



COMMISSIONE EUROPEA

Bruxelles, 15.1.2025
COM(2025) 10 definitivo

**COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL
CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL
COMITATO DELLE REGIONI**

Piano d'azione europeo sulla sicurezza informatica di ospedali e fornitori di servizi sanitari

1. Introduzione

L'ambiente di sicurezza dell'UE sta cambiando rapidamente, con un'escalation di attacchi ibridi e cyberattacchi che mirano a destabilizzare la nostra società, cercando di creare divisioni e disordini, ma anche profitti dalla criminalità informatica. L'Europa deve quindi rafforzare con urgenza la sua preparazione e la sua resilienza nei confronti di questa nuova realtà, in tutti i settori e in linea con un approccio "che coinvolge l'intera società" e "l'intero governo", come richiesto nella relazione del consigliere speciale del Presidente della Commissione europea, Sauli Niinistö.

Sistemi sanitari sicuri e resilienti sono una pietra miliare del modello sociale dell'UE. Tuttavia, gli ospedali e i sistemi sanitari si trovano ad affrontare minacce crescenti, in particolare da parte di bande di ransomware che li prendono di mira per ottenere un guadagno economico, a causa dell'elevato valore dei dati dei pazienti, comprese le cartelle cliniche elettroniche. Negli ultimi quattro il settore sanitario è diventato l'industria più attaccata nell'UE, anche durante la pandemia COVID-19, quando le infrastrutture sanitarie sono state sempre più bersagliate da attacchi informatici. I cyberattacchi agli ospedali e ai fornitori di servizi sanitari stanno causando danni diretti alle persone, ritardando le procedure mediche, causando blocchi nei pronto soccorso e, in casi estremi, potrebbero causare la perdita di vite umane.

La posta in gioco è ancora più alta, in quanto il settore sta subendo una trasformazione digitale fondamentale. La sanità digitale e l'uso e il riutilizzo dei dati sanitari possono consentire modelli di assistenza più adatti alle esigenze e alle preferenze delle persone e dei pazienti, prevenendo l'insorgere della malattia o consentendo un trattamento più precoce. L'integrazione di strumenti e soluzioni digitali nei processi clinici, così come l'uso e il riutilizzo dei dati sanitari, possono informare su decisioni cliniche migliori, contribuire all'automazione nel settore sanitario e a un'assistenza più rapida e migliore ai pazienti. Gli strumenti digitali, l'utilizzo dei dati e i dispositivi medici - spesso connessi a Internet e dotati di intelligenza artificiale (AI) - sono fondamentali anche per affrontare sfide come la carenza di professionisti della sanità.

Allo stesso tempo, gli strumenti digitali ampliano anche i potenziali obiettivi dei criminali informatici. Inoltre, alcuni attori statali non esitano a prendere di mira le strutture sanitarie, come testimonia l'attuale guerra di aggressione della Russia contro l'Ucraina. Questo rende il settore un potenziale obiettivo per i cyberattacchi come parte di una più ampia campagna ibrida. I cyberattacchi non solo mettono a repentaglio la sicurezza dei pazienti, ma erodono anche la fiducia del pubblico nelle infrastrutture sanitarie e comportano costi di recupero significativi. Oltre a difendersi dai cyberattacchi, un'infrastruttura digitale resiliente e sicura è essenziale anche per sostenere l'implementazione e la piena diffusione dello Spazio europeo dei dati sanitari¹ (EHDS).

È quindi giunto il momento di aumentare e rafforzare la sicurezza informatica e la resilienza degli ospedali e dei fornitori di servizi sanitari europei, come sottolineato dalla Presidente von der Leyen nei suoi orientamenti politici per la Commissione 2024-2029². Questo piano d'azione risponde all'urgenza della situazione e alle minacce uniche che il settore deve affrontare. Non esiste una soluzione semplice alle sfide della cybersicurezza nel settore sanitario. Il piano d'azione chiede invece di rafforzare la prevenzione, la preparazione e un approccio più coordinato alla solidarietà, sfruttando al contempo le competenze dell'industria europea della sicurezza informatica. In quanto tale, il piano d'azione riflette l'approccio dell'UE alla sicurezza che sarà ulteriormente sviluppato e formalizzato nella prossima Strategia europea di sicurezza interna, che definisce una risposta globale per affrontare tutte le minacce alla sicurezza interna.

¹ <https://www.consilium.europa.eu/en/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-sciopero-provisorio-deal/>

² https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

e concentrandosi sulla capacità di anticipare le minacce, prevenire i danni e proteggere le persone, agendo a tutti i livelli con un approccio globale alla società.

Il settore sanitario comprende un ampio numero di entità e attori, tra cui ospedali, cliniche, case di cura, centri di riabilitazione e vari fornitori di assistenza sanitaria, oltre all'industria farmaceutica, medica e biotecnologica, ai produttori di dispositivi medici e agli istituti di ricerca sanitaria. Il presente piano d'azione si concentra prevalentemente sulla sicurezza informatica degli ospedali e dei fornitori di assistenza sanitaria, intesi come persone fisiche o giuridiche - o qualsiasi altra entità - che forniscono legalmente assistenza sanitaria sul territorio di uno Stato membro³. Gli ospedali e i fornitori di assistenza sanitaria sono interdipendenti con altri enti sanitari e i più vicini alle persone. Allo stesso tempo, le misure volte a migliorare la cibersecurity degli ospedali e dei fornitori di assistenza sanitaria dovrebbero affrontare anche i rischi che interessano la catena di approvvigionamento e l'ecosistema più ampi, derivanti ad esempio da entità che utilizzano i dati sanitari per la ricerca e l'apprendimento automatico o che producono dispositivi medici, in particolare dispositivi medici abilitati digitalmente che si connettono a Internet o ad altri dispositivi ("Internet delle cose").

Sebbene la sicurezza dei sistemi sanitari sia principalmente di competenza nazionale, la sanità è anche un settore critico ai sensi della direttiva sulle misure per un elevato livello comune di cibersecurity nell'UE (NIS2)⁴. I criminali informatici e altri attori delle minacce operano a livello transfrontaliero e anche le sfide di sicurezza informatica che le organizzazioni sanitarie devono affrontare sono simili nei vari Stati membri. La cooperazione a livello europeo è preziosa per condividere e diffondere le migliori pratiche a livello europeo e nazionale. Pertanto, il piano d'azione propone un coordinamento e misure a livello di UE, invitando al contempo gli Stati membri ad agire per fare la differenza per l'assistenza sanitaria e l'ecosistema sanitario in generale.

Il piano d'azione si concentra sullo sviluppo delle capacità del settore di **prevenire** gli incidenti di cybersecurity in primo luogo, perché prevenire è sempre meglio che curare. In secondo luogo, il Piano d'azione illustra le azioni per migliorare la condivisione delle informazioni sulla sicurezza informatica e la capacità di **rilevare le** minacce informatiche, consentendo una reazione più rapida. In terzo luogo, prevede misure per **rispondere** meglio agli incidenti e per **riprendersi** da essi. Infine, il Piano d'azione prevede modalità per **dissuadere** gli attori delle minacce informatiche dal lanciare attacchi contro i sistemi sanitari in Europa.

Il piano d'azione sarà attuato in collaborazione con i fornitori di servizi sanitari e il più ampio ecosistema sanitario, gli Stati membri e la comunità della sicurezza informatica. Un approccio collaborativo è fondamentale per definire e perfezionare ulteriormente le azioni più incisive, in modo che tutti i fornitori europei di servizi sanitari critici possano beneficiarne. La cooperazione internazionale è importante per la sicurezza informatica a causa della natura senza confini e interconnessa delle minacce informatiche. Minacce simili alla sicurezza informatica sono presenti anche nei Paesi dell'allargamento e del vicinato e in altri Paesi partner strategici dell'UE. Ciò può mettere a repentaglio la sicurezza delle infrastrutture critiche dell'UE. Sarà quindi importante riflettere le lezioni apprese dall'attuazione del Piano d'azione anche in

³ L'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0024>.

⁴ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un elevato livello comune di cibersecurity nell'Unione (direttiva NIS 2), <https://eur-lex.europa.eu/eli/dir/2022/2555>.

la cooperazione dell'UE con i Paesi dell'allargamento e con gli altri Paesi partner, alla luce dei livelli di minaccia a cui sono rispettivamente esposti.

2. La sfida della cybersecurity per gli ospedali e i fornitori di servizi sanitari

Minacce informatiche al settore sanitario

Gli attacchi informatici sono in aumento a livello globale e all'interno dell'UE, con un panorama di minacce sempre più complesso e dinamico. I progressi dell'intelligenza artificiale stanno dotando gli attori criminali e malintenzionati di potenti strumenti per aumentare la precisione e l'impatto delle loro operazioni e, allo stesso tempo, stanno ridisegnando le possibilità di difesa informatica, consentendo un'azione automatizzata e in tempo reale contro gli attacchi.

