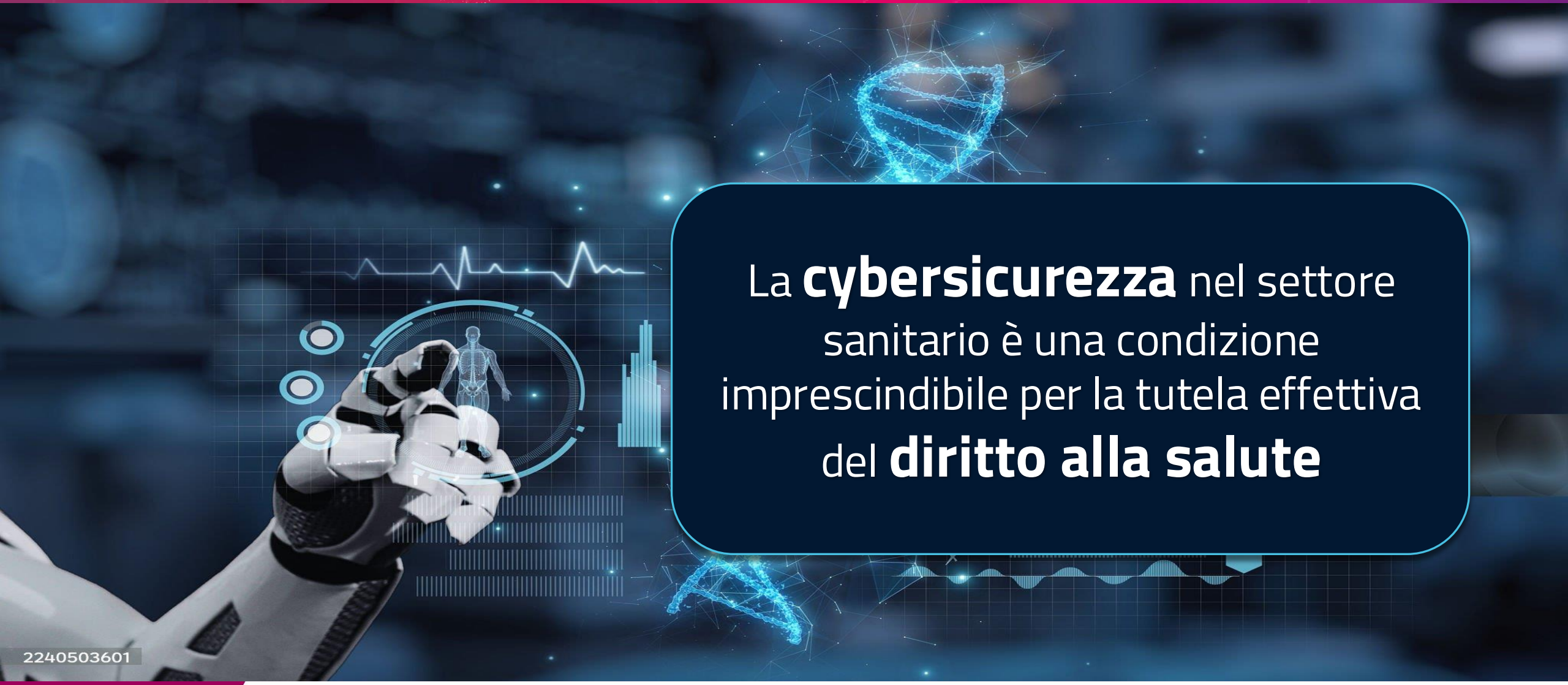
Agenzia per la cybersicurezza nazionale

Marcello Albergoni
Vice Capo di Gabinetto



La **cybersicurezza** nel settore sanitario è una condizione imprescindibile per la tutela effettiva del **diritto alla salute**

2240503601

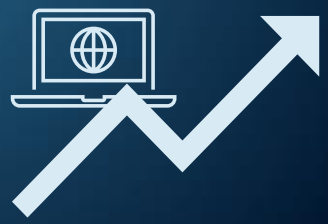
L'impiego dell'IA in questo ambito strategico

OPPORTUNITÀ

Telemedicina

Fascicolo Sanitario Elettronico (FSE)

Sistemi di IA clinica



VULNERABILITÀ

RISCHI ED IMPATTI

I NUMERI

primi 5 mesi del 2026

GENNAIO – MAGGIO 2025 vs GENNAIO - MAGGIO 2026

2025	EVENTI, INCIDENTI E VITTIME	2026
34	eventi cyber	**135**
10	incidenti	**94**
104	vittime univoche*	**121**

*Agli eventi sono state associate una più vittime, in molteplici casi interessate più volte.

