2025

CYBERSECURITY REPORT

“Cybersecurity is not only a technical issue; it’s a matter of culture, awareness, and continuous adaptation”

planetica

"kybernetikès techne”

κυβερνητικ τχνη

"L'arte del governo (kybernetikès techne) consiste nel guidare con sapienza, prevenendo i pericoli e mantenendo la rotta sicura.”

CHE SIGNIFICATO HA **“KYBERNETIKÈS TECHNE”**

ORIGINE

Il termine cyber nella moderna espressione cybersecurity ha origini molto più antiche di quanto si possa immaginare. La parola greca antica kybernetès (κυβερνήτης) indicava il pilota di una nave, con la radice kyber- che significa "timone". Questa radice trova un parallelo nel latino guber, presente nel termine gubernator (timoniere). Entrambi i vocaboli derivano da un’antica radice indoeuropea legata al concetto di guida e direzione.
Questo concetto fu ripreso nel XIX secolo da André-Marie Ampère nella sua classificazione delle scienze e, successivamente, nel 1947 da Norbert Wiener, che coniò il termine anglicizzato cybernetics.

RIFLESSIONE SUL SIGNIFICATO

L’arte del governo (kybernetikès techne) consiste nel guidare con saggezza, prevenendo i pericoli e mantenendo la rotta sicura.
Questo antico concetto riflette esattamente ciò che oggi intendiamo per gestione della sicurezza informatica: la capacità di guidare e proteggere i sistemi informativi attraverso una governance efficace, anticipando le minacce e garantendo accessi e navigazioni online sicure.

SOMMARIO

PREFAZIONE

Il presente rapporto si propone come una bussola essenziale per orientarsi nel panorama sempre più articolato della cybersecurity, offrendo una lettura trasversale delle principali sfide, vulnerabilità e strategie di difesa che caratterizzano l'attuale scenario globale e nazionale. L'analisi condotta mette in luce come la sicurezza informatica rappresenti oggi una questione strategica che coinvolge trasversalmente governi, imprese e cittadini, in un contesto segnato da una rapida evoluzione tecnologica e da una crescente interconnessione tra sistemi e infrastrutture. Il documento raccoglie numerosi contributi, fornendo una visione aggiornata sulle minacce emergenti, quali l'impiego dell'intelligenza artificiale nei processi di attacco e difesa, l'escalation degli attacchi ransomware, la crescita degli infostealer e le criticità legate alla gestione della sicurezza in ambienti Cloud e Edge (il Cloud computing centralizza i dati in data center remoti, l'Edge computing elabora i dati presso o in prossimità della loro fonte). Particolare attenzione è dedicata alle implicazioni normative, con un focus su direttive come NIS2 e AI Act, che impongono alle organizzazioni l'adozione di nuovi modelli di governance e compliance.

Il rapporto sottolinea inoltre l'importanza di un approccio integrato e multidisciplinare, in cui la collaborazione tra pubblico e privato, la condivisione di informazioni e la formazione continua rappresentano elementi chiave per rafforzare la resilienza dell'intero ecosistema digitale. L'analisi delle specificità settoriali dal finance, media, supply chain evidenzia come ogni comparto sia chiamato a misurarsi con rischi peculiari e a sviluppare strategie di difesa su misura.

In un contesto in cui l'Italia si conferma tra i Paesi maggiormente esposti alle minacce cyber, la capacità di anticipare i rischi, investire in tecnologie innovative e promuovere una cultura diffusa della sicurezza diventa un fattore determinante per la competitività e la stabilità del Sistema Paese. Il nostro Rapporto 2025 vuole essere uno strumento di analisi e un'occasione per suggerire spunti operativi per affrontare con consapevolezza e proattività le sfide di una realtà digitale in continua trasformazione.

Andrea Rivetti
Amministratore &
Equity Partner

Matteo Marco Marzan
Amministratore &
Equity Partner

INTRODUZIONE

Nel 2025 il panorama globale della cybersecurity continua a evolversi rapidamente e in modo drammatico, segnato da una "guerra cibernetica diffusa" in cui i confini tra criminalità informatica, operazioni di intelligence e attivismo digitale diventano sempre più sfumati. Le tensioni geopolitiche, la frammentazione normativa crescente e l'adozione accelerata di tecnologie emergenti — in particolare l'intelligenza artificiale generativa (GenAI) e i modelli linguistici di grandi dimensioni (LLM) — stanno ridefinendo le strategie di difesa e attacco a livello mondiale. L'IA si conferma un moltiplicatore di forza sia per i difensori sia per gli aggressori: da un lato automatizza la rilevazione delle minacce e rafforza le difese, dall'altro alimenta campagne di social engineering, disinformazione e ransomware sempre più sofisticate e su larga scala.

A questa complessità si aggiungono rischi crescenti associati alla diffusione del cloud, all'aumento degli attacchi infostealer, allo sfruttamento di dispositivi periferici e alla crescita di minacce ibride che intrecciano cybercrime e interessi statali. Il ransomware evolve verso modelli di estorsione basati sull'esfiltrazione dei dati, mentre le campagne di phishing e deepfake, potenziate dall'IA, intensificano la pressione su aziende e infrastrutture critiche. Il tutto si inserisce in un contesto caratterizzato da carenza di competenze specialistiche e da crescenti difficoltà nel mantenere la conformità a normative sempre più stringenti e disomogenee tra i diversi Paesi.

In questo scenario globale, l'Italia si conferma un bersaglio privilegiato e vulnerabile. Pur rappresentando una quota ridotta del PIL e della popolazione mondiale, il Paese ha subito nel 2024 circa il 10% degli attacchi globali, con un aumento degli incidenti cyber del 15% rispetto all'anno precedente — un dato inferiore all'incremento globale ma comunque allarmante e sproporzionato rispetto al peso economico nazionale. I settori più colpiti restano il manifatturiero, la sanità, i media e la logistica, con attacchi che spesso causano danni economici, interruzioni operative e violazioni della proprietà intellettuale. Il fenomeno dell'**hacktivism** e delle campagne **DDoS** a sfondo politico-sociale è in crescita, mentre il costo medio dei data breach continua a raggiungere livelli record.

L'evoluzione delle tecniche di attacco, la crescente esposizione delle infrastrutture critiche e la diffusione di vulnerabilità legate a sistemi legacy e supply chain pongono l'Italia di fronte a una sfida strutturale: rafforzare la resilienza nazionale, promuovere una cultura diffusa della sicurezza digitale e colmare il gap di competenze che ancora penalizza aziende e pubbliche amministrazioni. La risposta non può più limitarsi a soluzioni tecniche: è necessario un cambio di paradigma basato su una collaborazione attiva tra pubblico e privato, sull'adozione di tecnologie innovative e su una governance integrata e proattiva. Solo così sarà possibile trasformare la minaccia in opportunità, garantendo la protezione dei dati, la continuità operativa e la competitività del Paese nell'era digitale.

SCENARIO GLOBALE

Analisi degli incidenti cyber più rilevanti del 2024

La nostra analisi inizia con un esame degli incidenti informatici noti verificatisi nel 2024, sia a livello mondiale sia in Italia, confrontandoli con quelli registrati negli ultimi quattro anni.

Dal punto di vista **quantitativo, il trend è chiaramente in crescita: negli ultimi cinque anni, il numero medio mensile di attacchi è quasi raddoppiato, passando da 156 nel 2020 a 295 nel 2024. Solo nell'ultimo anno, gli incidenti noti e confermati sono aumentati del 27,4%, passando da 2.779 a 3.541.**

Oltre all'aumento numerico, si registra anche un peggioramento della gravità. L'indice medio di gravità ("Severity") degli attacchi è cresciuto ogni anno, con un'alta incidenza di episodi gravi o critici, che nel 2024 rappresentano circa l'80% del totale (rispetto al 50% del 2020). Tuttavia, si osserva una lieve **riduzione degli attacchi "critici"**, a fronte di un aumento di quelli classificati come "alti", dovuto in parte all'impatto medio minore degli attacchi a fini **cybercriminali**.

Va sottolineato che i **dati si riferiscono esclusivamente a incidenti andati a segno e resi pubblici: un indicatore parziale, ma comunque sufficiente a confermare il drastico peggioramento dello scenario globale di cyber-insicurezza rispetto al periodo 2011–2019.** A questo peggioramento non ha fatto seguito un adeguato aumento delle difese, della "cyberawareness" e degli investimenti nel settore. Già dal 2022, con l'inizio del conflitto in Ucraina, è emersa una nuova fase di "guerra cibernetica", che prosegue anche nel 2024. A questa si sommano fattori aggravanti come la crescente adozione dell'intelligenza artificiale generativa da parte degli attaccanti —

che ne amplifica la capacità d'azione — e l'inasprimento delle tensioni geopolitiche, che ha rilanciato l'attivismo digitale, in particolare tramite attacchi DDoS.

L'Italia: un bersaglio privilegiato

Anche nel 2024 l'Italia si conferma tra i Paesi più colpiti da attacchi informatici. I dati evidenziano un ulteriore aumento degli attacchi, pari al +15% rispetto al 2023, sebbene tale crescita risulti inferiore rispetto alla media globale, che registra un incremento del +27%.

Il **dato più preoccupante è la sproporzione tra il peso dell'Italia a livello globale — con lo 0,7% della popolazione mondiale e l'1,8% del PIL** — e la quota di attacchi subiti, che raggiunge il 10% del totale. Per confronto, Francia, Germania e Regno Unito oscillano tra il 3% e il 4%. Questa anomalia non può e non deve essere attribuita esclusivamente a un bias nei dati, ma richiede invece attenzione e interventi concreti.

I rischi informatici sono diventati una minaccia potenzialmente catastrofica. È dunque urgente adeguare le strategie di difesa su tutti i fronti: pubblica amministrazione, aziende private e infrastrutture critiche.

Evoluzione degli attacchi 2020-2024

Nel quinquennio 2020-2024 sono stati registrati 12.732 incidenti informatici gravi a livello globale. Solo nel 2024 ne sono avvenuti 3.541, il numero più alto mai rilevato. Il 56% di tutti gli incidenti censiti dal Clusit dal 2011 si è verificato negli ultimi cinque anni.

Rispetto al 2019, anno pre-pandemia e pre-IA, l'aumento degli attacchi è stato del 112%. La media mensile è salita da 139 a 295. Nel 2024 la distribuzione degli incidenti è risultata abbastanza omogenea nel corso dell'anno, con un picco tra ottobre e novembre.

Profilo degli attaccanti

Il cybercrime si conferma la causa principale degli incidenti informatici: nel 2024, l'86% degli attacchi è di matrice criminale, con un aumento del 3% rispetto al 2023. Si torna così ai livelli record del 2021. Questo dato dimostra come il crimine organizzato punti sempre più sul cyberspazio, favorito da modelli "as-a-Service" che rendono gli attacchi accessibili anche a chi non possiede competenze tecniche.

Distribuzione degli attaccanti nel 2024:

- Cybercrime: 86%
- Hacktivism: 8%
- Spionaggio/Sabotaggio: 4%
- Information Warfare: 2%

Il trend 2020-2024 evidenzia una crescita costante del cybercrime come motivazione prevalente, con un incremento del 31% solo nell'ultimo anno.

Analisi degli incidenti cyber più rilevanti a livello globale

In questa sezione presentiamo una panoramica degli incidenti di sicurezza informatica più significativi, verificatisi nel 2024 e resi pubblici, confrontandoli con quelli rilevati nei quattro anni precedenti

. L'analisi si basa su attacchi informatici noti, andati a segno e caratterizzati da un impatto rilevante — economico, tecnologico, legale o reputazionale — per le organizzazioni colpite.
L'aumento degli incidenti rilevati nel 2024 rispetto al 2023 è stato del +27%. Questo incremento **conferma una tendenza costante di crescita, sia in termini numerici sia per la gravità degli impatti.** L'analisi di questi eventi offre una visione concreta dell'evoluzione dello scenario globale delle minacce informatiche.
Nel periodo compreso tra gennaio 2020 e dicembre 2024, sono stati registrati complessivamente 12.732 incidenti, così distribuiti nel tempo:

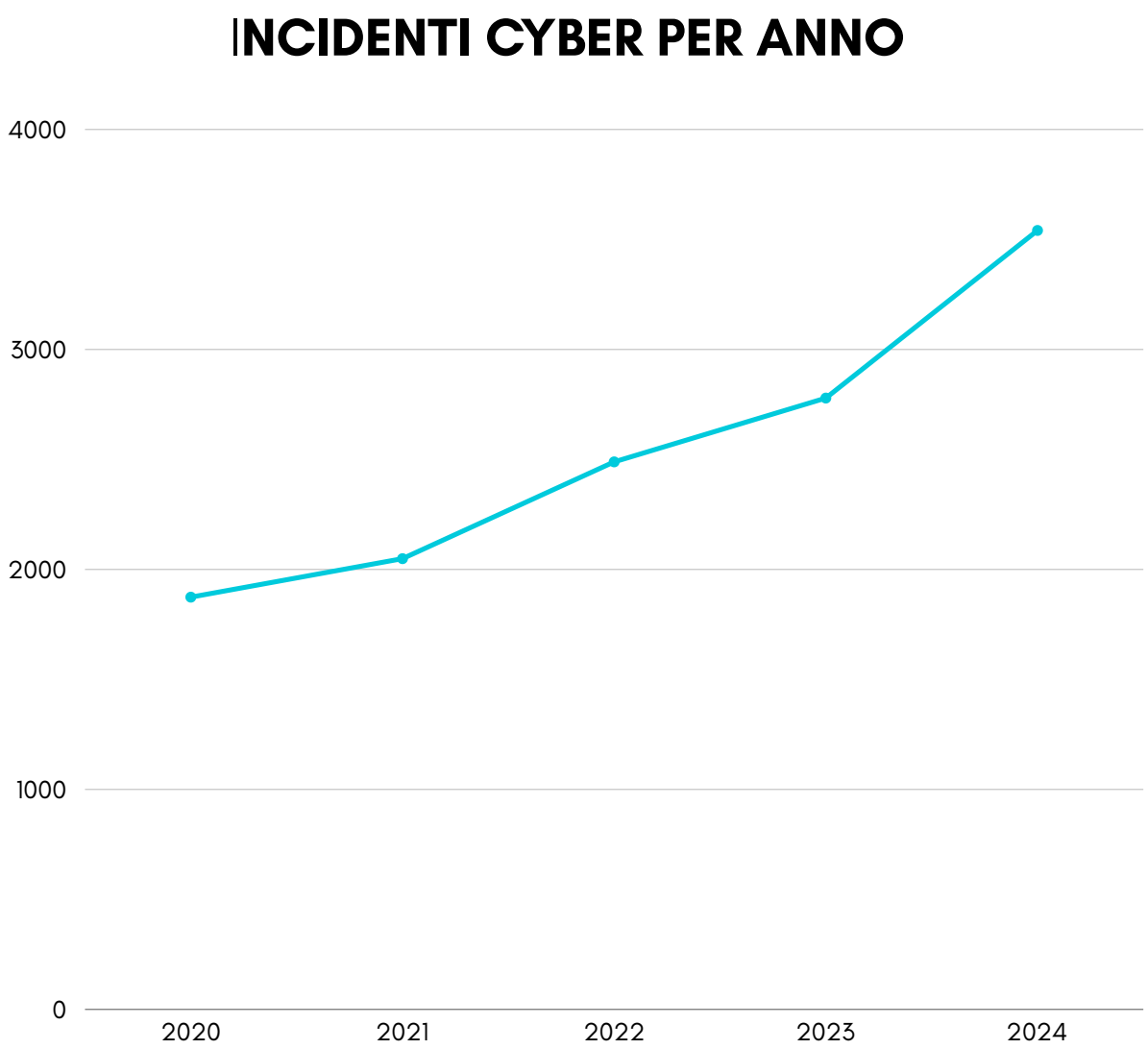


Fig.1-Andamento degli incidenti cyber nel periodo 2020-2024- Fonte: Rapporto Clusit 2025

Nel 2024 sono stati registrati **3.541 incidenti cyber, il numero più alto mai rilevato in un singolo anno. Questo dato non solo conferma la tendenza alla crescita, ma supera anche le previsioni tracciate negli anni precedenti.**
A dimostrazione della progressiva intensificazione dello scenario globale delle minacce informatiche, oltre il 56% di tutti gli incidenti classificati dal Clusit a partire dal 2011 si è verificato nel solo quinquennio 2020-2024 .
A dimostrazione della progressiva intensificazione dello scenario globale delle minacce informatiche, oltre il 56% di tutti gli incidenti classificati dal Clusit a partire dal 2011 si è verificato nel solo quinquennio 2020-2024.
Il confronto con gli anni passati evidenzia in modo netto l'accelerazione del fenomeno:

- +27% di incidenti rispetto al 2023 (da 2.779 a 3.541);
- +112% rispetto al 2019, ultimo anno prima della pandemia, dell'adozione massiva dello smart working e dell'introduzione pervasiva dell'intelligenza artificiale.

Anche la media mensile riflette questa crescita: dai 139 incidenti al mese nel 2019, si è passati a 232 nel 2023 fino a raggiungere 295 nel 2024.

A differenza di quanto osservato nel 2023, nel 2024 gli attacchi informatici si sono distribuiti in modo relativamente uniforme nel corso dell'anno, con un picco rilevante nei mesi di ottobre e novembre. Questo andamento suggerisce una continuità operativa sempre più professionale da parte degli attori delle minacce, caratterizzata da minori pause stagionali e da una pianificazione strategica più accurata.

