La fragilità della sanità digitale: crescita degli attacchi, nuovi rischi dall'IA e un perimetro sempre più esteso

[A cura di Sonia Montegiove, Manuela Santini, Sofia Scozzari e Anna Vaccarelli - Women For Security]

Lo scenario e le sfide

Negli ultimi anni la sanità è stata al centro di una trasformazione digitale profonda che, pur portando vantaggi indiscutibili in termini di efficienza clinica e qualità delle cure, ha anche esposto il settore a una pressione crescente delle minacce informatiche. Le strutture sanitarie - dagli ospedali pubblici alle cliniche private, dai servizi territoriali alle piattaforme di telemedicina - gestiscono oggi enormi volumi di dati sensibili, sistemi critici e servizi digitali interconnessi che rappresentano bersagli sempre più attraenti per gli attaccanti. Nel 2025, queste dinamiche si sono tradotte in un sensibile aumento degli incidenti cyber, sia in termini di frequenza sia di impatto operativo e organizzativo, come dimostrano i dati che presentiamo qui. Il campione di riferimento[1] comprende esclusivamente cyber attacchi andati a buon fine, che derivano dal monitoraggio continuativo di migliaia di fonti eterogenee, tra cui fonti aperte (OSINT), Dark Web, canali social e forum specializzati. Ogni evento viene classificato secondo tassonomie allineate agli standard internazionali e ai principali framework di cybersecurity, garantendo coerenza metodologica e comparabilità delle analisi.
I dati nazionali e internazionali evidenziano che nel 2025 sono stati registrati attacchi ai danni di strutture sanitarie, con un incremento significativo rispetto agli anni precedenti (vedi **fig.1**). Questa crescita non è soltanto statistica: riflette l'espansione della **superficie di attacco**, cioè l'insieme di sistemi, dispositivi, connessioni e identità che possono essere potenzialmente sfruttati dai criminali informatici.

Tra le tendenze rilevate per il 2025 si nota l'evoluzione delle **motivazioni e delle tecniche di attacco**. Se in passato il cybercrime finalizzato al profitto (ransomware, furto di dati) era predominante, recentemente si osserva anche un aumento degli attacchi di natura ideologica o hacktivista (vedi **figg. 3** e **10**), che mirano a compromettere sistemi critici per veicolare messaggi sociali o politici e che rendono ancora più difficile prevedere obiettivi e tempistiche.

[1] Fonte: Hackmanac Global Cyber Attacks Report 2026

Il motivo per cui la sanità è così vulnerabile è duplice. Da un lato, i dati sanitari sono tra i più preziosi sul mercato del cybercrime, facilmente monetizzabili o sfruttabili per estorsioni e frodi. Dall'altro lato, molte infrastrutture digitali sanitarie presentano **vulnerabilità note non risolte**, dovute a sistemi legacy, scarsa sicurezza dei dispositivi medici connessi e insufficiente formazione del personale sulla sicurezza informatica. In Italia, ad esempio, un discreto numero di aziende sanitarie ha subìto almeno un incidente informatico nell'ultimo anno, con un numero significativo di casi classificati come gravi (vedi **figg. 8** e **13**).

Un'altra criticità deriva dall'aumento delle tecnologie interconnesse: la diffusione di dispositivi IoT/IoMT, la telemedicina, i servizi cloud, gli ambienti ibridi e multi-cloud, le piattaforme di interoperabilità regionale e i sistemi di gestione amministrativa creano un ecosistema complesso in cui ogni nuovo collegamento digitale apre un potenziale punto di ingresso per gli attaccanti. Inoltre, l'evoluzione normativa, come la direttiva europea **NIS2**, impone requisiti più stringenti in materia di sicurezza, resilienza e gestione del rischio, spingendo le organizzazioni sanitarie ad adottare approcci più strutturati alla cyber defense. In questo contesto, il rischio informatico non è più un problema puramente tecnico, ma diventa una componente integrante della governance sanitaria, con implicazioni per la continuità operativa, la tutela dei dati e, in ultima analisi, la sicurezza dei pazienti.

I cyber attacchi verso il settore Healthcare nel 2025

Il settore sanità, nel 2025, ha registrato **1.053 cyber attacchi di successo e di pubblico dominio a livello globale**, con un incremento del **30%** rispetto all'anno precedente e un **volume cinque volte superiore rispetto al 2020** (**Fig. 1**).

Il trend di crescita si conferma quindi strutturalmente in aumento, sebbene la quota di incidenti diretti al settore sanitario sul totale degli attacchi globali diminuisca dal 9,8% al 5,9%.

La media sale a **88 incidenti al mese** (contro i 68 del 2024), mentre febbraio, marzo, aprile e luglio risultano i mesi più attivi, a differenza di agosto, settembre, novembre e dicembre, che mostrano attività malevole più contenute (**Fig. 2**).

Nel **90% dei casi (947 attacchi)**, le operazioni sono riconducibili a motivazioni di natura **cybercriminale**, mentre il restante **10%** deriva da attività di **hacktivism** (**Fig. 3**).