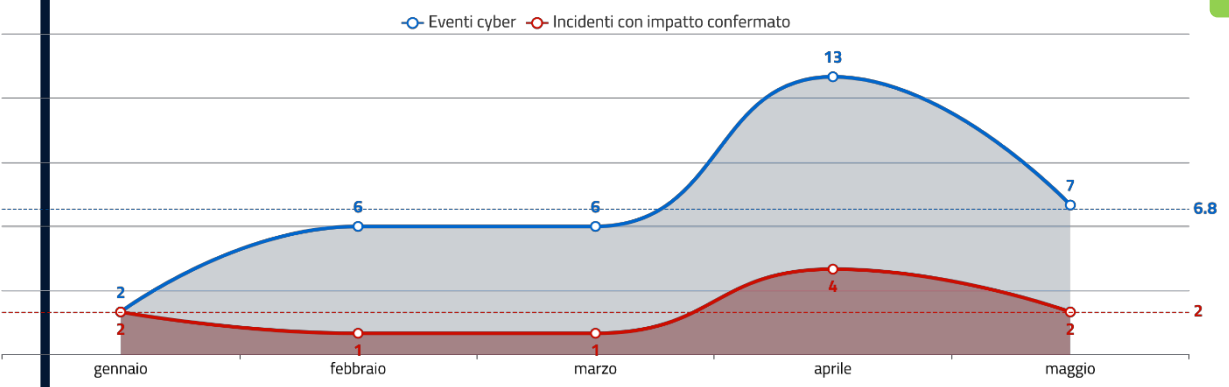
GLOSSARIO

Incidente cyber: evento con impatto confermato dalla vittima o dal CSIRT Italia

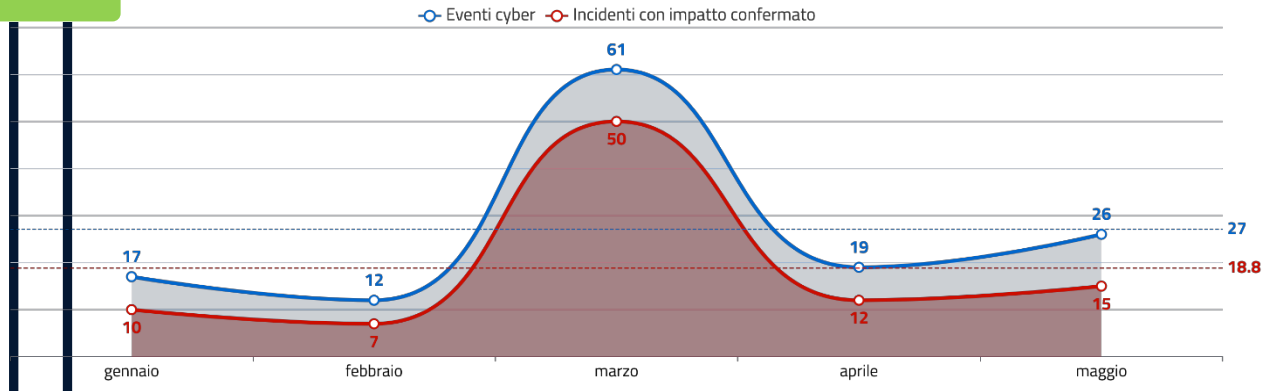
MONITORAGGIO E ALLERTAMENTO	NUMERI
asset potenzialmente **vulnerabili**	**520**
comunicazioni di **allertamento** inviate	**311**
segnalazioni di vulnerabilità **Legge n. 90/24** (anche massive)	**233**