Il ransomware rimane una sfida critica per la sicurezza informatica nell'UE e a livello globale, con un rapporto che stima un costo annuale globale di oltre 250 miliardi di euro entro il 2031⁵. Quando i criminali del ransomware colpiscono, non solo criptano i dati delle vittime per ottenere un riscatto, ma fanno trapelare sempre più spesso informazioni sensibili per esercitare ulteriore pressione. Un'altra sfida importante è rappresentata dalle vulnerabilità di software e hardware: secondo l'Agenzia dell'Unione europea per la sicurezza informatica (ENISA)⁶, il settore sanitario è quello che ha dichiarato il maggior numero di incidenti di sicurezza legati a tali vulnerabilità.⁷ Altre minacce in crescita sono gli attacchi DDoS (Distributed Denial of Service), progettati per sommergere un sistema mirato con un'ondata di traffico, inaccessibile agli utenti legittimi⁸.

Il settore sanitario si trova ad affrontare tendenze simili in termini di minacce alla sicurezza informatica, con un'enfasi pronunciata sugli attacchi ransomware. Secondo l'ENISA, il ransomware ha rappresentato il 54% degli incidenti di cybersicurezza analizzati nel settore sanitario nel periodo 2021-2023. L'83% degli attacchi aveva una motivazione finanziaria, dovuta all'elevato valore dei dati sanitari, mentre il 10% degli attacchi aveva una motivazione ideologica⁹. Analogamente, un rapporto della Commissione del 2024 ha rilevato che il 71% degli attacchi con effetti sull'assistenza ai pazienti, come ritardi nelle cure e nelle diagnosi e impossibilità di accesso ai servizi di emergenza, erano di tipo ransomware¹⁰. Gli attacchi ransomware possono avere un effetto particolarmente dirompente sulla fornitura di servizi sanitari, mettendo a rischio la sicurezza dei pazienti.

⁵ Cybersecurity Ventures (1 giugno 2024): "I costi globali dei danni da ransomware dovrebbero superare i 265 miliardi di dollari entro il 2031". Disponibile all'indirizzo <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>.

⁶ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione (legge sulla cibersicurezza), <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng>.

⁷ ENISA Threat Landscape: Health Sector (luglio 2023).

⁸ ENISA Threat Landscape 2024.

⁹ ENISA Threat Landscape: Health Sector (luglio 2023). Il rapporto ha analizzato i fornitori di servizi sanitari e altri tipi di organizzazioni, tra cui le organizzazioni che conducono ricerche in ambito sanitario, le entità che producono determinati prodotti sanitari, le autorità sanitarie, le organizzazioni di assicurazione sanitaria, le strutture di trattamento residenziale e i fornitori di servizi sociali. Disponibile su <https://www.enisa.europa.eu/publications/health-threat-landscape>

¹⁰ Commissione europea: Centro comune di ricerca, Reina, V. e Griesinger, C., Cyber security in the health and medicine sector - A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, Publications Office of the EU, 2024, <https://data.europa.eu/doi/10.2760/693487>

Inoltre, gli attacchi ransomware sono spesso associati a violazioni dei dati dei pazienti¹¹, che spesso includono dati sensibili relativi alla salute e violano il diritto fondamentale delle persone alla protezione dei dati personali.

Allo stesso tempo, con la crescente digitalizzazione dell'assistenza sanitaria, la superficie di attacco sta aumentando. Secondo la relazione sullo stato del decennio digitale 2024, in media il 79% dei cittadini dell'UE ha accesso online alle proprie cartelle cliniche elettroniche nell'assistenza primaria¹². Cartelle cliniche elettroniche, sistemi di informazione clinica, sistemi di workflow ospedaliero, sistemi informatici per la gestione dei rimborsi dei trattamenti, sistemi di imaging medico e dispositivi medici utilizzati per scopi diagnostici o per il monitoraggio dei pazienti sono tutti esempi di strumenti digitali che possono svolgere un ruolo importante nell'aumentare l'efficienza e le prestazioni del settore sanitario, ma sono anche potenziali obiettivi di un attacco di cybersecurity. Attività sanitarie specifiche come la terapia intensiva e la radiologia per immagini, o campi medici come l'oncologia e la cardiologia, che dipendono fortemente da dispositivi abilitati digitalmente, sono particolarmente a rischio di attacchi informatici. Inoltre, i problemi della catena di approvvigionamento possono portare all'acquisto di dispositivi con una sicurezza informatica insufficiente, aggravando i rischi generali esistenti.

Ad esempio, durante la pandemia COVID-19, un attacco ransomware ha paralizzato gran parte del sistema sanitario irlandese, portando alla cancellazione di almeno alcuni servizi in 31 dei 54 ospedali per acuti mattina stessa dell'incidente.¹³ I servizi sanitari sono dovuti tornare alle cartelle cliniche cartacee, rallentando l'efficienza delle operazioni. L'attacco ha avuto origine da un'e-mail di phishing contenente un allegato dannoso.¹⁴ L'incidente ha dimostrato la possibilità che i cyberattacchi si diffondano su diversi sistemi e, di conseguenza, l'importanza di proteggere l'intera superficie di attacco di un'organizzazione sanitaria. Ha inoltre sottolineato l'importanza di garantire una fondamentale igiene informatica e una cultura della sicurezza informatica in tutte le organizzazioni.

Maturità della cybersecurity di ospedali e fornitori di servizi sanitari

Il panorama dell'assistenza sanitaria nell'UE è molto diversificato, con ospedali e altri fornitori di assistenza sanitaria che variano notevolmente in termini di proprietà, struttura e dimensioni tra gli Stati membri. In alcuni casi, la governance dell'assistenza sanitaria può basarsi su un approccio centralizzato a livello nazionale, in altri a regionale e locale; i fornitori di assistenza sanitaria possono essere di proprietà pubblica o privata. Inoltre, possono esistere differenze anche all'interno dello stesso Paese, ad esempio in presenza di significative disparità socio-economiche e territoriali tra le regioni, che determinano un quadro complesso. Questo complesso panorama sanitario può essere messo a dura prova da importanti crisi sanitarie, dovute a malattie trasmissibili, come la pandemia COVID-19, ma anche ad altri rischi per la salute, ad esempio legati al cambiamento climatico. Infine, esiste una notevole variabilità e frammentazione nel livello di digitalizzazione e di adozione della tecnologia da parte degli operatori sanitari. Un esempio di questa complessità è che l'indisponibilità del servizio causata da un incidente di cybersecurity può comportare

¹¹ Secondo il Threat Landscape for the Health Sector dell'ENISA, la violazione o il furto di dati sono stati confermati nel 43% degli incidenti ransomware analizzati.

¹² [Relazione sullo stato del Decennio digitale 2024](#)

¹³ Irish Health Service Executive (2021): "Conti cyber attack on the HSE: Independent Post Incident Review".

¹⁴ Irish Health Service Executive: "Cyber-attack and HSE response". Disponibile all'indirizzo <https://www2.hse.ie/services/cyber-attack/what-happened/>.

gravi danni e pregiudizi ai pazienti anche in strutture sanitarie di piccole dimensioni, tra cui cliniche o servizi medici di emergenza che forniscono un servizio essenziale a un numero relativamente basso di utenti.

Secondo la relazione ENISA 2024 sullo stato della sicurezza informatica nell'Unione¹⁵, la maturità del settore sanitario dell'UE è moderata e vi sono ampie differenze nel livello di maturità della sicurezza informatica tra gli enti sanitari in Europa. Le carenze si riscontrano in aree chiave come la disponibilità di risorse umane sufficienti, la conoscenza da parte delle organizzazioni delle loro catene di fornitura di tecnologie dell'informazione e della comunicazione (TIC) e l'installazione di funzioni di sicurezza aggiornate nei prodotti. Il settore è alle prese con l'igiene informatica di base e le misure di sicurezza fondamentali, come dimostra il fatto che quasi tutte le organizzazioni sanitarie intervistate incontrano difficoltà quando si tratta di eseguire valutazioni del rischio di cybersecurity, mentre quasi la metà non ha mai eseguito un'analisi del rischio.¹⁶

Un'altra sfida significativa per la cybersicurezza degli ospedali è l'intersezione tra tecnologie informatiche (IT) e tecnologie operative (OT), dove si incontrano diverse priorità di sicurezza per quanto riguarda la riservatezza, la disponibilità e l'affidabilità, e dove una violazione in un'area può influenzare l'altra. La relazione ENISA 2024 sullo stato della sicurezza informatica nell'Unione sottolinea inoltre che il settore sanitario non riesce a garantire adeguatamente la sicurezza dei prodotti e dei processi TIC che utilizza, a causa della grande varietà di entità, dispositivi e prodotti sanitari.

Questa diversità, unita a livelli diversi di consapevolezza informatica tra il personale e il management degli ospedali, crea una sfida complessa per garantire la sicurezza informatica dei sistemi sanitari. Ad esempio, secondo l'Eurobarometro 2024 sulle competenze informatiche, solo il 25% delle aziende intervistate nel settore della sanità, dell'istruzione e dell'assistenza sociale ha fornito formazione o sensibilizzazione sulla sicurezza informatica nei 12 mesi precedenti¹⁷. È necessario intervenire per promuovere una cultura di sensibilizzazione alla cybersecurity tra gli operatori sanitari in prima linea. Ad esempio, la rotazione del personale, l'uso di postazioni di lavoro condivise, la scarsa gestione dell'autenticazione e l'uso di supporti rimovibili sono ulteriori fonti di vulnerabilità che incidono sulla sicurezza informatica degli operatori sanitari¹⁸.

