MATICMIND®
MAKES IT EASY

# ANALISI DELLA CYBERSECURITY NEL SETTORE GDO

## Attacchi, danni, impatti e rischi nel biennio 2024-2025

www.maticmind.it

# Sommario

# Introduzione

Il settore dei GDO rappresenta una delle infrastrutture critiche più esposte e vulnerabili agli attacchi informatici, con implicazioni significative per la sicurezza nazionale, l'economia e la vita quotidiana dei cittadini. La crescente digitalizzazione e interconnessione dei sistemi di GDO, unita alla loro criticità strategica, li rende obiettivi particolarmente appetibili per attori malevoli, dalle organizzazioni criminali ai gruppi hacktivisti con possibili legami statali.

## Obiettivo del Report

Questo report si propone di fornire un'analisi approfondita e strutturata dello stato della cybersecurity nel settore GDO nel biennio 2024-2025, con particolare attenzione al contesto italiano ed europeo. Gli obiettivi specifici includono:

- **Mappare il panorama delle minacce cyber** che interessano il settore GDO, identificando trend, vettori di attacco prevalenti e attori malevoli.
- **Quantificare l'impatto economico** degli attacchi informatici.
- **Analizzare i rischi specifici** per ciascun sottosettore, evidenziando vulnerabilità peculiari e scenari di rischio emergenti.
- **Esaminare il quadro normativo** attuale, con particolare riferimento alla Direttiva NIS2 e al suo recepimento in Italia.
- **Valutare lo stato degli investimenti** in cybersecurity nel settore GDO, identificando gap e opportunità.
- **Fornire raccomandazioni pratiche** per migliorare la resilienza cyber delle organizzazioni del settore.

Il documento intende servire come risorsa strategica per decision maker, responsabili della sicurezza e professionisti del settore GDO, offrendo una base informativa solida per orientare strategie di investimento e prioritizzazione degli interventi di sicurezza.

## Metodologia

La ricerca si fonda su un approccio multi-fonte che integra l'analisi critica di dati quantitativi e qualitativi. Un elemento distintivo della metodologia è l'incorporazione dell'esperienza operativa e delle evidenze raccolte dalla Business Unit Cyber di **Maticmind,** attraverso le sue strutture dedicate (Offensive Team, Cyber Defence Center, **Twin4Cyber**, Cyber Threat Intelligence Team, Incident Response

Management Team), che forniscono un riscontro diretto dal campo sul monitoraggio avanzato delle minacce, sulla verifica proattiva della sicurezza e sulla gestione degli incidenti reali. I dati quantitativi sono stati analizzati per identificare trend e correlazioni, mentre le informazioni qualitative hanno arricchito il contesto.

Il processo metodologico ha seguito queste fasi principali:

- **Raccolta dati: i**ntegrazione di fonti primarie (esperienza operativa Maticmind) e secondarie (report di ricerca, pubblicazioni accademiche, white paper di vendor, bollettini di sicurezza)
- **Validazione con esperti:** verifica dei risultati preliminari con specialisti di cybersecurity del settore GDO
- **Sintesi e visualizzazione:** elaborazione di grafici e infografiche per rappresentare efficacemente trend e correlazioni
- **Formulazione di raccomandazioni:** sviluppo di linee guida basate su evidenze empiriche e best practice

Le fonti principali includono articoli e report di organizzazioni primarie e riconosciute integrati con dati e con l'esperienza operative dirette del **team Cyber Maticmind.**

Nel report abbiamo adottato una nomenclatura internazionale, che segue le classificazioni comunemente utilizzate nei contesti di threat intelligence e nei principali report globali (es. "retail & grocery", "food distribution", "FMCG supply chain"). Questo approccio include, oltre ai supermercati, anche aziende della logistica, della produzione alimentare, del retail non alimentare ma adiacente, e relativi fornitori.

## Considerazioni

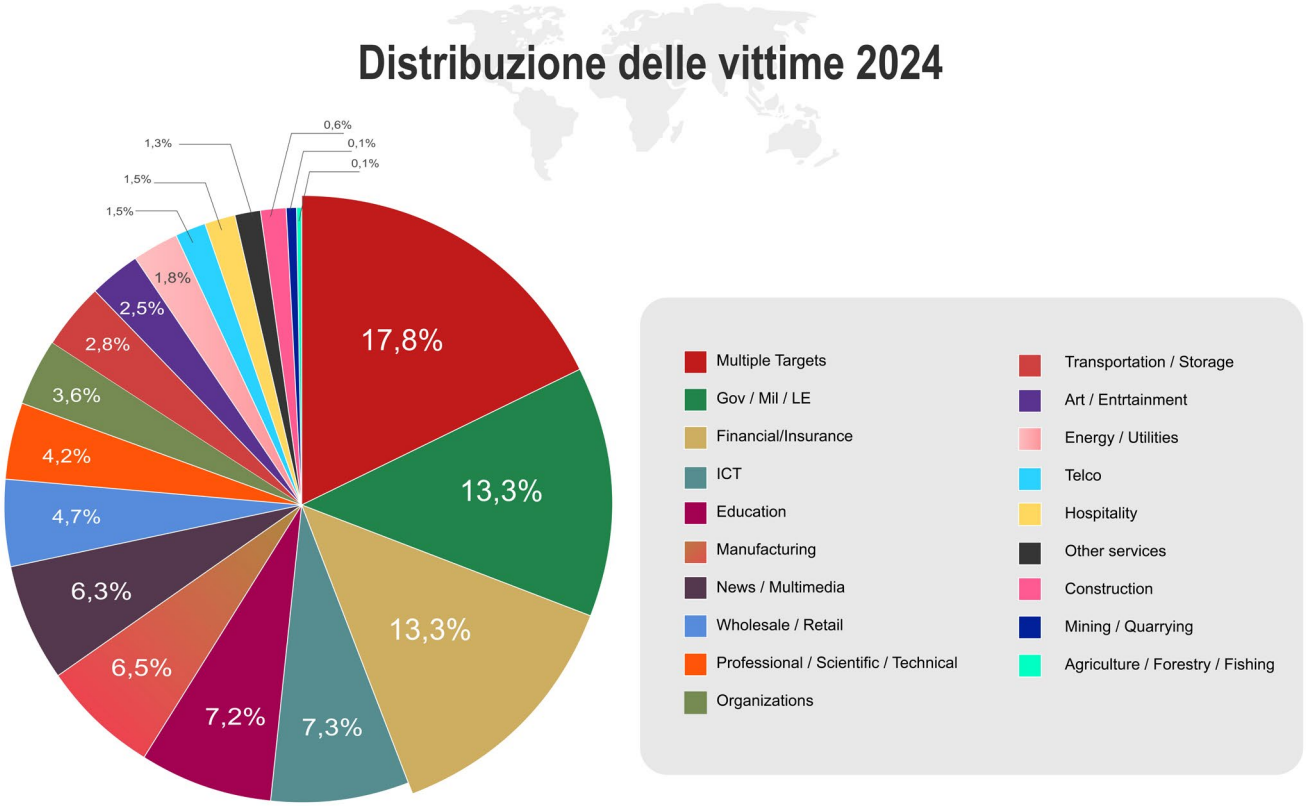
Nell'interpretazione dei risultati presentati in questo report, è importante considerare alcuni fattori contestuali:

- **Underreporting:** I dati sugli incidenti cyber rappresentano solo gli attacchi noti e segnalati, con una probabile sottostima del fenomeno reale.
- **Evoluzione rapida delle minacce:** Il panorama delle minacce cyber è in costante evoluzione, con nuove tecniche e tattiche che emergono continuamente.
- **Contesto geopolitico:** Molti attacchi al settore GDO hanno possibili motivazioni geopolitiche, rendendo il panorama delle minacce sensibile a tensioni internazionali.
- **Impatto della regolamentazione:** L'implementazione della Direttiva NIS2 sta modificando significativamente l'approccio alla cybersecurity nel settore.

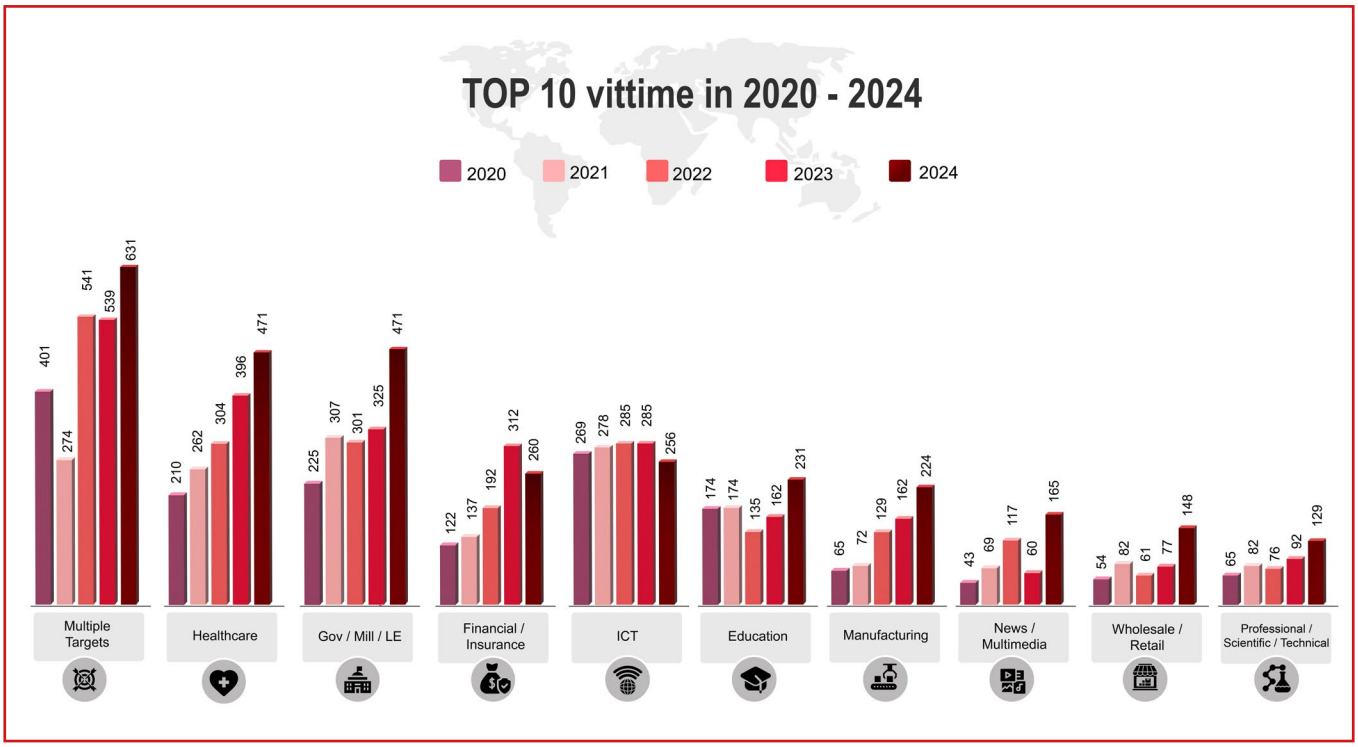
Questo report offre una fotografia del panorama attuale, ma deve essere interpretato come parte di un processo continuo di monitoraggio e adattamento alle minacce in evoluzione.

