Nuova edizione ottobre 2025

RAPPORTO

Clusit

sulla Cybersecurity
in Italia e nel mondo

2025

SECURITY SUMMIT

Indice

ASTREA

Via Copernico, 38 - 20125 Milano

Prefazione

Il rapporto di metà anno dà informazioni di "tendenza" sui dati degli incidenti relativi al primo semestre. È un dato parziale, ma certamente utile per interpretare l'andamento e l'evoluzione degli incidenti. Il primo semestre 2025 ne indica, in molti casi, un aumento: alcuni numeri sugli incidenti del primo semestre 2025 hanno già raggiunto quelli dell'intero 2024; c'è da sperare che non si arrivi a un raddoppio netto! Bisognerà anche capire se questo dato dipende da un reale aumento degli incidenti o se è un effetto delle nuove norme che obbligano alla denuncia: in questo caso si spiegherebbe perché il numero degli incidenti di dominio pubblico è aumentato. D'altro canto, le nuove norme (p.es. NIS2) obbligano ad adottare maggiori e più efficaci contromisure e questo potrebbe avere un effetto positivo sul numero di incidenti, come abbiamo osservato per le norme che recentemente hanno riguardato il settore finanziario e assicurativo. Da questo punto di vista è sicuramente un momento di transizione e nel prossimo rapporto potremo probabilmente capire in che direzione agiranno le norme: maggiori denunce e quindi maggior numero di incidenti o migliore difesa e quindi riduzione del numero di incidenti? Il confronto tra i nostri dati e quelli di altri soggetti preposti (ACN, Polizia Postale e per la Sicurezza Cibernetica, CSIRT ecc.) ci aiuterà a fare un quadro dell'evoluzione.

In ogni Rapporto ci sono contributi ricorrenti, che costituiscono un aggiornamento tra un periodo e il successivo, ma accogliamo sempre anche contenuti su temi di tendenza perché uno dei nostri obiettivi è creare consapevolezza: riuscire a informare su quello che sta per succedere o su quali sono gli strumenti a diposizione per affrontare le nuove sfide, fa parte del servizio che cerchiamo di offrire ai nostri lettori. Di volta in volta cerchiamo di sollevare l'attenzione su alcuni di questi aspetti nella speranza di aggiornare e di aggiungere informazioni.

L'Intelligenza Artificiale, per esempio, è costantemente tra i nostri temi: non è più una novità in sé (in tutti i consessi il commento ormai è: ancora Intelligenza Artificiale?), ma ci sono sempre nuove modalità di impiego nella cybersecurity sia in attacco che in difesa. Nel settore della cybersecurity l'Intelligenza Artificiale è particolarmente insidiosa e, per certi versi, sotterranea, non immediatamente evidente come accade invece con un nuovo malware, che è istantaneamente riconoscibile, e pertanto si tende a non attivare sollecitamente contromisure specifiche. La conoscenza delle nuove frontiere poste dall'intelligenza Artificiale nella realizzazione degli attacchi ci deve stimolare a adottare contromisure all'altezza della sfida, ricorrendo anche in difesa all'Intelligenza Artificiale: per esempio l'IA generativa può aiutare nel gestire i nuovi obblighi derivanti dalle normative entrate recentemente in vigore.

Spesso ci concentriamo ad analizzare i problemi della cybersecurity in ambiti "tradizionali" ma stanno nascendo sfide in settori che fino a poco fa non erano toccati (o lo erano poco) dagli attacchi informatici: il settore marittimo e quello dei beni culturali, per esempio, di cui parliamo in questo rapporto, con risvolti inconsueti rispetto agli attacchi conosciuti. L'allargarsi della tipologia delle potenziali vittime deve portarci ad avere un livello di attenzione alto, qualunque sia l'attività professionale e lavorativa nella quale siamo coinvolti, senza pensare "questo non mi riguarda": presto, purtroppo potrebbe riguardarci e conviene essere proattivi e cercare di prevenire i danni!

Come è stato sottolineato nel Security Summit del 15 ottobre a Verona, il primo passo per attivare la difesa è la percezione di essere in pericolo, da cui deriva la consapevolezza dei rischi che potremmo correre che ci porta ad attivare forme di prevenzione e di difesa. **È un ciclo virtuoso che dovremmo costantemente tenere presente e mettere in atto.**

Quanto le aziende siano ancora lontane da questi obiettivi lo fotografa la survey sulla Cybersecurity svolta tra 700 piccole e medie imprese, che è stata realizzata nel 2025 dalla Camera di Commercio di Modena in collaborazione con l'Università di Modena e Reggio Emilia e con il Clusit: un dato locale, ma significativo se si vanno a leggere i dati del Rapporto relativi al manifatturiero e industriale.

Per noi del Clusit l'obiettivo è far crescere la sensibilità degli utenti verso i problemi di sicurezza, siano essi semplici cittadini o aziende e organizzazioni. Lo facciamo attraverso il rapporto, attraverso i convegni, primo tra tutti il Security Summit e attraverso attività di formazione rivolte alle scuole: siamo già al terzo anno del progetto "SicuraMente" destinato agli studenti della scuola secondaria di secondo grado, che da quest'anno si allarga ai cittadini "Senior" (gli over 60), ai giornalisti e agli installatori di dispostivi domotici (le intrusioni nelle telecamere domestiche, configurate con la password di default, sono nella cronaca di tutti i giorni) e ai manager, convinti che debba diventare cultura comune dei vertici considerare la sicurezza informatica uno degli asset da coltivare e far crescere. Un danno informatico grave può mettere in ginocchio un'azienda con costi molto maggiori della prevenzione nella gestione dei rischi. Il nostro progetto di formazione, benché si vada allargando, non è certamente sufficiente a colmare le lacune che abbiamo nel Paese rispetto a questi temi, ma siamo orgogliosi di poter dare il nostro contributo!

*** *** ***

Il Rapporto è il risultato dello sforzo di un team di altissimo livello, che da anni lavora per sensibilizzare il mondo pubblico e privato sui temi della sicurezza informatica. A tutti i colleghi che hanno dedicato tempo e impegno nella stesura del rapporto va il ringraziamento mio, degli Associati e (assumo) anche dei lettori.

Oltre 3.000 copie cartacee distribuite durante gli ultimi 12 mesi, più di 80.000 copie scaricate e più di 1.000 articoli, sono l'evidenza della rilevanza del Rapporto CLUSIT, utilizzato come strumento di lavoro e di consultazione per le organizzazioni.
È importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Anna Vaccarelli
Presidente Clusit

Introduzione al Rapporto

Nel 2024 gli incidenti a livello mondiale erano aumentati del 36% rispetto al 2023 (quelli verso l'Italia del 20%). La tendenza globale del primo semestre 2025 mostra una ulteriore crescita, pari al **+36% rispetto al semestre precedente (+13% verso l'Italia)**.

Nel primo semestre 2025, secondo una tendenza ormai consolidata da diversi anni, non solo è aumentata la frequenza degli incidenti ma anche la loro gravità media. Nel 2024, gli incidenti con impatto "Critico" o "Alto" erano il 77% del totale (un aumento drammatico rispetto al 50% del 2020). Nella prima metà del 2025, l'impatto medio stimato a livello globale è cresciuto ulteriormente rispetto al 2024 (**82% di incidenti con gravità critica o alta**).

Nel 1° semestre del 2025 l'**ambito per cui si rileva un maggior numero di incidenti cyber in Italia è quello *Governativo / Militare / Law Enforcement*,** interessato da una significativa quota di eventi, pari al 38% del totale, che in valore assoluto si traduce in una quantità di incidenti pari al **279% rispetto all'intero anno precedente! La crescita rispetto allo stesso periodo dello scorso anno (I sem. 2024) è pari a oltre il 600%.**

Al secondo posto si trova invece **l'ambito *Transportation / Storage* (17% del totale**), solo ottavo a livello globale, che **realizza in sei mesi oltre una volta e mezzo il numero degli incidenti di tutto l'anno precedente.**

Il Rapporto inizia con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel primo semestre del 2025**, confrontandoli con i dati raccolti negli anni precedenti.

La panoramica degli attacchi in Italia è poi completata dalle **rilevazioni e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica**, che ci ha fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso dei primi sei mesi di quest'anno.

Segue un'**analisi sulla** evoluzione della **Cybersecurity in ambito manifatturiero/industriale**, con i dati di settore tratti dalle ultime rilevazioni Clusit al 30 giugno 2025.

Trovate poi un **approfondimento su Conformità alla NIS2 e CyberSecurity OT**, a cura di Enzo M. Tieghi e Mario Testino.

Segue uno **Speciale Intelligenza Artificiale**, con due articoli:

Intelligenza Artificiale (IA) agentica: quali evoluzioni ci attendono nella cybersecurity, a cura di Federica Maria Rita Livelli.

L'uso dei sistemi di AI generativa gratuiti nella gestione del ciclo di vita dei requisiti normativi, a cura di Giancarlo Butti.

Trovate in seguito i risultati della seconda edizione di **una survey sulla Cybersecurity nelle piccole e medie imprese.** Più di **700 aziende hanno risposto alla survey che è stata realizzata** nel 2025 **dalla Camera di Commercio di Modena** in collaborazione **con l'Università di Modena e Reggio Emilia** e con il Clusit.

Questi sono infine i temi trattati nella sezione FOCUS ON:

Cybersecurity nei sistemi portuali: dall'esigenza di adeguamento alla resilienza sistemica, a cura del *Centro di Competenza START 4.0 e dell'Autorità di Sistema Portuale del Mar Ligure Occidentale.*

Sicurezza delle applicazioni cloud: visibilità e controllo continuo dell'ecosistema SaaS, a cura di *CrowdStrike*

Analisi degli incidenti Cyber nel settore culturale italiano tra il 2020 e il 2024, a cura di Joram Marino e Federica Vennitti

Noi e i nostri dati in Rete: un universo da scoprire, a cura di Andrea Rui.

Analisi dei principali incidenti cyber del I semestre 2025

Italia (di nuovo) sotto assedio

In questo aggiornamento semestrale del Rapporto CLUSIT 2025, giunto ormai al suo tredicesimo anno di pubblicazione, analizziamo i più gravi incidenti avvenuti a livello globale (Italia inclusa) nell'ultimo quinquennio, ed in particolare confrontiamo numeri e caratteristiche degli eventi noti del 2024 e del primo semestre 2025, per evidenziare le principali tendenze.

Dimensione del campione e tendenze principali

A partire dal 2011, il gruppo di ricerca di CLUSIT ha tracciato e analizzato in modo indipendente circa **26.000 incidenti**.
Negli ultimi cinque anni e mezzo abbiamo documentato una pronunciata escalation di attività ostili. In totale, nel periodo 2020 – I sem. 2025, abbiamo registrato 15.717 incidenti, pari al **61% del nostro campione.**
A livello globale la media mensile di incidenti gravi che abbiamo rilevato è passata dai 156 del 2020 ai 314 del 2024, fino ai 459 del primo semestre 2025: in pratica, **in 5 anni il numero di eventi osservati ogni mese è triplicato**.
Nel 2024 gli incidenti a livello mondiale erano aumentati del 36% rispetto al 2023 (quelli verso l'Italia del 20%).
La tendenza globale del primo semestre 2025 mostra una ulteriore crescita, pari al **+36% rispetto al semestre precedente (+13% verso l'Italia)**.

Per sintetizzare i trend principali che emergono dai dati, discussi nei dettagli (con tutte le sfumature e le angolazioni del caso) nelle pagine successive, evidenziamo di seguito alcune osservazioni di alto livello.

Record storico

Nel primo semestre 2025 abbiamo registrato 2.755 incidenti, superando i 2.022 eventi documentati nel secondo semestre 2024, il numero più alto dall'inizio di questa pubblicazione. Queste cifre, di per sé impressionanti, rappresentano probabilmente solo una quota, sia pur significativa, del totale degli incidenti effettivamente avvenuti.

Aumento sensibile degli impatti

Nel primo semestre 2025, secondo una tendenza ormai consolidata da diversi anni, non solo è aumentata la frequenza degli incidenti ma anche la loro gravità media.
Nel 2024, gli incidenti con impatto "Critico" o "Alto" erano il 77% del totale (un

aumento drammatico rispetto al 50% del 2020). Nella prima metà del 2025, l'impatto medio stimato a livello globale è cresciuto ulteriormente rispetto al 2024 (**82% di incidenti con gravità critica o alta**).

Insufficienza delle contromisure

In base alle tendenze osservate sia a livello globale che nazionale, **il divario tra la capacità offensiva degli attaccanti e l'efficacia delle contromisure continua ad ampliarsi**, il che implica necessariamente un aumento dei rischi, sia per le singole vittime, sia a livello sistemico.

L'incertezza come "new normal"

L'aumento delle minacce (sia dal punto di vista quantitativo che qualitativo), la crescita dei rischi conseguenti e la pervasività degli incidenti, ci portano a ribadire (ancora una volta) che **non siamo di fronte a fenomeni contingenti**, passeggeri, ma a una tendenza consolidata e di lungo periodo.

Oltre all'allarmante aumento delle attività di matrice criminale, le operazioni condotte dagli Stati (direttamente o tramite gruppi sponsorizzati) sono ormai diventate la norma, e vengono implementate in modo sistematico, grazie ad un sofisticato arsenale di strumenti offensivi, con diverse finalità ed intensità.
Ciò comporta, in aggiunta alle consuete attività di spionaggio, anche una continua minaccia verso infrastrutture critiche e piattaforme di ogni tipo, sia governative che civili, nonché costanti attività di disinformazione mirate ad alterare la percezione della popolazione, provocando impatti socioeconomici significativi ed innalzando i livelli di incertezza a livelli senza precedenti.

L'Italia continua a subire in modo sproporzionato

In questo contesto di minaccia crescente, il nostro Paese si colloca tra le nazioni che più risultano **incapaci di contenere gli attacchi**. Nel 2023 l'Italia ha registrato l'11,2% di tutti gli incidenti globali (un aumento netto dal 3,4% del 2021 e dal 7,6% del 2022) confermando il suo status di "maglia nera della cybersecurity" tra le principali economie mondiali. Anche nel 2024 è rimasta vittima del 9,9% degli incidenti a livello mondiale, e il **10,2% nel primo semestre 2025**.
In proporzione al dato globale la percentuale di incidenti realizzati contro l'Italia risulta anomala, sia rispetto alla dimensione della popolazione che a quella del PIL nazionale, il che rappresenta uno svantaggio competitivo per il Paese.
In dettaglio, i dati del 2025 mostrano come l'Italia (rispetto alla media globale) sia stata molto più colpita da incidenti di tipo DDoS realizzati da gruppi di sedicenti attivisti, per esempio *NoName057(16)*, che in realtà sono sabotatori coordinati da strut-

ture governative russe. Pur trattandosi di incidenti con impatti di livello tipicamente medio-basso, la loro frequenza rende necessarie azioni di mitigazione specifiche.

In corsa contro il tempo

Nonostante i budget per la sicurezza informatica stiano nel complesso crescendo, i dati dimostrano che sia il numero di incidenti che la loro gravità stanno *comunque* aumentando.
Ciò suggerisce due considerazioni di alto livello: che tali investimenti non siano sufficienti in termini assoluti, e **che le risorse disponibili dovrebbero essere spese in maniera più efficace e mirata**.

Alla luce di quanto sopra, per concludere vorremo evidenziare quattro punti di attenzione.

1. l'aumento degli **incidenti con impatto Critico o Alto, che in 5 anni a livello globale sono cresciuti del +143%** (!), è spesso sottovalutato (o non considerato) nelle valutazioni del rischio e nelle stime delle perdite potenziali, mentre dovrebbe essere messo *al centro* del dibattito e guidare la definizione delle strategie difensive e dei relativi investimenti.
2. Oltre a ciò, **il fenomeno della insicurezza cibernetica va attentamente declinato in base ai diversi settori merceologici**. Ad esempio, dall'analisi dei nostri dati emerge una dinamica poco discussa, ovvero che il numero di incidenti a cui risulta vittima un particolare settore e il loro tasso di crescita non sono correlati in modo lineare con la loro gravità media e con il tasso di crescita relativo. Questo significa che, in un contesto di generale peggioramento della situazione, per alcuni settori gli impatti crescono più velocemente della media, anche se subiscono un numero di incidenti relativamente inferiore, il che può indurre a sottostimare i rischi. Nella realtà i diversi settori sono attaccati per ragioni diverse, con tecniche diverse e conseguenze molto diverse (anche a parità di tecniche), e questo fenomeno va compreso tramite un'analisi granulare delle motivazioni degli attaccanti, dei loro comportamenti e delle conseguenze dei fallimenti difensivi nei diversi scenari. *Ciò nonostante, la maggior parte delle organizzazioni continuano ad allocare risorse per la cyber security basandosi su requisiti (minimi) di conformità e su dati storici (non più attuali) piuttosto che su valutazioni del rischio basate su dati aggiornati, specifici e puntuali.*
3. In quest'ottica, **anche le strutture di policy e governance richiedono una riforma**, per allineare i framework regolatori con le conseguenze *pratiche* dell'insicurezza sistemica, assicurando che i meccanismi di finanziamento, le strutture di responsabilità e i requisiti di conformità riflettano profili di rischio

aggiornati piuttosto che baseline astratte dettate da negoziazioni avvenute anni fa.

4. Infine, vanno studiate a fondo le implicazioni di quella che ormai è una sfida strategica fondamentale: l'attuale traiettoria suggerisce che stiamo avvicinandoci (o potremmo aver già superato) una soglia critica dove la complessità, la velocità, il volume e l'intensità delle minacce cibernetiche eccedono la capacità culturale, organizzativa ed economica delle organizzazioni e dei governi di gestirle efficacemente.

Da questo punto di vista, la questione non è più se le minacce cibernetiche rappresentino un fattore di rischio primario per gli stati ed un rischio esistenziale per le singole organizzazioni (i dati lo confermano in modo inequivocabile, e non da oggi) ma piuttosto se le attuali strutture istituzionali, i modelli di allocazione delle risorse, le strategie di mitigazione ed i processi operativi di sicurezza **possano evolversi abbastanza rapidamente da consentirci di conseguire i livelli di resilienza necessari**, prima che il divario tra minaccia e difesa diventi irrecuperabile, e gli impatti insostenibili.

Confidando che anche questo aggiornamento semestrale del Rapporto CLUSIT possa apportare un contributo significativo al dibattito nazionale in merito alle problematiche della sicurezza cibernetica ed alle sue importanti ricadute sul benessere del Paese, auguriamo a tutti una buona lettura.

Premessa – uno scenario in evoluzione

Rispetto al 2024, si sottolinea che dall'ultima pubblicazione del Rapporto Clusit (marzo 2025) sono stati censiti ulteriori 230 incidenti attribuiti allo stesso periodo (passando così da 3541 a 3771), di cui è stato possibile venirne a conoscenza solo durante il 2025. Questo aspetto, purtroppo usuale nell'ambito dell'analisi di questo tipo di fenomeni, permette di sottolineare una criticità ancora rilevante nell'ambito della gestione della sicurezza delle organizzazioni: il tempo medio necessario per scoprire una violazione di sicurezza (nei casi in cui gli attaccanti non decidano di compiere azioni eclatanti ed esplicite) supera ancora oggi i sei mesi (194 giorni secondo i report più accreditati[1]).

In questa edizione di metà anno, per maggiore completezza, abbiamo deciso di utilizzare il campione di dati più aggiornato: il lettore più attento potrà rilevare alcune variazioni nelle serie storiche in riferimento al 2024, secondo quanto pubblicato nel Rapporto di Marzo 2025.

---

1 https://www.ibm.com/reports/data-breach

Analisi dei principali incidenti cyber noti a livello mondiale dal 2020 al I Semestre 2025

+36%

È la crescita degli incidenti rispetto al II semestre 2024

In questa sezione offriamo una panoramica degli incidenti di sicurezza più significativi avvenuti a livello mondiale nel primo semestre 2025, confrontandoli con i dati raccolti nei 5 anni precedenti.

Lo studio si basa sull'analisi di incidenti cyber di pubblico dominio, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali sulle organizzazioni vittima degli stessi.

Nel periodo in esame, tra gennaio 2020 e giugno 2025, si sono verificati un totale di **15.717 incidenti**, così distribuiti:

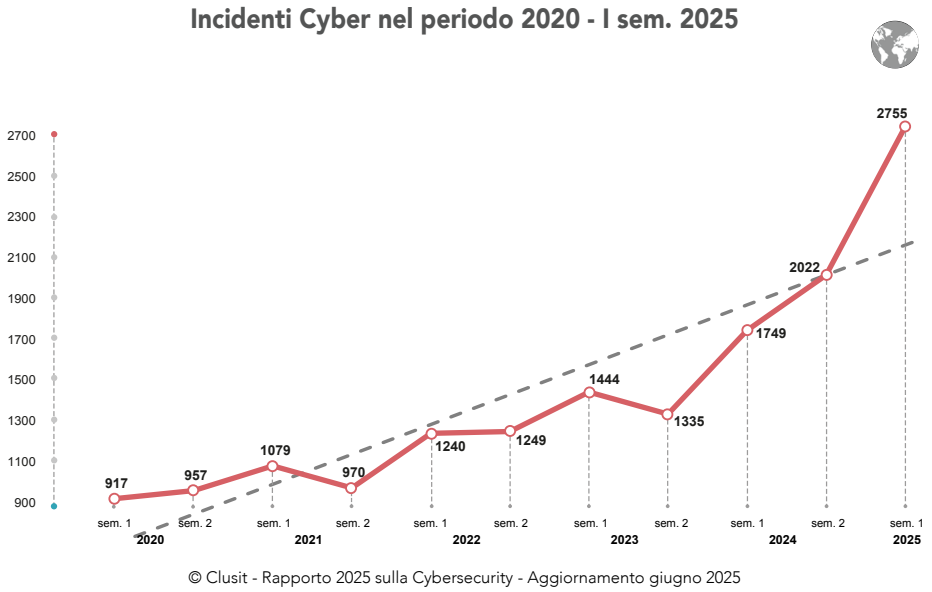


Fig. 1 - Andamento degli incidenti cyber nel periodo 2020 - I semestre 2025

~1/5

Degli incidenti censiti dal 2020 è avvenuto nel I sem. 2025

3x

È la crescita della media mesile degli incidenti rispetto al I sem 2020

Nell'ultimo semestre (**Fig. 1**) abbiamo registrato 2755 incidenti, il numero maggiore di sempre per un solo semestre, con **un aumento percentuale del 36% rispetto al semestre precedente.**

A conferma di una costante recrudescenza dello scenario degli incidenti, gli eventi dell'ultimo semestre costituiscono da soli quasi 1/5 del totale dal 2020; anche la media mensile degli incidenti cyber (**Fig. 2**) è aumentata considerevolmente, raggiungendo quota 459, il triplo di quanto avveniva il I semestre 2020 (153 incidenti).

