Prove coordinate di prontezza e altre azioni di preparazione
Coordinated preparedness testing and other preparedness actions

TOPIC ID:
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP

Ente finanziatore:
Commissione europea
Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi:
Risultato atteso:
I tipi di risultati attesi sono presentati in due parti.

La prima parte riguarda:

- Miglioramento della cooperazione, della preparazione e della resilienza in materia di sicurezza informatica nell'UE; servizi di supporto alla preparazione.
- Servizi di valutazione delle minacce e dei rischi.

La seconda parte riguarda:

Servizi di monitoraggio dei rischi.

- Migliore conformità, divulgazione coordinata delle vulnerabilità e monitoraggio.
- Miglioramento delle competenze, tramite esercitazioni e corsi di formazione, organizzazione di eventi, workshop, consultazioni delle parti interessate e libri bianchi.

Obiettivi:
Nell'ambito del programma di lavoro 2025-2027 dell'ECCC, questo argomento copre due azioni del Cyber Solidarity Act, dedicate al meccanismo di emergenza per la sicurezza informatica, vale a dire (1) test coordinati di preparazione delle entità che operano in settori ad alta criticità in tutta l'Unione e (2) altre azioni di preparazione per le entità che operano in settori ad alta criticità e in altri settori critici.

Si prega di notare che (1) i test coordinati di preparazione delle entità che operano in settori ad alta criticità in tutta l'Unione sono soggetti all'attuale invito a presentare proposte, mentre (2) altre azioni di preparazione saranno coperte solo dagli inviti a presentare proposte del 2026 e del 2027.

Per maggiori dettagli sull'azione (1) oggetto del presente invito a presentare proposte, si prega di consultare il documento dell'invito.

Queste azioni mirano a integrare e non a duplicare gli sforzi compiuti dagli Stati membri e a livello dell'Unione per aumentare il livello di protezione e resilienza alle minacce informatiche, in particolare per gli impianti e le infrastrutture industriali critici, assistendo gli Stati membri nei loro sforzi volti a migliorare la loro preparazione alle minacce e agli incidenti informatici, fornendo loro conoscenze e competenze.

Le proposte dovrebbero contribuire al raggiungimento di almeno uno dei seguenti obiettivi:

- (parte 1) Test coordinati di preparazione delle entità che operano in settori ad alta criticità in tutta l'Unione (compresi test di penetrazione e valutazione delle minacce) che prendono in considerazione le TIC e le tecnologie operative/i sistemi di controllo industriale.
- (parte 2) Altre azioni di preparazione per le entità che operano in settori ad alta criticità e in altri settori critici (ad esempio monitoraggio delle vulnerabilità, esercitazioni e corsi di formazione).

Ambito di applicazione:
[Parte 1 Test coordinati di preparazione]

La fornitura di servizi di supporto alla preparazione comprende le attività elencate di seguito, per le entità del settore o sottosettore identificate dalla Commissione in conformità con la legge sulla solidarietà informatica, tra i settori ad alta criticità elencati nell'allegato I della direttiva (UE) 2022/2555 e specificati nel documento di invito a presentare proposte per ciascuno degli inviti nell'ambito di questo argomento:

Supporto per i test sulle 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.
- Sostegno alla realizzazione di test di potenziali vulnerabilità per entità essenziali che gestiscono infrastrutture critiche.
- Sostegno alla diffusione di strumenti e infrastrutture digitali a supporto dell'esecuzione di scenari di test e alla realizzazione di esercitazioni quali lo sviluppo di cyber-range standardizzati o altre strutture di test, in grado di riprodurre le caratteristiche dei settori critici (ad esempio il settore energetico, il settore dei trasporti, ecc.) o di altri settori interessati dalla NIS 2 per facilitare l'esecuzione di esercitazioni informatiche, in particolare in scenari transfrontalieri, se del caso.
- Valutazione e/o test delle capacità di sicurezza informatica delle entità e dei settori degli Stati membri (comprese le capacità di prevenire, individuare e rispondere agli incidenti e gli stress test dell'intero settore), attività di valutazione e conformità volte ad aumentare la maturità, ad esempio sulla base di modelli di maturità consolidati e/o di schemi di valutazione e conformità pertinenti.
- Valutazione e/o test delle capacità di sicurezza informatica delle entità interessate (compresa la valutazione e la gestione dei rischi relativi alla catena di approvvigionamento).
- Servizi di consulenza, che forniscono raccomandazioni su come migliorare la sicurezza e le capacità delle infrastrutture.

Sostegno alla valutazione delle minacce e dei rischi, ad esempio:

- Attuazione del processo di valutazione delle minacce e ciclo di vita
- Analisi personalizzata degli scenari di rischio.
- Il sostegno sarà destinato alle autorità competenti degli Stati membri, che svolgono un ruolo centrale nell'attuazione della direttiva NIS 2, quali i gruppi di risposta agli incidenti informatici (CSIRT) e le autorità nazionali per la sicurezza informatica.

[Parte 2 altre azioni di preparazione]

Per la seconda parte, oltre ai servizi già elencati nella Parte 1 (supporto per il test delle potenziali vulnerabilità e supporto per la valutazione delle minacce e la gestione dei rischi), la

fornitura dei servizi di supporto alla preparazione indicati di seguito si rivolge alle entità che operano in settori altamente critici e in altri settori critici di cui agli allegati I e II della direttiva NIS 2.

