



III Convegno Nazionale SITLaB
7 - 8 giugno 2025 - Chieti

SITLaB
Società Scientifica Italiana dei TSLB



DIGITALIZZAZIONE E CYBERMINACCE: LA NUOVA SFIDA PER LA SANITÀ PUBBLICA

Di Padova Emily (ASL Lanciano Vasto Chieti), Di Donato Tiziano (AUSL Pescara), Esposito Elena (A.O.R.N. Caserta), Mariniello Alessia (AUSL Modena)

INTRODUZIONE.

Come ogni tecnologia potente, l'intelligenza artificiale (IA) offre numerosi vantaggi ma presenta anche sfide e rischi significativi. In ambito cybercrime, i criminali informatici hanno iniziato a sfruttare i sistemi di intelligenza artificiale come armi sofisticate per sferrare attacchi sempre più efficaci, convincenti e personalizzati. Parallelamente, i sistemi di intelligenza artificiale si stanno affermando solidi alleati nella lotta contro il crimine informatico grazie alla capacità di analizzare grandi volumi di dati, individuare schemi sospetti e rispondere in tempo reale alle minacce. Tuttavia, l'IA da sola non è sufficiente. In Italia, con il Decreto Legge n.82 del 14 Giugno 2021, è stata istituita l'**Agenzia per la Cybersicurezza Nazionale (ACN)**, l'Autorità responsabile della tutela degli interessi nazionali nel campo della sicurezza cibernetica. L'ACN svolge un ruolo chiave nella protezione delle infrastrutture digitali critiche, promuovendo attività formative e campagne di sensibilizzazione al rischio rivolte ai cittadini e alle istituzioni, con l'obiettivo di sviluppare nuove competenze informatiche. Una recente indagine dell'ACN ha evidenziato che **il settore della Sanità è il terzo più colpito da attacchi informatici**, con una frequenza crescente di tentativi riusciti. Questi sono dovuti principalmente alla scarsa implementazione o alla mancanza di conoscenza delle pratiche di sicurezza a livello gestionale. La Sanità è un bersaglio molto attraente per i criminali informatici considerando l'alto valore simbolico, oltre che economico, dei dati sanitari che sono tra i più sensibili fra quelli circolanti. Tali informazioni vengono spesso rivendute nel «dark web» e utilizzate per frodi assicurative, estorsioni e furti d'identità, rappresentando una fonte di ricchezza inestimabile per gli hacker. A partire da Gennaio 2022, in Italia si sono verificati mediamente 2,6 eventi cyber malevoli al mese contro le strutture sanitarie. Circa la metà di questi ha avuto conseguenze tangibili, compromettendo l'erogazione dei servizi sanitari e incidendo su disponibilità, riservatezza ed integrità dei dati clinici. (Figura 1)

OBIETTIVI.

Il settore sanitario italiano si trova di fronte ad una crescente minaccia cibernetica e non è difficile percepire la gravità della situazione e l'urgenza di trovare soluzioni adeguate. Il presente lavoro si propone di individuare le principali aree di fragilità del sistema, offrendo una mappatura dei punti strategici su cui intervenire per potenziare la resilienza digitale delle infrastrutture sanitarie e promuovere un approccio più solido e integrato alla sicurezza informatica.



«hack me, if you can!»

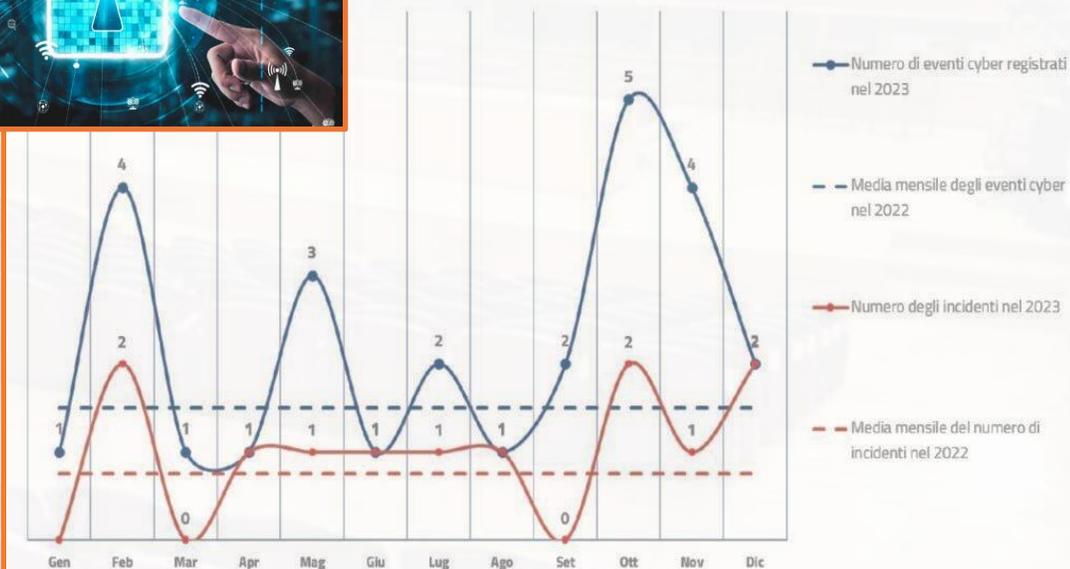


Figura 1: eventi cyber e incidenti nel settore sanitario nel 2023 rispetto alla media mensile dell'anno precedente

Figura 1.



