Anteprima Rapporto Clusit 2025

Rapporto Clusit: incidenti cyber gravi in aumento globale (+27%) nel 2024. L'Italia rimane un bersaglio, subisce il 10% degli attacchi mondiali.

Dati 2024 in evidenza dal Rapporto Clusit 2025:

- In media, si sono verificati nel mondo 295 incidenti cyber al mese
- 9 incidenti su 10 nel mondo sono stati di matrice cybercriminale
- Phishing e Ingegneria Sociale a livello globale sono cresciuti del 33% rispetto al 2023
- +15% la crescita degli attacchi in Italia rispetto al 2023
- +67% gli incidenti significativi in Europa
- +40% la crescita degli incidenti di matrice cybercrime in Italia rispetto al 2023
- 29% la percentuale degli incidenti subìti in Italia a seguito di azioni di attivismo rispetto al valore globale dell'8%
- Un quarto degli incidenti al settore Manifatturiero nel mondo è avvenuto contro realtà italiane
- Un quarto degli incidenti al settore Trasporti e Logistica nel mondo è avvenuto contro realtà italiane
- Oltre un terzo degli incidenti in Italia è stato causato da Malware

Milano, 25 febbraio 2025 – Sono stati **3.541 gli incidenti cyber rilevati a livello mondiale nel 2024 dai ricercatori di Clusit**[1], Associazione Italiana per la Sicurezza Informatica. La crescita percentuale rispetto all'anno precedente è stata del 27,4%.
In media, nel 2024 si sono verificati mensilmente 295 incidenti, contro i 232 del 2023 e i 139 del 2019.

I dati, contenuti nel Rapporto Clusit 2025[2] - che delinea in maniera indipendente l'andamento del cybercrime a livello globale e italiano - sono stati presentati questa mattina in anteprima alla stampa.

---

1 Incidenti rilevati da fonti pubbliche nel periodo 1° gennaio-31 dicembre 2024

2 Frutto della collaborazione continuativa di oltre cento professionisti nell'ambito di Clusit, il Rapporto Clusit fornisce da tredici anni il quadro esaustivo della situazione globale della sicurezza informatica, avvalendosi anche del contributo di soggetti pubblici e privati che condividono con Clusit esperienze e ricerche sul campo con informazioni e dati inediti. La presentazione del Rapporto Clusit al pubblico avverrà in apertura di Security Summit, il convegno dedicato ai temi della cyber security in programma a Milano dall'11 al 13 marzo 2025.

Oltre ad osservare una crescita costante della frequenza degli incidenti, i ricercatori di Clusit hanno rilevato un'evoluzione peggiorativa anche dal punto di vista delle conseguenze: nel 2024 si è confermata a livello mondiale una percentuale di incidenti con i**mpatti gravi o gravissimi pari al 79% del totale** (era l'80% nel 2023 e il 50% nel 2020), delineando una ulteriore moltiplicazione dei danni. Sono aumentati anche gli incidenti di gravità media (+42%), mentre quelli con impatto basso sono ormai scomparsi dal campione.

L'**Italia** è stata anche nel 2024 nel mirino dei cyber criminali, con un **tasso di crescita degli incidenti cyber pari al 15,2%** rispetto all'anno precedente. Il dato italiano rappresenta il **10,1% del campione complessivo** degli incidenti individuati in tutto il mondo, percentuale in leggera decrescita rispetto all'incidenza degli incidenti subìti nel 2023 da organizzazioni italiane (11,2%) rispetto al totale.

Tra il 2020 e il 2024, i ricercatori di Clusit hanno rilevato nel nostro Paese **973 incidenti noti** di particolare gravità; ben 357 - **quasi il 39% del totale – è avvenuto solo nell'ultimo anno in esame**. Sebbene registri una lieve ulteriore crescita rispetto all'anno precedente, il dato del 2024 sembra riportarsi nella linea di tendenza degli ultimi anni. Ovvero, gli incidenti sono effettivamente aumentati nel 2024 rispetto al 2023, ma con meno rilevanza di quanto fossero aumentati nei due anni precedenti, hanno commentato gli autori del Rapporto Clusit.

