Supporto alla preparazione e assistenza reciproca, mirato a operazioni e installazioni industriali più grandi

Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

TOPIC ID:
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Ente finanziatore:
Commissione europea

Obiettivi ed impatto attesi:
Risultato atteso:

- servizi di supporto alla preparazione
- Servizi di valutazione delle minacce e dei rischi
- servizi di monitoraggio del rischio

Obiettivo:
Questo meccanismo mira a integrare e non duplicare gli sforzi degli Stati membri e quelli a livello dell'Unione per aumentare il livello di protezione e resilienza alle minacce informatiche, in particolare per i grandi impianti e infrastrutture industriali, assistendo gli Stati membri nei loro sforzi per migliorare la preparazione alle minacce e agli incidenti informatici, fornendo loro conoscenze e competenze.
Ambito di applicazione:
La fornitura di servizi di supporto alla preparazione (ex-ante) comprende le attività elencate di seguito, rivolte ad esempio a grandi impianti o infrastrutture industriali, operatori di servizi essenziali, fornitori di servizi digitali ed enti governativi:
Supporto per la verifica di potenziali vulnerabilità:

- Sviluppo di scenari di test di penetrazione. Gli scenari proposti possono riguardare reti, applicazioni, soluzioni di virtualizzazione, soluzioni cloud, sistemi di controllo industriale e IoT.
- Supporto per la conduzione di test di enti essenziali che gestiscono infrastrutture critiche per individuare potenziali vulnerabilità.
- Sostenere la diffusione di strumenti e infrastrutture digitali a supporto dell'esecuzione di scenari di test e per la conduzione di esercitazioni, come lo sviluppo di cyber-ranges standardizzati o altre strutture di test, in grado di imitare le caratteristiche dei settori critici (ad esempio, settore energetico, settore dei trasporti, ecc.) per facilitare l'esecuzione di esercitazioni informatiche, in particolare nell'ambito di scenari transfrontalieri, se pertinenti.
- Valutazione e/o test delle capacità di sicurezza informatica degli Stati Uniti (comprese le capacità di prevenire, rilevare e rispondere agli incidenti).
- Servizi di consulenza, che forniscono raccomandazioni su come migliorare la sicurezza e le capacità dell'infrastruttura.

Supporto per la valutazione delle minacce e dei rischi:

- Implementazione e ciclo di vita del processo di valutazione delle minacce

- Analisi personalizzata degli scenari di rischio.

Servizio di monitoraggio dei rischi:

- Monitoraggio specifico del rischio continuo, come il monitoraggio della superficie di attacco, il monitoraggio del rischio degli asset e delle vulnerabilità.

Le azioni di preparazione dovrebbero andare a beneficio delle entità (comprese le PMI e le start-up) nei settori indicati come settori di infrastrutture critiche nella NIS2 (Direttiva (UE) 2022/2555), come l'energia, i trasporti e le banche, e delle entità in altri settori pertinenti.
Questa azione mira alla creazione di piattaforme che fungano da punto di riferimento e forniscano servizi quali test di penetrazione e valutazioni delle minacce per i fornitori di servizi essenziali e infrastrutture critiche, nonché per altri attori. Si tratta di dati e misure operative sulla sicurezza informatica, compresi i test di penetrazione e le vulnerabilità sfruttabili. Tali informazioni potrebbero essere sfruttate da attori malintenzionati e quindi devono essere protette da possibili dipendenze e vulnerabilità nella sicurezza informatica per prevenire l'influenza e il controllo stranieri. Come già osservato in precedenza, la partecipazione di entità non appartenenti all'UE comporta il rischio che informazioni altamente sensibili sulle infrastrutture di sicurezza, sui rischi e sugli incidenti siano soggette a una legislazione o a pressioni che obbligano tali entità non appartenenti all'UE a divulgare tali informazioni a governi non appartenenti all'UE, con un rischio imprevedibile per la sicurezza. Pertanto, sulla base delle ragioni di sicurezza esposte, le azioni relative a queste tecnologie sono soggette all'articolo 12, paragrafo 5, del Regolamento (UE) 2021/694, in coerenza con il WP 2021/2022.

Criteri di eleggibilità:
Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati)
- essere stabilito in uno dei paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) - Paesi SEE (Norvegia, Islanda, Liechtenstein) I beneficiari e le entità affiliate devono iscriversi al Registro dei partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà richiesto 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.
Tutte le entità 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 stabilite e controllate da Paesi ammissibili
- le attività del progetto (incluso il lavoro in subappalto) devono svolgersi in Paesi ammissibili (si veda la sezione localizzazione geografica e la sezione 10) - la Convenzione di sovvenzione può prevedere restrizioni sui diritti di proprietà intellettuale (si veda la sezione 10).
Questo tema si rivolge in particolare agli operatori industriali, alle autorità nazionali per la cybersecurity, ai centri nazionali di competenza in materia di cybersecurity, ai centri nazionali di coordinamento (come definiti nel Regolamento (UE) 2021/887), agli enti privati e a qualsiasi altro soggetto interessato in grado

di aggregare la domanda dei beneficiari finali, di lanciare gare d'appalto nello spazio di mercato della cybersecurity e di gestire bandi a valle per l'assegnazione del sostegno finanziario a terzi. La presentazione di proposte da parte di consorzi, pur non essendo obbligatoria, contribuirà positivamente all'impatto dell'azione.

Contributo finanziario:
Sovvenzioni per il sostegno finanziario - tasso di finanziamento del 100%.
Budget del progetto: indicativamente tra i 3 e i 5 milioni di euro per progetto, ma non sono esclusi altri importi.

Scadenza:
21 gennaio 2025 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-eccc-2024-deploy-cyber-07_en.pdf (europa.eu)