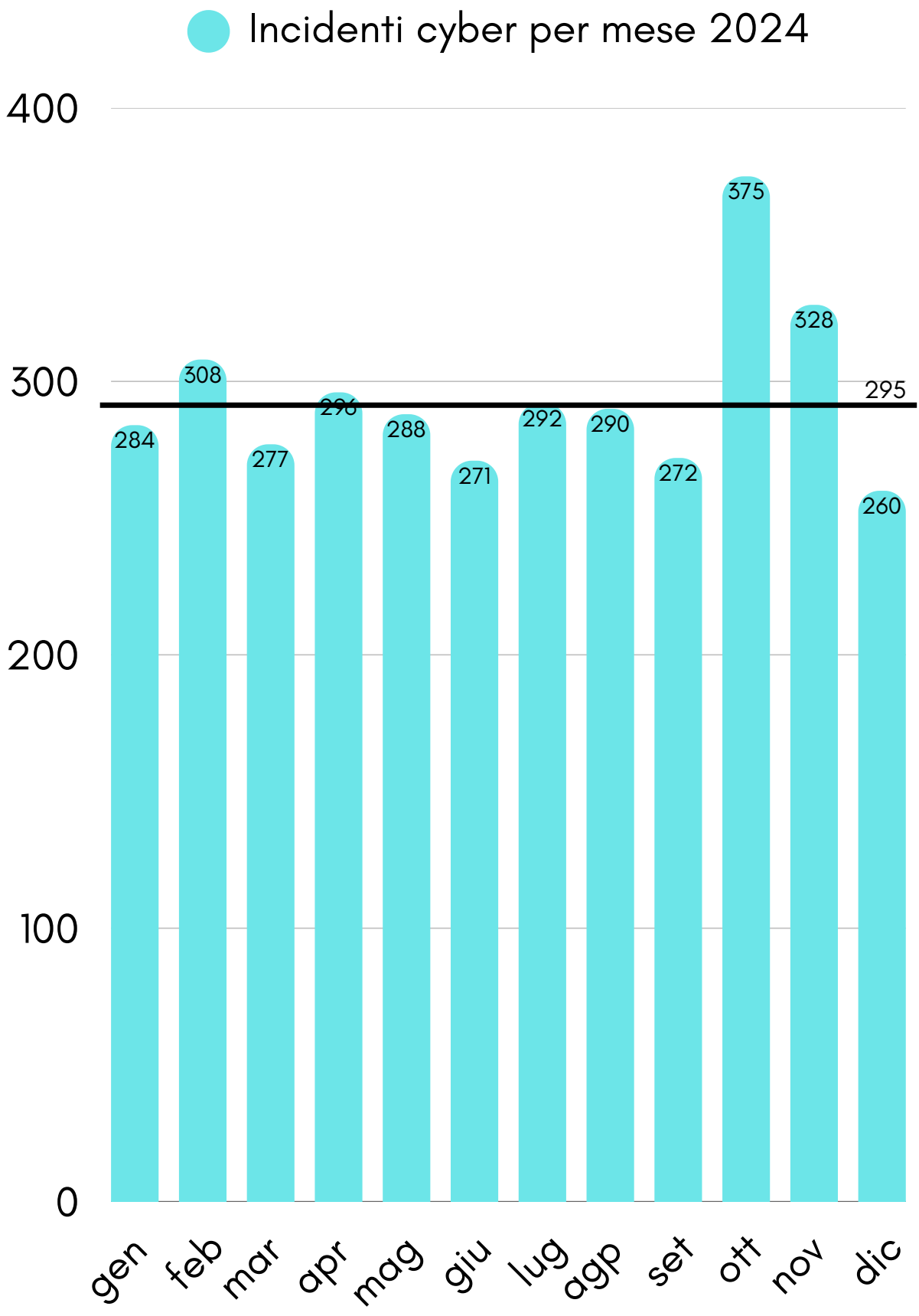


Fig.2 - Numero di incidenti cyber per mese nel mondo nel 2024- Fonte: Rapporto Clusit 2025

Analisi degli incidenti cyber più rilevanti a livello globale

Anche nel 2024 il **cybercrime** si conferma la principale motivazione alla base degli incidenti informatici noti a livello globale, rappresentando l'86% del totale — un aumento di tre punti percentuali rispetto al 2023, che riporta la situazione ai livelli record del 2021.

Quasi nove attacchi su dieci sono dunque attribuibili a gruppi o soggetti legati alla criminalità informatica, una tendenza in continua crescita. Questo dato evidenzia come il **cyberspazio** sia ormai diventato uno dei principali territori di espansione per la criminalità organizzata, attratta da margini elevati e rischi contenuti rispetto alle attività illegali tradizionali.
Un fattore determinante di questa espansione è rappresentato dai modelli **"as-a-Service"**, **che permettono di accedere a strumenti e servizi di attacco pronti all'uso, abbattendo la soglia tecnica di ingresso per nuovi attori criminali. In questo contesto, anche individui privi di competenze specifiche possono condurre operazioni malevole con facilità crescente.**

TIPOLOGIA E DISTRIBUZIONE ATTACCANTI 2024

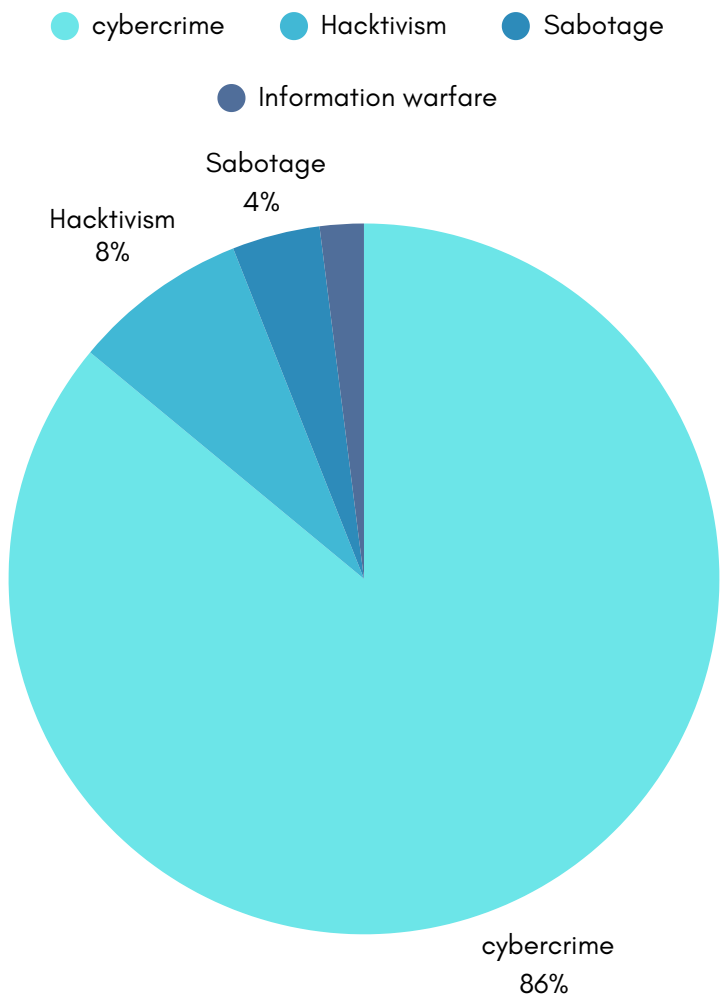


Fig. 3-Distribuzione percentuale degli attaccanti nel 2024- Fonte: Rapporto Clusit 2025

Il confronto della distribuzione degli attaccanti nel periodo 2020-2024 (vedi Fig. 4) conferma in modo inequivocabile che il **cybercrime rimane stabilmente la principale causa degli incidenti informatici.** La sua incidenza è cresciuta costantemente nel tempo, registrando un ulteriore incremento del +31% nel 2024 rispetto all'anno precedente. Questo andamento sottolinea non solo la persistenza del fenomeno, ma anche la sua capacità di evolversi rapidamente, consolidando il crimine informatico come minaccia dominante nello scenario globale della cybersecurity.

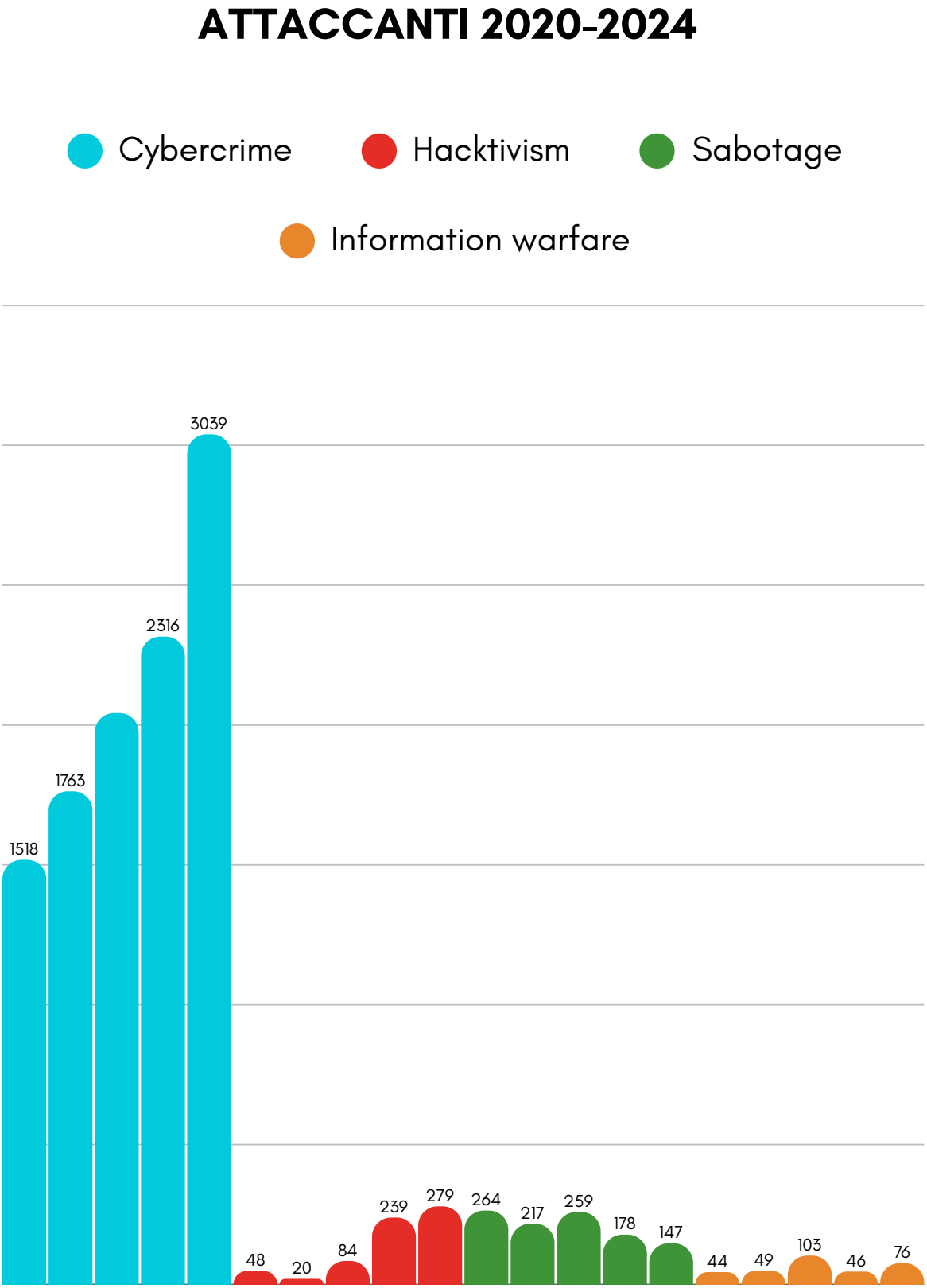


Fig. 4-Distribuzione degli attaccanti dal 2020 al 2024- Fonte: Rapporto Clusit 2025

Questa tendenza conferma quanto già evidenziato nel report dell'anno scorso: stiamo assistendo a una crescente integrazione tra criminalità tradizionale e cybercriminalità, con una vera e propria convergenza tra i mondi "offline" e "online". I profitti generati dalle attività illecite tradizionali vengono sempre più spesso reinvestiti nel cyberspazio, alimentando le risorse a disposizione degli attaccanti e massimizzando i ricavi.Parallelamente, l'incremento del cybercrime tende a oscurare altre minacce anch'esse in crescita, come l'hacktivism, che registra un aumento significativo (+16 punti percentuali rispetto all'anno precedente), e le operazioni di Information Warfare, che quasi raddoppiano nel periodo analizzato.
In controtendenza, invece, risultano le attività riconducibili a finalità di spionaggio e sabotaggio, in calo di circa 20 punti percentuali, suggerendo un momentaneo ridimensionamento di questo specifico tipo di minaccia nel panorama globale della cybersecurity.

Distribuzione delle vittime per categoria

L'analisi delle vittime degli incidenti cyber nel 2024 (Fig. 5) rivela che quasi la metà degli attacchi (44%) si concentra nelle prime tre categorie della nostra classificazione: **Multiple Targets** (18% del totale), **Gov / Mil / LE** (governo, forze militari e forze dell'ordine) (13%) e **Healthcare** (13%).
Mentre gli attacchi indiscriminati, tipici delle campagne di "pesca a strascico", continuano a essere una delle modalità preferite dai cybercriminali — grazie al loro alto tasso di successo, dovuto alla maggiore intensità di queste operazioni —, gli altri due settori rappresentano obiettivi particolarmente strategici, sia per il loro ruolo fondamentale sia per la rilevanza dei dati che gestiscono.

DISTRIBUZIONE DELLE VITTIME 2024

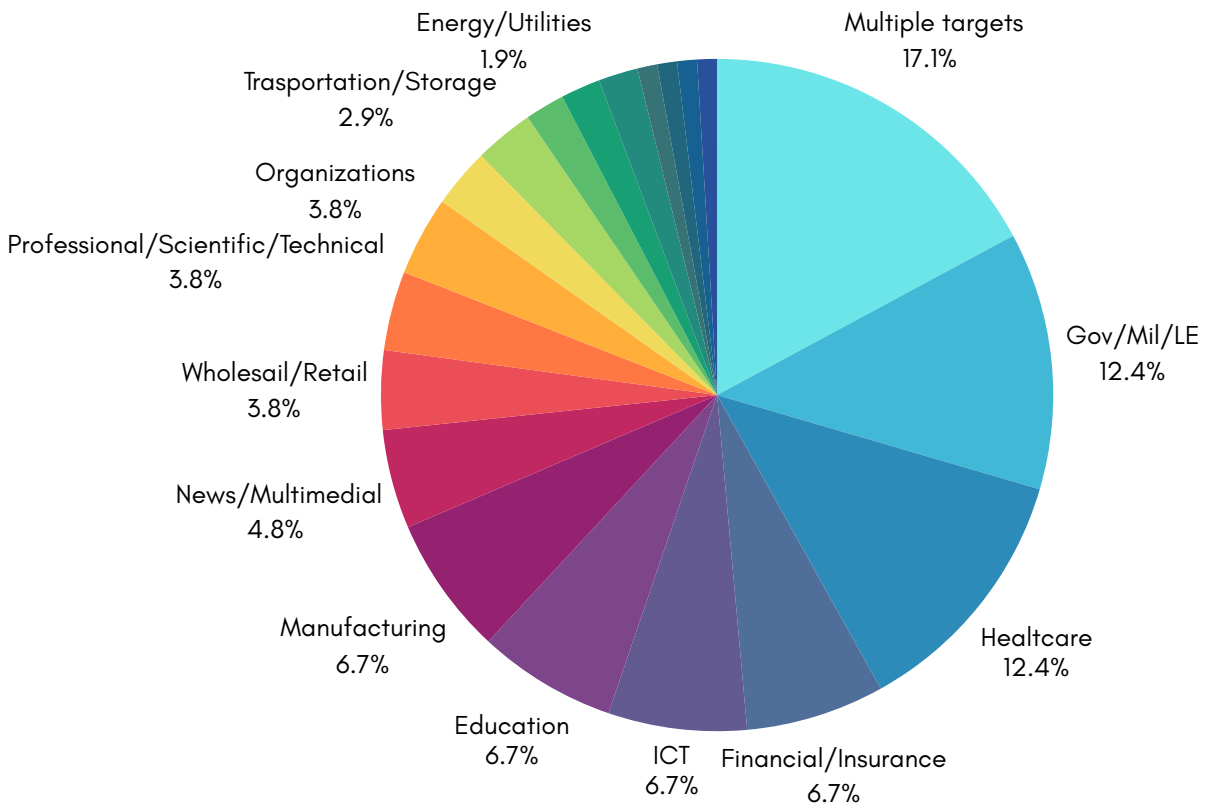


Fig. 5-Distribuzione della tipologia di vittime nel 2024 Fonte: Rapporto Clusit 2025

settore Healthcare segna un incremento del 18,9%. Infine, il segmento Multiple Target cresce di oltre 17 punti percentuali.

TOP 10 VITTIME 2020 - 2024

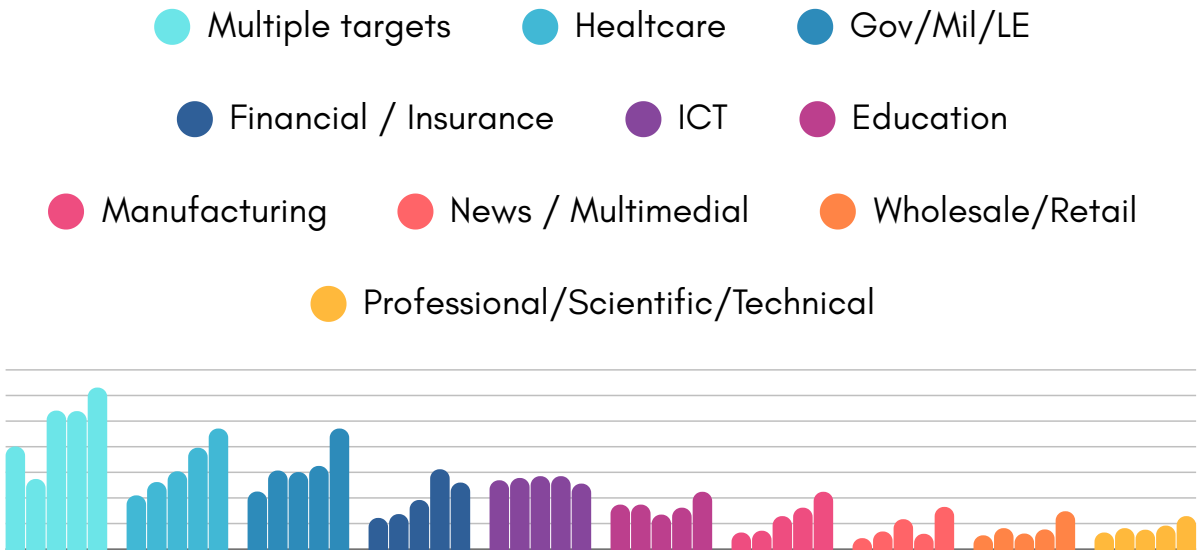


Fig.6-Distribuzione delle prime 10 tipologie di vittime dal 2020 al 2024 Fonte: Rapporto Clusit 2025

Dopo un tasso di crescita costante dal 2019 al 2023, il settore Financial/Insurance registra invece una diminuzione del 16% rispetto all'anno precedente. Tale calo può essere attribuito a due fattori principali: da un lato, l'introduzione di regolamentazioni più stringenti sulla resilienza operativa digitale nel settore, come il Regolamento **DORA** in Europa; dall'altro, una crescente attenzione della criminalità informatica nel perseguire economie di scala attraverso campagne di attacchi trasversali che colpiscono più settori o vittime con minori capacità difensive.

Anche il settore ICT, insieme al Financial/Insurance, è tra i pochi in cui si registra una riduzione degli incidenti (-10%) dopo una fase di stabilità nei due anni precedenti. Questa diminuzione sembra essere il risultato concreto di un progressivo rafforzamento delle capacità difensive del settore, con miglioramenti graduali e facilmente osservabili.