La percentuale di incidenti classificati con alto impatto in Italia è stata superiore nel 2024 alla media globale (53% contro 50%), mentre gli incidenti di gravità "critica" sono stati il 9%, rispetto al 29% del globale. Molto più frequenti, invece, gli incidenti di gravità "media" (38% contro 22% a livello globale); trascurabili quelli a basso impatto (meno dell'1%).

Come sempre, nell'illustrare i dati i ricercatori di Clusit hanno evidenziato che si tratta di una fotografia che rappresenta le linee tendenziali del fenomeno e che tuttavia rappresenta soltanto la punta dell'iceberg, poiché molte vittime tendono ancora a mantenere riservate le informazioni sugli incidenti cyber subìti e che relativamente ad alcune zone del mondo la possibilità di accesso alle informazioni è molto limitata.

"*Il quadro globale tracciato dal Rapporto Clusit 2025 è decisamente preoccupante: da un lato, i livelli di protezione delle organizzazioni sembrano insufficienti; dall'altro gli attacchi diventano sempre più sofisticati, grazie anche all'utilizzo dell'Intelligenza Artificiale, oltreché più facili da portare a compimento, grazie alla disponibilità di modelli di minacce 'As-A-Service' sempre più diffusi*", ha affermato **Anna Vaccarelli, presidente di Clusit**.

"Nel nostro Paese gli incidenti critici sono meno frequenti rispetto alla media globale, ma quelli di gravità media risultano più numerosi. Questo potrebbe indicare che le nostre organizzazioni subiscono attacchi probabilmente meno sofisticati, ma più frequenti. Appare sempre più urgente la necessità di migliorare le strategie difensive", ha proseguito **Anna Vaccarelli** commentando la situazione italiana.

Gli attaccanti nel mondo e in Italia

Il **Cybercrime** - che causa incidenti per estorcere denaro – è stato nel 2024 responsabile di quasi 9 attacchi su 10 (86% del totale +3 punti percentuali rispetto al 2023). La tendenza dimostra quanto anche la criminalità organizzata stia puntando sempre più sul cyberspazio: "*La resa dei reati informatici ha ormai superato quella di molte attività criminali tradizionali, grazie anche ai modelli as-a-Service che rendono il cybercrimine accessibile persino a chi non possiede competenze tecniche*", afferma **Sofia Scozzari**, **del Comitato Direttivo Clusit**. "*Assistiamo ad una commistione, quando non addirittura ad una integrazione, tra criminalità off-line e criminalità on-line che porta a reinvestire in questo business i proventi delle attività precedenti per aumentare le risorse a disposizione di chi attacca, a fronte di ricavi sempre maggiori*".
I ricercatori di Clusit hanno inoltre rilevato che anche il fenomeno dell'**Hacktivism** è in netta crescita (16 punti percentuali in più rispetto all'anno precedente), così come quello dell'**Information Warfare** - la

“guerra delle informazioni” - che raddoppia quasi rispetto al 2023. Solo gli incidenti con finalità di **Espionage / Sabotage** sono in diminuzione, di quasi 20 punti percentuali.
È particolarmente evidente che gli incidenti avvenuti a causa di Spionaggio ed Information Warfare nel 2024 hanno avuto gli impatti di gravità massima nel 70% dei casi: i diversi conflitti che hanno caratterizzato il 2024 hanno portato, secondo i ricercatori di Clusit al costante ricorso a queste tipologie di attacco.

Gli autori del Rapporto Clusit hanno inoltre evidenziato che alle migliaia di attacchi compiuti da cybercriminali e gruppi state-sponsored, nel 2024 si è affiancata anche una crescente quantità di sigle antagoniste, che hanno colpito un gran numero di organizzazioni e governi, alimentando un sempre maggiore senso di incertezza. In alcuni casi, è ragionevole supporre che queste cellule di sedicenti *hacktivist* siano in realtà manovrate da agenzie governative ed inquadrate in più ampie attività di guerra psicologica, disinformazione e sabotaggio.