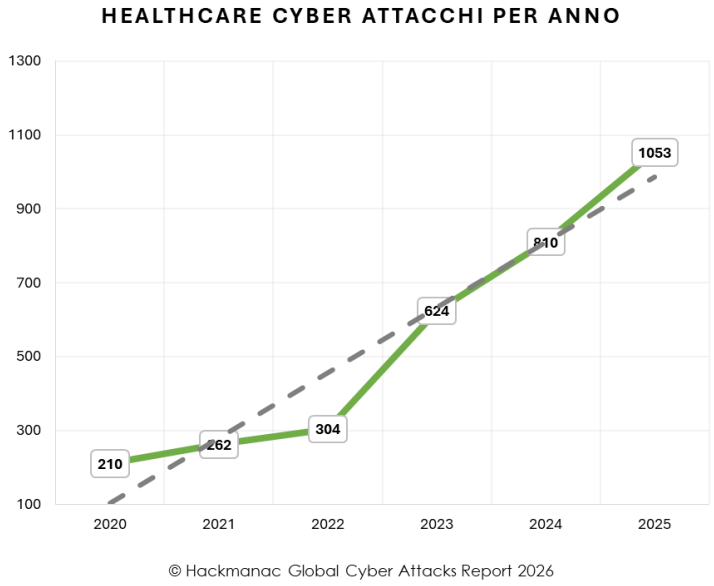

Fig. 1 - Trend dei cyber attacchi nel settore sanitario nel periodo 2020-25

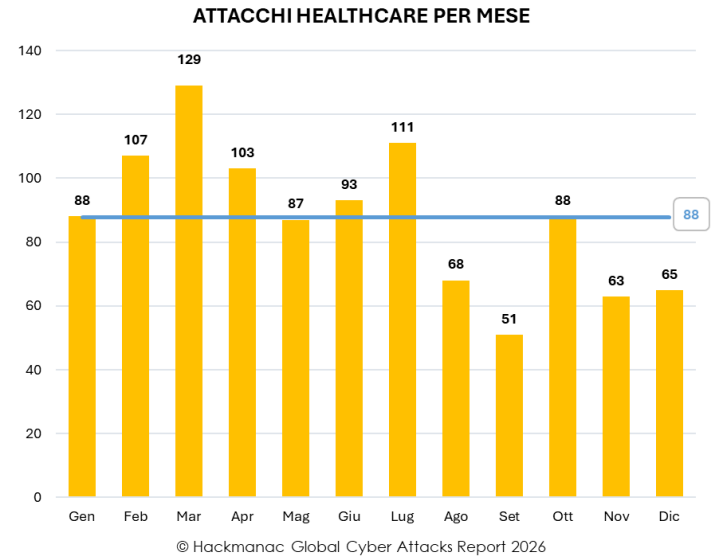

Fig. 2 - Andamento mensile degli attacchi globali verso il settore sanitario nel 2025

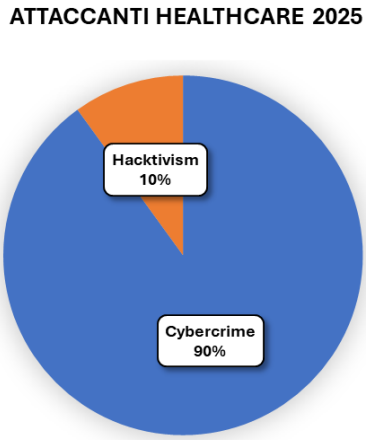

Fig. 3 - Distribuzione degli attaccanti verso il settore sanitario nel 2025

Dal punto di vista geografico, il settore sanitario viene colpito prevalentemente nel **continente americano** (72%, in calo rispetto al 78% del 2024). Seguono **Asia**, che raggiunge il **14%** con una crescita significativa di 9 punti percentuali, ed **Europa**, che si attesta al **10%**, in diminuzione di 4 punti percentuali. **Oceania** (3%) e **Africa** (1%) risultano invece marginalmente interessate.

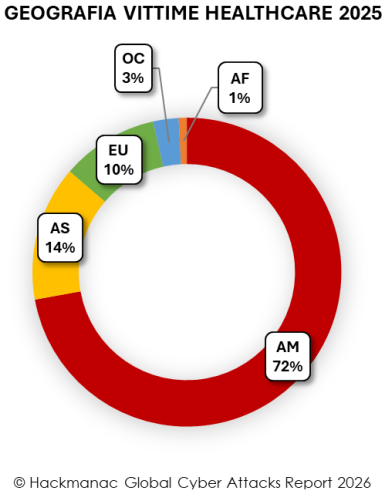

Fig. 4 - Geografia delle vittime dei cyber attacchi in ambito sanitario nel 2025

Anche nel 2025, come già osservato nei due anni precedenti, risulta assente la quota di attacchi verso località multiple, indicando una crescente tendenza verso operazioni mirate e focalizzate.

