Sanità e cybersecurity:

il nuovo Piano d'Azione Europeo

avv. silvia stefanelli

Chi sono, Avv. Silvia Stefanelli

Fondatrice e co-titolare dello Studio Legale Stefanelli&Stefanelli.

Esperta di diritto sanitario, con particolare competenza in ambito di sanità digitale, medical device, pubblicità sanitaria, contratti con la PA, protezione dei dati.

Seguo svariati progetti di sviluppo innovativi in sanità legati all'uso delle nuove tecnologie.

Svolgo il ruolo di DPO in diverse strutture complesse.

Dal 2022 sono entrata a far parte del team di Individual Expert per l'implementazione di un pool a supporto del EDPB - European Data Protection Board nei gruppi "Technical expertise in new technology and information security" e "Legal expertise in new technologies".

Collaboro con la Fondazione SmithKline su progetti nazionali in ambito di Digital Therapeutics.

Sono Team Leader di Clusit su progetti di Intelligenza Artificiale.

E membro del Comitato Scientifico dell'Osservatorio di Telemedicina di Altems- Unicatt.

Il mio profilo

s.stefanelli@studiolegalestefanelli.it

aree di azione giuridica della Comunità sulla cybersecurity

i prodotti (art. 114 TUFE)

I Parlamento europeo e il Consiglio..adottano le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno

l'organizzazione dei servizi sanitari (art. 168 TUFE)

L'azione dell'Unione, che completa le politiche nazionali, si indirizza al miglioramento della sanità pubblica, alla prevenzione delle malattie e affezioni e all'eliminazione delle fonti di pericolo per la salute fisica e mentale.

Lo studio ha identificato 21 incidenti cyber in strutture sanitarie europee tra maggio 2022 e aprile 2023 che potevano potenzialmente influire sulla salute dei pazienti.

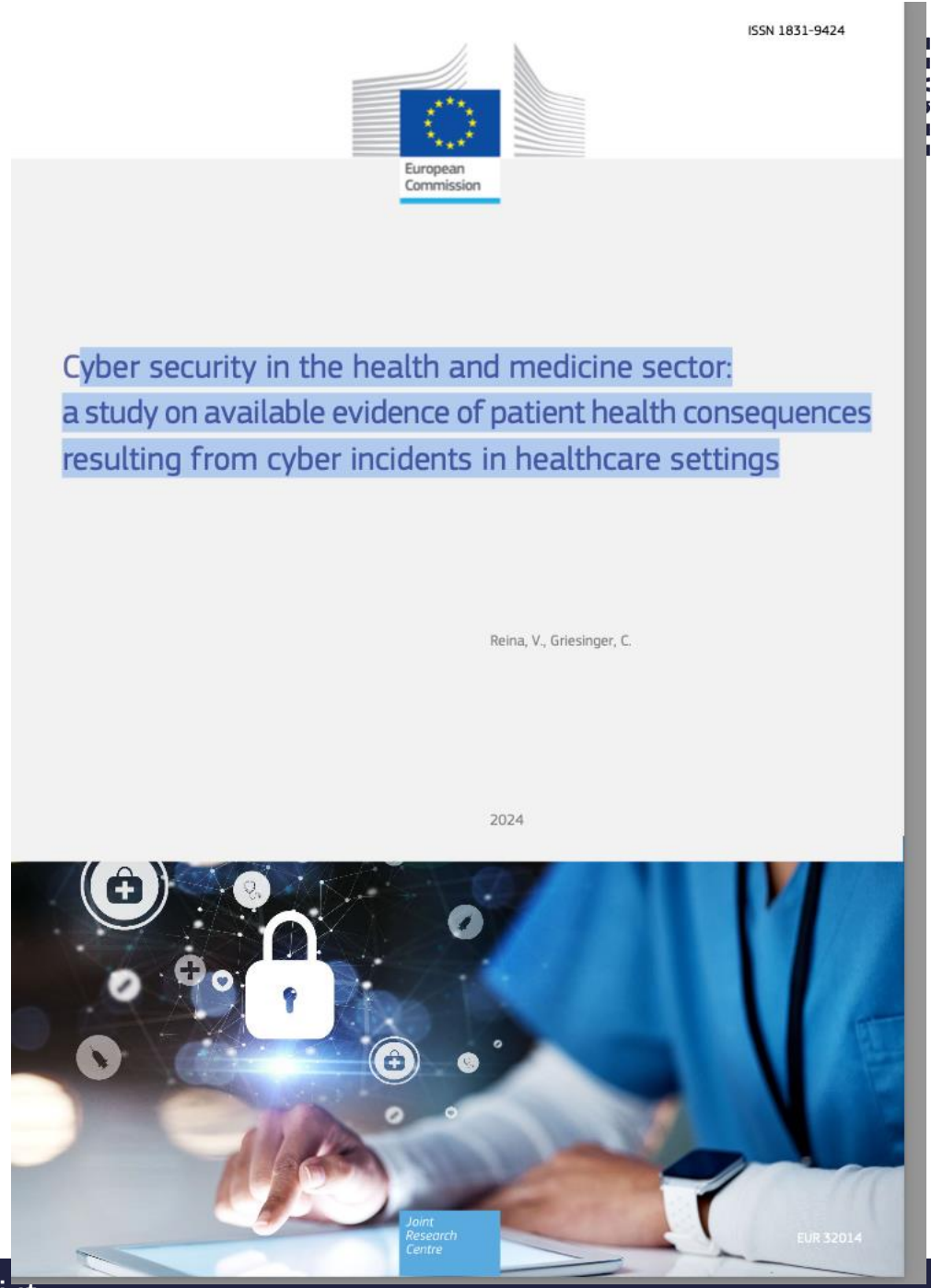
Gli impatti principali includevano:

- Terapie posticipate
- Interventi chirurgici ritardati
- Ambulanze deviate verso altre strutture
- Accesso limitato ai pronto soccorso

Il ransomware è risultato essere il tipo di attacco più frequente.

Il rapporto evidenzia l'importanza della cybersecurity e della resilienza cyber nel settore sanitario, in un contesto di crescente digitalizzazione.

2024



Dobbiamo fare di più per proteggere la sicurezza dei sistemi sanitari, che sempre più sono oggetto di attacchi informatici e ransomware.

Per migliorare l'individuazione delle minacce, la preparazione e la risposta alle crisi, proporrò, nei primi 100 giorni del mandato, un piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria.

