LA MINACCIA CIBERNETICA AL SETTORE SANITARIO

Analisi e raccomandazioni

gennaio 2023 – settembre 2025

TLP:CLEAR

*Il presente documento ha un livello di condivisione **TLP:CLEAR.** Le informazioni possono essere distribuite senza restrizioni rispettando eventuali disposizioni sul copyright. Ulteriori dettagli sono disponibili sulla pagina dedicata del CSIRT Italia e sulla pagina dedicata del FIRST.*

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal Decreto-legge n. 82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, anche attuando il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza, promuovendone azioni comuni.

L'Agenzia è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. In tale veste ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico del Paese promuovendo la realizzazione di azioni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese. A tal fine sviluppa anche capacità necessarie per proteggere dalle minacce informatiche reti, sistemi informativi e servizi informatici delle Pubbliche Amministrazioni e degli operatori di infrastrutture critiche nazionali, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Siti web: **Agenzia per la Cybersicurezza Nazionale** **CSIRT Italia**

Contatti: **info@acn.gov.it**

Seguici sui nostri canali social:

Esclusione di responsabilità

Il presente documento fornisce, a titolo esemplificativo e non esaustivo, indicazioni di mero ausilio alle attività di sicurezza delle organizzazioni e non solleva le stesse dall'onere di porre in essere, nel rispetto della normativa vigente in materia di cybersicurezza, tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dal verificarsi di eventi e incidenti informatici.

SOMMARIO

INTRODUZIONE

Il settore sanitario, a livello globale, risulta essere tra quelli maggiormente impattati in caso di attacchi cyber.

Sul territorio **nazionale**, a partire da gennaio 2023 si sono verificati mediamente **4,3 eventi cyber malevoli al mese** ai danni di strutture sanitarie, dei quali la metà circa ha dato luogo a "incidenti", ovvero ha avuto un impatto effettivo sui servizi sanitari erogati, in termini di disponibilità e/o di riservatezza, causandone talvolta il blocco con gravi ripercussioni a danno dell'utenza, anche per quanto concerne la privacy.

Le analisi sugli incidenti svolte dall'Agenzia per la Cybersicurezza Nazionale (ACN) mostrano che i tentativi di attacco spesso hanno successo poiché alcune **pratiche di sicurezza**, anche elementari, vengono **ignorate** o **mal implementate**. Nella maggior parte dei casi, ciò è frutto di scarsa attenzione agli aspetti di sicurezza connessi alla gestione di sistemi digitali, o di una carente formazione specifica sulla cybersicurezza del personale impiegato in ospedali, centri medici, cliniche e altre strutture sanitarie.

Anche le analisi condotte dall'Agenzia dell'Unione Europea per la sicurezza informatica (ENISA) sul **panorama europeo** evidenziano che negli ultimi anni il settore sanitario ha affrontato significative minacce cibernetiche, con numerosi incidenti riportati da varie organizzazioni in tutta Europa. Il primo studio[1] condotto da ENISA sulle minacce cibernetiche nel settore sanitario evidenzia la sua notevole vulnerabilità, dovuta alla sensibilità dei dati trattati e al crescente interesse dei criminali informatici. L'urgente coinvolgimento attivo della dirigenza sanitaria è fondamentale, specialmente con l'introduzione della direttiva NIS2[2] che prevede chiare responsabilità e una pianificazione adeguata delle misure di sicurezza cyber anche per questo settore.

In questo documento, destinato sia ai **livelli dirigenziali delle strutture sanitarie**, sia al **personale tecnico dipendente**, l'Agenzia per la Cybersicurezza Nazionale presenta una panoramica sulle

[1] Health Threat Landscape – ENISA, 2023

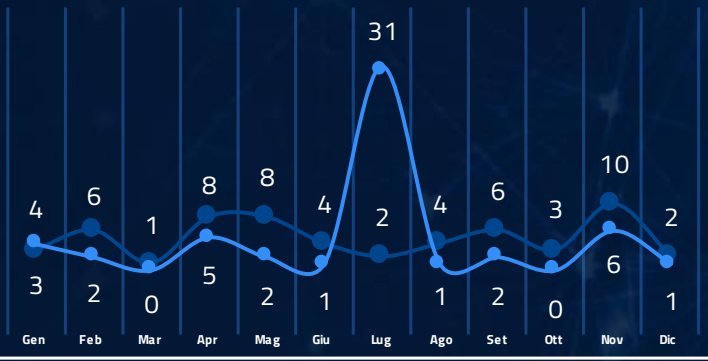
[2] Direttiva (UE) 2022/2555 recepita dal D. lgs. n. 138 del 2024.

principali minacce cyber nel settore sanitario.

In particolare, il capitolo 1 del documento è dedicato al panorama degli **eventi cyber e degli incidenti** rilevati e gestiti dall'Agenzia nel periodo gennaio 2023 – settembre 2025 a livello nazionale, mentre il capitolo 2 riporta una sintetica analisi delle principali **vulnerabilità** individuate nelle infrastrutture digitali. Le **raccomandazioni** e le **contromisure** primarie per potenziare la sicurezza informatica sono presentate, infine, nel capitolo 3.

IL SETTORE A COLPO D'OCCHIO

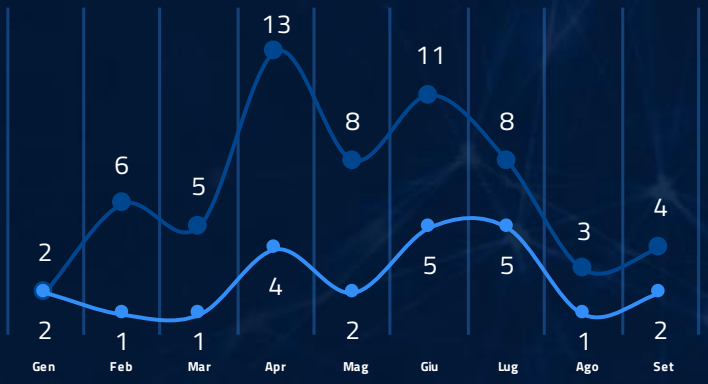
EVENTI CYBER E INCIDENTI (2023-2024)



Trend eventi cyber e incidenti dal 2023 al 2024

- Eventi cyber registratinel 2024
- Incidenti registratinel 2024

EVENTI CYBER E INCIDENTI (2025)



Trend eventi cyber e incidenti nel 2025

- Eventi cyber registratinel 2025
- Incidenti registratinel 2025

PRINCIPALI IMPATTI SUI SOGGETTI

BLOCCO TEMPORANEO DI SERVIZI

ESFILTRAZIONE DI DATI

MODIFICHE ALL'INTEGRITÀ

Minaccia con maggior impatto:
Ransomware

VULNERABILITÀ ESPOSTE

IP monitorati che presentano criticità:

CONFIGURAZIONI ERRATE CHE NON RISPETTANO BEST PRACTICE — **63%**

DISPOSITIVI E SERVIZI ESPOSTI INCAUTAMENTE — **26%**

SERVIZI CON VULNERABILITÀ O OBSOLETI — **11%**

PRINCIPALI CAUSE DELLE BAD PRACTICES

GESTIONE DECENTRALIZZATA

Diversi reparti ottengono hardware, software e servizi IT da fornitori esterni senza una gestione centralizzata.