In **Italia** sono state principalmente attive due tipologie di attaccanti nel 2024: i cybercriminali – che hanno causato il 78% del totale degli incidenti, in crescita percentuale del 40,6% rispetto al 2023 - e gli hacktivist. Gli eventi riferiti all’attivismo in questo periodo - prevalentemente di matrice geopolitica e correlati ai conflitti in essere durante l’anno - continuano a essere considerevoli: dei 279 incidenti rilevati complessivamente, 80 (circa il 29%) sono avvenuti nel nostro Paese.
Non sono stati rilevati in Italia incidenti significativi nelle categorie *Spionaggio* o *Information Warfare*.

Le vittime

A livello mondiale, quasi la metà degli incidenti (44%) ha colpito le tre categorie:

- **Obiettivi Multipli** (18% del totale, in crescita del 17% rispetto al 2023), che subiscono campagne di attacco non mirate, ma dagli effetti consistenti;
- **Settore Governativo, Militare, Forze Armate** (13% del totale, in crescita del 45% rispetto al 2023);
- **Settore Sanità** (13% del totale, in crescita del 19% rispetto all’anno precedente).
-

Gli attacchi indiscriminati agli Obiettivi Multipli si confermano tra i privilegiati del cybercrime, con un elevato successo a causa dell’intensità di questa tipologia di campagne. Gli altri due settori rappresentano obiettivi particolarmente appetibili, per il ruolo strategico che ricoprono e per la rilevanza dei dati trattati.

Sono cresciuti, inoltre, nel 2024 rispetto al 2023 gli incidenti registrati nei comparti mondiali:

- **News/ Multimedia**, con un picco del +175%;
- **Commercio all’ingrosso e al dettaglio**: + 92%;
- **Scolastico**: +43%;
- **Manifatturiero**: +38%;
- **Professionale / Scientifico / Tecnico**: +40%.

Al contrario, per la prima volta dopo il quinquennio 2019-2023, nel 2024 gli attacchi al settore **Finanziario e Assicurativo** sono stati rilevati in calo (-16 punti percentuale rispetto all’anno scorso). I ricercatori di Clusit spiegano il dato sia come primo effetto di una rinnovata regolamentazione sulla resilienza operativa digitale nel settore - almeno in Europa, a seguito del Regolamento DORA - sia imputando maggiore interesse del crimine informatico verso economie di scala, mediante campagne di attacchi trasversali ai settori o verso un numero maggiore di vittime che esprimono una minore capacità di difesa.

In calo nel 2024 anche gli incidenti nel settore **Informatico e Telecomunicazioni** (-10 punti percentuale), dopo una fase di stabilità nei due anni precedenti: questo caso sembra rappresentare l’effetto concreto di un percorso progressivo di irrobustimento delle capacità di difesa del settore, con effetti graduali facilmente osservabili.

Il settore pubblico è stato interessato da un importante aumento del numero degli incidenti fra il 2022 e il 2024: questo è spiegabile con l'incremento delle attività dimostrative, di disturbo e di fiancheggiamento legate ai conflitti in corso, le quali hanno come obiettivi di elezione soggetti legati alle sfere governative e della difesa di quei Paesi considerati avversari, e dei loro alleati. Nell'arco dei cinque anni si è registrato un incremento complessivo di oltre il 100%.

In Italia, la categoria merceologica che ha subìto più incidenti nel 2024 è stata **News e Multimedia**, con il 18% del totale degli incidenti. Segue il comparto **Manifatturiero**, con il 16% degli attacchi, al pari degli **Obiettivi Multipli**, seguiti dal settore **Governativo** (10% del totale).

I **Trasporti e Logistica** hanno subìto il 7% degli attacchi globali, in diminuzione di 4 punti percentuale rispetto al 2023. Tuttavia, i ricercatori di Clusit evidenziano che – al pari del comparto manifatturiero – in questo settore risultano particolarmente elevati i numeri delle vittime rispetto al resto del mondo: in entrambi i casi, oltre un quarto del totale degli incidenti avvenuti complessivamente riguarda realtà italiane.