In molti casi, l'IT e l'OT sono almeno in parte esternalizzati. L'Eurobarometro 2024 ha rilevato che la percentuale di aziende che esternalizzano almeno alcuni aspetti della propria cybersecurity è la più alta nel della sanità, dell'istruzione e dell'assistenza sociale, con il 57% delle aziende intervistate che lo fanno¹⁹. Analogamente, si registra una forte tendenza a migrare verso il cloud computing, spinta dalla necessità di archiviare e gestire i dati in modo scalabile, dall'efficienza dei costi, dal miglioramento della collaborazione e dal supporto di tecnologie avanzate come l'IA e l'Internet delle cose mediche. Nel 2022, il 58% delle organizzazioni sanitarie utilizzerà una piattaforma di sanità digitale basata sul cloud²⁰. Tuttavia, se da un lato questo passaggio può portare notevoli efficienze, dall'altro comporta anche dei rischi che richiedono decisioni informate sull'acquisto e sulla configurazione sicura.

¹⁵ ENISA: Relazione 2024 sullo stato della cibersicurezza nell'Unione
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

(settembre 2024). Disponibile su

¹⁶ ENISA Threat Landscape: Health Sector (luglio 2023). Disponibile all'indirizzo
<https://www.enisa.europa.eu/publications/health-threat-landscape>

¹⁷ Eurobarometro Flash 547 sulle competenze informatiche (maggio 2024). Disponibile su
<https://europa.eu/eurobarometer/surveys/detail/3176>

¹⁸ Panacea - Cybersecurity incentrata sulle persone nell'assistenza sanitaria (2021): Libro bianco - Lezioni apprese da PANACEA sulla protezione informatica di ospedali e centri di cura.

¹⁹ Eurobarometro Flash 547 sulle competenze informatiche (maggio 2024). Disponibile su
<https://europa.eu/eurobarometer/surveys/detail/3176>

²⁰ ENISA: NIS Investments Report 2022 (novembre 2022). Disponibile all'indirizzo
<https://www.enisa.europa.eu/publications/nis-investments-2022>

Tutte queste sfide sono collegate alla questione dello sviluppo delle capacità e dei finanziamenti. I finanziamenti per la sicurezza informatica nel settore sanitario sono stati limitati e rimangono una sfida universale in tutta l'UE²¹. Inoltre, queste sfide di finanziamento nascono nel contesto dell'invecchiamento della popolazione, che si prevede creerà ampie pressioni di bilancio sui sistemi sanitari europei nei prossimi decenni.

L'uso continuo di strumenti obsoleti e sistemi preesistenti, le risorse limitate per prevenire o reagire agli incidenti e le lacune nella maturità della cybersecurity derivano spesso da carenze di fondi. Gli ospedali si trovano ad affrontare una sfida continua per bilanciare un'infrastruttura sicura e digitale aggiornata con altri investimenti necessari per migliorare l'assistenza ai pazienti, come l'assunzione di medici e altri operatori sanitari, l'implementazione di nuovi metodi diagnostici e di trattamento e l'acquisto di dispositivi. Secondo l'ENISA⁽²²⁾, il settore sanitario si colloca solo al 7° posto dei 12 settori studiati per quanto riguarda la percentuale di spesa per la sicurezza delle informazioni rispetto alla spesa IT totale, con l'8,3% come mediana nel settore sanitario.

3. Centro europeo di supporto alla cybersecurity per ospedali e fornitori di servizi sanitari

Il quadro di riferimento dell'UE per la cybersecurity offre un'ampia gamma di strumenti che dovrebbero essere sfruttati per migliorare sicurezza e la resilienza di ospedali e fornitori di servizi sanitari. Per affrontare le numerose sfide evidenziate sopra, è necessario sviluppare un approccio unificato e strategico a livello dell'UE, riunendo le risorse, le competenze e gli strumenti necessari per affrontare efficacemente le minacce informatiche. Una visione d'insieme, così come una migliore pianificazione e un migliore coordinamento, sono essenziali per aiutare gli operatori sanitari in tutta l'UE a rafforzare le loro difese. A tal fine, l'ENISA si trova nella posizione migliore per istituire, all'interno della sua organizzazione, un **Centro europeo di sostegno alla cibersicurezza dedicato agli ospedali e ai fornitori di servizi sanitari**²³ nell'ambito del suo mandato²⁴ di salvaguardare e sostenere le infrastrutture critiche dell'UE.

Il Centro di supporto dovrebbe **sviluppare progressivamente un catalogo di servizi completo che risponda alle esigenze degli ospedali e dei fornitori di assistenza sanitaria**, delineando la gamma di servizi disponibili per la preparazione, la prevenzione, l'individuazione e la risposta. In collaborazione con le autorità degli Stati membri e sulla base delle esperienze degli ospedali e dei fornitori di assistenza sanitaria, il Centro di sostegno dovrebbe sviluppare un archivio di facile accesso di tutti gli strumenti disponibili a livello europeo, nazionale e regionale. Nello svolgimento delle sue attività, dovrebbe garantire un adeguato coordinamento con gli Stati membri e sostenere la definizione delle priorità e la realizzazione delle azioni necessarie in tempo reale.

Come importante elemento di base per lo sviluppo del catalogo di servizi del Centro di supporto, la Commissione proporrà di avviare progetti pilota in tutta l'UE per sviluppare le migliori pratiche per l'igiene informatica e la valutazione dei rischi per la sicurezza, nonché affrontare necessità di un monitoraggio continuo della sicurezza informatica, delle informazioni sulle minacce e della risposta agli incidenti utilizzando soluzioni di sicurezza informatica all'avanguardia. I risultati di questi progetti pilota, che saranno finanziati dal Programma Europa Digitale ed eseguiti dal Centro Europeo di Cybersecurity, saranno presentati al pubblico.

²¹ L'organizzazione e la fornitura di servizi sanitari e di assistenza medica sono di competenza nazionale ai sensi dell'articolo 168 del trattato sul funzionamento dell'Unione europea e il finanziamento dei sistemi sanitari varia da uno Stato membro all'altro.

²² ENISA: NIS Investments Report 2022 (novembre 2022). Disponibile all'indirizzo <https://www.enisa.europa.eu/publications/nis-investments-2022>.

²³ Nel presente documento, il termine "Centro di assistenza" è utilizzato in modo intercambiabile.

²⁴ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 (legge sulla cibersicurezza), GU L 151 del 7.6.2019, pag. 15-69.

Centro di competenza (ECCC), informerà ulteriori azioni a livello UE, compreso il lavoro del Centro di supporto.



Figura 1: Concetti per il catalogo di servizi del Centro di supporto per ospedali e fornitori di servizi sanitari

3.1. Prevenzione degli incidenti di sicurezza informatica

Azioni semplici che spostano le probabilità

Le misure di sicurezza informatica di base, come garantire che i sistemi siano , gestire i backup e implementare l'autenticazione a più fattori, secondo una stima possono proteggere le organizzazioni da

al 98% degli attacchi²⁵. Molte delle misure di igiene informatica e di gestione del rischio di maggiore impatto sono relativamente semplici da adottare, il che le rende un frutto a portata di mano per migliorare la sicurezza informatica. Uno dei ruoli chiave del Centro di supporto dovrebbe quindi essere quello di **sviluppare una guida chiara e mirata che evidenzia le pratiche di cybersecurity più critiche e aiuti gli operatori sanitari ad attuarle**. Questo supporto deve estendersi al di là dei grandi ospedali per includere consigli su misura per le entità più piccole, come gli uffici locali di medicina generale e le cliniche specializzate, che spesso non hanno le risorse per i team di cybersecurity dedicati ma rimangono ugualmente vulnerabili agli attacchi. Inoltre, è necessario considerare l'importanza regionale di specifiche entità sanitarie per garantire l'assistenza ai pazienti, ad nelle aree scarsamente popolate. Anche gli istituti di ricerca sanitaria che gestiscono grandi quantità di dati personali sensibili potrebbero trarre vantaggio dal ricevere indicazioni sulle misure di base di cybersecurity per migliorare la loro resilienza.

