Supporto all'attuazione della legislazione dell'UE sulla sicurezza informatica e delle strategie nazionali di sicurezza informatica (2024)

Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

TOPIC ID:
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02

Ente finanziatore:
Commissione europea
Programma Dogital Europe

Obiettivi ed impatto attesi:
L'azione si concentra sullo sviluppo delle capacità e sul rafforzamento della cooperazione sulla sicurezza informatica a livello tecnico, operativo e strategico, nel contesto della legislazione UE vigente e proposta sulla sicurezza informatica, in particolare la direttiva NIS2 (direttiva (UE) 2022/2555), il Cybersecurity Act e la direttiva sugli attacchi contro i sistemi di informazione (direttiva 2013/40). Integra il lavoro dei SOC nell'area del rilevamento delle minacce. È una continuazione del lavoro attualmente supportato nell'ambito del precedente Digital Work Programme.
Inoltre, questa azione mira anche a sostenere l'attuazione del proposto Cyber Resilience Act (CRA) da parte delle autorità di vigilanza del mercato/autorità di notifica/organismi nazionali di accreditamento, aumentando le loro capacità di garantire un'attuazione efficace del CRA.
Le proposte devono contribuire al raggiungimento di almeno uno di questi obiettivi:

- Sviluppo della fiducia tra gli Stati membri.
- Supportare le autorità di vigilanza del mercato/autorità di notifica/organismi nazionali di accreditamento nell'implementazione del CRA.
- Efficace cooperazione operativa tra le 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 di servizi essenziali, comprese le autorità pubbliche.
- Migliori processi e mezzi di sicurezza e notifica per le entità essenziali e importanti nell'UE, compresi sistemi di notifica (automatizzata) degli incidenti transfrontalieri.
- Migliorare la segnalazione degli attacchi informatici alle autorità preposte all'applicazione della legge, in linea con la direttiva sugli attacchi contro i sistemi di informazione.
- Miglioramento della sicurezza delle reti e dei sistemi informativi nell'UE.
- Maggiore allineamento delle implementazioni NIS2 da parte degli Stati membri (direttiva (UE) 2022/2555).
- Supportare la certificazione della sicurezza informatica in linea con il Cybersecurity Act.

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

- Implementazione, convalida, sperimentazione e distribuzione di tecnologie, strumenti e soluzioni, processi e metodi basati sull'IT per il monitoraggio e la gestione degli incidenti di sicurezza

informatica.

- Aumentare la capacità delle autorità di vigilanza del mercato/autorità di notifica/organismi nazionali di accreditamento in vista dei compiti previsti dalla CRA.
- Collaborazione, comunicazione, attività di sensibilizzazione, scambio di conoscenze e formazione, anche mediante l'uso di strumenti di sicurezza informatica, di organizzazioni pubbliche e private che lavorano all'attuazione della NIS2 (direttiva (UE) 2022/2555).
- Programmi di gemellaggio che coinvolgono organizzazioni ideatrici e adottanti di almeno 2 diversi Stati membri per agevolare l'implementazione e l'adozione di tecnologie, strumenti, processi e metodi per un'efficace collaborazione transfrontaliera volta a prevenire, rilevare e contrastare gli incidenti di sicurezza informatica.
- Misure volte a rafforzare la robustezza e la resilienza nell'ambito della sicurezza informatica che rafforzino la capacità dei fornitori di lavorare sistematicamente con informazioni rilevanti in materia di sicurezza informatica o di fornire dati fruibili ai CSIRT.
- Garantire che i produttori migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita.
- Garantire un quadro coerente di sicurezza informatica, facilitando la conformità per i 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 prodotti con elementi digitali.
- Supporto alla certificazione della sicurezza informatica, incluso il supporto alle autorità nazionali di certificazione della sicurezza informatica e ad altri stakeholder rilevanti, come le PMI. Ciò include attività come test di penetrazione basati sulle minacce, acquisizione di banchi di prova per la certificazione, condivisione di best practice, implementazione di metodi di valutazione innovativi per prodotti o componenti ICT specifici.

Le proposte possono essere rivolte, ove opportuno, alle autorità competenti degli Stati membri che svolgono un ruolo centrale nell'attuazione della direttiva NIS2 (direttiva (UE) 2022/2555), nonché ad altri attori che rientrano nell'ambito di applicazione della presente direttiva.