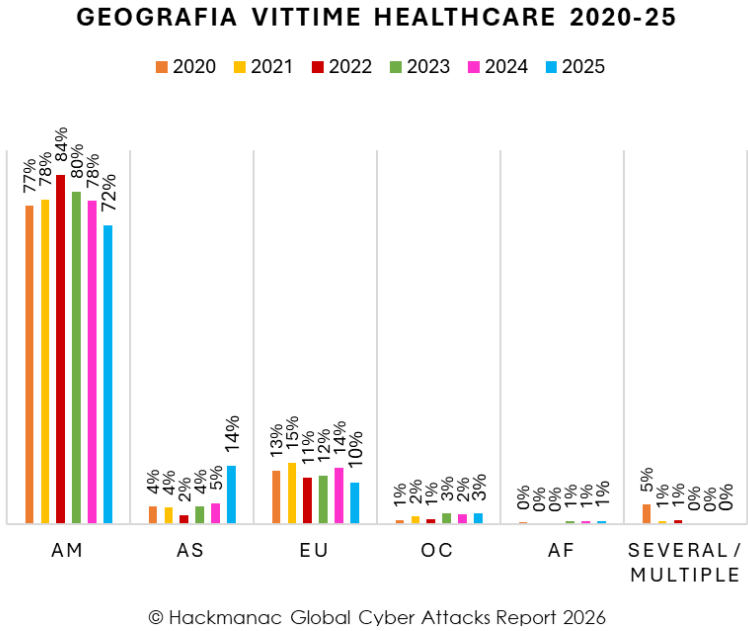

Fig. 5 - Distribuzione geografica delle vittime nel settore Healthcare nel periodo 2020-25

I **Malware**, e in particolare i **ransomware**[2], si confermano la tecnica di attacco più utilizzata ed efficace per i cyber criminali, impiegata in quasi la metà degli incidenti (**47%**) ai danni del settore sanitario (**Fig. 6**).

[2] https://it.wikipedia.org/wiki/Ransomware

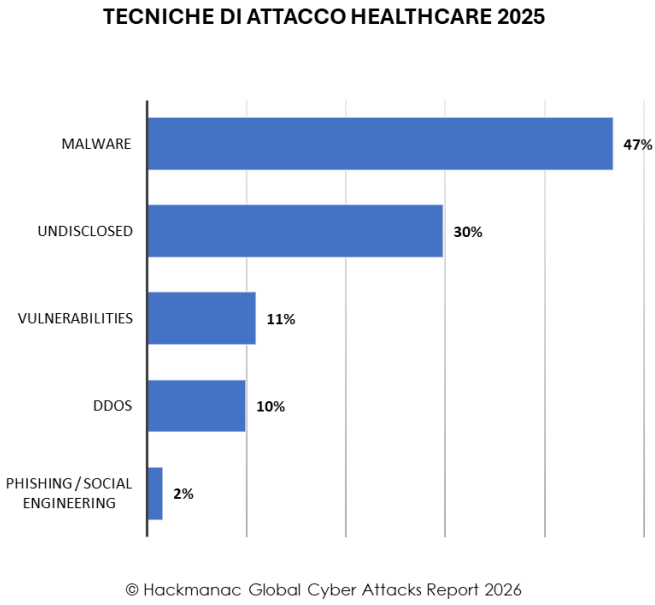

Fig. 6 - Tecniche di attacco verso il settore Healthcare nel 2025

Seguono le **tecniche "sconosciute"**, prevalentemente riconducibili a **data breach**[3] per i quali non sono emerse informazioni dettagliate, utilizzate nel **30%** degli attacchi, in crescita di 6 punti percentuali rispetto al 2024.

Aumenta inoltre lo **sfruttamento delle vulnerabilità** dei sistemi IT e delle applicazioni, incluse quelle particolarmente critiche e non ancora note come gli ***0-day***[4], che raggiungono l'**11% (+5 pp)**, e il ricorso agli **attacchi DDoS (10%)**, dopo un periodo di sostanziale marginalità negli anni precedenti.

Resta invece stabile l'utilizzo di **phishing**[5] e **ingegneria sociale**[6] **(2%)**, mentre si azzera il ricorso a furti di identità e violazioni di account, che nel 2024 **rappresentavano l'8%** degli incidenti.

[3] https://it.wikipedia.org/wiki/Data_breach

[4] https://it.wikipedia.org/wiki/0-day

[5] https://it.wikipedia.org/wiki/Phishing

[6] https://it.wikipedia.org/wiki/Ingegneria_sociale

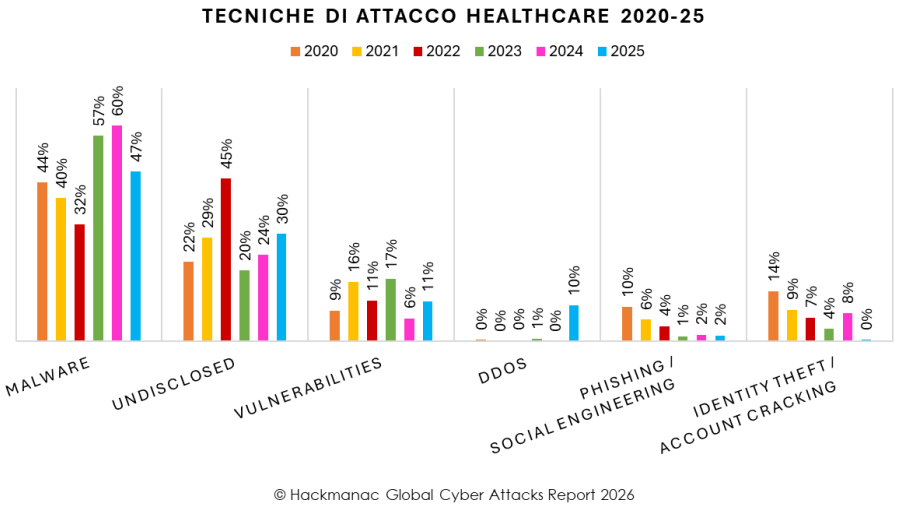

Fig. 7 - Distribuzione delle tecniche di attacco verso il settore sanitario nel periodo 2020-25

Per quanto riguarda infine le **conseguenze degli attacchi**, nel 2025 si osserva un netto peggioramento: la quota di incidenti con **ripercussioni gravissime raddoppia**, passando dal 23% al **48%**, mentre diminuiscono, pur rimanendo su livelli elevati, gli attacchi con **impatti gravi**, dal 67% al **43%**.