# Worldwide

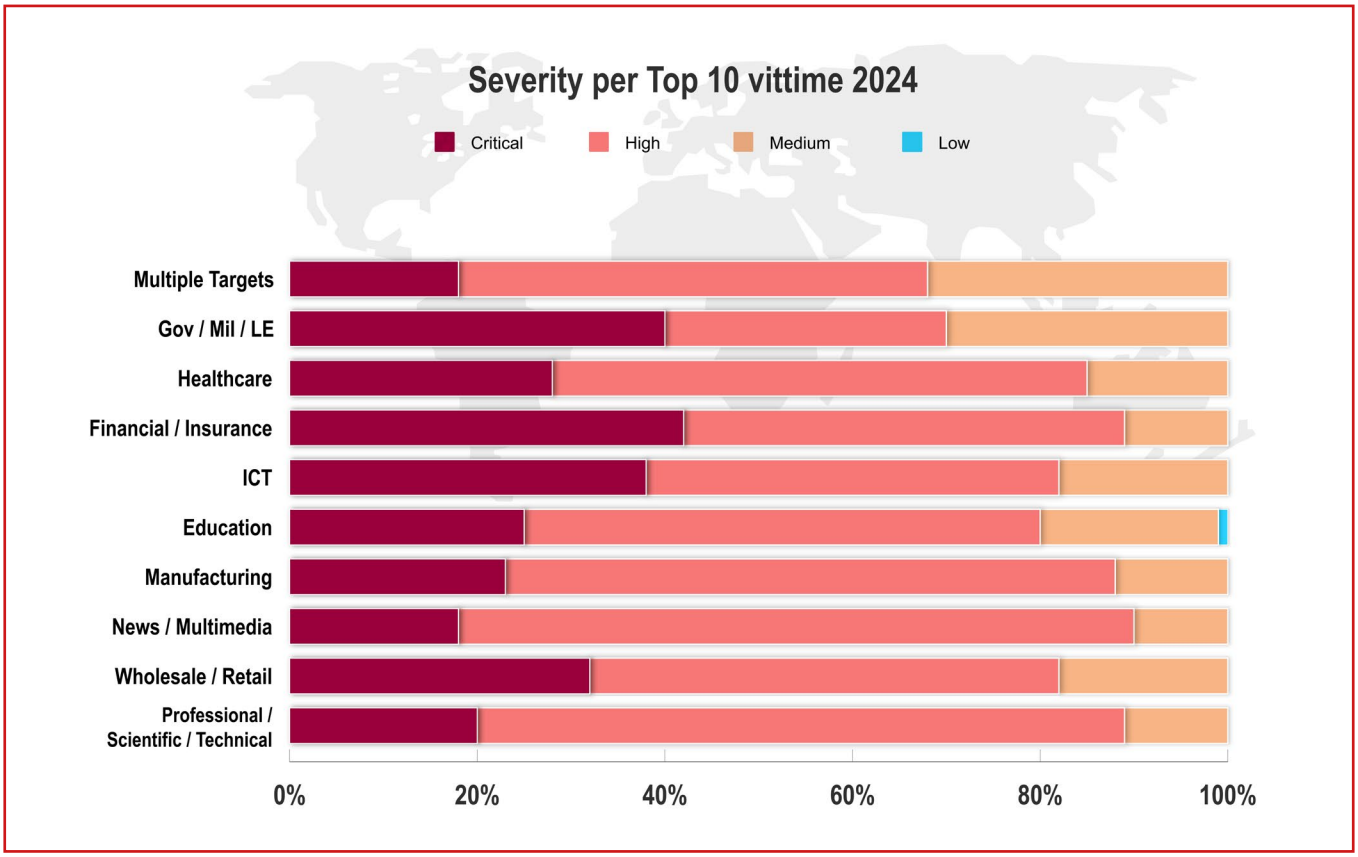
Il grafico illustra la distribuzione percentuale delle vittime di attacchi informatici a livello globale nel 2024 per settore industriale. Il settore Wholesale/Retail si colloca al 9° posto con il 4,2% delle vittime, ben distanziato dai settori più colpiti come Multiple Targets (17,8%), Gov/Mil/LE e Healthcare (entrambi 13,3%).




L'analisi dell'evoluzione quinquennale degli attacchi mostra per il settore retail un trend di crescita allarmante: il numero di vittime è aumentato da 54 nel 2020 a 148 nel 2024, con un incremento del 174%. L'accelerazione è particolarmente marcata negli ultimi due anni, con un aumento del 92% tra il 2023 (77) e il 2024 (148).

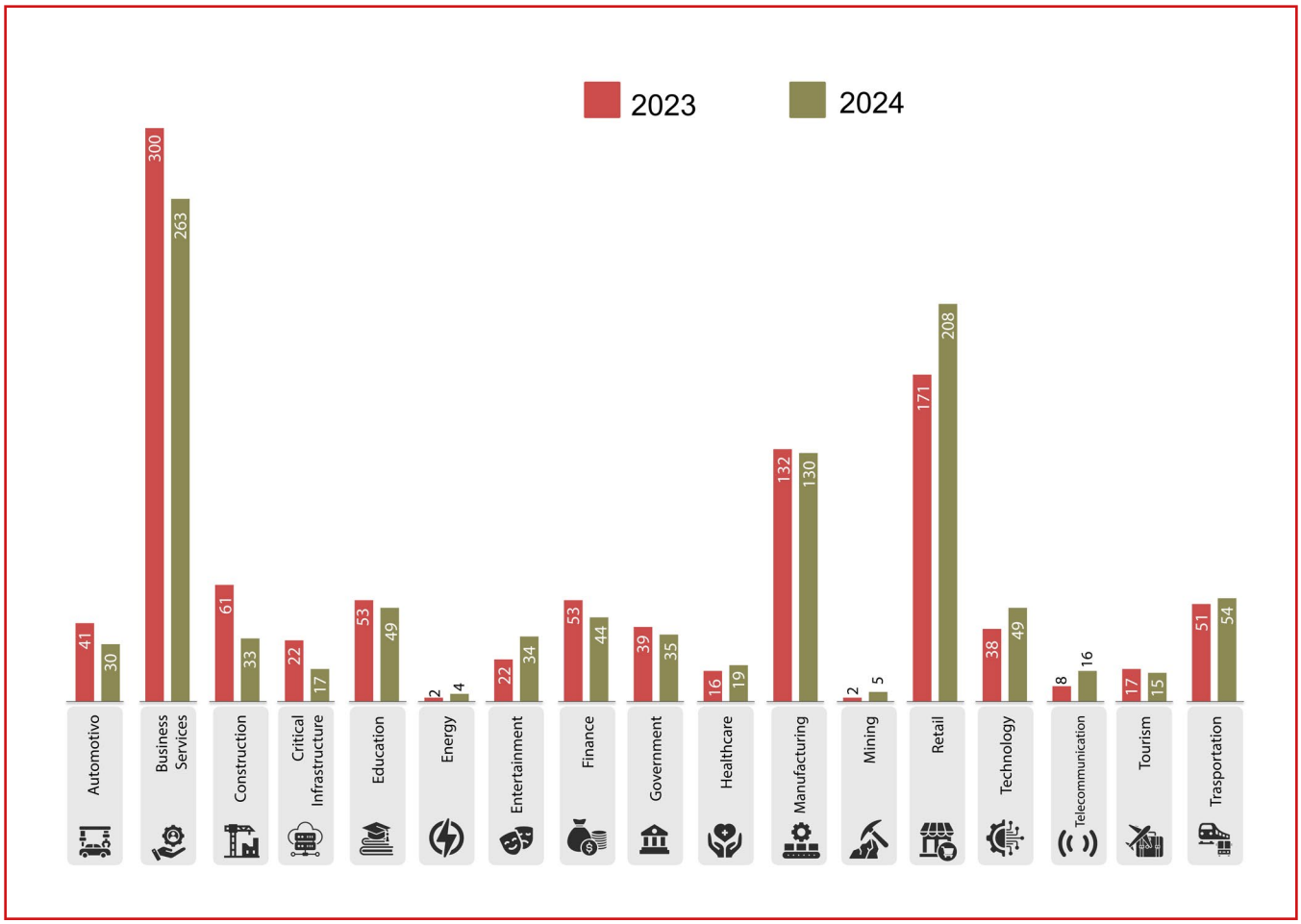



Un'analisi della dimensione qualitativa della minaccia illustra la distribuzione della severità degli attacchi nei dieci settori più colpiti: per il settore Wholesale/Retail, emerge un profilo caratterizzato da una percentuale del circa 30% di attacchi critici e da un'elevata incidenza di attacchi di media severità (circa 50-55%).