CARENZA DI PERSONALE DEDICATO A CYBERSICUREZZA

Il personale IT gestisce la sicurezza informatica senza avere risorse dedicate, facendo al meglio delle proprie possibilità.

OBSOLESCENZA DEI DISPOSITIVI

Apparati informatici obsoleti, non aggiornabili o supportatiche continuanoad essere utilizzati.

1 ATTACK LANDSCAPE

Il CSIRT Italia, componente tecnico-operativa dell'Agenzia, ricopre il ruolo di **hub nazionale** per la gestione delle **notifiche obbligatorie e volontarie** relative agli incidenti cibernetici previsti dalle normative di settore, quali il Perimetro di Sicurezza Nazionale Cibernetica (D.L. n. 105/2019), la Direttiva NIS2 (D. Lgs. n. 138/2024) e la Legge n. 90 del 2024. In tale contesto, gli operatori del CSIRT Italia eseguono un'attenta analisi delle informazioni raccolte durante la fase di **triage**, classificandole come *eventi cyber* o, se confermato l'impatto sulle vittime, come veri e propri *incidenti*.

Il presente capitolo fornisce dettagli numerici relativi agli **eventi cyber** e agli **incidenti** nel settore sanitario, supportati da un'analisi sulla tipologia degli eventi. Questo permetterà di esaminare con maggior precisione sia gli eventi cyber che non hanno avuto un impatto confermato dalla vittima, sia quelli con impatto confermato e quindi classificati quali incidenti, consentendo così un'analisi più granulare della natura e delle conseguenze di ciascun evento cyber rilevato nel periodo di riferimento. In particolare, dopo aver riportato un dettaglio dei dati rilevati nell'anno 2024 raffrontati con quelli del 2023, si fornisce un *focus* di quanto invece rilevato nel 2025.

1.1 Eventi cyber e incidenti

Al fine di fornire un quadro concettuale chiaro, si forniscono di seguito le definizioni a cui si farà riferimento nel corso del documento. Viene definito:

- **evento cyber**, un avvenimento con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti.
- **Impatto,** perturbazione causata da un evento cyber.
- **incidente**, evento cyber con impatto confermato dalla vittima o dal CSIRT Italia.

1.1.1 Eventi cyber e incidenti rilevati tra il 2023 e il 2024

Nel periodo compreso tra il 2023 e il 2024, si è osservato un notevole incremento nella frequenza degli eventi cyber, documentati in un totale di **84** casi. L'analisi del numero di **eventi cyber registrati nel 2024** rivela un **aumento del 111%** rispetto all'anno precedente, confermando la

tendenza di crescita nel settore.

Il CSIRT Italia ha censito **57 eventi nel 2024** a fronte dei **27 dell'anno precedente**[3]. Anche il numero di incidenti è sensibilmente aumentato (55 nel 2024 rispetto ai 12 del 2023).

In particolare, è emerso che nel 2024 **circa il 96% degli eventi cyber sono stati confermati come incidenti** (**55**). Questa tendenza pone in luce la crescente diffusione degli attacchi al settore, come mostrato nella Figura 1, che riporta la distribuzione degli eventi cyber e degli incidenti nel settore sanitario nel 2023, rispetto alla media mensile dell'anno precedente.

L'osservazione dei dati mensili mostra come a luglio 2024 si sia rilevato un aumento significativo degli incidenti riconducibile ad un attacco di tipo *supply chain* che ha coinvolto un fornitore di servizi IT operante a supporto di diversi soggetti nel settore sanitario. L'evento ha messo in evidenza le interconnessioni strutturali che caratterizzano il settore, dimostrando come la compromissione di un singolo fornitore possa generare effetti a cascata, con potenziali ricadute sull'erogazione dei servizi essenziali da parte di più soggetti.

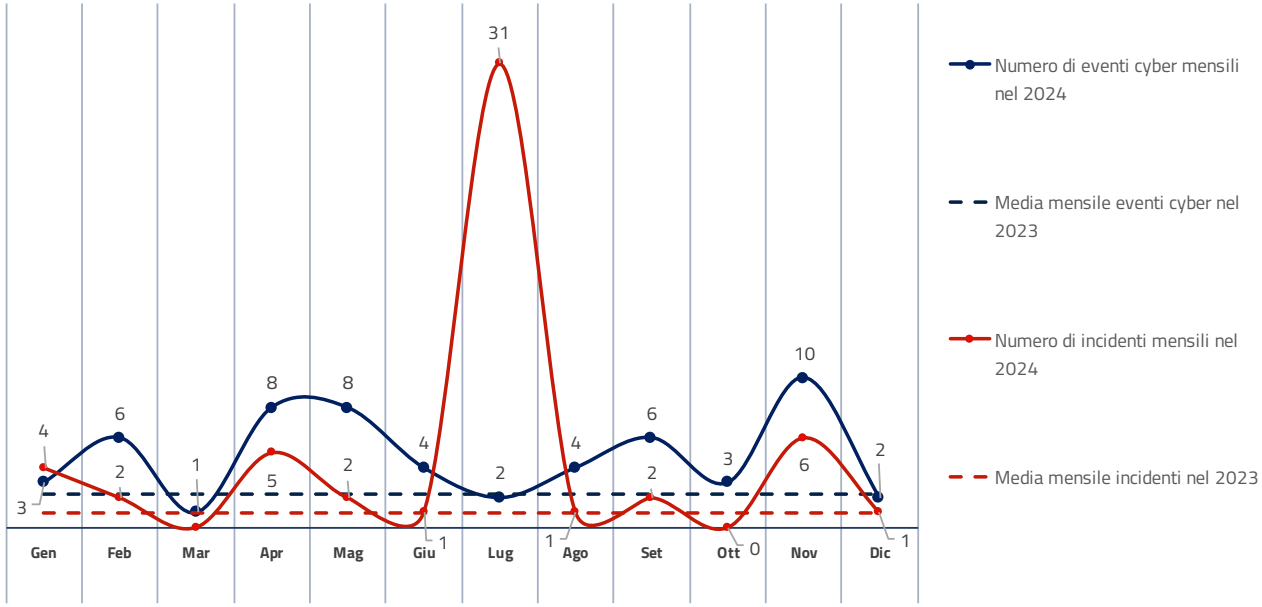


Figura 1: eventi cyber e incidenti nel settore sanitario nel 2024 rispetto alla media mensile dell'anno precedente

La Figura 2 combina l'analisi del numero di eventi cyber e incidenti nel corso del periodo in esame, evidenziando un aumento significativo per entrambi rispetto all'anno precedente. Inoltre, fornisce un'ulteriore analisi dell'andamento annuale, presentando le **variazioni percentuali** rispetto alla media del 2023 ed evidenziando un **aumento** sia degli eventi cyber che degli incidenti

[3] Si noti che determinati incrementi sono ascrivibili anche all'aumentata capacità del CSIRT Italia di rilevare eventi, incidenti e vulnerabilità, nonché al modificato impianto normativo.

nel 2024 **rispetto alla media dell'anno precedente**.

