

Cybersecurity

Proteggere il digitale per difendere la vita reale

Cyber Pills

03 Febbraio 2026

Non serve essere grandi per essere un bersaglio: **basta essere connessi**



Gli attacchi informatici sono reali e vicini:
un ransomware può bloccare un ospedale, un
attacco alla supply chain, fermare un intero
settore, un blackout digitale, **spegnere una
città**



La cybersecurity è diventata la prima
linea di difesa del nostro **modo di
vivere**



Cyber Minacce in Italia

Anno 2025

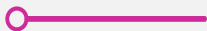
Scenario Cyber Italia 2025

Nel corso del 2025, l'Italia ha registrato un'escalation senza precedenti in termini di **attacchi informatici**: un aumento esponenziale in numero, complessità e impatto che ha messo alla prova la resilienza delle organizzazioni pubbliche e private, segnando un punto critico per la sicurezza digitale del Paese.

2.802

Eventi cyber

Gli attaccanti stanno facendo campagne sempre più opportunistiche



650

Incidenti

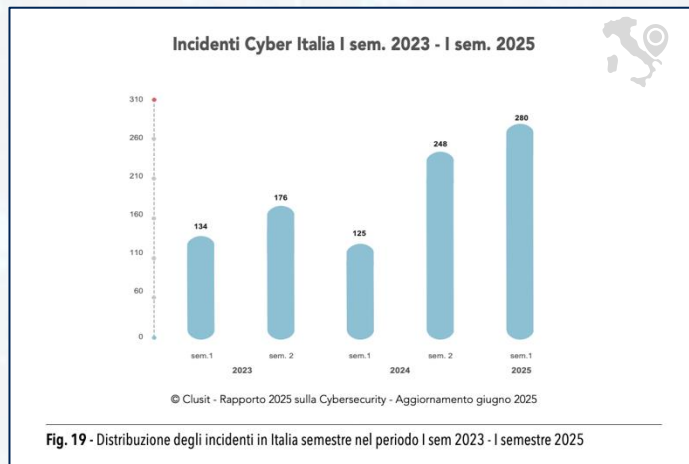
2 incidenti informatici confermati al giorno



Incidenti cyber 2025

Minacce sempre più sofisticate ma aumenta la consapevolezza nel Paese

Nel corso del 2025 l'Agenzia per la Cybersicurezza Nazionale (ACN), attraverso il CSIRT Italia, ha censito 2.802 eventi cyber di cui 650 incidenti con impatto confermato, evidenziando un incremento complessivo degli eventi rispetto al periodo precedente, attribuibile al rafforzamento delle capacità di rilevazione e al nuovo quadro normativo



Settori più colpiti:

Pubblica Amministrazione (centrale e locale), Telecomunicazioni, Sanità e Energia

Tipologia	1° Sem.2025	2° Sem.2025
Ransomware	91	82
DDoS	598	366
Phishing / URL malevoli	1.530	927
Esposizioni dati	186	232

Vettori e tecniche predominanti nel 2025

Dalle vulnerabilità note all'intelligenza artificiale: i nuovi strumenti del cybercrime

 Spear-phishing mirato	• Email/sms iper-personalizzati usati per ingegneria sociale ad alto valore (CEO fraud, “urgent payment”); • Aumento delle campagne che integrano deepfake vocali per autenticare richieste
 Sfruttamento di vulnerabilità note	• Attacchi che prendono di mira Citrix NetScaler, VPN e web-server non patchati; • Exploit automatici per ottenere accesso iniziale e pivoting
 Botnet attive (es. IcedID, Bumblebee)	• Infrastrutture usate per DDoS, distribuzione di malware, delivery di payload e movimenti laterali all'interno delle reti compromesse
 Malware e exploit assistiti da IA/LLM	• Modelli che aiutano a scrivere o adattare codice malevolo, accelerando lo sviluppo di exploit e bypass delle difese basate su signature
 Identità sintetiche e frodi documentali	• Generazione di volti, documenti e profili sintetici tramite AI per bypassare KYC, aprire conti fraudolenti o sostenere campagne di social engineering