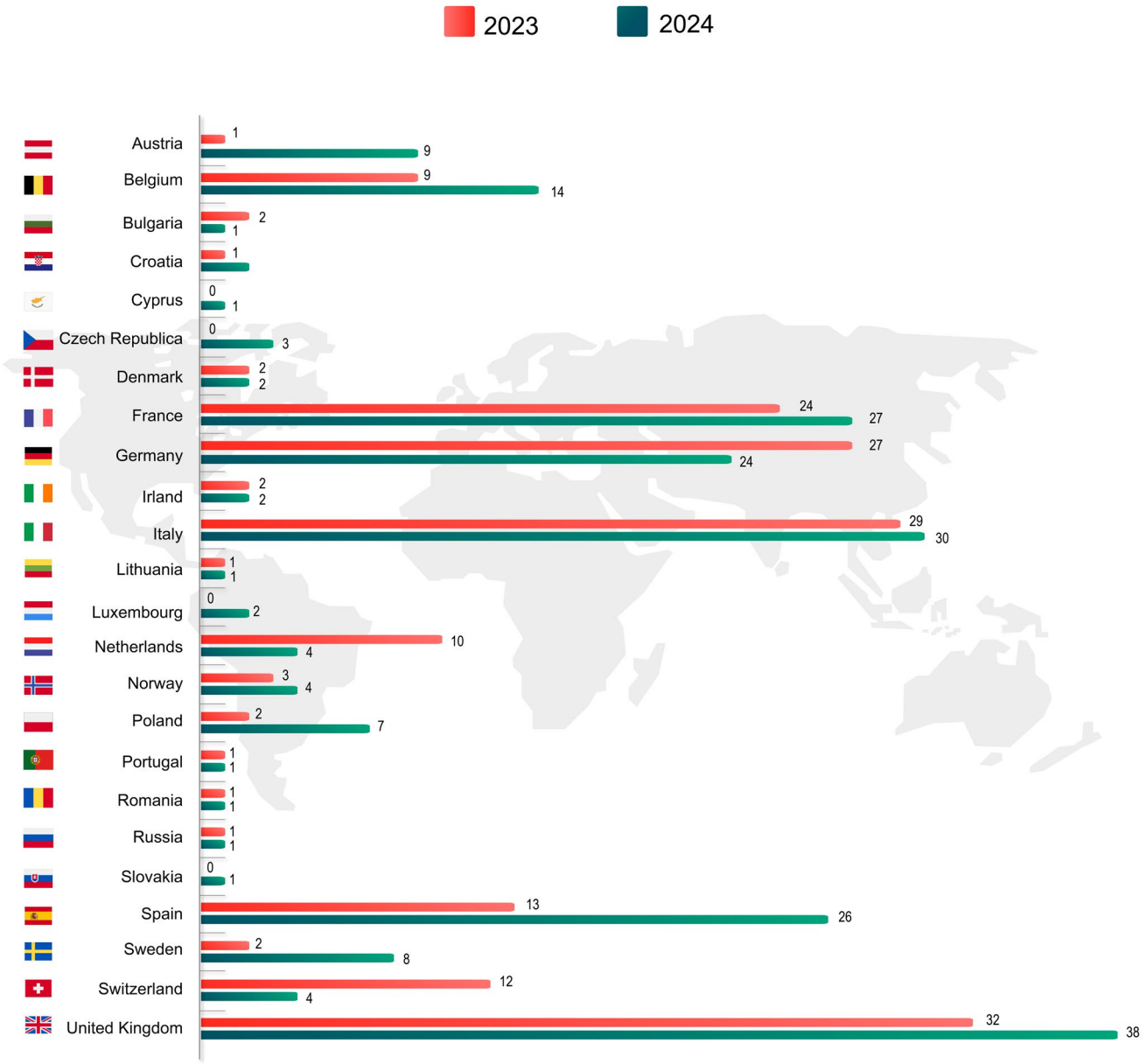
# Europa

Il ransomware si conferma la minaccia più grave per il settore retail nel 2024, con un incremento significativo degli attacchi su scala globale. Si stima un aumento di circa **+20–22%** degli incidenti ransomware rivolti alla GDO rispetto all'anno precedente. Questa crescita è trainata sia dall'intensificarsi delle operazioni delle cyber gang note, sia dall'emergere di nuovi gruppi criminali. In particolare, sono emersi nuovi operatori aggressivi come RansomHub e Hunters International, decisi a farsi un nome colpendo imprese di grandi dimensioni. Allo stesso tempo, l'attività di alcune delle gang "storiche" è temporaneamente calata per via di interventi di law enforcement: ad esempio, operazioni internazionali (es. Operation Cronos di Europol) hanno preso di mira la rete di LockBit e di BlackCat/ALPHV, influenzandone le capacità nel 2023-24. Ciò non ha però eliminato il pericolo: gruppi come LockBit 3.0, BlackBasta, Akira, Clop e altri Ransomware-as-a-Service restano attivi e hanno colpito svariate aziende retail nel 2024 (con LockBit ancora tra le varianti più diffuse, nonostante gli arresti di affiliati).



## Distribuzione geografica

Le campagne ransomware contro la GDO hanno colpito prevalentemente le economie maggiori. In **Europa**, i 5 **Paesi più bersagliati** nel 2024 sono stati Francia, Germania, Italia, Spagna e Regno Unito, che da soli rappresentano oltre **67%** degli incidenti ransomware nel retail europeo. Si notano picchi di crescita in particolare in **Spagna** (+100% di casi rispetto al 2023) e nel **Regno Unito** (+20%).



## Vettori di infezione

Le tecniche di intrusione ransomware si fanno sempre più mirate. Nella GDO, l'abuso di **credenziali compromesse** è stato il principale vettore iniziale (presente nel **43%** degli incidenti esaminati), seguito da **phishing** (29%) e dallo sfruttamento di vulnerabilità su applicazioni esposte (29%). In pratica, molte intrusioni iniziano con il furto di account validi (es. credenziali di accesso a sistemi aziendali), spesso tramite **phishing** mirati o infostealer, oppure tramite l'exploit di software non aggiornati esposti su internet. Tra i metodi osservati figurano ad esempio email di **phishing** ben congegnate (es. finte comunicazioni aziendali o offerte commerciali contenenti link/file malevoli), download di **software contraffatti/pirata** (armati di malware) e attacchi mirati a utenti con privilegi elevati (supply chain manager, amministratori IT, ecc.)

## Dati e impatti

Il ransomware nel settore GDO causa sia d**anni economici diretti** (costo di ripristino dei sistemi, mancati incassi dovuti a interruzioni operative) sia **impatti reputazionali** (perdita di fiducia dei clienti e partner, specialmente se vengono sottratti dati personali o finanziari). Molte aziende retail gestiscono infatti enormi moli di dati di pagamento e fidelizzazione; una crittografia o esfiltrazione di questi dati può paralizzare le attività (negozi offline impossibilitati a vendere, e-commerce fuori uso) e creare rischi per i consumatori.

## Tasso di pagamento del riscatto

Fortunatamente, le aziende tendono sempre meno a cedere alle richieste estorsive. Nel **Q1 2024 solo il 28%** delle vittime a livello globale ha pagato un riscatto, minimo storico. Questo dato (in calo dal 34% circa di inizio 2023) riflette **maggior resilienza** e preparazione: molte organizzazioni dispongono di backup efficaci e piani di disaster recovery testati, che permettono di ripristinare i dati senza pagare. Al contempo, tuttavia, gli attaccanti puntano a bersagli più grandi e richieste più esose: nel 2024 si è registrato il più alto riscatto singolo noto, ben **75 milioni di dollari** pagati dal distributore farmaceutico Cencora (USA) al gruppo Dark Angels. Questo caso dimostra che, sebbene la percentuale di pagamento sia in calo, la **somma totale estorta** dai ransomware rimane elevata perché i cybercriminali colpiscono più organizzazioni e chiedono cifre maggiori

## Furto di dati e credenziali

Nel 2024, il settore retail in Europa ha confermato la propria esposizione crescente a minacce malware, coerentemente con la progressiva digitalizzazione del canale di vendita. La superficie d'attacco si è ampliata in modo significativo, rendendo il settore un bersaglio privilegiato per campagne di infezione basate su vettori sofisticati e spesso difficili da rilevare.

Le tecniche osservate mostrano un chiaro spostamento verso l'abuso di piattaforme legittime e considerate affidabili dai sistemi di difesa per la diffusione di payload malevoli.

Le infezioni avvengono prevalentemente tramite:

- **Email di phishing**
- **Download di software contraffatti**
- **Attacchi mirati su utenti con privilegi elevati**

Nel 2024, i paesi europei più colpiti da infostealer sono stati:

| Paese | Infezioni stimate |
|---|---|
| **Spagna** | 232 |
| **Germania** | 232 |
| **Regno Unito** | 221 |
| **Francia** | 202 |
| **Italia** | 134 |
| **Polonia** | 141 |

Il panorama dei malware infostealer risulta frammentato ma dominato da pochi attori principali. La distribuzione in Europa nel 2024 è la seguente:

| Malware | Percentuale |
|---|---|
| **Redline** | 35% |
| **Lumma** | 34% |
| **Stealc** | 15% |
| **Aurora** | 8% |
| **Meta** | 6% |
| **Altri** | 2% |

L'elevato utilizzo di Redline e Lumma dimostra una preferenza da parte degli attaccanti per strumenti che combinano capacità di esfiltrazione rapida e facilità di distribuzione, spesso offerti in modalità Malware-as-a-Service.