Un altro dato significativo è rappresentato dalla crescita degli incidenti nel settore Healthcare, che ha visto un aumento del 18,9%. Inoltre, il comparto **Gov / Mil / LE** ha registrato un incremento del 45%, mentre il settore **Wholesale / Retail** ha fatto segnare un impressionante +92%.

Focalizzando l'attenzione sulla "top 10" delle vittime, si osserva che molti settori hanno registrato aumenti superiori al 40%: **Education** (+43%), **Manufacturing** (+38%) e **Professional / Scientific / Technical** (+40%). In particolare, il settore News / Multimedia ha fatto registrare una crescita straordinaria del 175%, rientrando nella parte alta della classifica dopo un anno di assenza.

Infine, il settore **Transportation / Storage**, che nel 2023 figurava tra i primi dieci più colpiti, ha registrato un calo nel 2024, scendendo al dodicesimo posto.

Distribuzione delle tecniche di attacco

Nel 2024, i cybercriminali continuano a fare affidamento su tecniche consolidate e facilmente industrializzabili. I Malware sono responsabili di oltre un terzo degli incidenti, mentre lo sfruttamento delle vulnerabilità, sia note sia sconosciute (zero-day), rappresenta il 15% del totale degli attacchi (Fig. 7). Nonostante un leggero calo percentuale rispetto al 2023 (-4 punti percentuali), i ransomware e i codici malevoli continuano a crescere in termini assoluti, con un aumento dell'11% (+114 incidenti), dimostrando la loro efficacia nelle strategie della criminalità informatica (Fig. 8).

Inoltre, si osserva un incremento significativo degli attacchi DDoS (+36%), che ora costituiscono l'8% del totale. Phishing e Social Engineering registrano una crescita del 33%, arrivando anch'essi all'8% del totale, mentre il Theft of Identity e Account Cracking sono aumentati drasticamente (+135%) e rappresentano il 6% degli incidenti. Questi dati evidenziano una crescente diversificazione nelle tecniche di attacco, che combinano metodi tradizionali e più sofisticati, ottenendo maggiore efficacia nel trasformarsi in incidenti di successo.

Inoltre, per un quarto degli incidenti, la tecnica utilizzata non è stata divulgata (undisclosed). Dopo una fase di calo, questi casi sono aumentati del 56% nell'ultimo anno.

DISTRIBUZIONE DELLE TECNICHE DI ATTACCO 2024

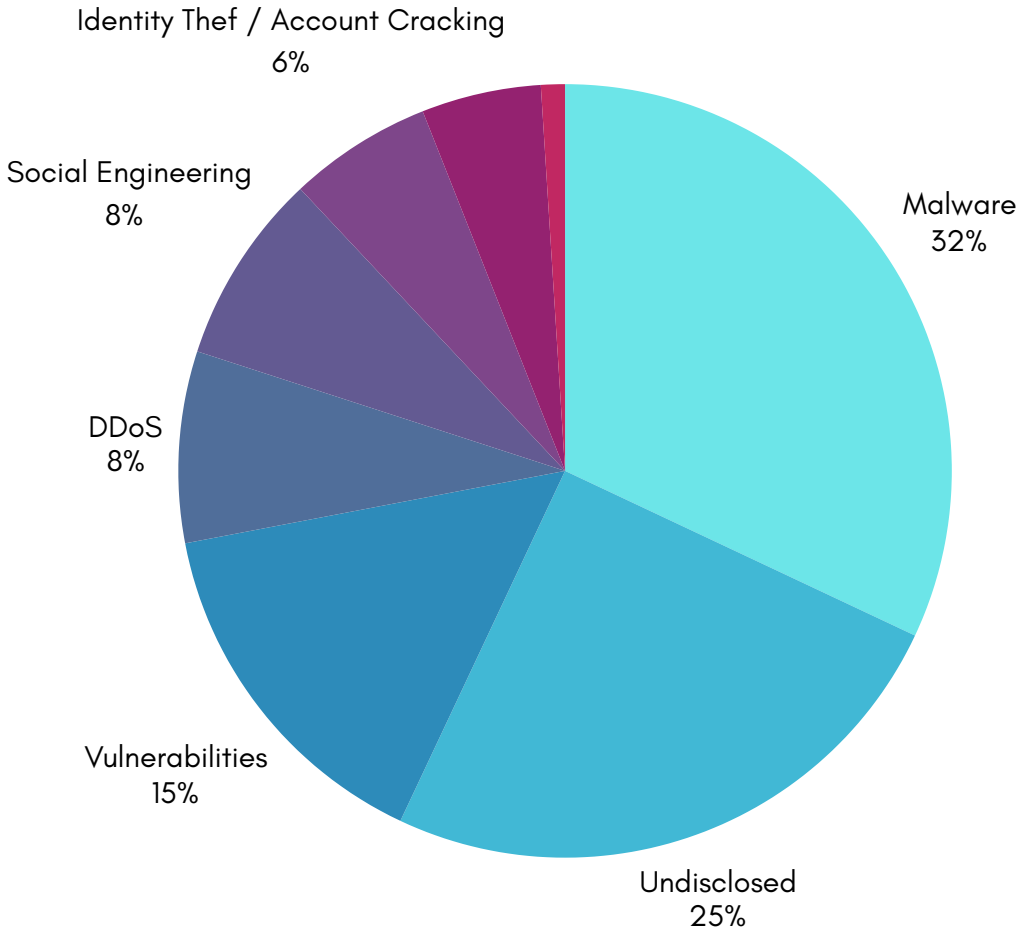
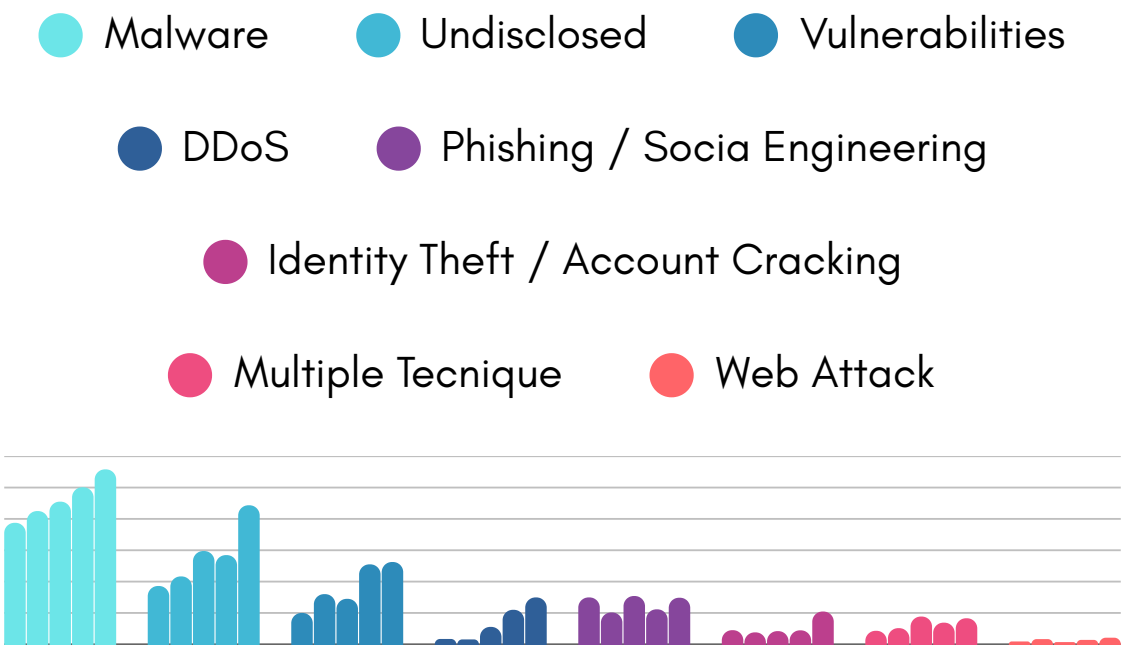


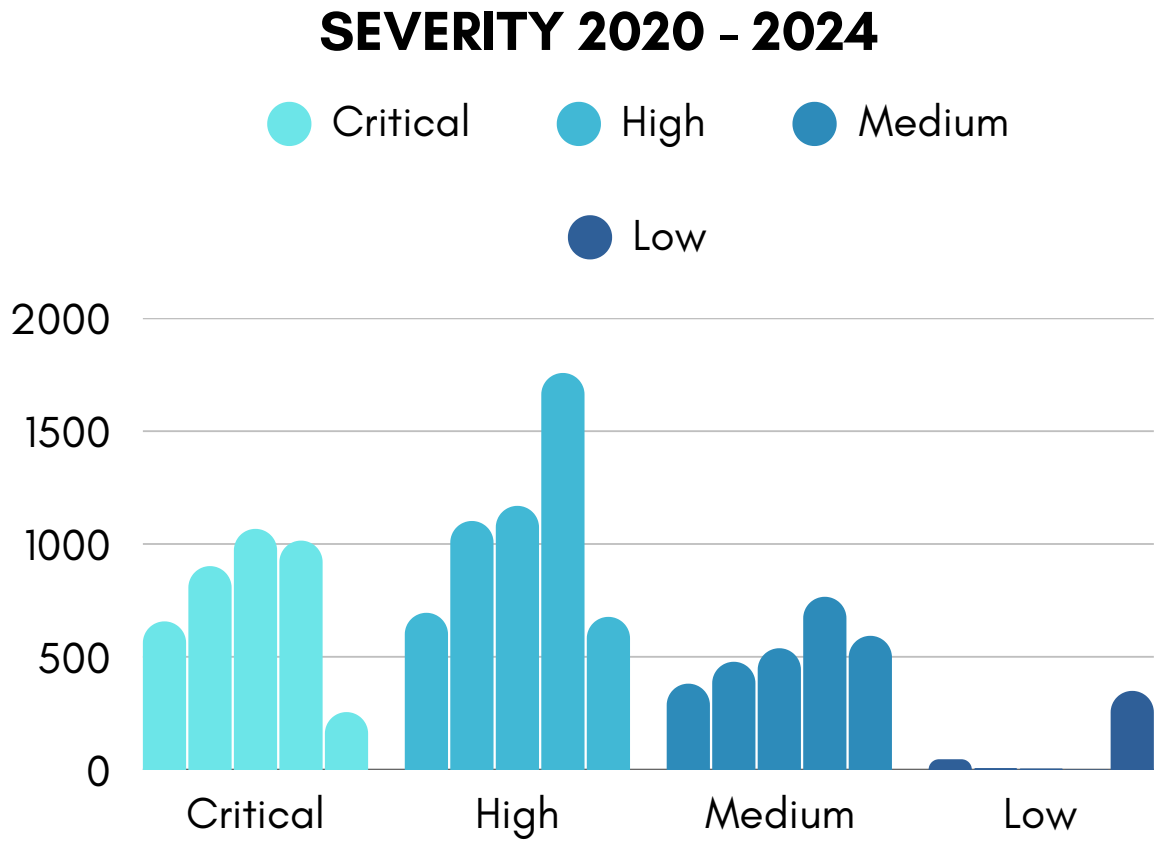
Fig.7 -Distribuzione delle tecniche di attacco nel 2024[MC1] Fonte: Rapporto Clusit 2025

TECNICHE DI ATTACCO 2020 - 2025



FFig. 8- Distribuzione delle tecniche di attacco nel periodo 2020-24 Fonte: Rapporto Clusit 2025

L'analisi della gravità (severity) degli incidenti si propone di mettere in evidenza gli impatti effettivi degli attacchi, che non sempre sono proporzionali al numero di incidenti né possono essere dedotti esclusivamente dal tipo di vittima o dalla tecnica utilizzata. Dal 2021 (Fig. 911) si è consolidata una tendenza preoccupante, con un costante aumento degli incidenti classificati come gravi o gravissimi. Nel 2023, questa tipologia ha rappresentato circa l'80% del totale, un dato che riflette anche la specificità del campione su cui si basa il nostro rapporto.
Anche nel 2024 questo trend viene confermato (Fig. 10), con un livello di gravità significativo (impatti Critical e High) che si attesta nuovamente al 79%. Aumentano inoltre gli incidenti con gravità media (+42%), mentre gli impatti bassi sono ormai sostanzialmente scomparsi dal campione mondiale.



Fg. 9-Andamento della Severity degli incidenti nel periodo 2020-24 Fonte: Rapporto Clusit 2025

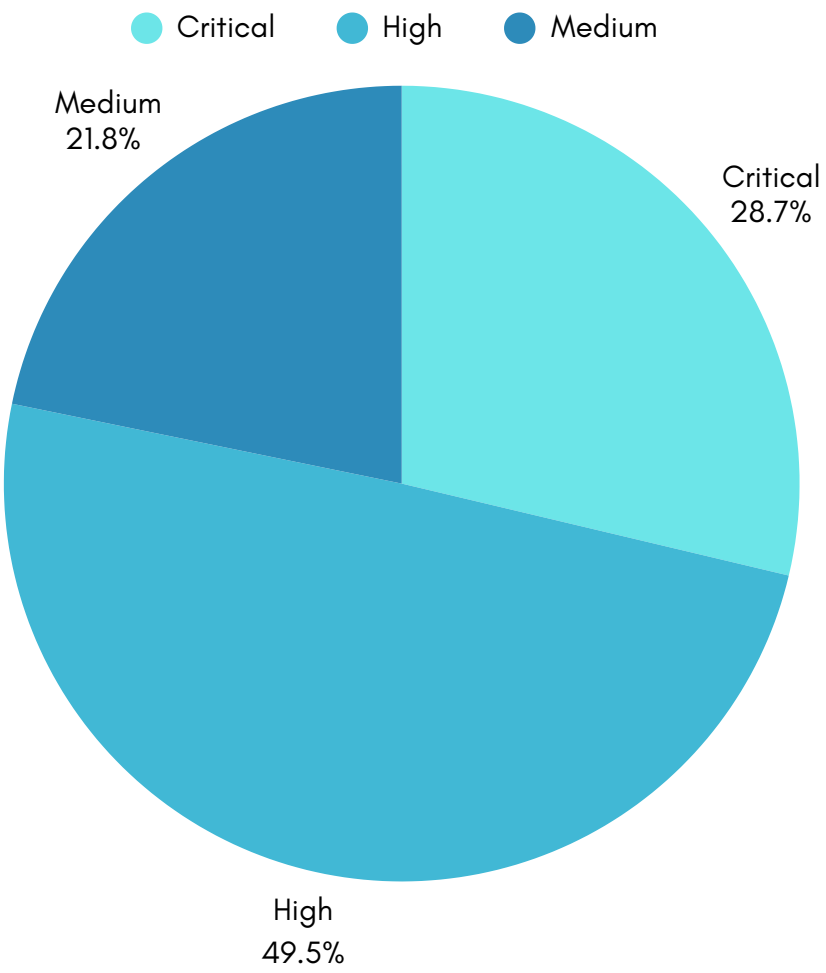


Fig. 10- Distribuzione della Severity nel 2024 Fonte: Rapporto Clusit 2025

SITUAZIONE IN ITALIA

Distribuzione delle tecniche di attacco

Tra il 2020 e il 2024, il campione ha rilevato **973 incidenti gravi** che hanno colpito organizzazioni italiane. Di questi, ben 357 – pari a quasi il 39% del totale – si sono verificati nell'ultimo anno analizzato. Come mostra il grafico (Fig. 11), il dato del 2024, pur segnando una lieve crescita rispetto al 2023, sembra rientrare nella tendenza osservata negli ultimi anni: gli incidenti sono aumentati, ma con un'intensità minore rispetto ai due anni precedenti. Nel 2024, **il tasso di crescita degli incidenti in Italia si attesta al 15,2%** rispetto all'anno precedente (Fig. 12), un **valore inferiore rispetto alla media globale, che è del 27,4%**. Si inverte quindi la tendenza registrata l'anno scorso, quando l'incremento degli attacchi in Italia (65%) era stato più marcato rispetto a quello a livello internazionale (11,7%). Infine, rispetto al quadro globale, si osserva un **lieve calo dell'incidenza degli attacchi subiti da organizzazioni italiane sul totale mondiale** (Fig. 13): nel 2024, questi rappresentano il 10,1% degli incidenti rilevati a livello globale, mantenendosi comunque vicino al picco negativo dell'anno precedente (11,2%).