Ursula von der Layen

luglio 2014

1 Sistemi sanitari sotto attacco

Sistemi sanitari sicuri e resilienti sono una pietra angolare del modello sociale dell'UE. Gli ospedali e i sistemi sanitari si trovano tuttavia ad affrontare minacce crescenti, provenienti in particolare da bande criminali che si servono dei ransomware e li prendono di mira a fini di lucro, attratte dall'elevato valore dei dati dei pazienti, comprese le cartelle cliniche elettroniche.

2 Impatto degli attacchi

Negli ultimi quattro anni il settore sanitario è infatti diventato quello più colpito, anche durante la pandemia di COVID-19, quando le infrastrutture sanitarie sono state oggetto di un numero sempre maggiore di attacchi informatici. Gli attacchi informatici contro ospedali e prestatori di assistenza sanitaria stanno causando danni diretti alle persone, ritardando le procedure mediche, paralizzando i reparti di pronto soccorso e potrebbero, in casi estremi, causare la perdita di vite umane.

Sfide della trasformazione digitale

STEFANELLI & STEFANELLI STUDIO LEGALE

1 Trasformazione digitale

La sanità digitale e l'utilizzo e il riutilizzo dei dati sanitari possono rendere possibili modelli di assistenza più adatti alle esigenze e alle preferenze delle persone e dei pazienti, prevenendo l'insorgenza di una malattia o consentendo trattamenti più precoci.

2 Processi clinici digitali

L'integrazione di strumenti e soluzioni digitali nei processi clinici, così come l'utilizzo e il riutilizzo dei dati sanitari possono orientare decisioni cliniche migliori, contribuire all'automazione in campo sanitario e a un'assistenza più rapida e di migliore qualità per i pazienti.

3 Maggiore vulnerabilità

Allo stesso tempo, con gli strumenti digitali aumentano altresì i potenziali obiettivi dei criminali informatici. Inoltre alcuni attori statali non risparmiano le strutture sanitarie nei loro attacchi, come dimostrato dall'attuale guerra di aggressione della Russia nei confronti dell'Ucraina.

Piano d'azione per la cibersicurezza negli ospedali e prestatori di assistenza sanitaria

Il contesto di sicurezza dell'UE sta cambiando rapidamente: stiamo assistendo a un'escalation di attacchi ibridi e di attacchi informatici che mirano a destabilizzare la nostra società, cercando di creare divisioni e perturbazioni, ma anche profitti attraverso attività informatiche criminali. L'Europa deve pertanto rafforzare urgentemente la propria preparazione e la propria resilienza a fronte di questa nuova realtà, in tutti i settori e in linea con un approccio esteso a tutta la società e a tutta l'amministrazione, come invocato nella relazione del consigliere speciale della presidente della Commissione europea Sauli Niinistö.

ss

EUROPEAN COMMISSION

Brussels, 15.1.2025
COM(2025) 10 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

European action plan on the cybersecurity of hospitals and healthcare providers

La necessità di un piano d'azione

Momento di agire

È pertanto giunto il momento di migliorare e rafforzare la cibersicurezza e la resilienza degli ospedali e dei prestatori di assistenza sanitaria europei, come sottolineato dalla presidente von der Leyen nei suoi orientamenti politici per la Commissione 2024-2029.

Focus del piano

Il piano d'azione si concentra principalmente sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria, intesi come una qualsiasi persona fisica o giuridica o qualsiasi altra entità che presti legalmente assistenza sanitaria nel territorio di uno Stato membro.

Approccio olistico

Allo stesso tempo, le misure volte a rafforzare la cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria dovrebbero anche affrontare i rischi che interessano la catena di approvvigionamento e l'ecosistema a livello più ampio, derivanti ad esempio da soggetti che utilizzano dati sanitari per la ricerca e l'apprendimento automatico o che producono dispositivi medici.

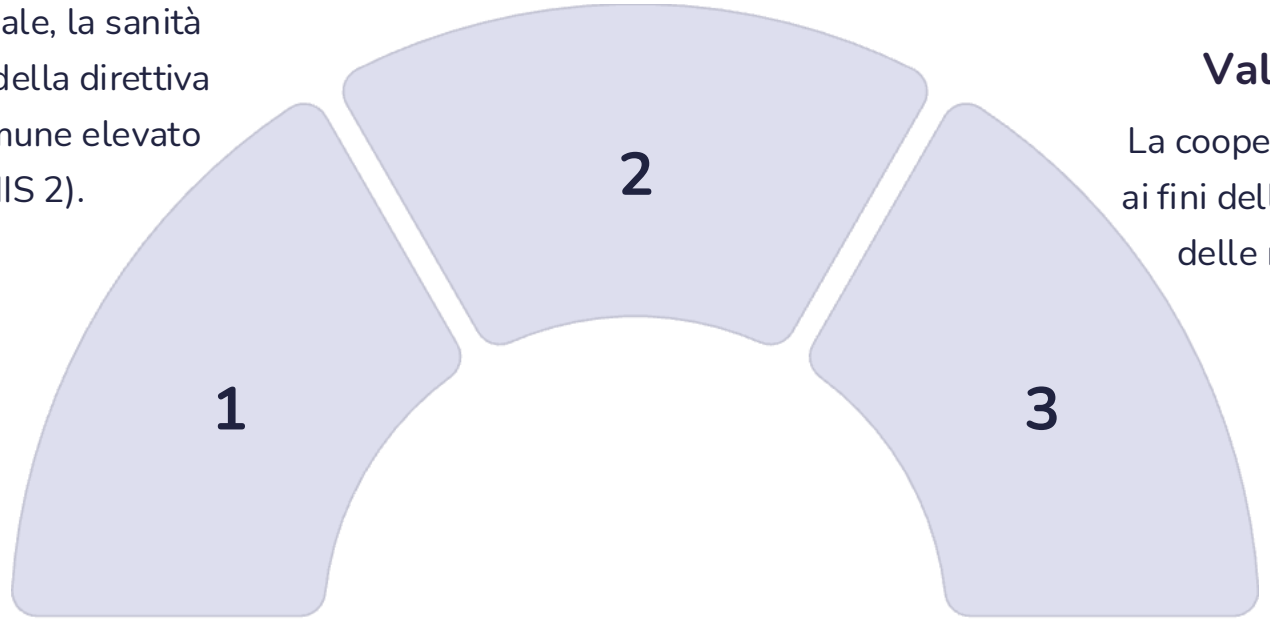
Cooperazione a livello europeo

Minacce transfrontaliere

I criminali informatici e altri autori delle minacce operano a livello transfrontaliero e anche le sfide in materia di cibersicurezza cui devono far fronte le organizzazioni sanitarie sono simili in tutti gli Stati membri.