Il **phishing** rimane uno dei vettori d'attacco più insidiosi per il settore retail, sfruttato sia per compromettere i sistemi interni sia per colpire i clienti dei brand. Nel 2024 i criminali hanno affinato queste tecniche, creando email e messaggi sempre più convincenti e brand impersonation sofisticate.

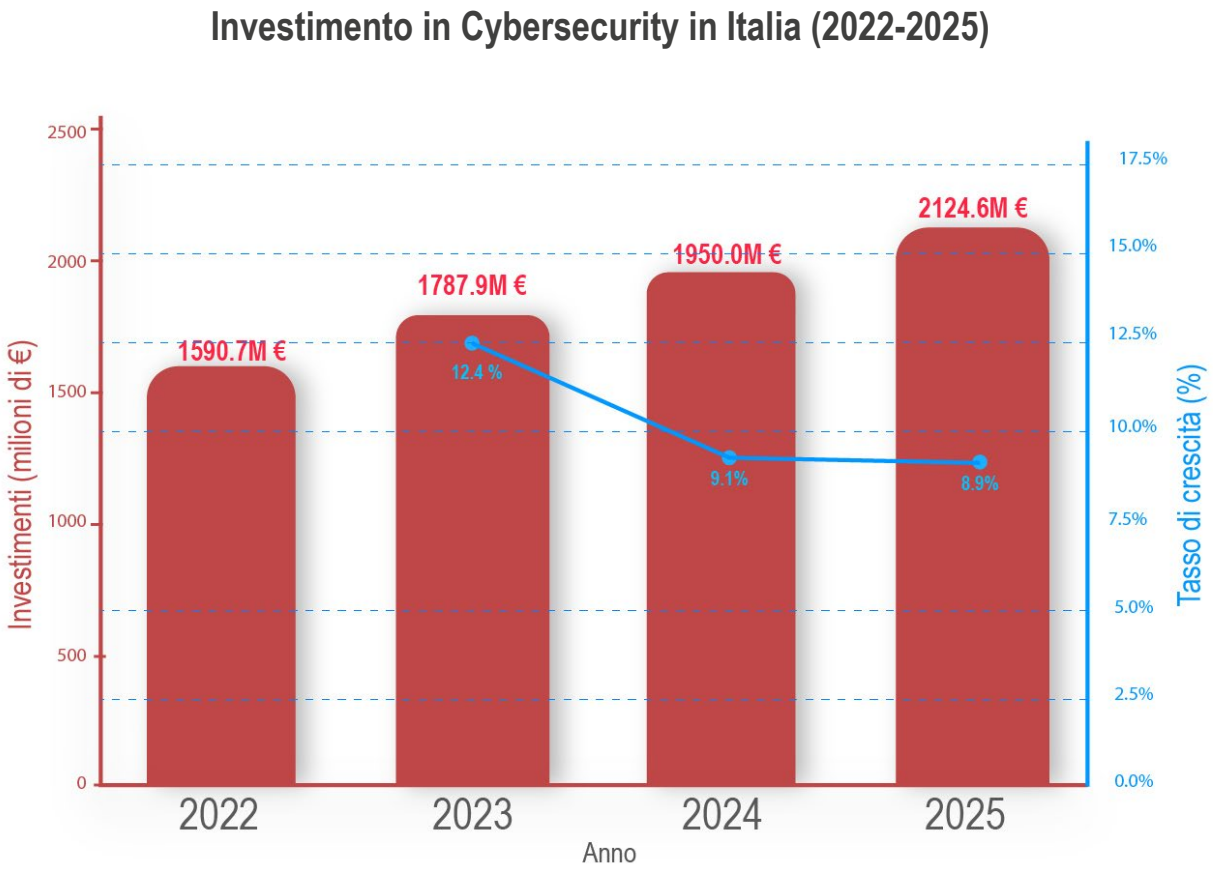
Tra le **tattiche emerse nel 2024** figurano: l'uso di **QR code malevoli** inseriti nelle email (per aggirare i filtri di sicurezza e portare l'utente su pagine phishing quando scansiona il codice); siti di phishing che **bypassano l'autenticazione a due fattori** (inducendo l'utente a inserire anche i codici OTP, subito intercettati dall'attaccante); e campagne via **SMS (smishing)** o social media che imitano comunicazioni di note catene durante periodi critici.

La **supply chain** del settore GDO è altamente interconnessa: i retailer dipendono da fornitori di prodotti, di servizi logistici, di software gestionali e di punti cassa, creando un ecosistema complesso. I cybercriminali ne sono consapevoli e sempre più spesso colpiscono **anelli deboli della catena** per propagare l'attacco ai distributori finali. Nel 2024, gli attacchi indiretti tramite terze parti hanno avuto un ruolo importante: secondo un'indagine globale, ben il **62% delle organizzazioni colpite da ransomware** ha riferito che l'infezione era originata da un partner o fornitore di software compromesso. In altre parole, *quasi 2 attacchi ransomware su 3* hanno sfruttato vulnerabilità nella supply chain digitale – ad esempio exploit di software di terze parti usati dal retailer, accesso attraverso credenziali di fornitori esterni, o malware introdotto via aggiornamenti compromessi.

# Italia

## Panorama degli investimenti in Italia

Secondo il rapporto “Il Digitale in Italia 2024” di Anitec-Assinform, gli investimenti in cybersecurity in Italia hanno mostrato una crescita costante negli ultimi anni, raggiungendo 1.787,9 milioni di euro nel 2023, con un incremento del 12,4% rispetto al 2022. Questa tendenza positiva è proseguita nel 2024, con investimenti stimati a 1.950 milioni di euro (+9,1%), e si prevede che raggiungerà i 2.124,6 milioni di euro entro il 2025 (+8,9%).

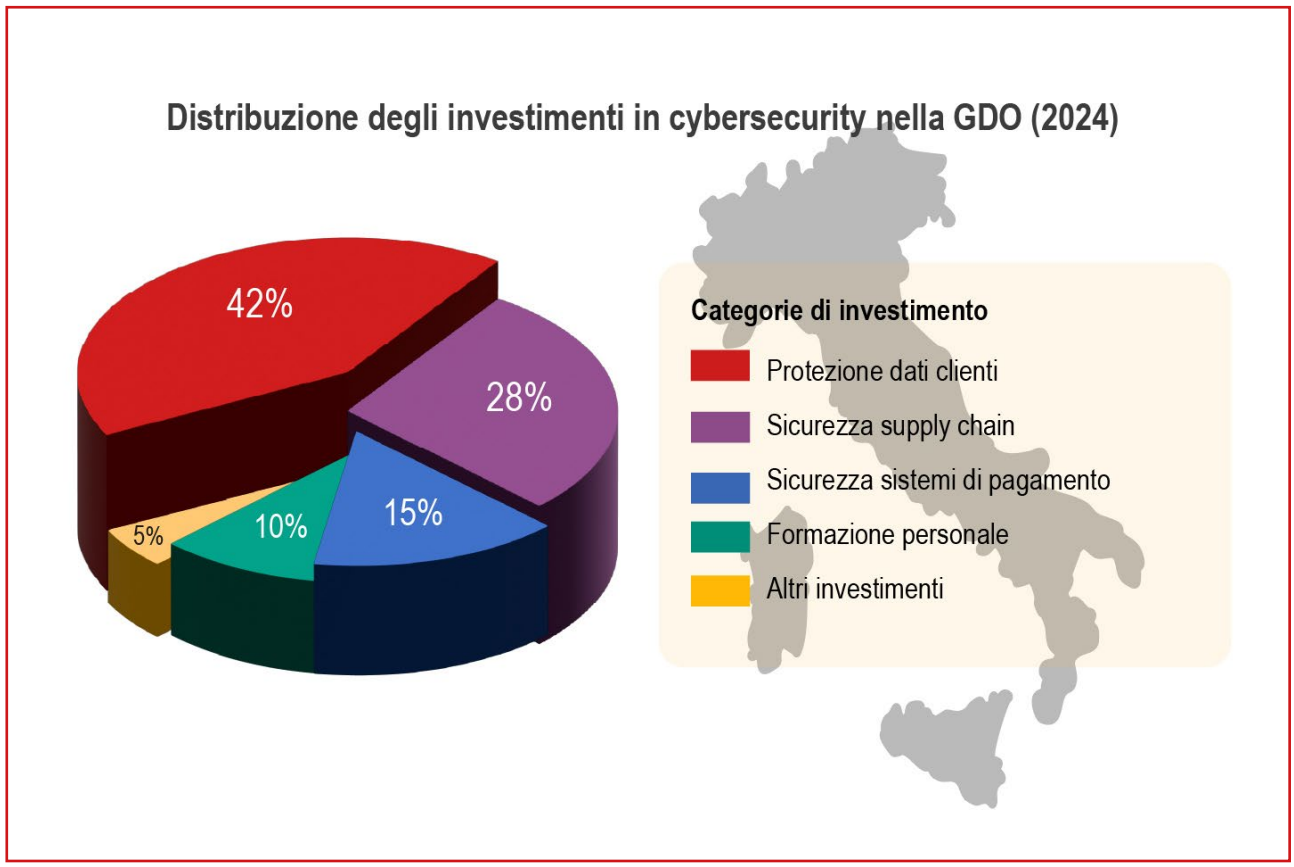



Questo trend di crescita, seppur in leggero rallentamento percentuale rispetto al picco del 2023, dimostra una crescente consapevolezza dell’importanza della sicurezza informatica nel panorama aziendale italiano. Tuttavia, è importante notare che, nonostante l’aumento degli investimenti, l’Italia rimane ancora al di sotto della media europea in termini di spesa pro capite in cybersecurity.