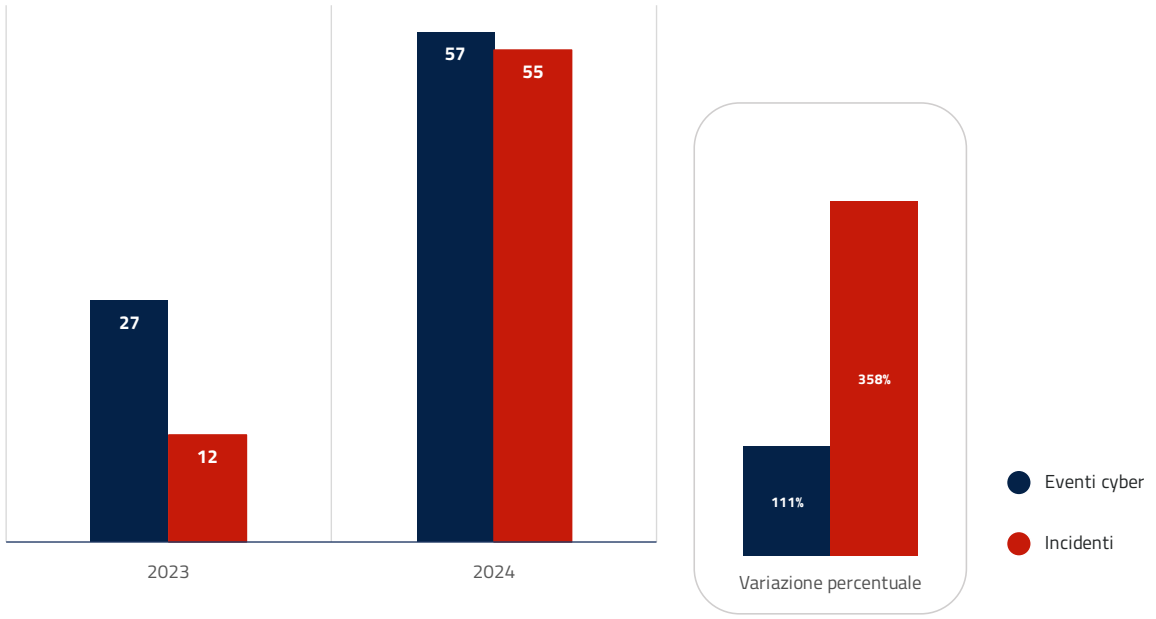


Figura 2: numero di eventi cyber e incidenti nel periodo 2023-2024 e loro variazione percentuale annua

Dall'analisi e classificazione degli **84 eventi cyber** rilevati nel periodo in esame (2023-2024) sono emerse le principali tipologie di minacce[4] riportate in Figura 3. Il settore sanitario ha registrato principalmente minacce riconducibili a **esposizione dati** (divulgazione non autorizzata di dati personali), **accessi non autorizzati tramite l'utilizzo di credenziali valide**, compromissione da **malware**, con una significativa incidenza di attacchi **ransomware**. Quest'ultima tipologia si conferma tra le più rilevanti in termini di impatto, per la capacità di compromettere la disponibilità dei sistemi informativi e di incidere in maniera significativa sulla continuità operativa delle strutture sanitarie. In particolare:

- gli attacchi **ransomware** risultano essere tra le minacce cibernetiche più diffuse per il settore, con l'**11% degli eventi** nel 2024 ed il **36% degli eventi** nel 2023;
- le attività di **esposizione dati** ed **intrusione tramite credenziali valide** sono state rilevate nel **15% degli eventi** nel 2024;
- l'**esfiltrazione** è stata rilevata nel **14% degli eventi** del 2023;
- le **compromissioni da malware** hanno caratterizzato il **13% degli eventi** nel 2024.

[4] Si noti che ognuno dei citati eventi può essere stato associato ad una o più tipologia di minacce.

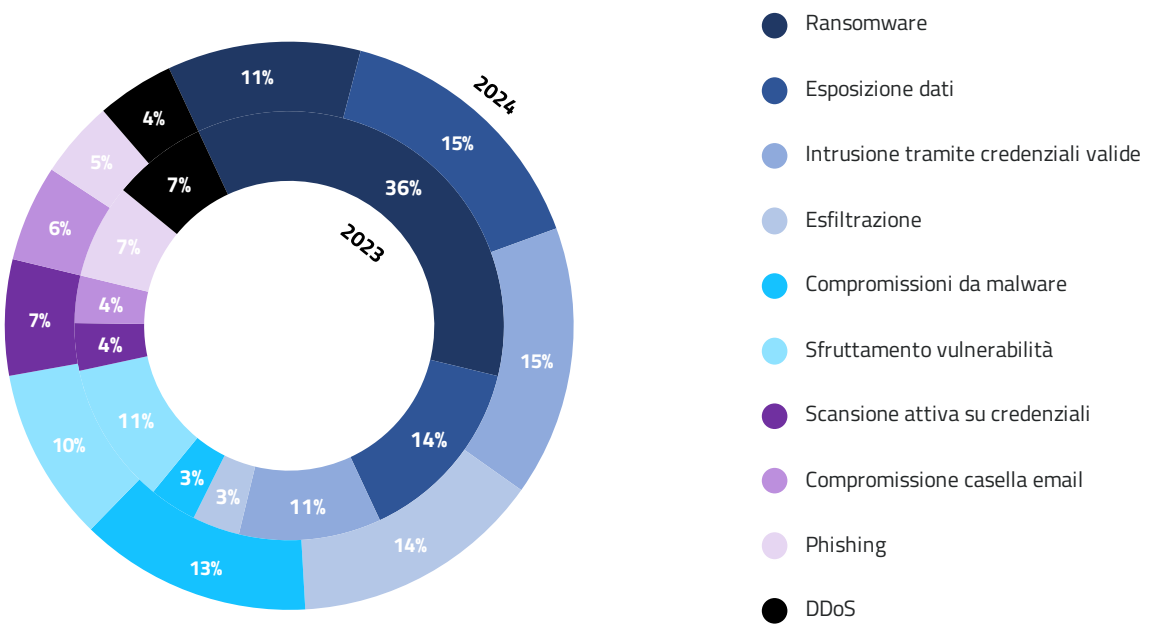


Figura 3: tipologie di minacce rilevate negli eventi cyber nel periodo 2023-2024 (top 10)

Anche la distribuzione degli **incidenti per tipologia** conferma tale andamento, come rappresentato dalla Figura 4, dove sono riportate le principali tipologie[5] di minacce rilevate nei **55 incidenti**. Da evidenziare che:

- i **ransomware** risultano essere la tipologia di incidente più impattante, rappresentano infatti il **17%** degli incidenti nel 2024 ed il **46%** nel 2023;
- le **compromissioni da malware** hanno caratterizzato il **17% degli incidenti** nel 2024;
- l'**intrusione tramite credenziali valide** è stata rilevata nel **17% degli incidenti** nel 2024;
- la **diffusione malware tramite e-mail** ha caratterizzato l'**11% degli incidenti** nel 2024.