Cyber Index PMI

Principali risultati e criticità emerse

CYBER
INDEX PMI
LA CULTURA
DIGITALE PROTEGGE
LA TUA IMPRESA

CHECKUP
Sicurezza IT
PID
Cyber
Check

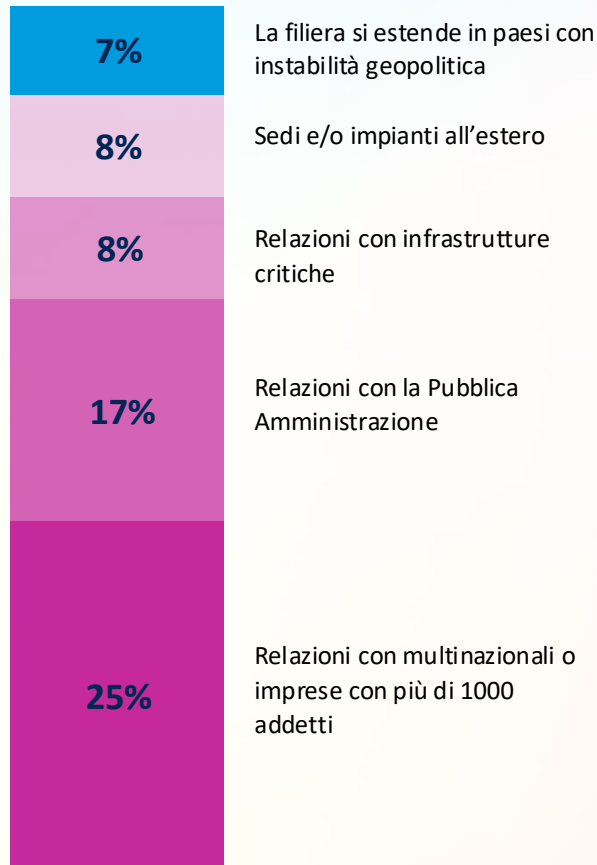
 Indicatore	 Valore	 Nota
Punteggio medio complessivo	52 / 100	Sotto soglia per la sufficienza
PMI con approccio “maturo”	15%	Solo 1 su 7 ha un approccio strategico completo
Distribuzione PMI per livello	Principiante: 18% Informato: 38% Consapevole: 29% Maturo: 15%	La maggioranza resta a metà strada
Identificazione del rischio	45 / 100	Area più debole: non è chiaro che cosa proteggere
Attuazione misure tecniche	57 / 100	Qualche progresso, ma lento (+1 dal 2024)
Approccio strategico	56 / 100	Migliora (+2 dal 2024), ma resta fragile
Copertura assicurativa cyber	31%	Cresce, ma minoranza
Uso fondi/bandi pubblici	~10%	48% non conosce le opportunità

Il ruolo cruciale delle PMI per la postura dell'intero

Quota di imprese che partecipa alle filiere critiche



- Opera all'interno di filiere critiche
- Non opera all'interno di filiere critiche



Quasi la metà delle PMI italiane opera in contesti sensibili, connessi a grandi player, PA o infrastrutture strategiche. Questo rende **la postura di sicurezza informatica delle PMI** cruciale per l'intero ecosistema nazionale, poiché un punto debole nella catena può compromettere la resilienza complessiva



Nasce un **nuovo quadro normativo** che
impone standard comuni
di sicurezza

Disposizioni europee in materia di sicurezza informatica

La stratificazione e complessità normativa

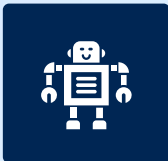
Non Specifiche

- ☐ Chip Act
- ☐ Data Act
- ☐ Digital Service Act



Include Disposizioni Cyber

- ☐ AI Act
- ☐ *Digital Euro Regulation**
- ☐ *European Health Data Space**



*In discussione**

Focalizzate Cyber

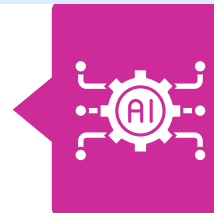
- ☐ NIS2, DORA
- ☐ Cyber Resilience Act
- ☐ RED
- ☐ Cybersecurity Act



GDPR
Dati personali



AI Act
Intelligenza
artificiale



Normativa Cyber EU
NIS 2, CRA, ..



Settoriali/Infrastrutture
DORA, CER



Governance, risorse e competenze

NIS 2 non è solo una direttiva: è una chiamata alla responsabilità digitale

GOVERNANCE

La leadership cyber parte dal vertice



- Coinvolgimento diretto del top management
- Strategia di sicurezza integrata nella governance aziendale
- Responsabilità chiare e tracciabili

RISORSE

Investire oggi per garantire resilienza domani



- Investimenti adeguati in persone, processi e tecnologie
- Collaborazione con partner e autorità competenti

COMPETENZE

La tecnologia evolve, le persone devono anticiparla



- Formazione continua e awareness diffusa
- Skill avanzate in risk management e incident response



Key takeaway verso un futuro digitale più sicuro



Gestione dei Dati e degli Asset

Protego ciò che conosco

Conoscenza del dato:



disporre di una mappatura completa dei dati trattati (dove sono, come si muovono, chi li utilizza), tramite inventari aggiornati di asset e servizi

Classificazione del dato:



attribuire ai dati un livello di criticità (operativi, strategici, sensibili, personali) per stabilire le priorità di protezione e definire le misure di sicurezza adeguate

Gestione degli asset:



inventariare i servizi, i sistemi e le applicazioni software che compongono i sistemi informativi e di rete, ivi incluse le applicazioni commerciali, open-source e sviluppi proprietari



Continuità operativa e gestione della crisi

La resilienza non si improvvisa: si costruisce ogni giorno

LE PRINCIPALI FASI DI GESTIONE DELLA CONTINUITÀ OPERATIVA



OBIETTIVI E REQUISITI



Garantire la capacità dell'organizzazione di mantenere i servizi essenziali anche in caso di incidente grave o crisi cyber.



Predisporre piani di business continuity e disaster recovery testati e aggiornati.



Attivare procedure di gestione della crisi per ridurre l'impatto e assicurare il ritorno alla normalità.



Coordinamento costante con ACN, CSIRT e Autorità competenti in caso di incidenti significativi.

Grazie!

Per info, comunicazione@tinextacyber.com

tinexta
cyber

think next,
secure now