## Investimenti specifici nel settore GDO

Il settore Retail/GDO rappresenta circa il 7,8% degli investimenti totali in cybersecurity in Italia nel 2024, per un valore di circa 152 milioni di euro. Si prevede un aumento degli investimenti nel settore del 14,2% nel 2025 rispetto al 2024, superando la media di crescita nazionale.

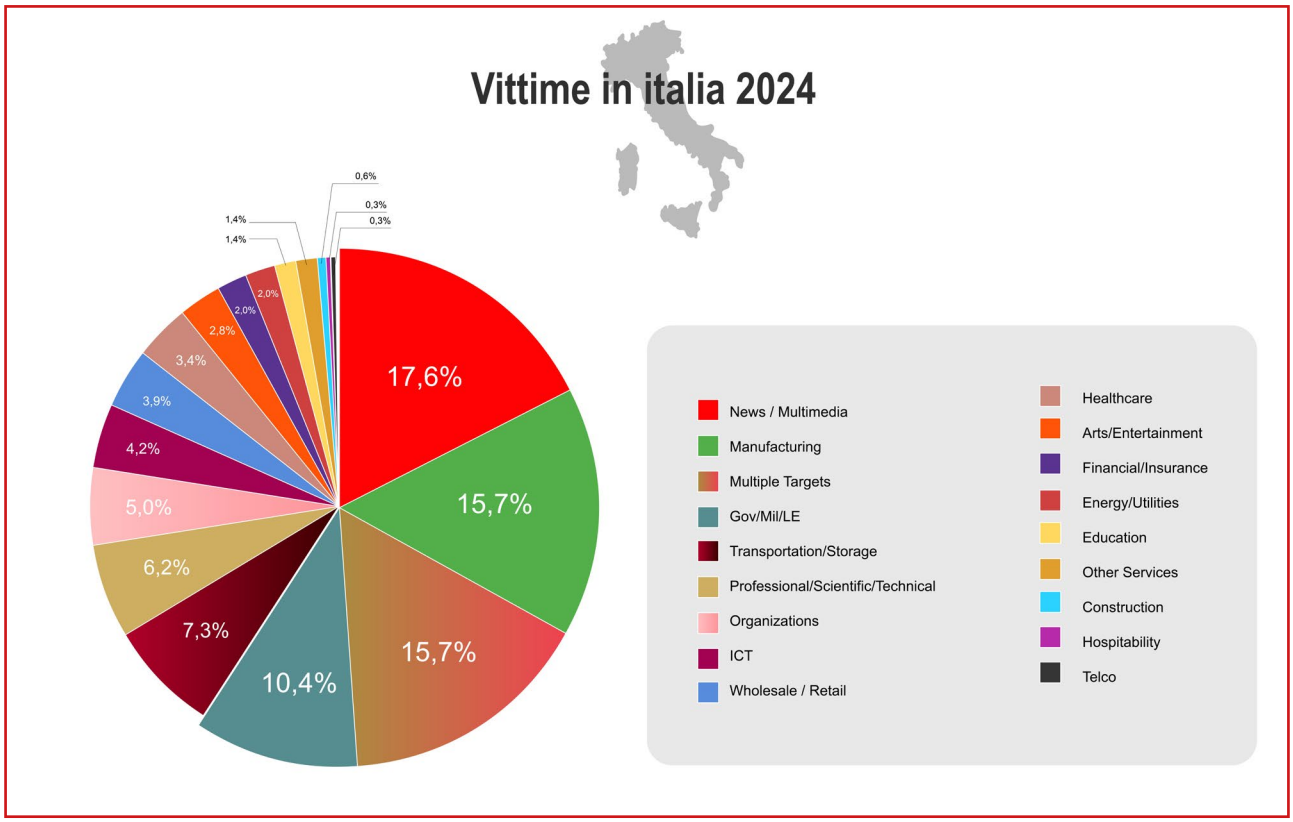
La distribuzione degli investimenti in cybersecurity nella GDO nel 2024 mostra una chiara prioritizzazione della protezione dei dati dei clienti, che rappresenta il 42% del totale, seguita dalla sicurezza della supply chain (28%), dalla sicurezza dei sistemi di pagamento (15%), dalla formazione del personale (10%) e da altri investimenti (5%).

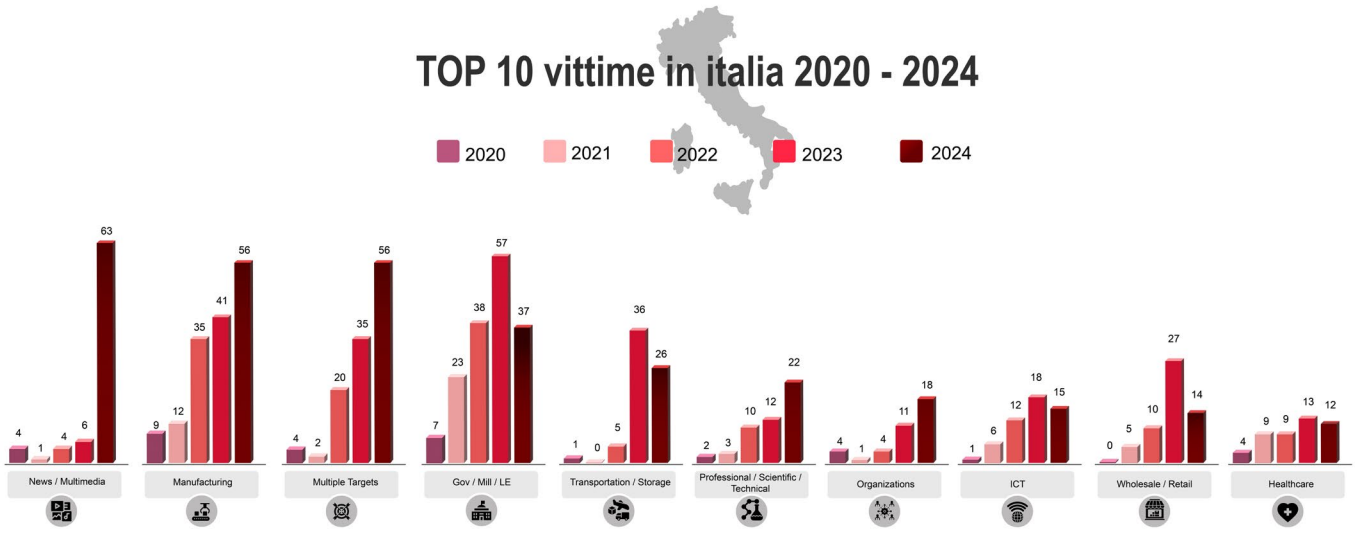



Anche in Italia il settore della grande distribuzione si trova infatti ad affrontare minacce cyber in aumento. Il settore Wholesale/Retail si posiziona al 9° posto con il 3,9% delle vittime, leggermente al di sotto del dato globale (4,2%).

Nel contesto italiano, i settori più colpiti sono News/Multimedia (17,6%), Manufacturing e Multiple Targets (entrambi al 15,7%), seguiti da Gov/Mil/LE (15,4%). Questa distribuzione diverge notevolmente dal quadro internazionale, con una vulnerabilità particolarmente marcata del comparto manifatturiero, che in Italia registra un'incidenza più che doppia rispetto al dato mondiale.

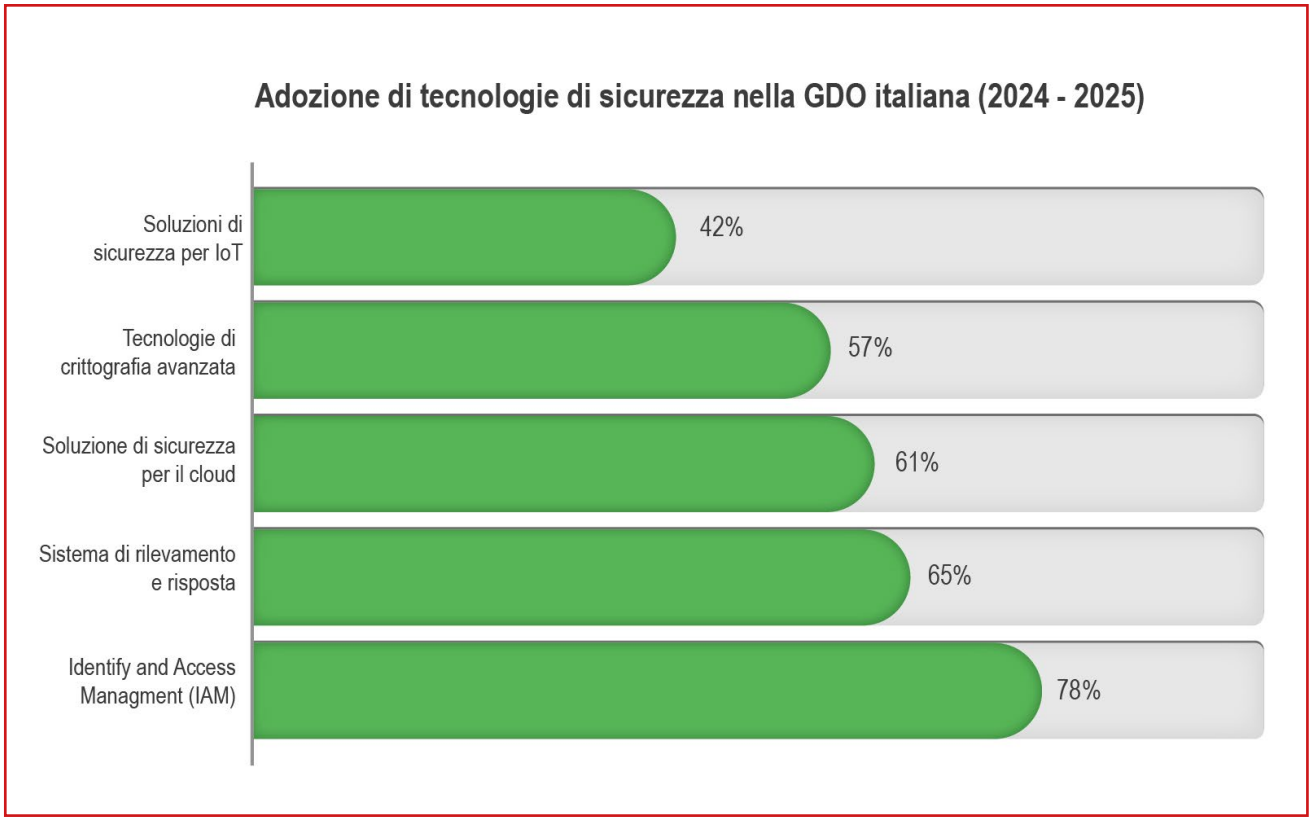
Negli ultimi cinque anni, il settore retail in Italia ha mostrato un’evoluzione preoccupante in termini di attacchi informatici.