[5] Si noti che ognuno dei citati incidenti può essere stato associato a una o più tipologia di minacce.

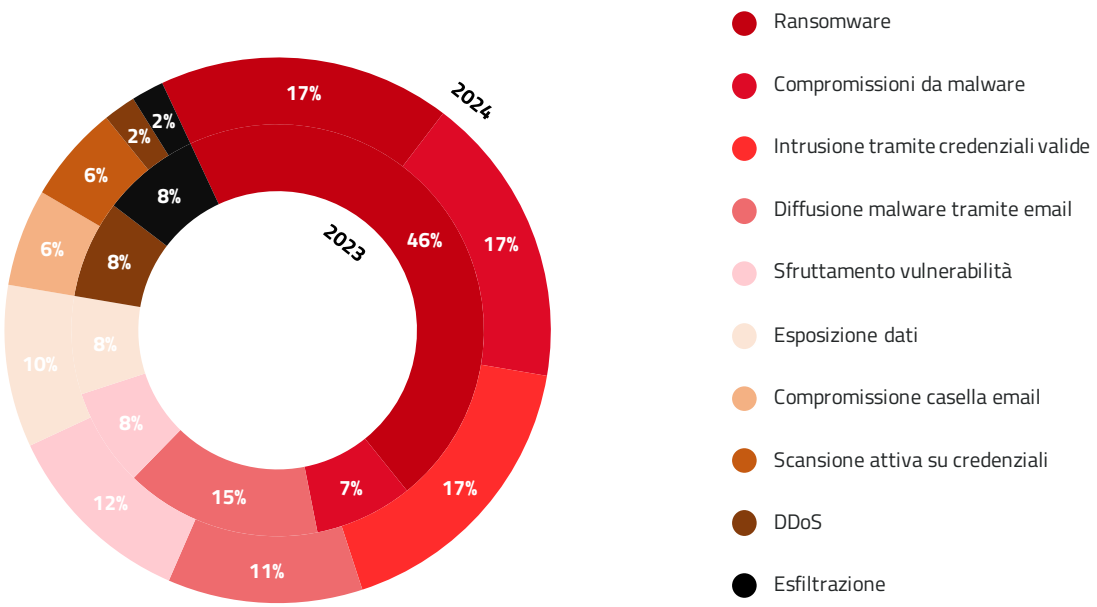


Figura 4: tipologie di minacce rilevate negli incidenti nel periodo 2023-2024 (top 10)

Queste tipologie di incidenti possono non solo interrompere i servizi e compromettere la **privacy dei pazienti**, ma anche mettere a rischio la sicurezza delle **informazioni mediche sensibili**.

Oltre agli impatti operativi e sulla protezione dei dati non può essere escluso un potenziale **danno reputazionale** per l'ente sanitario coinvolto, con possibili ripercussioni nel medio lungo periodo sulla fiducia da parte dell'utenza e dei soggetti operanti nel settore sanitario.

Sulla base dei dati esposti in Figura 3 e Figura 4, la successiva Figura 5 rappresenta le **principali minacce** al settore sanitario, offrendone una definizione e una sintesi dell'andamento corrispondente nel periodo di osservazione.

Figura 5: le principali minacce nel settore (2023-2024)

1.1.2 Focus eventi cyber e incidenti rilevati nel 2025

Nel periodo da **gennaio** a **settembre 2025** il numero complessivo degli **eventi cyber è aumentato di circa il 40%** rispetto allo stesso intervallo del 2024. Il CSIRT Italia ha infatti censito **60 eventi** a fronte dei 42 rilevati nell'anno precedente[6]. Mentre, il numero di incidenti è diminuito: **23** rispetto ai 47 del 2024, anno in cui un unico attacco di tipo *supply chain* causò 31 incidenti in altrettanti soggetti. In Figura 6 sono riportati gli eventi e gli incidenti dei primi nove mesi del 2025.

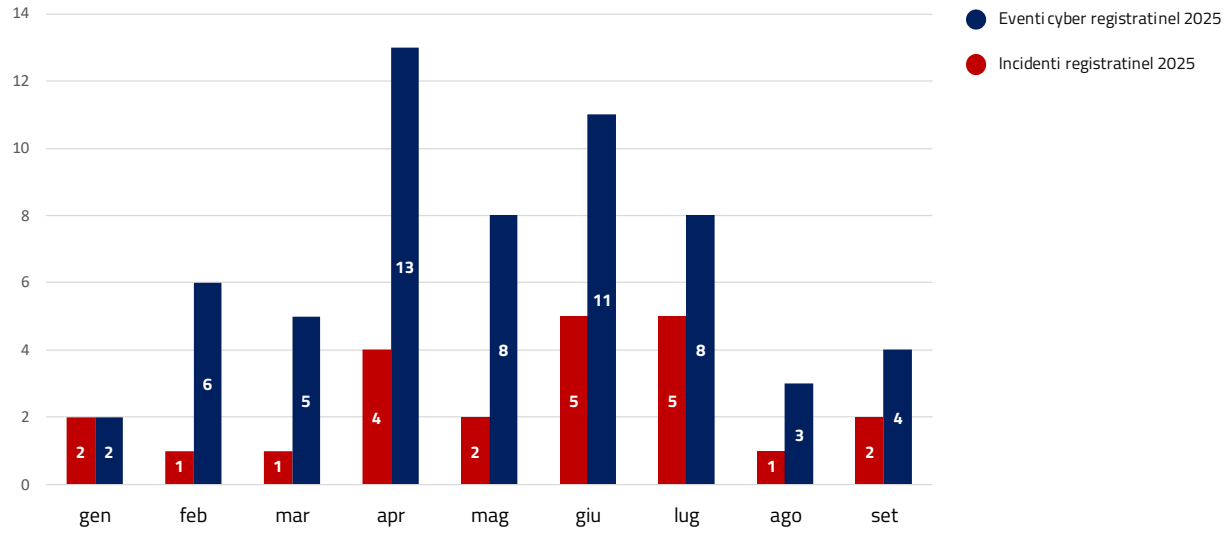


Figura 6: eventi cyber e incidenti nel 2025

In Figura 7 sono riportate le **principali tipologie** di minacce rilevate negli eventi cyber e negli incidenti dei primi nove mesi del 2025, da cui emerge che le minacce maggiormente rilevate risultano essere la **scansione attiva su credenziali**, il **phishing**, **compromissione delle caselle e-mail** e **esposizione dati**, a conferma della centralità del vettore e-mail e dell'utilizzo di tecniche basate sull'ingegneria sociale per la diffusione di campagne malevole.

Tali fenomeni risultano in larga parte propedeutici a fasi successive di compromissione. La raccolta di credenziali, in particolare, costituisce una componente preparatoria funzionale alla realizzazione di attacchi più strutturati, quali l'accesso illecito ai sistemi, il movimento laterale all'interno delle reti e l'esfiltrazione di informazioni personali.