Competenza nazionale

Per quanto la sicurezza dei sistemi sanitari sia in primo luogo di competenza nazionale, la sanità è anche un settore critico a norma della direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'UE (NIS 2).



Valore della cooperazione

La cooperazione a livello europeo è preziosa ai fini della condivisione e del potenziamento delle migliori pratiche a livello di UE e nazionale.

Focus del piano d'azione

Attuazione collaborativa

Cooperazione con prestatori di assistenza sanitaria, Stati membri e comunità della cibersicurezza

Dissuasione

Misure per dissuadere gli autori di minacce informatiche dal lanciare attacchi

Risposta e ripresa

Miglioramento della risposta agli incidenti e successiva ripresa

Rilevamento minacce

Miglioramento della condivisione delle informazioni e capacità di rilevare minacce

Prevenzione

Prevenzione degli incidenti di cibersicurezza, base fondamentale

La sfida della cibersicurezza degli ospedali

Minacce informatiche in aumento

Gli attacchi informatici sono in aumento a livello mondiale e all'interno dell'UE e il panorama delle minacce è sempre più complesso e dinamico. L'evoluzione dell'IA sta dotando i criminali e i malintenzionati di strumenti potenti per aumentare la precisione e l'impatto delle loro operazioni, ma ridefinisce nel contempo le possibilità di ciberdifesa rendendo possibile un'azione automatizzata e in tempo reale contro gli attacchi.

Il rischio dei ransomware

I ransomware continuano a rappresentare una sfida critica per la cibersicurezza nell'UE e a livello mondiale e una relazione ne stima il costo annuo globale a oltre 250 miliardi di EUR entro il 2031. Quando colpiscono, gli autori di attacchi ransomware non si limitano a criptare i dati delle vittime per chiedere un riscatto, ma rendono pubblico un numero gradualmente crescente di informazioni sensibili per esercitare ulteriore pressione.

1. Vulnerabilità nel settore sanitario

1

Incidenti legati a vulnerabilità

Seconda l'ENISA, l'assistenza sanitaria è il settore che ha dichiarato il maggior numero di incidenti di sicurezza connessi a vulnerabilità

2

Attacchi DDoS

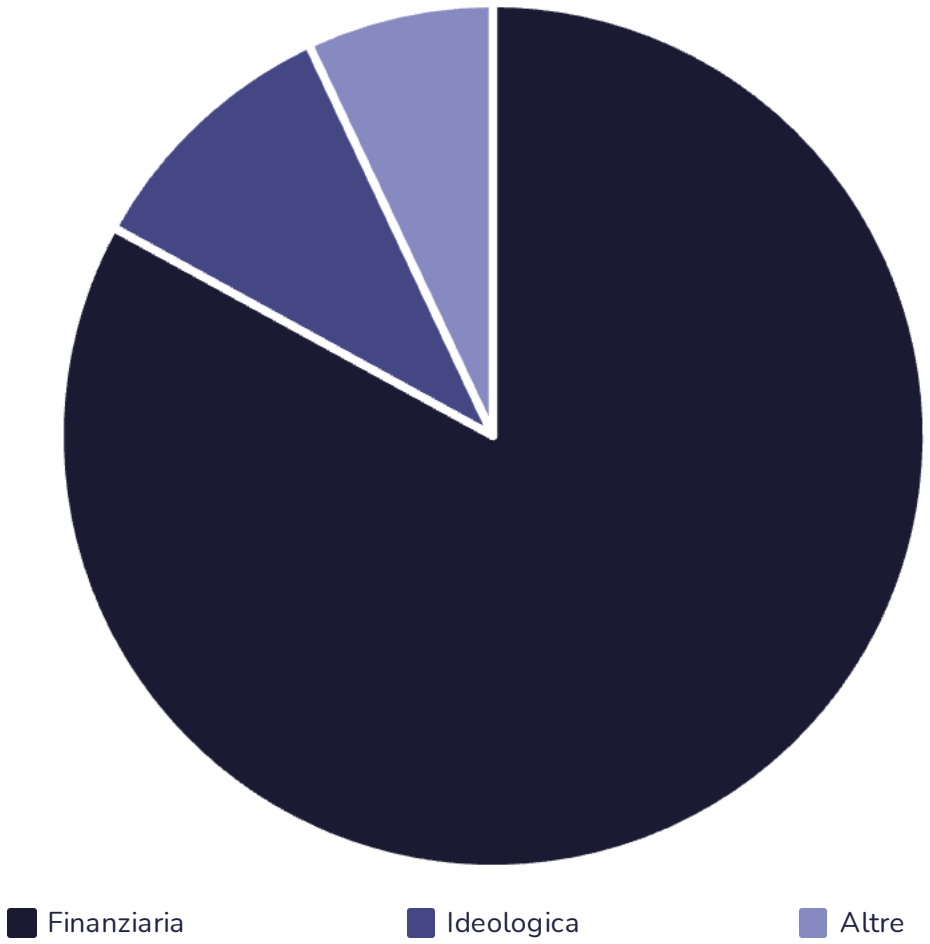
Minacce crescenti comprendono gli attacchi distribuiti di negazione del servizio (DDoS), concepiti per sovraccaricare il sistema preso di mira

3

Impatto dei ransomware

Secondo l'ENISA, nel periodo 2021-2023 i ransomware hanno rappresentato il 54% degli incidenti di cibersicurezza analizzati nel settore sanitario

Motivazioni degli attacchi informatici



L'83% degli attacchi aveva motivazione finanziaria, dato l'elevato valore dei dati sanitari, mentre il 10% degli attacchi nasceva da motivazioni ideologiche.

Analogamente, da una relazione della Commissione del 2024 emerge che il 71% degli attacchi che hanno avuto conseguenze sull'assistenza ai pazienti, quali ritardi nelle cure o nella diagnosi e difficoltà di accesso ai servizi di emergenza, erano del tipo ransomware.

Crescente digitalizzazione e rischi

Cartelle cliniche elettroniche

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 sanitaria di base.