III Convegno Nazionale SITLaB 7 - 8 giugno 2025 - Chieti

SITLaB
Società Scientifica Italiana dei TSLB



MATERIALI E METODI.

La complessità del settore sanitario nasce dall'interazione tra componenti tecnologiche, organizzative e umane, la cui interdipendenza incide profondamente sul funzionamento del sistema. Questa multidimensionalità complica la gestione della sicurezza informatica, aumentando la vulnerabilità delle infrastrutture digitali. Tra le criticità principali emerge **l'obsolescenza dei sistemi e delle tecnologie impiegate**: molte apparecchiature risultano inadeguate a sostenere il ritmo incalzante dell'innovazione in ambito di cybersicurezza. L'uso di hardware e software datati ostacola l'applicazione tempestiva di aggiornamenti e patch correttive, lasciando aperte falle note e facilmente sfruttabili dai cybercriminali. A questo si aggiunge la **scarsa formazione del personale sanitario**, spesso impreparato ad affrontare i rischi digitali ed inconsapevolmente esposto alle tecniche di ingegneria sociale che sfruttano l'errore umano come varco d'accesso. Un'ulteriore fragilità è rappresentata dalla **gestione decentralizzata dei sistemi informatici**: l'assenza di una governance centrale genera un ecosistema eterogeneo e privo di standard condivisi, ampliando la superficie d'attacco e rendendo difficile l'attuazione di strategie di sicurezza coerenti ed unitarie. Le più recenti analisi di cybersecurity hanno tracciato un quadro chiaro dei principali vettori di attacco informatico che hanno colpito il settore sanitario nel biennio 2022-2023. (Figura 2)

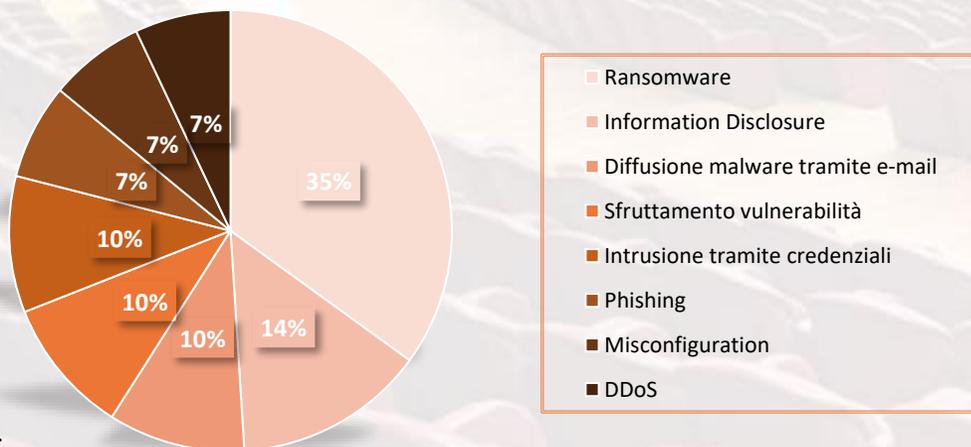


Figura 2.

RISULTATI.

Gli attacchi informatici non compromettono solo la riservatezza dei dati sensibili, ma minano alla radice il rapporto di fiducia tra i cittadini e il Sistema Sanitario. Quando le strutture sanitarie non riescono a garantire un'adeguata protezione delle informazioni personali, la credibilità dell'intero ecosistema sanitario viene messa in discussione, alimentando un clima di crescente diffidenza e scetticismo tra la popolazione. Le conseguenze possono essere devastanti, con danni reputazionali irreparabili per le strutture coinvolte che rischiano di perdere il sostegno della collettività. L'accesso illecito ai sistemi informatici può determinare una paralisi temporanea o un rallentamento significativo dei processi clinici, ostacolando il regolare flusso operativo delle strutture sanitarie. Questi disservizi compromettono la qualità e l'efficacia delle prestazioni erogate, esponendo a serio pericolo la vita dei pazienti. Inoltre, le violazioni della sicurezza dei dati personali comportano gravi implicazioni legali per le strutture coinvolte, con sanzioni severe e possibili obblighi di risarcimento per i pazienti danneggiati. A seguito di un attacco informatico, le risorse normalmente destinate a garantire la continuità dei servizi sanitari essenziali vengono dirottate verso la gestione della crisi. Questa riallocazione delle risorse compromette la capacità del sistema sanitario di fronteggiare le numerose emergenze sanitarie che si presentano quotidianamente. Di fatto, l'organizzazione sanitaria si allontana dalla sua missione primaria con il concreto rischio che vengano compromessi sia la tempestività che la validità delle risposte alle urgenti necessità di salute dei pazienti.