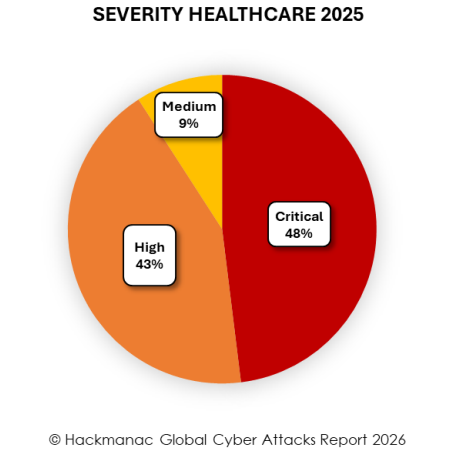

Fig. 8 - Severity cyber attacchi verso il settore sanitario nel 2025

Complessivamente la quota di severity importanti si mantiene stabilmente intorno ai **9 casi su 10** (**91% nel 2025**, contro il 90% dell'anno precedente).

Questo è un dato che conferma come **operazioni malevole siano progettate deliberatamente per massimizzare il danno operativo, economico e reputazionale**.

La situazione italiana

In Italia le attività malevole rivolte al settore sanitario mostrano un andamento in netta diminuzione dopo il picco registrato nel 2023. Nel 2025, infatti, sono stati analizzati **10 cyber attacchi di successo e di pubblico dominio**, in calo rispetto ai 13 dell'anno precedente.

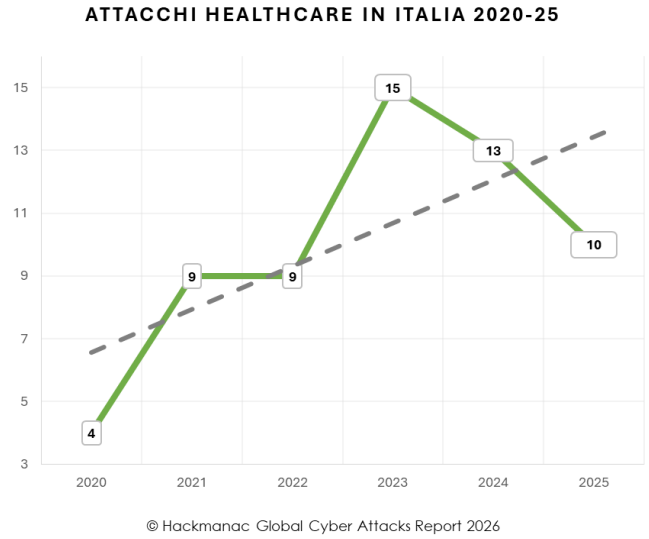

Fig. 9 - Andamento dei cyber attacchi verso il settore sanitario in Italia nel periodo 2020-25

A differenza di quanto osservato nel 2024, le motivazioni degli attacchi risultano più diversificate e si dividono tra **Cybercrime**, che rappresenta circa due terzi dei casi (**60%**, in calo dal 100% dell'anno precedente), e **Hacktivism**, che raggiunge quota **40%**.

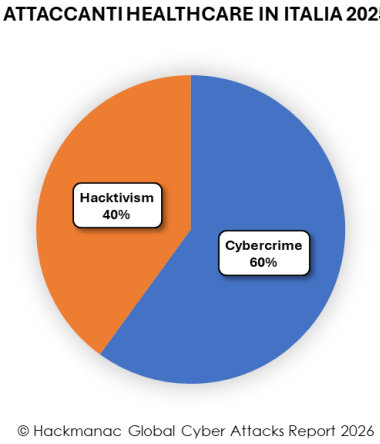

Fig. 10 - Distribuzione degli attaccanti dei cyber attacchi verso il settore sanitario in Italia nel 2025

Le tecniche di attacco mostrano una distribuzione significativamente diversa rispetto al campione globale. Se a livello internazionale i **malware** rappresentano la principale minaccia per le organizzazioni sanitarie, in Italia nel 2025 si collocano solo al terzo posto (**20%** dei casi), preceduti da **DDoS** (40%) e da **tecniche non chiaramente attribuibili** (30%).

Il **phishing e l'ingegneria sociale** risultano marginali e vengono utilizzati solo nel **10%** degli attacchi, mentre si azzera completamente il ricorso ad altre tecniche, incluso lo sfruttamento di vulnerabilità, che nel 2024 rappresentava il 31% degli incidenti.