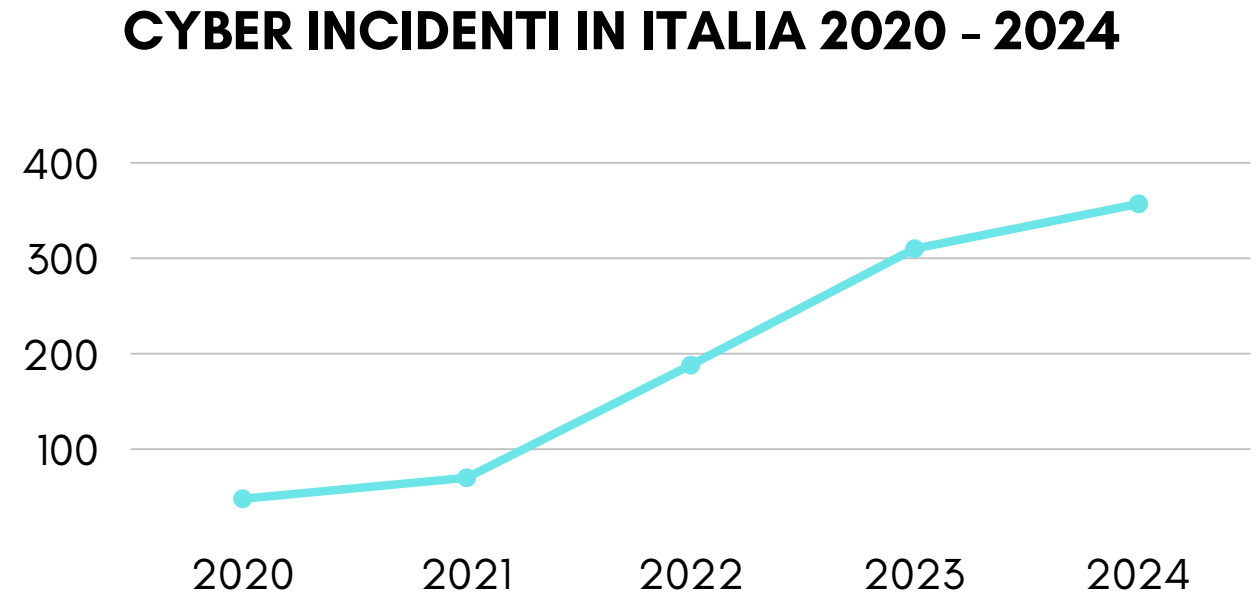


Fig. 11- Distribuzione degli incidenti cyber in Italia nel periodo 2020-2024 Fonte : Rapporto Clusit 2025

CONFRONTO ITALIA VS GLOBAL 2020 - 2024

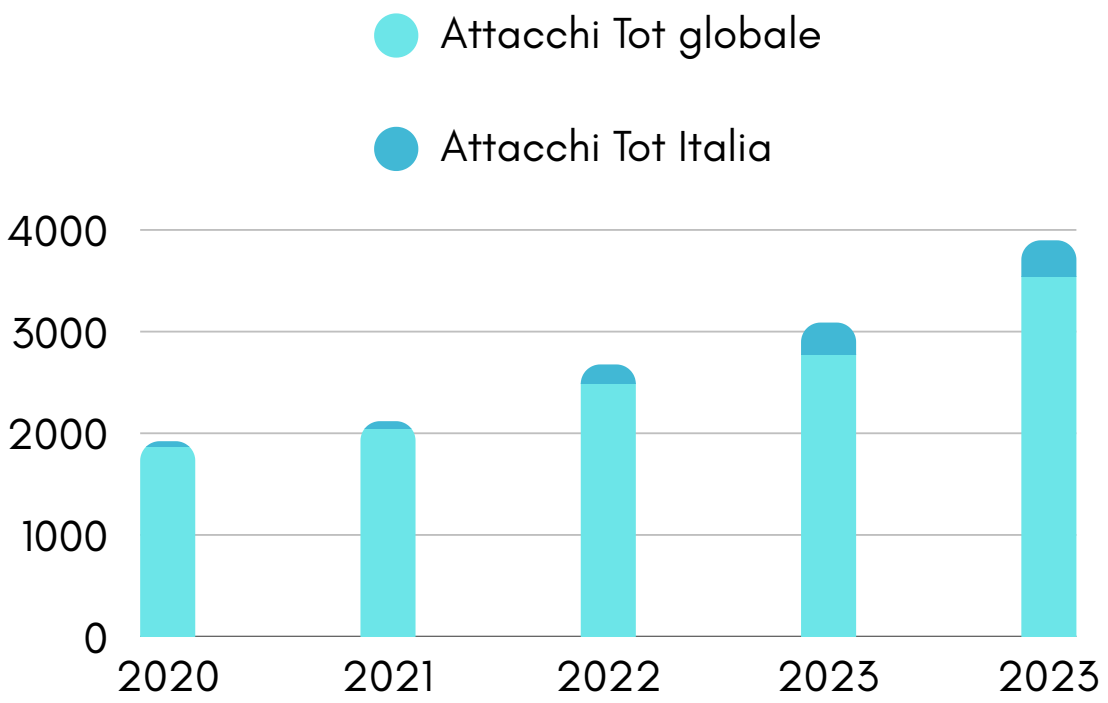


Fig. 12-Confronto crescita percentuale in Italia vs. Global nel periodo 2020-2024 Fonte: Rapporto Clusit 2025

CONFRONTO CRESCITA % ITALIA VS GLOBAL 2020 - 2024

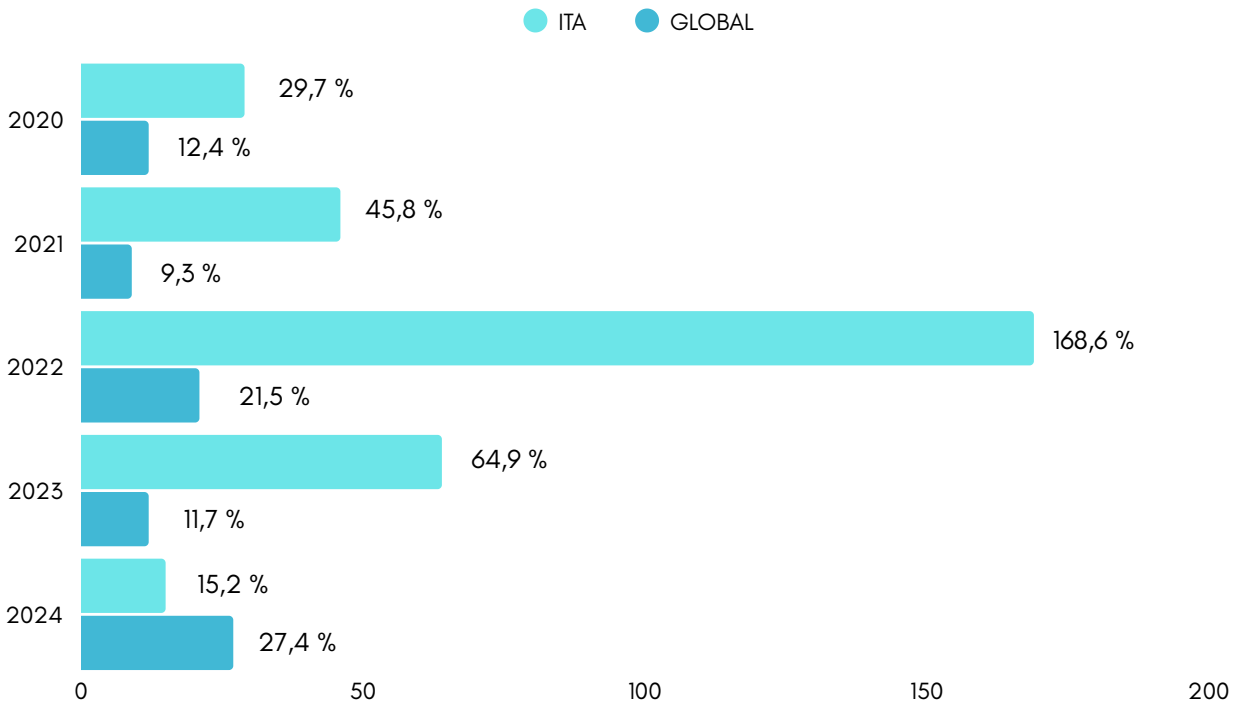


Fig. 13- Incidenza degli incidenti in Italia rispetto al campione globale - 2020-2024 Fonte: Rapporto Clusit 2025

Distribuzione degli attaccanti per tipologia

L'analisi degli incidenti in base alla tipologia degli attaccanti conferma le tendenze già osservate negli ultimi anni. In Italia, gli attacchi informatici sono riconducibili principalmente a due categorie: **cybercriminali** e **hacktivisti**. Al contrario, risultano marginali gli episodi attribuibili a operazioni di spionaggio, sabotaggio o guerra dell'informazione (Fig. 14).

Nel 2024, l'80% degli incidenti registrati in Italia è riconducibile al cybercrime. In particolare, questa categoria rappresenta il **78% del totale**, in netta crescita rispetto al 64% del 2023. Tale incremento riavvicina la distribuzione italiana a quella del contesto globale, dove gli attacchi di matrice criminale costituiscono l'86% del totale.

CONFRONTO ITALIA VS GLOBAL 2020 - 2024

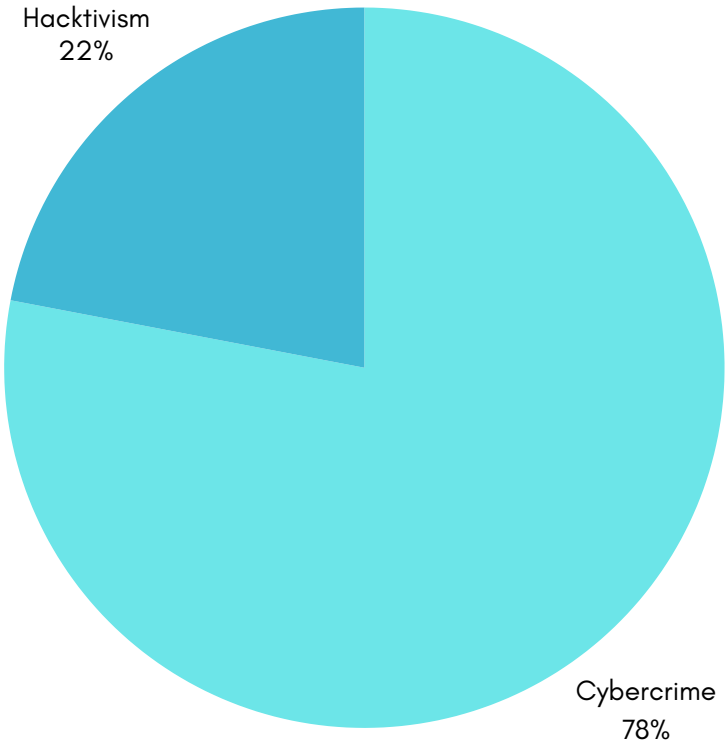


Fig. 14- Attaccanti in Italia nel 2024 Fonte: Rapporto Clusit 2025

Gli incidenti attribuiti ad azioni di hacktivism rappresentano il restante 22% del totale. Come osservato anche a livello globale, l'attribuzione di questo tipo di attacchi rimane un aspetto critico: nel 2024, gli episodi legati all'attivismo digitale sono in gran parte connessi a dinamiche geopolitiche e ai conflitti in corso nel periodo.

In particolare, **il protrarsi della guerra in Ucraina ha determinato un lieve rallentamento delle attività hacktiviste**, con una conseguente riduzione degli incidenti del 28% rispetto al 2023 (Fig. 15). Nonostante questo calo, l'incidenza degli attacchi di matrice hacktivista contro bersagli italiani resta significativa: su 279 incidenti globali, ben 80 – circa il 29% – hanno coinvolto organizzazioni italiane.

In termini assoluti, **colpisce il dato relativo al cybercrime, che non solo si conferma la tipologia di attacco più diffusa, ma registra una forte crescita**: nel 2024 si contano 277 episodi, contro i 197 dell'anno precedente, con un incremento pari al 40,6%.

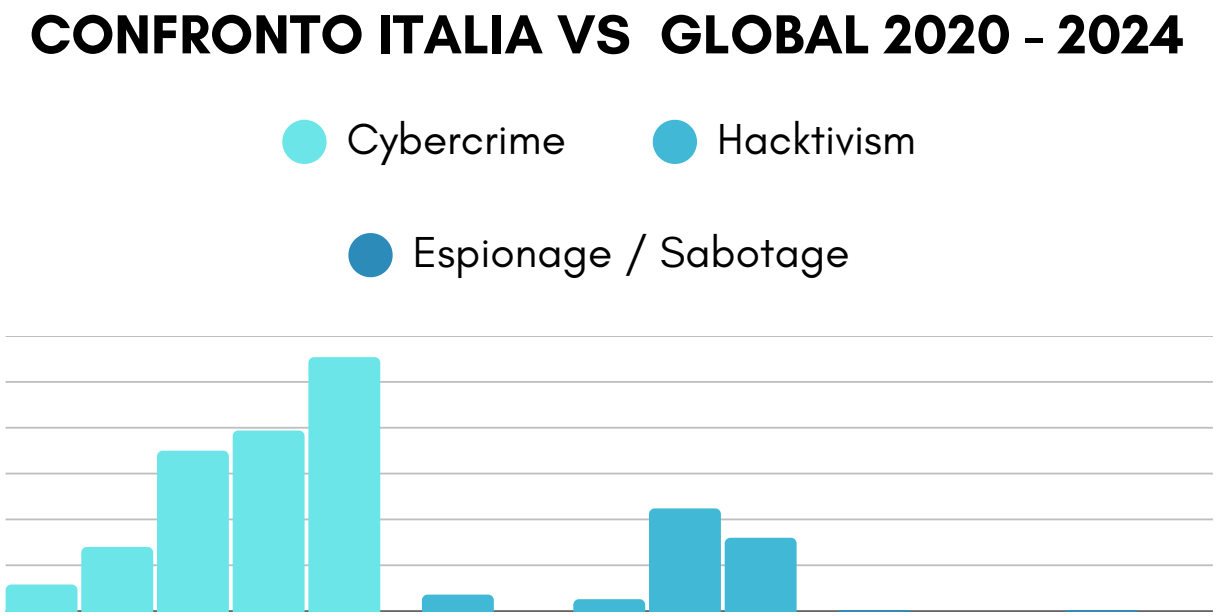


Fig. 15- Attaccanti in Italia nel periodo 2020-2024 Fonte: Rapporto Clusit 2025

Il marcato aumento degli attacchi di cybercrime evidenzia una tendenza ormai consolidata: **l'accesso agli strumenti necessari per condurre attività criminali online è diventato sempre più semplice**, anche per soggetti con competenze tecniche limitate. Come risulta anche dall'analisi dei dati globali, la diffusione del modello "as-a-Service" – che si sviluppa nel dark web attraverso vere e proprie piattaforme di e-commerce – ha reso l'infrastruttura del cybercrimine ampiamente accessibile. Questo fenomeno ha favorito il coinvolgimento di organizzazioni criminali tradizionali, contribuendo così a un aumento significativo degli attacchi su larga scala.

Distribuzione delle vittime per tipologia

Uno degli aspetti di rilievo di questo rapporto è la capacità di cogliere i cambiamenti significativi che, anno dopo anno, possono offrire indicazioni strategiche alle organizzazioni pubbliche e private nel ridefinire la propria postura di sicurezza.
Tra questi, spicca la distribuzione settoriale delle vittime italiane, che nel 2024 presenta una novità potenzialmente eccezionale più che indicativa di una tendenza consolidata (Fig. 16): il settore più colpito risulta essere quello **News / Multimedia, con il 18% degli incidenti totali**. Per ulteriori approfondimenti si rimanda alla sezione dedicata, "Il caso News / Multimedia".
I settori tradizionalmente più colpiti seguono a breve distanza: **il manufacturing si colloca al secondo posto con il 16%, mentre il comparto government** – che nel 2023 guidava la classifica – **scende al terzo con il 10%**.
Da segnalare anche la posizione dei cosiddetti multiple target, ovvero gli attacchi che colpiscono simultaneamente più soggetti, che quest'anno rappresentano meno di un quinto del totale, collocandosi a pari merito con il manufacturing.

Seguono i settori **transportation / storage (7%), professional / scientific / technical (6%) e organizations (5%)**.

CONFRONTO ITALIA VS GLOBAL 2020 - 2024

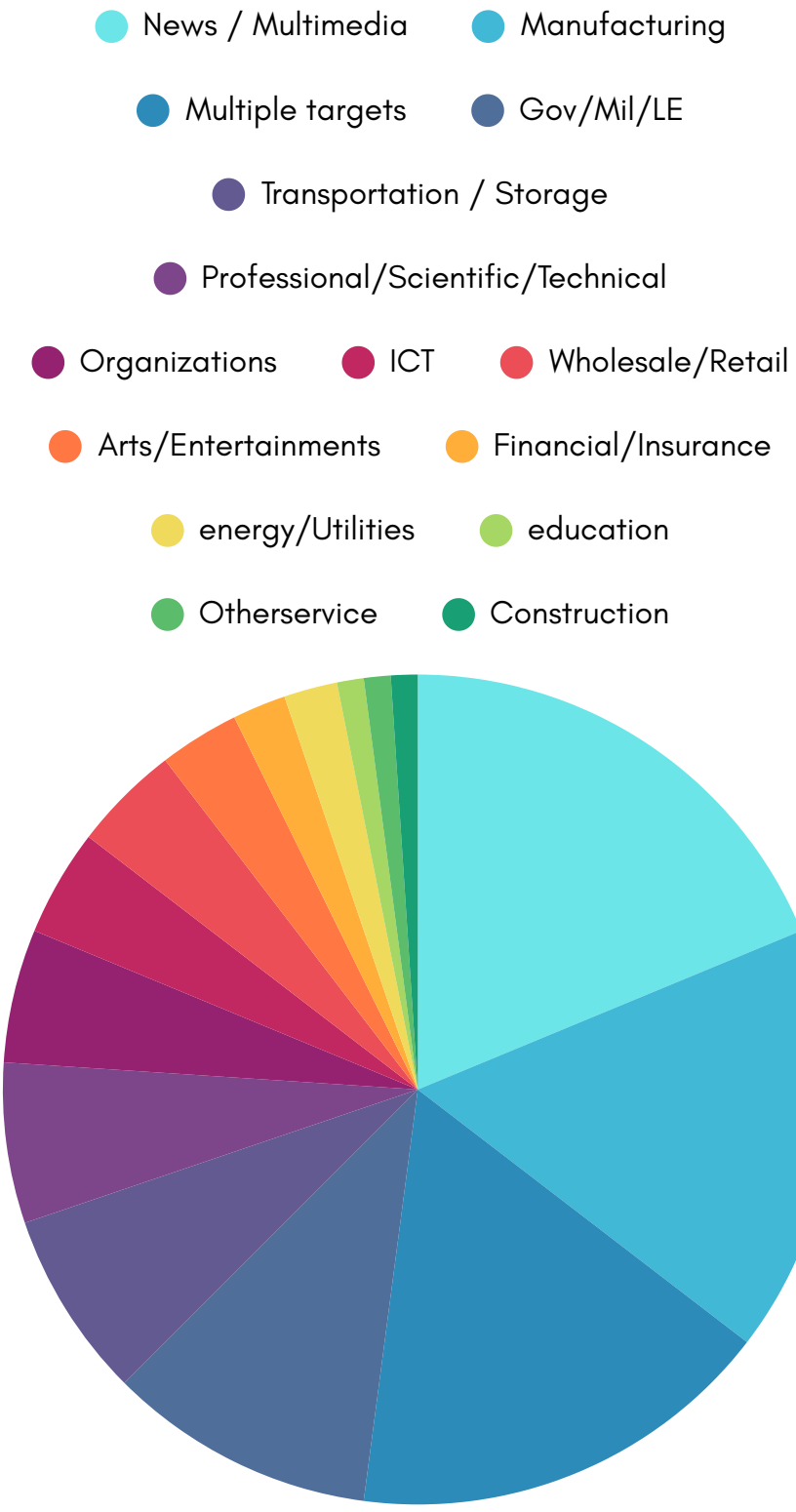


Fig. 16- Distribuzione delle vittime in Italia nel 2024 Fonte: Rapporto Clusit 2025

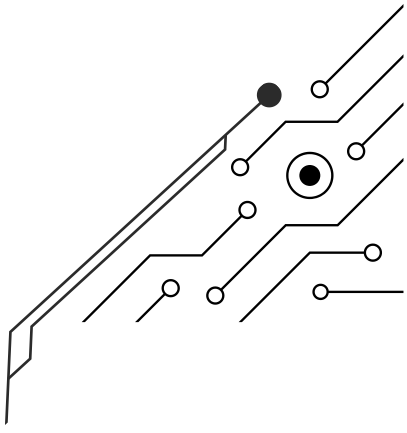
Il settore manifatturiero continua, purtroppo, **a confermarsi come uno dei più esposti agli attacchi informatici in Italia**. Anche nel 2024, un quarto degli incidenti globali che colpiscono il comparto manufacturing riguarda realtà italiane, a fronte di un'incidenza mondiale che si ferma al 6%.