EVENTI E INCIDENTI

GENNAIO – MAGGIO 2025



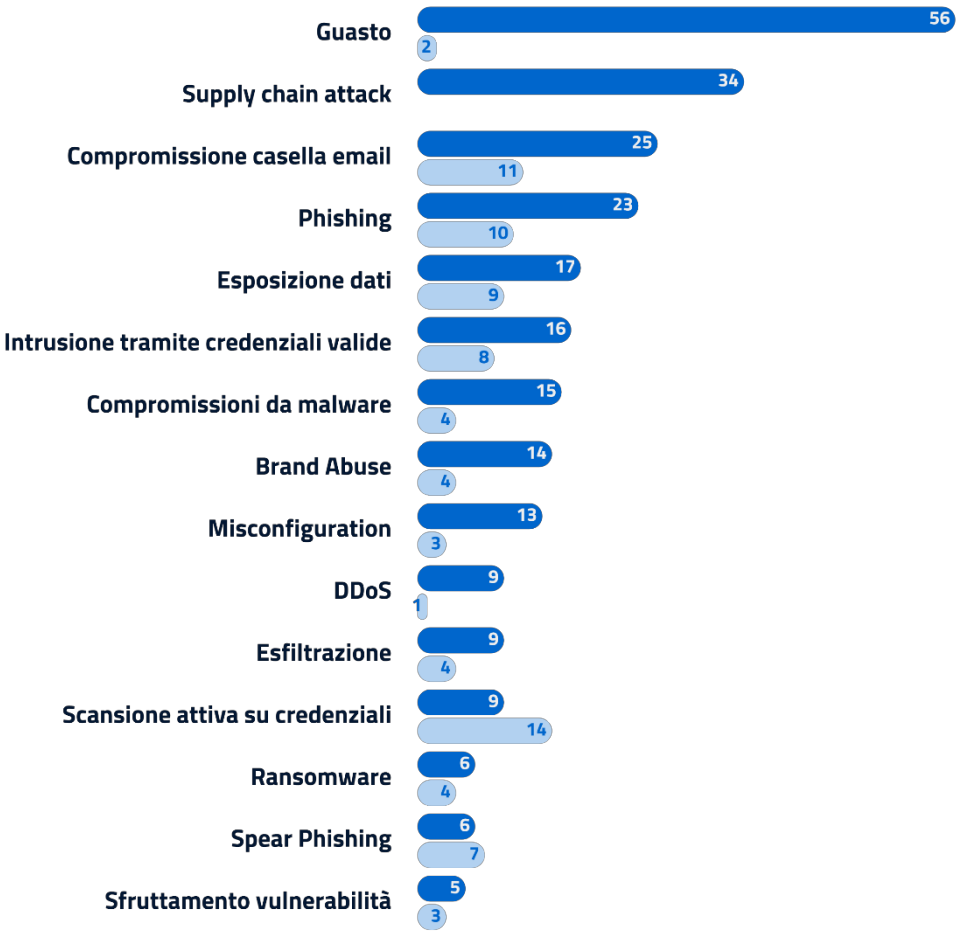
GENNAIO - MAGGIO 2026



Registrati **135 eventi cyber** nel periodo **gennaio - maggio 2026**. Nello stesso periodo del **2025** sono stati **34**
Di questi, **94** sono stati classificati quali **incidenti**. Nello stesso periodo del **2025** sono stati **10**

LEGENDA
EVENTI CYBER
INCIDENTI CON IMPATTO CONFERMATO

PRINCIPALI MINACCE RILEVATE NEGLI EVENTI



MINACCE CYBER PIÙ FREQUENTEMENTE RILEVATE NEL SETTORE SANITARIO

LEGENDA

- Primi 5 mesi 2026
- Primi 5 mesi 2025

Si riportano le **tipologie di minacce rinvenute** negli eventi nel periodo gennaio – maggio 2026, confrontate con lo stesso periodo del 2025.

Emerge come Guasto, Supply Chain attack e Compromissione casella email siano state le minacce prevalenti nei primi 5 mese del 2026.
Nel 2025 furono Compromissione casella email, Scansione attiva su credenziali e Phishing

FOCUS MINACCE

ATTACCO HACKER AD OSPEDALE DI NAPOLI, CHIESTO RISCATTO

(ANSA) - "L'azienda ospedaliera universitaria Luigi Vanvitelli di Napoli ha reso noto di essere stata vittima di un attacco informatico di tipo ransomware e che sono in corso valutazioni per definire la portata dell'attacco, oltre che la natura dei dati oggetto della violazione".

Lo fa sapere l'Agenzia per la cybersicurezza nazionale, che ha inviato una propria squadra di esperti presso il nosocomio napoletano per contribuire all'analisi dell'attacco e al ripristino dei sistemi impattati.

OSPEDALE VANVITELLI NAPOLI 3

MATERA, ATTACCO HACKER AL SISTEMA INFORMATICO SANITARIO DELLA BASILICATA: ECCO UNA COMUNICAZIONE PER I CITTADINI

27 MAGGIO 2024

Comunicazione pubblica della direzione generale per la salute e le politiche della persona della Regione Basilicata ai sensi dell'art. 34, par. 3, lett. c), del Regolamento (UE) 2016/679 **in merito all'attacco hacker** subito dall'Azienda del Servizio Sanitario (Azienda Sanitaria di Matera, Azienda Sanitaria di Potenza, AOR San Carlo Potenza ed IRCCS-CROB Rionero in V.) e dalla Regione Basilicata nel Gennaio 2024.