Nel medesimo periodo, sono stati rilevati numerosi tentativi di ricognizione e di invio di messaggi di posta elettronica fraudolenti, finalizzati ad acquisire informazioni o a indurre il personale a interagire con allegati malevoli e link verso siti di raccolta credenziali. Queste attività, sebbene spesso d'impatto limitato, contribuiscono al consolidamento di un insieme di tecniche

[6] Si noti che determinati incrementi sono ascrivibili anche all'aumentata capacità del CSIRT Italia di rilevare eventi, incidenti e vulnerabilità, nonché al modificato impianto normativo.

preparatorie finalizzate alla compromissione progressiva dei sistemi informativi.

In questo contesto, il monitoraggio delle piattaforme di scambio illecito di dati ha consentito di individuare credenziali riconducibili a diversi enti e operatori sanitari, evidenziando la circolazione di informazioni potenzialmente utilizzabili per azioni di intrusione mirata o campagne di social engineering.

Gli attacchi di tipo **ransomware**, nel 2025 sono diminuiti, ma pur presentando un numero inferiore di eventi rispetto ad altre categorie di minaccia, continuano a rappresentare la tipologia con l'impatto più elevato, sia in termini di interruzione dei servizi essenziali, sia di perdita di disponibilità e integrità dei dati.

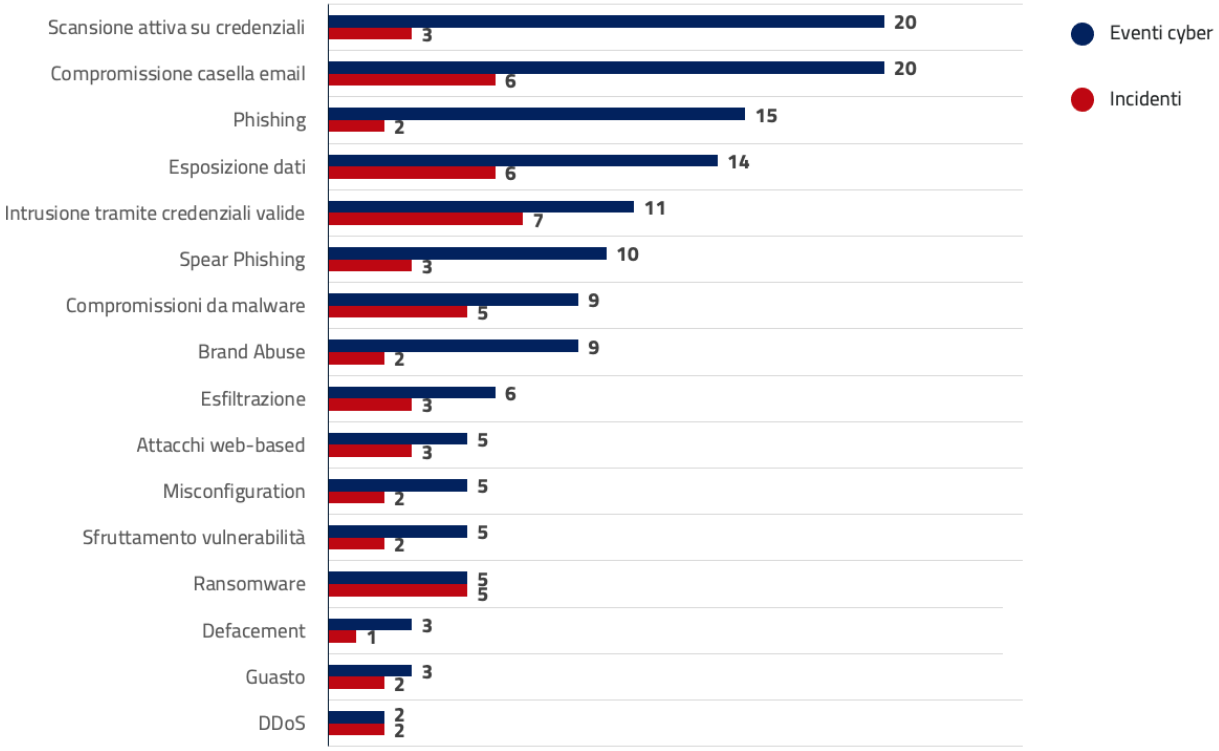


Figura 7: tipologie di minacce rilevate negli eventi cyber e incidenti nel periodo 2025 (gennaio-settembre)

1.1.3 Analisi degli impatti nel periodo 2023-2025

La numerosità degli attacchi di tipo ransomware potrebbe far pensare ad impatti esclusivamente sulla disponibilità dei servizi. In realtà le evidenze riscontrate nelle attività del CSIRT Italia sono più complesse. Se è vero, infatti, che negli **ospedali** gli impatti maggiori si sono registrati principalmente sulla **disponibilità** dei servizi, a causa della cifratura dei file, è altresì vero che sono stati rilevati anche altri impatti sulle infrastrutture IT: esfiltrazioni di dati (**riservatezza**), non sempre ai fini di riscatto, modifiche ai dati (e quindi perdita dell'**integrità**, con conseguente impossibilità per gli operatori sanitari di utilizzare alcuni macchinari) e cancellazioni di file

(**disponibilità**). In particolare, gli impatti rilevati sono stati:

- **blocco temporaneo** dell'erogazione di almeno un servizio, nella maggioranza dei casi, ma anche:
  - blocco di tutti i servizi IT;
  - blocco di tutti i servizi tranne uno;
  - blocco di almeno due servizi;
- **esfiltrazione di dati** con e senza cifratura;
- **modifiche arbitrarie dei dati effettuate dagli attaccanti** (violazione dell'integrità dei dati).

1.2 Analisi di un caso tipo di ransomware

Per il settore sanitario nel 2024 l'Agenzia ha registrato **10 eventi ransomware** significativi, valore in linea con l'andamento dell'anno precedente. Nel 2023, infatti, il dato si è attestato sempre su **10 eventi ransomware**, al tempo in aumento del **22%** rispetto al 2022.

Il **CSIRT Italia** da prassi interviene, anche in loco, a supporto della vittima, raccogliendo le evidenze e conducendo l'analisi forense sui sistemi della vittima. Sulla base delle evidenze raccolte, il CSIRT Italia definisce un piano di attività finalizzate al ripristino della piena efficienza dei servizi ospedalieri impattati, e fornisce le raccomandazioni necessarie all'innalzamento della postura di sicurezza dell'infrastruttura.

Le tipiche fasi di un incidente ransomware sono rappresentate in Figura 8, mentre all'indirizzo https://www.acn.gov.it/portale/w/report-su-minaccia-ransomware è possibile scaricare un documento di analisi approfondita della minaccia ransomware redatto dall'Agenzia, comprensivo di un insieme strutturato di raccomandazioni di ausilio alle attività di risposta ad un incidente di tipo ransomware, frutto dell'esperienza del CSIRT Italia nel supportare la gestione degli incidenti.