Allo stesso modo, il settore transportation / storage risulta particolarmente vulnerabile: gli incidenti registrati in Italia rappresentano ben il 26% del totale globale per questa categoria.

Analizzando l'andamento complessivo, si osserva un **incremento del numero di incidenti rispetto all'anno precedente in quasi tutte le aree merceologiche considerate**. Questo scenario evidenzia con chiarezza le **difficoltà che molte organizzazioni incontrano nel proteggersi efficacemente dagli attacchi**.

Le difese messe in campo si dimostrano spesso inadeguate e la presenza di vulnerabilità sistemiche rende determinati settori bersagli privilegiati. Si tratta di una tendenza preoccupante, che rischia di accentuarsi nei prossimi anni. Da un lato, le misure di sicurezza non evolvono con sufficiente rapidità; dall'altro, gli attacchi diventano sempre più sofisticati e accessibili, grazie anche all'impiego dell'intelligenza artificiale e alla diffusione dei modelli di minaccia "**as-a-Service**".

In assenza di un deciso rafforzamento delle contromisure, il divario tra attaccanti e vittime è destinato ad ampliarsi ulteriormente, rendendo sempre più difficile contenere il rischio in modo efficace.



Distribuzione delle tecniche di attacco

L'analisi delle tecniche di attacco consente di comprendere meglio le cause alla base dell'elevato numero di incidenti che, nel 2024, hanno colpito imprese e istituzioni italiane.

Il malware torna a essere la tecnica più utilizzata, responsabile del 38% degli attacchi (Fig. 17), con un incremento che lo riporta al primo posto, superando il **DDoS**, che **scende al 21% dopo aver dominato nel 2023 con il 36% degli incidenti.**

Una novità di rilievo riguarda la terza posizione, occupata dagli **attacchi basati su vulnerabilità**, che raggiungono una quota storica per l'Italia pari al **19%**. Questo aumento è in parte attribuibile all'ondata di attacchi contro il settore News / Multimedia, già trattata nei paragrafi precedenti.

Il phishing e il social engineering si attestano all'11%, confermando il ruolo centrale del fattore umano come punto debole nei sistemi di sicurezza: tecniche semplici ma ancora estremamente efficaci per aggirare le difese.

Le tecniche non classificate (undisclosed) scendono al 7%, segnando un calo significativo rispetto agli anni precedenti. Questo trend positivo riflette probabilmente una maggiore trasparenza da parte delle vittime nella condivisione delle informazioni sugli attacchi, così come una crescente tendenza degli attaccanti a rivendicare pubblicamente le proprie azioni, fornendo dettagli tecnici.

Nel grafico (Fig. 17) emergono anche due ulteriori evidenze: da un lato, la comparsa della categoria multiple techniques (2%), indicativa di attacchi particolarmente complessi; dall'altro, la stabilità degli attacchi web, anch'essi al 2%.

TECNICHE DI ATTACCO IN ITALIA 2024

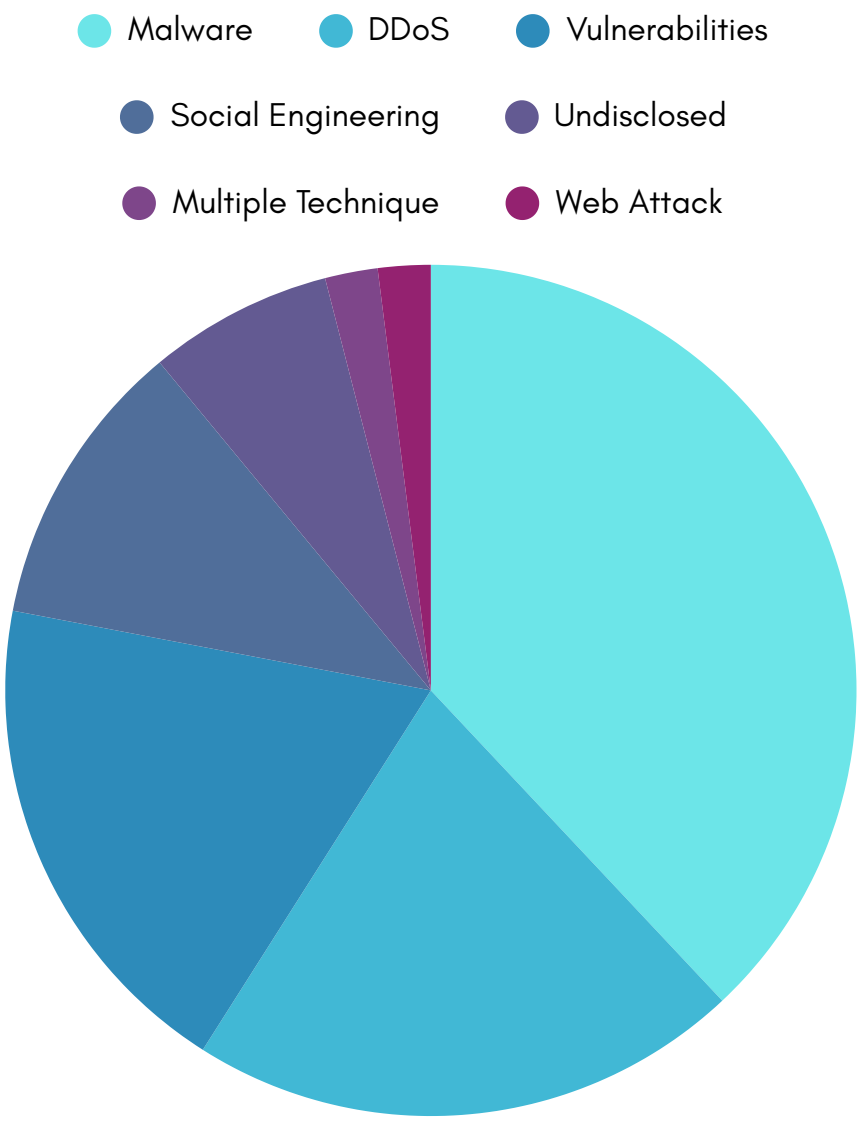


Fig.17- Tecniche di attacco in Italia nel 2024 Fonte: Rapporto Clusit 2025

L'analisi storica delle tecniche di attacco (Fig. 18) mostra una **crescita generalizzata** per quasi tutte le tipologie, ad **eccezione** delle **undisclosed** e dei **DDoS**. Questi ultimi registrano una **flessione netta**, con un **calo** del **36%** in termini assoluti (76 incidenti nel 2024 contro i 111 del 2023), segnando **un'inversione rispetto** alla **crescita** costante degli anni precedenti. È **interessante** notare che questa **dinamica** è in **controtendenza** rispetto al **panorama globale**, dove gli attacchi **DDoS** risultano invece in **aumento**.

TECNICHE DI ATTACCO IN ITALIA 2020-2024

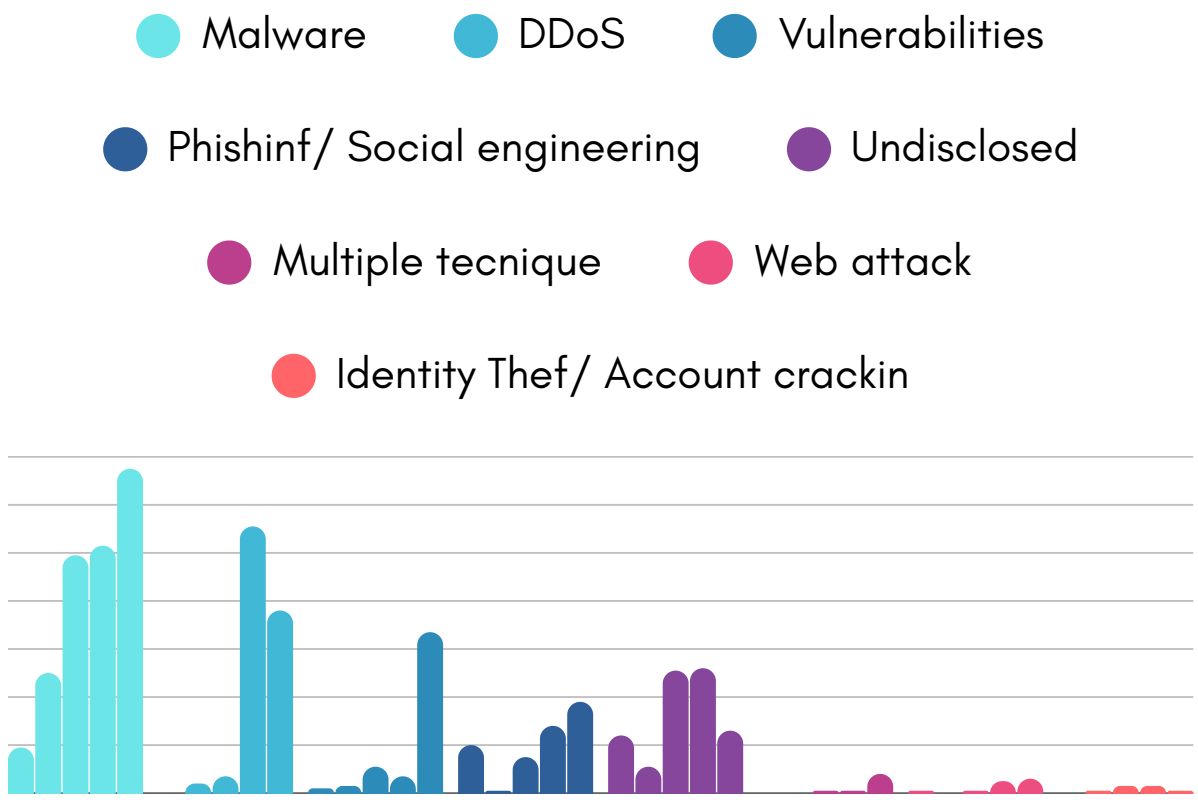


Fig 18- Tecniche di attacco in Italia nel periodo 2020-2024 2024 Fonte: Rapporto Clusit 2025

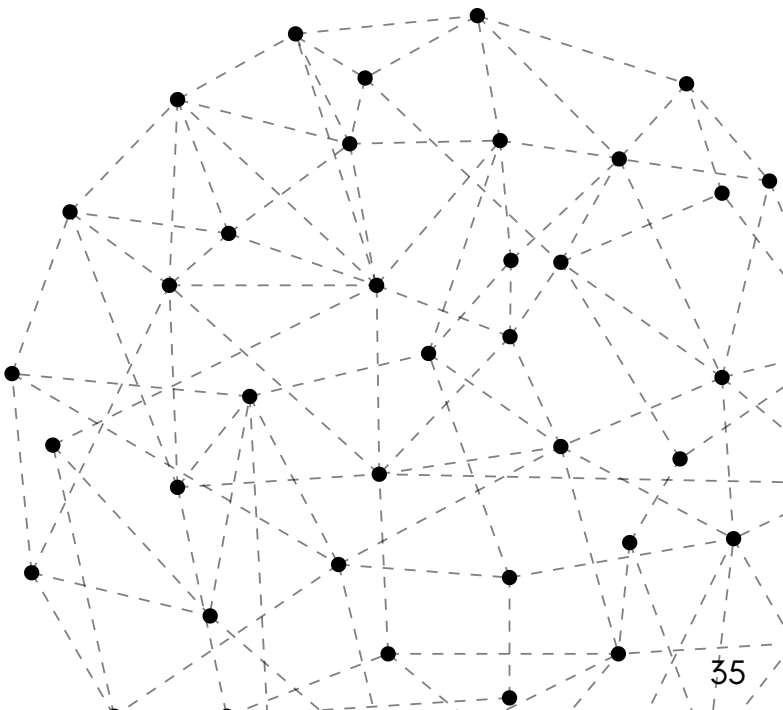
Questo andamento può essere interpretato in due modi: da un lato, è possibile che **l'interesse** degli **hacktivisti** si sia spostato verso **paesi maggiormente coinvolti** nei conflitti **attualmente** in **corso**; dall'altro, si potrebbe ipotizzare che gli **attacchi non generino** più in **Italia**, come in passato, un **numero** rilevante di **incidenti** significativi grazie a una **migliorata postura difensiva** delle **vittime**.

In ogni caso, il **calo** degli attacchi **DDoS** risulta coerente con la **diminuzione** delle **attività** di **hacktivismo** già evidenziata nei paragrafi precedenti. I **DDoS**, infatti, sono **spesso impiegati** per **scopi dimostrativi** dagli **attivisti**, e nel **2024** il loro impatto sulle organizzazioni italiane si è **sensibilmente ridotto**.

Diversamente, il malware registra un aumento considerevole: gli **incidenti** sono **passati** da **103** nel **2023** a **135** nel **2024**, con un **incremento** superiore al **30%**, in linea con quanto osservato a livello globale. Particolarmente **rilevante** è la crescita degli **attacchi** che **sfruttano vulnerabilità**: da 7 a 67 episodi, pari a un aumento di quasi il **90%**, trainato dagli attacchi al settore News / Multimedia. Su scala globale, tuttavia, questa categoria rimane stabile.

I **web attacks** in **Italia** restano **pressoché invariati**, mentre a **livello globale** crescono di circa il **50%**. Preoccupante, invece, è **l'aumento** delle **multiple techniques**, che passano da 1 a 8 incidenti (**+700%**), indicando una **crescente complessità** degli attacchi. Anche il **phishing** e il **social engineering** registrano una **crescita significativa**: da 28 a 38 incidenti, con un incremento del **35%**.

Infine, sebbene la percentuale di incidenti legati al furto d'identità in Italia rimanga marginale, è importante ricordare quanto già sottolineato nel rapporto dell'anno scorso: **nel nostro Paese le cosiddette "truffe linformatiche"** — rivolte sia ai privati cittadini sia alle piccole imprese — **sono in costante crescita**



Analisi della “Severity” degli incidenti

Dal punto di vista della **severity degli incidenti,** il dato italiano (Fig. 22) si distacca parzialmente da quello internazionale.

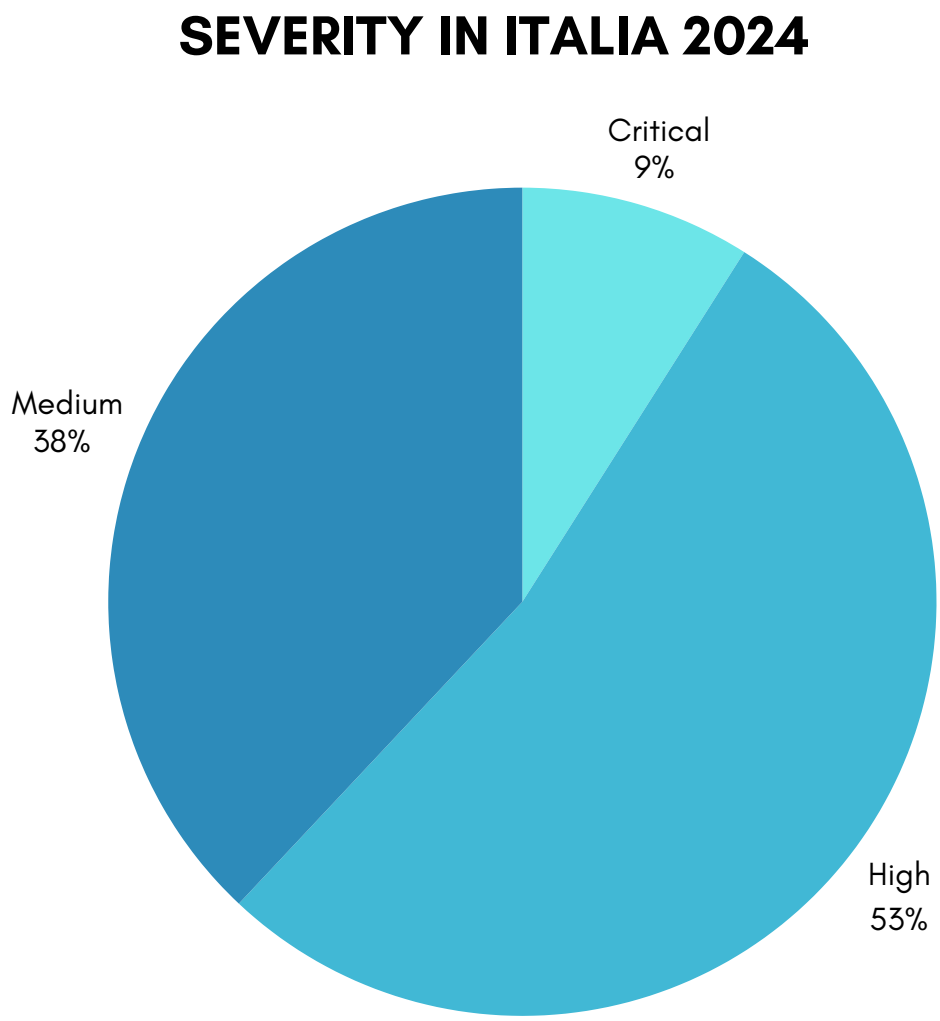


Fig.19-Severity degli attacchi in Italia nel 2024 Fonte: Rapporto Clusit 2025

In termini di **gravità degli incidenti**, il confronto tra il dato italiano e quello globale evidenzia alcune peculiarità significative. **La quota di incidenti** classificati **come high in Italia si attesta al 53%**, tre punti percentuali in più rispetto alla media globale (50%), un valore comunque comparabile.

Diversa è la situazione per gli **incidenti critical**, che risultano decisamente inferiori nel nostro Paese: **solo il 9% contro il 29% a livello mondiale.**
Al contrario, gli episodi a **gravità medium s**ono molto più diffusi in Italia, con una quota pari al 38%, rispetto al 22% osservato globalmente. Gli incidenti a basso impatto restano marginali anche in Italia, rappresentando meno dell'1% del totale.
Questi dati possono essere letti da **due prospettive**. Da un lato, è **positivo** che gli **incidenti critici** siano **molto meno frequenti** in Italia rispetto al **resto del mondo** e che, pur essendo **più numerosi quelli di media gravità**, i loro effetti siano **generalmente più contenuti**. Dall'altro lato, la **maggiore incidenza** di eventi di **gravità media** potrebbe indicare una più **elevata esposizione a minacce meno complesse**, suggerendo una certa **difficoltà**, da parte delle **organizzazioni italiane**, nel contrastare anche attacchi non particolarmente sofisticati.
Una considerazione simile emerge anche dai dati dell'**Osservatorio Cybersecurity** del **Politecnico di Milano**: il 73% delle grandi aziende italiane dichiara di aver subito almeno un attacco nei 12 mesi precedenti. Tuttavia, **nel 37% dei casi tali attacchi non hanno rappresentato** una minaccia concreta per l'organizzazione. Va **segnalato** però che nel **7% dei casi** gli incidenti hanno richiesto **interventi di mitigazione** significativi, con **impatti tangibili** sui costi e sulle attività operative. Considerando che si tratta di **aziende strutturate** e con investimenti consistenti in **cybersecurity**, questo dato rivela **difficoltà** nel mettere **in atto strategie di difesa** realmente efficaci.