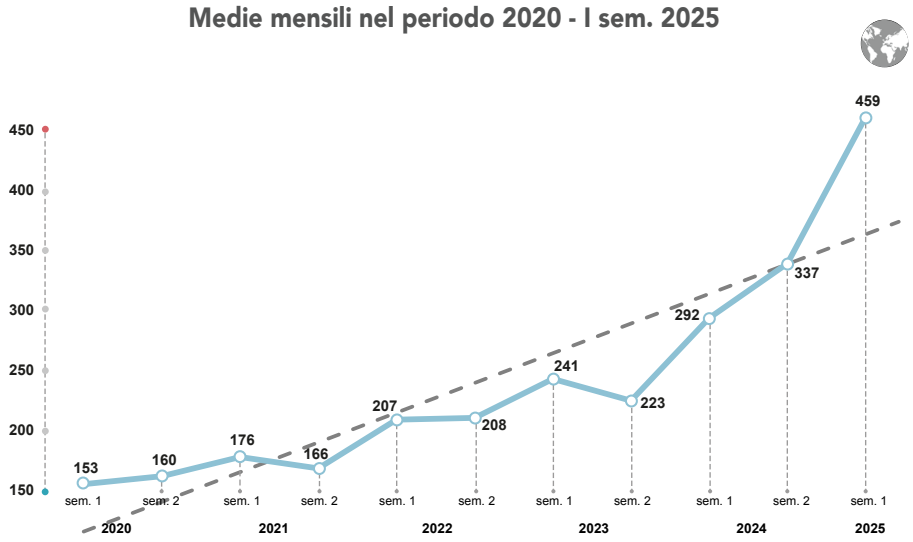


Fig. 2 - Andamento delle medie mensili nel periodo 2020 - I semestre 2025

Distribuzione degli attaccanti per tipologia

76%
è la quantità di incidenti cybercrime del I sem 2025 rispetto alla categoria in tutto il 2024

La crescita in volume degli incidenti è sostenuta (**Fig. 3**) da un aumento del fenomeno *Cybercrime*: in valore assoluto, con 2401 incidenti, il I semestre 2025 realizza il 76% degli eventi registrati in tutti i 12 mesi del 2024!

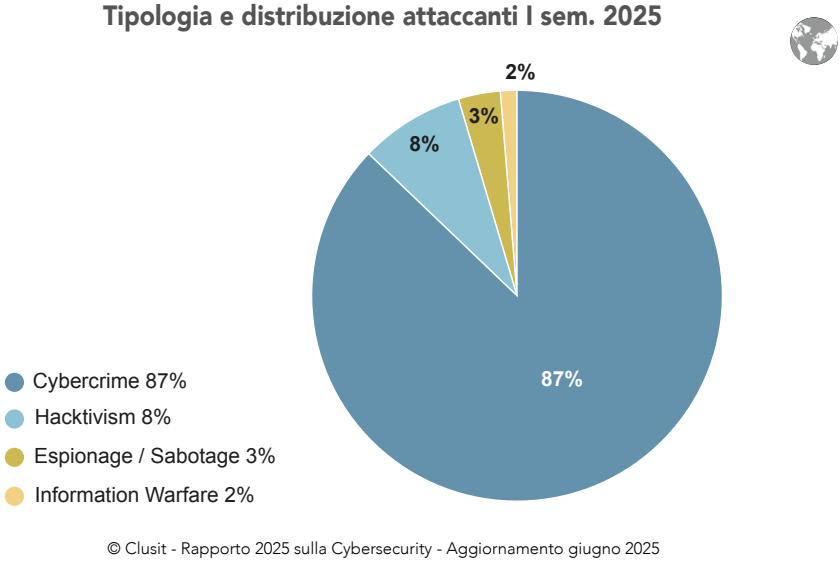


Fig. 3 - La distribuzione percentuale degli attaccanti nel I semestre 2025

I fenomeni di *Espionage/Sabotage* e *Information Warfare* sono in calo rispetto al 2024 di 1 punto percentuale ciascuno, a dispetto dell'estensione dei conflitti già attivi nel 2024 e dell'acuirsi delle ulteriori problematiche nel primo semestre dell'anno.

1 su 10
è un incidente con matrice Warfare o Hacktivism

Ricordando il problema ormai noto della complessità della reale attribution degli attacchi di *Information Warfare*, le tensioni in corso si riflettono conseguentemente in un aumento sostanziale degli incidenti classificabili come *Hacktivism*, **che nei primi sei mesi del 2025 raggiungono quasi la totalità**

della quota percentuale del 2023 (Fig. 4), realizzando in valore assoluto il 59% degli eventi di tutto il 2024.

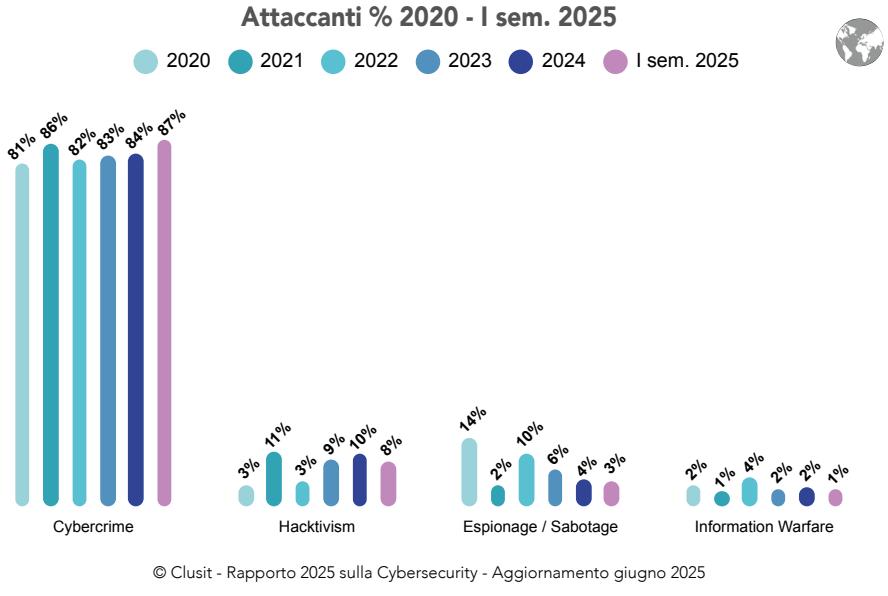


Fig. 4 - La distribuzione percentuale degli attaccanti nel periodo 2020 - I semestre 2025

Distribuzione delle vittime per categoria

Nelle prime otto posizioni della classifica dei settori più colpiti dagli incidenti informatici, in valore assoluto il numero degli eventi registrati nel solo I semestre 2025 supera per tutte le categorie il 60% della quantità di incidenti registrati in tutto il 2024, ed in più casi in modo allarmante; valutare questo dato ci permette di identificare, al di là della posizione in classifica, quali sono i settori che presumibilmente in corso d'anno risulteranno più colpiti, e la dimensione della discontinuità di tale tendenza rispetto al passato.

Gli eventi che hanno colpito con successo più settori contemporaneamente (*multiple target*), ad esempio, **coprono nella metà dell'anno corrente oltre l'85% della quantità di incidenti registrati nel 2024**, e determinano il 21% delle vittime nel I semestre del 2025, in aumento rispetto al 2024 di 3 punti percentuali (**Fig. 5**).

90%
è il numero di incidenti verso il settore Manifacturing nel I sem. 2025 rispetto a tutto il 2024

Al secondo posto la categoria Governenment / Military / Law Enforcement, stabile al 14% (tuttavia con una quantità di incidenti pari al 75% di quelli registrati nel 2024).
Il settore Healthcare, apparentemente in discesa di un punto percentuale rispetto all'anno precedente, con 337 incidenti **nel I sem. 2025 realizza il 67% dei 500 incidenti registrati in tutto il 2024.**

Cresce la percentuale sul totale degli incidenti verso il settore Manifacturing (dal 6% del 2024 all'8% nel primo semestre 2025) che passa dal settimo al quarto posto in classifica: in questo caso **il settore in un solo semestre raggiunge il 90% degli incidenti registrati in tutto il 2024.**

Perde una posizione in classifica Financial/Insurance (7%), con una quota di eventi del I sem. 2025 sul 2024 di poco superiore al 60%, così come il settore ICT: in uno scenario di crescita generalizzata del numero degli incidenti, per entrambi i settori possiamo quindi affermare che non si osserva nessuna variazione significativa rispetto alla tendenza consolidata nel periodo precedente.

110%
è il numero di incidenti verso il settore Transportation/Storage nel I sem. 2025 rispetto a tutto il 2024

I settori Professional / Scientific / Technical e Transportation/ Storage risalgono di numerose posizioni la nostra triste classifica, poiché **raggiungono, se non superano, in soli sei mesi il numero di incidenti di tutto l'anno precedente:** il 94% per Professional / Scientific / Technical e addirittura il 110% per Transportation/Storage.
Il settore Education è fortunatamente in controtendenza rispetto ai precedenti: non solo perde 2 punti percentuali sul totale, ma realizza meno del 50% degli eventi di tutto l'anno precedente.

Al contrario, Wholesale/Retail si allinea alla crescita di incidenti dei primi settori citati, realizzando oltre il 65% del numero di incidenti dell'anno precedente in soli sei mesi. News/Multimedia, che a seguito di una campagna mirata nel 2024 aveva raggiunto l'8° posto tra i settori colpiti, torna ora al 14°, coerentemente con il dodicesimo posto che occupava nel 2023. Di questo episodio resta importante sottolineare come periodicamente alcuni settori corrano il rischio di veder mietere molte vittime a causa di campagne mirate che sfruttano la loro dipendenza da alcune particolari soluzioni tecnologiche o da specifici soggetti nella loro supply chain.

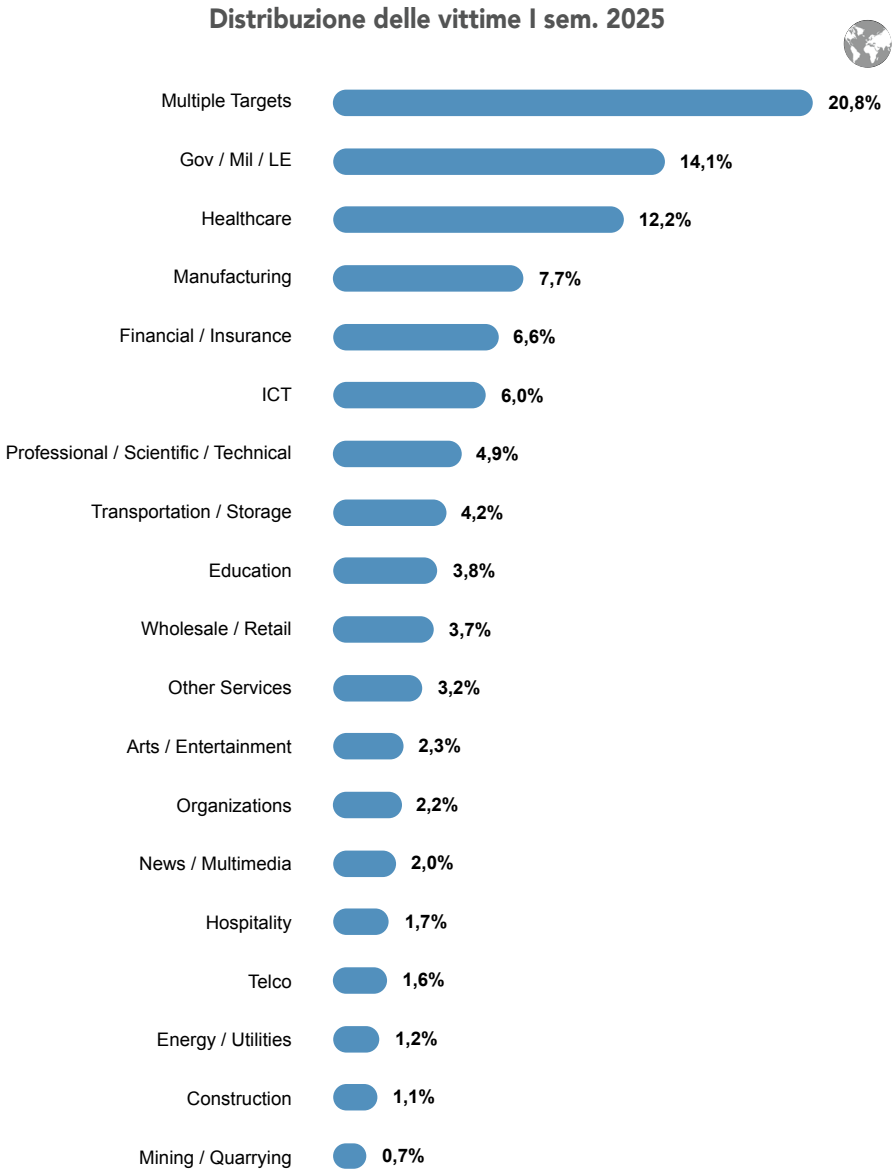


Fig. 5 - Distribuzione della tipologia di vittime nel I semestre 2025

Distribuzione delle vittime per area geografica

1 su 4

sono gli incidenti che avvengono in Europa rispetto al resto del mondo

+121%

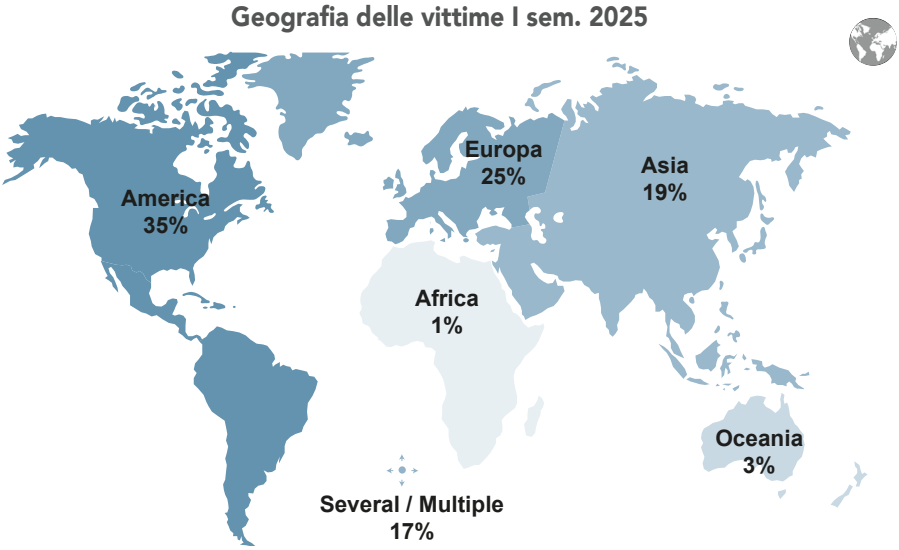
Sono gli incidenti nel continente asiatico nel I sem. 2025 rispetto a tutto il 2024

La lettura dei dati della distribuzione geografica delle vittime rende indirettamente la fotografia di come stiano variando la digitalizzazione e la normazione sui temi legati alla cybersecurity nel mondo, nonché di quali siano i Paesi maggiormente presi di mira dalle operazioni cybercriminali.

Nel primo semestre 2025 (**Fig. 6**) si conferma la preponderanza di vittime nel continente americano (stabile al 35% rispetto al 2024), mentre **gli incidenti verso l'Europa scendono di 5 punti percentuali.**

L'aumento più marcato e degno di nota è verso il continente asiatico che cresce di 7 punti percentuali raggiungendo il massimo picco mai registrato in questo territorio: **nel solo I sem. 2025 in valore assoluto si realizzano più incidenti di quanto avvenuto in tutto il 2024,** 523 eventi (+121%).

Sostanzialmente stabili invece Oceania (3%, -1 p.p.) e Africa (1%), che come sempre occupano posizioni marginali nella nostra classifica, così come gli incidenti verso località multiple (17%).



© Clusit - Rapporto 2025 sulla Cybersecurity - Aggiornamento giugno 2025

Fig. 6 - Distribuzione geografica delle vittime in percentuale nel I semestre 2025

Distribuzione delle tecniche di attacco

Il *Malware* si conferma nel I semestre 2025 la tecnica che genera maggiori incidenti (Fig. 7) ed è utilizzata in circa un quarto dei casi registrati nel nostro campione. Sebbene questa categoria comprenda molte tipologie di codici malevoli, il ransomware è in assoluto quella principale e maggiormente utilizzata grazie anche all'elevata resa economica per gli aggressori. Rispetto alla distribuzione 2024, questa tecnica **riduce la sua magnitudine di 7 punti percentuali rispetto al totale, in favore degli incidenti basati su vulnerabilità, DDoS e Web Attack**, che crescono in numero con maggiore rapidità nel I semestre di questo anno.

1/4

Degli incidenti nel mondo sono causati da attacchi malware

DDOS

è la tecnica che ha il più alto trend di crescita nel I sem. 2025

Gli incidenti basati sullo sfruttamento di vulnerabilità costituiscono come nel 2024 la seconda tecnica più utilizzata, e nei primi sei mesi 2025 si realizzano **un numero di eventi pari all'83% dell'intero 2024.**

In valore assoluto i DDoS crescono in modo più rilevante (in sei mesi si realizzano **l'84% degli incidenti dell'intero 2024**), confermando l'intensificazione del fenomeno dell'Hacktivism, di norma principale detentore di questa tecnica.

In termini di distribuzione percentuale sul totale, il *phishing* risulta stabile rispetto al 2024 (8%) al quinto posto, mentre diminuisce l'utilizzo di tecniche multiple (da 5% a 3%) e Identity Theft / Account Cracking (-3 punti percentuali). Un'ipotesi plausibile di questo fenomeno potrebbe essere la contemporanea spinta di norme che richiedono formazione continua per tutti gli operatori, l'adozione di strumenti efficaci di gestione delle identità (Multi Factor Authentication in primis e, rispetto a quest'ultima, una maggior presenza di questa caratteristica in servizi enterprise), con una maggiore disponibilità a adottare queste soluzioni da parte di molte organizzazioni, consce di quanto il rischio sia alto ma mitigabile.
Aumentano, infine, di un punto percentuale i web attack, che continuano a rappresentare la percentuale minore delle tecniche prese in esame nel nostro campione (in termine di modalità primaria di attacco), anche se in valore assoluto **il dato del I sem. 2025 supera di poco la somma degli eventi dell'intero 2024.**

Nel primo semestre 2025 gli incidenti "undisclosed" costituiscono oltre un terzo del totale (34%): ci auguriamo che maggiori informazioni in corso d'anno permettano di caratterizzare al meglio la natura di questi eventi.

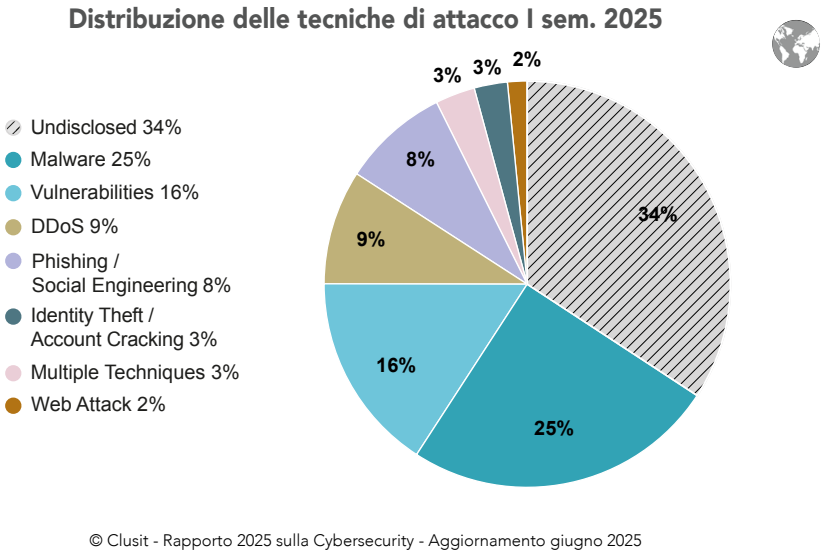


Fig. 7 - Distribuzione delle tecniche di attacco nel I semestre 2025

Analisi della "Severity" degli incidenti

L'analisi della gravità degli incidenti si pone come obiettivo la valutazione degli impatti degli attacchi avvenuti con successo, che non necessariamente corrisponde con la variazione del numero degli eventi, né si può banalmente dedurre dalla vittima o dalla tecnica utilizzata.

Nel I semestre dell'anno in corso (**Fig. 8**), si conferma la tendenza di **crescita consistente della gravità degli incidenti**, in linea con quanto già avvenuto negli anni precedenti.

+143%

è l'aumento degli incidenti con impatto Critico o Alto negli ultimi 5 anni

Se, infatti nel 2024 la quota di attacchi andati a buon fine con impatti gravi o gravissimi si attestava al 77%, a inizio 2025 si arriva all'82%, un chiaro segno che la crescita non accenna a diminuire e che i cybercriminali stiano predisponendo operazioni sempre più sofisticate.

All'interno di questa quota, pur raggiungendo quasi un terzo del totale (29%), gli impatti critici restano sotto il 30%, una tendenza iniziata già nel 2024, mentre gli impatti "high" rappresentano la fetta maggiore (53% del totale).

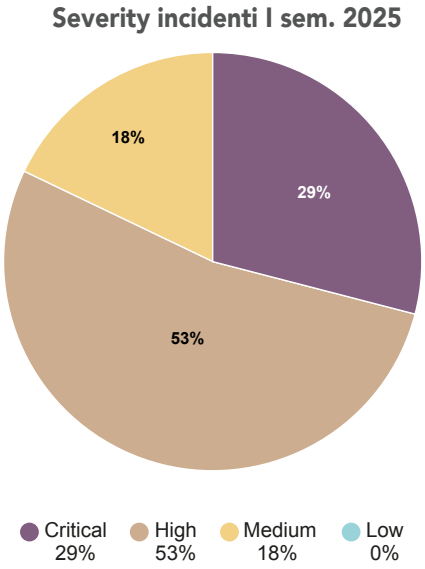


Fig. 8 - Distribuzione della Severity nel I semestre 2025

Pur non minimizzando l'importanza del dato, ci auguriamo che le organizzazioni siano a questo punto maggiormente preparate se non per impedire l'attacco, quanto meno per minimizzarne e contenerne gli effetti.
A conferma della tendenza principale, gli incidenti con severity media diminuiscono di 6 punti percentuali, mentre continuano ad essere praticamente assenti quelli con impatti bassi.

Severity per tipologia di attaccante

In termini di *Severity* degli incidenti per tipologia di attaccante, nella maggior parte dei casi le distribuzioni nel I semestre 2025 (**Fig. 9**) rispecchiano in modo pressoché fedele quelle del 2024 (**Fig. 10**). Si nota facilmente che gli incidenti con matrice *Espionage* e *Information Warfare* sono progettati ed eseguiti per massimizzare i successi degli attaccanti e gli impatti sulle vittime.