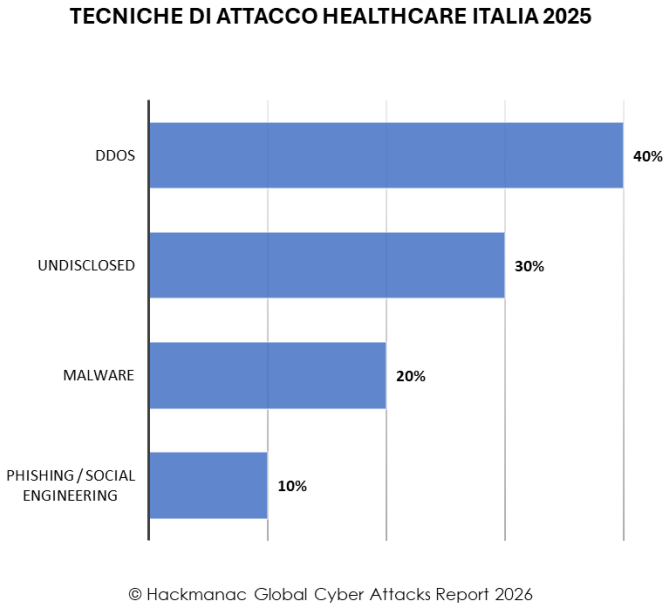

Fig. 11 - Tecniche di attacco verso il settore sanitario in Italia nel 2025

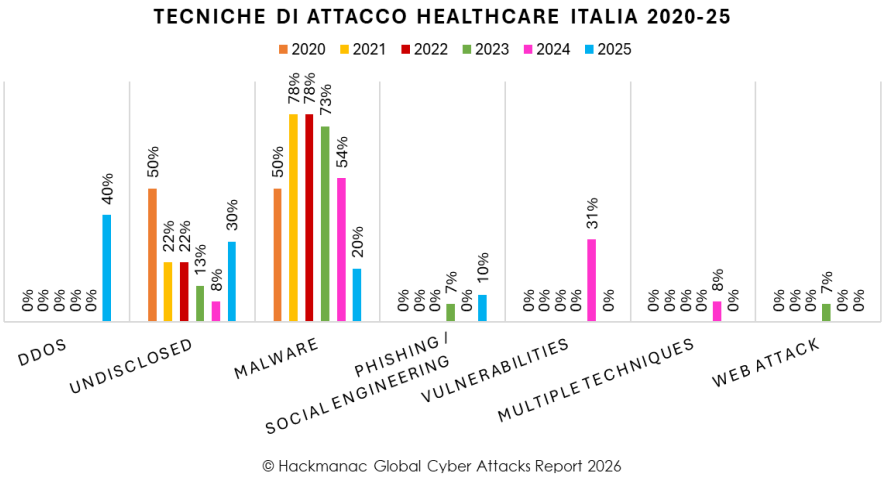

Fig. 12 - Distribuzione delle tecniche di attacco verso il settore sanitario in Italia nel periodo 2020-25

Per quanto riguarda gli **impatti**, nel 2025 si osserva una fase di apparente "normalizzazione". Se nel 2024 la totalità degli attacchi aveva prodotto conseguenze gravi o gravissime, nel 2025 questa quota si riduce al **50%**.
In particolare, diminuiscono gli attacchi con **severity critica** (dal 30% al **10%**) e quelli con **severity High** (dal 62% al **40%**), mentre tornano a crescere gli **impatti medi**, che incidono su metà degli incidenti analizzati.

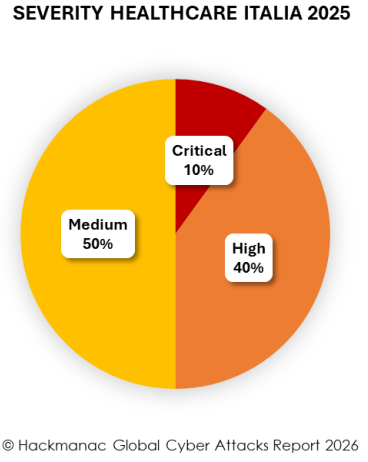

Fig. 13 - Severity degli attacchi verso il settore sanitario in Italia nel 2025

Se da un lato questo trend in calo degli impatti può essere interpretato come un segnale positivo per il settore sanitario nazionale, dall'altro evidenzia una criticità strutturale. Anche in assenza di operazioni particolarmente sofisticate, è evidente che le infrastrutture difensive non sono riuscite a prevenire o fermare gli attacchi, un chiaro indicatore del fatto che, **in Italia, la cybersecurity del settore healthcare presenta ancora ampi margini di miglioramento**.

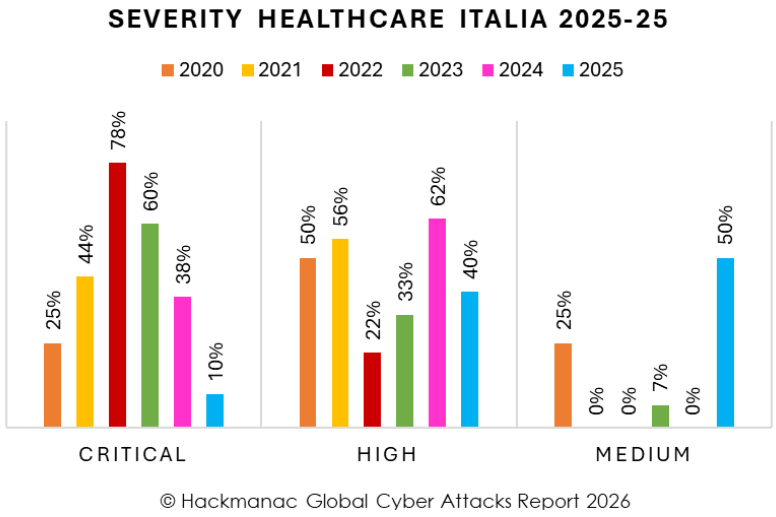

Fig. 14 - Distribuzione della severity degli attacchi verso il settore sanitario in Italia nel periodo 2020-25