Le organizzazioni sanitarie sono inoltre soggette a una serie di obblighi in materia di sicurezza informatica derivanti dalla legislazione dell'UE²⁶. Sebbene gli obblighi siano fondamentali per garantire una base comune elevata per la sicurezza informatica e dei dati, è essenziale garantire che il panorama normativo non sia inutilmente difficile e oneroso da navigare. Una forte attenzione alla conformità non dovrebbe essere in contrasto con l'obiettivo di promuovere una forte cultura della sicurezza informatica. Uno **strumento di mappatura normativa di facile accesso può contribuire a ridurre al minimo l'onere amministrativo per le entità soggette a più strumenti normativi**. Oltre a sviluppare orientamenti e kit di strumenti, il Centro di sostegno dovrebbe lavorare a stretto contatto con la Commissione e gli Stati membri per sviluppare e diffondere tale strumento il prima possibile. Il Centro di sostegno svolgerebbe quindi un ruolo importante nel rendere le norme di cibersicurezza semplici da comprendere e da attuare, ad esempio fornendo orientamenti per l'attuazione²⁷ e, se necessario, promuovendo gli standard pertinenti.

I portafogli europei per l'identità digitale, di prossima realizzazione, sono un altro strumento per facilitare la semplice attuazione di buone pratiche di igiene informatica. Ridurre la dipendenza da meccanismi di identificazione deboli, come le password, è essenziale per mitigare i rischi di accesso non autorizzato ai dati sanitari. È fondamentale passare a soluzioni di accesso sicure basate su un'identificazione affidabile. L'UE Digitale

²⁵ Rapporto Microsoft sulla difesa digitale 2022. Disponibile all'indirizzo <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022>.

²⁶ Come la direttiva NIS2; il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (Cyber Resilience Act), <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>; il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, sui dispositivi medici, <https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng>; il regolamento (UE) 2017/745/oj/eng (Medical Devices Regulation), <https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng>; il Regolamento sui dispositivi medici; Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro (In vitro diagnostic medical devices Regulation), <https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng>; Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>; Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate in materia di intelligenza artificiale (legge sull'intelligenza artificiale), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>; Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sullo spazio europeo dei dati sanitari, COM(2022)197 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197>. I negoziati si sono conclusi con un accordo politico nella primavera del 2024 e, dopo la finalizzazione, la pubblicazione sulla Gazzetta Ufficiale è prevista per la primavera del 2025.

²⁷ L'elaborazione di orientamenti sull'interpretazione del regolamento generale sulla protezione dei dati (GDPR) è di competenza del Comitato europeo per la protezione dei dati (EDPB). L'elaborazione di linee guida da parte dell'ENISA dovrebbe rispettare pienamente le prerogative dell'EDPB.

Identity Wallet offre un approccio armonizzato a livello europeo all'identificazione elettronica degli operatori sanitari, fornendo una soluzione solida e unificata a partire dalla fine del 2026. Tutti i sistemi di informazione sanitaria online che devono implementare un'autenticazione forte degli utenti saranno obbligati ad accettare il Wallet per l'identificazione a partire dalla fine del 2027²⁸.

Preparazione e sostegno mirato

I test di preparazione, che comprendono azioni come i test di penetrazione, sono una pietra miliare di un'efficace sicurezza informatica e la Commissione ha già stanziato finanziamenti all'ENISA per iniziative pilota di preparazione, che hanno rivelato che il settore sanitario è tra le aree più richieste per i test e le ulteriori valutazioni per identificare le lacune nella maturità della sicurezza informatica. Con l'entrata in vigore della legge sulla solidarietà informatica, questi sforzi si espanderanno in modo significativo, con l'ECCC che assumerà un ruolo guida. Per rispondere a questa esigenza, la Commissione proporrà, in consultazione con il gruppo di cooperazione NIS, l'EU-CyCLONe²⁹ e l'ENISA, di identificare la sanità come un settore per il quale può essere fornito un sostegno per **test coordinati di preparazione** nell'ambito del Cyber Solidarity Act. Inoltre, il Centro di supporto dovrebbe sviluppare un **quadro su misura per le valutazioni di maturità della cybersecurity specifiche per il settore sanitario**. Tali valutazioni di maturità fornirebbero agli enti informazioni utili sulle loro vulnerabilità e consentirebbero loro di dimostrare la loro preparazione in materia di cybersecurity ai pazienti e alle parti interessate, rafforzando la fiducia nei loro servizi. A livello aggregato, il Centro di supporto dovrebbe effettuare una **valutazione annuale della ciber-maturità del settore sanitario**, che fornirebbe una chiara panoramica della sicurezza informatica del settore a livello nazionale e dell'UE.

Il settore sanitario si affida in larga misura ad appaltatori esterni per i servizi di cybersecurity³⁰, evidenziando la necessità di un sostegno mirato per rafforzare le difese. Sulla base di iniziative di successo come i voucher per l'innovazione dell'UE, gli **Stati membri dovrebbero prendere in considerazione misure mirate come i voucher per la cybersecurity per gli ospedali e i fornitori di servizi sanitari di micro, piccole e medie dimensioni**. Questi voucher fornirebbero assistenza finanziaria per mettere in atto misure specifiche di cybersecurity. La definizione delle priorità per l'assegnazione dei voucher dovrebbe basarsi sui risultati dei test di preparazione e delle valutazioni di maturità.

Le conoscenze e il contesto locali sono fondamentali per un'efficace diffusione dei voucher o di altri programmi di sostegno, garantendo la pertinenza e l'accessibilità. I fondi dell'UE, come il Fondo europeo di sviluppo regionale, sono già attivi nel sostenere iniziative di cybersecurity e sanità digitale e potrebbero quindi servire come veicolo per sviluppare programmi mirati di voucher per la cybersecurity per i fornitori di servizi sanitari. Per guidare questo sforzo, il Centro di supporto collaborerebbe con gli Stati membri e le autorità di programma regionali per sostenere lo sviluppo di tali schemi di voucher regionali, traendo insegnamento dai progetti nazionali esistenti e dalle azioni finanziate nell'ambito del Programma Europa digitale per garantire un'attuazione pratica e d'impatto.

Inoltre, dal 2014, i programmi Horizon hanno contribuito a finanziare una serie di iniziative di ricerca incentrate sul miglioramento della resilienza delle istituzioni sanitarie, come gli ospedali, contro le minacce informatiche.

²⁸ Articolo 5, lettera f), paragrafi 1 e 2, del regolamento (UE) n. 910/2014.

²⁹ Rete europea di organizzazioni di collegamento in caso di crisi informatica

³⁰ Si veda la relazione sugli investimenti nella sicurezza delle reti e dell'informazione dell'ENISA per il 2023 (novembre 2023), che evidenzia l'importanza del supporto esterno per l'audit e la conformità della sicurezza informatica. Disponibile su <https://www.enisa.europa.eu/publications/nis-investments-2023>

e attenuare i rischi associati all'uso improprio delle tecnologie emergenti. I risultati ottenuti comprendono una suite di strumenti, strutture e sistemi specializzati, come strumenti di valutazione del rischio, piattaforme di condivisione dei dati che preservano la privacy, soluzioni crittografiche, programmi di formazione sulla consapevolezza della sicurezza informatica e sistemi di rilevamento delle minacce in tempo reale. In particolare, queste soluzioni sono state rigorosamente convalidate attraverso implementazioni pilota nel mondo reale in ambienti sanitari, garantendone l'efficacia e l'applicabilità pratica nella protezione dalle minacce informatiche.

Proteggere le catene di fornitura dell'assistenza sanitaria

Una sfida fondamentale per le organizzazioni sanitarie è la gestione di catene di fornitura ICT complesse, che coinvolgono una serie di prodotti come dispositivi medici connessi, sistemi di cartelle cliniche elettroniche e hardware per ufficio. Gli ospedali e i fornitori di servizi sanitari hanno bisogno di sistemi e servizi TIC affidabili e sicuri per le loro operazioni. Per contribuire ad affrontare le sfide della cybersicurezza nel settore sanitario, il gruppo di cooperazione NIS dovrebbe eseguire una **valutazione coordinata del rischio di sicurezza, valutando i rischi tecnici e strategici legati alle catene di fornitura di dispositivi medici e proponendo misure di attenuazione**.³¹ Se opportuno, il gruppo di cooperazione NIS dovrebbe collaborare con il gruppo di coordinamento dei dispositivi medici.

Il Cyber Resilience Act è un quadro nuovo e completo che stabilisce i requisiti di cybersecurity per la pianificazione, la progettazione, lo sviluppo, nonché la gestione, il patching e la segnalazione delle vulnerabilità attivamente sfruttate per quasi tutti i prodotti hardware e software, in ogni fase della catena del valore³². I dispositivi medici sono un tipo di prodotto utilizzato in una delle aree più sensibili della nostra società. I requisiti di cybersecurity per questi prodotti derivano dal preesistente regolamento sui dispositivi medici e dal regolamento sui dispositivi medici diagnostici in vitro³³. La valutazione in corso di questi regolamenti sta esaminando il potenziale per una maggiore coerenza e sinergia tra questi quadri al fine di garantire una semplificazione e una cybersecurity all'avanguardia.