Sono state in lieve calo le vittime del settore della **Sanità** in Italia (-0,8 punti percentuale rispetto al 2023).

"*Il settore News e Multimedia ha raggiunto un primato negativo nel 2024, con un singolo attacco che ha compromesso i dati di 5 milioni di persone. Questo evento è stato emblematico di come una tecnologia informatica, quando utilizzata in modo prevalente in un settore, possa diventare un bersaglio estremamente appetibile per gli attaccanti che, concentrando l'investimento, hanno la certezza di generare con una sola campagna di attacchi un numero ingente di danni verso la società*", ha commentato **Luca Bechelli**, **del Comitato Direttivo Clusit**. "*Si pensi ad esempio se ad essere bersagliata fosse una tecnologia utilizzata nell'ambito della distribuzione alimentare, o della logistica di beni e servizi ai cittadini. Non è un caso che tali scenari sono e devono essere esattamente quelli da considerare nell'ambito dell'applicazione della Direttiva NIS2, particolarmente in quei settori che sono stati introdotti in perimetro nel passaggio dalla versione precedente a quella attualmente in vigore*".

Sono diminuiti anche in Italia come nel resto del mondo gli incidenti nel settore **Finanziario e Assicurativo**, con un'incidenza di solo il 2% sul totale e una diminuzione di 7 punti percentuali. Anche in questo caso, gli autori del Rapporto Clusit spiegano la decrescita con la forte regolamentazione del comparto, che ha imposto alle istituzioni finanziarie di conformarsi a requisiti stringenti, stimolando gli investimenti in sicurezza e l'introduzione di contromisure all'avanguardia.

La geografia delle vittime: i continenti più colpiti

L'**Europa** ha registrato nel 2024 un picco di incidenti significativo, pari al **+67%**; oltre i due terzi degli incidenti livello globale (65%) nel 2024 hanno colpito i territori americano ed europeo.
In entrambi i continenti, notano i ricercatori di Clusit, le normative sulla divulgazione degli incidenti informatici sono in vigore da più tempo rispetto ad altre regioni del mondo e ciò prospetta una maggiore trasparenza nella segnalazione. In Europa, in particolare, oltre al GDPR, che ha contribuito sensibilmente a favorire la disclosure dei cosiddetti "Data Breach", nell'ultimo periodo si sono intensificate ed estese normative generali e settoriali che impongono adempimenti sulla notifica degli incidenti, come il Regolamento DORA e le Direttive NIS 1 e 2, oltre all'infrastruttura strategica del Perimetro di Sicurezza Nazionale Cibernetica in Italia e a norme equivalenti negli altri paesi UE.

Per la prima volta, si è registrata nel 2024 un'impennata di attacchi verso l'**Oceania** (+228%), spiegabile sia con un'attenzione crescente da parte degli threat actors verso questa regione sia, come per l'Europa, per recenti aggiornamenti delle normative nei Paesi della regione in materia di cybersecurity.

Le tecniche d'attacco, nel mondo e in Italia

Nel 2024, un incidente su tre nel mondo ha avuto come causa un **Malware.** Questo conferma secondo i ricercatori di Clusit, che i cybercriminali continuano a puntare su tecniche consolidate e "industrializzabili".

I **Codici Malevoli**, soprattutto i **Ransomware**, pur registrando un leggero calo percentuale rispetto al 2023, hanno mostrato una crescita dell'11% in termini assoluti (con +114 incidenti nel 2024 rispetto al 2023), confermando la loro affidabilità nelle strategie cybercriminali.
Lo scorso anno si è inoltre registrato un aumento significativo di incidenti causati da attacchi **DDoS** (+36%). **Phishing / Social Engineering** sono stati causa dell'8% del totale degli incidenti, in crescita del 33% rispetto al 2023; **Furto delle identità e Violazione di Account** hanno invece registrato una variazione percentuale del +135%.

Lo sfruttamento delle **Vulnerabilità**, sia note che sconosciute (zero-day), hanno inciso per il 15% sul totale.