Supporto per la valutazione delle minacce e dei rischi:

- Gestione dei rischi della catena di approvvigionamento nell'ambito dei servizi di valutazione dei rischi.
- Servizio di monitoraggio dei rischi:

- Monitoraggio continuo specifico dei rischi, come il monitoraggio della superficie di attacco, il monitoraggio dei rischi delle risorse e delle vulnerabilità.

Supporto alla divulgazione e alla gestione coordinata delle vulnerabilità:

- Promuovere l'adozione delle politiche nazionali in materia di divulgazione delle vulnerabilità (CVD)1 e della banca dati dell'UE sulle vulnerabilità.
- Coordinare la divulgazione delle vulnerabilità e la diffusione tempestiva delle patch di sicurezza. Standardizzazione delle modalità di condivisione delle informazioni tra i diversi soggetti interessati nel processo di gestione delle vulnerabilità.
- Applicazioni CVD che gestiscono più fonti di informazioni sulle vulnerabilità utilizzando standard o tecnologie aperte. (ad esempio ricercatori, fornitori, CSIRT)
- Sensibilizzazione sull'adozione delle migliori pratiche di gestione delle vulnerabilità.

Esercizi e corsi di formazione dedicati:

Sviluppare programmi di formazione e workshop completi, anche a livello internazionale, per i professionisti della sicurezza informatica che copriranno le ultime tendenze in materia di minacce informatiche, metodologie di attacco e migliori pratiche per la gestione e la prevenzione delle minacce. Verifiche di maturità, valutazione delle capacità di sicurezza informatica.

Incoraggiare lo sviluppo di attività di apprendimento continuo in materia di sicurezza informatica per stare al passo con tutti i requisiti di sicurezza informatica previsti dalle normative e dalle direttive dell'UE in materia di sicurezza informatica, tra cui la direttiva NIS 2, CSA, CSoA, DORA, EECC, GDPR, CRA.
Il sostegno sarà destinato alle autorità competenti degli Stati membri, che svolgono un ruolo centrale nell'attuazione della direttiva NIS 2, squadre di risposta agli incidenti informatici (CSIRT), comprese le CSIRT settoriali, centri operativi di sicurezza (SOC)/hub informatici, settori altamente critici e altri settori critici, parti interessate del settore (compresi i centri di condivisione e analisi delle informazioni - ISAC) e qualsiasi altro attore che rientri nell'ambito di applicazione della direttiva NIS 2, DORA, CSA, ecc.

Il sostegno potrà essere fornito, tra l'altro, per l'adesione alle piattaforme di servizi fondamentali per la sicurezza informatica del CEF da parte di organizzazioni pubbliche e private che stanno lavorando all'attuazione della direttiva NIS 2 e sono potenziali utenti delle piattaforme di servizi fondamentali per la sicurezza informatica del CEF.

L'azione può anche sostenere l'industria, con particolare attenzione alle start-up e alle PMI, affinché colgano le opportunità industriali e di mercato create dal Cyber Resilience Act e può sostenere l'attuazione della direttiva NIS 2.

Criteri di eleggibilità:
Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde in tutto (o almeno in parte) alla descrizione dell'argomento per il quale sono state presentate. Partecipanti ammissibili (paesi beneficiari potenziali) 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 Validazione (REA Validation). 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 sul 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. la sezione Ubicazione geografica di seguito e la sezione 10)

− la Convenzione di sovvenzione può prevedere restrizioni in materia di diritti di proprietà intellettuale

Contributo finanziario:
Il budget stimato disponibile per la call è di € 10.000.000

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

− per il tema DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP: circa 1,5 milioni di euro per progetto, ma non sono esclusi altri importi, se debitamente giustificati.

La sovvenzione concessa può essere inferiore all'importo richiesto. La sovvenzione consisterà in una sovvenzione per i costi effettivi misti basata sul budget (costi effettivi, con elementi di costo unitario e a tasso forfettario). Ciò significa che rimborserà SOLO alcuni tipi di costi (costi ammissibili) e costi che sono stati effettivamente sostenuti per il tuo progetto (NON i costi preventivati). Per i costi unitari e i tassi forfettari, è possibile addebitare gli importi calcolati come spiegato nella convenzione di sovvenzione (cfr. articolo 6 e allegati 2 e 2a). I costi saranno rimborsati al tasso di finanziamento fissato nella convenzione di sovvenzione. Questa percentuale dipende dal tipo di azione che si applica al tema (cfr. sezione 2). Le sovvenzioni NON possono produrre un profitto (ossia un'eccedenza di entrate + sovvenzione dell'UE rispetto ai costi). Le organizzazioni a scopo di lucro devono dichiarare i loro ricavi e, se c'è un profitto, lo detrarremo dall'importo finale della sovvenzione (vedi art 22.3). Inoltre, si prega di notare che l'importo finale della sovvenzione può essere ridotto in caso di mancato rispetto della convenzione di sovvenzione

Scadenza:
31 Marzo 2026

Ulteriori informazioni:
Call for proposals: DIGITAL-ECCC-2025-DEPLOY-CYBER-09 | European Cybersecurity Competence Centre and Network