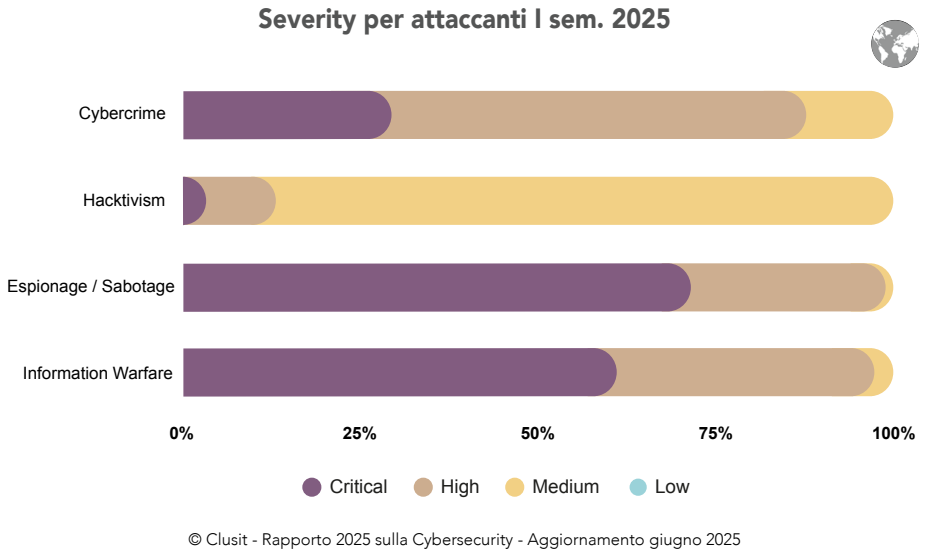


Fig. 9 - Distribuzione della Severity per attaccanti nel I semestre 2025

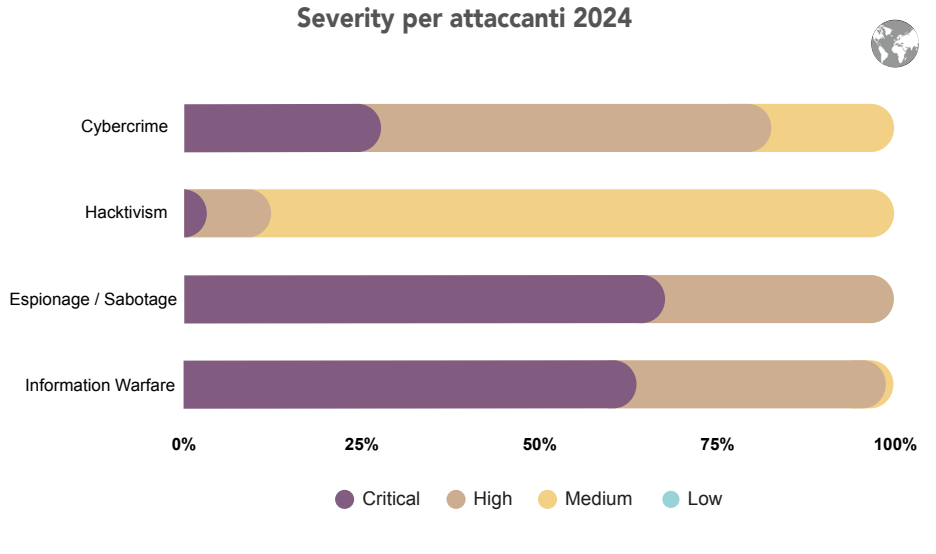


Fig. 10 - Distribuzione della Severity per attaccanti nel 2024

Severity per tipologia di vittima

x2

è l'aumento degli incidenti con severità «critica» rispetto al totale subiti dal settore Healthcare

Dall'analisi della *Severity* per tipologia di vittima tra il primo semestre 2025 (Fig. 11) e l'anno 2024 (Fig. 12) si nota immediatamente **un notevole aumento della severity "critica" nel settore *Healthcare***, che di fatto raddoppia, dimostrando quanto le azioni malevoli contro questo settore siano costruite per massimizzare gli effetti (tipicamente, ottenere un riscatto o generare gravi disservizi) a dispetto del numero di eventi registrati.

Naturalmente saranno i dati consolidati a fine anno a indicare se questa tendenza è stabile. Anche il ***Manufacturing* è oggetto di un aumento notevole di incidenti con impatto critico**, passando dal circa il 20% a circa il 30%, mentre nel caso degli altri settori si confermano sostanzialmente le distribuzioni del 2024.

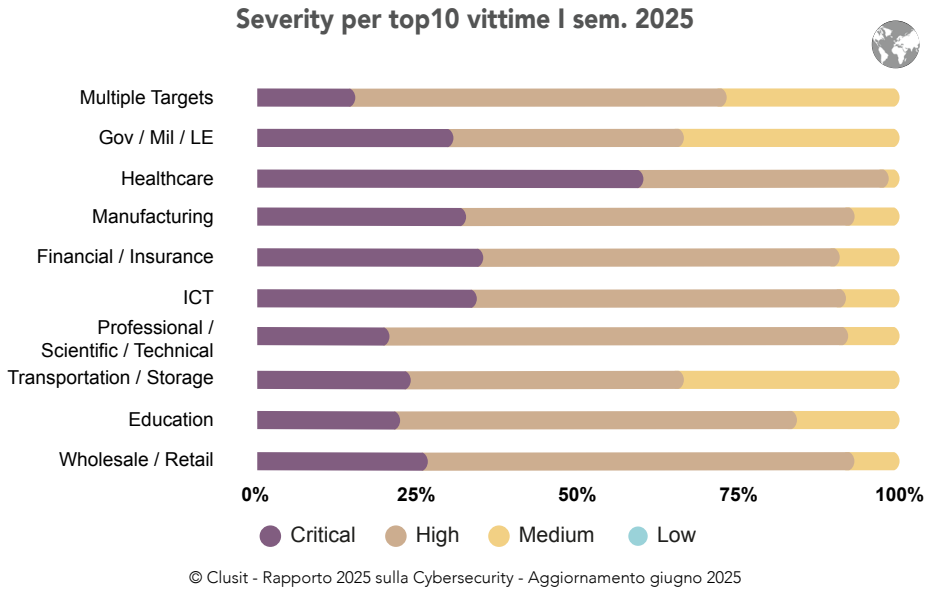


Fig. 11 - Distribuzione della Severity per prime 10 vittime nel I semestre 2025

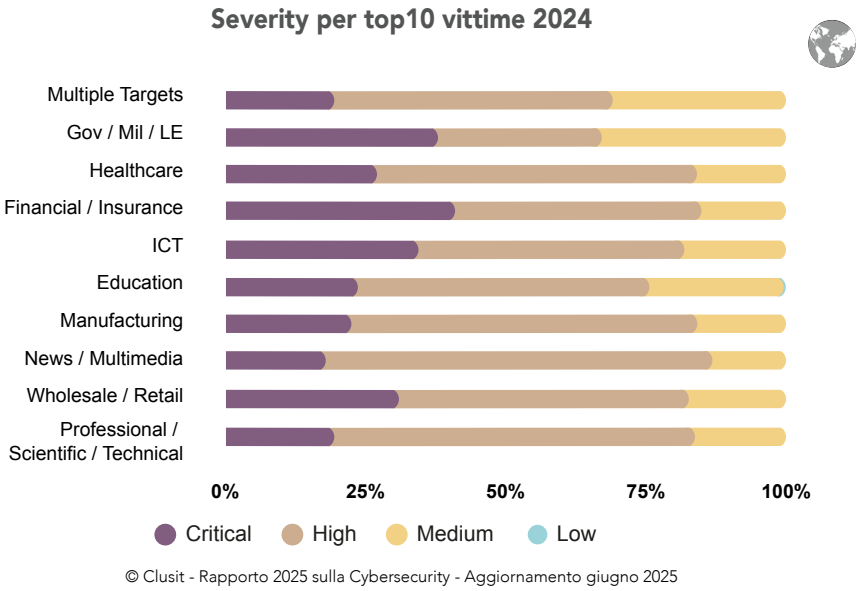


Fig. 12 - Distribuzione della Severity per prime 10 vittime nel 2024

Severity per tecniche di attacco

Analizzando le severity delle tecniche utilizzate, è evidente che, indipendentemente dai numeri assoluti degli incidenti, gli effetti provocati sulle vittime differiscono notevolmente in base alle modalità utilizzate per compere gli attacchi.

Nel primo semestre del 2025 (Fig. 13) **decrescono gli incidenti critici basati su malware** (da circa il 40% del 2024 al 30%) rispetto all'anno precedente (Fig. 14). Una possibile spiegazione potrebbe riguardare il fatto che gli attacchi di questo tipo, particolarmente attenzionati dalle organizzazioni, trovano oggi risposte di contenimento e mitigazione più efficaci di quanto avvenuto in passato.
Una tendenza che si inverte invece nel caso dello sfruttamento delle vulnerabilità, dove **la quota di impatti gravissimi passa da quasi il 30% al 50%.** Ricordiamo a questo proposito che questa tecnica include anche le vulnerabilità zero-day, per cui non esiste di fatto nessuna soluzione, e che sono state ampliamente sfruttate nei primi mesi dell'anno.

Restano sostanzialmente inalterati gli impatti dei DDoS, mentre diminuisce la quota critica di Phishing / Social Engineering, Multiple Techniques e Web Attacks.
Raddoppiano gli impatti critici di Identity Theft / Account Cracking.

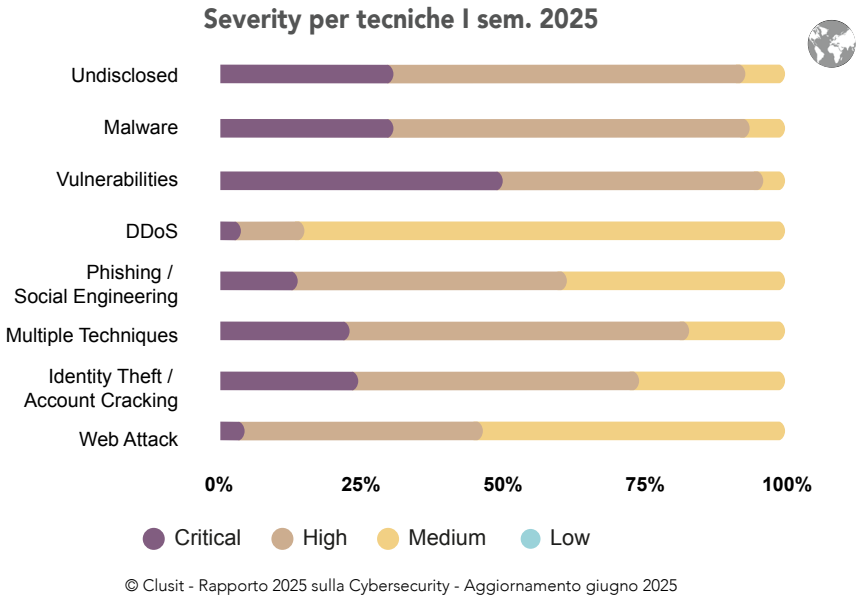


Fig. 13 - Distribuzione della Severity per tecniche di attacco nel I semestre 2025

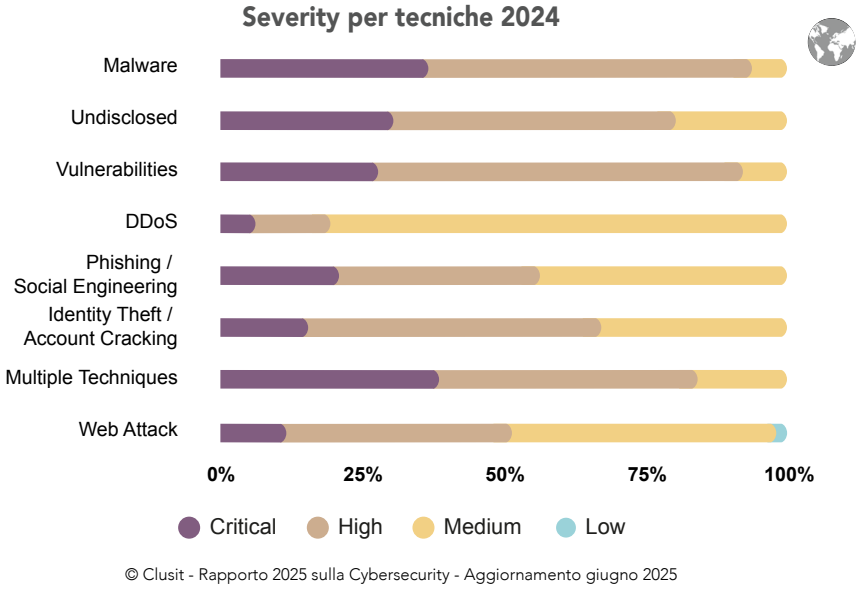


Fig. 14 - Distribuzione della Severity per tecniche di attacco nel 2024

Analisi degli incidenti cyber subiti da organizzazioni governative e dalle Pubbliche Amministrazioni

Il settore pubblico è stato interessato da un importante aumento del numero degli incidenti fra il 2023 e il 2024: questo è spiegabile con l'incremento delle attività dimostrative, di disturbo e di fiancheggiamento legate ai conflitti internazionali in corso, le quali hanno come obiettivi di elezione soggetti legati alle sfere governative e della difesa di quei Paesi considerati avversari. **Tale tendenza è confermata anche nei dati del primo semestre 2025** (Fig. 15).

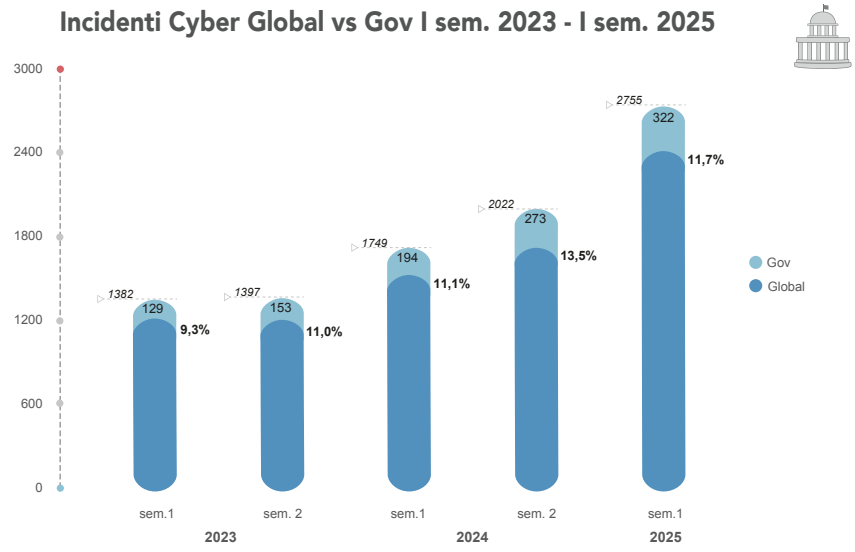


Fig. 15 - Incidenti subiti dal settore GOV (CENTRAL/LOCAL) nel periodo I semestre 2023 - I semestre 2025

~12%
degli incidenti nel mondo avviene contro Pubbliche Amministrazioni centrali e locali

Tra il 2020 e il primo semestre 2025 il campione ha incluso 1.751 eventi noti di particolare gravità che hanno coinvolto realtà governative nel mondo; quelli nel primo semestre 2025 sono stati 322, che corrisponde al **76% degli incidenti analoghi nell'intero 2024.** Il settore incide rispetto al totale degli incidenti del I semestre 2025 di circa il 12%, e tale percentuale risulta in linea rispetto al 2024.

La distribuzione degli attaccanti (**Fig. 16**) mostra che l'incidenza del fenomeno cybercrime in questo primo semestre del 2025 è rimasta grosso modo in linea con quella dell'anno 2024, con circa il 61% di incidenti andati a segno; aumenta invece il fenomeno hacktivism, che in ogni caso si rivolge per propria natura a questo settore con particolare attenzione, con un 35% di incidenti rispetto al 30% registrato nel 2024, in coerenza con l'inasprirsi delle tensioni internazionali in questi primi mesi del 2025.

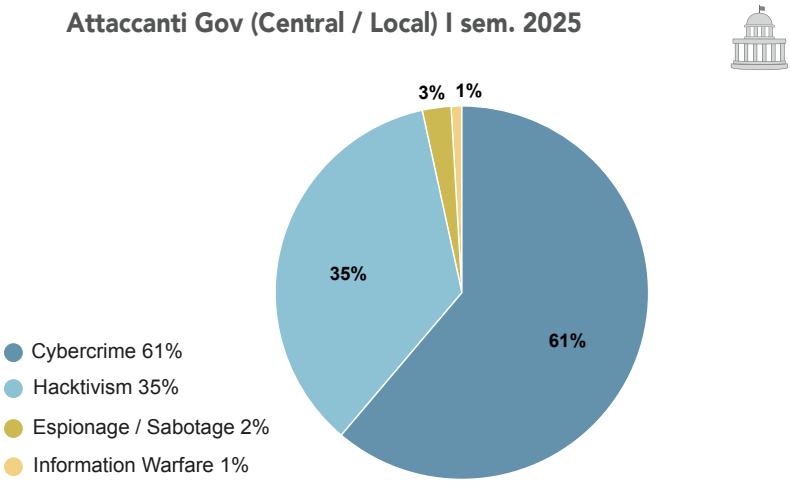


Fig. 16 - Distribuzione degli attaccanti per il settore GOV (CENTRAL / LOCAL) nel I semestre 2025

52%
degli incidenti che colpiscono il settore pubblico avvengono in Europa

La distribuzione geografica delle vittime (**Fig. 17**) mostra che nel primo semestre 2025 **gli incidenti sono cresciuti prepotentemente in Europa, passando al 52% del totale dal 44% registrato nel 2024**; anche qui si legge chiaramente l'effetto dell'inasprimento dei conflitti internazionali in aree limitrofe del continente europeo. L'incidenza rimane invece costante in America e in Africa, mentre in proporzione diminuisce in Asia e in Oceania

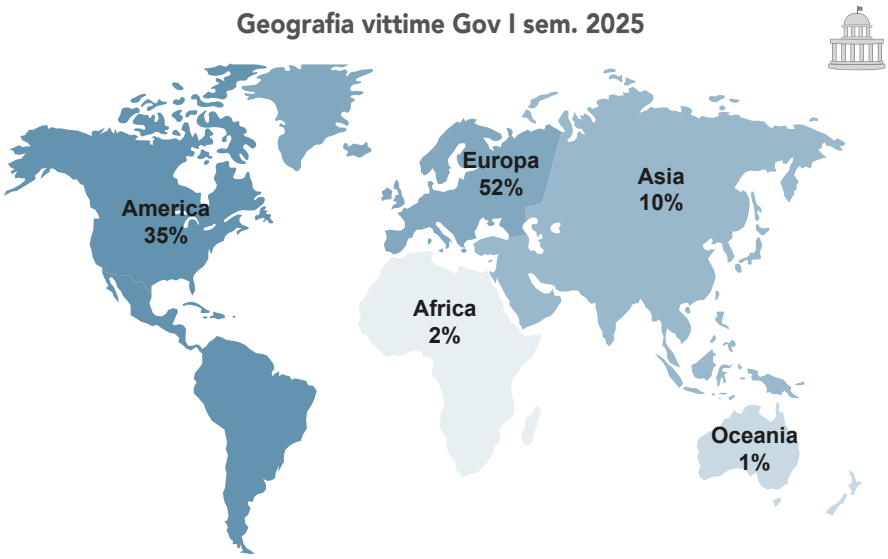


Fig. 17 - Distribuzione geografica delle vittime nel settore GOV (CENTRAL / LOCAL) nel I semestre 2025

DDOS

la tecnica di attacco che causa più incidenti verso le Pubbliche Amministrazioni

Per quanto riguarda le tecniche utilizzate (**Fig. 18**) notiamo che gli incidenti generati mediante DDoS, tipici dei fenomeni di attivismo, i quali erano più che raddoppiati nel 2024 rispetto al 2022, sono ancora cresciuti: nel primo semestre 2025 infatti se ne sono verificati 123, quasi l'80% di quanti se ne sono verificati in tutto il 2024. Da notare tuttavia che gli incidenti di natura non divulgata sono aumentati enormemente: nel primo semestre 2025 pesano per oltre un terzo del totale, contro il meno di un quarto nel 2024, e questo fattore certamente rende più complessa ogni analisi.

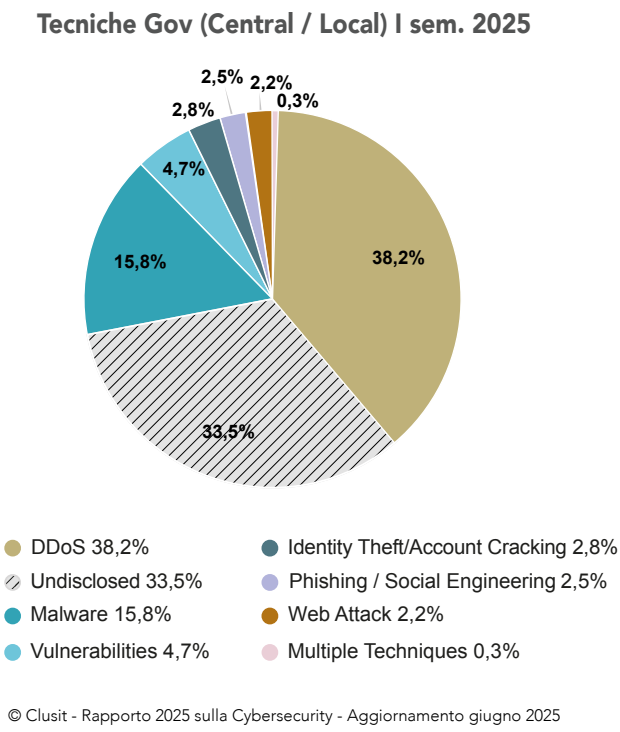


Fig. 18 - Distribuzione delle tecniche di attacco nel settore GOV (CENTRAL / LOCAL) nel I semestre 2025

Analisi degli incidenti cyber in Italia

In questa sezione offriamo un approfondimento sulla situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti negli scorsi 6 mesi, confrontati con l'andamento dal 2020 in poi.

Nel primo semestre 2025 (**Fig. 19**), gli incidenti noti di particolare gravità che hanno coinvolto vittime italiane sono ben **280**. Complessivamente, tra il 2020 e il 2025 il campione ha incluso **1.269** eventi solo nel nostro paese. Come si evince dal grafico in **Fig. 19**, la tendenza degli ultimi 18 mesi definisce un trend di crescita significativa del numero di incidenti: **nel solo I sem. 2025 si sono registrati il 75% degli eventi rilevati nei 12 mesi del 2024.**

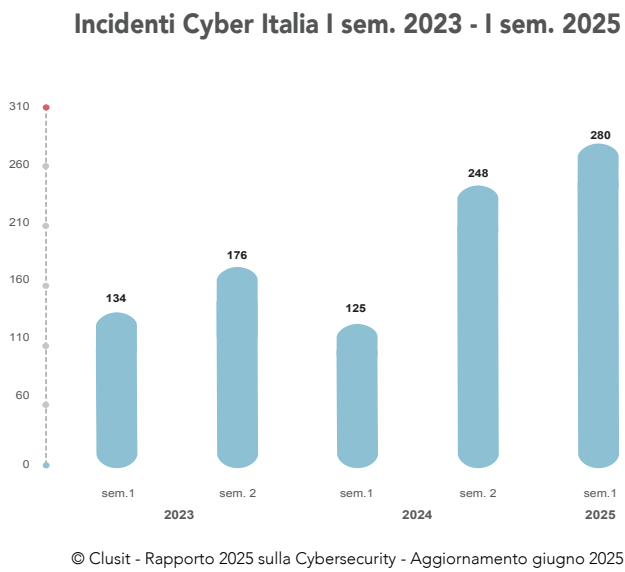


Fig. 19 - Distribuzione degli incidenti in Italia semestre nel periodo I sem 2023 - I semestre 2025

10%+

è la percentuale degli incidenti subiti dalle organizzazioni italiane rispetto al totale mondiale

Nei primi 6 mesi del 2025, **gli attacchi avvenuti con successo contro le realtà del nostro Paese costituiscono il 10,2%** (Fig. 20) **del totale degli eventi rilevati nello stesso periodo a livello mondiale** (2.755). L'incidenza degli incidenti in Italia rispetto al campione complessivo risulta in lieve miglioramento rispetto al secondo semestre 2024 (dove era pari al 12,3%), ma in peggioramento rispetto ai dati rilevati storicamente nello stesso periodo dell'anno (9,6% nel primo semestre 2023 e 7,1% nel primo semestre 2024).