## Furto di dati e credenziali

L'analisi dell'adozione di tecnologie di sicurezza nella GDO italiana nel biennio 2024-2025 mostra una diffusione significativa delle soluzioni di Identity and Access Management (IAM), adottate dal 78% delle aziende del settore. Seguono i sistemi di rilevamento e risposta agli incidenti (65%), le soluzioni di sicurezza per il cloud (61%), le tecnologie di crittografia avanzata (57%) e le soluzioni di sicurezza per IoT (42%).




Questa distribuzione riflette le priorità del settore in termini di protezione degli accessi e gestione delle identità, un aspetto cruciale considerando l'elevato numero di dipendenti e fornitori che interagiscono con i sistemi informatici della GDO. La crescente adozione di soluzioni cloud e IoT evidenzia inoltre la progressiva digitalizzazione del settore, con la conseguente necessità di proteggere adeguatamente questi nuovi ambienti tecnologici.

# Danni e impatti economici degli attacchi cyber nella GDO

## Costi generali dei data breach in Italia

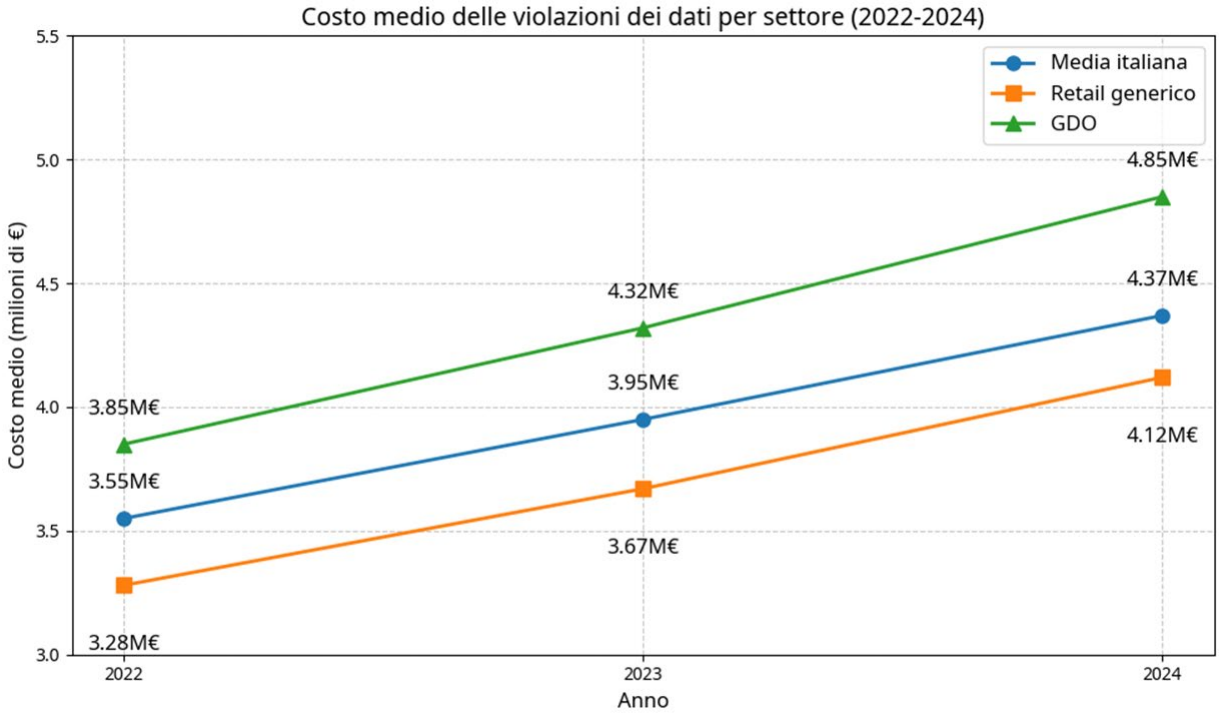
Secondo il Cost of Data Breach Report 2024 di IBM, l'impatto economico degli attacchi informatici in Italia ha raggiunto livelli preoccupanti:

- Il costo medio di un data breach in Italia è di 4,37 milioni di euro nel 2024
- Si registra un aumento del 23% rispetto al 2023
- L'Italia è tra i paesi con i costi più alti a livello mondiale

Questi dati collocano l'Italia tra i Paesi con il maggior impatto economico dovuto agli attacchi informatici, evidenziando la crescente vulnerabilità delle aziende italiane nell'ambito della protezione dei dati.

## Costo medio delle violazioni dei dati per settore

L'analisi del costo medio delle violazioni dei dati per settore nel triennio 2022-2024 mostra un trend di crescita costante per tutti i settori, con la GDO che presenta i costi più elevati rispetto alla media italiana e al retail generico.



Nel 2024, il costo medio di una violazione dei dati nel settore retail in Italia è stato di 4,12 milioni di euro, mentre per la GDO, considerando la complessità della supply chain e la gestione di prodotti deperibili, questo costo è salito a 4,85 milioni di euro. Questi valori sono significativamente superiori alla media italiana di 4,37 milioni di euro, evidenziando la particolare vulnerabilità del settore.

## Fattori che influenzano il costo di un data breach

Il costo di una violazione dei dati non dipende solo dalla quantità di informazioni compromesse, ma da una serie di fattori chiave:

- **Tempo di rilevamento e contenimento:** In media in Italia occorrono 218 giorni per identificare e mitigare una violazione. Più di tre quarti delle aziende che sono riuscite a riprendersi completamente da una violazione hanno impiegato oltre 100 giorni, con il 35% che ha richiesto più di 150 giorni per il ripristino completo.
- **Tipo di attacco subito:** Gli attacchi basati su ingegneria sociale in Italia hanno un costo medio di 4,78 milioni di euro per violazione. Il phishing, che rappresenta il 17% degli attacchi, ha un costo medio di 4,18 milioni di euro. Gli attacchi ransomware hanno rappresentato il 35% degli incidenti informatici nel 2023.
- **Informazioni compromesse:** Il 46% delle violazioni ha riguardato dati personali dei clienti, mentre il 43% ha coinvolto dati di proprietà intellettuale. Il costo per record violato è passato da 156 a 173 dollari per unità.
- **Ambiente IT coinvolto:** I data breach che interessano dati archiviati su cloud pubblico sono i più costosi, con una media di 5,17 milioni di dollari per violazione.

## Impatti specifici per il settore GDO

- **Interruzione della catena di approvvigionamento:** Un attacco può causare il blocco dei sistemi di gestione della logistica, l'impossibilità di tracciare le merci e gestire gli ordini, con il rischio di deterioramento dei prodotti deperibili.
- **Compromissione dei dati dei clienti:** Il furto di dati delle carte di credito e informazioni personali dei clienti può portare a una perdita di fiducia da parte dei consumatori e a danni reputazionali significativi.
- **Impatto sui sistemi di pagamento:** Il blocco dei sistemi POS e delle casse può rendere impossibile processare pagamenti elettronici, costringendo a tornare temporaneamente a sistemi manuali con conseguente rallentamento delle operazioni.
- **Effetti sulla supply chain:** Secondo il World Economic Forum (gennaio 2025), il 54% delle grandi organizzazioni vede le sfide legate alla supply chain come il principale ostacolo alla resilienza. La GDO, essendo al centro di una complessa rete di fornitori, è particolarmente esposta a questo rischio.

# Rischi specifici per il settore GDO in ambito cybersecurity

## Vulnerabilità strutturali del settore GDO

La Grande Distribuzione Organizzata presenta alcune vulnerabilità strutturali che la rendono particolarmente esposta agli attacchi informatici:

1. **Complessità della supply chain:** La GDO si caratterizza per una catena di approvvigionamento particolarmente articolata e complessa. Come evidenziato dalla direttiva NIS2 (FreshPlaza, giugno 2024), un attacco alla rete informatica di un singolo fornitore può incidere in pochi minuti su un'intera organizzazione o catena di fornitura. Le PMI della filiera sono spesso bersaglio di attacchi informatici a causa delle loro misure di gestione dei rischi meno rigorose, e la GDO dovrà verificare che i propri fornitori siano in regola con la cybersecurity, aumentando la complessità gestionale.
2. **Gestione di prodotti deperibili:** A differenza di altri settori retail, la GDO presenta un'ulteriore criticità legata alla natura dei prodotti venduti. I prodotti alimentari devono soddisfare determinati standard igienici e di conservazione (Cybersecitalia, gennaio 2025), e un'interruzione dei sistemi informatici può compromettere la catena del freddo o la gestione delle scadenze, con potenziali rischi per la salute pubblica in caso di compromissione dei sistemi di tracciabilità e controllo qualità.
3. **Elevata dipendenza dai sistemi informatici:** La moderna GDO dipende in modo critico dai sistemi informatici per tutte le operazioni quotidiane, dalla gestione logistica all'elaborazione di fatture e ordini, dai sistemi di pagamento alla gestione del magazzino.