Inoltre, i risultati della valutazione del rischio dovrebbero aiutare le organizzazioni sanitarie a rivedere le loro pratiche di cybersicurezza della catena di approvvigionamento, come richiesto dalla direttiva NIS2, e potrebbero informare lo sviluppo di nuove **linee guida sugli appalti**³⁴. Sviluppate dall'ENISA attraverso il suo Centro di supporto, queste linee guida dovrebbero riflettere le tendenze recenti, come la cloudificazione dell'archiviazione dei dati dei pazienti, compresa la necessità di una migrazione sicura dei dati sanitari elettronici verso ambienti cloud. Inoltre, le nuove linee guida dovrebbero offrire alle organizzazioni strumenti pratici per tenere sotto controllo le loro catene di approvvigionamento, tra cui fornitori di servizi di sicurezza gestiti (MSSP), rapporti di attestazione o valutazioni del rischio di terze parti.

³¹ Ai sensi dell'articolo 22 della direttiva NIS2.

³² In una prima fase, a partire dal 1° agosto 2025, ampie categorie di apparecchiature radio, che non rientrano nell'ambito di applicazione del regolamento sui dispositivi medici e del regolamento sui dispositivi medico-diagnostici in vitro, saranno tenute a rispettare i requisiti essenziali della direttiva sulle apparecchiature radio relativi alla cybersicurezza quando saranno immesse nel mercato unico. In una seconda fase, a partire dall'11 dicembre 2027, entrerà in vigore il Cyber Resilience Act.

³³ Nel dicembre 2019, il Medical Devices Cooperation Group ha pubblicato una guida sulla cybersecurity per i dispositivi medici, supportando i fabbricanti nel soddisfare i requisiti dell'allegato I dei due regolamenti:
<https://ec.europa.eu/docsroom/documents/41863>.

³⁴ Basandosi sulle linee guida ENISA 2020 sugli appalti per la sicurezza informatica negli ospedali (febbraio 2020). Disponibile su <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>

Per quanto riguarda il cloud, sono necessarie ulteriori azioni per affrontare le sfide uniche della gestione dei dati sanitari sensibili, tra cui l'aumento della sicurezza, della privacy e dei rischi operativi. Per rafforzare le salvaguardie, gli esperti raccomandano di incorporare nei servizi cloud la "Security by Default and by Design". Questo approccio dà priorità a un'infrastruttura sicura, alla gestione proattiva delle vulnerabilità e a un mix di soluzioni cloud governative e private. Il monitoraggio continuo e le attestazioni specifiche dei fornitori, come le certificazioni dei fornitori di sicurezza e gli audit di conformità agli standard nazionali e internazionali, sono anch'essi essenziali per garantire pratiche di sicurezza solide.

Per servizi come Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) e Software-as-a-Service (SaaS), l'implementazione della sicurezza è spesso a carico del cliente. Tuttavia, molte organizzazioni sanitarie non dispongono delle risorse necessarie per soddisfare questi requisiti in modo indipendente. Per risolvere questo problema, i **fornitori di servizi cloud dovrebbero essere incoraggiati a implementare misure di sicurezza di base come caratteristica standard**. Queste misure ridurrebbero il rischio di configurazioni errate, manterrebbero una protezione coerente negli ambienti gestiti dal cliente e fornirebbero maggiori garanzie agli utenti. La definizione di una linea di base di sicurezza predefinita mirerebbe a bilanciare una protezione solida con la praticità, garantendo l'usabilità per un'ampia gamma di organizzazioni sanitarie. Questo sforzo comporterebbe una stretta collaborazione tra i fornitori di cloud e settore sanitario, sfruttando le migliori pratiche del settore per creare soluzioni efficaci e scalabili.

Formazione e sviluppo delle competenze

Avere una forza lavoro con competenze richieste è importante per la crescita sostenibile a lungo termine e la competitività in Europa, nonché per servizi di alta qualità, compresi i servizi sanitari. La carenza di professionisti qualificati nel campo della cybersecurity è una sfida significativa in tutta Europa, con un gap stimato di 299.000 professionisti per colmare il fabbisogno di forza lavoro nell'UE³⁵. Secondo l'Eurobarometro 2024 sulle competenze informatiche³⁶, l'81% delle aziende considera le difficoltà di assunzione di personale di cybersecurity come un rischio chiave per potenziali attacchi informatici. Nei settori dell'istruzione, della sanità e dell'assistenza sociale, il 66% dei ruoli di cybersecurity è ricoperto da dipendenti in transizione da posizioni non di cybersecurity, evidenziando l'urgente necessità di riqualificazione e aggiornamento.

Per affrontare questa sfida, il Centro di supporto dovrebbe collaborare con il futuro Consorzio europeo per le infrastrutture digitali (EDIC) per le competenze in materia di cibersicurezza, previsto dalla comunicazione della Commissione sull'Accademia delle competenze in materia di cibersicurezza³⁷. Il lavoro dovrebbe facilitare gli scambi tra i professionisti della cybersecurity nel settore sanitario, come i Chief Information Security Officer (CISO). Un'azione potenziale potrebbe essere la creazione di una **rete europea di CISO del settore sanitario**, a partire da un pool di esperti per condividere e sviluppare le migliori pratiche, le strategie di fidelizzazione dei talenti e le soluzioni per attrarre i professionisti della cybersecurity nel sanitario. Inoltre, sotto l'egida della Cybersecurity Skills Academy, dovrebbero essere sviluppate risorse per migliorare la forza lavoro della cybersecurity nel settore sanitario con l'obiettivo di

³⁵ [Il panorama della cybersecurity per il 2024: spunti dallo studio sulla forza lavoro nel settore della cybersecurity dell'ISC2|le competenze e i lavori digitali Piattaforma per](#)

³⁶ Eurobarometro Flash 547 sulle competenze informatiche.

³⁷ Comunicazione della Commissione al Parlamento europeo e al Consiglio: Colmare il deficit di talenti nel campo della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia delle competenze di cibersicurezza"). COM(2023) 207 definitivo.

sostegno dell'industria e del mondo accademico. A questo proposito, le parti interessate dell'industria dovrebbero essere incoraggiate a sostenere il miglioramento della formazione in materia di cybersicurezza.

L'errore umano continua a essere uno dei principali responsabili degli incidenti di cybersecurity nel settore sanitario, sottolineando la necessità critica di una formazione completa del personale e di una consapevolezza informatica. Dato il frequente utilizzo di strumenti digitali da parte degli operatori sanitari, è fondamentale dotarli di conoscenze sulle pratiche sicure. Campagne di formazione e sensibilizzazione mirate possono ridurre significativamente i rischi. Per affrontare questo problema, il Centro di supporto dovrebbe lavorare con gli operatori e i fornitori di servizi sanitari e collaborare con i fornitori di istruzione e formazione, con l'industria, con l'EDIC per le competenze in materia di sicurezza informatica e con le autorità degli Stati membri per creare e diffondere **moduli e corsi di formazione online completi e di facile accesso**.

L'inserimento di moduli di competenza digitale e di cybersecurity nei curricula formativi è fondamentale per costruire una solida base di cybersecurity nell'assistenza sanitaria. Questi moduli dovrebbero affrontare questioni specifiche del settore, come la protezione dei dati dei pazienti e le vulnerabilità nella sicurezza dei dispositivi medici. Lo sviluppo di queste risorse dovrebbe tenere conto di azioni precedenti, come il progetto BeWell finanziato dal programma Erasmus+³⁸ e il progetto PANACEA finanziato da Horizon 2020³⁹.

3.2. Capacità europee di rilevare le minacce informatiche contro il settore sanitario

Un rilevamento efficace delle minacce informatiche è essenziale per una risposta tempestiva agli incidenti. Gli attori delle minacce possono sfruttare tecniche per rendere le intrusioni difficili da rilevare, consentendo periodi prolungati di accesso non autorizzato a un sistema⁴⁰. Pertanto, migliori capacità di rilevamento delle minacce possono contribuire a fermare gli attacchi informatici sul nascere. Ad esempio, nell'attacco ransomware contro il fornitore finlandese di servizi di psicoterapia Vastaamo, durante il quale l'autore ha estorto ai pazienti le cartelle cliniche riservate, l'intrusione iniziale è avvenuta nel 2018, ma è diventata nota al fornitore solo nel 2020⁴¹.

Una condivisione efficiente delle informazioni e una collaborazione sono essenziali per migliorare l'individuazione delle minacce e la consapevolezza della situazione in tutta l'UE. I Computer Security Incident Response Teams (CSIRT) svolgono un ruolo fondamentale nel ricevere le segnalazioni di incidenti, quasi incidenti e potenziali minacce, offrendo indicazioni sulle misure di mitigazione a livello nazionale. Tuttavia, **gli Stati membri sono fortemente incoraggiati a condividere con il Centro di supporto dell'ENISA tutte le notifiche di incidenti informatici provenienti da ospedali e fornitori di servizi sanitari, per consentire una conoscenza della situazione a livello europeo**. Idealmente, ciò dovrebbe essere accompagnato da una caratterizzazione significativa delle varie dimensioni dell'incidente, comprese le vulnerabilità di base conosciute e gli effetti sui servizi sanitari e sugli eventi avversi dei pazienti. Inoltre, i produttori di dispositivi medici e diagnostici in vitro sono incoraggiati a segnalare volontariamente, attraverso la piattaforma di segnalazione unica che sarà istituita e gestita dall'ENISA nell'ambito della legge sulla resilienza informatica,

³⁸ BeWell - Blueprint alliance for a future health workforce strategy on digital and green skills. Disponibile su <https://bewell-project.eu/>.