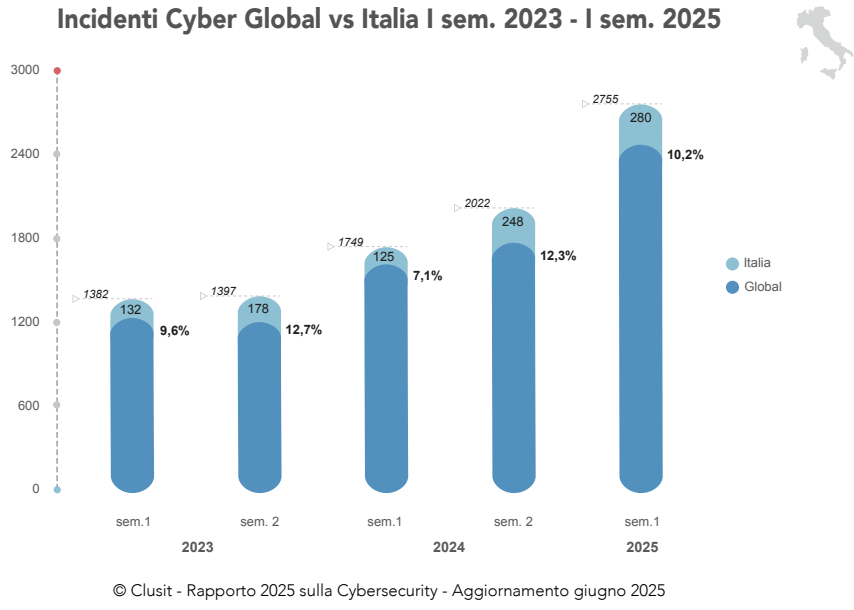


Fig. 20 - Confronto incidenti in Italia vs. Mondo nel periodo I semestre 2023-I semestre 2025

Distribuzione degli attaccanti per tipologia

x1,5
è l'aumento del numero degli incidenti derivanti da Hacktivism in Italia rispetto a tutto il 2024

Per provare a evidenziare alcune tendenze che stanno caratterizzando il panorama degli incidenti e le peculiarità che caratterizzano il nostro Paese, è possibile innanzitutto valutare la tipologia di attaccanti, indicativa delle finalità e propedeutica a capire quali fenomeni prevalenti dobbiamo tenere sotto attenzione (Fig. 21).

1° hacktivism
è la motivazione principale degli incidenti causati in Italia

Tra quelli avvenuti In Italia nei primi 6 mesi del 2025, **la maggioranza degli incidenti noti si riferisce alla categoria *Hacktivism***, che si attesta al 54% superando a livello nazionale il peso percentuale del *Cybercrime*. La tendenza segna una discontinuità netta con ciò che avviene a livello globale, dove l'Hacktivism incide "solo" per l'8% (*vedere Fig. 3*).

Ancora una volta, e più che mai, le organizzazioni italiane risultano quindi particolarmente vulnerabili ad iniziative con finalità dimostrativa, di matrice politica o sociale.

Da sottolineare che il dato 2025 in soli sei mesi rappresenta più di una volta e mezza il totale degli incidenti del 2024.

Il peso percentuale del *Cybercrime* (che nel 2024 rappresentava il 74% del totale degli eventi che avevano interessato l'Italia) diminuisce e raggiunge il 46%, sebbene gli incidenti di questa tipologia siano superiori in valore assoluto a quelli rilevati nello stesso periodo dello scorso anno (130 nel primo semestre 2025 vs 89 nel primo semestre 2024).

Infine, nel nostro Paese non rilevano in modo significativo gli eventi nelle categorie *Espionage / Sabotage* o *Information Warfare*.

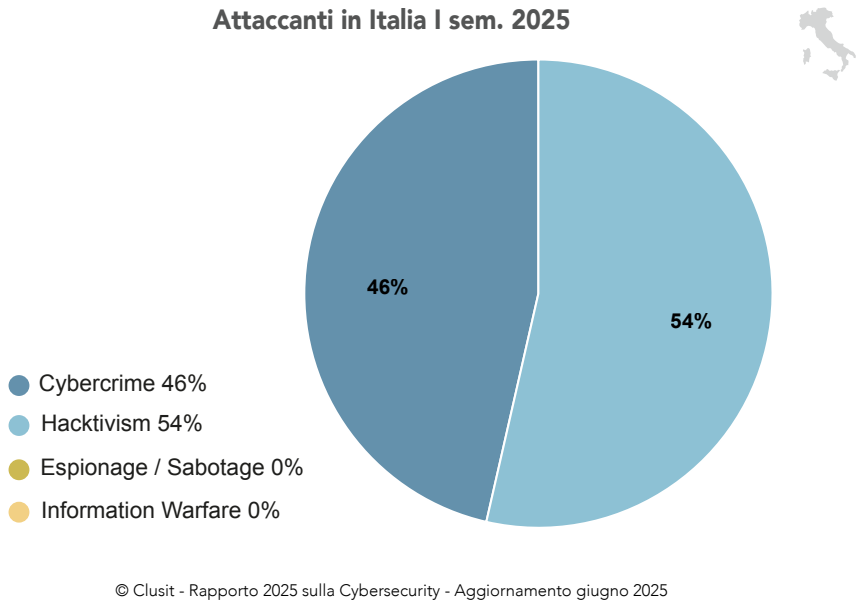


Fig. 21 - Attaccanti in Italia nel I semestre 2025

Come discusso per i dati a livello mondiale, anche in questo caso l'analisi dei singoli incidenti permette di evidenziare sia attacchi con finalità politica specificatamente destinati a enti o aziende del nostro Paese, ma anche situazioni nelle quali le medesime azioni, perpetrate come campagne verso più nazioni, nel bel paese causano conseguenze di maggiore portata (i.e. tale da rientrare nelle statistiche del nostro Rapporto) in relazione alle minori capacità di prevenzione e mitigazione della media delle piccole e medie imprese e pubbliche amministrazioni italiane.

Distribuzione delle vittime per categoria

Guardando alla distribuzione delle vittime (**Fig. 22**), il primo semestre del 2025 in Italia risulta tristemente "vivace" nelle variazioni, che interessano – in positivo o in negativo – pressoché tutti i settori.

x2,8
è l'aumento del numero degli incidenti verso il settore GOV/MIL/LE rispetto a tutto il 2024

L'ambito per cui si rileva un maggior numero di incidenti cyber in Italia è quello *Governativo / Militare / Law Enforcement*, interessato da una significativa quota di eventi, pari al 38% del totale, che in valore assoluto si traduce in una quantità di incidenti pari al 279% rispetto all'intero anno precedente! La crescita rispetto allo stesso periodo dello scorso anno (I sem. 2024) è pari a oltre il 600%.

Questo dato può essere almeno in parte spiegato con l'aumento della pressione del fenomeno Hacktivism nel primo semestre 2025, come visto poc'anzi: gli attacchi di tipo dimostrativo, infatti, sono spesso motivati da finalità politiche o geopolitiche e rivolti, di conseguenza, a vittime nella sfera delle istituzioni pubbliche e militari, che rappresentano un simbolo del potere e dell'autorità di uno Stato. Colpire questo tipo di target, inoltre, genera grande attenzione da parte dell'opinione pubblica, amplificando la visibilità del messaggio che gli attaccanti vogliono veicolare.

x1,5
è l'aumento del numero degli incidenti verso Transportation / Storage rispetto a tutto il 2024

Al secondo posto si trova invece l'ambito *Transportation / Storage* (17% del totale), solo ottavo a livello globale, che **realizza in sei mesi oltre una volta e mezzo il numero degli incidenti di tutto l'anno precedente** e incrementa l'incidenza sul totale del campione, rispetto all'anno precedente, di 10 punti percentuali. Il fatto che questo settore dal 2022 a oggi abbia compiuto un salto rilevantissimo nel numero degli incidenti, salendo rapidamente ai primi posti della nostra triste classifica, può essere ricondotto alla volontà degli attaccanti di mettere in crisi interi settori dipendenti dalle filiere di fornitori di trasporti e logistica, nonché di generare eventi di portata elevata su più filiere di mercato contemporaneamente, limitando la loro capacità di assicurare approvvigionamenti e distribuzione degli stessi. Ciò è verificabile dal fatto che il settore ha subito un'impennata di attacchi di matrice attivista con tecniche DDOS, nonché violazioni ad alcuni soggetti della supply-chain che hanno determinato conseguenze trasverali su più organizzazioni di questo ambito.

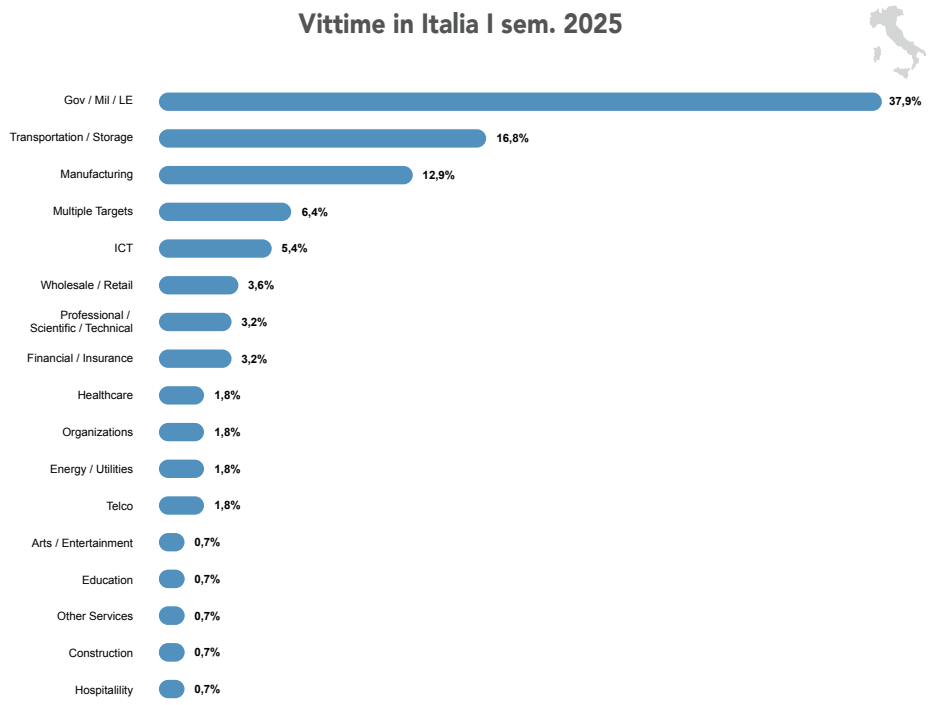


Fig. 22 - Distribuzione delle vittime in Italia I semestre 2025

Il settore *Manufacturing* (13%) che storicamente – vista la peculiarità del tessuto economico del nostro Paese - raccoglie in Italia una quota più significativa di incidenti rispetto al resto del mondo (nella vista globale si ferma infatti all'8%) anche se non risente di un'impennata consistente in termini di crescita del numero degli incidenti come per i due settori che lo precedono.

Proseguendo, restano rilevanti anche nella fotografia italiana gli incidenti che riguardano la categoria *Multiple Targets* (6%), ovvero campagne generalizzate utilizzate per causare attacchi non mirati, che continuano però a generare effetti consistenti e su larga scala, che si trovano al primo posto nella classifica globale. Raccolgono poi il 5% gli eventi che interessano il settore ICT, segno della fragilità delle infrastrutture digitali che, in caso di incidente, può generare un forte impatto a cascata sulle organizzazioni clienti che utilizzano servizi informatici: nel I sem. 2025 si sono verificati pressoché lo stesso numero di incidenti dei 12 mesi precedenti.

Wholesale / Retail scala di tre posizioni la classifica (dal 9° al 6° posto) ed è l'unico settore che registra una crescita statisticamente rilevante di incidenti, considerato che nel semestre si attesta su un numero di eventi pari al 70% dei 12 mesi precedenti. A confronto con i dati del 2024, si segnala una diminuzione gli incidenti rivolti al settore *Healthcare*.

Questi dati definiscono un quadro preoccupante della capacità di protezione sia delle organizzazioni pubbliche sia delle imprese: è evidente che le tecniche di difesa introdotte non sono all'altezza di quelle degli attaccanti e che la presenza di vulnerabilità rende questi obiettivi particolarmente appetibili per gli hacker. È una tendenza da seguire con molta attenzione, che rischia di peggiorare ulteriormente nel prossimo futuro: le tecniche di attacco sono infatti sempre più sofisticate, anche grazie all'utilizzo di Intelligenza Artificiale, ed è necessario che anche le contromisure adottate dalle organizzazioni si adeguino al livello tecnologico degli attaccanti.

Distribuzione delle tecniche di attacco

Anche l'analisi delle tecniche di attacco aiuta a comprendere le cause sottostanti l'elevata crescita degli incidenti subiti dalle nostre imprese e istituzioni.

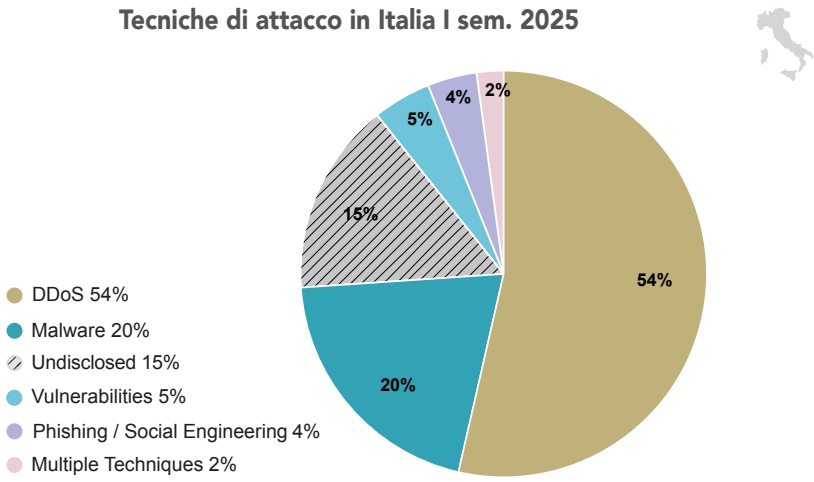


Fig. 23 - Tecniche di attacco in Italia I semestre 2025

DDOS
è la principale tecnica di attacco che causa incidenti in Italia

Come evidenziato dalla Fig. 23, **la tecnica prevalente a causa degli incidenti in Italia è quella dei DDoS**, riprendendosi il primo posto in classifica come già avvenuto nel 2023. Gli incidenti DDoS si attestano al 54%, con un peso significativamente maggiore rispetto a quello occupato a livello globale, dove costituiscono solo il 9% del totale. Ancora una volta, si evidenzia la correlazione con gli incidenti causati da campagne di Hacktivism: molto spesso la tecnica di attacco utilizzata dagli hacktivist è proprio il DDoS, poiché si punta a interrompere l'operatività di servizio dell'organizzazione o istituzione individuata come vittima. Lo scopo degli hacktivist è di innalzare l'attenzione sulla loro causa e l'interruzione di servizi basati su internet può essere un mezzo efficace per rendere evidente al pubblico il proprio messaggio di denuncia o protesta.

1/5
degli incidenti in Italia sono causati da attacchi malware

Seguono le tecniche basate su malware, con il 20% degli eventi, un'incidenza leggermente minore rispetto a quanto rilevato a livello globale (dove costituiscono il 25% del campione). Da sottolineare come in uno scenario di crescita complessiva degli incidenti, **per la prima volta da tempo l'utilizzo di questa tecnica sembra essere lievemente in calo** (da confermare poi con la rilevazione del prossimo semestre): gli incidenti di questa categoria costituiscono circa il 40% degli eventi avvenuti nel 2024, e sono altresì in lieve diminuzione rispetto allo stesso periodo dell'anno precedente (57 incidenti nel I sem. 2025 vs 63 nel I sem. 2024).

Al terzo posto (15%) si trovano gli eventi *Undisclosed* (ovvero quelli per i quali le tecniche utilizzate non sono di pubblico dominio): nonostante le diverse normative che impongono l'obbligo di segnalazione di alcune tipologie di incidenti, molto spesso le informazioni rimangono non note, confermando una tendenza rilevata anche a livello globale.

Proseguendo, si trovano gli incidenti che fanno leva su *Vulnerabilità* (5%), anche questi in valore assoluto in diminuzione (sono solo il 19% del totale degli incidenti dello stesso tipo rispetto a tutto il 2024), e quelli che si basano su tecniche di *Phishing / Social Engineering* (4%).
Completano il campione gli incidenti basati su *Multiple Techniques* (2%).

Analisi della "Severity" degli incidenti

Dal punto di vista della *Severity*, il dato italiano (**Fig. 24**) si distacca da quello internazionale, confermando una tendenza già evidenziata nei nostri Rapporti degli anni passati.

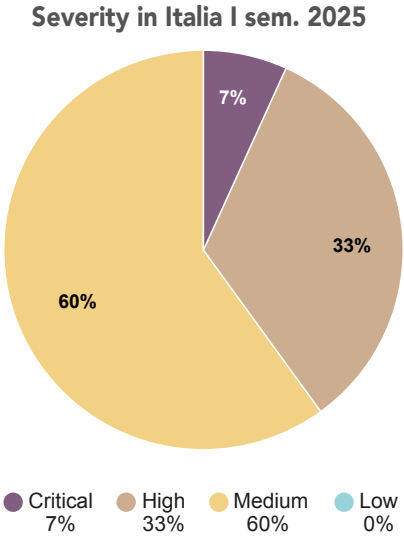


Fig. 24 - Severity degli incidenti in Italia I semestre 2025

Se infatti la quota di *severity* Critical è molto più bassa in Italia che nel resto del mondo (7% contro 29%), così come quella High (33% degli incidenti in Italia e 53% a livello globale), quella degli incidenti di gravità Medium, al contrario, è molto più alta: 60% nel nostro Paese contro 18% complessivo. In generale quindi, appare un segnale positivo: come già riscontrato negli anni passati, **gli attacchi danneggiano in maniera critica molto meno che nel resto del mondo** e, anche se gli incidenti con impatto medio sono molto più numerosi, è pur vero che i loro danni sono più circoscritti.

Rispetto al 2024 (**Fig. 25**), si rileva un ulteriore diminuzione del livello medio di gravità associata agli incidenti del campione italiano. In particolare, mentre la severity Critical rimane pressoché invariata (8% nel primo semestre 2024 vs 7% dello stesso periodo 2025, la severity High passa dal 50% al 33%. All'opposto, la severity Medium cresce dal 41% del campione nel primo semestre 2024 al 60% dei primi 6 mesi del 2025.

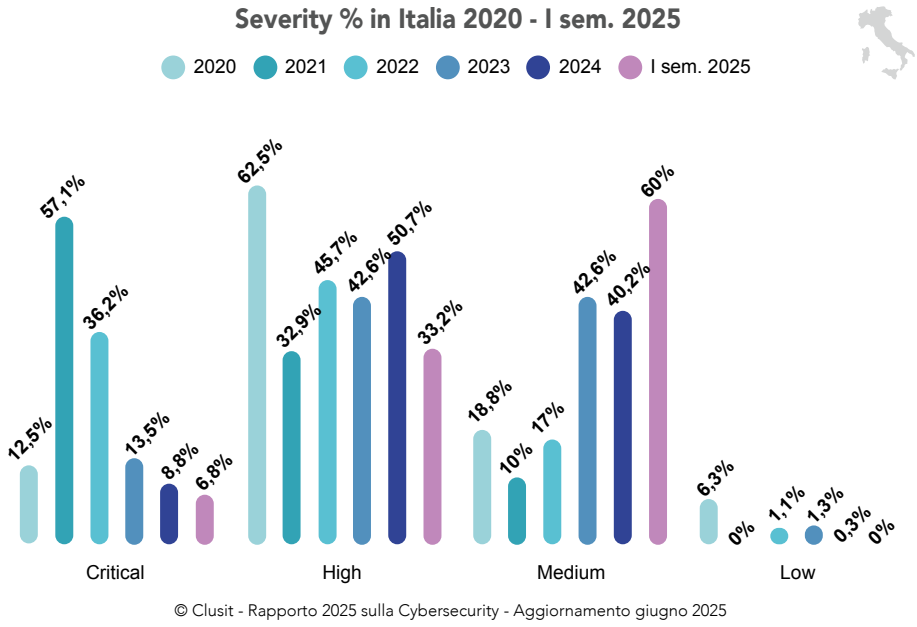


Fig. 25 - Severity degli incidenti in Italia nel periodo 2020 - I semestre 2025

Come ampiamente trattato anche nel Rapporto riferito al 2024, dobbiamo però analizzare queste tendenze nello scenario di insieme, ricordando che gli incidenti italiani costituiscono oltre il 10% del campione mondiale. In tale contesto, le variazioni significative di *severity* sono determinate anche e soprattutto da quegli incidenti che incidono maggiormente in Italia che nel resto del mondo. Partendo da queste considerazioni, asserire che nel contesto italiano la *Severity* media degli incidenti italiani sia minore non è corretto; piuttosto, **i dati suggeriscono che nel nostro paese tutta una serie di attacchi potenzialmente a minore gravità, che negli altri paesi probabilmente tendono mediamente ad essere prevenuti o mitigati in misura maggiore (e quindi non entrano nelle nostre statistiche), in Italia arrivano ad avere gravità *Medium* e, talvolta, *High*** innalzando il bel paese in questo triste ranking internazionale.

Allo stesso modo, come visto anche a livello globale (*Fig. 9*), gli incidenti di categoria Hacktivism che in Italia incidono particolarmente, sono tipicamente associati a **una *severity* mediamente più bassa** (*Medium o High* e più raramente *Critical*).

Un ragionamento analogo vale per le tecniche di attacco. I DDoS, ad esempio, possono generare disagi notevoli alle vittime e ripercussioni sugli utenti, compromettendo la disponibilità di servizio e causando danni in termini sia economici sia reputazionali, ma in genere non presentano conseguenze di particolare gravità nel lungo termine.

Naturalmente, molto dipende anche dalla tipologia di servizio preso di mira: un attacco DDoS a un servizio non particolarmente critico, come un sito web messo fuori uso con finalità dimostrativa, potrebbe avere un impatto relativamente basso, ma è bene ricordare che questa tipologia di incidenti può bersagliare anche servizi o infrastrutture critiche, come reti elettriche o sistemi di comunicazione, generando impatti significativi anche a livello sociale o mettendo a rischio la sicurezza nazionale.

Appendice metodologica

Le decisioni in ambito cybersecurity sono basate principalmente su analisi dei rischi, legate anche a valutazioni di scenario. Che si tratti di attivare o non attivare un servizio, implementare o non implementare un controllo, accettare o non accettare un rischio, a fine giornata il manager dovrà aver preso una decisione, e lo farà con i dati che ha a disposizione. Non decidere è comunque una decisione, di solito la peggiore, e un lusso che il manager non si può permettere. Quello che possiamo fare, come Clusit, è fornirgli i migliori dati che possiamo raccogliere, insieme agli strumenti per valutarne la qualità ed i limiti.