13 MAGGIO 2023 12:48

Migliaia di persone stanno leggendo i dati sanitari rubati dagli hacker in Abruzzo

Il gruppo hacker Monti ha sferrato uno degli attacchi ransomware più importanti nella storia della cybersecurity in Italia. Vittima dell'attacco sono stati i sistemi informatici della Asl 1 – Avezzano Sulmona L'Aquila: Monti dice di aver trafugato 522 Gb di dati sanitari. Ora stanno cominciando a diffonderli sul dark web.

Attacco hacker Ospedale Alessandria, l'esperto: "Vittime anche più illustri ma esistono contromisure"

ALESSANDRIA – "*Purtroppo questo tipo di cyber criminali ha colpito aziende anche più illustri dell'Ospedale di Alessandria, basti pensare alla statunitense* ***Dassault Falcon Jet****, produttrice di aerei da combattimento*". **Cosimo Anglano**, professore ordinario di Informatica del Dipartimento di Scienze e Innovazione Tecnologica dell'Università Piemonte Orientale, ha commentato così il grave attacco hacker dello scorso 29 dicembre ai danni dell'Ospedale di Alessandria. Su Radio Gold abbiamo intervistato il docente per saperne di più.

RANSOMWARE

Gli **attacchi ransomware** sono operazioni malevole in cui attori informatici **bloccano l'accesso a dati** o **sistemi** attraverso tecniche di **cifratura**, richiedendo un riscatto per ripristinarne l'utilizzo.

Nel settore **sanitario**, tali attacchi sono **particolarmente critici** perché compromettono la **disponibilità** di informazioni essenziali, **interrompono l'erogazione dei servizi sanitari** e **mettono a rischio la vita dei pazienti**. Inoltre, **l'esfiltrazione di dati sensibili** espone strutture e individui a gravi violazioni della privacy e a sanzioni normative.

PRINCIPALI CAUSE ABILITANTI LA MINACCIA NEL SETTORE

GESTIONE DECENTRALIZZATA

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

OBSOLESCENZA DEI DISPOSITIVI

Apparati informatici obsoleti, non aggiornabili o supportati, che continuano ad essere utilizzati.

CARENZA DI PERSONALE DEDICATO A CYBERSICUREZZA

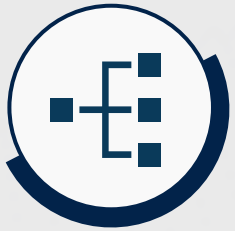
Il personale IT gestisce la sicurezza informatica senza avere risorse dedicate, facendo al meglio delle proprie possibilità.

I POTENZIALI PROBLEMI DELL'IA

I POTENZIALI PROBLEMI DELL'IA

I POTENZIALI PROBLEMI DELL'IA

Phishing avanzato e personalizzato



Automazione di attacchi su larga scala

Massificazione della minaccia

I POTENZIALI VANTAGGI DELL'IA

L'IA tuttavia può **supportare il rilevamento degli eventi cyber**

→ **analizzando grandi volumi di dati in tempo reale**,

→ identificando **anomalie** e segnali di **compromissione** con maggiore **rapidità** e **precisione** rispetto ai metodi tradizionali,

→ **potenziando così le capacità difensive** delle organizzazioni.

Misura #55

Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR

Anche dopo il PNRR l'attuazione della Strategia non si ferma

Interventi di potenziamento in ambito sanitario per le Regioni e le Province Autonome a valere sui Fondi nazionali

REPORT: LA MINACCIA CIBERNETICA AL SETTORE SANITARIO

Il report viene aggiornato periodicamente. Il prossimo aggiornamento con dati fino a settembre 2026 sarà pubblicato entro **ottobre**.

https://www.acn.gov.it/portale/analisi-sullo-stato-della-minaccia

AI E APPLICAZIONI SANITARIE

VIGILANZA

- ✓ MDR - Medical Device Regulation
- ✓ IVDR - In Vitro Device Regulation

SUPPORTO AL SETTORE SANITARIO

Reg. Cloud (ACN 2024)

adeguamento delle infrastrutture digitali della PA

adeguamento delle infrastrutture dei servizi cloud degli operatori privati

qualifica dei servizi cloud per la PA

Ecosistema dei Dati Sanitari (EDS)

INTEGRAZIONE tra Cybersicurezza e Protezione dei dati

GPDP

D.L. n. 82/2021

Protocollo d'intenti del 2022

Innovazione sicura,

responsabile

e centrata sull'uomo

Papa Leone XIV (*Magnifica Humanitas* 2026), **Governatore della Banca d'Italia** (*Relazione annuale*, 2026)

Non cediamo la nostra intima umana sovranità

https://www.acn.gov.it
m.albergoni@acn.gov.it