## Rischi specifici emergenti (2024-2025)

Nel biennio 2024-2025 sono emersi alcuni rischi specifici per il settore GDO:

- **Attacchi ransomware con doppia estorsione:** gli attacchi ransomware al settore GDO stanno evolvendo verso un modello di doppia estorsione, con crittografia dei dati e esfiltrazione preliminare di dati sensibili, seguita da una doppia richiesta di riscatto sia per sbloccare i sistemi sia per non pubblicare i dati sottratti.
- **Compromissione della catena di approvvigionamento digitale:** secondo il World Economic Forum (gennaio 2025), il 54% delle grandi organizzazioni vede le sfide legate alla supply chain come il principale ostacolo alla resilienza. Gli attacchi possono avvenire attraverso la compromissione di aggiornamenti software utilizzati nella GDO, l'infiltrazione attraverso terze parti con minori protezioni o la manipolazione dei dati di approvvigionamento.

- **Phishing mirato al personale GDO:** Le campagne di phishing contro il settore GDO stanno diventando sempre più sofisticate, sfruttando periodi critici come le festività, impersonificando marchi noti e prendendo di mira i responsabili acquisti.
- **Attacchi ai sistemi di pagamento:** Il settore retail è particolarmente esposto a pericoli informatici legati ai sistemi di pagamento, come lo skimming digitale, la compromissione dei POS e le frodi con carte di credito.
- **Attacchi DDoS ai servizi online:** Con l'aumento dell'e-commerce nel settore GDO, cresce il rischio di attacchi DDoS che possono interrompere i servizi di vendita online, causare perdite economiche dirette e danneggiare la reputazione dell'azienda.

# Il contesto normativo: la direttiva NIS2

Da ottobre 2024, in tutta l'Unione europea è entrata in vigore la **direttiva NIS2** (Network and Information Security Directive 2), una normativa finalizzata a migliorare la sicurezza delle reti e dei sistemi informativi. Come evidenziato da FreshPlaza (giugno 2024), lo scopo principale è proteggere le infrastrutture critiche, comprese quelle del settore alimentare, da attacchi informatici e altre minacce digitali.

La direttiva impone alle imprese di implementare misure adeguate e proporzionate per gestire i rischi relativi alla sicurezza dei sistemi di rete. Sebbene siano escluse le piccole

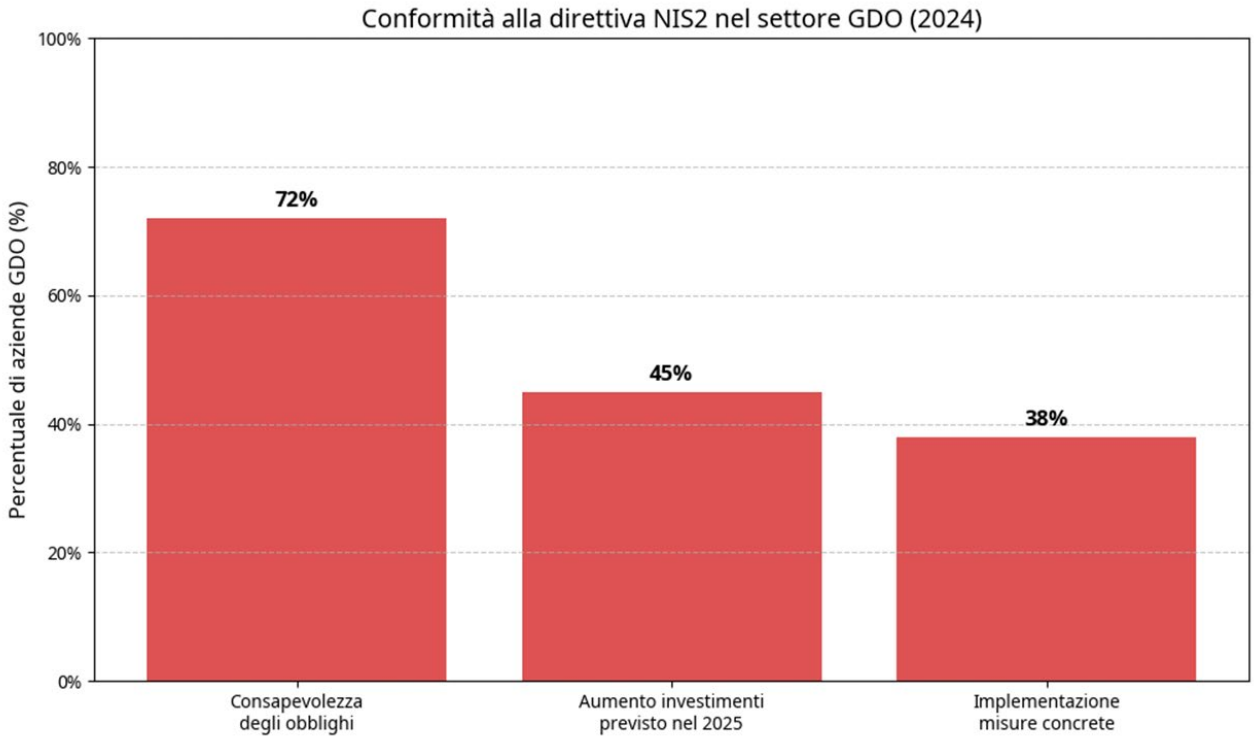
imprese (con meno di 50 dipendenti e un fatturato annuo o un totale di bilancio annuo non superiore a 10 milioni di euro), la Grande Distribuzione Organizzata (GDO) è tra i soggetti obbligati. Questo comporta che anche le piccole imprese della filiera dovranno rivedere i propri aspetti di cybersecurity per essere in regola con le richieste dei clienti della GDO.

Un aspetto significativo della nuova disciplina è che la gestione della sicurezza informatica non è più un compito relegato esclusivamente alla funzione IT, ma diventa una responsabilità diretta dell'organo di gestione aziendale, come ad esempio il Consiglio di amministrazione. Questo cambiamento riflette la crescente consapevolezza che la cybersecurity non è solo una questione tecnica, ma un elemento strategico per la continuità operativa e la reputazione aziendale.

Le violazioni della direttiva NIS2 possono comportare sanzioni amministrative significative: fino a 10 milioni di euro o fino al 2% del totale del fatturato mondiale globale per gli operatori essenziali, e fino a 7 milioni di euro o fino all'1,4% del totale del fatturato mondiale globale per gli operatori importanti.

## Conformità alla direttiva NIS2 nel settore GDO

Nonostante l'importanza della direttiva NIS2, i dati sulla conformità nel settore GDO mostrano un quadro preoccupante. Se da un lato il **72%** delle **aziende GDO** ha dichiarato di essere a conoscenza degli obblighi imposti dalla normativa, solo il **38%** ha effettivamente implementato **misure concrete** per adeguarsi. Il 45% delle aziende prevede di aumentare gli investimenti in cybersecurity nel 2025 specificamente per conformarsi alla direttiva.




Questo divario tra consapevolezza e implementazione rappresenta un rischio significativo per il settore, considerando le potenziali sanzioni e, soprattutto, l'esposizione a minacce cyber in un contesto di crescente digitalizzazione.

# Strategie di mitigazione e best practices

Per affrontare efficacemente le minacce cyber nel settore GDO, è possibile adottare diverse strategie di mitigazione:

**1. Approccio integrato alla cybersecurity**

La sicurezza informatica non deve essere considerata solo un problema tecnico, ma un elemento strategico per la continuità operativa e la reputazione aziendale. Come evidenziato dalla direttiva NIS2, la gestione della sicurezza informatica deve diventare una responsabilità diretta dell'organo di gestione aziendale.

**2. Formazione e sensibilizzazione del personale**

Nell'80% dei casi le prime fasi di un attacco informatico sfruttano principalmente il fattore umano. È quindi essenziale investire nella formazione e nella sensibilizzazione del personale, in particolare per quanto riguarda il riconoscimento di tentativi di phishing e altre tecniche di social engineering.

**3. Verifica della sicurezza della supply chain**

La GDO deve verificare che i propri fornitori siano in regola con la cybersecurity, come richiesto dalla direttiva NIS2. Questo può includere l'inserimento di clausole di sicurezza nei contratti, la richiesta di certificazioni di sicurezza e l'implementazione di procedure di verifica periodica.

**4. Implementazione di soluzioni tecniche avanzate**

L'adozione di soluzioni tecniche avanzate, come sistemi di rilevamento e risposta agli incidenti, backup immutabili, e sistemi di autenticazione a più fattori, può contribuire a ridurre il rischio di attacchi e a mitigarne l'impatto.

**5. Sviluppo di piani di risposta agli incidenti**

La preparazione di piani dettagliati di risposta agli incidenti può ridurre significativamente i tempi di ripristino e, di conseguenza, i costi associati a un attacco. Questi piani dovrebbero includere procedure per l'identificazione, il contenimento, l'eradicazione e il recupero da un incidente, nonché per la comunicazione con le parti interessate.

**6. Collaborazione con le autorità e condivisione delle informazioni**

L'adozione di protocolli d'intesa con i Centri Operativi per la Sicurezza Cibernetica da parte di varie aziende del settore evidenzia come la cooperazione con le autorità competenti e lo scambio di informazioni sulle minacce siano elementi chiave per rafforzare la postura di sicurezza dell'intero comparto della GDO.

# Conclusioni

L’analisi della cybersecurity nel settore GDO per il biennio 2024-2025 evidenzia un panorama in rapida evoluzione, caratterizzato da un aumento significativo degli attacchi informatici e da una crescente sofisticazione delle tecniche utilizzate dai cybercriminali.