È quindi evidente, secondo gli autori del Rapporto Clusit, la progressiva diversificazione delle strategie di attacco e la relativa efficacia nel trasformarsi con successo in incidenti – con una combinazione tra tecniche tradizionali e metodi più sofisticati.

Per un quarto degli incidenti, rilevano ancora gli esperti di Clusit, non è stato possibile conoscere la tecnica utilizzata, in quanto non resa nota; questi casi nell'ultimo anno sono in crescita del 56%.
In Italia, nel 2024 è tornata ad occupare la prima posizione la categoria del **Malware**, con il 38% degli incidenti. I cyber incidenti causati da **DDoS** si attestano quest'anno al 21%, cedendo il primo posto occupato nel 2023 con il 36% del totale. Al terzo posto, con il 19% del totale, si trovano gli incidenti basati su **Vulnerabilità**, una quota storica per il nostro Paese. Seguono **Phishing e Social Engineering**, all'11%, confermando che il fattore umano continua a rappresentare un punto debole facilmente aggirabile dagli attaccanti.

Le **tecniche non classificate** ("*Undisclosed"*) si attestano al 7%, con un rilevante calo rispetto agli anni precedenti: le informazioni che vengono rese note sugli incidenti sono sempre più complete e accurate, probabilmente sia per una volontà di maggiore trasparenza da parte delle vittime sia per una tendenza da parte dei cybercriminali alla rivendicazione degli attacchi, con dovizia di particolari, confermano gli autori del Rapporto Clusit.

Gli attacchi per mezzo di **DDoS** sono stati invece in calo del 36% nel nostro Paese; il dato, in controtendenza con il dato globale che vede invece un aumento di incidenti che sfruttano questa tecnica, è coerente con il calo di Hacktivism già evidenziato per l'Italia. Come notano gli esperti di Clusit, i DDoS sono infatti prevalentemente attacchi dimostrativi, perpetrati dagli attivisti, che nel 2024 hanno avuto un impatto decisamente minore sulle organizzazioni italiane.

Analisi Fastweb della situazione italiana in materia di cyber-crime

Anche per l'anno 2024 Fastweb, oggi Fastweb + Vodafone, ha contribuito a fotografare la situazione del cyber crime in Italia sulla base dei dati del proprio Security Operations Center (SOC), attivo 24 ore su 24 e dai propri centri di competenza di sicurezza informatica.

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 7 milioni di indirizzi IP pubblici, su ognuno dei quali possono comunicare centinaia di dispositivi e server, sono stati registrati nel 2024 oltre 69 milioni di eventi di sicurezza, in aumento del 23% rispetto al 2023. Questo incremento è stato accompagnato da un progressivo avanzamento nelle capacità di risposta, con sistemi di difesa e monitoraggio più sofisticati e metodi di rilevamento più efficaci che hanno permesso una migliore rilevazione e mitigazione delle minacce.

L'impiego dell'AI assume un ruolo sempre più centrale nell'evoluzione del paradigma della sicurezza informatica, sul fronte offensivo, con l'automatizzazione della ricerca di vulnerabilità nei sistemi target, lo sviluppo e l'evoluzione di malware sofisticati, e il perfezionamento delle tecniche di evasione, rendendo gli attacchi più difficili da rilevare e contrastare per i tradizionali sistemi di sicurezza. Parallelamente, sul versante difensivo, l'IA sta migliorando significativamente la rilevazione precoce delle minacce, potenziando la prevenzione degli attacchi e ottimizzando i tempi di risposta agli incidenti. L'integrazione sempre più profonda dell'AI all'interno delle infrastrutture di cybersicurezza di Fastweb ha permesso all'azienda di identificare anomalie ed eventi malevoli con più efficacia riducendo la rilevazione di falsi positivi in linea con le tendenze di settore (fino al 70%).

