Potenziamento della rete NCC
Enhancing the NCC Network

TOPIC ID:
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Ente finanziatore:
Commissione europea
Programma
Programma Europa digitale (DIGITAL)
CALL
Rafforzamento dell'ecosistema della cibersicurezza (DIGITAL-ECCC-2025-DEPLOY-CYBER-08)

Obiettivi ed impatto attesi:
I centri nazionali di coordinamento (NCC) istituiti dal regolamento (UE) 2021/887 sono concepiti per lavorare insieme attraverso una rete e per contribuire al conseguimento degli obiettivi del regolamento e per promuovere la comunità delle competenze in materia di cibersicurezza in ciascuno Stato membro, contribuendo all'acquisizione delle capacità necessarie. I centri nazionali di coordinamento possono inoltre sostenere settori prioritari quali l'attuazione della legislazione dell'UE (direttiva (UE) 2022/2555, la proposta di legge sulla cyber resilienza e il regolamento sulla cibersicurezza).
L'obiettivo di questo tema è sostenere il funzionamento dei NCC e consentire loro di sostenere la comunità della cibersicurezza, comprese le PMI, per l'adozione e la diffusione di soluzioni di cibersicurezza all'avanguardia e rafforzare le capacità di cibersicurezza. Ciò potrebbe essere conseguito anche utilizzando il sostegno finanziario a terzi. Sulla base dei finanziamenti ricevuti negli anni precedenti e delle diverse date di inizio delle operazioni negli Stati membri, questa attività mira a continuare a fornire sostegno ai NCC.
A questo proposito, è importante sottolineare che i singoli NCC possono scegliere dall'elenco delle attività e dei deliverable inclusi in questo argomento a seconda del loro interesse e del loro mandato. Non vi è alcun obbligo per gli NCC di eseguire tutte le azioni.
La tematica riguarda anche la fornitura di sostegno all'adozione di tecnologie e prodotti dell'UE in materia di cibersicurezza, alla commercializzazione e all'espansione dell'ecosistema europeo delle start-up/PMI in materia di cibersicurezza, in collaborazione e complementarità con le iniziative europee e nazionali e regionali in corso, come i programmi di accelerazione e incubazione e i programmi di trasferimento tecnologico. Tale strategia dovrebbe includere anche il sostegno alle scale-up, considerando il ricorso agli appalti pubblici e agli investimenti privati.
Un aspetto essenziale di questa azione consiste nel creare un quadro per l'emergere di tali incubatori e acceleratori negli Stati membri, sulla base delle migliori pratiche e tenendo conto delle esigenze e dei requisiti specifici derivanti dalla legislazione dell'UE (come la legge sulla cyber resilienza, la direttiva NIS 2).
Inoltre, questo argomento potrebbe contribuire alla consapevolezza della sicurezza informatica. Sta diventando sempre più importante informare ed educare i cittadini dell'UE sui temi della cibersicurezza

nell'uso quotidiano delle tecnologie digitali. La consapevolezza della sicurezza informatica aiuta gli individui e le organizzazioni a identificare le minacce e ad adottare le misure appropriate. Promuovendo la consapevolezza, è possibile ridurre la probabilità di incidenti e violazioni dei dati. Nell'ambito di questo tema, i NCC sono incoraggiati a basarsi sulle iniziative in corso, tra cui ad esempio quelle della CE e dell'ENISA, per migliorare la consapevolezza dei cittadini, delle imprese e delle organizzazioni dell'UE in merito ai rischi e alle minacce alla cibersicurezza e a sostenere azioni a livello europeo per aumentare il numero di studenti che frequentano corsi di cibersicurezza, studenti impegnati in attività di ricerca sulla cibersicurezza e studenti e giovani professionisti che scelgono una carriera nel campo della cibersicurezza. Inoltre, le imprese europee sono innovative e sviluppano prodotti altamente competitivi, ma il mercato unico digitale, ancora poco sviluppato, confina la maggior parte di queste imprese (in particolare le PMI e le start-up) nel loro paese d'origine. Una piattaforma in grado di aprire il mercato europeo alle piccole e medie imprese fungerebbe anche da trampolino di lancio verso i mercati internazionali. Questa piattaforma garantirà la competitività delle soluzioni europee di cibersicurezza. In quanto tale, questo argomento potrebbe anche sostenere la crescita del mercato dell'UE nei prodotti e nei servizi di cibersicurezza fornendo una piattaforma su cui le PMI e le start-up europee possono pubblicare i loro prodotti e soluzioni (pronti per il mercato) e su cui le imprese, le autorità pubbliche e i privati possono cercare la soluzione migliore per le loro esigenze, indipendentemente dal paese.
1 Per l'utilizzo degli FSTP, il GB predisporrà una procedura dedicata prima del lancio del bando.
Portata:
Il centro nazionale di coordinamento dovrebbe svolgere, a seconda della sua decisione, uno o più dei seguenti compiti:

- fungere da punti di contatto a livello nazionale per la comunità delle competenze in materia di cibersicurezza al fine di sostenere l'ECCC nel raggiungimento dei suoi obiettivi e delle sue missioni.
- Fornire competenze e contribuire attivamente ai compiti strategici dell'ECCC, tenendo conto delle sfide nazionali e regionali pertinenti per la cibersicurezza in diversi settori, e svolgere compiti a sostegno dell'attuazione della Cyber skills Academy.
- Promuovere, incoraggiare e agevolare la partecipazione della società civile e dell'industria, in particolare delle start-up e delle PMI, delle comunità accademiche e di ricerca e di altri attori a livello di Stati membri, ai progetti transfrontalieri e alle azioni di cibersicurezza finanziati attraverso tutti i pertinenti programmi dell'Unione.
- Fornire assistenza tecnica alle parti interessate, supportandole nella fase di candidatura per i progetti gestiti dall'ECCC, nel pieno rispetto delle norme di sana gestione finanziaria, in particolare per quanto riguarda i conflitti di interesse. Ciò dovrebbe avvenire in stretto coordinamento con i pertinenti PCN istituiti dagli Stati membri.
- Cercare di stabilire sinergie con le attività pertinenti a livello nazionale, regionale e locale, ad esempio affrontando la questione della cibersicurezza nelle politiche nazionali in materia di ricerca, sviluppo e innovazione nell'ambito delle politiche indicate nelle strategie nazionali per la cibersicurezza. Se del caso, attuare azioni specifiche per le quali l'ECCC ha concesso sovvenzioni, anche attraverso la fornitura di sostegno finanziario a terzi conformemente all'articolo 204 del regolamento finanziario alle condizioni specificate nelle convenzioni di sovvenzione in questione, in particolare volte a rafforzare l'adozione e la

diffusione di soluzioni all'avanguardia in materia di cibersicurezza (in particolare da parte delle PMI).

- Sostenere l'espansione delle start-up trovando altri finanziamenti per implementare i progetti esistenti.
- Promuovere e diffondere i risultati pertinenti del lavoro della Rete e dell'ECCC a livello nazionale, regionale o locale.
- valutare le richieste di adesione alla comunità delle competenze in materia di cibersicurezza da parte di soggetti stabiliti nello stesso Stato membro dell'NCC.
- sostenere e promuovere il coinvolgimento dei soggetti pertinenti nelle attività derivanti dall'ECCC, dalla rete dei centri nazionali di coordinamento e dalla comunità delle competenze in materia di cibersicurezza e monitorare, se del caso, il livello di coinvolgimento con le azioni aggiudicate per la ricerca, lo sviluppo e la diffusione della cibersicurezza.
- Sostenere la registrazione della Cybersecurity Competence Community (su piattaforme come ATLAS) e contribuire allo sviluppo di strumenti di gestione della community adeguati.

Inoltre, questa azione mira a promuovere comportamenti digitali più sicuri, a far crescere i talenti e ad attirare un maggior numero di giovani verso le carriere nel campo della sicurezza informatica; i NCC potrebbero inoltre, a seconda del contesto nazionale, svolgere uno o più dei seguenti compiti:

- Fornire sostegno alle idee innovative verso la preparazione al mercato.
- Promuovere la consapevolezza, le migliori pratiche e le carriere in materia di cibersicurezza nelle scuole, nelle università e negli eventi comunitari (ad esempio lanciando un programma paneuropeo in cui i giovani saranno formati come ambasciatori per promuovere la sicurezza informatica).
- Rafforzare la collaborazione tra gli istituti di istruzione superiore, ad esempio organizzando eventi in comune, insegnando agli studenti e collaborando alla ricerca all'avanguardia. Sostenere le attività nei livelli di istruzione primaria e secondaria per aumentare la consapevolezza e l'igiene della sicurezza informatica, attraverso la formazione degli insegnanti e degli educatori.
- Costruisci partnership più solide con PMI affermate, aziende tecnologiche e agenzie governative per sviluppare e distribuire strumenti e servizi software che assistono nel rilevamento precoce delle minacce, nell'identificazione degli attori e nel monitoraggio dell'evoluzione delle minacce. Queste collaborazioni possono garantire che i professionisti della sicurezza informatica abbiano accesso agli strumenti e alle tecnologie più recenti per una gestione efficace delle minacce.
- In collaborazione con altri soggetti, se necessario, organizzare periodicamente boot camp, sfide, campagne di sensibilizzazione e corsi di formazione in materia di cibersicurezza in tutta Europa, in particolare per le PMI o gli studenti (ad esempio, concentrandosi sul fornire ai partecipanti competenze pratiche per gestire le minacce informatiche prevalenti attraverso sessioni di formazione, workshop e attività di simulazione su misura per il loro settore). Organizzare campagne periodiche di sensibilizzazione, a livello nazionale e regionale, per aumentare la consapevolezza e l'igiene della sicurezza informatica rivolte a diverse fasce demografiche. Organizzare esercitazioni informatiche nazionali e regionali per migliorare la sicurezza e la resilienza dei settori critici e delle PMI.
- Promuovi una community di professionisti della sicurezza informatica in grado di condividere le loro esperienze, sfide e soluzioni.
- Sostenere e incoraggiare l'adozione degli obiettivi delle politiche educative in materia di cibersicurezza nelle strategie nazionali (di cibersicurezza).

- Promuovere comportamenti digitali più sicuri e un maggior numero di giovani che prendono in considerazione una carriera nel campo della sicurezza informatica.

Criteri di eleggibilità:
Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:
− essere persone giuridiche (enti pubblici o privati)
− essere stabiliti in uno dei paesi ammissibili, ovvero:
− Stati membri dell'UE (compresi i paesi e territori d'oltremare (PTOM)) − paesi SEE (Norvegia, Islanda, Liechtenstein)

I beneficiari e le entità affiliate devono registrarsi nel registro dei partecipanti — prima di presentare la proposta — e dovranno essere convalidati dal servizio centrale di convalida (REA Convalida). Per la convalida, verrà richiesto di caricare documenti che dimostrino lo status legale e l'origine. Altri soggetti possono partecipare ad altri ruoli del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13).
Si prega di notare tuttavia che tutti gli argomenti di questo bando sono soggetti a restrizioni per motivi di sicurezza; pertanto, le entità non devono essere controllate direttamente o indirettamente da un paese che non è un paese ammissibile. Tutti i soggetti dovranno compilare e presentare una dichiarazione sulla proprietà e il controllo.

Inoltre:
− la partecipazione a qualsiasi titolo (in qualità di beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata a entità stabilite e controllate da paesi ammissibili
− le attività del progetto (compreso il lavoro in subappalto) devono svolgersi in paesi ammissibili (cfr. sezione Ubicazione geografica e sezione 10)
− la Convenzione di sovvenzione può prevedere restrizioni in materia di diritti di proprietà intellettuale (cfr. sezione 10).

Contributo finanziario:
Il bilancio stimato disponibile per le chiamate è di 10 000 000 EUR.

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno fissati nella Convenzione di sovvenzione (Scheda tecnica, punto 3 e art 5).
Budget del progetto (importo del contributo richiesto):: indicativamente tra i 3 e i 4 milioni di euro per progetto ma non sono esclusi altri importi, se debitamente giustificati. La sovvenzione concessa può essere inferiore all'importo richiesto. Il budget minimo per ogni argomento, come elencato sopra, è fortemente raccomandato.

Dopo la firma della sovvenzione, di norma si riceve un prefinanziamento per iniziare a lavorare al progetto (flottante di norma pari all'80% dell'importo massimo della sovvenzione; eccezionalmente un

prefinanziamento inferiore o nullo). Il prefinanziamento sarà versato 30 giorni dopo l'entrata in vigore/10 giorni prima della data di inizio/garanzia finanziaria (se richiesta), se posteriore. Sono previsti uno o più pagamenti intermedi (con rendicontazione dei costi attraverso il report sull'utilizzo delle risorse).

Scadenza:
07 ottobre 2025 17:00:00 ora di Bruxelles

Ulteriori informazioni:
Bando di concorso DIGITAL-ECCC-2025-DEPLOY-CYBER-08 - bando | Centro e rete europei di competenza sulla cibersicurezza