Europeo - Digital Europe - EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges

Beneficiari

Per essere ammissibili, i beneficiari e gli enti associati devono:

- essere soggetti giuridici;
- essere stabiliti in un paese ammissibile:
  - paesi membri UE;
  - paesi appartenenti all’area economica europea.

Non ci sono restrizioni riguardanti la composizione del consorzio.

Interventi

I risultati attesi saranno una forte capacità degli Stati membri di reagire in modo coordinato a incidenti di cybersecurity su larga scala, nonché gamme di cybersecurity di alto livello che offrano competenze avanzate, conoscenze e piattaforme di prova.

L'implementazione di questo tema ha due obiettivi principali:

- rafforzare la capacità degli attori della cybersecurity nell'Unione di monitorare gli attacchi e le minacce informatiche e i rischi della catena di approvvigionamento, reagire congiuntamente ai grandi incidenti e migliorare le conoscenze, le competenze e la formazione pertinenti. Questo obiettivo sarà perseguito attraverso l'attuazione del Blueprint e della futura Joint Cyber Unit considerando l'importante ruolo della rete Computer Security Incident Response Teams (CSIRT) e della Cyber Crisis Liaison Organization Network (CyCLONe);
- creare, interconnettere e rafforzare gli ambiti di cybersecurity a livello europeo, nazionale e regionale, nonché all'interno e tra le infrastrutture critiche, compresi, ma non solo, i settori coperti dalla direttiva NIS, al fine di condividere le conoscenze e l'intelligence sulle minacce alla cybersecurity tra le parti interessate nel settore Stati membri, monitorare meglio le minacce alla cybersecurity e rispondere congiuntamente agli attacchi informatici.

Scopo:

- le proposte che affrontano il primo obiettivo dovrebbero sviluppare la capacità degli attori della cybersecurity di reagire in modo coordinato agli incidenti di cybersecurity su larga scala, promuovendo nel contempo il ruolo dei CSIRT, della rete CyCLONe, della futura unità comune per la cybersecurity e tenendo conto del piano;
- Le proposte relative al secondo obiettivo dovrebbero sostenere la creazione, il funzionamento, l'aumento della capacità e/o l'adozione di gamme di sicurezza informatica, nonché promuovere il collegamento in rete tra di esse al fine di sviluppare competenze e competenze in materia di sicurezza informatica nelle tecnologie chiave (ad esempio 5G, Internet degli oggetti, cloud, Intelligenza artificiale, sistemi di controllo industriale) nonché settori di applicazione (ad esempio sanità, energia, finanza, trasporti, telecomunicazioni, produzione agroalimentare, gestione delle risorse), compresa la considerazione degli effetti a cascata tra i settori. Questa azione mirerà a:
  - scambiare conoscenza tra gli ambiti della sicurezza informatica e creare archivi di dati comuni;
  - sostenere scenari su larga scala e intersettoriali che coprano un'ampia gamma di avversari e strategie di attacco, comprese ad esempio esercitazioni di gioco serio

tra centri; consentire simulazioni realistiche del traffico che riflettano le condizioni della rete;

- sostenere la formazione strutturata e gli esercizi di cybersecurity per preparare i difensori della cybersecurity presso le 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 coinvolgendo tutti i livelli rilevanti per rilevare, mitigare e prevenire gli attacchi informatici (tattici, operativi, strategici) creando al contempo un ambiente in cui possono addestrare la comunicazione, il coordinamento e il processo decisionale;
- fornire servizi aggiuntivi agli stakeholder come metodologie di esame strutturate, database delle vulnerabilità e strumenti forensi, sviluppare opzioni di invio di contenuti che supportino specifici profili lavorativi.

Agevolazione

Dotazione Finanziaria: Euro 15.000.000,00.

Tipologia di progetto: DIGITAL-JU-SME DIGITAL JU SME Support Actions. Il finanziamento massimo per progetto sarà fra gli **Euro 1.000.000,00** e **Euro 4.000.000,00**.

Fonte

Bando

Scadenza

15-02-2023

Link

Informazioni