I principali incidenti italiani

L'anno nero degli attacchi Ddos, finalizzati a mettere ko ii portali istituzionali di aziende ospedalire e sanitarie, inizia poco dopo lo scoccare della mezzanotte, il 3 gennaio 2025. A colpire e rivendicare le azioni in diversi casi è il gruppo filorusso ServerKiller, attivo dal 2023, che opera in modo analogo ad altri gruppi hacktivisti come NoName057(16), per fare pressione politica nei confronti dei Paesi NATO che sostengono l'Ucraina. Vittime a inizio anno sono ben quattro ospedali di rilievo nazionale colpiti in un solo giorno: il **Policlinico Gemelli**, l'**Istituto Europeo di Oncologia IEO, il Salvator Mundi International Hospital e gli Istituti Fisioterapici Ospitalieri.** Queste campagne di DDoS, seppure classificate come di severity media, non sono certo le più preoccupanti, visto che altre sono le tipologie di attacco che fanno preoccupare di più e che, oltre a causare disservizi nelle operazioni di accesso ai sistemi online e rallentamenti nei servizi al pubblico, possono portare anche alla esfiltrazione di dati sanitari.

Tra il 26 e il 29 maggio - come riportato anche da Wired[7] - a essere sotto attacco è il settore italiano della distribuzione dei farmaci, colpito da una serie di attacchi informatici distinti, che hanno coinvolto Alliance Healthcare, D.M. Barone e Farmacisti Più Rinaldi. Pur non risultando collegati tra loro, gli incidenti hanno richiamato l'attenzio-

[7] https://www.wired.it/article/attacchi-informatici-farmaci-italia/

ne della Polizia Postale e dell'Agenzia per la Cybersicurezza Nazionale ACN, poiché mettendo a rischio la continuità della catena di distribuzione dei farmaci essenziali, hanno mostrato la fragilità del sistema, con potenziali impatti negativi sulla salute pubblica. Il caso più critico in termini operativi è stato quello di Farmacisti Più Rinaldi, azienda che gestisce circa il 50% delle forniture farmaceutiche in Friuli-Venezia Giulia e Veneto. Inizialmente attribuito a un generico guasto informatico, il blocco della distribuzione è stato successivamente ricondotto a un probabile attacco ransomware, che ha causato l'interruzione dei servizi per diverse ore.

Di natura diversa l'attacco subito da **Alliance Healthcare**, rivendicato dal gruppo ransomware DATACARRY, che ha pubblicato online un campione di circa 400 MB di dati sottratti. I file diffusi includevano credenziali di accesso, documentazione finanziaria e dati tecnici dei sistemi di gestione, probabilmente frutto di una compromissione potenzialmente più ampia. Pur non essendo chiaro se l'attacco abbia avuto effetti sull'operatività, l'azienda aveva dichiarato in questo caso che non c'erano stati disservizi o blocchi delle attività.

Nel caso di D.M. Barone, attiva nella distribuzione intermedia del farmaco in Sicilia e Calabria, l'attacco è stato rivendicato da Devman, un attore singolo legato all'ecosistema ransomware. In questo episodio non risultano dati esfiltrati, ma i sistemi sarebbero stati completamente bloccati, con una richiesta di riscatto pari a 130.000 dollari.

Nonostante la coincidenza temporale e settoriale, l'ipotesi di un attacco coordinato è ritenuta improbabile.

Nel corso dell'estate, gli attacchi legati al **malware** hanno colpito realtà anche fuori dal nucleo ospedaliero tradizionale: a fine giugno a subire un attacco malware ad alto impatto è Fratellanza Popolare Valle del Mugnone Caldine, associazione di pubblica assistenza aderente a A.N.P.AS che opera sul territorio di Fiesole e Firenze e che è impegnata in numerosi servizi sanitari, di protezione civile e aiuti alla popolazione. All'inizio di luglio anche Meleam S.p.A., che offre servizi di medicina polispecialistica e telemedicina è stata vittima di un attacco malware classificato di severità alta.

Altra rivendicazione - pur in assenza di comunicazione ufficiale, esterna, dell'incidente da parte del gestore dell'app - arriva in estate, quando viene pubblicato in un forum un avviso riferito alla esfiltrazione di dati provenienti dall'applicazione iGyno, utilizzata per il monitoraggio della salute riproduttiva. Secondo quanto rivendicato, la violazione ha riguardato circa 20.000 indirizzi email e informazioni sanitarie altamente sensibili, come cicli mestruali, eventuale stato di gravidanza ed età.