L'analisi dei principali incidenti cyber noti a livello globale si scontra necessariamente con la disponibilità di un campione parziale e non necessariamente rappresentativo dello scenario complessivo di rischio di attacco, che deve comunque essere valutato nel contesto specifico in cui opera una singola organizzazione. Per valutare il valore dei dati raccolti e delle analisi effettuate, è necessario chiedersi prima di tutto quali siano le modalità di raccolta e di analisi, e quali quindi i limiti dei risultati ottenuti.

I dati riportati si riferiscono ad incidenti riportati in fonti di informazione pubbliche. Da quando, nel 2011, è iniziata questa attività, il numero di fonti utilizzato è molto aumentato, e le modalità di ripulitura dei dati, ad esempio dalle duplicazioni, sono migliorate. L'utilizzo di fonti pubbliche introduce comunque un *bias* rispetto alla totalità degli incidenti occorsi e, quindi, all'esposizione ai rischi. In questa sezione cerchiamo di dare una maggiore visibilità a questi possibili bias, in modo che se ne possa tenere conto. Per contro, quando un incidente arriva ad essere pubblicato sulle fonti analizzate, di solito le caratteristiche descritte risultano essere abbastanza affidabili. Quando non lo sono, normalmente le parti interessate tendono a pubblicare o chiedere la pubblicazione di informazioni corrette.

Gli incidenti analizzati rappresentano certamente un campione significativo di quelli resi pubblici dalle fonti principali. Fra quelli resi pubblici, rimangono quindi esclusi incidenti riportati ad esempio da testate minori, locali o di Paesi del mondo non coperti dall'analisi. Nel corso degli anni, è aumentata l'attenzione alla copertura più ampia delle fonti italiane anche minori. In questo senso, possiamo avere quindi un bias verso la rappresentatività dei paesi occidentali maggiormente presenti (ad esempio, gli Stati Uniti) e verso l'Italia. Questo aspetto, se correttamente gestito, può essere più di aiuto che di svantaggio per i manager italiani.

Fra gli incidenti noti pubblicamente, rimangono esclusi quelli che non hanno avuto una rilevanza tale da essere inclusi nelle fonti analizzate. Si tratta per lo più di incidenti di lieve entità, o che interessano aziende di minori dimensioni e che non hanno particolarità tali da renderli di interesse per le fonti principali. Possono essere, ad esempio, attacchi malware di minore entità che, per chi deve gestire la sicurezza di un'organizzazione, probabilmente aggiungono poco rispetto alla valutazione della necessità di adottare una baseline di misure di sicurezza che è ormai da considerare indispensabile.

Ci sono poi incidenti che, pur essendo divenuti noti in contesti circoscritti, non hanno raggiunto le fonti pubbliche. Anche dove vi siano obblighi di notifica, infatti, questo non vuole dire che tutti gli incidenti siano notificati (dipende da caratteristiche dell'incidente e dalla normativa locale e di settore); soprattutto, le autorità in generale non rendono pubblici gli incidenti notificati. Lo stesso per vale per le denunce alle autorità di polizia, alle assicurazioni, e per i dati raccolti dai fornitori di connettività e di servizi di gestione incidenti. Si tratta di dati interessanti, ma in generale disponibili solo a questi soggetti, e quindi molto frammentati. Alcuni li pubblicano a loro volta sotto forma di statistiche. Il Clusit collabora con le autorità ed organizzazioni interessate a pubblicare questi dati all'interno del Rapporto, ma i dati rappresentano comunque viste diverse e più verticali su specifici ambiti, e quindi non sono integrati in questa analisi, ma pubblicati in altre parti del Rapporto, dando loro anche la giusta e specifica visibilità.

Nel campione di questa analisi sono certamente meglio rappresentati gli incidenti realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage, che tendono ad essere condotti con grande cautela e pertanto emergono più difficilmente. Questo può essere un limite importante da considerare: gli attacchi che colpiscono la riservatezza dei dati sono sicuramente sottorappresentati perché, a meno che gli attaccanti per qualche motivo pubblichino l'informazione, le stesse organizzazioni colpite potrebbero non averne evidenza. Si tratta di known unknown rispetto ai quali è difficile avere dati statisticamente significativi.

Anche venendone a conoscenza, le organizzazioni colpite potrebbero avere interesse a non darne evidenza a nessuno. Un tema analogo è legato alle attività di information warfare, che possono essere condotte con altrettanta cautela, anche per non esporre gli strumenti utilizzati[2]. In questi casi, una delle parti potrebbe avere interesse a dare evidenza dell'attacco per motivi di propaganda, ma può essere difficile validare la veridicità di quanto affermato. Dove non vi siano sufficienti conferme sulle caratteristiche dell'attacco, o addirittura sul fatto stesso che l'attacco sia avvenuto, l'attacco non viene incluso nell'analisi.

Nel complesso, quindi, possiamo considerare i dati di questa analisi rappresentativi della maggior parte degli attacchi di grandi dimensioni, con una sottostima difficile da quantificare in termini di attacchi banali o di lieve entità, e di attacchi, come quelli di cyber espionage, che possono facilmente non essere né rilevati né pubblicizzati.

In termini numerici, il campione analizzato è ormai piuttosto consistente, e si può quindi considerare rappresentativo di quanto reso pubblico. Le analisi fatte sul campione stesso danno quindi una rappresentazione chiara di quanto si sa, e possono essere utilizzate dai manager per avere quel quadro della situazione complessiva a livello globale che è sempre più necessario per definire le strategie di un'organizzazione in tema di cyber security.

Un'ultima nota riguarda le variazioni anno su anno. Quelli che analizziamo non sono fenomeni fisici, che hanno una certa regolarità e sui quali variazioni percentuali anche piccole possono, in alcuni casi, essere indicative di tendenze importanti. Qui parliamo di fenomeni influenzati da un numero enorme di parametri. Il fatto stesso che, in talune situazioni, da anno ad anno le variazioni percentuali relative siano tutto sommato limitate per la maggior parte dei valori, seppure in un contesto di generale aumento, depone a favore della qualità complessiva dei risultati, e dà anzi maggior valore alle variazioni più evidenti ed ampie. È quindi utile focalizzarsi su queste ultime e sull'andamento complessivo, piuttosto che su piccole fluttuazioni annuali. Per questo, nella nostra metodologia abbiamo aumentato l'attenzione ai fenomeni più significativi, riducendo la disamina di singole variazioni meno rilevanti.

[2] Salvo quando vengano esposti per errore, come nel caso di Stuxnet

Attività e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica nel primo semestre 2025

Dal dato digitale alla resilienza: analisi, prevenzione e contrasto nella sicurezza cibernetica

Il primo semestre del 2025 ha rappresentato per il Servizio Polizia Postale e per la Sicurezza Cibernetica un periodo di intensa attività, in cui la quotidianità operativa si è intrecciata con la necessità di guardare oltre l'immediato, anticipando scenari e predisponendo strumenti adeguati a fronteggiarli.
La dimensione digitale, ormai parte integrante della vita sociale, economica e istituzionale del Paese, ha imposto un approccio che non può più limitarsi alla gestione dell'emergenza, ma che deve fondarsi su un equilibrio tra prevenzione, contrasto e costruzione di competenze.

La complessità delle minacce emerse in questi mesi ha richiesto un'avanzata capacità di analisi, indispensabile per interpretare fenomeni in continua trasformazione; una rapidità di risposta, necessaria per contenere gli effetti di attacchi e incidenti; e una costante capacità di operare in sinergia, sia all'interno della rete territoriale della Polizia di Stato, sia nel dialogo con istituzioni, imprese e cittadini. Non si è trattato soltanto di affrontare singoli episodi criminali, ma di trasformare ogni intervento in occasione di apprendimento, così da rafforzare progressivamente la resilienza complessiva del sistema Paese.

In questo quadro, la gestione del dato digitale si è confermata elemento centrale. Il dato non è stato considerato soltanto come prova giudiziaria, ma anche come risorsa preventiva, capace di orientare le indagini, anticipare le minacce e indirizzare le strategie di protezione. La solidità delle procedure di acquisizione, conservazione e analisi ha reso possibile un'azione investigativa affidabile e tempestiva.

I risultati del semestre lo dimostrano: migliaia di attacchi informatici sono stati gestiti e neutralizzati; centinaia di alert di sicurezza sono stati diramati a soggetti pubblici e privati; il CNCPO ha condotto operazioni complesse contro reti criminali transnazionali dedite alla diffusione di materiale pedopornografico; mentre sul fronte della tutela dei cittadini, migliaia di segnalazioni di truffe online hanno dato luogo a indagini e campagne di prevenzione. Il Commissariato di PS Online, con la sua funzione di presidio digitale per la sicurezza, ha rappresentato un punto di contatto diretto con la collettività, raccogliendo segnalazioni, orientando le vittime e diffondendo consigli di sicurezza.

Accanto ai risultati conseguiti, in questi mesi hanno preso forma iniziative che guardano con decisione al futuro. Tra queste, la più significativa è la preparazione del corso per vice ispettori tecnici del settore della sicurezza cibernetica, primo del suo genere, il cui avvio è programmato per settembre 2025. Si tratta di un percorso formativo di nove mesi, concepito per dare vita a figure professionali capaci di coniugare la tradizione della polizia giudiziaria con le competenze tecniche più avanzate. L'organizzazione di questo corso, che nel primo semestre del 2025 ha richiesto un impegno intenso e mirato, rappresenta un investimento strutturale e un vero punto di svolta: un passo destinato a rafforzare in modo duraturo la capacità di presidio del cyberspazio e a colmare la distanza tra tecnologia e indagine.

A sostenere questa evoluzione contribuisce in modo determinante la rete territoriale della Polizia Postale, composta da diciotto Centri Operativi a livello regionale e ottantadue Sezioni a livello provinciale. Questa articolazione garantisce prossimità, ascolto e continuità di intervento, trasformando le linee guida diramate dai vertici dipartimentali in azioni concrete sul territorio. La presenza capillare consente di intercettare segnali deboli, supportare gli uffici giudiziari e mantenere un contatto diretto con le comunità locali, rafforzando così la capacità di prevenzione e di risposta.

Fondamentale, inoltre, il partenariato pubblico–privato, che ha reso più rapido e ordinato lo scambio di informazioni con imprese, operatori di servizi essenziali e mondo accademico. La collaborazione ha permesso di condividere tempestivamente indicatori di compromissione, tattiche e tecniche emergenti, riducendo i tempi di contenimento e migliorando la capacità di ripristino dei servizi. Questa fiducia reciproca, costruita nel tempo, è ormai parte integrante della strategia di prevenzione e rappresenta un valore aggiunto per la sicurezza complessiva del Paese.

In questo contesto si collocano i contributi delle cinque divisioni del Servizio, che offrono una visione articolata e complementare del lavoro svolto.

La Prima Divisione delinea il quadro strategico, curando la formazione, la pianificazione delle risorse, le campagne di prevenzione e le relazioni internazionali. La Seconda si concentra sulla tutela dei minori e sulla prevenzione dei reati contro la persona in rete, coordinando il Centro Nazionale per il Contrasto alla Pedopornografia Online e l'Unità di Analisi del Crimine Informatico, anima psicologica dell'azione preventiva e repressiva della Polizia Postale. La Terza affronta la protezione delle infrastrutture critiche e la prevenzione delle minacce eversivoterroristiche, valorizzando anche lo sviluppo di soluzioni tecnologiche e forensi, attraverso l'operatività del Centro Nazionale per le Protezione delle Infrastrutture Critiche. La Quarta Divisione si occupa del contrasto al *financial cyber crime* e alle frodi digitali, con particolare attenzione alle truffe online e

ai reati postali, in raccordo con gli operatori del settore. La Quinta, infine, assicura la componente tecnica e di supporto specialistico, garantendo coerenza metodologica e continuità operativa. L'insieme di questi elementi restituisce un quadro unitario, in cui analisi, prevenzione e contrasto si intrecciano in un'unica trama. È in questa coralità, fatta di competenze diverse ma complementari, che si misura la capacità del Servizio di affrontare le sfide del cyberspazio e di tradurre la strategia in azione quotidiana al servizio del Paese.

La Prima Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La Prima Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica rappresenta il centro di regia dell'intera Specialità. In questa sede vengono tracciate le linee di indirizzo, pianificate le risorse e sviluppate le attività di formazione, prevenzione, cooperazione internazionale, affari giuridici e analisi dei dati, così da assicurare continuità e coerenza all'azione complessiva del Servizio. È una funzione che non si limita a coordinare, ma che garantisce uniformità operativa su tutto il territorio nazionale, traducendo le direttive centrali in pratiche concrete. Allo stesso tempo, la Divisione cura i rapporti con le istituzioni, mantiene un dialogo costante con gli organismi internazionali e promuove campagne di sensibilizzazione rivolte a cittadini e imprese, rafforzando la cultura della sicurezza digitale e consolidando la fiducia collettiva nelle istituzioni. In questo quadro si inserisce il Commissariato di P.S. online, accessibile all'indirizzo www.commissariatodips.it, che costituisce il presidio telematico di prossimità della Polizia Postale, offrendo ai cittadini uno spazio digitale sicuro e diretto per segnalare reati, ricevere assistenza e accedere a strumenti di prevenzione senza doversi recare fisicamente in un ufficio di polizia.

La formazione specialistica è uno degli elementi più qualificanti della missione della Divisione. Non si tratta di percorsi teorici, ma di programmi costruiti a partire dall'analisi dei dati e dall'osservazione dei fenomeni criminali. Le informazioni raccolte attraverso il monitoraggio delle minacce digitali e le segnalazioni dei cittadini vengono trasformate in contenuti didattici e in percorsi di alta specializzazione, così da fornire agli operatori strumenti aggiornati e metodologie aderenti alle sfide reali. Nel 2025 è previsto l'avvio, a settembre, del corso per vice ispettori tecnici del settore della sicurezza cibernetica, pensato per rafforzare le competenze di comando e coordinamento nelle indagini digitali. A questo si affiancano i numerosi corsi OSINT e di analisi del traffico di dati telematici e telefonici, i corsi per operatori cyber e quelli dedicati al contrasto della pedopornografia online. L'insieme di questi percorsi compone un'offerta formativa coerente e progressiva, che unisce la tradizione della

polizia giudiziaria alle competenze tecniche più avanzate, mettendo ogni operatore nelle condizioni di affrontare il cyberspazio con preparazione e consapevolezza.

L'attività di analisi costituisce il nucleo strategico della Divisione. Attraverso l'elaborazione di indicatori e scenari previsionali è possibile orientare le priorità investigative, anticipare le minacce emergenti e calibrare l'impiego delle risorse. Questo approccio, fondato sui dati, non solo rafforza la capacità di risposta operativa, ma alimenta anche la progettazione delle campagne di prevenzione e la definizione dei contenuti formativi, creando un circuito virtuoso tra conoscenza, azione e comunicazione.

Come anticipato nella premessa, il Commissariato di P.S. online si inserisce pienamente in questo sistema. Nel primo semestre 2025 sono state gestite 45.762 segnalazioni complessive, di cui oltre 15.000 relative a *phishing*, più di 14.000 a contenuti e abusi sui social, circa 14.400 a episodi di *hacking* e oltre 1.000 a casi di pedopornografia online. A queste si aggiungono 681 segnalazioni di matrice antiterrorismo, che confermano la centralità del portale anche nella prevenzione delle minacce più gravi. Parallelamente, sono state evase 12.954 richieste di informazioni da parte dei cittadini. L'impatto del sito è testimoniato anche dai numeri di fruizione: nello stesso periodo si sono registrate quasi 2 milioni di visite con oltre 32 milioni di pagine consultate, con una crescita costante mese dopo mese. A ciò si aggiungono 962 segnalazioni inoltrate tramite social network, 21 richieste di soccorso pubblico direttamente dal sito e 139 casi gestiti in collaborazione con i media, oltre a 15 alert di sicurezza diffusi per avvisare tempestivamente la collettività di minacce emergenti.

Accanto a questa attività di prossimità digitale, la Divisione è impegnata nella progettazione e realizzazione delle campagne di prevenzione, che rappresentano un lavoro corale e sinergico tra tutte le sue componenti. La complessità dinamica della minaccia cibernetica che investe bambini e ragazzi in rete richiede una professionalizzazione progressiva e multidisciplinare del personale della Polizia Postale chiamato giornalmente a incontrare i ragazzi nelle scuole. Per garantire uniformità, standardizzazione e correttezza scientifica a questi interventi sono state stilate e diffuse presso il personale le Linee Guida "A SCUOLA TUTTO BENE?", redatte dagli psicologi dell'UACI, in collaborazione con criminologi e ricercatori, sotto la supervisione scientifica della Facoltà di Psicologia dell'Università Sapienza di Roma.

Nel primo semestre 2025, la campagna itinerante "Una Vita da Social" ha coinvolto oltre 247.000 studenti, 17.000 docenti e 14.000 genitori, consolidando il suo ruolo di progetto educativo di riferimento. L'evento "#CuoriConnessi", organizzato in occasione del Safer Internet Day, ha visto la partecipazione di 1.200 studenti in presenza e oltre 230.000 collegamenti in streaming. Il progetto editoriale "Sulle Tracce

dell'Hacker", realizzato in collaborazione con la "Fondazione Geronimo Stilton", ha raggiunto migliaia di alunni delle scuole primarie con la distribuzione complessiva di 12.000 copie del volume grazie alla collaborazione con Google. Proprio quest'ultima iniziativa ha ottenuto un prestigioso riconoscimento internazionale: nel maggio 2025, alla quarta edizione del World Police Summit di Dubai, la Polizia Postale ha ricevuto il primo premio nella categoria "Excellence in Customer Service in Policing Award", a conferma del valore educativo e sociale del progetto e della capacità di costruire modelli di prevenzione innovativi grazie alla collaborazione tra pubblico e privato.

Un ulteriore fronte di impegno è rappresentato dalla partecipazione al progetto europeo STARLIGHT, dedicato allo sviluppo di strumenti di intelligenza artificiale a supporto delle forze di polizia. Nel 2025, presso il Compendio Tuscolano di Roma, la Divisione ha organizzato un evento operativo che ha visto la presentazione e la dimostrazione di tool innovativi sviluppati nell'ambito del progetto, in collaborazione con Europol e numerosi partner internazionali. L'iniziativa ha confermato come l'intelligenza artificiale stia diventando un alleato imprescindibile delle forze dell'ordine, capace di rafforzarne le capacità investigative e di prevenzione, e al tempo stesso uno strumento da presidiare con attenzione per contrastarne l'uso distorto da parte della criminalità comune e organizzata.

L'insieme di queste attività dimostra come l'analisi dei fenomeni, la formazione del personale, la prevenzione rivolta alla collettività, l'innovazione tecnologica e l'interazione diretta con i cittadini attraverso il Commissariato online siano parti di un unico disegno strategico. **I dati orientano le scelte, le scelte guidano la formazione, la formazione sostiene le campagne, e le campagne restituiscono nuove evidenze da analizzare.** Attraverso questa funzione di regia integrata, il Servizio riesce a garantire che l'azione non sia la somma di singole attività, ma un sistema coeso e dinamico, capace di prevenire, contrastare e comunicare in maniera efficace le minacce digitali, rafforzando la sicurezza nazionale e consolidando la fiducia dei cittadini nelle istituzioni.

La Seconda Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La Seconda Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica è il presidio dedicato alla **tutela dei minori e alla prevenzione dei reati contro la persona in rete**, ambiti che toccano in modo diretto la sfera più sensibile della collettività. La sua missione si concentra sul contrasto alla pedopornografia online, alla diffusione di contenuti illeciti e alle condotte predatorie che sfruttano la vulnerabilità

dei più giovani, con un impegno costante a proteggere l'infanzia e a garantire un ambiente digitale più sicuro.

Elemento centrale dell'attività è il **Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO)**, che agisce come punto di riferimento nazionale e internazionale per la raccolta, l'analisi e la condivisione delle segnalazioni.

Accanto al Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), opera l'Unità di Analisi del Crimine Informatico (UACI), struttura unica nel suo genere che integra competenze tecniche e psicologiche. L'UACI, composta da funzionari psicologi specializzati, supporta l'attività investigativa nelle sue fasi più complesse (audizioni, perquisizioni domiciliari, interrogatori di minori autori di reati cibernetici) ed elabora profili criminologici di autori di reato, contribuendo a orientare le indagini. Allo stesso tempo offre supporto psicologico e ascolto agli operatori impegnati nelle attività più delicate, come quelle contro lo sfruttamento sessuale dei minori online e l'antiterrorismo, garantendo equilibrio e resilienza a chi è quotidianamente esposto a contenuti traumatici.

La Divisione svolge inoltre un ruolo di **coordinamento nazionale**, assicurando indirizzo operativo e metodologico alle attività dei Centri Operativi territoriali e mantenendo un costante raccordo con le Autorità giudiziarie, le istituzioni internazionali e le principali organizzazioni non governative impegnate nella protezione dei minori.

Attraverso indagini complesse, operazioni coordinate e campagne di sensibilizzazione rivolte a scuole, famiglie e comunità, la Seconda Divisione contribuisce a rafforzare la consapevolezza collettiva e a costruire una cultura della sicurezza digitale, trasformando la prevenzione in uno strumento di protezione concreta per le nuove generazioni.

Il Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO)

La protezione delle vittime vulnerabili e la tutela dei diritti di bambini e adolescenti rappresentano una priorità per la Polizia di Stato e richiedono un'attenta valutazione delle minacce emergenti, l'impiego di tecnologie innovative e un approccio metodologico e operativo in linea con lo sviluppo dei mezzi di comunicazione che possa consentire nuove prospettive in termini di conoscenza e interazione sociale.

Le competenze della Specialità in materia di tutela dei minori si sono ampliate nel tempo grazie a disposizioni normative volte a rafforzare il sistema di protezione e estese a ambiti e servizi della rete presso i quali, negli anni, si sono riversate quantità

crescenti di minori di età sempre più precoce, con una sorveglianza da parte degli adulti non sempre adeguata. Si pensi a fenomeni come il *cyberbullismo* che continua a mutare, aggredendo bambini e ragazzi in "luoghi virtuali" sempre diversi e secondo modalità pervasive e violente.

In qualità di organo del Ministero dell'Interno, il Servizio Polizia Postale e per la Sicurezza Cibernetica ha competenze istituzionali esclusive, sancite dalla normativa istitutiva del Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), incaricato della prevenzione e repressione dei reati legati allo sfruttamento sessuale dei minori sul web (legge 6 febbraio 2006, n. 38), competenze ampliate dal decreto del Ministro dell'Interno 15 agosto 2017 - Direttiva sui comparti di specialità delle Forze di Polizia e sulla razionalizzazione dei presidi di polizia. In un'ottica di prevenzione e contrasto delle varie forme di aggressione e abuso di minori online, sono stati emanati diversi provvedimenti normativi per la loro tutela (es. legge 29 maggio 2017, n. 71, *Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo*, così come modificata dalla legge 17 maggio 2024, n.70, *Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e cyberbullismo*), volti a creare una rete strutturata e coordinata di intervento che fornisca un supporto tempestivo alle vittime.

Per svolgere queste funzioni, il Servizio impiega avanzate tecniche investigative e assicura il coordinamento internazionale con le forze di polizia estere, oltre a coordinare e dare supporto a livello nazionale ai 18 Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) e alle 82 Sezioni Operative (S.O.S.C.) della Polizia Postale. Nell'ambito della previsione normativa di cui alla legge n. 38/2006 – art.19, che affida al CNCPO il compito esclusivo di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati, relative alla presenza di contenuti di pornografia minorile nel *web*, nel corso del 2024, sono stati intensificati i rapporti con le associazioni impegnate nella protezione dei minori, strutturando la funzionalità operativa a logiche efficaci e inclusive di 'partenariato pubblico e privato'. Tra questi: *Telefono Azzurro*, *Save The Children*, *Terres Des Hommes*, *Operation Underground Railroad Rescue*, *National Centre for Missing and Exploited Children*, *Child Rescue Coalition* (C.R.C.) e l'*Associazione Meter di don Fortunato di Noto,* la *Comunità di Sant'Egidio*.