Sistemi di diagnostica

I sistemi di diagnostica per immagini e i dispositivi medici utilizzati a fini diagnostici o di monitoraggio dei pazienti sono tutti esempi di strumenti digitali che possono avere un ruolo importante nel potenziare l'efficienza e le prestazioni del settore sanitario, ma sono anche obiettivi potenziali di un attacco alla cibersicurezza.

Settori vulnerabili

Attività specifiche di assistenza sanitaria, come la terapia intensiva e la radiologia per immagini, o settori medici come l'oncologia e la cardiologia, che dipendono fortemente da dispositivi basati sul digitale, sono particolarmente a rischio di attacchi informatici.

Esempio di attacco significativo

1

2

3

Inizio dell'attacco

Durante la pandemia di COVID-19, un attacco ransomware ha paralizzato ampie parti del sistema sanitario irlandese, causando in 31 dei 54 ospedali che offrono servizi quali pronto soccorso e terapia intensiva la cancellazione di almeno alcuni servizi la mattina dell'incidente.

Conseguenze immediate

I servizi sanitari hanno dovuto tornare ai registri cartacei, rallentando l'efficienza delle operazioni.

Origine dell'attacco

L'attacco proveniva da un'e-mail di phishing contenente un allegato dannoso.

STEFANELLI & STEFANELLI STUDIO LEGALE

Lezioni apprese dagli attacchi

Riconoscimento della minaccia

L'incidente ha dimostrato il potenziale degli attacchi informatici che si diffondono in diversi sistemi e, di conseguenza, l'importanza di proteggere l'intera superficie di attacco di un'organizzazione sanitaria.

Importanza dell'igiene informatica

L'attacco ha sottolineato l'importanza di garantire l'igiene informatica di base in tutte le organizzazioni sanitarie.

Necessità di una cultura della cibersicurezza

È fondamentale sviluppare una cultura della cibersicurezza in tutte le organizzazioni sanitarie per prevenire attacchi simili in futuro.

2. Maturità della cibersicurezza negli ospedali

Panorama eterogeneo

Il panorama sanitario dell'UE è molto eterogeneo: gli ospedali e gli altri prestatori di assistenza sanitaria presentano differenze significative in termini di proprietà, struttura e dimensioni nei vari Stati membri. La governance dell'assistenza sanitaria può essere basata su un approccio centralizzato in alcuni casi a livello nazionale, in altri a livello regionale e locale; la proprietà dei prestatori di assistenza sanitaria può essere pubblica o privata.

Disparità territoriali

Possono inoltre sussistere differenze anche all'interno dello stesso paese, ad esempio quando vi sono notevoli disparità socioeconomiche e territoriali tra le regioni, che danno vita a un quadro complesso. Questo panorama sanitario complesso può essere messo a dura prova da importanti crisi sanitarie dovute a malattie trasmissibili, come la pandemia di COVID-19, ma anche ad altri rischi sanitari, connessi ad esempio ai cambiamenti climatici.

Livelli di digitalizzazione e tecnologia

1 Frammentazione della tecnologia

Il livello di digitalizzazione e adozione della tecnologia da parte dei prestatori di assistenza sanitaria risulta notevolmente variabile e frammentato.

2 Rischi per strutture di piccole dimensioni

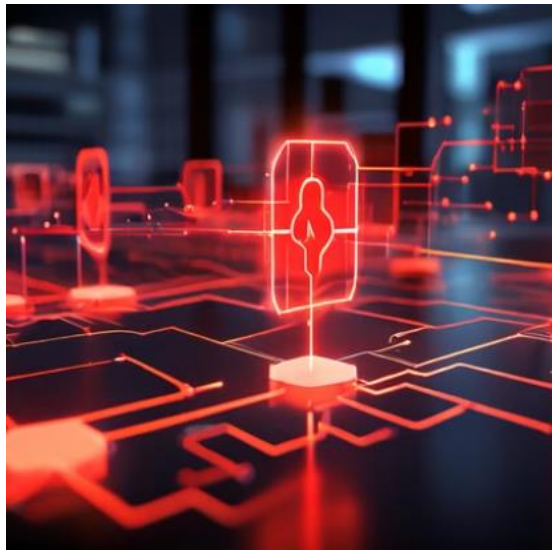
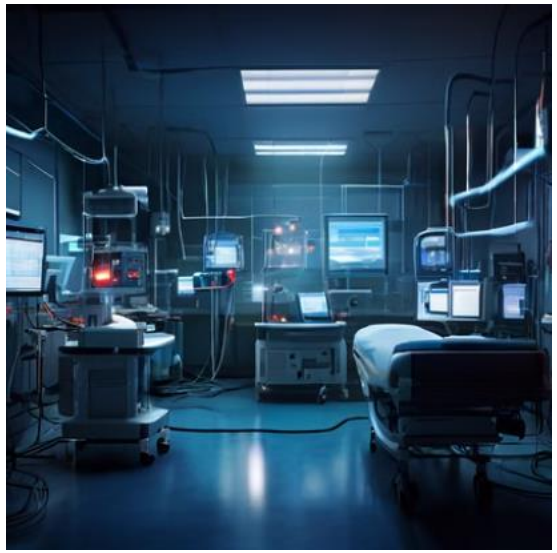
Il fatto che l'indisponibilità del servizio causata da un incidente di cibersicurezza possa causare gravi danni e pregiudizi ai pazienti anche in strutture sanitarie di piccole dimensioni, comprese cliniche o servizi medici di emergenza che forniscono un servizio essenziale a un numero relativamente basso di utenti, è un esempio della complessità sopra descritta.

3 Diversi livelli di maturità

Secondo la relazione dell'ENISA del 2024 sullo stato della cibersicurezza nell'Unione, la maturità del settore sanitario dell'UE è moderata e sussistono ampie differenze nel livello di maturità della cibersicurezza tra gli enti sanitari in Europa.