Il giorno successivo al Ferragosto 2025 a essere protagonista di un attacco classificato critico è A.R.N.A.S. Ospedali Civico di Cristina Benfratelli, clinica di rilievo nazionale e di alta specializzazione con sede a Palermo.
A chiudere la carrellata di attacchi ad alto impatto c'è poi l'incidente informatico alla piattaforma sanitaria utilizzata dai medici di medicina generale per prescrizioni, esami e gestione dei pazienti. Come riportato dal Corriere della Sera[8], a seguito dell'attacco ai server dell'azienda, è stato registrato un furto massivo di dati sanitari, successivamente sfruttati per una campagna di phishing mirata ai cittadini.
Gli utenti hanno, infatti, ricevuto email fraudolente, inviate a nome di una finta società di recupero crediti di Monza, CreditLex srl, in cui veniva richiesto il pagamento di presunti arretrati per prestazioni sanitarie, farmaci ed esami. Le comunicazioni risultavano particolarmente credibili perché contenevano dati reali dall'app violata, inclusi informazioni anagrafiche e dettagli su prescrizioni mediche recenti, aumentando significativamente il rischio di truffa. La Procura di Milano ha aperto un'indagine per truffa, affidando le verifiche alla Polizia Postale, mentre la piattaforma colpita è stata temporaneamente sospesa per consentire le attività di messa in sicurezza e contenimento dell'incidente.

Regione Lombardia ha chiarito che non risultano violazioni dei sistemi sanitari regionali né delle aziende sanitarie pubbliche, precisando che l'attacco ha riguardato esclusivamente una piattaforma privata utilizzata da parte dei medici di medicina generale. L'incidente conferma come le campagne di phishing basate su dati reali rappresentino una minaccia crescente per il settore sanitario, con impatti rilevanti sulla fiducia dei cittadini e sulla sicurezza complessiva dell'ecosistema digitale della sanità.

AI tra opportunità per la salute e rischi cyber in aumento

L'intelligenza artificiale sta trasformando profondamente la sanità, migliorando l'efficienza operativa, il supporto alle diagnosi e la gestione dei dati clinici. Algoritmi avanzati possono analizzare immagini radiologiche o esami di laboratorio, accelerando la rilevazione di patologie e aumentando la precisione diagnostica. L'automazione di procedure amministrative e cliniche riduce gli errori umani e consente al personale sanitario di concentrarsi su attività ad alto valore. Tuttavia, la diffusione di strumenti AI generativa come ChatGPT per informazioni mediche, senza il supporto di professionisti sanitari, può portare a ritardi diagnostici o interpretazioni errate dei sintomi, evidenziando la necessità di un approccio consapevole e guidato dalla competenza clinica.

[8] https://milano.corriere.it/notizie/cronaca/25_ottobre_10/milano-maxi-cyber-attacco-su-piattaforma-sanitaria-usata-dai-medici-di-base-per-le-prescrizioni-ai-pazienti-rubati-migliaia-di-8e0fe4e5-831c-42b5-bb9f-ccbe5b615xlk.shtml

La sanità gestisce dati altamente sensibili, infrastrutture critiche e processi essenziali per la vita delle persone, rendendola un target molto appetibile per gli aggressori. Questo scenario richiede un cambiamento nell'approccio alla valutazione del rischio: non basta reagire agli incidenti quando si verificano. È necessario spostare la gestione dei rischi "a sinistra", anticipando l'analisi e la mitigazione dei rischi già nella progettazione dei sistemi, nell'adozione di nuovi strumenti AI e nella gestione della supply chain digitale. Analizzare i rischi in fase precoce significa valutare preventivamente i sistemi e le componenti esterne, considerare le dipendenze indirette e garantire integrità e affidabilità lungo tutta la catena del valore digitale.

Nel contesto sanitario, il threat modeling deve superare la tradizionale visione perimetrale della difesa e adottare una prospettiva orientata all'attaccante. Anche infrastrutture interne fortemente protette possono essere aggirate, poiché gli aggressori possono sfruttare corridoi esterni o vulnerabilità indirette, come componenti software di terze parti, librerie riutilizzate, firmware di dispositivi medicali o servizi cloud integrati nei sistemi clinici. Pensare come un attaccante significa chiedersi non solo "come posso violare questo sistema?", ma anche "quale componente a monte può compromettere per colpire più strutture contemporaneamente?". Questo approccio permette di mappare non solo gli asset interni, ma anche le connessioni esterne, trasformando la gestione del rischio in una valutazione continua della fiducia lungo tutta la catena del valore digitale. In particolare, diventa fondamentale monitorare i modelli AI addestrati su dataset non verificati, librerie non aggiornate e firmware di dispositivi forniti da terze parti, per ridurre le vulnerabilità che potrebbero essere sfruttate a monte.

Per proteggere efficacemente le strutture sanitarie, è quindi necessario un approccio integrato che combini governance, formazione e resilienza tecnologica. Politiche di sicurezza centralizzate, monitoraggio costante, backup affidabili e disaster recovery sono strumenti essenziali, così come programmi formativi mirati per medici, tecnici e personale amministrativo, per diffondere una cultura della cyber hygiene. La verifica continua della supply chain, l'autenticità e l'integrità dei componenti hardware, software e AI, e una mentalità di "trust zero" nei confronti dei fornitori esterni completano il quadro di difesa, consentendo di ridurre la superficie di attacco prima che i sistemi diventino operativi.

L'intelligenza artificiale in sanità rappresenta un'opportunità straordinaria, ma la sua adozione richiede una gestione attenta dei rischi. La sicurezza non può limitarsi al perimetro dell'ospedale: è necessario considerare l'intero ecosistema digitale, dai fornitori di software ai dispositivi medicali, passando per servizi cloud e modelli AI.