³⁹ PANACEA - Protection and privacy of hospital and health infrastructures with smart Cyber security and cyber threat toolkit for data and people. Disponibile su <https://cordis.europa.eu/project/id/826293>.

⁴⁰ ENISA Health Threat Landscape 2023.

⁴¹ Decisione 1150/161/2021 dell'Ombudsman finlandese per la protezione dei dati.

vulnerabilità attivamente sfruttate o gravi incidenti informatici che hanno un impatto sulla sicurezza di questi dispositivi, nonché potenzialmente altre vulnerabilità, incidenti, quasi incidenti o minacce informatiche che possono influire sul profilo di rischio di questi dispositivi.

Quando le informazioni contenute nei rapporti non sono più sensibili, il Centro di supporto potrebbe un catalogo europeo di vulnerabilità sfruttate note (KEV) sponsorizzato dall'ENISA per i dispositivi medici, i sistemi di cartelle cliniche elettroniche e i fornitori di apparecchiature e software TIC nel settore sanitario. Per affrontare le sfide significative del rilevamento delle minacce, il Centro di supporto dovrebbe introdurre **un servizio di abbonamento di allerta precoce a livello europeo per il settore sanitario, che fornisca avvisi quasi in tempo reale**. Questo servizio si avvarrebbe dei dati elaborati dai CSIRT, dagli enti e dai produttori del settore sanitario, dall'Open-Source Intelligence (OSINT) e da altri attori rilevanti come i Cyber Hubs, i Centri di condivisione e analisi delle informazioni (ISAC) e le autorità di polizia. Una maggiore cooperazione tra l'ENISA e l'Agenzia dell'Unione Europea per la Cooperazione con le Forze dell'Ordine (Europol), ad esempio sui modelli di criminalità informatica contro il settore sanitario, aumenterebbe ulteriormente la consapevolezza della situazione.

Gli ISAC fungono da risorse centrali per l'intelligence sulle minacce informatiche, favorendo la condivisione bidirezionale delle informazioni tra il settore pubblico e quello privato e promuovendo la costruzione della fiducia. Il Centro di supporto dovrebbe intensificare il sostegno all'**ISAC europeo per la salute** con strumenti e scambio di informazioni, rapporti sulla consapevolezza della situazione settoriale e la promozione di una comunità di fiducia per la collaborazione tattica e strategica. Gli Stati membri dovrebbero incoraggiare lo sviluppo di ISAC sanitari nazionali⁴². Gli ISAC dovrebbero anche essere incoraggiati a riunire i fornitori di servizi sanitari e i produttori per dare origine a una comprensione congiunta delle minacce alla sicurezza informatica, anche nella catena di approvvigionamento, e facilitare il dialogo sulla progettazione sicura dei prodotti che tenga veramente conto delle realtà di impiego sul campo.

3.3. Risposta rapida e recupero

Data l'elevata sensibilità dei dati sanitari dei pazienti e gli effetti potenzialmente devastanti degli attacchi informatici sui servizi sanitari, una risposta rapida ed efficace agli incidenti di sicurezza informatica è fondamentale per salvaguardare la sicurezza dei pazienti. Quando un ospedale o un'azienda sanitaria subisce un attacco informatico, il primo punto di contatto è il CSIRT nazionale competente⁴³. Il CSIRT ha la responsabilità di fornire un supporto tempestivo, idealmente entro 24 ore, per aiutare a gestire gli incidenti significativi. Tuttavia, se un incidente supera le capacità del CSIRT, dovrebbe essere disponibile un supporto dell'UE per garantire una risposta rapida ed efficace.

La riserva dell'UE per la sicurezza informatica, istituita ai sensi della legge sulla solidarietà informatica, fornisce servizi di risposta agli incidenti da parte di fornitori di sicurezza gestiti di fiducia per assistere gli incidenti di sicurezza informatica significativi o su larga scala e gli sforzi iniziali di recupero. La riserva è concepita per integrare gli sforzi dei CSIRT degli Stati membri, consentendo loro di richiedere un supporto aggiuntivo nei casi che coinvolgono settori critici come la sanità.

⁴² Ad esempio, la Finlandia ha un ISAC nazionale per il settore dell'assistenza sociale e sanitaria. Cfr. Finnish National Cybersecurity Centre: "ISAC information sharing groups", disponibile all'indirizzo <https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups>.

⁴³ L'articolo 23, paragrafo 1, della direttiva NIS2 stabilisce l'obbligo per i soggetti essenziali e importanti di notificare gli incidenti significativi al CSIRT competente o, se del caso, all'autorità competente.

Per migliorare questo sistema, la **Commissione e l'ENISA dovrebbero garantire che la riserva includa un servizio di risposta rapida specifico per il settore sanitario**. In complementarità con altri quadri esistenti, questo servizio dispiegherebbe esperti per gestire senza indugio incidenti di cybersecurity significativi o su larga scala nel settore sanitario quando il supporto nazionale è insufficiente.

Per migliorare la risposta e il recupero, il Centro di supporto, in collaborazione con il gruppo di cooperazione NIS, la rete dei CSIRT e, se del caso, Europol, dovrebbe sviluppare **dei playbook di risposta agli incidenti informatici adattati all'assistenza sanitaria**. Questi manuali guiderebbero sia i CSIRT che le organizzazioni sanitarie nella risposta a specifiche minacce alla sicurezza informatica, tra cui il ransomware. Data l'importanza di un'efficace cooperazione tra CSIRT e autorità di contrasto nel rispondere e indagare sugli incidenti di cybersecurity di natura criminale, i playbook dovrebbero, tra gli altri aspetti, fornire chiare indicazioni sulla segnalazione di tali incidenti alle autorità di contrasto. Inoltre, il Centro di supporto potrebbe **facilitare un'ampia diffusione di esercitazioni nazionali di cybersecurity, basandosi sull'esperienza di esercitazioni come quella di Cyber Europe 2022 dell'ENISA, per testare i playbook e rafforzare i protocolli di risposta agli incidenti**.

Per informare le politiche e valutare l'efficacia delle misure adottate contro gli attacchi ransomware, è necessario raccogliere ulteriori dati. A tal , gli Stati membri dovrebbero richiedere agli enti soggetti alla direttiva NIS2, comprese le organizzazioni sanitarie, di riferire in merito ai pagamenti di riscatti effettuati e a quelli che intendono effettuare, insieme ad altre informazioni che forniscono quando riferiscono su incidenti significativi di sicurezza informatica. Tale segnalazione supporta le indagini efficaci sugli incidenti di ransomware, compresa la tracciabilità dei pagamenti sulle piattaforme di scambio di criptovalute al fine di identificare i destinatari.

La velocità di ripristino è un fattore critico per mantenere la resilienza e la fiducia del pubblico, in particolare nel settore sanitario, dove i tempi di inattività possono interrompere l'assistenza ai pazienti. Per un ripristino efficace dagli attacchi ransomware, i fornitori di servizi sanitari devono disporre di backup sicuri, aggiornati e isolati che possano essere ripristinati rapidamente. Come parte del suo catalogo di servizi, il Centro di supporto potrebbe offrire **un servizio di abbonamento per il recupero da ransomware, aiutando gli ospedali e i fornitori di servizi sanitari a preparare piani di recupero in anticipo**. L'ENISA e l'Europol dovrebbero collaborare per identificare i ceppi di ransomware più comuni che colpiscono le organizzazioni sanitarie e **ampliare l'archivio di strumenti di decrittazione** disponibili attraverso il progetto No More Ransom⁴⁴. Dovrebbero inoltre sviluppare e promuovere una guida accessibile per aiutare gli operatori sanitari a evitare di pagare riscatti utilizzando strumenti di decriptazione.

L'Iniziativa internazionale contro il ransomware⁴⁵ è un'arena preziosa per lo scambio di informazioni su specifici incidenti di ransomware, nonché per costruire le capacità dei Paesi membri di rafforzare i loro quadri di sicurezza informatica e le loro capacità investigative contro gli attori del ransomware. La Commissione, in collaborazione con l'Alto rappresentante, continuerà a promuovere la cooperazione nell'ambito dell'iniziativa contro il ransomware, anche per quanto riguarda le minacce di ransomware al settore sanitario. Inoltre, la Commissione cercherà di collaborare con **il Gruppo di lavoro sulla cybersecurity del G7** per rafforzare la cybersecurity del settore sanitario. In particolare, il gruppo di lavoro potrebbe valutare la possibilità di sostenere

⁴⁴ <https://www.nomoreransom.org/en/index.html>.

⁴⁵ <https://www.counter-ransomware.org/>

il settore sanitario contro minacce come il ransomware, basandosi su riflessioni come la Dichiarazione congiunta sugli attacchi di ransomware contro le strutture sanitarie dell'8 novembre 2024 presentata nel contesto del Consiglio di Sicurezza delle Nazioni Unite⁴⁶.