La Polizia Postale partecipa a numerosi tavoli di lavoro interistituzionali per la protezione dei minori, tra cui il *Safer Internet Center Italy*, in collaborazione con il Ministero dell'Istruzione e del Merito, l'*Osservatorio Nazionale per l'Infanzia e l'Adolescenza* e l'*Osservatorio per la Prevenzione e il Contrasto della Pedofilia e della Pornografia Minorile*, promosso dal Ministero della Famiglia. Inoltre, il *Gruppo di Lavoro sulle Sfide*

e Opportunità del Gaming, istituito dal Dipartimento per la Trasformazione Digitale, dimostra come la complessità di questi fenomeni richieda un approccio sinergico per una comprensione e gestione efficace.

In considerazione della dimensione transnazionale di questi reati è stato rafforzato attraverso gli uffici di *Europol* e *Interpol* anche lo scambio di informazioni nei canali di cooperazione internazionale con l'obiettivo di promuovere a livello nazionale un'azione coordinata da parte degli Uffici della Polizia Postale e per la Sicurezza Cibernetica, per individuare autori e vittime di abusi.

Nel corso del 2025, il Centro è intervenuto attivamente nella definizione, per il Ministero dell'Interno, della proposta di Regolamento del Parlamento europeo e del Consiglio, che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale dei minori, intensificando, tra l'altro, l'impegno dei fornitori di connettività nella rilevazione, blocco e segnalazione di materiale pedopornografico. Il CNCPO ha fornito periodicamente alla Commissione europea contributi di natura tecnica, basati sull'esperienza acquisita nel corso degli anni nel settore, per indirizzare, per quanto di competenza, l'attività legislativa in atto, in un'ottica di bilanciamento tra l'interesse individuale alla riservatezza delle comunicazioni telematiche e l'interesse delle forze di polizia ad avere accesso a informazioni utili alle attività investigative.

Il Centro ha partecipato a diversi *tavoli di lavoro internazionali*, tra cui il gruppo di lavoro G7 per il contrasto alla pedopornografia all'interno dell'*High Tech Crimes Sub-Group* e il sottogruppo di lavoro G7 *Law Enforcement Practioners*, nell'ambito dei quali sono state portate avanti iniziative finalizzate all'implementazione dei canali di cooperazione internazionale di polizia per la protezione dei minori.

Nel contesto della cooperazione internazionale di polizia, il CNCPO ha preso parte a significativi *meeting* e T*ask Forces* operativi, quali la *Victim Identification Task Force*, volta all'identificazione degli autori di abusi sessuali ai danni di minori e delle vittime, la *High Value Targets Task Force*, che si propone l'obiettivo di deanonimizzare i membri delle comunità virtuali di pedofili attive nel *darkweb* e il *Global Covert Internet Investigations Meeting*, durante il quale esperti investigatori dei diversi Paesi condividono le tecniche investigative e le buone prassi utilizzate nell'ambito delle indagini *under cover online* per il contrasto allo sfruttamento sessuale dei minori sul *web*.

Il personale del Centro è periodicamente avviato a corsi formativi di aggiornamento tecnico professionale, anche a livello europeo promossi dall'Agenzia dell'Unione europea per la formazione delle autorità di contrasto CEPOL.

Nel 2025 l'attenzione nella lotta contro la diffusione di contenuti illeciti online è stata rivolta al potenziamento del monitoraggio dei siti web che diffondono materiale CSAM (*child sexual abuse material*), attraverso l'Area Operativa 'Black List' del CNCPO. Questo sforzo ha portato alla sorveglianza di 7.826 siti web segnalati e all'inserimento di 2.821 di questi nella cosiddetta *black list*.

L'identificazione delle vittime è una priorità e viene affidata a un'unità investigativa specializzata che, seguendo le linee guida internazionali, analizza e gestisce i file multimediali illeciti attraverso la Banca Dati I.C.S.E. (*International Child Sexual Exploitation Database*), accessibile tramite *Interpol* e alimentata dalle segnalazioni delle forze di polizia di tutto il mondo.

A tale settore affluiscono anche le informazioni fornite dall'*Unità di Informazione Finanziaria* (U.I.F.) della Banca d'Italia che segnalano transazioni sospette legate alla vendita di materiale pedopornografico sul web, utili per approfondimenti investigativi.

Grazie agli strumenti normativi che permettono indagini sotto copertura online, sono state condotte operazioni nel *Dark Web* e nel *Deep Web* per contrastare lo sfruttamento sessuale dei minori tramite sistemi informatici. Gli Uffici territoriali hanno ricevuto supporto tecnico-investigativo dal CNCPO, che ha cooperato con agenzie estere per lo scambio di informazioni e buone pratiche, inclusa la gestione di operazioni internazionali sotto copertura.

Pedopornografia e adescamento - anno 2024

CNCPO	Primi semestre 2024	Primo semestre 2025
Casi trattati	1.418	1.383
Persone arrestate	62	148
Persone indagate	557	648
Perquisizioni	532	604
Siti in Black List	2.759	2.821
Siti visionati	15.170	7.826

Fonte: Polizia Postale e per la sicurezza cibernetica © 2025

Nel raffronto tra il primo semestre 2025 e quello del 2024, i dati elaborati dal Centro Nazionale per il Contrasto alla Pedopornografia delineano un quadro che, sotto il profilo investigativo e repressivo, presenta andamenti tra loro disomogenei, con significative implicazioni in termini di risposta giudiziaria e capacità di presidio del fenomeno.

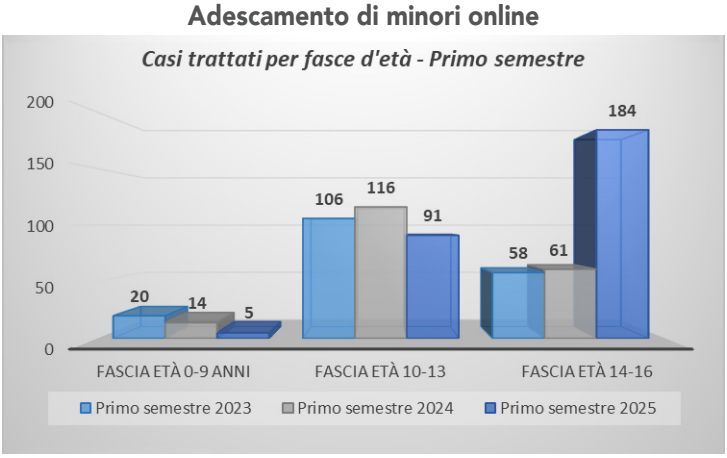
In primo luogo, il numero complessivo dei casi trattati registra una lieve contrazione progressiva: dai 1.418 procedimenti del 2024 si scende ai 1.383 del 2025, con una variazione negativa del 2% nell'ultimo anno e del 4% nell'arco del biennio 2023-2025.

Il dato maggiormente rilevante sotto il profilo della repressione è quello relativo alle persone in stato di arresto: si passa dalle 62 del primo semestre 2024 alle 148 del corrispondente periodo del 2025, con un incremento del 139% in un solo anno e del 279% rispetto al 2023. Ciò denota l'aumento di condotte di particolare gravità o flagranza, tali da giustificare l'adozione della misura precautelare afflittiva. Parallelamente, anche i soggetti denunciati in stato di libertà risultano in aumento: dai 557 del 2024 ai 648 del 2025 (+16% nell'anno e +20% sul biennio), circostanza che segnala un ampliamento della platea di indagati, a fronte di un numero di casi complessivi in lieve flessione.

Sul piano delle attività investigative, le perquisizioni passano da 532 a 604 (+14% in un anno, +50% sul biennio), confermando l'intensificazione delle iniziative di ricerca della prova e di sequestro dei dispositivi informatici, strumenti centrali per l'accertamento dei reati in materia di pornografia minorile e adescamento online.

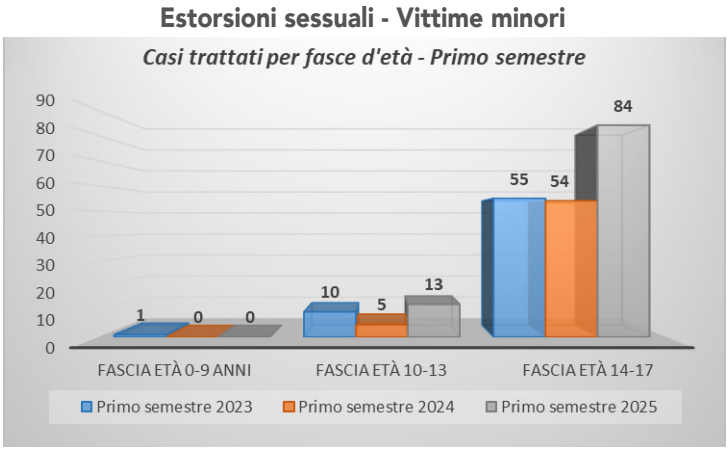
Per quanto concerne i siti web monitorati, la "black list" — ossia l'elenco dei portali inibiti per contenuti illeciti — registra un incremento marginale, passando da 2.759 a 2.821 unità (+2% nell'anno, +5% nel biennio). Tale crescita modesta appare in netto contrasto con il drastico calo dei siti effettivamente visionati, che si dimezzano da 15.170 nel 2024 a 7.826 nel 2025, con una variazione negativa del 48% nell'ultimo anno e del 44% nell'arco del biennio. Questo elemento può essere letto come esito di una più mirata selezione delle fonti da analizzare, o, in alternativa, come indice di una riduzione dell'offerta visibile di contenuti illeciti sul web aperto, con conseguente migrazione verso circuiti criptati e meno accessibili.

Nell'ambito dell'adescamento dei minori online, il raffronto tra primo semestre 2024 e primo semestre 2025 delinea un quadro in cui, a fronte di un generale aumento dei procedimenti, il fenomeno si concentra in misura crescente sugli adolescenti, imponendo una rimodulazione della risposta giudiziaria e investigativa, orientata tanto alla protezione immediata delle vittime quanto alla neutralizzazione rapida e incisiva degli autori di reato.



Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Il confronto tra il primo semestre 2025 e il corrispondente periodo del 2024, con specifico riferimento ai casi di sextortion (estorsioni sessuali) aventi come vittime soggetti minorenni, restituisce un quadro allarmante, connotato da una crescita marcata dei procedimenti e da una concentrazione significativa delle condotte criminose nelle fasce di età adolescenziale.

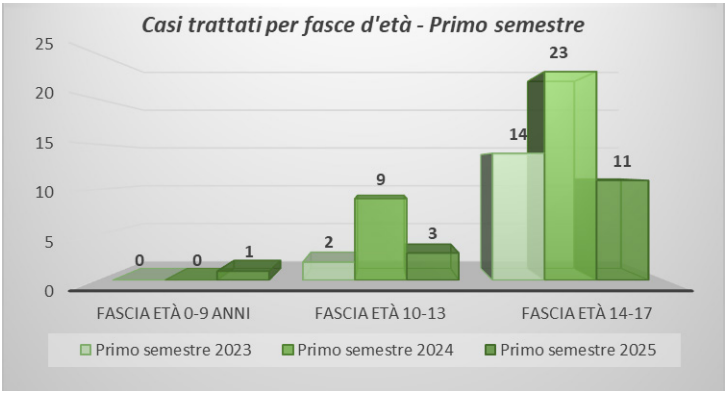


Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Il numero complessivo dei casi trattati sale dai 59 del 2024 ai 97 del 2025, con un incremento del 64%, che interrompe la tendenza lievemente decrescente del biennio precedente (2023-2024). L'aumento appare indicativo di una recrudescenza del fenomeno, probabilmente connessa alla sempre maggiore pervasività delle piattaforme digitali a contenuto multimediale e alla vulnerabilità dei minori nell'utilizzo degli strumenti di comunicazione online. In sintesi, il raffronto tra primo semestre 2024 e primo semestre 2025 mostra come la sextortion ai danni di minori non solo sia in forte espansione, ma si stia consolidando come fenomeno criminale strutturato, con incidenza prevalente sugli adolescenti. Ciò impone una risposta giudiziaria incisiva e multilivello, capace di coniugare la repressione penale con interventi di prevenzione e alfabetizzazione digitale, al fine di ridurre l'area di vulnerabilità e proteggere in maniera effettiva le fasce più esposte della popolazione minorile.

Il raffronto tra il primo semestre 2025 e il corrispondente periodo del 2024 in materia di pubblicazione e diffusione non consensuale di contenuti sessualmente espliciti con vittime minorenni restituisce un quadro che, pur evidenziando una flessione complessiva del fenomeno, non consente di abbassare la soglia di allarme, in quanto la riduzione quantitativa dei procedimenti si accompagna a elementi di novità che incidono in maniera significativa sull'analisi giudiziaria.

Pubblicazione e diffusione non consensuale di contenuti sessualmente espliciti - Vittime minori

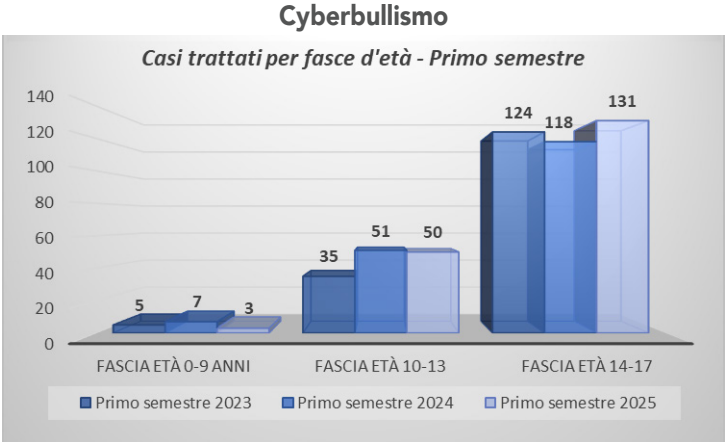


Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Il totale dei casi trattati passa dai 32 del 2024 ai 15 del 2025, con una contrazione pari al 53%, che interrompe la crescita costante registrata nel biennio precedente (2023-2024). Tale ridimensionamento, se considerato isolatamente, sembrerebbe indicare un indebolimento della diffusione del fenomeno; tuttavia, un'analisi più approfondita della distribuzione anagrafica delle vittime mostra come la riduzione non sia uniforme e come si siano aperte nuove aree di vulnerabilità.

In definitiva, il raffronto tra primo semestre 2024 e primo semestre 2025 evidenzia una contrazione numerica che, tuttavia, non attenua la gravità sociale e giuridica del fenomeno. Al contrario, la novità del coinvolgimento della fascia 0-9 anni e la perdurante incidenza tra gli adolescenti pongono l'accento sulla necessità di una risposta giudiziaria e investigativa sempre più mirata, che sappia affiancare alla repressione penale la prevenzione, con particolare attenzione alla protezione delle fasce di età più vulnerabili

Il confronto tra primo semestre 2024 e primo semestre 2025 restituisce un quadro in cui il cyberbullismo si conferma fenomeno in crescita, con una flessione nelle fasce più giovani, ma con un rafforzamento netto nella fascia adolescenziale, dove le condotte risultano più numerose e più strutturate. Tale scenario impone un approccio giudiziario e investigativo che non si limiti alla mera repressione, ma che integri interventi preventivi e formativi, affinché l'azione penale possa effettivamente coniugarsi con la finalità di tutela e recupero propria della giustizia minorile.



Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Tra le attività di polizia giudiziaria condotte dagli Uffici territoriali della Specialità e coordinate dal Centro, alcune delle quali svolte in modalità sotto copertura *online* e scaturite da segnalazioni pervenute nell'ambito della costante e proficua attività di cooperazione internazionale di polizia svolta dal CNCPO, si evidenziano, in particolare, le seguenti operazioni:

- *Operazione 'STREAM'*. La Procura Distrettuale di Napoli ha coordinato una vasta operazione nazionale contro lo sfruttamento sessuale dei minori online avviata dal CNCPO con la collaborazione del COSC Campania. Sono state tratte in arresto 4 persone e indagate 15 per detenzione di ingente materiale pedopornografico, con il sequestro di numerosi *wallet* di criptovalute, nonché dispositivi informatici contenenti decine di migliaia di *file* illegali. L'operazione ha visto il coinvolgimento nella fase esecutiva dei C.O.S.C. della Lombardia, Lazio, Piemonte, Toscana, Emilia Romagna, Puglia, Veneto e Sardegna nell'esecuzione di 15 decreti di perquisizione delegati dalla Procura della Repubblica di Napoli. La cooperazione con il collaterale tedesco nell'ambito di una più ampia operazione coordinata da Europol e le complesse analisi delle *blockchain* hanno permesso di identificare le persone che hanno effettuato diversi pagamenti in *criptovaluta* per accedere alla piattaforma nel *Dark web* denominata "KidFlix" - nome che si ispira alla nota piattaforma di contenuti *on-demand Netflix* - utilizzata per la riproduzione *on-demand* di contenuti multimediali a carattere pedopornografico raggruppati per categorie. Grazie al coordinamento di Europol, l'operazione ha potuto garantire un'efficace cooperazione transfrontaliera tra le forze dell'ordine di oltre 35 Paesi tra cui Germania, Italia, Stati Uniti, Regno Unito, Francia, Spagna, Canada con la chiusura della piattaforma e l'identificazione di quasi 1.400 sospettati a livello globale.
- *Operazione "Hello"*. La Procura Distrettuale di Catania, congiuntamente al CNCPO e COSC Sicilia Orientale, ha coordinato una vasta operazione nazionale contro lo sfruttamento sessuale dei minori online con 120 persone indagate di cui 31 tratte in arresto per detenzione di ingente materiale pedopornografico e il sequestro di numerosi dispositivi informatici. L'operazione condotta dagli investigatori della Polizia di Stato ha consentito di indagare in totale 120 persone, residenti in 56 città italiane, per i reati detenzione e divulgazione di pornografia minorile su una nota piattaforma di messaggistica istantanea. Sono stati impegnati nell'esecuzione di perquisizioni personali e informatiche oltre 500 operatori nelle città di Agrigento, Arezzo, Avellino, Bari, Bergamo, Bologna, Brescia, Cagliari, Caltanissetta, Caserta, Catania, Chieti, Como, Cosenza, Cremona, Firenze, Foggia, Frosinone, Genova, Latina, Lecce, Livorno, Mantova,

Massa Carrara, Messina, Milano, Modena, Monza Brianza, Napoli, Oristano, Palermo, Parma, Pesaro, Pescara, Pisa, Pistoia, Pordenone, Potenza, Ragusa, Ravenna, Reggio Calabria, Rimini, Roma, Salerno, Savona, Siracusa, Sondrio, Sud Sardegna, Taranto, Torino, Trapani, Treviso, Varese, Verona, Vicenza e Viterbo. La gran parte degli indagati utilizzava sistemi di crittografia o di archiviazione in cloud al fine di occultare il materiale pedo-pornografico, rinvenuto grazie all'esperienza degli investigatori e all'utilizzo di sofisticate apparecchiature di *digital forensic*. Gli indagati, di varie estrazioni sociali (studenti, disoccupati o operai), tutti di sesso maschile, hanno un'età compresa tra 21 e 59 anni. Tra di loro, alcuni ricoprono posizioni particolari che prevedono incarichi amministrativi presso il consiglio comunale o svolgimento di attività sportive con i giovani. Due degli arrestati, oltre a detenere migliaia di file pedopornografici, avevano immagini e video autoprodotti con abusi sessuali su minori, vittime che sono state già identificate dagli operatori di Polizia.

- Operazione di contrasto nazionale alla pedopornografia in collaborazione con la ONG, no profit americana *"Child Rescue Coalition"*. L'indagine, avviata dal Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) del Servizio Polizia Postale, nell'ambito dell'attività di cooperazione internazionale, ha consentito a diversi COSC su tutto il territorio nazionale di portare a termine diverse operazioni di Polizia. Eseguiti 87 decreti di perquisizione per detenzione e diffusione di materiale pedopornografico, emessi rispettivamente dalle Procure della Repubblica di Firenze, Pescara, Reggio Calabria, Napoli, Bologna, Trieste, Roma, Genova, Milano, Torino, Cagliari, Palermo e Catania, Perugia, Venezia e Bari e eseguiti dai rispettivi Centri Operativi per la Sicurezza Cibernetica. Le attività hanno determinato l'arresto in flagranza di reato per detenzione di ingente quantità di materiale pedopornografico di 55 persone e l'identificazione di 10 vittime.

- *Operazione "Viper"*. L'indagine, coordinata dal Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO) del Servizio Polizia Postale, è stata condotta in modalità sotto copertura dal Centro Operativo per la Sicurezza Cibernetica di Venezia sulla piattaforma di messaggistica Viber all'interno di gruppi dediti allo scambio di materiale pedopornografico raffigurante anche torture perpetrate in danno dei minori. Sono stati identificati numerosi utenti italiani e stranieri, localizzati in 44 diversi Stati esteri. Il carattere transnazionale dell'attività, considerato il coinvolgimento dei Paesi esteri, ha visto nella fase esecutiva la pianificazione con il coordinamento di Europol di una Joint Action, per l'esecuzione dei decreti di perquisizione emessi delle Autorità giudiziarie

dei Paesi coinvolti. In Italia, la Procura della Repubblica di Venezia ha emesso 57 decreti di perquisizione nei confronti di altrettanti indagati che, in fase esecutiva, si concludevano con l'arresto di 28 persone, per detenzione di ingente quantità di materiale pedopornografico e la denuncia di 24 persone in stato di libertà.

- Una lunga e complessa attività sotto copertura svolta dagli operatori specializzati del Centro Nazionale per il Contrasto alla Pedopornografia Online, in raccordo con la competente Procura della Repubblica presso il Tribunale di Roma, all'interno di un gruppo sulla piattaforma Telegram dedito allo scambio di materiale pedopornografico, ha portato all'arresto di un parroco a Brescia per detenzione di ingente quantità di materiale pedopornografico. In particolare, nel corso delle interlocuzioni all'interno del gruppo sulla piattaforma, veniva individuato un utente che, utilizzando connessioni criptate tramite VPN e utenze telefoniche anonime, si rendeva particolarmente attivo nello scambio di messaggi e nella pubblicazione di contenuti multimediali ritraenti minori degli anni diciotto coinvolti in attività sessuali esplicite. Grazie alle attività sotto copertura è stato possibile identificare l'utente in un parroco di 51 anni della provincia di Brescia. La perquisizione informatica sui dispositivi in uso allo stesso con il supporto delle psicologhe della Polizia di Stato e dagli operatori della S.O.S.C. di Brescia, ha consentito di riscontrare la presenza di ingente quantità di materiale pedopornografico (oltre 1.500 file multimediali) che ne determinava l'arresto con detenzione presso la locale Casa circondariale.
- Il COSC Marche ha arrestato un insegnante per detenzione di materiale pedopornografico e atti sessuali con una minore di anni 13, con la quale era stato previamente condiviso materiale dal contenuto sessualmente esplicito, sequestrando i dispositivi dove era stato rinvenuto ingente quantitativo di materiale illecito a seguito della perquisizione informatica.
- La Sezione Operativa per la Sicurezza Cibernetica di Padova a seguito della denuncia querela sporta dai genitori di una 14enne, adescata tramite l'applicazione "Snapchat" da un profilo, presentatosi come un ragazzo quindicenne di PADOVA, ha eseguito la perquisizione informatica nei confronti di un 53enne successivamente tratto in arresto per diffusione e detenzione di ingente quantitativo di materiale pedopornografico, circa 2.000 file multimediali rappresentanti minori presumibilmente di un'età compresa tra i 6 mesi e 14 anni.