Carenze nella cibersicurezza



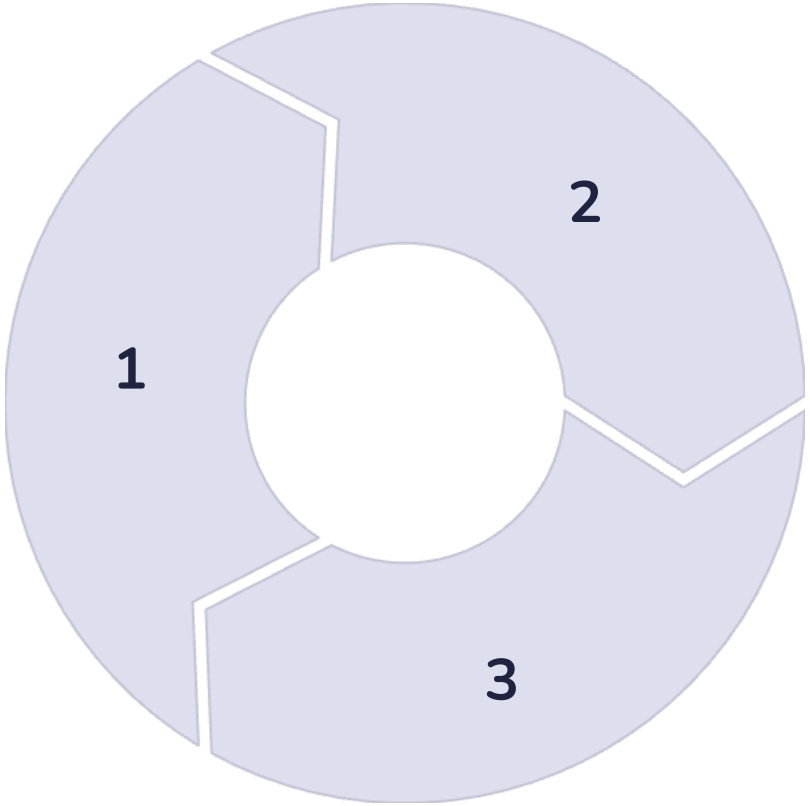



Sono emerse carenze in alcuni aspetti fondamentali, quali risorse umane sufficienti, conoscenza da parte delle organizzazioni delle loro catene di approvvigionamento delle tecnologie dell'informazione e della comunicazione (TIC) e installazione di elementi di sicurezza aggiornati nei prodotti. Il settore incontra difficoltà per quanto riguarda l'igiene informatica di base e le misure fondamentali di sicurezza, come dimostra il fatto che per quasi tutte le organizzazioni sanitarie prese in esame la realizzazione di valutazioni dei rischi di cibersicurezza rappresenta una sfida; pressoché la metà di tali organizzazioni non ha peraltro mai effettuato un'analisi dei rischi.

Sfide di interoperabilità IT/OT

Intersezione di tecnologie

Un'altra sfida significativa per la cibersicurezza degli ospedali è l'intersezione tra tecnologia dell'informazione (IT) e tecnologia operativa (OT)



Priorità divergenti

Si incontrano diverse priorità in materia di sicurezza per quanto riguarda la riservatezza, la disponibilità e l'affidabilità

Rischio di propagazione

Una violazione commessa in un settore in corrispondenza di detta intersezione può colpire anche l'altro settore

Sicurezza dei prodotti e formazione

Difficoltà nella gestione delle TIC

Nella relazione dell'ENISA del 2024 sullo stato della cibersicurezza nell'Unione si sottolinea inoltre che il settore sanitario non riesce a garantire in maniera adeguata la sicurezza dei prodotti e dei processi TIC che utilizza, a causa della grande varietà di entità, dispositivi e prodotti sanitari.

Scarsa formazione del personale

Detta varietà, associata a livelli variabili di consapevolezza informatica tra il personale ospedaliero e la dirigenza, rende il compito di garantire la cibersicurezza dei sistemi sanitari una sfida complessa. Secondo l'Eurobarometro del 2024 sulle competenze informatiche, ad esempio, solo il 25% delle imprese oggetto dell'indagine nel settore della sanità, dell'istruzione e dell'assistenza sociale aveva fornito formazione o svolto attività di sensibilizzazione in materia di cibersicurezza nei 12 mesi precedenti.

Fonti di vulnerabilità specifiche

57%

Esternalizzazione

Dall'Eurobarometro del 2024 è emerso che nei settori della sanità, dell'istruzione e dell'assistenza sociale si registra la percentuale più elevata di imprese che esternalizzano almeno alcuni aspetti della loro cibersicurezza.

58%

Uso del cloud

Nel 2022 il 58% delle organizzazioni sanitarie ha utilizzato una piattaforma sanitaria digitale basata sul cloud. Tale cambiamento tuttavia, pur essendo in grado di apportare efficienze significative, comporta anche rischi che richiedono decisioni informate in materia di appalti e configurazione sicura.

8.3%

Spesa per sicurezza

Secondo l'ENISA il settore sanitario occupa solo il 7° posto tra i 12 settori esaminati per quanto riguarda la percentuale della spesa per la sicurezza delle informazioni sul totale della spesa informatica: la media nel settore sanitario è pari all'8,3%.

STEFANELLI & STEFANELLI STUDIO LEGALE

proposta del Piano d'azione

CENTRO EUROPEO DI SOSTEGNO ALLA CIBERSICUREZZA

EUROPEAN CYBERSECURITY COMPETENCE CENTRE - ECCC

Centro europeo di sostegno alla cibersicurezza

Approccio strategico unificato

Il quadro dell'UE in materia di cibersicurezza offre un'ampia gamma di strumenti che dovrebbero essere sfruttati per migliorare la sicurezza e la resilienza degli ospedali e dei prestatori di assistenza sanitaria. Per far fronte alle numerose sfide sopra evidenziate, è necessario sviluppare un approccio strategico unificato a livello di UE, che riunisca le risorse, le competenze e gli strumenti necessari per affrontare efficacemente le minacce informatiche.

Ruolo dell'ENISA

L'ENISA si trova a tal fine nella posizione migliore per istituire, all'interno della sua organizzazione, un apposito centro europeo di sostegno alla cibersicurezza per ospedali e prestatori di assistenza sanitaria nell'ambito del suo mandato di salvaguardare e sostenere le infrastrutture critiche dell'UE.

sviluppo di un Catalogo dei servizi del centro di sostegno

Servizio	Descrizione
Catalogo completo	Il centro di sostegno dovrebbe progressivamente sviluppare un catalogo completo dei servizi che risponda alle esigenze degli ospedali e dei prestatori di assistenza sanitaria, delineando la gamma di servizi disponibili a fini di preparazione, prevenzione, rilevamento e risposta.
Archivio di strumenti	In collaborazione con le autorità degli Stati membri e attingendo alle esperienze degli ospedali e dei prestatori di assistenza sanitaria, il centro di sostegno dovrebbe sviluppare un archivio di facile accesso e di facile utilizzo di tutti gli strumenti disponibili a livello europeo, nazionale e regionale.
Coordinamento con Stati membri	Nello svolgimento delle sue attività il centro dovrebbe garantire un coordinamento adeguato con gli Stati membri e contribuire alla definizione delle priorità riguardo alle azioni e alla loro realizzazione, secondo necessità, in tempo reale.