4. Azioni nazionali

La capacità di questo Piano d'azione di migliorare la sicurezza informatica nel settore sanitario dipende dal coinvolgimento attivo e dall'impegno degli Stati membri. Per attuare con successo il Piano d'azione, gli Stati membri potrebbero designare **Centri nazionali di supporto alla cibersecurity specifici per gli ospedali e i fornitori di servizi sanitari**. Questi centri fungerebbero da punti di contatto primari per il settore sanitario a livello nazionale, collaborando strettamente con il Centro di supporto ENISA. Ove possibile e pertinente, gli Stati membri dovrebbero designare come Centri nazionali di supporto alla cibersecurity organismi esistenti, come i CSIRT sanitari nazionali o le autorità competenti.

Gli Stati membri sono inoltre incoraggiati a creare **piani d'azione nazionali incentrati sulla sicurezza informatica nel settore sanitario**. Questi piani dovrebbero delineare i rischi specifici di cibersecurity affrontati dai sistemi sanitari e le azioni nazionali intraprese per , garantendo al contempo che le risorse e le pratiche a livello europeo siano utilizzate in modo efficace. Il Centro di supporto ENISA può aiutare a sviluppare questi piani, conto dei piani nazionali già esistenti e coordinando gli sforzi per garantire che le risorse e le strategie dei singoli Stati membri si integrino a vicenda.

Un altro obiettivo fondamentale per gli Stati membri è quello di facilitare la condivisione delle risorse tra i fornitori di servizi sanitari, che potrebbe avvenire attraverso **appalti congiunti o risorse comuni** a livello nazionale, regionale o addirittura europeo. Questo approccio ridurrebbe l'onere finanziario per i singoli enti, aumentando al contempo il loro potere contrattuale nei confronti dei fornitori di servizi di cybersecurity.

Ad esempio, il programma francese CaRE⁴⁷ ha introdotto una serie di misure a livello nazionale e regionale per affrontare le sfide in termini di risorse: un catalogo informatico fornisce una panoramica delle soluzioni e dei pacchetti informatici messi a disposizione degli ospedali attraverso l'agenzia nazionale per la sicurezza informatica, l'agenzia per la salute digitale, le agenzie regionali, le organizzazioni nazionali di acquisto e le soluzioni commerciali. A ciò si aggiungono finanziamenti aggiuntivi per le agenzie regionali che offrono risorse condivise.

Gli Stati membri dovrebbero anche affrontare i livelli insufficienti di investimento nella cibersecurity all'interno del settore sanitario. Per garantire un finanziamento adeguato, dovrebbero stabilire **parametri di riferimento non vincolanti e monitorare gli obiettivi di finanziamento destinati specificamente alla cibersecurity**, assicurando al contempo che questi investimenti non vadano a discapito delle cure essenziali per i pazienti. Questi obiettivi di finanziamento dovrebbero anche mirare a integrare le considerazioni sulla sicurezza in tutte le attività di sicurezza.

⁴⁶ <https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/>

⁴⁷ Agenzia francese per la salute digitale: Cybersécurité acceleration et Résilience des Établissements (CaRE). Disponibile all'indirizzo <https://esante.gouv.fr/strategie-nationale/cybersecurite>.

investimenti digitali nel settore. Gli Stati membri possono scambiarsi le migliori pratiche e consigli su questi obiettivi attraverso piattaforme come la rete eHealth⁴⁸.

5. Cooperazione pubblico-privato

La cooperazione e la consultazione tra pubblico e privato con i fornitori di assistenza sanitaria, altri enti del settore sanitario e gli operatori del settore della cibersecurity sono essenziali per il successo dell'attuazione del piano d'azione. Per alimentare ulteriormente il lavoro del Centro di supporto, la **Commissione, con il sostegno dell'ENISA, istituirà un comitato consultivo congiunto per la cibersecurity sanitaria**, composto da rappresentanti di alto livello di entrambi i settori, sanità e cibersecurity, in grado di consigliare la Commissione e il Centro di supporto su azioni di impatto e di discutere l'ulteriore sviluppo di partenariati pubblico-privati in questo campo. Il comitato si baserà sulle iniziative esistenti per i partenariati pubblico-privati, tra cui l'ISAC europeo per la salute.

Inoltre, la Commissione lancerà **un invito all'azione** rivolto alle imprese, alle fondazioni, agli istituti di istruzione e alle parti interessate del settore della cibersecurity **affinché si impegnino ad affrontare le sfide del settore**. Sulla base dell'esperienza della Cybersecurity Skills Academy, tali impegni potrebbero essere, ad esempio, la fornitura di corsi di formazione e materiali incentrati sul settore sanitario per i professionisti della cybersecurity⁴⁹. Altri impegni potrebbero riguardare anche attività di sensibilizzazione o la fornitura di servizi di sicurezza gestiti a enti specificamente vulnerabili, gratuitamente o a costi ridotti, al fine di aumentarne la preparazione e la resilienza alla cybersecurity. Inoltre, gli impegni potrebbero consistere nella condivisione di informazioni sulle minacce informatiche con il Centro di supporto dell'ENISA. Il Centro di supporto dovrebbe mantenere una panoramica degli impegni presi nell'ambito dell'invito all'azione, con l'obiettivo di garantirne la coerenza e la complementarietà.

6. Dissuadere gli attori delle minacce informatiche

Le politiche di sicurezza informatica interne ed esterne dell'UE dovrebbero sostenere l'obiettivo di dissuadere gli attori delle minacce informatiche dall'attaccare i sistemi sanitari europei. Gli attacchi informatici contro le organizzazioni sanitarie sono tipo di attività informatica dannosa particolarmente inaccettabile, data la loro capacità di minacciare la sicurezza dei pazienti e le vite umane. Pertanto, la piena forza delle capacità di deterrenza dell'UE nel campo della sicurezza informatica e dell'applicazione della legge dovrebbe essere utilizzata per minare il modello commerciale complessivo degli attori delle minacce che prendono di mira il settore sanitario e per privarli di facili profitti. A tal fine, sarebbe opportuno promuovere le indagini transfrontaliere attraverso una maggiore condivisione degli indicatori di compromissione e di altri dati rilevanti, nonché una maggiore attenzione agli obiettivi di alto valore e ai principali facilitatori criminali, come i servizi di hosting a prova di proiettile o di miscelazione di criptovalute.

Il **Cyber Diplomacy Toolbox** offre un quadro per prevenire, scoraggiare e rispondere agli attacchi informatici contro l'UE, gli Stati membri e i partner. L'Alto rappresentante continuerà a utilizzare il quadro di sanzioni informatiche esistente per rispondere alle minacce che colpiscono i sistemi sanitari.

⁴⁸ La Rete eHealth è una rete volontaria di autorità nazionali responsabili della sanità elettronica designate dagli Stati membri e istituita ai sensi dell'articolo 14 della direttiva 2011/24/UE.

⁴⁹ [Accademia delle competenze informatiche: Partecipa! Piattaforma per le competenze e i lavori digitali](#)

Ritenere gli attori criminali responsabili delle loro azioni è un importante deterrente. Pertanto, gli Stati membri dovrebbero garantire che l'applicazione della legge sia pienamente integrata nei loro piani d'azione nazionali. In particolare, dovrebbero sfruttare appieno le disposizioni della direttiva sugli attacchi contro i sistemi di informazione⁵⁰ e della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica per scoraggiare gli attacchi, consegnare i criminali alla giustizia e smantellare le infrastrutture criminali che facilitano gli attacchi⁵¹. Un'attuazione efficace di questi strumenti dovrebbe garantire che le azioni criminali e dolose contro l'assistenza sanitaria siano punite.

7. Attuazione e monitoraggio del Piano d'azione

Nel corso del presente piano d'azione, sono stati previsti diversi compiti per un centro di supporto da istituire all'interno dell'ENISA. Ciò garantisce un'attuazione olistica e coerente del piano d'azione, evitando al contempo la creazione di nuovi enti che potrebbero causare sovrapposizioni e costi generali. La Commissione intende garantire un'adeguata dotazione di risorse al Centro di supporto.

Una volta che il Centro di supporto sarà operativo, l'ENISA, in consultazione con la Commissione, dovrà fornire regolarmente aggiornamenti sul lavoro del Centro di supporto al consiglio di amministrazione dell'ENISA e alle reti pertinenti degli Stati membri, in particolare il gruppo di cooperazione NIS, la rete dei CSIRT, la rete eHealth e, se del caso, il consiglio dello spazio europeo dei dati sanitari. Inoltre, l'ENISA dovrebbe scambiare continuamente con il comitato consultivo pubblico-privato per la cibersecurity sanitaria informazioni sull'attuazione delle azioni fornite dal Centro di supporto.

Le relazioni periodiche dell'ENISA, come la Relazione sullo stato della cibersecurity nell'Unione, che fornisce una valutazione aggregata del livello di maturità delle capacità e delle risorse di cibersecurity in tutta l'UE, anche nel settore sanitario, dovrebbero servire come occasione per pubblicare dati pertinenti, a sostegno del monitoraggio del Piano d'azione. Inoltre, l'EU Cybersecurity Index⁵² dell'ENISA può fornire dati quantitativi e qualitativi, fungendo da base di prova per valutare la criticità e la maturità del settore sanitario.