Quali dati devono essere protetti?

- Cartelle cliniche elettroniche e Fascicolo Sanitario Elettronico
- Referti, analisi di laboratorio, immagini diagnostiche
 - Dati anagrafici e assicurativi dei pazienti
- Dispositivi sanitari collegati ad una rete (IoMT)



III Convegno Nazionale SITLaB 7 - 8 giugno 2025 - Chieti

SITLaB
Società Scientifica Italiana dei TSLB



DISCUSSIONI E CONCLUSIONI.

La digitalizzazione del settore sanitario apre a straordinarie opportunità in termini di efficienza, accessibilità e qualità dei servizi; tuttavia, espone anche a minacce informatiche sempre più evolute, in particolare agli attacchi ransomware, che possono bloccare interi sistemi informatici e rendere inaccessibili dati clinici vitali. Perché l'innovazione tecnologica possa davvero tradursi in benefici concreti e duraturi, è fondamentale affiancarla ad una strategia di cybersecurity solida e ben articolata, costruita in modo condiviso e capace di coinvolgere l'intero ecosistema sanitario: dai professionisti IT al personale sanitario, fino ai vertici istituzionali. Le vulnerabilità, infatti, non si limitano ai sistemi tecnologici, ma si annidano anche nei comportamenti umani, nelle prassi organizzative obsolete e nella scarsa consapevolezza dei rischi. Diventa quindi essenziale investire in una vera e propria **«cultura della cybersicurezza»**. (Figura 3) In questo scenario, la sicurezza informatica non può più essere relegata ad un aspetto tecnico marginale, ma deve affermarsi come un pilastro strategico dell'organizzazione sanitaria, al pari della qualità delle cure e della sostenibilità economica. Solo così sarà possibile trasformare l'innovazione digitale da potenziale punto di vulnerabilità a motore di crescita per una sanità moderna, sicura e resiliente. Sul piano normativo, il percorso verso una sanità digitale sicura richiede un quadro legislativo chiaro e coerente. In Europa, il riferimento principale è il Regolamento Generale sulla Protezione dei Dati (GDPR), che riconosce i dati sanitari come *«sensibili»* e vieta il loro trattamento salvo casi specifici, come il consenso esplicito dei pazienti. Le strutture sanitarie devono adottare misure tecniche e organizzative adeguate per tutelare i dati, riducendo al minimo i rischi di accesso non autorizzato.

La Direttiva NIS2 (Network and Information Systems Security), approvata dall'UE nel 2022, include ospedali, cliniche e altre strutture sanitarie tra gli *«operatori di servizi essenziali»*, imponendo l'adozione di tecnologie avanzate di protezione e l'implementazione di politiche di gestione proattiva del rischio. Ciò significa che le strutture devono monitorare costantemente reti e sistemi per identificare tempestivamente le vulnerabilità e neutralizzare le minacce prima che possano causare danni. La direttiva introduce anche l'obbligo di notifica degli incidenti informatici entro 24 ore, così da consentire una risposta rapida e coordinata da parte delle autorità competenti. Tra queste ricordiamo il CSIRT (Computer Security Incident Response Team), hub di riferimento nazionale per la gestione delle segnalazioni, in grado di fornire supporto ai soggetti impattati. La ISO/IEC 27000 è una famiglia di standard internazionali fondamentali per la gestione della sicurezza delle informazioni, in particolare nel settore sanitario. La norma ISO/IEC 27001 definisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS), che aiuta le strutture sanitarie a proteggere i dati da accessi non autorizzati. Accanto ad essa, la norma ISO/IEC 27002 fornisce linee guida operative per implementare le misure di protezione, mentre la norma ISO/IEC 27005 si concentra sull'analisi e gestione del rischio, essenziale per mitigare le vulnerabilità. Difendere gli ospedali dalle minacce informatiche va oltre una semplice sfida tecnologica: è un dovere etico, sociale e umano. Non si tratta solo di proteggere dati personali o infrastrutture digitali, ma di garantire la continuità delle cure, la fiducia nei servizi sanitari, e in ultima analisi, la salvaguardia della vita stessa. Ogni violazione non colpisce soltanto un sistema informatico, ma intacca il cuore di un'istituzione che ha il compito di prendersi cura delle persone nei momenti più fragili. Un ospedale sicuro non è solo un luogo più efficiente, ma è un rifugio affidabile, dove ogni paziente deve sentirsi tutelato non solo fisicamente, ma anche nel rispetto della propria identità e riservatezza.

Figura 3.



In caso di incidente, compilare il modulo
disponibile sul sito del CSIRT Italia



BIBLIOGRAFIA.

- «I sistemi di intelligenza artificiale come strumento di supporto alla diagnostica», Ministero della Salute, Consiglio Superiore di Sanità sezione V – novembre 2021
- La minaccia cibernetica al settore sanitario, analisi e raccomandazioni gennaio 2022 - dicembre 2024, Agenzia per la Cybersicurezza Nazionale