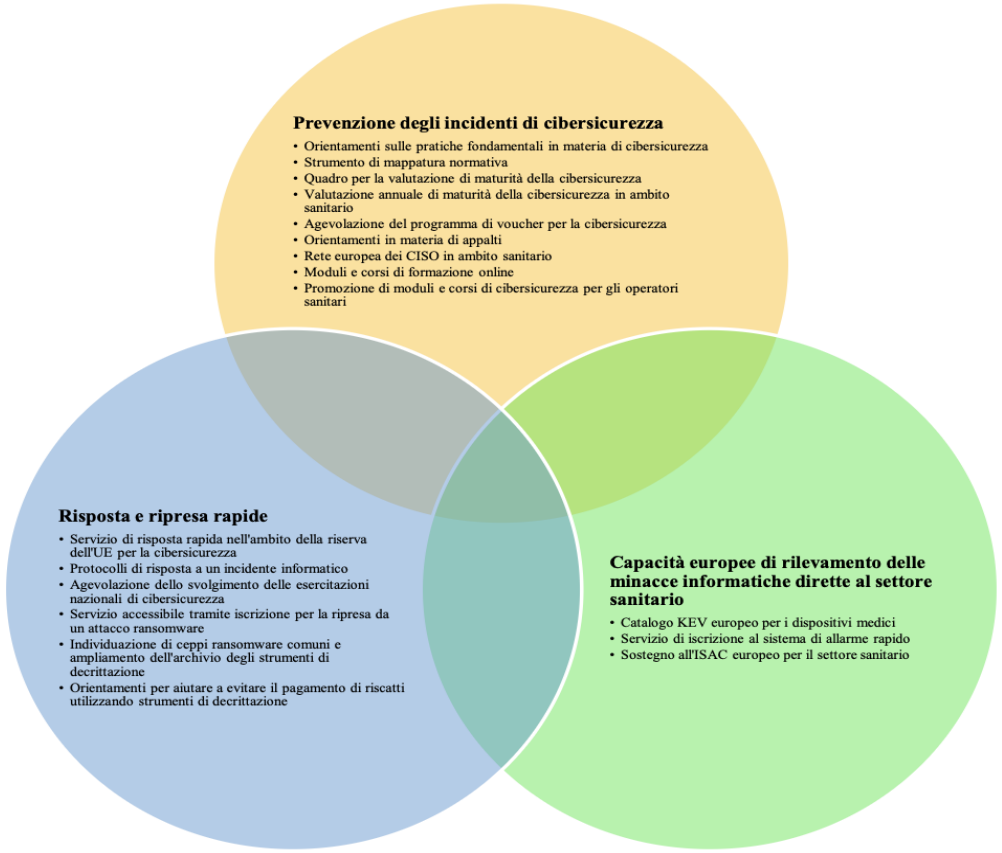


Figura 1: concetti per il catalogo dei servizi del centro di sostegno per ospedali e prestatori di assistenza sanitaria

- **prevenzione incidenti sicurezza**
- **risposte e ripresa rapida**
- **capacità di rilevamento minacce**

Progetti pilota per sviluppo del catalogo

Approccio basato su progetti pilota

Quale importante elemento costitutivo per lo sviluppo del catalogo dei servizi del centro di sostegno, la Commissione proporrà di avviare progetti pilota in tutta l'UE per elaborare le migliori pratiche di igiene informatica e di valutazione dei rischi di sicurezza, come pure per far fronte alla necessità di un monitoraggio continuo della cibersicurezza, di intelligence sulle minacce e di una risposta agli incidenti che si avvalga di soluzioni di cibersicurezza all'avanguardia.

Finanziamento e realizzazione

I risultati di tali progetti pilota, che saranno finanziati dal programma Europa digitale e realizzati dal Centro europeo di competenza per la cibersicurezza (European Cybersecurity Competence Centre, ECCC), orienteranno azioni ulteriori a livello di UE, compreso il lavoro del centro di sostegno.

1. PREVENZIONE DEGLI INCIDENTI DI CIBERSICUREZZA

STEFANELLI & STEFANELLI STUDIO LEGALE

1

Azioni semplici ma efficaci

Secondo una stima le misure di cibersicurezza di base, quali l'aggiornamento costante dei sistemi, la gestione dei backup e l'implementazione dell'autenticazione a più fattori, possono proteggere le organizzazioni dal 98% degli attacchi.

Molte delle misure più incisive in materia di igiene informatica e gestione dei rischi sono relativamente semplici da adottare e sono pertanto un obiettivo di facile conseguimento per migliorare la cibersicurezza.

2

Orientamenti mirati

Uno dei ruoli chiave del centro di sostegno dovrebbe pertanto essere l'elaborazione di orientamenti chiari e mirati che diano risalto alle pratiche fondamentali in materia di cibersicurezza e aiutino i prestatori di assistenza sanitaria ad attuarle.

Tale sostegno non deve limitarsi ai grandi ospedali, ma prevedere anche consulenze personalizzate per gli enti di dimensioni inferiori, come gli ambulatori locali dei medici generalisti e le cliniche specializzate.

3

Conformità normativa semplificata

Uno strumento di mappatura normativa di facile accesso può contribuire a ridurre al minimo gli oneri amministrativi per gli enti soggetti a molteplici strumenti normativi. Oltre a elaborare orientamenti e strumenti, il centro di sostegno dovrebbe collaborare a stretto contatto con la Commissione e con gli Stati membri per sviluppare e diffondere quanto prima il suddetto strumento.

Portafogli europei di identità digitale

1

Identificazione sicura

I futuri portafogli europei di identità digitale sono un altro strumento inteso a facilitare la semplice attuazione di buone pratiche di igiene informatica. Ridurre il ricorso a meccanismi di identificazione deboli, come le password, è essenziale per attenuare i rischi di accesso non autorizzato ai dati sanitari.

2

Soluzione armonizzata

Il portafoglio di identità digitale dell'UE offre un approccio armonizzato a livello di UE all'identificazione elettronica per gli operatori sanitari, fornendo una soluzione robusta e unificata a partire dalla fine del 2026.