La GDO italiana si trova ad affrontare sfide particolarmente complesse, dovute sia alle vulnerabilità strutturali del settore (complessità della supply chain, gestione di prodotti deperibili, elevata dipendenza dai sistemi informatici) sia a fattori di rischio aggravanti specifici del contesto italiano (esposizione sproporzionata agli attacchi cyber, scarsa consapevolezza del rischio, tempi di ripristino prolungati).

La direttiva NIS2, entrata in vigore da ottobre 2024, rappresenta un’importante evoluzione normativa che impone nuovi standard di sicurezza e responsabilità diretta degli organi di gestione aziendale. Sebbene comporti nuovi obblighi e potenziali sanzioni, può essere vista anche come un’opportunità per migliorare la resilienza del settore e promuovere una cultura della sicurezza informatica.

In conclusione, la cybersecurity nel settore GDO non è più solo una questione tecnica, ma un elemento strategico per la continuità operativa, la reputazione aziendale e, in ultima analisi, la competitività sul mercato. Investire nella sicurezza informatica, nella formazione del personale e nella verifica della supply chain non è più un’opzione, ma una necessità imprescindibile per affrontare le sfide del presente e del futuro.

# Cyber Framework Maticmind

### Predittiva – Anticipare

Monitoraggio costante del panorama delle minacce tramite Cyber Threat Intelligence e tecniche OSINT, per identificare rischi emergenti prima che si manifestino.

### Preventiva – Prevenire

Valutazione e gestione del rischio tecnologico, umano, organizzativo e compliance, per rafforzare la postura di sicurezza e ridurre la probabilità di incidenti.

### Progettuale – Costruire Sicuro

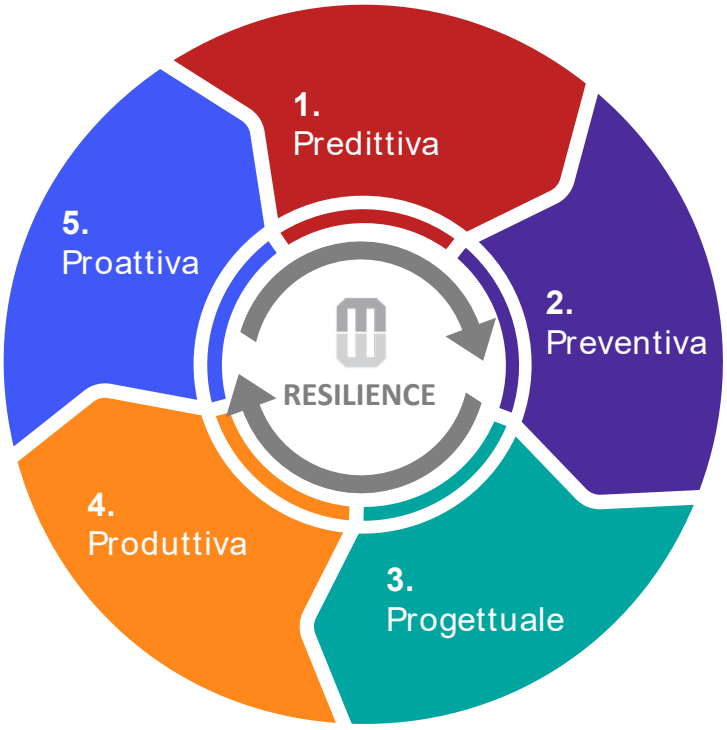
Integrazione della sicurezza nei processi di design e architettura, secondo principi di “secure by design” e “security by resilience”, per garantire sistemi resilienti.

### Produttiva – Implementare Soluzioni

Adozione e gestione di tecnologie di difesa (firewall, EDR, IAM, SIEM) che trasformano le strategie in protezione operativa e misurabile.

### Proattiva – Reagire e Migliorare

Monitoraggio continuo, risposta agli incidenti e analisi forense: la sicurezza come processo dinamico e adattivo, guidato dal miglioramento continuo.



# Una Cyber Acies

## Cinque centri di competenza, un'unica forza cyber

1

Centro strategico per l'analisi e gestione del rischio cyber: governance, compliance, modelli di maturità, supply chain security posture.

- Offensive Security
- Consulting Services (CisoasaService, PM,..)
- Governance, Risk e Compliance
- Social Engineerinf Simulation
- Risk Assessment
- Maturity Model checkup
- Supply Chain Security Posture
- Cyber Academy


2

Continuità operativa e sicurezza in tempo reale assicurata da presidio operativo che integra SOC H24, con le capacità tecniche del TAC e il controllo infrastrutturale del NOC. Garantisce un monitoraggio continuo, una risposta tempestiva agli incidenti e un supporto tecnico evoluto.

- **SOC (Security Operation Center)**
  - SOC H24
  - Cyber Threat Intelligence
  - Malware Analysis
- **SOS (SECURITY OPERATION SERVICES)**
  - Crisis Management
  - IncidentResponse & Digital Forensic Analysis
- **TAC (Technical Assistance Center)**
  - Gestione di ticket e supporto tecnico avanzato
  - Assistenza su soluzioni proprietarie e terze parti
  - Troubleshooting di sicurezza e infrastruttura
  - Supporto su incidenti tecnici e configurazioni complesse
- **NOC (Network Operation Center)**
  - Monitoraggio infrastrutturale H24
  - Supervisione performance di rete, cloud e sistemi
  - Gestione allarmi e segnalazioni
  - Coordinamento tecnico con il SOC in caso di anomalie

3

Esecuzione ed implementazione di progetti complessi di sicurezza: infrastrutture, cloud, OT/IoT, application security e integrazione di soluzioni cyber.

- Infrastructure & Network Security Management
- Cyber Resiliency e Data Protection
- Microsoft, Fortinet & CISCO Competence Center
- Cloud Security By Design
- Application Security SSDLC
- OT & IoT Security Management
- Security System Integration and Monitoring

4

Gestione e integrazione di soluzioni proprietarie e tecnologie di terze parti: piattaforme EDR, firewall, IAM, SIEM, DLP.

- Piattaforma Twin4Cyber
- Cyber Range
- Fortinet/Cisco/Palo Alto
- SIEM/SOAR
- EDR/XDR/NDR
- Identity & Access Management (IAM/PAM)
- NGFW
- Data Loss Prevention

5

Progetti speciali e sperimentazione: architetture avanzate, droni, AI, cyber-physical systems, prototipi e soluzioni non convenzionali.

- Architetture avanzate multi-layer e ibride
- Sistemi di comando e controllo per droni e UAV
- Integrazione AI in contesti cyber e sicurezza industriale
- Progetti su ambienti cyber-physical / smart infrastructure
- Soluzioni sperimentali
- Cyber testbed per ambienti OT e industriali
- Soluzioni cyber per difesa e protezione civile
- Soluzioni sperimentali edge & fog computing.

# Bibliografia

## Fonti primarie

Maticmind – Business Unit Cyber. Evidenze operative e intelligence raccolte tramite le seguenti strutture interne:

- Offensive Security Team
- Cyber Threat Intelligence Team
- Cyber Defence Center (SOC H24)
- Incident Response Management Team
- Twin4Cyber Platform
- Cyber Projects Hub e Innovation Lab

## Fonti secondarie


- Anitec-Assinform (2024). Il Digitale in Italia 2024 – Rapporto sull'evoluzione del digitale nel Paese. Milano: Confindustria Digitale.
- Clusit (2025). Rapporto Clusit sulla Sicurezza ICT in Italia – Edizione 2025. Milano: Associazione Italiana per la Sicurezza Informatica.
- Cybersecitalia (gennaio 2025). Cyberattacchi ai colossi alimentari. I rischi per le aziende della grande distribuzione organizzata. Roma: Cybersecitalia.it.
- ENISA – European Union Agency for Cybersecurity (2024). ENISA Threat Landscape 2024
- Cyberint (2024). Europe Retail Threat Landscape.
- FreshPlaza (giugno 2024). "La GDO dovrà verificare che i propri fornitori siano in regola con la cybersecurity". Articolo online.
- IBM Security (2024). Cost of a Data Breach Report 2024: Understanding the Financial Impact of Cybersecurity Incidents.
- World Economic Forum (gennaio 2025). Global Cybersecurity Outlook 2025: Building Resilience in a Fragmented World.

# Disclaimer

Il presente report è stato elaborato utilizzando esclusivamente fonti di informazioni open source (OSINT) e dati pubblicamente accessibili. Le informazioni contenute in questo documento riflettono lo stato dell'arte al momento della sua redazione.

L'azienda che ha commissionato la creazione di questo report è esonerata da qualsiasi responsabilità riguardante:

- L'accuratezza, completezza o validità delle informazioni presentate
- Eventuali errori od omissioni nei dati analizzati
- Qualsiasi danno diretto o indiretto derivante dall'utilizzo delle informazioni contenute
- L'interpretazione dei dati e delle analisi presentate

Le conclusioni e le raccomandazioni fornite nel report sono basate sulle evidenze disponibili al momento della ricerca e non costituiscono garanzia di risultati futuri. Il panorama delle minacce cyber è in continua evoluzione, pertanto le informazioni potrebbero diventare obsolete rapidamente.

Questo documento è stato creato con l'unico scopo di fornire una panoramica generale sullo stato della cybersecurity nel settore GDO e non deve essere considerato come consulenza professionale o legale.

L'azienda che ha commissionato il report declina ogni responsabilità per:

- Decisioni operative o strategiche prese sulla base delle informazioni contenute
- Eventuali conseguenze derivanti dall'implementazione delle raccomandazioni suggerite
- L'uso improprio delle informazioni presentate

Si raccomanda vivamente ai lettori di consultare esperti del settore prima di intraprendere azioni basate sul contenuto di questo report.

MATICMIND®

MAKES IT EASY

www.maticmind.it

info@maticmind.it