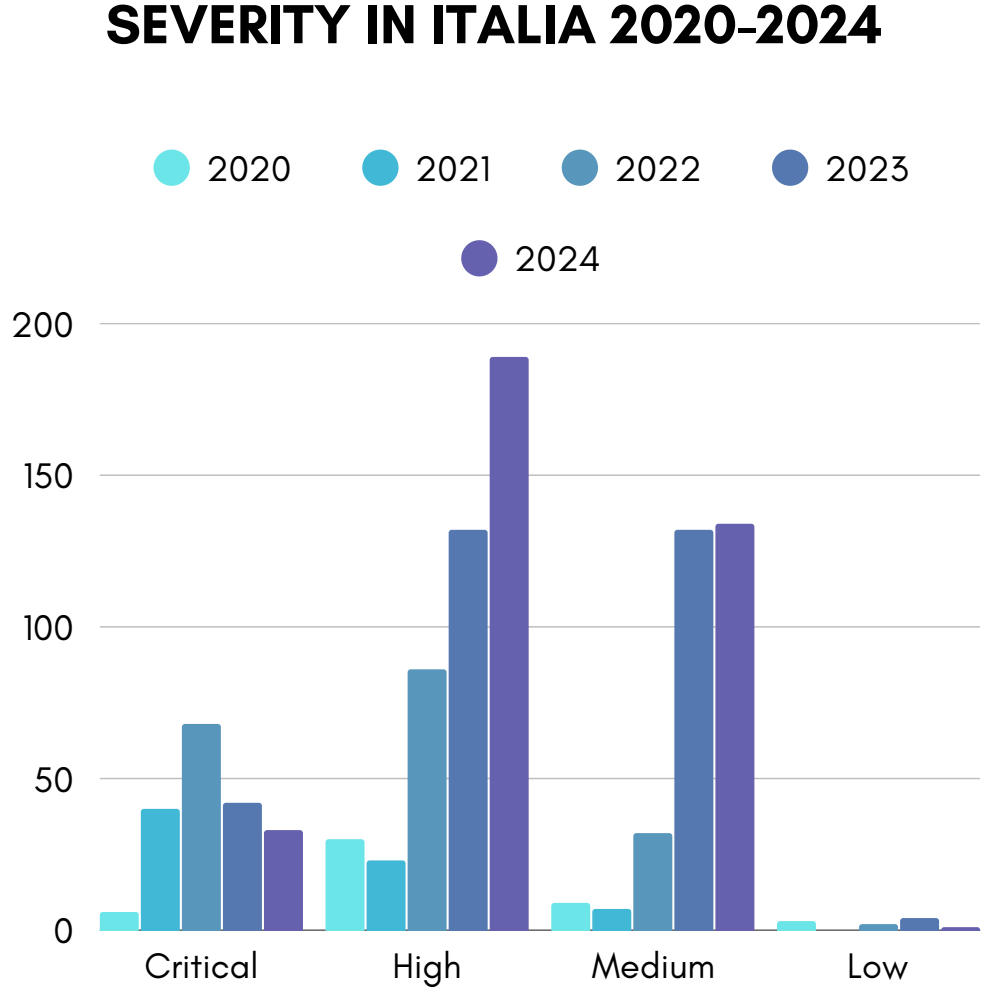


Fig.20-Severity degli attacchi in Italia nel periodo 2020-2024 Fonte: Rapporto Clusit 2025

L'**analisi della progressione storica** (Fig. 20) **mostra chiaramente** un **calo costante** degli incidenti classificati come critical, passati dal picco del 57,1% nel 2021 all'attuale 9,2%, con 35 episodi in meno rispetto al 2022. Questa **diminuzione** è più che **compensata** dalla **crescita degli incidenti** high, che aumentano di 10 punti percentuali rispetto al 2023, raggiungendo quota 189 nel 2024. **Gli eventi con gravità medium**, pur perdendo 5 punti percentuali in termini relativi, **restano stabili in valore assoluto**. Infine, gli incidenti a bassa gravità continuano a rappresentare una percentuale residuale del campione analizzato.

DORA E NIS2: LA NUOVA FRONTIERA DELLA CYBERSECURITY EUROPEA NEL 2025

Analisi degli incidenti cyber più rilevanti del 2024

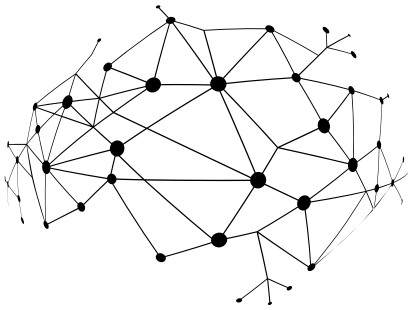
Nel 2025 la sicurezza informatica in Europa si trova al centro di una trasformazione epocale, guidata dall'entrata in vigore di due normative fondamentali: **il Digital Operational Resilience Act, noto come DORA, e la Direttiva NIS2**. Questi strumenti rappresentano la risposta dell'Unione Europea alle crescenti minacce informatiche, sempre più sofisticate e pervasive, e alla necessità di garantire una resilienza digitale efficace e omogenea su tutto il territorio comunitario.
Il rapporto ENISA Threat Landscape 2024 evidenzia un aumento costante degli attacchi informatici, con particolare riferimento ai ransomware e agli attacchi alla supply chain, che provocano danni economici e reputazionali significativi per le organizzazioni di ogni settore.

In questo scenario complesso, DORA e NIS2 non si limitano a rappresentare semplici obblighi normativi, ma **diventano veri e propri driver di innovazione e strumenti essenziali per una gestione efficace del rischio digitale**. Le aziende sono chiamate a rivedere profondamente le proprie strategie di sicurezza, integrando nuovi paradigmi e tecnologie avanzate.

DORA: Resilienza Digitale per il Settore Finanziario

DORA, entrato in vigore il 17 gennaio 2025, impone standard rigorosi per la gestione del rischio ICT nel settore finanziario. Il suo scopo è garantire che banche, assicurazioni, società di investimento, fornitori di servizi di pagamento e i loro fornitori tecnologici possano resistere, rispondere e riprendersi da eventi digitali che potrebbero compromettere la continuità operativa.
L'ambito di applicazione è ampio e **include non solo le grandi istituzioni finanziarie, ma anche fintech e fornitori di servizi cloud**, sottoponendo tutti a un regime di vigilanza uniforme e stringente.

Le organizzazioni devono implementare un framework strutturato che consenta di identificare, valutare e mitigare i rischi ICT, estendendo il controllo anche ai fornitori terzi, con l'obiettivo di mappare e monitorar3 costantemente l'intera supply chain tecnologica.



Inoltre, DORA introduce **l'obbligo di effettuare test regolari di resilienza operativa**, come **penetration test avanzati e simulazioni di attacchi complessi**, per verificare la capacità dei sistemi e dei processi di resistere a scenari di attacco sofisticati.
La tempestività nella gestione degli incidenti rappresenta un altro aspetto cruciale: gli eventi significativi devono essere notificati alle autorità competenti entro 72 ore dalla loro rilevazione, accompagnati da una dettagliata descrizione della natura dell'incidente, dell'impatto e delle contromisure adottate.

Questo obbligo mira a migliorare la trasparenza e a favorire una risposta coordinata a livello europeo.
Un'attenzione particolare è dedicata alla gestione della supply chain ICT, con la richiesta di una due diligence rigorosa sui fornitori tecnologici, audit periodici e la possibilità per le autorità di intervenire direttamente su soggetti critici in caso di non conformità.
DORA coinvolge direttamente i **vertici aziendali**, che devono garantire una **supervisione attiva** della gestione del rischio ICT e della compliance, sottolineando l'importanza di una **governance solida** e responsabile.
La sua **implementazione** comporta una trasformazione profonda dei **processi interni** e delle relazioni con i partner tecnologici, **richiedendo investimenti** in tecnologie di mo**nitoraggio continuo**, automazione e piattaforme di orchestrazione della sicurezza.
Le società di consulenza **come Deloitte e KPMG** evidenziano come la **compliance a DORA** possa diventare un fattore competitivo, rafforzando la fiducia degli stakeholder e contribuendo alla stabilità del sistema finanziario.

NIS2: Sicurezza Estesa a Tutti i Settori Critici

Parallelamente, la **Direttiva NIS2,** recepita entro ottobre 2024 dagli **Stati membri,** rappresenta un'evoluzione sostanziale rispetto alla precedente NIS1, estendendo la sicurezza informatica a un numero molto **più ampio** di settori critici e i**nfrastrutture essenziali**. L'obiettivo è proteggere servizi fondamentali quali **energia, trasporti, sanità, infrastrutture digitali, acqua potabile, servizi postali e pubblica amministrazione**,

coinvolgendo anche medie imprese con almeno 50 dipendenti e un fatturato superiore a 10 milioni di euro.

NIS2 introduce una serie di obblighi stringenti che riguardano la **gestione attiva del rischio**, la notifica tempestiva degli incidenti e la **responsabilità diretta** del management. Le organizzazioni devono adottare **misure tecniche e organizzative** proporzionate ai rischi, che includono politiche di sicurezza, formazione del personale, gestione degli accessi e protezione dei dati. **Gli incidenti rilevanti** devono essere notificati alle **autorità competenti entro 24** ore dall'identificazione, con un report completo da fornire entro 30 giorni, garantendo così una comunicazione tempestiva e coordinata.

Un **elemento distintivo di NIS2** è il rafforzamento della responsabilità del **top management**, chiamato a rispondere personalmente della conformità, con **sanzioni severe** in caso di violazioni. **Le autorità nazionali** di vigilanza dispongono di poteri estesi di supervisione, ispezione e applicazione di **sanzioni**, che possono arrivare **fino a 10 milioni di euro** o al **2% del fatturato globale.**

Questo quadro normativo richiede un cambio di paradigma culturale e organizzativo, in cui la cybersecurity diventa un elemento trasversale e strategico, coinvolgendo tutte le funzioni aziendali. ENISA sottolinea come la collaborazione tra pubblico e privato e la condivisione di informazioni sulle minacce siano essenziali per aumentare la resilienza collettiva.

Convergenze, sinergie e differenze tra DORA e NIS2

Sebbene **DORA e NIS2** abbiano ambiti di applicazione diversi, presentano molteplici punti di **contatto e sinergie** che, nel 2025,

stanno ridefinendo le strategie di cybersecurity delle aziende europee. Entrambe le **normative puntano a rafforzare** la **resilienza operativa** e la **capacità di risposta** agli incidenti, promuovendo una cultura della sicurezza diffusa e una gestione **proattiva del rischio.**

Sia **DORA sia NIS2** impongono **obblighi rigorosi** di notifica degli incidenti, con l'obiettivo di **migliorare la trasparenza**, la **collaborazione e la capacità** di risposta coordinata a livello europeo.

La **gestione dei rischi** legati ai **fornitori e ai partner tecnologici** è un elemento centrale di entrambe le normative, che richiedono **audit, monitoraggio continuo** e valutazione delle contromisure adottate da terzi. Le due normative rafforzano il **ruolo della governance**, coinvolgendo i vertici aziendali nella definizione delle strategie di sicurezza e nella supervisione delle **attività di compliance.**

Le principali differenze riguardano invece l'ambito di applicazione — settore finanziario per DORA, settori critici per NIS2 —, la natura degli obblighi (regolamento direttamente applicabile per DORA, direttiva da recepire per NIS2) e alcune specificità operative, come la frequenza e la tipologia dei test di resilienza richiesti.

Impatti Trasversali e Sfide Operative

L'entrata in vigore di **NIS2** rappresenta una sfida di portata trasversale per tutte

le imprese considerate essenziali o **importanti**. Oltre agli adeguamenti tecnologici, è richiesto un cambio di mentalità: la sicurezza non è più solo un tema IT, ma una priorità strategica che coinvolge l'intera organizzazione, dalla governance alla formazione del personale, dalla gestione dei fornitori alla comunicazione con le autorità.Dal 2025, la conformità a **DORA e NIS2** non è più soltanto una questione di adempimento normativo, ma un vero e proprio **fattore abilitante** per la **competitività e la fiducia digitale**. Le aziende hanno investito in piattaforme di monitoraggio continuo, strumenti di automazione per la **gestione della compliance**, formazione del personale e soluzioni di orchestrazione della sicurezza.
La **collaborazione tra pubblico e privato**, la condivisione delle informazioni sulle minacce e l'**adozione di standard comuni** sono diventati elementi imprescindibili per costruire un ecosistema digitale europeo sicuro e resiliente.

FOCUS: SPECIALE FINANCE

Nel **contesto contemporaneo**, il settore finanziario si configura stabilmente come uno degli **obiettivi primari** e più redditizi per la **criminalità informatica**. L'analisi dell'evoluzione del **cybercrime** nel 2024 **evidenzia** che **quasi la totalità** degli attacchi **diretti a questo comparto** è motivata da f**inalità economiche**, con il 95% degli incidenti registrati riconducibili al tentativo di **conseguire un illecito profitto**. Tale **pressione criminale** si traduce in una focalizzazione sulle azioni di sottrazione di credenziali: **dati di accesso** ai servizi di home banking, elementi identificativi delle carte di credito, **quali PAN e CVV**, e altre informazioni sensibili rappresentano il primo anello della catena che **conduce alle transazioni fraudolente** eseguite all'insaputa dei **legittimi titolari**.

Le credenziali risultano i dati più frequentemente compromessi, coinvolgendo il 50% degli incidenti rilevati. La **gravità di questi episodi** è testimoniata dal fatto che tra il 20% e il 40% degli attacchi nel **settore finanziario e assicurativo** è stato classificato come "Critical", con impatti potenzialmente devastanti sia per le istituzioni sia per i clienti.

Le tecniche d'attacco impiegate contro il settore finanziario sono molteplici e spesso combinate tra loro. **Il phishing** si conferma il vettore iniziale di accesso più **diffuso ed efficace**, responsabile del 73% delle violazioni secondo le più recenti analisi.

Il phishing si declina in molteplici forme: dallo **smishing**, che sfrutta messaggi SMS per indurre l'utente a cliccare su link malevoli o a fornire dati personali, al **quishing**, che utilizza codici QR per indirizzare le vittime verso siti fraudolenti.

Questi **attacchi** sono spesso associati a **strategie di pretexting**, nelle quali l'attaccante costruisce una narrazione ingannevole — come la **simulazione di un problema** legato a una carta di credito bloccata — per **manipolare la vittima** e indurla a rivelare informazioni sensibili, scaricare software malevolo, inviare denaro o compiere altre azioni dannose per sé stessa o per la propria organizzazione.

Una volta **sottratte le credenziali** iniziali, i criminali instaurano frequentemente **un'interazione diretta** con la vittima, impersonando **falsi operatori** di servizi finanziari al fine di ottenere ulteriori fattori di autenticazione o informazioni sui dispositivi utilizzati. Questo passaggio è fondamentale per completare le transazioni illecite, eludendo le misure di sicurezza avanzate adottate dagli istituti di credito.

Anche l'introduzione della Multi-Factor Authentication (MFA), pur rappresentando una contromisura fondamentale e ormai imprescindibile, si è dimostrata vulnerabile a queste tecniche di social engineering. Quando **il secondo fattore** di autenticazione richiede l'inserimento di **codici o PIN su form online**, o la comunicazione a **finti operatori telefonic**i o tramite **chat, i criminali sono in grado di creare form verosimili** o manipolare la vittima per ottenere questi fattori, **rendendo inefficace** la protezione introdotta dall'**MFA** in assenza di una corretta implementazione e di una solida **consapevolezza da parte dell'utente.**

Nonostante questa vulnerabilità, **l'adozione della MFA** resta essenziale, **soprattutto per l'accesso a soluzioni cloud** interne e per le **applicazioni rivolte** ai clienti, poiché una corretta implementazione **eleva significativamente** il livello di sicurezza, pur non rendendolo assoluto.

Un'altra tattica ampiamente diffusa consiste nella **creazione di siti web falsi**, i cosiddetti **siti clone**, che replicano in modo estremamente **fedele le interfacce** dei servizi bancari o di pagamento legittimi. **L'obiettivo è ingannare** gli utenti e raccogliere le loro **credenziali di accesso.**

Per **conferire un'apparenza di legittimità** e sicurezza a queste pagine fraudolente, i **cybercriminali utilizzano certificati SSL/TLS,** spesso di tipo **Domain Validation**. L'uso di questi certificati attiva il protocollo HTTPS e mostra l'**icona del lucchetto nel browser**, elementi che la maggior parte degli utenti associa erroneamente a un sito sicuro.

Tuttavia, un certificato di tipo **Domain Validation** attesta unicamente che il **richiedente controlla** il dominio a cui il certificato è associato, non **l'identità o l'affidabilità** del

proprietario del sito, una sottigliezza spesso ignorata dagli utenti e sfruttata dai criminali per aumentare l'efficacia dei loro attacchi. Nel **2024 è stato rilevato** un fenomeno particolarmente preoccupante: **l'esposizione dei dati delle vittime** da parte di numerosi kit di phishing.
Questi kit rendono accessibili i dati raccolti, come le credenziali di accesso, tramite URL facilmente raggiungibili da chi ne conosce il percorso esatto. Tale esposizione può derivare da errori di configurazione o da scelte deliberate degli attaccanti, volte a facilitare l'accesso ai dati sottratti,senza richiedere autenticazione al sito di phishing.Questa situazione non solo **semplifica il lavoro degli attaccanti** originari, ma costituisce un grave pericolo per le vittime, poich**é i loro dati rimangono visibi**li e possono essere facilmente **sottratti da altri attori malevoli.** Questi attaccanti parassiti **possono sfruttare le credenziali** rubate per orchestrare nuove campagne di attacco o per **creare e vendere** sul **dark web** insiemi di credenziali compromesse, che possono essere testate su vari servizi online, ampliando così il perimetro del rischio.

Si osserva inoltre una tendenza crescente **nell'utilizzo di InfoStealers, software** malevoli progettati per sottrarre informazioni sensibili. Questi strumenti stanno progressivamente sostituendo i **malware bancari più specializzati,** la cui diffusione è in calo da alcuni anni.

Questo cambiamento, unito alla disponibilità di strumenti di **hacking "as a service"** e modelli come il Ransomware-as-a-Service, ha abbassato **la soglia di accesso** alla commissione di frodi finanziarie e ad **attacchi più complessi**, come il ransomware. Anche criminali con **competenze tecniche medio-basse** possono ora **acquistare o affittare kit di attacco** pronti all'uso, **ampliando significativamente** la platea di potenziali attaccanti e vittime.