8. Le prossime tappe

Questa comunicazione ha definito un'agenda ambiziosa per un settore sanitario più sicuro dal punto di vista informatico nell'UE. Con la proposta di sviluppare il Centro di supporto alla cibersecurity per gli ospedali e i fornitori di servizi sanitari nel cuore dell'ENISA, il piano d'azione definisce un percorso verso la creazione di un approccio europeo coerente e condiviso alla sfida della cibersecurity nel settore.

⁵⁰ Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio: <https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng>

⁵¹ La Convenzione sulla criminalità informatica (Convenzione di Budapest, ETS n. 185) e i suoi protocolli: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

⁵² ENISA, Indice di cibersecurity dell'UE, quadro e nota metodologica (2024). Disponibile all'indirizzo https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

La presente comunicazione deve essere vista come l'inizio di un processo volto a migliorare la sicurezza informatica nel settore sanitario. Pertanto, l'adozione del piano d'azione sarà accompagnata dall'avvio di ampie consultazioni con le parti interessate e dal proseguimento degli scambi con gli Stati membri e le reti pertinenti per raccogliere informazioni. Sulla base dei risultati delle consultazioni, la Commissione intende presentare raccomandazioni nel quarto trimestre del 2025 per perfezionare ulteriormente il piano d'azione.

La Commissione invita gli Stati membri e tutte le parti interessate a collaborare per realizzare l'ambizione del piano d'azione.

ALLEGATO - Panoramica delle azioni proposte

La Commissione:

Centro di supporto alla sicurezza informatica dell'ENISA per ospedali e fornitori di servizi sanitari	
Garantire risorse adeguate per il Centro di supporto per la sicurezza informatica. Collaborare con l'ECCC per avviare progetti pilota volti a sviluppare le migliori pratiche per l'igiene informatica e la valutazione del rischio di sicurezza, e per affrontare la necessità di un monitoraggio continuo della sicurezza informatica, dell'intelligence sulle minacce e della risposta agli incidenti utilizzando soluzioni di sicurezza informatica all'avanguardia, per lo sviluppo del catalogo di servizi del Centro europeo di supporto alla sicurezza informatica.	2025
Prevenzione degli incidenti di sicurezza informatica	
In consultazione con il gruppo di cooperazione NIS, l'UE-Cyclone e l'ENISA, valutare la possibilità di identificare la sanità come un settore a cui fornire sostegno per test di preparazione coordinati nell'ambito della legge sulla solidarietà informatica.	Q1 2025
Risposta rapida e recupero	
Insieme all'ENISA, garantire che la riserva di sicurezza informatica dell'UE includa un servizio di risposta rapida specifico per il settore sanitario.	Q4 2025
Cooperazione pubblico-privato	
Con il supporto dell'ENISA, è stato istituito un comitato consultivo congiunto per la sicurezza informatica in ambito sanitario.	Q1 2025
Lanciare un invito all'azione per le aziende di cybersecurity, le fondazioni, le istituzioni educative e le parti interessate del settore per impegnarsi ad affrontare le sfide nel settore sanitario.	Q2 2025
Dissuadere gli attori delle minacce informatiche	
Insieme all'Alto Rappresentante, esplorare l'uso delle misure del Cyber Diplomacy Toolbox per prevenire, scoraggiare, dissuadere e rispondere alle attività dannose contro i sistemi sanitari.	2025
Avanzamento internazionale cooperazione internazionale contro gli attori del ransomware , in particolare in l' Internazionale	2025-2026

Iniziativa di contrasto al ransomware, in collaborazione con l'Alto Rappresentante	
Cercare la cooperazione nel gruppo di lavoro sulla cybersecurity del G7 per rafforzare la cybersecurity del settore sanitario.	2025-2026
Le prossime tappe	
Avviare consultazioni complete con le parti interessate	Q1 2025
Adottare le raccomandazioni per perfezionare ulteriormente il Piano d'azione.	Q4 2025

ENISA:

Centro di supporto per la sicurezza informatica dell'UE per ospedali e fornitori di servizi sanitari	
Avviare i lavori per la creazione di un Centro europeo di supporto alla sicurezza informatica per gli ospedali e i fornitori di servizi sanitari.	Q2 2025
Sviluppare un catalogo completo di servizi fornire da parte del Centro di supporto per la sicurezza informatica.	Dal 4° trimestre 2025
Prevenzione degli incidenti di sicurezza informatica	
Pubblicare una guida che metta in evidenza le pratiche di cybersecurity più critiche e aiuti i fornitori di servizi sanitari ad attuarle	Q3 2025
In stretta collaborazione con la Commissione e gli Stati membri, sviluppare uno strumento di mappatura della normativa.	Q1 2025
Sviluppare un quadro di riferimento per la valutazione della maturità della cybersecurity specifica per il settore sanitario.	Q3 2025
Trasportare eseguire un annuale Salute Cyber Maturità sanitaria	2025-2026
Collaborare con gli Stati membri e le autorità di programma regionali per creare programmi modello di voucher per la sicurezza informatica.	2025-2026
Sviluppare nuovi appalti linee guida per la sicurezza informatica di ospedali e fornitori di servizi sanitari.	Q3 2025
Creare una rete europea di CISO della salute	Q1 2026

Progettare e promuovere moduli e corsi di formazione per i professionisti della sanità	Q1 2026
Capacità europee di rilevare le minacce informatiche contro il settore sanitario	
Creare un catalogo europeo di KEV per i dispositivi medici, i sistemi di cartelle cliniche elettroniche e i fornitori di apparecchiature e software TIC nel settore sanitario.	Q4 2025
Introdurre un servizio di abbonamento di allerta precoce a livello europeo per il settore sanitario	A partire dal 2026
Sostenere l'ISAC europeo per la salute con strumenti e scambio di informazioni.	2025-2026
Risposta rapida e recupero	
Insieme alla Commissione, garantire che la riserva di sicurezza informatica dell'UE includa un servizio di risposta rapida specifico per il settore sanitario.	Q4 2025
In collaborazione con la rete dei CSIRTs, sviluppare playbook di risposta agli incidenti informatici su misura per il settore sanitario.	Q3 2025
Facilitare un ampio lancio di esercitazioni nazionali di cybersecurity per testare i playbook e rafforzare i protocolli di risposta agli incidenti.	A partire dal 4° trimestre 2025
Fornire un servizio di abbonamento per il recupero dei ransomware	A partire dal 2026
Insieme a Europol, identificare i ceppi di ransomware più comuni che colpiscono le organizzazioni sanitarie e ampliare l'archivio di strumenti di decrittazione attraverso il progetto No More Ransom.	Q4 2025
Insieme a Europol, sviluppare una guida accessibile per aiutare gli operatori sanitari a non pagare riscatti.	Q3 2025
Azioni nazionali	
Assistere gli Stati membri nello sviluppo di piani d'azione nazionali	2025
Coordinare gli sforzi per garantire la complementarietà delle risorse e delle strategie dei singoli Stati membri.	2025-2026
Attuazione e monitoraggio del Piano d'azione	

In consultazione con la Commissione, fornire regolarmente aggiornamenti sul lavoro del Centro di supporto per la cibersicurezza alle reti pertinenti degli Stati membri.	2025-2026
Scambio continuo con il Comitato consultivo per la cibersicurezza sanitaria.	2025-2026

Stati membri:

Capacità europee di rilevare le minacce informatiche contro il settore sanitario	
Condividere le notifiche di incidenti da parte di ospedali e fornitori di servizi sanitari nell'ambito del NIS2 con il Centro europeo di supporto alla cibersicurezza.	A partire dal 4° trimestre 2025
Incoraggiare lo sviluppo di ISAC nazionali per la salute.	2025-2026
Prevenzione degli incidenti di sicurezza informatica	
Nell'ambito del gruppo di cooperazione NIS, eseguire una valutazione coordinata dei rischi per la sicurezza, valutando i rischi tecnici e strategici legati alle catene di fornitura dei dispositivi medici.	Q4 2025
Risposta rapida e recupero	
Avviare esercitazioni nazionali di cybersecurity per testare i playbook e rafforzare i protocolli di risposta agli incidenti.	A partire dal 2026
Azioni nazionali	
Designare centri nazionali di supporto alla sicurezza informatica per gli ospedali e i fornitori di servizi sanitari.	Q2 2025
Creare piani d'azione nazionali incentrati sulla sicurezza informatica nel settore sanitario.	Q4 2025
Facilitare la condivisione delle risorse tra gli operatori sanitari	2025-2026
Stabilire parametri di riferimento non vincolanti e monitorare gli obiettivi di finanziamento destinati specificamente alla cibersicurezza.	Q4 2025
Richiedere alle organizzazioni sanitarie e ad altre entità soggette alla Direttiva NIS2 di segnalare la loro intenzione di pagare riscatti.	Q4 2025