană, cât și din perspectivă tehnică. Sprijinul din partea Uniunii este structurat sub forma unui proiect care cuprinde trei activități ce corespund a două dintre cele 47 de activități ale programului OIAC.

2. Scopul proiectului

Scopul general al proiectului este de a se asigura capacitatea secretariatului OIAC de a menține un nivel adecvat de securitate cibernetică și reziliență în abordarea provocărilor recurente și emergente în materie de apărare cibernetică la sediul și la instalațiile auxiliare ale OIAC, pentru a permite îndeplinirea mandatului OIAC și punerea în aplicare eficace a CWC.

3. Obiective

— Modernizarea infrastructurii TIC în conformitate cu cadrul instituțional de continuitate a activității al OIAC, cu un accent puternic pe reziliență;

— Asigurarea guvernanței accesului privilegiat, precum și gestionarea și separarea informațiilor fizice, logice și criptografice pentru toate rețelele strategice și ale misiunilor.

4. Rezultate

Rezultatele preconizate la care contribuie proiectul sunt următoarele:

— Echipamentele și serviciile TIC asigură o fiabilitate solidă a sistemului (redundanță hibridă/geografică) și facilitează o mai mare disponibilitate a sistemelor și serviciilor TIC în sprijinul continuității activității;

— Reducerea la minimum a capacităților oricărui factor sau persoană de a avea un impact negativ asupra confidențialității și integrității informațiilor sau sistemelor din cadrul OIAC.

5. Activități

5.1. Activitatea 1 – Operaționalizarea unui mediu propice pentru eforturile în curs de derulare în materie de securitate cibernetică și reziliență în cadrul operațiunilor OIAC cu mai multe amplasamente

Această activitate urmărește să asigure un mediu propice pentru desfășurarea fără probleme a planificării continuității activității OIAC referitor la securitatea și reziliența cibernetică. Acest lucru se va realiza prin abordarea modernizării infrastructurii – rearhitectura și/sau arhivarea pentru continuitatea activității OIAC în cadrul operațiunilor cu amplasamente multiple, precum și prin facilitarea și permiterea în continuare a integrării guvernanței accesului privilegiat în procesele de planificare a continuității activității și de răspuns.

5.2. Activitatea 2 – Elaborarea unei soluții personalizate pentru integrarea și configurarea sistemelor de la fața locului și de tip cloud cu sistemele TIC ale OIAC și cu soluțiile de gestionare privilegiată a accesului

Această activitate se axează pe transpunerea mediului favorabil într-o concepție personalizată pentru integrarea și configurarea sistemelor de la fața locului și de tip cloud cu sistemele TIC ale OIAC și cu soluțiile de gestionare privilegiată a accesului. Se preconizează că acest lucru va spori eficiența infrastructurii sistemelor TIC și va conduce la proiectarea unui sistem integrat de gestionare privilegiată a accesului pentru activele critice, care să poată descuraja și detecta amenințările și care să fie aliniat la capabilități corespunzătoare de depistare a amenințărilor.

5.3. Activitatea 3 – Inițierea și testarea soluțiilor de gestionare privilegiată a accesului

Această activitate se bazează pe infrastructura implementată și pe soluțiile de gestionare privilegiată a accesului concepute pentru a trece integrarea și configurarea de la teorie la practică. Sistemele trebuie cartografiate, profilate și integrate în sistemele existente, luând în considerare factorii de politică și umani asociați. În continuare, testarea aprofundată verifică și asigură robustețea sistemului (toate sistemele noi dispun de o autentificare solidă pentru utilizatori și dispozitive, o clasificare și o protecție adecvată a informațiilor, precum și un sistem avansat de prevenire a pierderilor de date) în momentul implementării, iar, de-a lungul timpului, va permite secretariatului OIAC să identifice și să abordeze lacunele în măsura în care este posibil.

6. Durată

Se preconizează că durata totală estimată a implementării, finanțate prin intermediul acestui proiect va fi de 24 de luni și se va încheia în acest interval.

7. Beneficiari

Beneficiarii proiectului vor fi personalul Secretariatului tehnic al OIAC, organele de elaborare a politicilor, organismele subsidiare și părțile interesate din cadrul CWC, inclusiv statele părți.

8. Vizibilitatea UE

OIAC ia toate măsurile corespunzătoare, în cadrul unor considerente de securitate rezonabile, pentru a face cunoscut faptul că acest proiect a fost finanțat de Uniune.