3

Obblighi di implementazione

Per tutti i sistemi di informazione sanitaria online tenuti a implementare l'autenticazione forte dell'utente vigerà l'obbligo di accettare il portafoglio a fini di identificazione a partire dalla fine del 2027.

1a. Preparazione e sostegno mirato

Verifica della preparazione

La verifica della preparazione, che prevede azioni quali i penetration test è una pietra angolare di una cibersicurezza efficace e la Commissione ha già stanziato finanziamenti all'ENISA per iniziative pilota di preparazione, dalle quali è emerso che il settore sanitario è uno dei settori in cui è più elevata la richiesta di test e di ulteriori valutazioni per individuare le lacune nella maturità della cibersicurezza.

Quadro di valutazione

Il centro di sostegno dovrebbe elaborare un quadro su misura per le valutazioni di maturità della cibersicurezza specifico per l'assistenza sanitaria. Tali valutazioni di maturità fornirebbero ai soggetti conoscenze utili sulle loro vulnerabilità, consentendo loro nel contempo di dimostrare ai pazienti e ai portatori di interessi la loro preparazione in materia di cibersicurezza e consolidando così la fiducia nei loro servizi.

Voucher per la cibersicurezza

Sulla base di iniziative efficaci quali i voucher per l'innovazione dell'UE, gli Stati membri dovrebbero prendere in considerazione misure mirate come i voucher per la cibersicurezza per le micro, piccole e medie strutture ospedaliere e di prestazione di assistenza sanitaria.
Tali voucher fornirebbero un'assistenza finanziaria ai fini dell'attuazione di specifiche misure di cibersicurezza.

1b. Sicurezza delle catene di approvvigionamento




Una sfida fondamentale per le organizzazioni sanitarie è la gestione di complesse catene di approvvigionamento delle TIC, che riguardano una serie di prodotti quali dispositivi medici connessi, sistemi per le cartelle cliniche elettroniche e hardware per gli uffici. Gli ospedali e i prestatori di assistenza sanitaria necessitano di sistemi e servizi TIC affidabili e sicuri per il loro funzionamento. Per contribuire ad affrontare le sfide di cibersicurezza nel settore sanitario, il gruppo di cooperazione NIS dovrebbe effettuare una valutazione coordinata dei rischi per la sicurezza, valutando i rischi sia tecnici che strategici connessi alle catene di approvvigionamento dei dispositivi medici e proponendo misure di attenuazione.

1c. Formazione e sviluppo delle competenze

Carenza di professionisti

Disporre di personale dotato delle competenze più richieste è importante per la crescita sostenibile e la competitività a lungo termine in Europa, come anche per offrire servizi di alta qualità, compresi i servizi sanitari. La carenza di professionisti della cibersicurezza qualificati rappresenta una sfida significativa in tutta Europa; si stima che manchino 299.000 professionisti per soddisfare le esigenze di personale dell'UE nel settore.

Difficoltà di assunzione

Secondo l'Eurobarometro del 2024 sulle competenze in materia di cibersicurezza, l'81% delle imprese ritiene che le difficoltà nell'assunzione di personale addetto alla cibersicurezza costituiscano un rischio fondamentale per potenziali attacchi informatici. Nei settori dell'istruzione, della sanità e dell'assistenza sociale, il 66% dei ruoli di cibersicurezza è ricoperto da dipendenti che vengono da posizioni non legate alla cibersicurezza, il che evidenzia l'urgente necessità di riqualificazione e miglioramento del livello delle competenze.

Accademia per le competenze

Per affrontare questa sfida, il centro di sostegno dovrebbe collaborare con il futuro consorzio per l'infrastruttura digitale europea (EDIC) per le competenze in materia di cibersicurezza, previsto nella comunicazione della Commissione sull'Accademia per le competenze in materia di cibersicurezza.

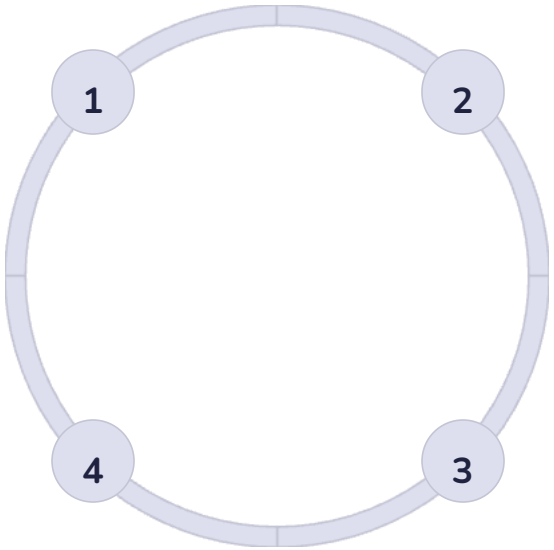
2. CAPACITÀ EUROPEE DI RILEVAMENTO DELLE MINACCE NEL SETTORE SANITARIO

Monitoraggio continuo

Un rilevamento efficace delle minacce informatiche è essenziale per una risposta rapida agli incidenti.
Gli autori delle minacce possono sfruttare tecniche volte a rendere le intrusioni difficili da rilevare, che consentono l'accesso non autorizzato a un sistema per periodi di tempo prolungati.

Sistema di allarme rapido

Per affrontare le sfide significative dell'individuazione delle minacce, il centro di sostegno dovrebbe introdurre un servizio di allarme rapido a livello di UE per il settore sanitario accessibile tramite iscrizione, che fornisca allerte in tempo quasi reale.



Condivisione delle informazioni

Una condivisione delle informazioni e una collaborazione efficienti sono essenziali per migliorare il rilevamento delle minacce e la conoscenza situazionale nell'UE.
I gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) svolgono un ruolo fondamentale nel ricevere segnalazioni di incidenti, quasi incidenti e potenziali minacce, offrendo orientamenti sulle misure di attenuazione a livello nazionale.

Catalogo delle vulnerabilità

Una volta che le informazioni contenute nelle relazioni non saranno più sensibili, il centro di sostegno potrebbe creare un catalogo europeo, sponsorizzato dall'ENISA, delle vulnerabilità note sfruttate per i dispositivi medici, i sistemi di cartelle cliniche elettroniche e i fornitori di apparecchiature e software TIC nel settore sanitario.