Oltre il perimetro: la superficie di attacco si amplia

Negli ultimi anni il settore sanitario è stato attraversato da una profonda trasformazione digitale. L'introduzione di cartelle cliniche elettroniche, piattaforme di telemedicina, servizi cloud e dispositivi medici connessi ha migliorato l'efficienza dei processi clinici e l'accesso alle cure, ma ha anche ampliato in modo significativo la **superficie di attacco informatica**. Questo fenomeno rappresenta uno dei principali fattori di rischio cyber per le strutture sanitarie pubbliche e private.

L'ampliamento della superficie di attacco in sanità

Per superficie di attacco si intende l'insieme di sistemi, dispositivi, utenti e interconnessioni potenzialmente sfruttabili da un attaccante. In ambito sanitario, tale superficie è cresciuta rapidamente per una combinazione di fattori strutturali e tecnologici.
Un primo elemento critico è rappresentato dall'**Internet of Medical Things (IoMT)**: monitor multiparametrici, pompe di infusione, ventilatori, sistemi di imaging e dispositivi wearable clinici sono sempre più spesso connessi alle reti ospedaliere. Molti di questi apparati utilizzano sistemi operativi embedded, firmware difficilmente aggiornabili e credenziali di default, e non consentono l'installazione di strumenti di sicurezza tradizionali. La loro priorità progettuale è la continuità clinica, non la resilienza informatica, rendendoli bersagli ideali per movimenti laterali all'interno delle reti.
Un secondo fattore è la **diffusione della telemedicina e dell'assistenza remota**. Medici e operatori sanitari accedono ai sistemi clinici da reti domestiche, spesso tramite dispositivi personali, mentre i pazienti utilizzano app e device IoT al di fuori del controllo diretto delle strutture sanitarie. Il perimetro tradizionale dell'ospedale si dissolve, trasformandosi in un ecosistema distribuito in cui ogni endpoint può diventare un potenziale punto di ingresso.
A ciò si aggiunge la crescente **integrazione tra sistemi eterogenei**: cartelle cliniche elettroniche, laboratori, radiologia, sistemi amministrativi, piattaforme regionali e applicazioni per i pazienti comunicano tramite API e account di servizio. Ogni integrazione introduce nuove dipendenze tecniche e nuove identità digitali, spesso poco monitorate e raramente sottoposte a rotazione delle credenziali.
Infine, non va sottovalutato il fenomeno dello **shadow IT clinico**. Per esigenze operative e di rapidità, personale sanitario utilizza talvolta strumenti non autorizzati – applicazioni di messaggistica, cloud personali, software non certificati – che portano dati clinici sensibili al di fuori dei canali governati dall'organizzazione.

I rischi concreti: dal dato al paziente

L'ampliamento della superficie di attacco non comporta solo un aumento del rischio di violazioni dei dati, ma ha un impatto diretto sulla **sicurezza dei pazienti**.

Un attacco ransomware o un incidente informatico possono bloccare l'accesso alle cartelle cliniche, ritardare diagnosi e terapie, compromettere la disponibilità di dispositivi salvavita e generare effetti a catena sull'intera operatività ospedaliera. In sanità, il rischio cyber non è mai solo digitale: è anche clinico, etico e, in alcuni casi, vitale.

Le contromisure: ridurre l'esposizione senza bloccare le cure

Di fronte a questo scenario, le contromisure non possono limitarsi a soluzioni tecnologiche isolate. È necessario un approccio sistemico, che tenga conto delle specificità operative della sanità.

Una prima misura fondamentale è la **conoscenza continua dell'esposizione**. Inventari dinamici di dispositivi, sistemi e connessioni consentono di sapere in ogni momento cosa è realmente connesso alla rete e con quali livelli di rischio. In particolare per l'IoMT, il monitoraggio passivo del traffico di rete (che oggi può essere realizzato anche con l'aiuto dell'intelligenza artificiale) permette di individuare anomalie senza interferire con il funzionamento clinico dei dispositivi.

La **segmentazione di rete** rappresenta un'altra contromisura chiave. Separare logicamente dispositivi medici, sistemi clinici centrali e servizi amministrativi riduce drasticamente la possibilità di movimenti laterali in caso di compromissione. La segmentazione deve essere progettata in modo "clinicamente consapevole", evitando di introdurre rigidità incompatibili con le urgenze sanitarie.

Sul fronte degli accessi, diventa essenziale rafforzare la **gestione delle identità e dei privilegi**. Autenticazione multifattore, accessi contestuali, principio del minimo privilegio e revisione periodica degli account – inclusi quelli tecnici e di servizio – sono elementi imprescindibili in un contesto in cui l'identità è il nuovo perimetro.
Per quanto riguarda la telemedicina e il lavoro remoto, occorre adottare soluzioni che vadano oltre la VPN tradizionale, introducendo controlli basati su dispositivo, contesto e comportamento, senza ostacolare l'operatività clinica.

Infine, la gestione dello shadow IT non può basarsi solo su divieti. È necessario offrire **alternative sicure e usabili**, accompagnate da **programmi di formazione mirata** che aiutino il personale sanitario a comprendere i rischi senza scaricare su di esso responsabilità che non potrebbero gestire.

L'ampliamento della superficie di attacco in sanità è una conseguenza inevitabile della digitalizzazione delle cure. Il vero rischio non è innovare, ma farlo senza una strategia di governo dell'esposizione informatica. Solo integrando sicurezza, organizzazione e contesto clinico sarà possibile costruire una sanità digitale resiliente, capace di proteggere allo stesso tempo dati, sistemi e, soprattutto, pazienti.