

Test coordinati di preparazione e altre azioni di preparazione

Coordinated preparedness testing and other preparedness actions

TOPIC ID:

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP

Ente finanziatore:

Commissione europea
Programma Europa Digitale

Obiettivi ed impatto attesi:

La presente azione comprende due tipologie di intervento previste dal Cyber Solidarity Act, nell'ambito del Cybersecurity Emergency Mechanism, a sostegno degli Stati membri:

1. test coordinati di preparazione degli enti operanti in settori ad alta criticità nell'Unione, selezionati preventivamente ai sensi dell'articolo 12, paragrafo 4, del Cyber Solidarity Act;
2. altre azioni di preparazione rivolte agli enti operanti in settori ad alta criticità e in altri settori critici, ai sensi dell'articolo 13 del Cyber Solidarity Act.

Obiettivi

Le azioni mirano a integrare, senza duplicarli, gli interventi degli Stati membri e quelli realizzati a livello dell'Unione per aumentare il livello di protezione e resilienza rispetto alle minacce informatiche, in particolare per gli impianti e le infrastrutture industriali critiche. L'obiettivo è sostenere gli Stati membri nel miglioramento della preparazione alle minacce e agli incidenti informatici, mettendo a loro disposizione conoscenze e competenze specialistiche.

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

- Parte 1 – Test coordinati di preparazione: test coordinati degli enti operanti in settori ad alta criticità nell'Unione, selezionati ai sensi dell'articolo 12, paragrafo 4, del Cyber Solidarity Act, compresi penetration testing e valutazione delle minacce, considerando sia le ICT sia le Operational Technology/ Industrial Control Systems (OT/ICS).
- Parte 2 – Altre azioni di preparazione: azioni di preparazione rivolte agli enti operanti in settori ad alta criticità e in altri settori critici, comprese attività di monitoraggio delle vulnerabilità, esercitazioni e corsi di formazione.

Ambito di applicazione

Parte 1 – Test coordinati di preparazione

Ai sensi dell'articolo 12, paragrafo 4, del Cyber Solidarity Act, la Commissione ha individuato tre settori ammissibili al sostegno agli Stati membri mediante sovvenzioni per lo svolgimento di test coordinati di preparazione:

1. settore energetico, in particolare il sottosettore dell'energia elettrica;
2. settore dei trasporti, in particolare i sottosettori ferroviario e del trasporto per vie d'acqua (porti);
3. settore della pubblica amministrazione.

Le proposte presentate dagli Stati membri nell'ambito della Parte 1 devono fare riferimento a uno scenario di rischio elaborato dal NIS Cooperation Group ai fini della presente call (baseline, medium, high). La proposta deve includere almeno lo scenario di rischio baseline, corrispondente a un basso livello di stress. Gli scenari elaborati per ciascun settore sono riportati nell'Allegato 3.

Il sostegno ai test sulle potenziali vulnerabilità comprende, in particolare:

- sviluppo di penetration testing sulla base degli scenari dell'Allegato 3;
- test delle vulnerabilità degli enti essenziali che gestiscono infrastrutture critiche;
- implementazione di strumenti e infrastrutture digitali per l'esecuzione di scenari di test ed esercitazioni, compresi cyber-range standardizzati o altre strutture di test in grado di riprodurre le caratteristiche dei settori critici;
- valutazione e test delle capacità di cibersecurity degli enti e dei settori degli Stati membri, comprese le capacità di prevenire, rilevare e rispondere agli incidenti e gli stress test di interi settori;
- valutazione e test delle capacità di cibersecurity, anche con riferimento alla valutazione e gestione dei rischi della supply chain;
- servizi di consulenza e raccomandazioni finalizzati al miglioramento della sicurezza delle infrastrutture e delle relative capacità sulla base degli scenari di rischio eseguiti.

Sono inoltre previste attività di valutazione delle minacce e dei rischi, comprese l'implementazione e la gestione del ciclo di vita dei processi di Threat Assessment e l'analisi di scenari di rischio personalizzati.

Il sostegno è rivolto alle autorità competenti degli Stati membri che svolgono un ruolo centrale nell'attuazione della NIS 2 Directive, quali i CSIRTs e le autorità nazionali di cibersecurity.

Parte 2 – Altre azioni di preparazione

La Parte 2 riguarda gli enti operanti nei settori ad alta criticità e negli altri settori critici indicati negli Allegati I e II della NIS 2 Directive che non rientrano nei settori selezionati per i test coordinati di preparazione ai sensi dell'articolo 12 del Cyber Solidarity Act.

Oltre alle attività previste dalla Parte 1, il sostegno comprende:

- gestione dei rischi della supply chain nell'ambito dei servizi di valutazione del rischio;
- servizi di monitoraggio continuo dei rischi, compresi il monitoraggio della superficie di attacco, degli asset e delle vulnerabilità;
- sostegno alla Coordinated Vulnerability Disclosure (CVD) e alla gestione delle vulnerabilità, promuovendo l'adozione delle politiche nazionali CVD e dell'EU Vulnerability Database;
- coordinamento della divulgazione delle vulnerabilità e della tempestiva distribuzione delle patch di sicurezza;

- standardizzazione delle modalità di condivisione delle informazioni tra gli stakeholder coinvolti nella gestione delle vulnerabilità;
- applicazioni CVD per la gestione di diverse fonti di informazioni sulle vulnerabilità mediante standard o tecnologie aperte;
- sensibilizzazione sull'adozione delle migliori pratiche per la gestione delle vulnerabilità;
- esercitazioni dedicate, programmi di formazione e workshop, anche internazionali, rivolti ai professionisti della cibersecurity;
- attività di formazione continua in materia di cibersecurity per garantire l'adeguamento ai requisiti derivanti dalla normativa UE, comprese NIS 2 Directive, CSA, CSoA, DORA, EECC, GDPR e CRA.