3. RISPOSTA E RIPRESA RAPIDE

STEFANELLI & STEFANELLI STUDIO LEGALE

24h

Tempo di risposta

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 cibersicurezza è fondamentale per salvaguardare la sicurezza dei pazienti. Quando un ospedale o un prestatore di assistenza sanitaria si trova di fronte a un attacco informatico, il primo punto di contatto è il CSIRT nazionale pertinente. Il CSIRT ha il compito di fornire un sostegno tempestivo, idealmente entro 24 ore, per contribuire alla gestione degli incidenti significativi.

art. 23 NIS 2 – OBBLIGO DI NOTIFICA

EU

EU Cybersecurity Reserve

La EU Cybersecurity Reserve per la cibersicurezza, istituita a norma del'art. 14 Regolamento sulla Cibersolidarietà, prevede servizi di risposta agli incidenti erogati da fornitori di fiducia di servizi di sicurezza gestiti per fornire assistenza in caso di incidenti di cibersicurezza significativi o su vasta scala e negli sforzi di ripresa iniziali.

0

Servizio di risposta rapida

Per rafforzare tale sistema, la Commissione e l'ENISA dovrebbero garantire che la riserva comprenda un servizio di risposta rapida specifico per il settore sanitario.

In complementarità con altri quadri esistenti, tale servizio consentirebbe di inviare esperti per gestire tempestivamente incidenti di cibersicurezza significativi o su vasta scala nel settore dell'assistenza sanitaria, quando il sostegno nazionale è insufficiente.

AZIONI A LIVELLO NAZIONALE

STEFANELLI & STEFANELLI STUDIO LEGALE

Centri nazionali di sostegno

La capacità del presente piano d'azione di migliorare la cibersicurezza 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 sostegno alla cibersicurezza dedicati specificamente agli ospedali e ai prestatori di assistenza sanitaria. Tali centri costituirebbero i punti di contatto primari per il settore sanitario a livello nazionale, collaborando strettamente con il centro di sostegno dell'ENISA.

Piani d'azione nazionali

Gli Stati membri sono inoltre incoraggiati a elaborare piani d'azione nazionali incentrati sulla cibersicurezza nel settore sanitario. Tali piani dovrebbero delineare i rischi di cibersicurezza specifici cui sono esposti i sistemi sanitari e le azioni nazionali intraprese per affrontarli, garantendo nel contempo che le risorse e le pratiche a livello europeo siano utilizzate in modo efficace.

Condivisione delle risorse

Un altro obiettivo fondamentale per gli Stati membri è facilitare la condivisione delle risorse tra i prestatori di assistenza sanitaria, che potrebbe essere conseguita mediante appalti congiunti o la messa in comune di risorse a livello regionale, nazionale o persino europeo. Tale approccio ridurrebbe l'onere finanziario per i singoli soggetti, aumentando nel contempo il loro potere contrattuale con i fornitori di servizi di cibersicurezza.

Cooperazione pubblico-privato

La cooperazione pubblico-privato e la consultazione con i prestatori di assistenza sanitaria, gli altri soggetti del settore sanitario e i pertinenti operatori del settore della cibersicurezza sono essenziali per l'efficace attuazione del piano d'azione.

Per contribuire ulteriormente ai lavori del centro di sostegno, la Commissione, con il sostegno dell'ENISA, istituirà un comitato consultivo comune per la cibersicurezza del settore sanitario con rappresentanti di alto livello dei settori dell'assistenza sanitaria e della cibersicurezza, che potrà fornire consulenza alla Commissione e al centro di sostegno su azioni incisive e discuterà l'ulteriore sviluppo di partenariati pubblico-privato in questo campo.

Scoraggiare gli autori delle minacce informatiche

STEFANELLI & STEFANELLI STUDIO LEGALE

Politiche di deterrenza

Le politiche interne ed esterne dell'UE in materia di cibersicurezza dovrebbero sostenere l'obiettivo di scoraggiare gli autori delle minacce informatiche dall'attaccare i sistemi sanitari europei.

Strumenti diplomatici

Il pacchetto di strumenti della diplomazia informatica 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 l'attuale quadro di sanzioni contro gli attacchi informatici per rispondere alle minacce rivolte ai sistemi sanitari.

Responsabilità criminale

Far sì che i criminali siano ritenuti responsabili delle loro azioni costituisce un importante deterrente. Gli Stati membri dovrebbero quindi garantire che le attività di contrasto siano pienamente integrate nei rispettivi piani d'azione nazionali.

PROSSIME TAPPE

STEFANELLI & STEFANELLI STUDIO LEGALE

1 Definizione dell'agenda

La presente comunicazione definisce un'agenda ambiziosa per una maggiore cibersicurezza del settore sanitario dell'UE.

2 Istituzione del Centro di Sostegno

Proponendo l'istituzione di un centro di sostegno alla cibersicurezza per gli ospedali e i prestatori di assistenza sanitaria nel cuore dell'ENISA, il piano d'azione traccia la strada verso la definizione di un approccio europeo coerente e condiviso alle sfide di cibersicurezza in tale settore.

3 Consultazioni e scambi

L'adozione del piano d'azione sarà pertanto accompagnata dall'avvio di ampie consultazioni dei portatori di interessi e dal proseguimento degli scambi con gli Stati membri e le reti pertinenti per raccogliere informazioni.

4 Raccomandazioni future

Sulla base dei risultati delle consultazioni, la Commissione intende presentare raccomandazioni nel quarto trimestre del 2025, al fine di perfezionare ulteriormente il piano d'azione.

La presente comunicazione dovrebbe essere considerata l'inizio di un processo volto a migliorare la cibersicurezza nel settore sanitario.
L'adozione del piano d'azione sarà pertanto accompagnata dall'avvio di ampie consultazioni dei portatori di interessi 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, al fine di perfezionare ulteriormente il piano d'azione.

LE NOSTRE RISORSE ONLINE:

www.studiolegalestefanelli.it

https://privacygdpr.it/

https://www.medicaldevicenews.eu/

Osservatorio europeo della privacy

Osservatorio sanzioni privacy

Rubrica ricerca scientifica e privacy

Rubrica e raccolta fonti normative sull'IA

Rubrica DM in collaborazione con Aboutpharma

Osservatorio europeo DM

GRAZIE DELL' ATTENZIONE!

Restiamo a Vostra disposizione
contattateci su:

info@studiolegalestefanelli.it

O su

Linkedin