Sostegno all'attuazione della legislazione UE sulla cybersecurity e delle strategie nazionali di cybersecurity

Support for implementation of EU legislation on cybersecurity and national cybersecurity strategies

TOPIC ID: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION

Ente finanziatore: Commissione europea, Programma Digital Europe

Obiettivi ed impatto attesi: L'azione si concentra sullo sviluppo delle capacità e sul rafforzamento della cooperazione in materia di cibersicurezza a livello tecnico, operativo e strategico, nel contesto della legislazione UE esistente e proposta in materia di cibersicurezza, in particolare la direttiva NIS2 (direttiva (UE) 2022/2555), la legge sulla cibersicurezza e la proposta di legge sulla resilienza informatica, nonché la direttiva sugli attacchi contro i sistemi informativi (direttiva 2013/40). Il progetto integra il lavoro dei SOC nell'area del rilevamento delle minacce. Si tratta di una continuazione del lavoro attualmente sostenuto nell'ambito del precedente WP.

Inoltre, l'azione mira anche a migliorare la preparazione dell'industria e del mercato ai requisiti di cybersecurity stabiliti nella proposta di regolamento sui requisiti di cybersecurity per i prodotti con elementi digitali, nota come Cyber Resilience Act, rafforzando le norme di cybersecurity per garantire prodotti hardware e software più sicuri.

Le proposte devono contribuire al raggiungimento di almeno uno di questi obiettivi;

- Sviluppo della fiducia tra gli Stati membri.
- Efficace cooperazione operativa delle organizzazioni incaricate della sicurezza informatica a livello nazionale dell'UE o degli Stati membri, in particolare la cooperazione dei CSIRT (anche in relazione alla rete CSIRT) o la cooperazione degli operatori dei servizi essenziali, comprese le autorità pubbliche.
- Migliori processi e mezzi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali nell'UE.
- Migliore segnalazione degli attacchi informatici alle autorità di polizia, in linea con la direttiva sugli attacchi ai sistemi informativi.
- Maggiore sicurezza delle reti e dei sistemi informativi nell'UE.
- Maggiore allineamento delle implementazioni degli Stati membri della NIS2 (Direttiva (UE) 2022/2555).
- Supporto alla certificazione della cybersecurity in linea con la legge sulla cybersecurity.

Ambito di applicazione:
L'azione si concentrerà sul sostegno di almeno una delle seguenti priorità:

- Implementazione, convalida, sperimentazione e diffusione di tecnologie, strumenti e soluzioni basate sull'IT, processi e metodi per il monitoraggio e la gestione degli incidenti di cybersecurity.
- Collaborazione, comunicazione, attività di sensibilizzazione, scambio di conoscenze e formazione,

anche attraverso l'uso di gamme di cybersicurezza, di organizzazioni pubbliche e private che lavorano all'attuazione della NIS2 (Direttiva (UE) 2022/2555).
- Schemi di gemellaggio che coinvolgano organizzazioni originatrici e adottanti di almeno due Stati membri diversi per facilitare la diffusione e l'adozione di tecnologie, strumenti, processi e metodi per un'efficace collaborazione transfrontaliera per prevenire, rilevare e contrastare gli incidenti di cibersicurezza.
- Misure di rafforzamento della solidità e della resilienza nell'area della cybersecurity che rafforzino la capacità dei fornitori di lavorare sistematicamente con le informazioni rilevanti per la cybersecurity o di fornire dati utilizzabili ai CSIRT.
- Garantire che i produttori migliorino la sicurezza dei prodotti con elementi digitali sin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita.
- Garantire un quadro coerente di cybersecurity, che faciliti la conformità dei produttori di hardware e software.
- Migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali.
- Consentire alle aziende di tutti i settori e ai consumatori di utilizzare in modo sicuro i prodotti con elementi digitali.
- Sostegno alla certificazione di sicurezza informatica, compreso il supporto alle autorità nazionali per la sicurezza informatica e ad altre parti interessate, come le PMI.
- Il sostegno sarà rivolto alle autorità competenti degli Stati membri, che svolgono un ruolo centrale nell'attuazione della NIS2 (Direttiva (UE) 2022/2555), nonché ad altri attori che rientrano nell'ambito di applicazione della direttiva.

L'azione può sostenere, tra l'altro, la continuazione del tipo di attività di cybersecurity finanziate attraverso il programma CEF Telecom, basandosi, se del caso, sui risultati dei progetti CEF.

Verrà fornito un sostegno, tra l'altro, per l'accesso alle piattaforme di servizi di base per la sicurezza informatica del CEF da parte di organizzazioni pubbliche e private che lavorano all'attuazione della NIS2 (direttiva (UE) 2022/2555) e che sono potenziali utenti delle piattaforme di servizi di base per la sicurezza informatica del CEF.

L'azione sostiene inoltre l'industria, con particolare attenzione alle start-up e alle PMI, a cogliere le opportunità industriali e di mercato offerte dalla proposta di legge sulla resilienza informatica e dalla legge sulla sicurezza informatica.

Criteri di eleggibilità: Le domande saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del tema per cui sono state presentate. Partecipanti ammissibili (Paesi ammissibili)
Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati) - avere sede 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. Altre entità possono partecipare in altri ruoli del consorzio, come partner associati, subappaltatori, terze parti che forniscono contributi in natura, ecc.
Questo bando è soggetto 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 partecipanti 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 entità provenienti da Paesi ammissibili
- le attività del progetto (incluso il lavoro in subappalto) devono svolgersi in Paesi ammissibili
- l'Accordo di sovvenzione può prevedere restrizioni sui Diritto di proprietà intellettuale

Targeted stakeholders
Questo argomento si rivolge alle parti interessate del settore industriale, comprese le PMI e le start-up che rientrano nell'ambito di applicazione del prossimo CRA, interessate dalla direttiva NIS2 o che possono beneficiare dei sistemi europei di certificazione della sicurezza informatica. Si riferisce anche alle autorità competenti degli Stati membri, che svolgono un ruolo centrale nell'attuazione della direttiva NIS2, ai Computer Security Incident Response Teams (CSIRT), compresi i CSIRT settoriali, ai Security Operation Centres (SOC), agli Operatori di Servizi Essenziali (OES), ai fornitori di servizi digitali (DSP), agli Information Sharing and Analysis Centres- ISAC, attori che svolgono un ruolo nell'implementazione del Cyber Resilience Act (compresi gli enti di certificazione), e qualsiasi altro attore che rientri nell'ambito delle legislazioni sopra citate La composizione di consorzi multipaese non è obbligatoria per questo tema, ma contribuirà positivamente all'impatto dell'azione.
Durata
La durata indicativa dell'azione è fino a 36 mesi, ma non sono escluse altri periodi di implementazione del progetto .

Contributo finanziario: Il budget disponibile per la call è di 30 milioni di euro
Il budget massimo richiedibile è tra 1 milione e 5 milioni di euro per ogni proposta progettuale
Tipo di azione e tasso di finanziamento
Sovvenzioni semplici - Tasso di finanziamento del 50%.

Scadenza: 26 September 2023 17:00:00 Brussels time

Ulteriori informazioni:
call-fiche_digital-eccc-2023-deploy-cyber-04_en.pdf (europa.eu)