Sono inoltre inclusi nel Rapporto Clusit 2025 i seguenti contributi:

- **le attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2024**;
- **Speciale FINANCE** Elementi sul cybercrime nel settore finanziario in Europa

Un capitolo sull'Intelligenza Artificiale, con i due contributi:

- **Proteggere il data center ibrido nell'era dell'intelligenza artificiale**, a cura di Cisco
- **Intelligenza Artificiale nella Cybersecurity: Opportunità e Minacce**, a cura di Palo Alto Networks

Un approfondimento sulla Cybersecurity in Sanità:

- **Incidenti in crescita e nuove misure di protezione e sanzioni con NIS2,** Women for Security

La survey:

- **Cybersecurity nelle micro e piccole/medie imprese**, con un quadro aggiornato dall'analisi dei dati del PID Cyber Check delle Camere di Commercio, realizzata dal DINTEC - Consorzio per l'innovazione tecnologica - società in house di Unioncamere, dell'ENEA e delle Camere di commercio italiane, partendo da un modello predisposto dall'istituto di informatica e telematica (IIT) del CNR, assieme al Centro di Competenza START 4.0.

Il contributo

- **Community For Security** CyberFutures, come sarà il nostro lavoro nel 2035?

Gli approfondimenti "**Focus On**":

- Le tendenze 2025 nel settore della sicurezza ibrida, a cura di Netwrix
- Guida Pratica alla Cloud Threat Detection, Investigation e Response, a cura di Wiz
- Trends e osservazioni di un SOC OT Gestito, a cura di HWG Sababa
- Settore dell'energia ad idrogeno: le sfide di cyber resilience, a cura di Federica Maria Rita Livelli
- Proteggere la Supply Chain: strategie di difesa per MSP e MSSP in un panorama di minacce globali, a cura di Acronis
- Attacchi alle Infrastrutture Critiche Italiane, a cura di Fortinet
- I percorsi di attacco, a cura di CrowdStrike
- La sicurezza della Gestione Documentale nei sistemi di acquisizione e stampa, a cura di ASSOIT
- Autismo e Cybersecurity, a cura di Lorenzo J.S. e Andrea Mazzola.

Il Rapporto Clusit 2025 sarà presentato al pubblico il prossimo 11 marzo, in apertura di Security Summit, la tre giorni dedicata alla cybersecurity organizzata a Milano da Clusit con Astrea, Agenzia di Comunicazione ed Eventi specializzata nel settore della Sicurezza Informatica.

Clusit è l'Associazione Italiana per la Sicurezza Informatica. Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta oggi oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Clusit collabora con la Presidenza del Consiglio, con diversi Ministeri, Authority, Istituzioni e organismi di controllo, tra cui Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali. Svolge inoltre un'intensa attività di supporto e di scambio con Cyber 4.0, il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity e con Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA, con Università e Centri di Ricerca. In ambito internazionale, Clusit partecipa a diverse iniziative in collaborazione con i CERT, i CLUSI, con la Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), con le principali Associazioni Professionali del settore, con Università e Centri di Ricerca in oltre 20 paesi. Ulteriori informazioni sulle attività di Clusit sono disponibili sul sito www.clusit.it.

Per ulteriori informazioni si prega di contattare:
Daniela Sarti
Ufficio Stampa Security Summit | Clusit
press@securitysummit.it - dsarti@clusit.it Tel. 335 459432

Rapporto Clusit 2025
Tre Spunti di Riflessione
A cura degli autori del Rapporto Clusit 2025

Cybersecurity e Persone
Resta fondamentale, nel nostro Paese, mantenere una forte attenzione sul tema della consapevolezza delle persone: la crescita dell'87% degli attacchi di phishing ed ingegneria sociale testimonia che quanto fatto fino ad oggi non è ancora sufficiente. Ci sono i termini per lanciare un allarme, anche guardando ai dati di altri contributi contenuti nel Rapporto Clusit, come, ad esempio, il contributo della Polizia Postale e delle Comunicazioni, che ricomprendono anche tutti quegli eventi che interessano i singoli cittadini e le PMI. Il fenomeno sta infatti assumendo un grado di estensione che diventa sempre più preoccupante. È pertanto imprescindibile che la Scuola, l'Università, i soggetti pubblici e privati lavorino in sinergia per **sviluppare una cultura della sicurezza che sia parte del patrimonio di conoscenze di tutti i cittadini, a partire dalle nuove generazioni**. Insieme alla consapevolezza, rimane anche aperto il tema delle competenze più specifiche, il cui gap rispetto alle esigenze del mercato continua ad aumentare. Deve quindi essere ancora al centro dell'attenzione il tema del "*Reskill and upskill*" con riguardo alle **competenze STEM.**