RANSOMWARE
le fasi di un caso tipo di ransomware

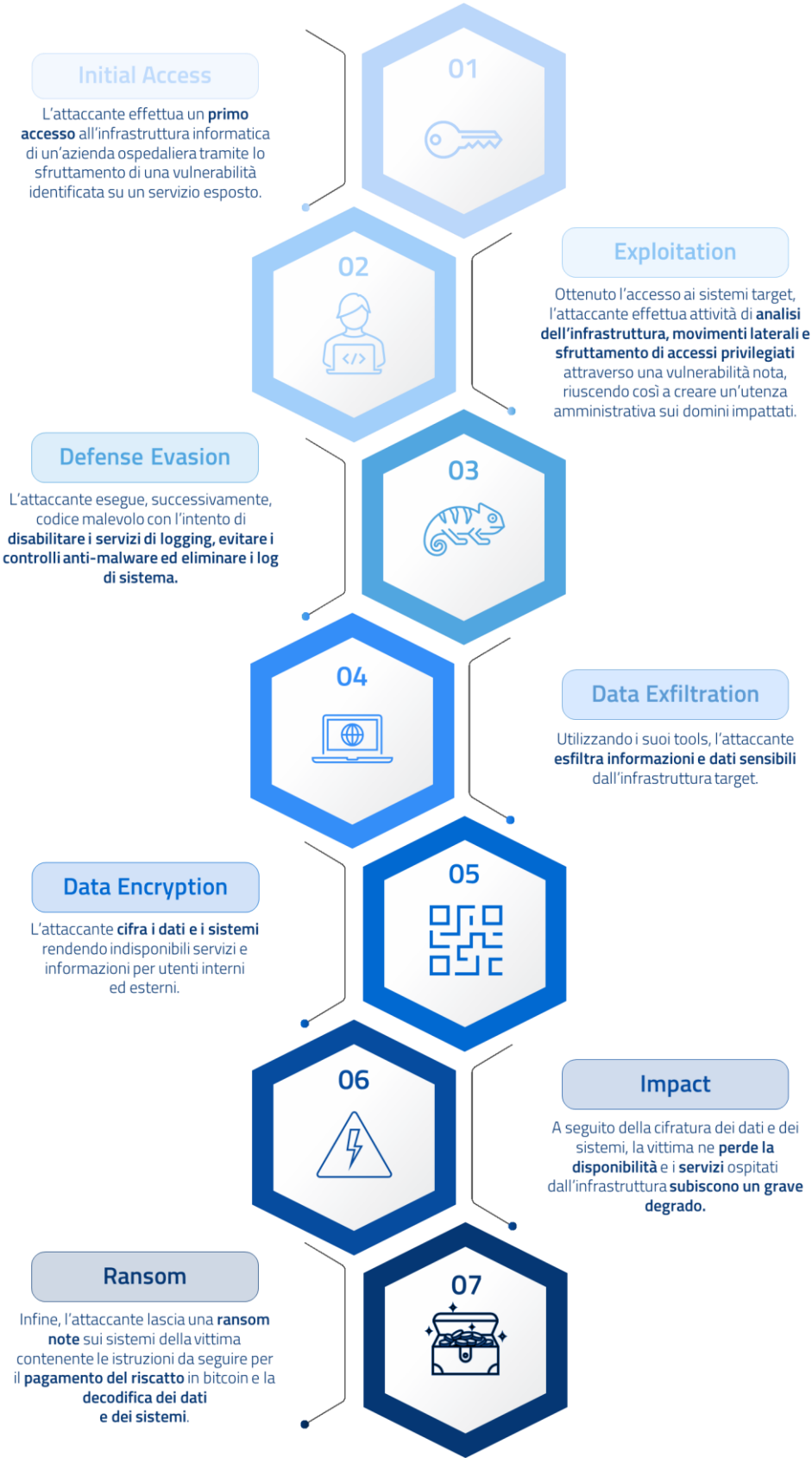


Figura 8: le fasi di un caso tipo di ransomware

2 VULNERABILITÀ ESPOSTE DEL SETTORE

Sviluppare strategie di sicurezza efficaci per il settore richiede l'identificazione accurata delle **vulnerabilità** nei servizi e dispositivi. Le vulnerabilità esposte possono rappresentare rischi di sicurezza per i sistemi informatici utilizzati nel settore sanitario, potenzialmente compromettendo la **privacy dei dati dei pazienti** e la **sicurezza delle informazioni mediche.** Pertanto, è fondamentale monitorare e affrontarle prontamente per garantire la sicurezza e l'integrità dei sistemi e delle informazioni.

L'insieme dei dispositivi esposti su internet, delle loro vulnerabilità e delle loro errate configurazioni costituisce la "**superficie di attacco esposta**", ovvero l'insieme di punti critici che offrono accessi ai potenziali attaccanti.

Ovviamente, non tutte le criticità riscontrate hanno lo stesso livello di gravità. Ve ne sono alcune, con gravità alta, come quelle associate a **vulnerabilità critiche** che permettono ad un attaccante di assumere con facilità il controllo del servizio o del dispositivo esposto, mentre ve ne sono altre meno gravi che spesso sono solo errate configurazioni non direttamente sfruttabili da un attaccante, ma, comunque, indice di un **servizio potenzialmente poco manutenuto** e **presidiato**.

L'analisi riportata in questa sezione è stata svolta **analizzando passivamente** (ovvero senza interazione diretta) oltre 50.000 indirizzi IP associati al settore sanitario[7] dal 1° aprile 2024 al 31 settembre 2025. Su questi ultimi è stato possibile identificare un elevato numero di criticità

[7] L'analisi qui riportata prende in considerazione una porzione limitata della superficie esposta del settore sanitario: i soggetti di questo settore fanno spesso uso di aziende terze per la gestione delle proprie infrastrutture informatiche rendendo impossibile, con i dati a disposizione, individuare l'esatto indirizzamento IP in uso all'azienda sanitaria. Tuttavia, si ritiene che la superficie monitorata sia un campione sufficientemente rappresentativo del settore.

(spesso sullo stesso servizio ne sono presenti diverse) alle quali è stato attribuito un livello di gravità.

Tutte le criticità rilevate sono state classificate nelle **tre categorie** riportate in Figura 9.

