Adozione di soluzioni innovative di cibersicurezza per le PMI

Uptake of innovative cybersecurity solutions for SMEs

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

Ente finanziatore:
Commissione europea
Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi:

L'azione mira a migliorare la preparazione industriale e di mercato alle esigenze di sicurezza informatica delle PMI, come specificato nella pertinente legislazione dell'UE in materia di sicurezza informatica, ad esempio nella legge sulla resilienza informatica che garantisce prodotti hardware e software più sicuri.

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

- Disponibilità di strumenti e servizi innovativi che aiutino le PMI a conformarsi alla legislazione dell'UE in materia di sicurezza informatica.
- Disponibilità di strumenti e servizi innovativi che aiutino le PMI a segnalare gli incidenti e, se possibile, ad assistere nel ripristino, nonché a comunicare con le autorità competenti (ad esempio, cooperazione con i cyber hub, i CSIRT (anche in relazione alla rete CSIRT) e/o gli ISAC, ad esempio per le entità dei settori altamente critici e di altri settori critici).
- Miglioramento dei processi e dei mezzi di sicurezza e notifica nell'UE.
- Miglioramento della sicurezza delle reti e dei sistemi informativi nell'UE.
- Preparazione dell'industria e del mercato alla proposta di legge sulla resilienza informatica.
- Sostegno alla certificazione della sicurezza informatica in linea con la legge sulla sicurezza informatica.
- Sostegno ai partner della catena di approvvigionamento nelle autovalutazioni e nelle certificazioni standardizzate. Aiutare i partner a valle della catena di approvvigionamento in un approccio graduale per aumentare la resilienza informatica.
- Superamento della sfida di trovare le competenze tecniche necessarie per affrontare un panorama tecnologico complesso che si basa fortemente su configurazioni e capacità estese.
- Cyber toolkit come servizio a supporto delle PMI1 nella gestione dei rischi informatici, nella definizione e nell'attuazione della loro strategia di sicurezza informatica, comprese diverse funzioni dedicate alla valutazione dei rischi, all'individuazione delle vulnerabilità e delle minacce, ecc.
- Capacità di supporto e di risposta agli incidenti per le PMI.

Risultati attesi:
Lo sviluppo di un toolkit informatico come servizio a supporto delle PMI nella gestione dei rischi informatici, nella definizione e nell'attuazione della loro strategia di sicurezza informatica. Il toolkit potrebbe includere almeno uno dei seguenti elementi:

- Interfacce che si collegheranno alle applicazioni SaaS esistenti, quali sistemi di gestione delle risorse umane, della fatturazione e della contabilità, CRM e contabilità, ecc., spesso utilizzati dalle PMI per aumentare la loro sicurezza informatica.
- Una funzionalità che consenta la mappatura e la manutenzione delle risorse digitali di una PMI e delle possibili vulnerabilità, interfacciandosi con altre applicazioni SaaS che gestiscono un inventario delle risorse e archivi di dati.
- Una funzione che supporti la valutazione e la gestione dei rischi di sicurezza informatica di una PMI e la gestione dei rischi della catena di approvvigionamento. Questa funzione dovrebbe eseguire una valutazione dei rischi, fornire raccomandazioni per la mitigazione dei rischi e identificare le opzioni.
- Un'interfaccia con gli strumenti esistenti che supportano l'analisi e la valutazione dell'entità del rischio informatico di una PMI sulla base delle informazioni raccolte dalla scansione dell'infrastruttura digitale e dei dati forniti dagli utenti autorizzati.
- Una funzione che emette avvisi sulle vulnerabilità e sulle minacce sulla base delle informazioni raccolte dalla funzione di gestione dei rischi.
- Una funzione che collega le PMI a un CSIRT o a un Cyber Hub per segnalare un incidente e assistere nel ripristino, se possibile.
- Una mappatura e uno sportello/portale unico per gli strumenti e le soluzioni esistenti destinati al supporto della sicurezza informatica delle PMI.
- Strumenti che supportano il rilevamento, la prevenzione e la risposta nelle infrastrutture di tecnologia operativa utilizzando standard o tecnologie aperte.

Capacità di supporto e risposta agli incidenti per le PMI:

- Hotline non commerciale dedicata alla sicurezza informatica con un quadro normativo standardizzato e linee guida relative ai tempi di risposta, alle procedure di escalation e all'ambito dell'assistenza fornita.
- Una linea di assistenza multilingue pienamente operativa che fornisce assistenza tempestiva e accurata in materia di sicurezza informatica alle PMI, contribuendo a ridurre il numero di truffe informatiche riuscite e a migliorare l'igiene digitale.
- Una piattaforma nazionale di risposta informatica per i primi soccorritori informatici per scambiare le loro esperienze, condividere notizie rilevanti e avviare discussioni sulle sfide e sulle minacce informatiche emergenti a complemento delle strutture esistenti di gestione delle crisi informatiche.
- Moduli di formazione specializzati per i servizi di primo soccorso (pubblici e privati) rivolti a diversi settori quali la sanità, la finanza, l'energia e i trasporti.

Strumenti e piattaforme di supporto:

- Centro di controllo e pannello per la segnalazione degli incidenti e l'invio dei soccorritori.
- Interfaccia utente per le PMI per la segnalazione di incidenti associata al kit di strumenti informatici. Gli utenti possono segnalare un incidente, ottenere istruzioni su come reagire e ottenere informazioni su come ricevere supporto per la risposta. Potrebbe essere incluso anche un assistente AI collegato a un centro di controllo.
- Interfacce con le autorità nazionali e le piattaforme transfrontaliere (CBP) per la notifica degli incidenti e la condivisione delle informazioni.

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 € 15 000 000

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 circa 3 milioni di euro per progetto, ma non sono esclusi altri importi, se debitamente giustificati. Si prevede il finanziamento di circa 5 progetti

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