L'attività della Sezione Operativa della Seconda Divisione del Servizio Polizia Postale e per la sicurezza cibernetica

Per quanto riguarda l'attività di contrasto alle fenomenologie e reati commessi online contro la persona, la II Divisione del Servizio Polizia Postale e per la sicurezza cibernetica cura attraverso la Sezione Operativa tutte le attività di prevenzione e repressione in materia di reati realizzati con l'utilizzo di dispositivi elettronici e dei social network: quali diffamazione, minacce, atti persecutori (*stalking*), diffusione illecita di immagini o video a contenuto sessualmente esplicito senza il consenso della persona ritratta (*revenge porn*), romance scam, sostituzione di persona, estorsione, diffusione illecita di immagini, molestie, reati d'odio.

Primo semestre 2024 - 2025 – Reati contro la persona
Rilevazione nazionale

Fenomeno / Reato	Casi 2024	Casi 2025	Indagati 2024	Indagati 2025
Stalking	100	98	84	32
Diffamazione online	984	1.092	313	294
Minacce	306	291	63	61
Revenge Porn	159	120	51	61
Molestie	293	240	42	31
Sextortion	818	588	68	59
Trattamento illecito dati	510	390	17	6
Sostituzione di persona	1.605	1.687	76	63
Hate Speech	44	48	11	11
Propositi suicidari	25	36	0	1
Totale	**4.844**	**4.590**	**725**	**619**

Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Particolare attenzione è stata dedicata al coordinamento delle attività operative condotte dagli uffici territoriali alla luce delle significative previsioni con l'approvazione del testo normativo *n.168/2023 recante' Disposizioni per il contrasto della violenza sulle donne e della violenza domestica'* che ha esteso, tra le varie novità, la possibilità di procedere con l'arresto in flagranza differita. La Sezione espleta altresì funzioni di coordinamento delle indagini su territorio nazionale e internazionale, analizza i feno-

meni, cura tutte le informazioni per i reati in questione provenienti dai paesi esteri e gestisce a iniziativa indagini di polizia giudiziaria.

Sono state inoltre gestite le informazioni e il coordinamento delle attività di indagine svolte dagli uffici territoriali con particolare riguardo a quelle rientranti nella tipologia degli atti intimidatori nei confronti dei giornalisti. Puntuale il raccordo con il '*Centro di coordinamento delle attività di monitoraggio, analisi e scambio permanente di informazioni sul fenomeno degli atti intimidatori nei confronti dei giornalisti*' presso la Direzione Centrale della Polizia Criminale.
In merito all'attività operativa svolta dal settore dei reati contro la persona si evidenziano le seguenti operazioni:

- Gli operatori del settore reati contro la persona hanno dato esecuzione ad un'ordinanza di applicazione della misura cautelare personale del divieto di avvicinamento con divieto di comunicazione e applicazione del braccialetto elettronico nei confronti di una persona, per atti persecutori e diffamazione continuata e aggravata; l'indagine trae origine dalla querela presentata al Centro Operativo di Bologna da un avvocato che ha segnalato la reiterata condotta persecutoria dell'indagata mediante ripetute molestie e minacce poste in essere tramite telefonate, messaggi WhatsApp, invio di email e post pubblicati sul social Facebook. L'indagata ha rifiutato l'applicazione del braccialetto elettronico e, come da ordine di esecuzione, è stata sottoposta alla misura aggiuntiva del divieto di dimora nella città Metropolitana in cui risiedeva la persona.

- Personale specializzato della II Divisione del Servizio Polizia Postale ha proceduto all'arresto di una persona per atti persecutori, culminati in gravi minacce di morte nei confronti della vittima e di alcune sue conoscenti. L'arresto è scaturito a seguito della denuncia presentata dalla parte offesa che seguita da una tempestiva ricostruzione dei fatti segnalati e supportata da una perquisizione informatica, consentiva di documentare in maniera inequivocabile le condotte, permettendo l'arresto immediato ai sensi della normativa vigente.

- Il Centro Operativo per la sicurezza cibernetica di Perugia, a seguito del ritrovamento del corpo esamine di uno studente fuori sede all'interno di un B&B ubicato nel centro storico perugino, riusciva a identificare e arrestare due persone responsabili del reato di istigazione al suicidio, una delle quali sottoposta successivamente agli arresti domiciliari.

- Il personale del Centro Operativo per la sicurezza cibernetica Piemonte, a seguito di una querela presentata per il reato di diffamazione on line, riusciva a identificare e deferire alla locale Autorità Giudiziaria gli utenti che avevano po-

stato commenti diffamatori su Facebook nei confronti della vittima, quest'ultima imprenditrice e personaggio molto conosciuto nell'hinterland torinese. Il video della vittima relativo alla rottura del suo fidanzamento con un noto banchiere torinese era divenuto virale e veniva ripreso dai mezzi di comunicazione. Il Pubblico ministero che inizialmente aveva richiesto l'archiviazione, a seguito dell'opposizione della stessa parte offesa, delegava il COSC di Torino a svolgere specifiche indagini per l'identificazione degli autori delle condotte lesive.

- Una donna denunciava alla Sezione Operativa per la sicurezza cibernetica di Lucca di aver contattato, tramite Facebook e su consiglio di alcune amiche, un sedicente professionista psicologo; il quale la invitava a trasferire la conversazione da Messenger alla piattaforma Viber e successivamente su Whatsapp, dove le veniva richiesto di inviare video hard. Successivamente le veniva intimato di pagare una grossa somma, pena la divulgazione dei relativi filmati. Al termine delle investigazioni veniva individuato e denunciato un cittadino nigeriano residente a Cuneo.
- Il Centro Operativo per la sicurezza cibernetica di Perugia ha identificato 4 utenti social per crimini d'odio (discriminatorio per l'orientamento sessuale delle vittime) perpetrati nei confronti del Presidente di un'associazione dedita alla tutela dei diritti e al contrasto delle discriminazioni basate sull'orientamento sessuale e l'identità di genere e dei suoi aderenti; nonché dell'identificazione di un utente social, autore di commenti sessisti nei confronti di un Assessore locale.
- Il personale del Centro Operativo per la sicurezza cibernetica di Torino ha acquisito elementi probatori a carico di una persona, eseguendo un decreto di perquisizione, per le condotte persecutorie in danno delle atlete della Federazione Italiana di Tiro con l'Arco a cui aveva indirizzato messaggi di contenuto sessuale, nonché video, foto e videochiamate dello stesso tenore.

La Terza Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La Terza Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica è il presidio specializzato nella **protezione delle infrastrutture critiche nazionali** e nella prevenzione delle minacce eversivo–terroristiche in ambito digitale. In un contesto in cui la sicurezza del Paese dipende sempre più dalla continuità dei servizi essenziali – energia, trasporti, comunicazioni, sanità, finanza – la Divisione svolge un ruolo strategico di vigilanza e difesa, garantendo che il cyberspazio non diventi terreno fertile per attacchi capaci di compromettere la stabilità economica e sociale.

La sua attività si fonda su un approccio integrato che combina **intelligence, analisi tecnica e capacità forense**, con l'obiettivo di individuare tempestivamente vulnerabilità, intercettare segnali di minaccia e neutralizzare azioni ostili prima che possano produrre effetti concreti. Accanto all'attività investigativa, la Divisione promuove lo sviluppo di soluzioni tecnologiche avanzate e metodologie di analisi digitale, rafforzando la capacità di risposta della Polizia di Stato e assicurando supporto specialistico agli uffici giudiziari e agli altri attori istituzionali.

Elemento distintivo della Terza Divisione è il suo **ruolo di coordinamento nazionale**: essa indirizza e armonizza le attività dei Centri Operativi territoriali, garantendo uniformità di approccio e tempestività di intervento. Al tempo stesso, mantiene un costante raccordo con le strutture di sicurezza nazionali e internazionali, contribuendo alla costruzione di una rete di cooperazione indispensabile per fronteggiare minacce che, per natura e portata, travalicano i confini geografici.

Attraverso indagini complesse, attività di prevenzione e un dialogo continuo con istituzioni e operatori strategici, la Terza Divisione assicura un contributo essenziale alla **resilienza del sistema Paese**, trasformando la tecnologia in uno strumento di protezione e difesa al servizio della collettività.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - C.N.A.I.P.I.C.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - C.N.A.I.P.I.C., istituito con decreto del Ministro dell'Interno 9 gennaio 2008, costituisce uno dei Centri di Specialità del Servizio Polizia Postale.

Nell'anno in corso è stato ancor di più rafforzato il suo ruolo quale "*Organo del Ministero dell'Interno per la sicurezza e regolarità dei servizi di telecomunicazioni*". In tale veste, esso è incaricato, in via esclusiva, della prevenzione e della repressione dei crimini informatici di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

Mediante la stipula di appositi protocolli di intesa con gli altri attori istituzionali che costituiscono l'architettura nazionale di cybersicurezza e con gli organi di direzione dell'autorità giudiziaria, si è realizzata una migliore e più efficace esplicazione delle funzioni di coordinamento e impulso delle attività preventive e di indagine, di competenza del Centro in ordine ai più importanti reati informatici.

Nello specifico, in ossequio alle nuove disposizioni legislative, sono stati previsti specifici doveri di informazione circa le notizie concernenti gli attacchi registrati ai

danni dei sistemi informatici o telematici dei soggetti che rientrano nel perimetro di sicurezza nazionale cibernetica, con la previsione di un'implementazione continuativa nella trasmissione di dati, notizie e informazioni acquisite, anche successivamente alla prima comunicazione.

La natura composita dell'attività svolta dal Centro ha richiesto, anche nel periodo di riferimento, una continua esplicazione di poteri, tanto di coordinamento delle dipendenti articolazioni territoriali, quanto direttamente operativi, costituendo per tale via un unicum nel panorama delle istituzioni Dipartimentali della P.S.

Il suo *modus operandi* si caratterizza per la stipula di apposite convenzioni, che permettono al C.N.A.I.P.I.C. di esercitare una più efficace azione di tutela delle singole Società e Enti sensibili consorziati, mediante un continuativo contatto e scambio di informazioni, anche di natura tecnica, rilevanti sulla minaccia cibernetica.

Negli anni il processo riorganizzativo della Specialità si è adeguato alla natura variegata e mutevole delle minacce cibernetiche, con l'emersione sempre più impellente di una rimodulazione interna degli *asset,* al fine di garantire una maggiore vicinanza alle realtà da proteggere e un intervento ancor più incisivo e risolutivo.

L'esito di tale processo ha previsto l'istituzione di una nuova Direzione Centrale a livello Dipartimentale e il riconoscimento di un ruolo importante del C.N.A.I.P.I.C. all'interno del rinnovato Servizio Polizia Postale e per la Sicurezza Cibernetica; nonché una rimodulazione della struttura dipendente con l'acquisizione, nei territori di competenza, di compiti sempre più qualificati da parte dei Centri Operativi per la Sicurezza Cibernetica (COSC), quali uffici operativi specificamente dedicati alla protezione delle infrastrutture sensibili di rilevanza locale, e dei Nuclei Operativi per la Sicurezza Cibernetica (NOSC), quali articolazioni riproducenti i tratti del Centro nazionale all'interno delle citate articolazioni.

L'attività anticrimine del C.N.A.I.P.I.C. e dei NOSC ha consentito, nel periodo di riferimento, di rilevare complessivamente **4.911** attacchi, nonché di diramare **22.990** *alert*. Le indagini avviate esclusivamente dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche sono state **39**, mentre **49** sono le persone indagate con la collaborazione delle articolazioni territoriali e **21** le richieste di cooperazione internazionale in ambito Rete 24/7 High Tech Crime (Convenzione di Budapest) pervenute, a cui si è dato corso.

Contrasto al Cybercrime
Attività del C.N.A.I.P.I.C. e dei N.O.S.C.

	PRIMO SEMESTRE 2023	PRIMO SEMESTRE 2024	PRIMO SEMESTRE 2025
TOTALE ATTACCHI RILEVATI	5.775	5.903	4.911

Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

I dati riportati permettono di sottolineare come, nel corso del periodo di riferimento, le analisi condotte dal C.N.A.I.P.I.C. abbiano confermato una continua e progressiva evoluzione della minaccia informatica, che si manifesta non solo in termini quantitativi, ma soprattutto nella crescente sofisticazione degli attacchi e nella loro capacità di incidere su ambiti strategici. L'avanzamento tecnologico e la digitalizzazione diffusa continuano ad ampliare la superficie esposta, trasformando la rete in un ambiente operativo sempre più complesso, dove le condotte illecite si diversificano e si adattano con rapidità. In questo scenario, internet non è soltanto vettore di progresso, ma anche spazio d'azione privilegiato per fenomeni criminali trasversali, che richiedono strumenti di contrasto sempre più avanzati e coordinati.

In tale contesto, il fenomeno della criminalità informatica si manifesta in forme diverse, ancorché accomunate dal perseguimento di fini illeciti. In tal senso, la rete diventa oggetto di attenzione da parte delle organizzazioni criminali, che trovano in essa uno strumento agevolatore delle condotte illecite per massimizzare i profitti, in considerazione delle grandi potenzialità che derivano dai continui e immediati scambi che in essa avvengono e che la stessa è in grado di facilitare.

Cosicché, le organizzazioni, associandosi, sono state in grado di elaborare strumenti sempre più pervasivi e avanzati, contro i quali il C.N.A.I.P.I.C. mette in campo tutte le professionalità e tecnologie di cui dispone, per esplicare la sua funzione pubblica di prevenzione e contrasto al crimine. Il continuo aggiornamento professionale, unito a un ammodernamento degli strumenti e degli applicativi usati, permettono al personale del C.N.A.I.P.I.C. di essere al passo con i più agguerriti e attivi hackers, sia a livello nazionale che internazionale.

A tal fine, il processo quotidiano di studio delle tecniche e tattiche utilizzate dai gruppi criminali ha permesso di rivelare, anticipandole, quelle che sono le modalità

utilizzate dagli attori ostili e intervenire sia in fase repressiva sia, ancor prima, in fase preventiva.

La diramazione tempestiva di appositi *alert* alle infrastrutture critiche ha permesso, infatti, di adeguare la struttura di questi enti, che costituiscono l'ossatura fondamentale del nostro sistema economico-finanziario, affinché essa risulti resiliente rispetto ad azioni ostili in corso.

Il personale del C.N.A.I.P.I.C., in aderenza all'architettura di sicurezza cibernetica nazionale, ha offerto anche un pronto supporto sul posto per l'avvio delle attività di *remediation,* utili alla messa in sicurezza dei sistemi bersaglio degli enti citati.

Dall'altro canto, lo studio degli attacchi cibernetici ha permesso di evidenziare come essi seguano generalmente un ciclo di vita strutturato e metodico, che, pur rinnovandosi nelle metodologie, permette agli attori ostili di penetrare in una rete, mantenere un accesso prolungato e persistente, raccogliere informazioni e, infine, completare la loro azione criminosa nell'intento di non essere scoperti per lungo tempo. Questo ciclo di vita riflette l'applicazione di tecniche di ingegneria sociale, seguite dagli attaccanti per studiare i comportamenti delle vittime e perseguire il fine illecito insito nella loro azione criminosa, rendendo al contempo difficile la loro rilevazione e l'attuazione di politiche di mitigazione.

L'azione del C.N.A.I.P.I.C. è diretta ad attribuire, con il maggior grado di certezza possibile, un attacco a entità individuabili, per l'utile avvio e perseguimento delle azioni di polizia giudiziaria, in costante raccordo con l'autorità giudiziaria, necessarie per l'identificazione dei responsabili "c.d. *attribution*".

L'esito positivo di tale verifica deriva, invero, da una combinazione di fattori tecnici e strategici, oltre che dalla scoperta delle tattiche ingannevoli che gli attaccanti adottano per sfuggire alla rilevazione e confondere gli investigatori. Una delle sfide principali è rappresentata proprio dal disvelamento delle tecniche sempre più sofisticate, utilizzate dagli attori ostili per nascondere o manipolare le tracce del loro passaggio: a tal fine, gli attaccanti utilizzano vari metodi di offuscamento per evitare di essere rilevati o identificati. La rilevazione casistica ha fatto emergere l'utilizzo di infrastrutture di comando e controllo (C2), situate per lo più in Paesi lontani o reti proxy, per rendere difficile individuare l'origine dell'attacco. Inoltre, vengono sempre più spesso utilizzati malware personalizzati o ancora strumenti di attacco resi più performanti da una combinazione di strumenti (l'uso diffuso di tecnologie di crittografia e anonimizzazione, come Tor e VPN, l'utilizzo di Bulletproof Hosting e la condivisione delle infrastrutture rende più difficile tracciare il traffico e attribuirlo a una fonte specifica).

Le investigazioni devono spesso fare affidamento su dettagli sottili e su prove indirette, come modelli comportamentali, tempistiche delle operazioni e caratteristiche uniche del codice malware.

Risultano inoltre sempre più utilizzate tattiche di "*false flag*", in cui si cerca di far ricadere la colpa su un altro attore, utilizzando strumenti che imitano le tecniche e tattiche utilizzate da gruppi rivali o di altre nazioni: questo rende l'attribuzione ancora più complessa e incerta, poiché richiede agli investigatori di avere le capacità di distinguere tra un attore autentico e una simulazione intenzionale. Oltre agli aspetti di natura squisitamente tecnica, la difficoltà intrinseca nel collegare un attacco informatico a un'entità specifica è ricollegata al fatto che sempre più i gruppi hacker sono patrocinati da governi o hanno legami indiretti con agenzie statali (APT).

Nel quadro delle minacce cyber, si assiste a un utilizzo maggiormente significativo degli attacchi DDoS (Distributed Denial of Service), azioni criminose che si sono evolute nel tempo: dalle prime forme basate su software open-source fino agli attuali attacchi più sofisticati che coinvolgono botnet e servizi a pagamento. In particolare, un attacco DDoS si caratterizza per sovraccaricare le risorse di un server o una rete con traffico malevolo, provocando l'interruzione del servizio per gli utenti legittimi, con una differenziazione in base alla tipologia: attacchi a livello applicativo, attacchi ai protocolli di rete e attacchi volumetrici. Le tendenze più recenti evidenziano l'impiego crescente di botnet avanzate e il ruolo strategico degli attacchi DDoS all'interno di scenari geopolitici, con particolare riferimento al conflitto tra Russia e Ucraina.

Assistiamo sempre più spesso all'utilizzo di tecniche basate su *exploit zero-day* (attraverso lo sfruttamento di vulnerabilità non conosciute dal pubblico o dai fornitori di software), *malware* formati su misura e attacchi multi-vettore, che combinano *phishing* mirato, tecniche di social *engineering* e sfruttamento delle vulnerabilità di reti e sistemi, la cui complessità deriva dal fatto che non si limitano all'utilizzo di metodi standard, ma si adattano in base alle difese delle vittime, implementando tecniche di evasione a carattere avanzato.

Un altro dato di natura allarmante è che gli attacchi cibernetici, stimati nell'ordine di decine di milioni ogni giorno, sono sempre più volontariamente diretti verso gli anelli più vulnerabili delle catene di processo e delle *supply chain* (come i singoli cittadini, i singoli funzionari pubblici e privati, le piccole e medie imprese).

Per quanto riguarda i target e gli obiettivi degli attacchi, il trend - già registrato a partire dallo scorso anno - mostra un'attenzione particolare verso le strutture del comparto sanitario. I dati in esse contenuti sono molto ricercati dagli attori ostili, in quanto hanno un mercato fiorente sul dark web, essendo molto richiesti e venduti

facilmente a un prezzo elevato e sicuramente maggiore rispetto a dati di altra natura. Queste informazioni, una volta che entrano nella disponibilità delle *crew* criminali, costituiscono una fonte di lucro considerevole, rivelando dati sensibili dei pazienti in cura, la cui violazione può avere conseguenze molto gravi.
Da tali dati è possibile sottolineare che le strutture sanitarie oggi stanno progressivamente adeguando il livello di protezione cyber richiesto dai processi di digitalizzazione della nostra società. Occorre tuttavia incentivare campagne di sensibilizzazione da parte di queste istituzioni, che risultano maggiormente esposte, ovverosia far in modo che esse dimostrino concretamente di possedere le *skills* per gestire questi dati sensibili, strutturando al loro interno processi affidabili e disponendo di un'organizzazione interna in grado di risolvere problemi di gestione di attacchi in tempi rapidi.

Infine, il carattere comune della "*transnazionalità*" delle condotte, associato sempre di più alla "*delocalizzazione*" delle stesse, rendono arduo il contrasto al fenomeno. In tal senso, l'effettività della risposta preventivo/investigativa risente, in maniera assai incisiva, della disomogeneità dei sistemi legislativi nazionali, soprattutto in tema di regole per l'acquisizione della prova digitale e in materia di *data retention*. La sottoposizione ad apparati regolatori assai diversificati tra loro e la presenza di *policy* aziendali eterogenee rendono complicata la risposta giudiziaria e di polizia - nonostante l'efficienza dei modelli di cooperazione internazionale - e non aiutano l'ottenimento di dati di interesse investigativo da parte delle agenzie di *law enforcement*.
In soccorso, si registra un aumento delle richieste di cooperazione internazionale e l'utilizzo sempre più consapevole, da parte del C.N.A.I.P.I.C., del suo ruolo di Punto nazionale della Convenzione di Budapest sul crimine informatico.

Tale strumento pattizio annovera tra i suoi scopi quello di favorire l'accesso transfrontaliero alle prove elettroniche da utilizzare nei procedimenti penali, oltre a facilitare la collaborazione tra i vari Stati membri e Paesi terzi nella lotta al cyber crime e non solo, garantendo il rispetto delle norme UE in materia di protezione dei dati. L'applicazione di tali misure di assistenza ha sicuramente migliorato la cooperazione internazionale tra le autorità, così come rafforzato la collaborazione con i fornitori di servizi e le entità che si trovano negli altri Paesi, favorendo la divulgazione di informazioni dettagliate su abbonati, dati di traffico e registrazione dei nomi di dominio, con il coinvolgimento anche dei prestatori di servizi privati (come i gestori di provider o le società fornitrici dei servizi di telecomunicazione) e stabilito procedure più veloci per l'assistenza giudiziaria reciproca d'urgenza.

Infine, la combinazione di strumenti investigativi tradizionali e le nuove tecniche derivanti dall'introduzione di modifiche legislative - tra tutte il riconoscimento di

importanti attribuzioni di polizia giudiziaria riconnesse all'attivazione di operazioni sotto copertura, ex art. art. 9 Legge 16 marzo 2006, n. 146 - permettono oggi al C.N.A.I.P.I.C. di mettere in campo strumenti adeguati di contrasto a una minaccia cibernetica sempre più pervasiva e strutturata. L'approvazione del D.L. 105/2023 ("DL Giustizia"), convertito in L. 137/2023, ha apportato significative modificazioni alla disciplina generale dell'indagine sotto copertura delineata dall'art. 9 della L. 146/2006, ampliando significativamente il ventaglio delle condotte scriminabili, che ora si estende al compimento di condotte proattive in ambiente informatico. La novella legislativa dedica una specifica previsione al tema delle indagini in materia di protezione delle infrastrutture critiche nazionali, affidate dalla legge al Servizio Polizia Postale, prevedendo in particolare che gli Ufficiali di p.g. assegnati – oltre al compimento delle attività tradizionalmente previste in capo all'agente undercover – possano compiere condotte di violazione, manipolazione o danneggiamento di sistemi e dati informatici, ovvero possano attivare domini e identità digitali finalizzati all'attività di ricerca della prova.