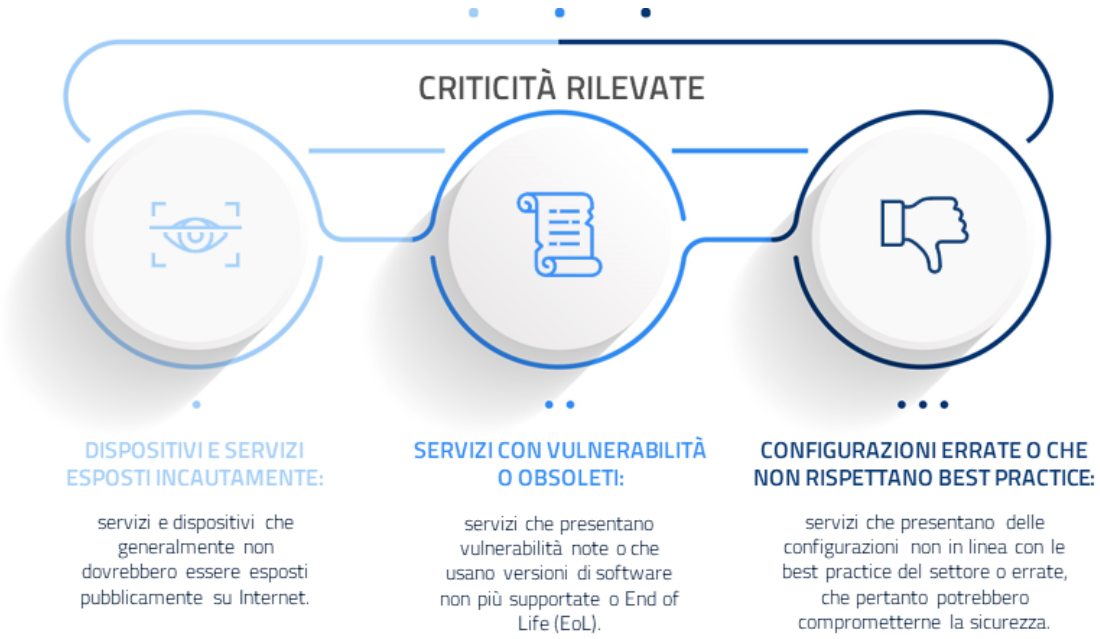


Figura 9: classificazione delle criticità rilevate nel settore sanitario

La classificazione mostrata risulta utile per caratterizzare al meglio le azioni di **mitigazione delle criticità** necessarie e, allo stesso tempo, supportare l'implementazione delle raccomandazioni indicate nei successivi paragrafi.

Se generalmente per la **prima categoria** è sufficiente evitare l'esposizione di tali servizi su Internet, tutte le criticità riscontrate nella **seconda categoria** necessitano di un aggiornamento del software per essere risolte. Infine, le criticità appartenenti alla **terza e ultima categoria** possono essere risolte nella maggior parte dei casi modificando le configurazioni del servizio.

Analizzando l'andamento nel tempo delle criticità riscontrate mediamente ogni mese, riportato in Figura 10, emerge come la maggioranza di esse afferisca alla terza categoria (ovvero "configurazioni errate"), mentre le criticità relative ai servizi e ai dispositivi esposti incautamente risultino essere in larga parte minori. Si rappresenta che **il significativo incremento del numero di servizi con configurazioni errate è ascrivibile anche all'aumentata capacità del CSIRT Italia di rilevare tali criticità**.

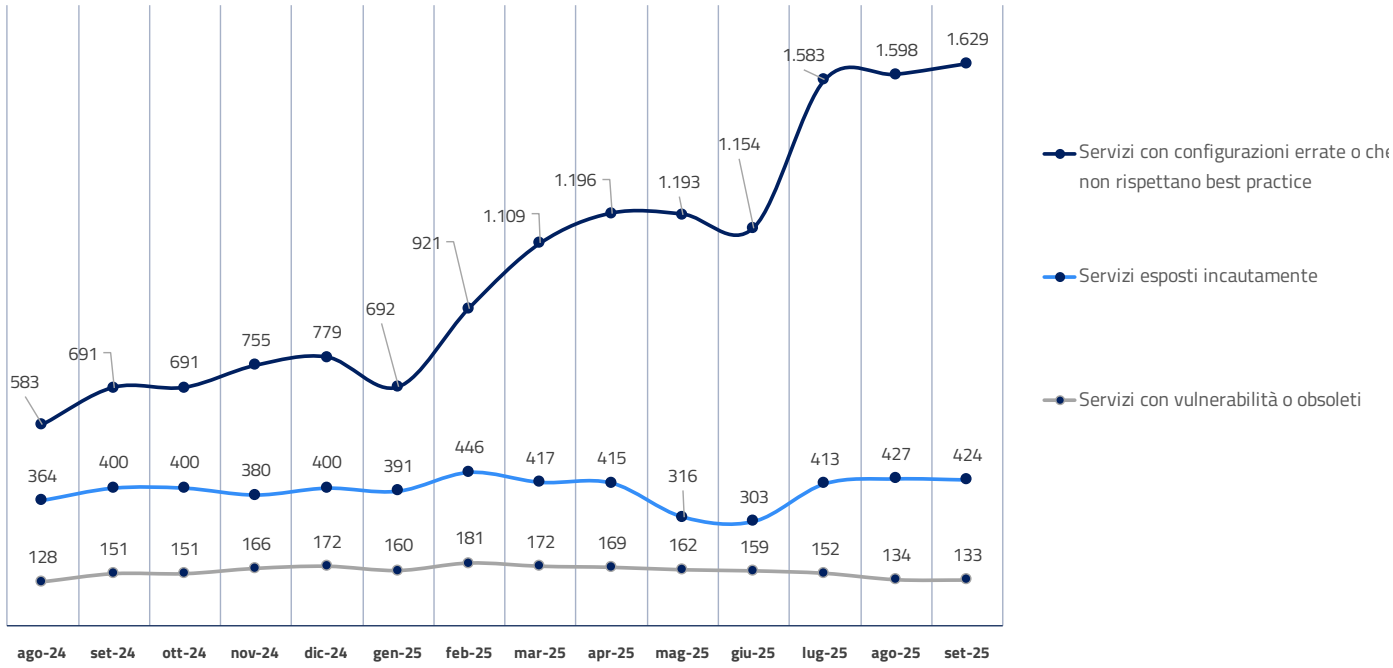


Figura 10: media giornaliera del numero di criticità esposte per categoria da agosto 2024 a settembre 2025

3 RACCOMANDAZIONI E CONTROMISURE

Il presente capitolo offre un'analisi delle **peggiori pratiche di sicurezza** riscontrate nel corso delle attività **DFIR** (*Digital Forensic Incident Response*), ovvero quelle in cui il personale del CSIRT Italia ha supportato**, in loco o da remoto**, le vittime degli incidenti nel settore sanitario.

L'analisi che segue mira a promuovere l'adozione di prassi e comportamenti responsabili attraverso l'identificazione di cattive pratiche, fornendo delle **raccomandazioni** per agevolare la mitigazione delle pratiche errate rilevate e incentivando il rafforzamento della sicurezza di sistemi, dati e risorse digitali.

Nella pagina a seguire sono riassunte **le più gravi pratiche errate rilevate dai team d'intervento**. Ognuna di queste è corredata di alcune **raccomandazioni** per agevolarne la mitigazione.

