Azione dedicata al rafforzamento degli ospedali e dei fornitori di assistenza sanitaria

Dedicated action to reinforcing hospitals and healthcare providers

TOPIC ID:
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH

Ente finanziatore:
Commissione europea
Programma
Programma Europa digitale (DIGITAL)
CALL
Rafforzamento dell'ecosistema della cibersicurezza (DIGITAL-ECCC-2025-DEPLOY-CYBER-08)

Obiettivi ed impatto attesi:
Risultato atteso:

- Mappatura delle esigenze comuni di sicurezza informatica degli ospedali e degli operatori sanitari.
- Linee guida per gli operatori sanitari per valutare il loro stato attuale di protezione della sicurezza informatica e le esigenze pertinenti.
- Piani tecnici di cibersicurezza per migliorare la preparazione e la resilienza informatica: migliori capacità di rilevamento e risposta per le istituzioni sanitarie che riducono al minimo l'impatto degli attacchi informatici, in particolare per i ransomware. Questo include anche corsi di formazione dedicati al personale.
- Installazioni dimostrative pilota di sicurezza informatica presso ospedali partner e sedi di fornitori di servizi sanitari per garantire che gli ospedali e gli operatori sanitari possano mantenere la continuità operativa di fronte agli incidenti di sicurezza informatica. Questo dovrebbe essere monitorato attraverso KPI specifici.
- Ampie campagne di divulgazione per contribuire a migliorare la preparazione degli ospedali e dei fornitori di assistenza sanitaria in Europa.

Obiettivo:
Questa azione mira a rafforzare la sicurezza informatica degli ospedali e dei fornitori di servizi sanitari. L'obiettivo è garantire che gli ospedali e i prestatori di servizi sanitari, che sono operatori cruciali nel settore sanitario, siano in grado di rilevare, monitorare e rispondere efficacemente alle minacce informatiche, in particolare ai ransomware, che comportano rischi significativi, rafforzando così la resilienza del sistema sanitario europeo.
L'azione contribuirà al piano d'azione dell'UE sulla cibersicurezza negli ospedali e nell'assistenza sanitaria, adottato dalla Commissione1 nel gennaio 2025.
1 https://commission.europa.eu/cybersecurity-healthcare_en
Portata:

Questa azione risponde alla crescente necessità di monitoraggio continuo della sicurezza informatica, intelligence sulle minacce e risposta agli incidenti negli ospedali e negli operatori sanitari, che spesso non dispongono di risorse di sicurezza informatica dedicate per proteggersi adeguatamente dalle minacce informatiche.
L'azione sosterrà progetti pilota che riuniranno portatori di interessi quali cluster regionali e/o nazionali, associazioni di ospedali e fornitori di servizi sanitari (come sistemi sanitari nazionali, ospedali o associazioni di ospedali, fornitori di servizi sanitari e/o associazioni professionali di operatori sanitari), nonché fornitori di servizi di cibersicurezza.
I progetti pilota definiranno lo stato di preparazione dei cluster di ospedali e fornitori di servizi sanitari nell'Unione europea, per essere in grado di valutare le loro esigenze. Sulla base di questa analisi, prepareranno una panoramica delle soluzioni di cibersicurezza all'avanguardia e delle risorse necessarie (tecnologie, servizi, strumenti, risorse umane, esigenze di formazione, ecc.) agli ospedali e ai fornitori di servizi sanitari per soddisfare l'ambito dell'azione. Questi possono includere, ad esempio: centri operativi di sicurezza che offrono monitoraggio in tempo reale, rilevamento delle minacce e risposta rapida agli incidenti e strumenti avanzati di sicurezza informatica, come piattaforme di gestione delle informazioni e degli eventi di sicurezza (SIEM), intelligence sulle minacce e capacità di risposta automatizzata, tra gli altri.
I progetti pilota svilupperanno piani tecnici, adattati alle esigenze degli ospedali rappresentativi e dei fornitori di assistenza sanitaria (ad esempio ospedali piccoli o grandi, fornitori di assistenza sanitaria privata, ecc.) che dovranno anche includere le migliori raccomandazioni di attuazione e le stime dei costi per un'implementazione efficace.
I progetti pilota condurranno un'attuazione dimostrativa di questi piani tecnici per dimostrarne l'efficacia nelle operazioni presso i siti delle parti interessate, mostrando diversi casi d'uso per diversi gruppi di utenti presso ospedali e fornitori di assistenza sanitaria di piccole, medie e grandi dimensioni, almeno in due diversi Stati membri.
I progetti pilota serviranno come progetti dimostrativi e forniranno anche istruzione e formazione in materia di sicurezza informatica al personale degli ospedali e dei fornitori di assistenza sanitaria partner, aumentando la consapevolezza e garantendo le migliori pratiche nella salvaguardia delle informazioni sanitarie sensibili.
Infine, in collaborazione tra loro, i progetti pilota intraprenderanno un'ampia attività di diffusione delle migliori pratiche in tutta l'UE, con l'obiettivo specifico di contribuire a replicare e ampliare il più possibile le attività dei progetti pilota.
I progetti pilota sosterranno le istituzioni sanitarie che rispettano la direttiva NIS 2.

Criteri di eleggibilità:
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 convalida (REA Convalida).

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 soggetti8 dovranno compilare e presentare una dichiarazione sulla proprietà e il 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. sezione Ubicazione geografica e sezione 10)
− la Convenzione di sovvenzione può prevedere restrizioni in materia di diritti di proprietà intellettuale (cfr. sezione 10).

Contributo finanziario:
Il bilancio stimato disponibile per le chiamate è di 30 000 000 EUR.

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). DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH: indicativamente tra i 3 e i 5 milioni di euro per progetto ma non sono esclusi altri importi, se debitamente giustificati.
La sovvenzione concessa può essere inferiore all'importo richiesto. Il budget minimo per ogni argomento, come elencato sopra, è fortemente raccomandato.

Dopo la firma della sovvenzione, di norma si riceve un prefinanziamento per iniziare a lavorare al progetto (flottante di norma pari all'80% dell'importo massimo della sovvenzione; eccezionalmente un prefinanziamento inferiore o nullo). Il prefinanziamento sarà versato 30 giorni dopo l'entrata in vigore/10 giorni prima della data di inizio/garanzia finanziaria (se richiesta), se posteriore. Sono previsti uno o più pagamenti intermedi (con rendicontazione dei costi attraverso il report sull'utilizzo delle risorse).

Scadenza:
07 ottobre 2025 17:00:00 ora di Bruxelles

Ulteriori informazioni:
Bando di concorso DIGITAL-ECCC-2025-DEPLOY-CYBER-08 - bando | Centro e rete europei di competenza sulla cibersicurezza