Le proposte possono sostenere, tra le altre cose, la prosecuzione delle attività di sicurezza informatica finanziate attraverso il programma CEF Telecom, basandosi, ove pertinente, sui risultati dei progetti CEF.

Le proposte possono supportare, tra le altre cose, l'integrazione nelle piattaforme di servizi di base per la sicurezza informatica del CEF di organizzazioni pubbliche e private che lavorano all'implementazione di NIS2 (direttiva (UE) 2022/2555) e possono contribuire potenzialmente al raggiungimento degli obiettivi della piattaforma di servizi di base per la sicurezza informatica del CEF.

Questa azione mira a supportare la posizione europea in materia di sicurezza informatica creando un ecosistema europeo di aziende e organizzazioni che supporterà l'attuazione della legislazione UE in materia di sicurezza informatica che contribuirà a rafforzare le capacità europee nella protezione del cyberspazio. I risultati del lavoro svolto nei progetti finanziati nell'ambito di questa azione possono includere l'implementazione, la convalida, la sperimentazione e l'implementazione di tecnologie, strumenti e soluzioni basate sull'IT, processi e metodi per il monitoraggio e la gestione degli incidenti di sicurezza informatica che coinvolgono la sicurezza informatica dei fornitori di servizi essenziali e infrastrutture

critiche, nonché di altri attori. Come precedentemente osservato, la partecipazione di entità non UE comporta il rischio che informazioni altamente sensibili su infrastrutture, rischi e incidenti di sicurezza siano soggette a legislazione o pressione che obbliga tali entità non UE a divulgare tali informazioni a governi non UE, con un rischio per la sicurezza imprevedibile. Pertanto, sulla base delle ragioni di sicurezza delineate, le azioni relative a queste tecnologie sono soggette all'articolo 12(5) del regolamento (UE) 2021/694, in coerenza con WP 2021/2022.

Questo argomento è rivolto a stakeholder industriali rilevanti, tra cui PMI e start-up nell'ambito del prossimo CRA, interessati dalla direttiva NIS2 o che potrebbero beneficiare degli schemi di certificazione della sicurezza informatica europea. Si riferisce anche alle autorità competenti degli Stati membri, che svolgono un ruolo centrale nell'attuazione della direttiva NIS2, ai Computer Security Incident Response Team (CSIRT), tra cui CSIRT settoriali, Security Operation Centre (SOC), Operators of Essential Services (OES), Digital Service Provider (DSP), Information Sharing and Analysis Centres (ISAC), attori che svolgono un ruolo nell'attuazione del Cyber Resilience Act (inclusi gli organismi di certificazione) e qualsiasi altro attore nell'ambito delle legislazioni sopra menzionate.

Criteri di eleggibilità:
Per essere ammissibili, i richiedenti (beneficiari e soggetti affiliati) devono: − essere persone giuridiche (enti pubblici o privati)

− essere stabilito in uno dei paesi ammissibili, vale a dire:
− 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 di convalida centrale (REA Validation).

Per la convalida, verrà richiesto loro di caricare documenti che dimostrino lo stato legale e l'origine. Si prega di notare che tutti gli argomenti di questo bando sono soggetti a restrizioni dovute alla sicurezza, pertanto le entità non devono essere direttamente o indirettamente controllate da un paese che non sia un paese ammissibile. Tutte le entità dovranno compilare e presentare una dichiarazione di proprietà e controllo. Inoltre: − la partecipazione in qualsiasi veste (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità stabilite e controllate da paesi ammissibili − le attività del progetto (incluso il lavoro subappaltato) devono svolgersi in paesi ammissibili − il Grant Agreement può prevedere restrizioni IPR

Contributo finanziario:
Tipologia di azione e tasso di finanziamento Sovvenzioni semplici — tasso di finanziamento del 50%

Il budget totale disponibile per il tema DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Supporto all'implementazione della legislazione dell'UE sulla sicurezza informatica e delle strategie nazionali di sicurezza informatica (2024) è di 20.000.000 di EURO

Scadenza:
27 marzo 2025 17:00:00 ora di Bruxelles

Ulteriori informazioni:
Bando di proposte "Azioni di implementazione nell'area della sicurezza informatica" (DIGITAL-ECCC-2024-DEPLOY-CYBER-07)