Il sostegno mira a integrare le attività delle autorità nazionali competenti degli Stati membri, dei CSIRTs, compresi i CSIRTs nazionali settoriali, e dei SOC/Cyber Hubs nazionali.

Articolazione delle azioni

Il topic COORDPREP comprende pertanto due categorie di azioni nell'ambito del Cybersecurity Emergency Mechanism:

- Parte 1: test coordinati di preparazione degli enti operanti nei settori ad alta criticità nell'Unione, ai sensi dell'articolo 12, paragrafo 4, del Cyber Solidarity Act;
- Parte 2: altre azioni di preparazione per gli enti operanti nei settori ad alta criticità e negli altri settori critici, ai sensi dell'articolo 13 del Cyber Solidarity Act.

I test coordinati di preparazione devono essere condotti utilizzando scenari di rischio e metodologie comuni sviluppati dal NIS Cooperation Group, in cooperazione con la Commissione, l'EEAS, l'ENISA e, nell'ambito del proprio mandato, l'EU-CyCLONe.

Criteri di eleggibilità:

Ammissibilità delle candidature

Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del topic per il quale sono presentate.

Partecipanti ammissibili (Paesi ammissibili)

Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:

- essere entità giuridiche (organismi pubblici o privati);
- essere stabiliti 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 Participant Register — prima della presentazione della proposta — e dovranno essere convalidati dal Central Validation Service (REA Validation). Ai fini della convalida, sarà loro richiesto di caricare documenti attestanti lo status giuridico e l'origine.

Altre entità possono partecipare ricoprendo altri ruoli all'interno del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13).

Si tenga presente che tutti i topic del presente invito sono soggetti a restrizioni per motivi di sicurezza; pertanto, le entità non devono essere direttamente o indirettamente controllate da un Paese che non sia un Paese ammissibile. Tutte le entità¹⁷ dovranno compilare e presentare una dichiarazione relativa alla proprietà e al 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 alle entità stabilite e controllate da Paesi ammissibili;
- le attività del progetto (compresi i lavori subappaltati) devono svolgersi nei Paesi ammissibili (cfr. la sezione relativa alla localizzazione geografica di seguito e la sezione 10);
- il Grant Agreement può prevedere restrizioni in materia di diritti di proprietà intellettuale (IPR) (cfr. sezione 10).

Contributo finanziario:

Budget disponibile 15.000.000 EUR

Forma della sovvenzione, tasso di finanziamento e importo massimo della sovvenzione

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi ammissibili totali, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Grant Agreement) (Scheda dati, punto 3 e articolo 5).

Budget del progetto (importo della sovvenzione richiesta)

Importo della sovvenzione richiesta

Il contributo UE richiesto dovrebbe essere pari a 1,5 milioni di EUR per progetto. Tuttavia, potranno essere prese in considerazione anche proposte che richiedano importi diversi, purché ciò sia debitamente giustificato.

La sovvenzione concessa potrà essere inferiore all'importo richiesto.

Forma della sovvenzione e costi ammissibili

La sovvenzione assumerà la forma di una sovvenzione basata sul budget a costi effettivi misti (budget-based mixed actual cost grant: costi effettivi, con elementi basati su costi unitari e tassi forfettari).

Ciò significa che saranno rimborsate ESCLUSIVAMENTE determinate tipologie di costi (costi ammissibili) e i costi effettivamente sostenuti per il progetto (NON i costi preventivati).

Per i costi unitari e i tassi forfettari, potranno essere imputati gli importi calcolati secondo le modalità indicate nella Convenzione di sovvenzione (cfr. articolo 6 e Allegati 2 e 2a).

Tipologia di azione e tasso di finanziamento

Sovvenzioni semplici (Simple Grants) — tasso di finanziamento del 50%.

Divieto di profitto

Le sovvenzioni NON possono generare un profitto, vale a dire un'eccedenza dei ricavi + sovvenzione UE rispetto ai costi.

Le organizzazioni a scopo di lucro devono dichiarare i propri ricavi e, qualora si realizzi un profitto, questo sarà dedotto dall'importo finale della sovvenzione (cfr. articolo 22.3).

Riduzione dell'importo finale della sovvenzione

Si tenga inoltre presente che l'importo finale della sovvenzione potrà essere ridotto in caso di mancato rispetto della Convenzione di sovvenzione, ad esempio in caso di attuazione non corretta, violazione degli obblighi, ecc.

Scadenza:

14 Gennaio 2027 17:00:00 Brussels time

Ulteriori informazioni:

[8e1d6074-95ed-4b23-8bd3-2ca42b096411_en](#)