La sicurezza informatica dell'UE

EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges

TOPIC ID: DDIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE
Ente finanziatore: Commissione europea, Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi: Le proposte devono riguardare almeno uno dei seguenti obiettivi:
1. Rafforzare la capacità degli attori della sicurezza informatica nell'Unione di monitorare gli attacchi e le minacce informatiche e i rischi della catena di approvvigionamento, di reagire congiuntamente contro gli incidenti di grandi dimensioni e di migliorare le conoscenze, le competenze e la formazione pertinenti. Questo obiettivo sarà perseguito attraverso l'attuazione del Piano, considerando l'importante ruolo della rete dei Computer Security Incident Response Teams (CSIRTs) e della Cyber Crisis Liaison Organization Network (CyCLONe).
2. Creare, interconnettere e rafforzare le gamme di sicurezza informatica a livello europeo, nazionale e regionale, nonché all'interno e tra le infrastrutture critiche, compresi, ma non solo, i settori coperti dalla direttiva NIS3 , al fine di condividere le conoscenze e le informazioni sulle minacce alla sicurezza informatica tra le parti interessate negli Stati membri, monitorare meglio le minacce alla sicurezza informatica e rispondere congiuntamente agli attacchi informatici. Ambito di applicazione

Le proposte che riguardano il primo obiettivo dovrebbero rafforzare la capacità degli attori della sicurezza informatica di reagire in modo coordinato agli incidenti di sicurezza informatica su larga scala, promuovendo il ruolo dei CSIRT, della rete CyCLONe e prendendo in considerazione il piano d'azione. Tali proposte dovrebbero ad esempio mirare a fornire alle parti interessate metodologie di test strutturate, database di vulnerabilità e strumenti forensi, o la distribuzione automatizzata di contenuti.

Le proposte relative al secondo obiettivo dovrebbero sostenere la creazione, il funzionamento, l'aumento della capacità e/o l'adozione di gamme di cybersicurezza, nonché promuovere la creazione di reti tra di esse al fine di sviluppare le competenze e l'esperienza in materia di cybersicurezza nelle tecnologie chiave (ad esempio, 5G, Internet degli oggetti, cloud, intelligenza artificiale, sistemi di controllo industriale) e nei settori applicativi (ad esempio, sanità, energia, finanza, trasporti, telecomunicazioni, produzione agroalimentare, gestione delle risorse), tenendo conto anche degli effetti a cascata tra i settori.

Tali proposte devono raggiungere almeno uno dei seguenti obiettivi:
- Scambiare le conoscenze tra le gamme di cybersicurezza e creare archivi di dati comuni.
- Sostenere scenari su larga scala e intersettoriali che coprano un'ampia gamma di avversari e strategie di attacco, compresi ad esempio esercizi di serious gaming intersettoriali; consentire simulazioni realistiche del traffico che riflettano le condizioni della rete.
- Sostenere la formazione strutturata e le esercitazioni di cybersecurity per preparare i difensori

della cybersecurity presso organizzazioni pubbliche e private a migliorare la protezione e la resilienza delle infrastrutture critiche, delle imprese e delle reti di comunicazione;
-Consentire lo svolgimento di formazioni ibride che coinvolgano tutti i livelli rilevanti per l'individuazione, l'attenuazione e la prevenzione degli attacchi informatici (tattici, operativi, strategici), creando al contempo un ambiente in cui allenare la comunicazione, il coordinamento e il processo decisionale.

Criteri di eleggibilità: Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati) - essere stabiliti in uno dei Paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) per tutti i temi
- Paesi SEE (Norvegia, Islanda, Liechtenstein) per tutti i temi.
I beneficiari e gli enti affiliati devono registrarsi nel Registro dei partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation).
Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine.
Si ricorda che tutti i temi di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese che non sia un Paese ammissibile. Tutti i soggetti dovranno compilare e presentare una dichiarazione sulla proprietà e sul controllo.
Inoltre:
- la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata a soggetti provenienti da Paesi ammissibili
- le attività del progetto (incluso il lavoro in subappalto) devono svolgersi in Paesi ammissibili (si veda la sezione localizzazione geografica qui sotto e la sezione 10)
- l'Accordo di sovvenzione può prevedere restrizioni sui DPI

Contributo finanziario: Condizioni specifiche del tema
- Per questo tema si applicano le restrizioni di sicurezza di cui all'articolo 12, paragrafo 5, del regolamento sul programma Europa digitale
- Per questo tema si applica la seguente opzione di rimborso per i costi delle attrezzature: ammortamento e costo totale per le attrezzature elencate
- Per questo tema è consentito il sostegno finanziario a terzi
- Le seguenti parti dei criteri di aggiudicazione di cui alla sezione 9 non sono eccezionalmente applicabili per questo tema:
- misura in cui il progetto rafforzerebbe e renderebbe sicura la catena di approvvigionamento di tecnologia digitale nell'Unione
- misura in cui la proposta può superare gli ostacoli finanziari come la mancanza di finanziamenti di mercato
- misura in cui la proposta affronta la sostenibilità ambientale e gli obiettivi del Green Deal europeo,

in termini di effetti diretti e/o di consapevolezza degli effetti ambientali

Bilancio tematico DIGITAL-ECCC-2022- CYBER-03-CYBER RESILIENCE : 15.000.000 EUR
I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno stabiliti nella Convenzione di sovvenzione
Budget del progetto (importo massimo della sovvenzione): - per il tema DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE: tra 1 e 4 milioni di euro per progetto.

Tipo di azione e tasso di finanziamento
Azioni di sostegno alle PMI - tasso di finanziamento del 50% e del 75% (per le PMI)

Scadenza: 24 gennaio 2023 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)