Il "doppio uso" dell'Intelligenza Artificiale
In ottica strategica, particolare attenzione dovrà essere posta verso le opportunità e ai rischi dell'adozione dell'AI nell'ambito dei processi di business delle imprese. L'AI è uno degli ambiti di innovazione in cui lo stesso concetto di *dual use* diventa obsoleto: ne parliamo tanto in relazione alle tecnologie di protezione e di detection degli attacchi informatici, quanto nell'ambito delle tecniche stesse di attacco, ma soprattutto come strumento che in modo pervasivo accompagnerà sempre più – talvolta sostituendo, talvolta potenziando – l'attività operativa delle persone; soprattutto, sarà il mezzo tramite il quale nasceranno nuovi servizi fino ad oggi inimmaginati/bili. Nel cercare di comprendere quali saranno i nuovi rischi, le organizzazioni non dovranno sottovalutare l'impatto in termini di dipendenza dalla tecnologia che questo strumento avrà nel pervadere ogni ambito delle attività umane e automatizzate; ciò si sostanzierà in un incremento del livello di impatto che i rischi tradizionali sulla sicurezza, che ancora oggi fatichiamo a mitigare, potranno avere dal momento che si concretizzeranno in incidenti informatici.

Governance della Sicurezza e dei Processi

Emerge sempre più – anche dai dati del Rapporto Clusit 2025 - come sia necessario rafforzare la **governance della sicurezza e la capacità di identificare, analizzare, valutare e gestire i rischi**, sia con misure preventive che di mitigazione, ma anche nella prospettiva di gestire il trasferimento del rischio verso terzi, sia in ottica di coperture assicurative, ma anche trasferendo l'onere dell'implementazione delle misure di mitigazione mediante il ricorso ad un outsourcing di qualità, per esempio nell'ambito di percorsi di *Cloud Journey*. La **capacità di determinare, anticipare e gestire** le evoluzioni legate alle minacce esogene, oltre che al contesto interno dell'organizzazione, è ormai fondamentale nel quadro che il Rapporto ci permette di delineare.
Resta poi imprescindibile rafforzare la **governance dei processi di patch & vulnerability management**. Tanto si è fatto in Italia, come si riscontra dalla riduzione degli incidenti a Severity massima, ma il preoccupante dato globale di crescita del 76% degli attacchi basati su vulnerabilità note e 0-day deve essere di stimolo a mantenere alta l'attenzione.
È necessario **ragionare in ottica di** processi di reale **presidio continuo della sicurezza di prodotti e servizi lungo l'intero ciclo di vita** (SSDLC - Secure Software Development LifeCycle), sia in ambienti waterfall che agili (SecDevOps), adottando **soluzioni** che affrontino efficacemente l'**ambito della sicurezza delle applicazioni** su ogni elemento (servizi esposti, front end, middleware, applicazioni mobili, IoT) e non solo in fase di scrittura del codice.
In particolare, le logiche di **security by design** devono diventare parte dei processi di sviluppo di prodotti e servizi a partire da quando i servizi vengono concepiti, dall'on-premise al cloud, con una sempre più stringente **gestione dei processi di sourcing e delle terze parti**, non solo in ottica di

compliance, ma anche in ottica di tutela aziendale. Il fenomeno degli impatti derivanti dalla sicurezza della catena di fornitura è forse uno di quelli che si dimostra più difficile da intercettare dai dati del nostro Rapporto, ma è certamente un fenomeno importante, sul quale si sta concentrando anche lo sforzo legislativo europeo e nazionale.
Tale tema diventa particolarmente rilevante nel mondo manufatturiero, o comunque ovunque siano presenti sistemi **OT/IoT**, spesso bersagli semplici per attacchi come i DDoS o che sfruttano le connessioni utilizzate dai manutentori.