Il **cybercrime nel settore finanziario** non si limita ad azioni individuali, ma è spesso **opera di organizzazioni criminali** strutturate, anche con ramificazioni internazionali. Le indagini condotte **dalla Polizia Postale** e per la **Sicurezza Cibernetica** hanno fornito evidenze concrete di sodalizi criminali articolati su più livelli.

L'Operazione **Money Box**, ad esempio, ha portato alla scoperta di una complessa **organizzazione criminale** con cellule radicate in Spagna e in Italia, avvalendosi di ulteriori cellule specializzate in ruoli specifici. Questa organizzazione utilizzava tecniche di **phishing, hacking e smishing** per carpire dati sensibili di accesso alle piattaforme di h**ome banking.**

Le indagini hanno **permesso di effettuare numerose perquisizioni,** arrestare persone coinvolte in reati quali falso documentale, frode informatica e porto abusivo di armi, e sequestrare materiale informatico pertinente.

In un altro caso, **un sodalizio criminale** ha **attaccato** il sistema informatico di una **società di transazione di criptovalute, sottraendo asset digitali per un valore significativo** e riciclandoli attraverso operazioni di trasferimento, a dimostrazione di come **il cybercrime finanziario si estenda anche al mondo degli asset digitali**.

Il quadro normativo cerca di stare al passo con l'evoluzione delle minacce. Le disposizioni derivanti dalla Direttiva PSD2, recepita in Italia, impongono ai prestatori di servizi di pagamento l'obbligo di rimborsare le operazioni non autorizzate qualora non sia stata utilizzata l'autenticazione forte. Una revisione ulteriore è attesa con la finalizzazione, prevista per il 2025, della direttiva PSD3 e del regolamento PSR, strumenti normativi mirati a rafforzare la protezione degli utenti e la fiducia nei servizi di pagamento, in risposta ai progressi tecnologici e all'evoluzione delle minacce.

L'adeguamento al quadro normativo rappresenta una sfida costante per gli operatori del settore, chiamati a coniugare innovazione, sicurezza e compliance in un contesto di crescente complessità.

Per contrastare efficacemente le minacce nel settore finanziario, è indispensabile adottare strategie di difesa stratificate e robuste. La formazione e la consapevolezza del personale e degli utenti rappresentano un pilastro fondamentale, ma non sono sufficienti da sole a fronteggiare gli attacchi più sofisticati.

L'adozione della Multi-Factor Authentication (MFA) è considerata essenziale, soprattutto per l'accesso a soluzioni cloud interne e per le applicazioni rivolte ai clienti. Pur non eliminando totalmente il rischio, una corretta implementazione dell'MFA è cruciale per innalzare significativamente il livello di sicurezza.

La gestione degli accessi privilegiati, nota come Privileged Access Management (PAM), riveste un ruolo centrale nella strategia di difesa. Le soluzioni PAM consentono di applicare il principio del privilegio minimo, garantendo agli utenti e ai sistemi solo i diritti strettamente necessari per il tempo richiesto. Questo limita drasticamente il movimento laterale degli attaccanti una volta ottenuta una prima compromissione e riduce la superficie di attacco.

Le **compagnie assicurative**, sempre più **attente** alla gestione del **rischio cyber**, richiedono spesso l'implementazione di **soluzioni PAM** come **prerequisito** per **l'emissione** di **polizze** sui rischi informatici, riconoscendo che tali misure rendono più difficile per gli attaccanti muoversi nell'ambiente, aumentare i privilegi e lasciare tracce, aumentando così le opportunità di rilevamento e risposta per prevenire perdite significative.
Le soluzioni di **Identity Threat Detection** and **Response** stanno suscitando **crescente interesse** per la loro **capacità** di **identificare**, **bloccare** e **rispondere rapidamente** agli attacchi che hanno come obiettivo le identità digitali. Queste **soluzioni integrano strumenti** e **processi focalizzati** sulla **sicurezza** delle **identità**, un aspetto sempre più critico dato **l'aumento** delle **minacce** rivolte a identità e accessi.

L'utilizzo della **Cyber Threat Intelligence** (**CTI**) è **fondamentale** per **anticipare** e prevenire le **minacce**: i feed di CTI forniscono descrizioni **aggiornate** di minacce e **attacchi**, consentendo di **aggiornare** le soluzioni di **sicurezza** in **tempo reale** o quasi, in modo simile agli aggiornamenti antivirus. La condivisione di informazioni attraverso reti specializzate è di grande valore per gli attori del settore, favorendo una risposta coordinata e tempestiva agli attacchi.
Un **approccio proattivo** alla gestione dell'esposizione al rischio **implica l'analisi continua** delle superfici d'attacco, la comprensione di come le vulnerabilità potrebbero essere sfruttate e l'applicazione mirata di misure correttive per mitigare i rischi più rilevanti.

Questo **consente** ai **team** di **sicurezza** di **concentrare risorse** e **sforzi** dove sono maggiormente necessari per **prevenire** le **opportunità di attacco.**

Sebbene non direttamente correlata alle frodi di pagamento, la sicurezza nella gestione documentale costituisce un aspetto importante nel settore finanziario, in ragione del volume e della sensibilità delle informazioni trattate. Dispositivi come stampanti, scanner e multifunzione possono rappresentare punti di rischio se non adeguatamente protetti.

Documenti riservati possono essere abbandonati sulle periferiche di stampa, accessibili a persone non autorizzate, violando politiche di privacy e potendo essere utilizzati per scopi impropri. Le indagini stimano che una quota significativa di documenti stampati non venga mai prelevata dalla stampante.

Per **mitigare** questo **rischio**, è possibile **implementare limitazioni** di **accesso** e funzioni sui dispositivi di stampa per **gruppi** o **individui specifici**. La **formazione** degli utenti e l'adozione di **regole chiare** per la gestione dei documenti, sia digitali sia cartacei, sono essenziali per ridurre questi rischi.

La **trasformazione digitale** in atto nel **settore finanziario** impone una riflessione sulla **resilienza** dei **dati** e sulla **sicurezza operativa**, soprattutto alla luce delle rigide normative e dell'incremento delle minacce informatiche. La **resilienza cyber** si fonda sulla **capacità** di **prevenire**, **resistere** e **rispondere efficacemente** agli **incidenti**, garantendo la continuità operativa e la protezione degli asset critici.

Le **istituzioni finanziarie** sono chiamate a **investire** in **soluzioni tecnologiche avanzate**, a **rafforzare** la **cultura** della **sicurezza** e a sviluppare piani di risposta agli incidenti che prevedano la collaborazione tra tutti gli attori coinvolti,

inclusi fornitori di servizi, autorità di vigilanza e organismi di settore.

Alla luce di quanto emerso, il **settore finanziario** opera in un **ambiente** di **minaccia cyber estremamente dinamico** e complesso, caratterizzato da motivazioni prevalentemente economiche.

Le **tecniche d'attacco** si **evolvono**, **combinando metodi** consolidati come il **phishing** con l'uso di **strumenti** sempre più **accessibili** e **sofisticati**, spesso resi disponibili da organizzazioni criminali strutturate.

La **risposta efficace** a questo scenario richiede un **impegno** costante nell'adozione di **misure** di **sicurezza** tecniche **all'avanguardia**, **un'attenzione scrupolosa** alla gestione delle identità e degli accessi, un **adeguamento continuo** al quadro normativo e una forte **enfasi** sulla **formazione** e consapevolezza a tutti i livelli.

La **gestione** del **rischio cyber** si configura come una **sfida sistemica** e **globale**, che va ben oltre i danni subiti dalle singole vittime. La protezione delle infrastrutture, dei dati sensibili e della fiducia degli utenti rappresenta una sfida continua che richiede un approccio olistico e proattivo, in grado di coniugare innovazione, resilienza e compliance per garantire la stabilità e la sicurezza dell'intero ecosistema finanziario.

FOCUS: CYBERSECURITY 2030-2035

Il **2030** si avvicina come una frontiera decisiva per la cybersecurity, un orizzonte in cui la sicurezza digitale non sarà più un semplice baluardo tecnico, ma un **pilastro** della **stabilità economica**, **sociale** e **geopolitica globale**.

Geopolitica digitale: la nuova Guerra Fredda delle supply chain

Uno degli aspetti più inquietanti del prossimo decennio sarà la crescente **vulnerabilità delle supply chain digitali**. La dipendenza globale da semiconduttori e componenti IoT, prodotti in hub strategici come Taiwan, trasformerà la catena di approvvigionamento in un vero e proprio campo di battaglia. Secondo **ENISA**, entro il **2030** il **70%** delle **organizzazioni** subirà **almeno un attacco** legato a **vulnerabilità** di **terze parti**.

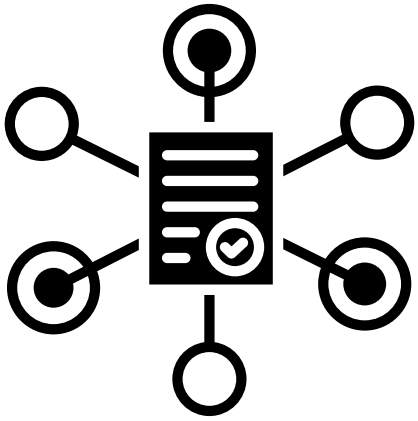
Immaginiamo l'impatto di un cyberattacco a un produttore di chip: la produzione di veicoli autonomi, dispositivi medici e infrastrutture critiche potrebbe essere paralizzata, con danni economici stimati in centinaia di miliardi di euro.

Per rispondere a queste minacce, saranno necessari standard avanzati di tracciabilità, come il **framework SLSA** (Supply-chain Levels for Software Artifacts), e accordi transnazionali per la creazione di riserve strategiche di componenti.

Il SLSA, sviluppato da Google e rilasciato nella versione 1.0 nell'aprile 2023, è un framework **volto a garantire l'integrità e la sicurezza degli artefatti software lungo tutta la catena di fornitura**. Esso fornisce linee guida e requisiti di sicurezza che coprono l'intero ciclo di vita del software, dallo sviluppo al deployment, con l'obiettivo di ridurre il rischio di attacchi alla supply chain software.

L'importanza di **SLSA** deriva dalla **crescente complessità** e **interconnessione** delle **catene** di **fornitura software**, che espongono le **organizzazioni** a **vulnerabilità sfruttabili** per **accessi non autorizzati**, **inserimento** di **codice malevolo** o **furto** di **dati sensibili**, con **conseguenze** gravi quali danni **reputazionali**, **perdite economiche** e **responsabilità legali**.

Il **framework** definisce **controlli** su aspetti quali la **firma** del **software**, la **provenienza** degli **artefatti**, i **processi** di **build** e **rilascio**, la **scansione** delle **vulnerabilità** e le **attestazioni** di **sicurezza**. Seguendo **SLSA**, team di sviluppo e **DevOps** possono adottare best practice condivise per migliorare



la **sicurezza** della **supply chain** e **aumentare** la **fiducia** nella qualità e nell'integrità del software.

Diventerà così una **questione** di **sicurezza nazionale** e di **stabilità internazionale**, richiedendo una **cooperazione** senza precedenti tra **governi** e **settore privato**.

Disinformazione quantistica e manipolazione sociale

L'avvento del **6G** e **dell'intelligenza artificiale generativa** promette di **rivoluzionare** la **comunicazione**, ma porta con sé **rischi inediti**. **Deepfake** iperrealistici, prodotti e **diffusi** in tempo reale da botnet **distribuite** su **dispositivi IoT**, potranno **influenzare elezioni**, **destabilizzare** mercati finanziari e **minare** la **fiducia** nelle **istituzioni**. Secondo gli scenari **ENISA**, nel **2028 elezioni** in paesi chiave come Francia e India **potrebbero** essere **compromesse** da video **falsi indistinguibili** dalla **realtà**.

La **risposta** a questa minaccia passerà per **piattaforme** di **fact-checking** basate su **blockchain**, **leggi** che impongano **l'etichettatura obbligatoria** dei contenuti sintetici e una **nuova alfabetizzazione digitale** che renda i cittadini più consapevoli e resilienti di fronte alla manipolazione informativa.

L'integrità democratica, nel 2030, sarà difesa tanto dalla tecnologia quanto dalla cultura civica.

Cybercrime as a Service: l'industrializzazione del crimine digitale

Il cybercrime si sta **trasformando** in un **settore industriale**, **accessibile** anche a **utenti privi** di **competenze** tecniche. Entro il **2027**, strumenti come "**Ransomware GPT**" permetteranno di **lanciare attacchi** su **misura**, **acquistabili** nel **dark web** per **importi frazionati** di **Bitcoin**. Un **dipendente** scontento **potrà bloccare** le **apparecchiature** di un ospedale connesso, causando danni immediati e potenzialmente letali.
Per **fronteggiare** questa **industrializzazione** del **crimine**, le **organizzazioni** dovranno adottare piattaforme **SOAR** (Security Orchestration, Automation and Response) e **istituire task force** transnazionali capaci di reagire in tempo reale. La collaborazione tra forze dell'ordine, aziende tecnologiche e istituzioni internazionali sarà fondamentale per contrastare un fenomeno che rischia di sfuggire a ogni controllo.

Quantum Apocalypse: la corsa alla crittografia post-quantum

L'arrivo dei primi computer **quantistici operativi**, previsto entro il **2029**, rappresenta una **minaccia** esistenziale per la **crittografia tradizionale**. Algoritmi oggi considerati sicuri, come **RSA-2048**, diventeranno **vulnerabili** agli attacchi "**harvest now, decrypt later**": i dati cifrati oggi potrebbero essere sottratti e decifrati in futuro, esponendo segreti industriali, dati finanziari e informazioni sensibili.

La migrazione verso standard post-quantum, come **CRYSTALS-Kyber**, e l'adozione di **crittografia omomorfica** saranno **fondamentali** per **proteggere** la **riservatezza** delle **informazioni**. La **transizione** richiederà **investimenti** massicci in ricerca e sviluppo, oltre a una pianificazione strategica a livello globale per evitare una nuova corsa agli armamenti digitali.

Smart city e il paradosso della connettività

Entro il **2030**, le **smart city** ospiteranno oltre **50 miliardi** di dispositivi **IoT**, **trasformando** le **infrastrutture urbane** in **bersagli** privilegiati per attacchi coordinati. Un attacco alle reti elettriche di una grande città europea potrebbe causare blackout prolungati, con effetti a catena su trasporti, sanità e servizi essenziali.

La situazione è aggravata dalla persistenza di **sistemi legacy**: nel **2023**, il **45%** dei **controller industriali** utilizzava ancora Windows XP, un sistema operativo **privo** di **aggiornamenti** di **sicurezza**.

Per costruire resilienza, sarà necessario **adottare framework zero trust**, **sostituire** gradualmente i **sistemi obsoleti** e rendere **obbligatorie polizze** assicurative **cyber** per le infrastrutture critiche.

Tecno-autoritarismo e sorveglianza di massa

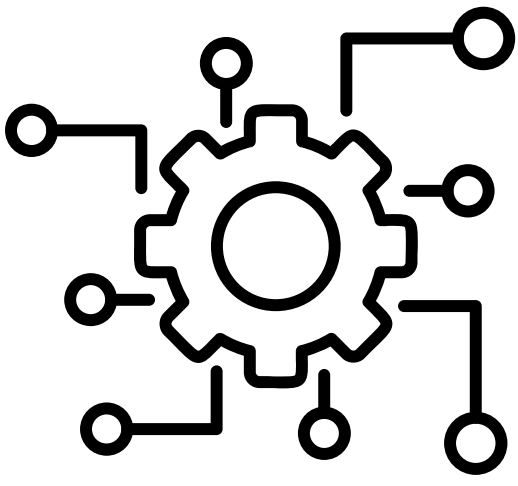
Il **lato oscuro** dell'**innovazione tecnologica** si manifesta nell'**espansione** dei **modelli di sorveglianza** di massa. Sistemi come il **credito sociale cinese** verranno esportati in Africa e America Latina tramite investimenti in tecnologie di riconoscimento facciale e piattaforme di e-commerce

Per contrastare questa deriva, l'Unione Europea dovrà implementare sanzioni mirate contro i data broker e aggiornare il GDPR con standard di anonimizzazione avanzati. La difesa dei diritti digitali diventerà una delle principali sfide politiche del prossimo decennio, richiedendo una regolamentazione agile e una vigilanza costante.

La crisi delle competenze e l'automazione difensiva

Il **gap globale** di **professionisti** della **cybersecurity**, stimato in oltre 4 milioni di unità, spingerà verso l'**iper-automazione** della **difesa**. Tuttavia, **l'eccessivo affidamento su sistemi automatizzati espone a rischi**: il **40%** degli **attacchi fileless**, che sfruttano strumenti legittimi per colpire, potrebbe **eludere** i **controlli automatizzati**. Inoltre, le stesse **intelligenze artificiali difensive** potranno essere **manipolate** per generare **falsi positivi** e **saturare** i centri di controllo (**SOC**).

La **soluzione** passa **dall'integrazione** della **cybersecurity** nei **curricula scolastici**, da **programmi** di **upskilling finanziati** da **partnership pubblico-private** e da una **cultura** della **sicurezza** diffusa a tutti i livelli organizzativi. La **formazione** continua e la collaborazione tra università, aziende e istituzioni saranno **essenziali** per **colmare** il **divario** di **competenze** e garantire una **difesa efficace**.



Impatto ambientale sulle infrastrutture digitali

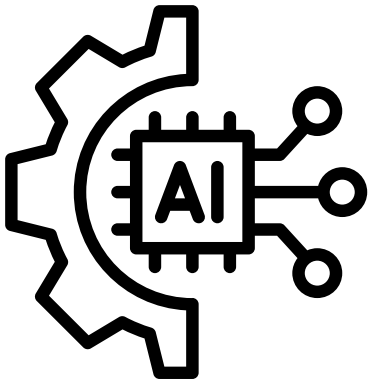
Un aspetto spesso sottovalutato riguarda l'impatto dei **cambiamenti climatici** sulle infrastrutture digitali. **Eventi estremi**, come uragani e alluvioni, potrebbero danneggiare data center e reti di comunicazione, causando **interruzioni** prolungate dei servizi critici. Nel 2027 si prevede che un uragano nel Golfo del Messico possa isolare temporaneamente l'Europa dal cloud statunitense per 48 ore, sottolineando l'importanza della ridondanza geografica e dell'adozione di data center modulari subacquei.

Verso un nuovo ordine cyber-globale

Per affrontare queste sfide, la **comunità internazionale** dovrà ridefinire le **regole** del **gioco** digitale. Trattati per vietare attacchi alle infrastrutture civili, investimenti annuali di **100 miliardi** di euro in **ricerca** e **sviluppo** per **l'IA etica** e la **crittografia post-quantum**, nonché una **cyber-diplomazia** attiva a sostegno di tecnologie open-source saranno i pilastri di un nuovo ordine cyber-globale.