3.1 Le principali bad practices e le contromisure

PEGGIORI PRATICHE RILEVATE	CONTROMISURE
Assenza di autenticazione multi-fattore sulle Virtual Private Network (VPN).	Implementazione dell'autenticazione multifattore (MFA).
Utilizzo di protocolli di autenticazione e cifratura obsoleti.	Utilizzo di versioni recenti di protocolli di autenticazione e comunicazione e disabilitazione protocolli obsoleti sul Domain Controller).
Password Policy inadeguata.	Creazione di una password policy che rispetti le best practice, anche supportata dagli strumenti preposti quali password manager.
Errata gestione dei privilegi utente.	Applicazione del principio del privilegio minimo su account utente e di servizio e revisione periodica dei privilegi ad essi assegnati.
Assenza di inventario dei servizi critici.	Redazione e costante aggiornamento di una lista aggiornata dei servizi IT critici e una lista delle funzionalità e dati dati critici degli ospedali.
Prodotti non aggiornati.	Creazione di un asset inventory dei dispositivi con relativa versione del software e firmware in uso; applicazione degli aggiornamenti di sicurezza ed eventuali patch rilasciati dai produttori; isolamento o dismissione dei dispositivi non più supportati e non aggiornabili.
Errata gestione di Microsoft Active Directory.	Corretta architettura e gestione dell'AD secondo le indicazioni di hardening fornite dal Vendor e utilizzo di tool specifici che consentano il monitoraggio e il rilevamento di criticità nella configurazione.
Errata gestione dei log.	Redazione di una policy di gestione dei log per il rilevamento e l'analisi degli eventi, adozione di strumenti dedicati quali SIEM, SOAR, XSOAR e log collector e backup dei log e corretta conservazione degli stessi.
Errata gestione dei backup.	Implementazione di una politica di gestione dei backup per la memorizzazione in porzioni di rete segregate ed una frequenza di backup proporzionata alla criticità delle informazioni memorizzate, nonché un piano di ripristino in caso di perdita dei dati.
Rete non segmentata.	Rete isolata e segmentata per gestire proattivamente la sicurezza e la conformità, e utilizzo approccio Zero Trust in caso di gestione decentralizzata dell'infrastruttura IT.
Mancanza di procedure di Incident Response.	Redazione e aggiornamento costante di un piano di risposta agli incidenti informatici che individui ruoli e responsabilità di tutti i soggetti incaricati nelle varie fasi della gestione degli incidenti, e che includa elenchi di eventuali fornitori di servizi, di hardware e di software.
Assenza di Endpoint Detection and Response.	Adozione di soluzioni EDR o XDR in grado di rilevare e bloccare comportamenti anomali negli host.

3.2 Raccomandazioni generali

In base a quanto rilevato dalle attività operate dall'Agenzia e dagli esiti del monitoraggio proattivo effettuato nel settore sanitario, l'ACN raccomanda per il settore sanitario **l'implementazione delle pratiche di sicurezza** rappresentate nella figura a seguire, che consentirebbero un incremento sensibile nella postura di sicurezza delle strutture sanitarie.

È chiaro che tali raccomandazioni risultano più efficaci e gestibili ove assicurata una **governance centralizzata della cybersecurity e dell'IT**, garantendo la separazione di ruoli (*Segregation of Duties*), ottenibile con un approccio programmatico, strutturato e integrato, fondato sulla gestione del rischio. Infatti, solo attraverso la definizione di un corretto assetto organizzativo, in termini di ruoli e responsabilità, ed efficienti processi di sicurezza sarà possibile, insieme all'adozione di soluzioni tecnologiche, ridurre il rischio di rimanere vittime di incidenti informatici.

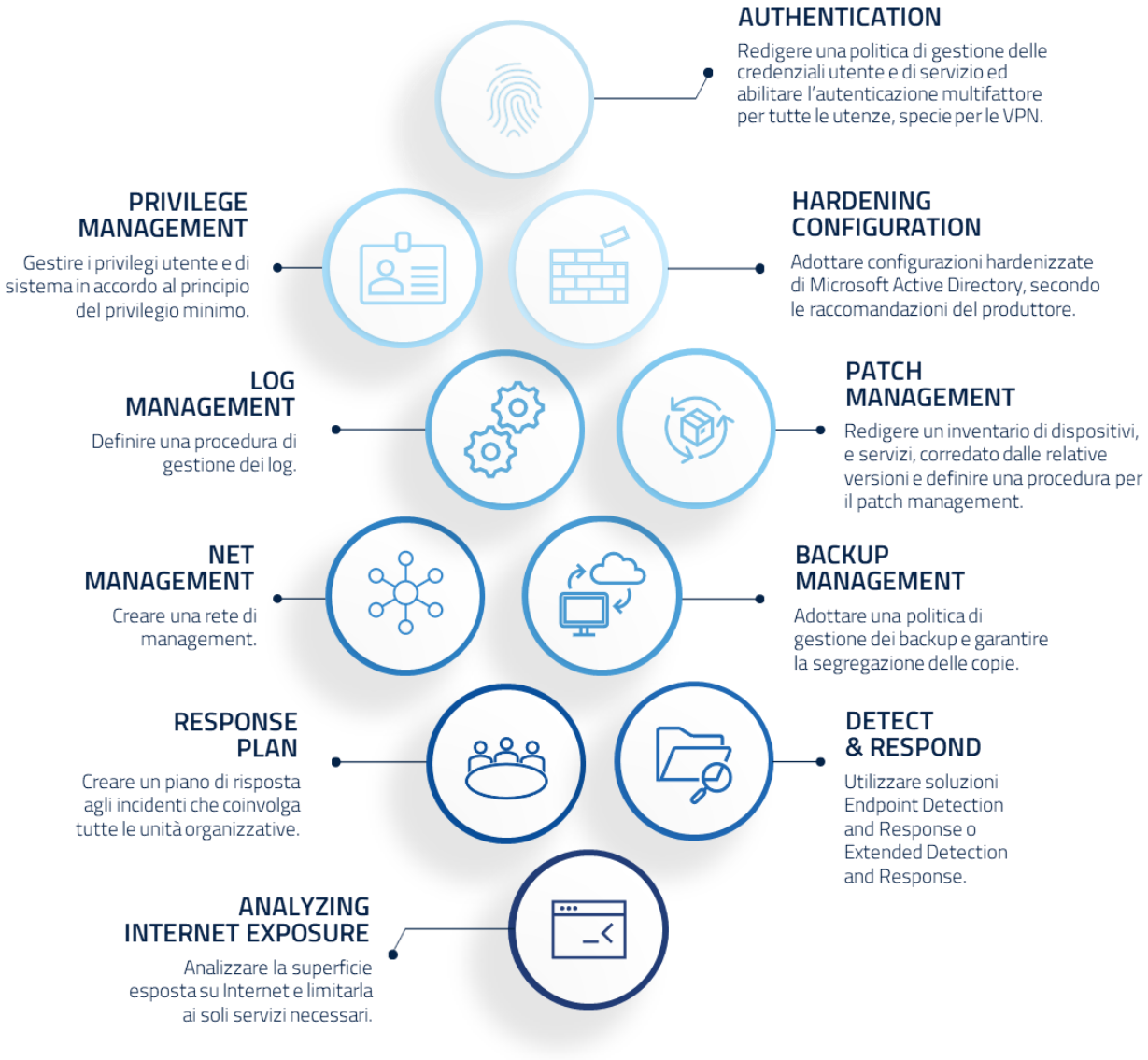


Figura 11: le 10 raccomandazioni più rilevanti per il settore

TLP:CLEAR

IN CASO DI INCIDENTE CONTATTA CSIRT ITALIA

Il **CSIRT Italia** si occupa delle attività di natura reattiva e proattiva nei confronti della minaccia cibernetica; è hub nazionale per la ricezione delle segnalazioni e notifiche di incidenti ed eventi e fornisce supporto ai soggetti impattati. Indirizza, altresì, i prodotti di allertamento preventivo sulle minacce e relative attività di mitigazione attraverso i suoi canali pubblici quali la sua pagina web, l'account X e il canale Telegram.

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

https://segnalazioni.acn.gov.it/