Come sottolinea **ENISA**, la **resilienza non è un prodotto, ma un processo continuo**: solo un approccio olistico, che integri tecnologia, politica e formazione, potrà garantire un 2030 sicuro e inclusivo.

La **cybersecurity** del **futuro** sarà una **sfida collettiva**, un'opportunità per costruire un **ecosistema digitale** più **sicuro**, **trasparente** e **sostenibile** per tutti.



Cybersecurity 2030-2035: la nuova frontiera per le PMI italiane

Nel decennio 2030-2035, la **cybersecurity** rappresenterà una **sfida strategica** e imprescindibile per le **PMI** italiane, chiamate a operare in un contesto digitale sempre più interconnesso e complesso. L'adozione massiva di **tecnologie cloud**, piattaforme **SaaS** e **dispositivi IoT**, unita alla crescente **dipendenza** da **fornitori esterni** e **supply chain globali**, **amplierà** notevolmente la **superficie d'attacco**, esponendo le aziende a rischi inediti e minacce sofisticate. In questo scenario, le PMI saranno spesso considerate dagli attaccanti come anelli deboli della catena produttiva, vulnerabili sia a violazioni dirette sia a impatti a cascata derivanti da attacchi a terze parti.

La **carenza** di **competenze** interne in **ambito cybersecurity**, la **persistenza** di **sistemi legacy** e **l'errore umano** continueranno a rappresentare **fattori critici**, mentre l'automazione difensiva, pur fondamentale, non potrà sostituire la formazione continua e una cultura della sicurezza condivisa. Inoltre, le nuove frontiere della disinformazione digitale e **l'arrivo** dei **computer quantistici** introdurranno **ulteriori sfide**, imponendo l'adozione di **strumenti** di **monitoraggio reputazionale** e la **migrazione** verso **standard crittografici** post-quantum.

Non va infine trascurato l'impatto dei **cambiamenti climatici** sulle infrastrutture digitali, che richiederà alle **PMI** di **investire** in **soluzioni** di **backup distribuite** e piani di continuità operativa.

In questo contesto, la capacità di **valutare** e **certificare** la sicurezza dei fornitori, adottare **tecnologie** zero trust, **monitorare** la **reputazione** digitale e **pianificare** la **resilienza** operativa diventerà **cruciale**.

FOCUS: INTELLIGENZA ARTIFICIALE E IL FUTURO DELLA CYBERSECURITY

Se **DORA e NIS2** rappresentano il quadro normativo di riferimento per la sicurezza digitale europea, **l'intelligenza artificiale (AI)** è il vero fattore di discontinuità tecnologica che sta già trasformando — e trasformerà sempre di più — le strategie di **difesa e attacco** nel cyberspazio. Nel prossimo futuro, l'AI sarà al centro di una nuova generazione di **strumenti, processi e minacce,** imponendo alle organizzazioni una riflessione profonda su come integrare questa tecnologia in modo **sicuro, etico** e conforme alle regole europee.

L'**intelligenza artificiale** sta **rivoluzionando la cybersecurity** grazie alla sua capacità di processare enormi quantità di dati in tempo reale, individuare **pattern anomali** e automatizzare la risposta agli **attacchi**. I sistemi **AI-based** sono sempre più utilizzati per la **threat detection avanzata**: algoritmi di machine learning analizzano i log di sistema, il traffico di rete e i comportamenti degli utenti, identificando minacce che sfuggirebbero all'analisi umana. L'AI consente di bloccare automaticamente attività sospette, isolare dispositivi compromessi e avviare procedure di **remediation** senza intervento umano, riducendo drasticamente i tempi di reazione. Modelli **predittivi** anticipano nuove vulnerabilità e attacchi, consentendo alle aziende di rafforzare preventivamente le proprie difese. L'**AI** viene impiegata anche per monitorare la conformità alle normative come **DORA e NIS2**, identificando in tempo reale eventuali gap o anomalie nei processi di sicurezza.

Parallelamente, l'AI rappresenta una **minaccia crescente**, poiché viene adottata anche dai **cybercriminali** per **potenziare** la **sofisticazione** e l'**efficacia degli attacchi**. L'AI genera email di phishing iper-personalizzate, **deepfake vocali** e **video**, rendendo più **difficile per gli utenti** distinguere tra comunicazioni autentiche e fraudolente. **Botnet** intelligenti possono **lanciare** attacchi **DDoS** adattivi, **cambiare strategia** in tempo reale e aggirare le difese tradizionali. **Algoritmi di AI** sono in **grado di testare** e **aggirare i sistemi** di rilevamento, identificando le **vulnerabilità** più deboli e sfruttandole in modo mirato.

Nel prossimo futuro, la **cybersecurity** sarà sempre più **"AI-driven"**. Le **organizzazioni** dovranno **investire in piattaforme** di **sicurezza** basate su **intelligenza artificiale**, capaci di integrare **dati** provenienti da **fonti eterogenee**, correlare eventi in tempo reale e orchestrare risposte automatizzate su vasta scala. Tuttavia, questa evoluzione comporta **nuove sfide**: l'utilizzo dell'**AI** in **ambito sicurezza** richiede trasparenza sugli algoritmi, **auditabilità** delle **decisioni automatiche** e rispetto dei **principi etici**, in linea con quanto **previsto** dal **futuro AI Act** europeo. Le **aziende** dovranno **valutare** non solo i **rischi** informatici tradizionali, ma anche quelli legati all'**uso improprio** o non intenzionale dell'AI, adottando modelli di **risk management** specifici. La **diffusione dell'AI** impone nuove competenze, sia **tecniche** che **organizzative**, per gestire sistemi complessi e garantire una collaborazione efficace tra uomo e macchina. L'**integrazione tra AI** e normative come **DORA e NIS2** richiederà l'adozione di nuovi standard di sicurezza, audit e controllo, per assicurare che l'AI sia un fattore di rafforzamento — e non di vulnerabilità — della postura di sicurezza aziendale.

Guardando al futuro, l'**AI** sarà **sempre più centrale** nelle strategie di **cybersecurity**, ma il suo utilizzo dovrà essere r**egolato e integrato** in **un quadro normativo** chiaro e condiviso. Il **prossimo AI Act europeo**, insieme a **DORA e NIS2**, definirà le regole per un'adozione responsabile e sicura dell'**intelligenza artificiale**, promuovendo **trasparenza**, **accountability** e rispetto dei **diritti fondamentali**. Le aziende che sapranno integrare efficacemente **AI**, **compliance normativa** e **cultura della sicurezza** saranno in grado di affrontare con successo le sfide di un **ambiente digitale** sempre più **complesso**, **proteggendo dati**, **infrastrutture e reputazione**, e garantendo la **continuità operativa** anche di fronte a minacce inedite e sofisticate.

Strategie di Conformità e Best Practice per il 2025

Per adeguarsi efficacemente a **DORA** e **NIS2**, le aziende devono adottare un **approccio** basato sul **rischio**, strutturato e continuo, che preveda innanzitutto un inventario completo degli asset IT e OT. È fondamentale **mappare** tutti gli **asset** tecnologici, inclusi hardware, software, dati, infrastrutture di rete e sistemi operativi industriali, per definire il perimetro di rischio e identificare le vulnerabilità. Questa attività rappresenta la base per ogni valutazione del rischio e per la definizione delle misure di sicurezza.

La **valutazione** del rischio deve essere un **processo dinamico**, con **revisioni** almeno **annuali** o in seguito a cambiamenti significativi nell'infrastruttura.

Business Continuity e Disaster Recovery: Pilastri della Resilienza

La conformità a **DORA e NIS2** non può prescindere da solide strategie di **business continuity** e **disaster recovery**. Questi asset strategici garantiscono la capacità di mantenere operativi i servizi essenziali anche in caso di attacchi o malfunzionamenti. È necessario **sviluppare piani dettagliati**, testati regolarmente, che prevedano **scenari di crisi realistici** e coinvolgano tutte le funzioni aziendali. La capacità di dimostrare l'**efficacia** di questi piani rappresenta un requisito fondamentale per la **compliance** e contribuisce significativamente a ridurre i rischi operativi.

Sanzioni e Responsabilità: Un Incentivo alla Cultura della Sicurezza

Le sanzioni previste da **DORA e NIS2** sono severe e rappresentano un **forte incentivo** al rispetto delle norme. Le multe possono raggiungere decine di **milioni di euro** o percentuali significative del fatturato globale, con **conseguenze anche reputazionali** rilevanti. Inoltre, entrambe le normative introducono **la responsabilità personale dei dirigenti,** che possono essere chiamati a rispondere in caso di violazioni gravi. Questo spinge verso **una cultura aziendale** in cui la **cybersecurity** è una priorità strategica e non un mero adempimento formale.

Prospettive Future e Trend Emergenti

I principali **report di settore**, tra cui quelli di **ENISA, Gartner, Deloitte e EY**, indicano che il **2025** e gli anni a venire saranno caratterizzati da un'intensa **automazione** e dall'adozione di **intelligenza artificiale** per la **gestione proattiva** delle minacce e la compliance continua.

La **cybersecurity** sarà sempre più **integrata nei processi** di business e nella **governance aziendale**, mentre la collaborazione tra pubblico e privato si rafforzerà per favorire la condivisione di informazioni e **best practice**. La sicurezza della **supply chain** continuerà a essere un'area di grande attenzione, con l'obiettivo di mitigare rischi sistemici. Infine, si sta già lavorando alla preparazione per l'era **post-quantum,** con l'adozione di tecnologie crittografiche resistenti ai computer quantistici, che rappresenteranno una nuova frontiera della sicurezza digitale.

L'entrata in **vigore di DORA e NIS2** segna una svolta decisiva nella **cybersecurity** europea, imponendo **standard elevati** e un **approccio integrato** alla **gestione del rischio digitale**. Le aziende sono chiamate a fronteggiare una sfida complessa, ma anche un'**opportunità** per rafforzare la resilienza, migliorare la **fiducia** degli **stakeholder e competere** in un **mercato** globale sempre più digitale e interconnesso. La compliance non è più un mero **adempimento formale**, ma un elemento chiave della strategia aziendale, che richiede **investimenti mirati**, innovazione tecnologica e un cambiamento culturale profondo

Il Supporto di Planetica per la Cybersecurity e la Compliance Normativa

Alla luce dei **recenti cambiamenti normativi** e dell'**evoluzione** del panorama delle **minacce**, Planetica ha **maturato competenze** specifiche nell'ambito della **cybersecurity** e della compliance a **DORA, NIS2** e alle **principali normative europee**. Siamo in grado di **affiancare i clienti** nell'interpretazione dei nuovi **requisiti**, nell'**adeguamento dei processi** e nell'implementazione delle misure tecniche e organizzative richieste.

Il **supporto** può **includere** attività di **assessment**, **definizione** di **strategie** di **gestione del rischio**, **formazione del personale** e predisposizione della **documentazione** necessaria per la conformità.
In questo modo, le **organizzazioni** possono **affrontare** con maggiore consapevolezza e preparazione le **sfide** poste dal nuovo contesto normativo e tecnologico.

CONCLUSIONI: UN IMPEGNO CONDIVISO PER UN FUTURO DIGITALE SICURO

L'analisi condotta nel presente report evidenzia come la cybersecurity sia ormai un elemento strutturale e imprescindibile per la resilienza e la competitività di organizzazioni pubbliche e private, in un contesto globale caratterizzato da una crescita costante sia del numero sia della gravità degli incidenti informatici. Il 2024 ha segnato un nuovo record per numero di attacchi rilevati e per impatto sugli asset critici, confermando il trend di intensificazione delle minacce e la professionalizzazione degli attori malevoli.

Il cybercrime si consolida come principale vettore di rischio, favorito dalla diffusione di modelli "as-a-Service" che abbassano la soglia tecnica di ingresso e amplificano la portata delle campagne offensive. Parallelamente, l'adozione accelerata di tecnologie emergenti — in particolare l'intelligenza artificiale generativa, il cloud e l'edge computing — introduce nuove vulnerabilità e impone una revisione continua delle strategie di difesa e dei modelli di governance. Le direttive europee DORA e NIS2, insieme al futuro AI Act, rappresentano un cambio di paradigma normativo che richiede alle organizzazioni di adottare un approccio proattivo, integrato e basato sul rischio.

Il quadro nazionale riflette le stesse criticità: l'Italia, pur rappresentando una quota limitata di PIL e popolazione a livello globale, continua a essere sovraesposta agli attacchi, con un'incidenza di incidenti superiore alla media europea. La carenza di competenze specialistiche, la presenza di sistemi legacy e la frammentazione delle responsabilità restano fattori di vulnerabilità diffusa.

Alla luce di queste evidenze, risulta prioritario:

- *rafforzare la collaborazione pubblico-privato e la condivisione tempestiva delle informazioni sulle minacce;*
- *investire in formazione continua e sviluppo di competenze specialistiche, colmando il gap tra domanda e offerta di professionisti qualificati;*
- *integrare la gestione del rischio cyber nei processi di business e nella governance aziendale, superando la logica del mero adempimento normativo;*
- *sviluppare strategie di resilienza che includano la business continuity, il disaster recovery e la protezione della supply chain;*
- *adottare tecnologie di sicurezza avanzate, con particolare attenzione all'automazione, all'intelligenza artificiale e alle architetture zero trust.*
-

In quest'ottica, Planetica si propone come partner strategico per la definizione di modelli di governance della sicurezza, per l'assessment della postura cyber e per il supporto operativo alla compliance, in particolare in riferimento a normative di ultima generazione come il Regolamento DORA e i suoi atti esecutivi.
Inoltre, Planetica è impegnata attivamente nel promuovere la consapevolezza e la formazione su tematiche cyber presso le istituzioni finanziarie, contribuendo alla diffusione di una cultura della sicurezza resiliente, condivisa e sostenibile.
La cybersecurity non può più essere considerata una funzione accessoria, ma va riconosciuta come fattore abilitante per la protezione degli asset, la continuità operativa e la fiducia degli stakeholder. Solo un approccio multidisciplinare, proattivo e sostenuto da una governance solida potrà garantire la capacità di adattamento necessaria per fronteggiare minacce sempre più sofisticate e mutevoli.

La sfida è sistemica e globale: la capacità di anticipare, prevenire e rispondere efficacemente agli attacchi determinerà la stabilità e la competitività dell'intero ecosistema digitale nei prossimi anni.

BIBLIOGRAFIA / SITOGRAFIA

- Rapporto Clusit 2024 sulla sicurezza ICT in Italia – Security summit
- Global Threat Report 2024 di CrowdStrike
- https://www.zscaler.it/resources/security-terms-glossary/what-is-cloud-native-application-protection-platform-cnapp
- https://www.trendmicro.com/it_it/what-is/cloud-native/cnapp.html
- Report ISC2 Cybersecurity Workforce Study, 2023 "How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce"
- IA 4 Italy: impatti e prospettive dell'Intelligenza Artificiale generativa per l'Italia e il made in Italy – The European House – Ambrosetti
- https://www.automazionenews.it/rapporto-clusit-2024-in-italia-cyber-attacchi-65-ma-e-solo-punta-delliceberg/
- https://www.ilsole24ore.com/art/italia-impreparata-attacchi-cyber-2024-timori-infrastrutture-critiche-AFTuukFC
- https://www.cybersecurity360.it/news/attacchi-cyber-nei-dati-clusit-uno-scenario-fosco-nel-2023-piu-12-per-cento/

- https://prothect.it/cybersecurity/cybersecurity-2025-le-previsioni-del-rapporto-clusit/
- https://www.analisidifesa.it/2025/02/italia-bersaglio-privilegiato-degli-hacker-cresce-il-mercato-della-cybersicurezza/
- https://www.cybersecurity360.it/nuove-minacce/cybersecurity-2025-rapporto-clusit-dati-tendenze/
- https://www.cyberguru.it/2025/03/17/clusit-2025-italia-sempre-nel-mirino/
- https://www.plurimedia.it/blog/rapporto-clusit-2025-analisi-del-cybercrime-2024-e-previsioni-per-il-futuro
- https://www.agendadigitale.eu/sicurezza/governance-della-cybersecurity-la-sfida-strategica-per-litalia-2025/
- https://www.overlux.tech/info-express/
- https://www.agendadigitale.eu/sicurezza/cybersecurity-2025-guida-pratica-per-pmi-nel-nuovo-contesto-normativo/
- https://blog.cyberoo.com/cybersecurity-2025-come-difendersi-dagli-attacchi-informatici
- https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-our-2025-cybersecurity-forecast-report
- https://www.linkedin.com/pulse/cybersecurity-crossroads-geopolitics-navigating-2025s-faisal-yahya-uzbrc

- Security summit - Rapporto Clusit 2025 sulla sicurezza ICT in Italia
- Politecnico di Milano - Osservatorio Cybersecurity
- CrowdStrike - Global Threat Report 2025
- World Economic Forum – Global Cybersecurity Outlook 2025
- NTT Data - DORA e NIS2: strategia di cybersecurity sostenibile
- Telefónica - DORA, NIS2 and CRA: Decoding Europe's Cybersecurity Regulatory Landscape
- Swisscom - Cybersecurity 2025: Unlock growth with DORA, NIS2, and Digital Trust
- TechBusiness - Cybersecurity nel 2025, tra nuove normative europee e trend
- Tresorit - From NIS2 to zero trust: IT security predictions for 2025
- Atos - Understanding new EU cybersecurity regulations: DORA & NIS2
- NordLayer - DORA and NIS2: Overview, Importance & Key Differences
- OneSpan - How NIS2 and DORA seek to strengthen cybersecurity for enterprises in the EU
- Ecovis - DORA NIS2: New changes in the law ensure cyber security
- ENISA - Threat Landscape 2024 e linee guida tecniche per NIS2
- Commissione Europea - Regolamento DORA (EUR-Lex)

- Deloitte – Report su DORA e NIS2
- KPMG – Report su DORA e NIS2
- EY – Report su DORA e NIS2
- Gartner - Cybersecurity Risk Management Trends 2025
- https://skillogic.com/blog/the-future-of-cyber-security-what-to-expect/
- htttps://www.enisa.europa.eu/sites/default/files/2024-11/Cybersecurity_Threats_for_2030_-_Update_2024_-_Executive_Summary_0.pdf
- https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report
- https://www.cybersecitalia.it/wp-content/uploads/2024/05/Foresight-Cybersecurity-Threats-for-2030-Update-fullreport_en.pdf

CONTATTI

Matteo M. Marzan
matteo.marzan@planetica.it

Andrea Rivetti
andrea.rivetti@planetica.it

Team di lavoro

Riccardo Mandiroli

Federico Alfano

Alessandro Croce

Marta Allievi

Per maggiori informazioni:
Tel: +39 02 82785 740 | E-mail: segreteria@planetica.it | Indirizzo: Via Crocefisso 5, Milano

Visita il nostro sito web per ricevere il report completo

planetica

www.planetica.it