Grazie all'attivazione di questi strumenti, il C.N.A.I.P.I.C. è assoluto protagonista della lotta contro il crimine informatico.

L'impegno di personale del C.N.A.I.P.I.C. in contesti internazionali ha permesso inoltre di migliorare la conoscenza di *best practice* e buone prassi estere, la cui trasposizione nel nostro ordinamento costituisce un valore aggiunto per il miglioramento degli strumenti già utilizzati e un utile approfondimento per la realizzazione di indagini complesse.

Di seguito sono elencate le principali attività svolte dal personale specialista del C.N.A.I.P.I.C. nello specifico settore, in occasione di importanti eventi e riunioni internazionali. In questi ambiti viene svolto un duplice compito, sia di prevenzione che di monitoraggio costante di tutte le attività connesse all'evento.

La rilevanza dell'evento comporta infatti uno studio preliminare dell'infrastruttura tecnologica utilizzata nel corso dell'evento, mediante l'inserimento dello stesso nel contesto nazionale e internazionale sussistente al momento (in atto contraddistinto dalla presenza dei due conflitti bellici), con l'obiettivo di predisporre le più opportune e migliori misure di sicurezza, ordine e vigilanza, per assicurare il regolare svolgimento dei singoli appuntamenti, nonché la tutela e l'incolumità dei partecipanti con il conseguente innalzamento delle attività di prevenzione.

Considerata la necessità di acquisire elementi conoscitivi utili alla valutazione del rischio, i Centri Operativi competenti per territorio - con il coordinamento generale del C.N.A.I.P.I.C. - sono incaricati di svolgere specifiche attività di monitoraggio sul

web che si innestano all'interno di un dispositivo di polizia integrato, che tiene conto degli elementi informativi già noti e condivisi anche per il tramite di interlocuzioni con le altre articolazioni Dipartimentali.

75° Festival della Canzone Italiana di Sanremo

Il Servizio Polizia Postale e per la sicurezza cibernetica ha espletato un dedicato servizio di sicurezza informatica a tutela del 75° Festival della Canzone Italiana di Sanremo, in collaborazione con la struttura di sicurezza cibernetica della RAI, infrastruttura critica convenzionata con il C.N.A.I.P.I.C.

In particolare, come in occasione di importanti eventi nazionali, personale del C.N.A.I.P.I.C. del predetto Servizio e del Centro Operativo per la Sicurezza Cibernetica "Liguria", in stretto raccordo con la Questura di Imperia, ha garantito un dispositivo attivo h24 presso una sala operativa dedicata, allestita dalla RAI in Sanremo, per la diretta tutela dei sistemi e dei servizi informatici che hanno supportato l'intera produzione.

Giubileo della Chiesa Cattolica 2025

Il Servizio Polizia Postale e per la Sicurezza Cibernetica ha espletato un dedicato servizio di sicurezza informatica connesso allo svolgimento degli Eventi Giubilari, che nel complesso delle attività assicurate dalla Specialità vede il CNAIPIC assicurare il proprio compito istituzionale di tutela delle infrastrutture critiche unitamente all'Agenzia Nazionale per la Cybersicurezza attraverso l'attivazione di dedicate *war room* per la rapida condivisione di situazioni di minaccia cibernetica che facilita l'eventuale immediato contenimento, anche tramite l'attivazione di azioni di intervento e supporto.

Conferenza sulla Ripresa dell'Ucraina 2025

La conferenza si è svolta il 10-11 luglio. Il Summit internazionale, che ha riunito i rappresentanti dei governi, le organizzazioni internazionali e il settore privato per discutere e coordinare gli sforzi di supporto alla ricostruzione e alla ripresa dello stato ucraino, ha visto l'attivo coinvolgimento del Centro Nazionale sia in fase preparatoria, nell'ambito di un dispositivo di coordinamento presieduto dal MAECI, sia in concomitanza dell'evento, con personale direttamente impiegato in loco in sinergia con i responsabili della gestione dell'intera infrastruttura informatica. Le attività si sono incentrate nel monitoraggio della sicurezza dei sistemi online serventi l'evento ed esposti verso l'esterno, al presidio della sicurezza dei processi informatizzati di accredito e, più in generale, al monitoraggio della rete – in ambiente *clear* e *underground* - volto alla precoce intercettazione di minacce, di matrice statuale, attivistica e criminale, dirette all'ordinato svolgimento del Vertice.

Olimpiadi e le Paraolimpiadi Invernali Milano-Cortina

Le Olimpiadi Invernali Milano-Cortina previste per il prossimo febbraio 2026 la cui organizzazione dell'evento è affidata alla omonima Fondazione, hanno già visto l'avvio di intense interlocuzioni e attività preparatorie – ivi comprese simulazioni - finalizzate alla miglior definizione del dispositivo di protezione delle infrastrutture informatiche coinvolte.
Un'attenzione particolare è stata dedicata al fronte della collaborazione internazionale, settore sempre più strategico e funzionale nel contrasto dei reati cyber, per loro natura di carattere sovrannazionale in virtù della loro matrice, dinamica o portata.
In proposito si rappresenta che il CNAIPIC già garantisce, quale punto di contatto in ambito High Tech Crime (Convenzione di Budapest), l'invio e la ricezione delle richieste di collaborazione e supporto da e per i paesi sottoscrittori, comportando la gestione di 21 casi in entrata nell'arco del primo semestre 2025.
La cooperazione si è inoltre esplicitata anche sotto il profilo operativo attraverso l'attiva partecipazione ad azioni di polizia congiunte.

In ambito Europol, la stretta collaborazione e lo scambio info-operativo con i collaterali cyber delle forze di polizia estere ha portato alla conclusione di importanti operazioni, alcune delle quali di rilevanza internazionale in ragione dell'obiettivo perseguito. Tra queste spicca l'***Operazione "Eastwood",*** recentemente condotta nei confronti del collettivo hacker filorusso "NoName057(16)", responsabile, sin dal 2022, di numerosi attacchi informatici di tipo DDoS ai danni di infrastrutture critiche nazionali e occidentali. La complessa attività, frutto di una strutturata indagine condotta nell'ambito di un gruppo investigativo internazionale coordinato da Eurojust e Europol e che ha coinvolto 14 paesi europei, ha consentito di ricostruire puntualmente l'infrastruttura utilizzata dall'attore ostile per condurre gli attacchi (costituita da una fascia di server di Comando e Controllo stabiliti nella Federazione Russa, oltre a ulteriori server distribuiti sul territorio europeo), di identificare 3 persone di nazionalità russa, operanti quali verosimili amministratori del gruppo, e ulteriori presunti sodali del gruppo, residenti in diversi paesi del mondo. Le indagini del CNAIPIC, condotte sotto la direzione della Procura della Repubblica di Roma e il coordinamento della Direzione Nazionale A.A hanno portano all'individuazione di 9 persone, 5 delle quali ritenute effettivamente responsabili della partecipazione agli attacchi informatici portati dal collettivo e, pertanto, attinti da perquisizione in occasione dell'*action day* concertato a livello internazionale. L'operazione, che in ambito nazionale ha consentito l'acquisizione di determinanti elementi a conferma della responsabilità degli indagati, ha globalmente portato al sequestro dell'infrastruttura informatica illecita e all'interruzione dell'operatività del gruppo criminale, riscuotendo notevole risalto a livello mediatico.

In ambito Interpol, gli scambi informativi con i collaterali stranieri - principalmente americani – hanno portato a proficue collaborazioni operative. Tra queste si segnala l'***arresto di un cittadino cinese,*** resosi responsabile di gravi attacchi informatici per conto del governo di Pechino. Il cittadino, che da indagini condotte dall'FBI risultava aver violato e esfiltrato informazioni sensibili dai sistemi informatici di università impegnate nella ricerca vaccinale e trattamentale della pandemia da Covid-19, nonché dai sistemi di agenzie governative e policy maker statunitensi, è stato fermato a Milano da personale del dipendente Centro Operativo lombardo, sotto il coordinamento del CNAIPIC che ha gestito la richiesta di assistenza giudiziaria e di polizia proveniente dal collaterale americano.

Inoltre, dalla sede del C.N.A.I.P.I.C., sono stati costantemente diramati *alert* - di natura tecnica - contenenti gli indicatori di compromissione relativi alle principali campagne malevole in atto, nonché aggiornamenti relativi a possibili iniziative in ambito *hacktivism* per prevenire l'azione di gruppi ideologicamente orientati quale possibile causa di turbativa dell'evento.

Il CNAIPIC collabora attivamente con l'*European Cyber Crime Centre (EC3)* di Europol per contrastare le minacce informatiche a livello internazionale. Questa sinergia si basa sulla condivisione di informazioni, competenze e risorse, che consentono una risposta tempestiva e coordinata alle attività ostili nei confronti delle infrastrutture critiche a livello nazionale ed europeo.

Attraverso questa collaborazione, il CNAIPIC e l'EC3 sviluppano strategie e progetti congiunti, mirati a rafforzare la capacità degli Stati membri di affrontare le minacce informatiche sempre più insidiose ed evolute. La collaborazione rende più efficace la diffusione di *best practices* e la formazione e l'aggiornamento degli operatori delle forze dell'ordine, anche attraverso un addestramento congiunto, contribuendo così a creare un ambiente digitale più sicuro.

Non da ultimo, nel corso dell'anno si sono svolte le riunioni periodiche del Comitato di Analisi per la Sicurezza Cibernetica (CASC), il neo organismo di raccordo tra le Agenzie di Law Enforcement e il Comparto Intelligence finalizzato alla condivisione strategica e info-operativa funzionale a una maggiore efficacia all'azione di contrasto in materia cyber.

Concepito come contesto di facilitazione e promozione dello scambio informativo in ordine alle principali minacce osservate dai vari interlocutori istituzionali nel corso delle rispettive attività, sta acquistando sempre più il ruolo di camera di compensazione e di allineamento tra le istanze investigative, le esigenze di resilienza e la tutela della sicurezza cibernetica nazionale.

Il Settore Cyberterrorismo

Il primo semestre del 2025 è stato contraddistinto da molteplici tensioni geopolitiche globali che hanno coinvolto in primis gli scenari Russo-Ucraino e Israelo – Palestinese, determinando proiezioni interne sui profili di gestione dell'ordine e sicurezza pubblica.

Il mutamento delle tecniche di attacco, delle forme di radicalizzazione, nonché l'ampliamento delle azioni di reclutamento e di finanziamento online dei fenomeni terroristici, ha richiesto una puntuale riconfigurazione degli strumenti di contrasto, imponendo altresì uno studio continuativo dei *network* radicali, interessati da una rapida evoluzione.

Nel periodo in esame la Sezione Cyberterrorismo del Servizio Polizia Postale e per la Sicurezza Cibernetica ha avviato molteplici attività preventive di monitoraggio *O.S.Int* del web, nonché indagini di polizia giudiziaria in cui è stata approfondita la correlazione tra ideologie radicali e la dimensione digitale; di rilievo anche l'attività di coordinamento dei dipendenti Centri Operativi per la Sicurezza Cibernetica, attivi sul territorio e impegnati in una raccolta informativa più diretta, orientata ai fenomeni d'interesse per le Questure.

Peculiare attenzione è stata dedicata al fenomeno della minaccia ibrida, contraddistinta da asimmetricità e dal sistematico ricorso alla componente *cyber* per la destabilizzazione di enti istituzionali e infrastrutture critiche. In tale ambito è stato proseguito il monitoraggio del fenomeno della disinformazione e delle strategie poste in campo da attori ostili per l'alterazione dei processi elettorali attraverso la divulgazione di *fake news,* nonché la creazione di falsi profili istituzionali che possono disorientare la cittadinanza; l'attività di raccolta informativa ha consentito di individuare e rimuovere, con la cooperazione dei *provider*, numerosi profili *fake* impiegati per attività fraudolente o ancora più complesse strategie di impersonificazione.

La ricorrenza delle festività giubilari, il decesso del Pontefice Francesco e la successiva elezione al soglio pontificio di Papa Leone XIV, sono state tematiche di estrema sensibilità mediatica e pertanto oggetto di un'attenta analisi condotta su post, account, domini web, al fine di evitare che la peculiare contingenza storica venisse sfruttata per l'affermazione di ideologie radicali.

Il contrasto all'islamismo radicale violento di matrice jihadista è stato condotto guardando a molteplici fronti, tra cui percorsi individuali di radicalizzazione *online*, piattaforme di reclutamento attestate su social network alternativi non mainstream e forme di finanziamento occulto al terrorismo tramite il ricorso a criptovalute.

La propaganda jihadista online ha assunto molteplici diramazioni, con canali, riviste periodiche, contenuti multimediali, gruppi che vengono puntualmente analizzati per ricostruire le possibili proiezioni sul territorio nazionale. Queste componenti sono state altresì affiancate dal contrasto alla c.d. "*cyber jihad*" ,ossia quell'espressione radicale dell'hacktivismo che vede crew di hacker attivi nell'attacco a infrastrutture sensibili per motivazioni di carattere religioso; in tal senso l'azione ha consentito di comprendere collegamenti tra crew, tecniche di attacco, nonché di apprendere in anticipo le possibili campagne ostili.

Il conflitto israelo - palestinese ha determinato l'estensione di un ampio fronte di dissenso interno che ha visto in particolare i movimenti antagonisti e i gruppi studenteschi attivi nell'organizzare eventi di contestazione, blocchi stradali, occupazioni universitarie, circostanze che hanno trovato una proiezione sistematica nell'ecosistema digitale; il monitoraggio del web in questo caso ha consentito di reperire e isolare le possibili progettualità radicali o violente, sottoponendo alle Questure il materiale informativo utile ad affinare e integrare l'analisi di contesto svolta dalle D.I.G.O.S.

Altro fronte considerevole di attività è stato rappresentato dall'accelerazionismo neonazista, fenomeno che coinvolge soggetti giovanissimi, spesso adolescenti, i quali vengono affascinati da narrazioni estreme in cui vengono scaricati elementi di disagio psicologico e scarsa integrazione sociale. I *network* accelerazionisti sono un contesto prolifico per la divulgazione di istruzioni per la preparazione di armi, esplosivi o ancora concernenti tecniche e metodi per il compimento di atti violenti o di sabotaggio di servizi pubblici essenziali; le istruzioni divulgate online sono poi applicate reperendo risorse facilmente accessibili quali ad esempio stampanti 3D o elementi chimici di libera vendita.

In ambito di cooperazione internazionale il Servizio Polizia Postale costituisce il punto di contatto italiano della rete *Europol IRU - Internet Referral Unit*, coordinata dal Centro ECTC di Europol (European Counter Terrorism Center) – per il monitoraggio dei contenuti terroristici online, e partecipa insieme agli operatori di polizia di altri paesi anche agli *action day* che in tale ambito vengono promossi con notevoli risultati operativi.

Di peculiare importanza operativa è inoltre la cooperazione strutturale svolta nell'ambito del progetto SIRIUS, attraverso strumenti operativi quali la piattaforma *PERCI*, funzionali all'attuazione della disciplina sulla rimozione dei contenuti terroristici online. Sul piano statistico, nel primo semestre 2025 la Sezione Cyberterrorismo ha trattato 46 segnalazioni emergenziali afferenti all'art. 14 co. 5 del regolamento sulla rimozione dei contenuti terroristici e dell'art. 18 del Digital Service Act.

Sono state trattate 34 segnalazioni OSCAD, 106 messaggi SIENA nonché 24 richieste di cooperazione internazionale.

L'attività, funzionale al contrasto del proselitismo e alla prevenzione dei fenomeni di radicalizzazione estremista religiosa e dell'eversione di estrema destra e antagonista, ha permesso di sviluppare una dedicata attività informativa in contesti di interesse, per oltre **101.000** spazi web oggetto di approfondimento investigativo; tra questi, oltre **270** risorse digitali sono state oscurate poiché caratterizzate da un contenuto illecito. La Sezione ha altresì coordinato l'esecuzione di 38 perquisizioni sul territorio nazionale.

Si riepilogano di seguito le attività di maggiore rilievo svolte nel periodo dal 1 gennaio al 30 giugno 2025.

- Nel mese di gennaio il C.O.S.C. e la D.I.G.O.S di Bari hanno eseguito la perquisizione di una persona indagata per i reati di cui agli artt. 81, 414 (istigazione a delinquere), 703 (accensioni e esplosioni pericolose) c.p. e artt. 9, 10 e 12 L. n. 497 del 14/10/74 (reati in materia di armi).
  Il provvedimento è stato emesso a seguito degli accertamenti svolti dal C.O.S.C. in merito a gruppi operanti sul web dove venivano pubblicati messaggi contenenti file multimediali relativi a materiale esplosivo. All'esito degli accertamenti l'indagato è risultato essere amministratore di un gruppo Telegram all'interno del quale venivano inoltre date indicazioni su come effettuare *data breach* e/o come violare siti web.
  Durante la perquisizione sono state individuate foto di prodotti idonei alla preparazione di esplosivi, video di esplosioni di ordigni manufatti rudimentali e evidenze di numerosi *data breach* contenenti credenziali di accesso ad account bancari e assicurativi.

- Nel mese di febbraio, personale della Centro Operativo per la Sicurezza Cibernetica di Milano e della locale D.I.G.O.S, ha dato esecuzione al decreto di perquisizione personale, locale e informatica emesso dalla Procura di Milano nei confronti di 5 minori residenti a Milano.
  L'attività investigativa ha avuto origine nel corso degli approfondimenti svolti sulla rete internet durante i quali il COSC di Milano ha individuato una storia pubblicata sul social Instagram che promuoveva l'adesione a un'azione criminosa contro le Forze dell'Ordine, inizialmente prevista per il 7 febbraio presso lo stadio San Siro. Gli indagati incitavano a partecipare all'evento portando in piazza del liquido infiammabile e dei fuochi pirotecnici da usare per assaltare e danneggiare le pattuglie della Polizia.

- Nel mese di marzo, personale del C.O.S.C. di Perugia e della D.I.G.O.S. di Brescia, ha dato esecuzione all'ordinanza di custodia cautelare in carcere emessa dal Tribunale di Perugia – Sezione GIP nei confronti di una persona indagata per il reato di cui all' art. 270 quinquies c.p. La posizione è emersa all'esito di un'articolata attività d'indagine svolta nell'ambito del contrasto al radicalismo islamico online di matrice jihadista; gli elementi acquisiti hanno consentito di rilevare una progressione nel comportamento dell'indagato da uno stadio di semplice partecipazione *online* a canali tematici a concrete progettualità per la causa jihadista.
- Nel mese di aprile i C.O.S.C di Bologna Genova e Milano, unitamente alle D.I.G.O.S competenti, hanno dato esecuzione alla perquisizione di 6 cittadini italiani indagati per il reato di cui all'art. 604 bis c.p., legati al gruppo neonazista "*Movimento Nazionalista e Socialista dei Lavoratori*", attivo sul social network russo VKontate.
- Nel mese di maggio 2025, personale del C.O.S.C e della Digos di Palermo, ha dato esecuzione al provvedimento di fermo di p.g nei confronti di due persone residenti nel palermitano, indagate per propaganda radicale di matrice jihadista attraverso la piattaforma Instagram; questi avevano pubblicato *post*, *nasheed*, e *stories* con esplicito riferimento a Islamic State e alla dottrina radicale salafita.

La Quarta Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La Quarta Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica rappresenta il presidio specializzato nel contrasto al **financial cyber crime** e alle **frodi digitali**, ambiti che incidono in maniera diretta sulla fiducia dei cittadini e sulla stabilità del sistema economico. La sua attività si colloca in un terreno complesso, dove la rapidità di evoluzione delle tecniche criminali impone un costante aggiornamento degli strumenti investigativi e una stretta collaborazione con il settore bancario, gli operatori postali e le principali piattaforme digitali.

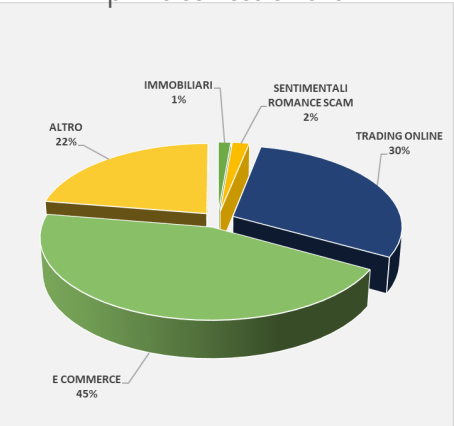
Il lavoro della Divisione non si limita alla repressione dei reati, ma integra **prevenzione, monitoraggio e sensibilizzazione**, con l'obiettivo di ridurre l'impatto delle truffe online e di rafforzare la consapevolezza collettiva. Attraverso indagini mirate, operazioni coordinate e un dialogo continuo con i partner istituzionali e privati, la Quarta Divisione contribuisce a proteggere i risparmi dei cittadini, a tutelare la regolarità dei mercati e a garantire la sicurezza delle transazioni digitali.
Elemento qualificante della sua missione è il **ruolo di coordinamento nazionale**: la Divisione assicura l'indirizzo operativo e metodologico delle attività svolte dai Centri

Operativi e dalle Sezioni territoriali, armonizzando le indagini e garantendo uniformità di approccio su tutto il territorio. Questa funzione di regia consente di valorizzare le informazioni raccolte a livello locale, trasformandole in conoscenza condivisa e in strategie comuni, e di mantenere un costante raccordo con le Autorità giudiziarie, le istituzioni di vigilanza e i principali attori del settore finanziario.

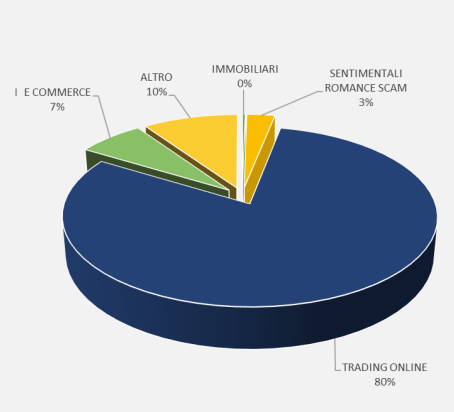
L'analisi delle evidenze riferibili al primo semestre dell'anno 2025 rivela come il *financial cybercrime* sia sempre più una delle forme predominanti e preminenti del crimine informatico, con una tendenza in aumento che permane a livello globale.

Indicatore	Primo semestre 2023	Primo semestre 2024	Primo semestre 2025	Δ 23→24	Δ 24→25	Δ Biennio
Truffe online (ril. nazionale)	7.661	9.690	9.261	↑**+26%**	↓**-4%**	↑**+21%**
Persone indagate	1.853	1.761	1.950	↓**-5%**	↑**+11%**	↑**+5%**
Somme sottratte	€ 58.253.567	€ 98.555.935	€ 109.235.401	↑**+69%**	↑**+11%**	↑**+88%**

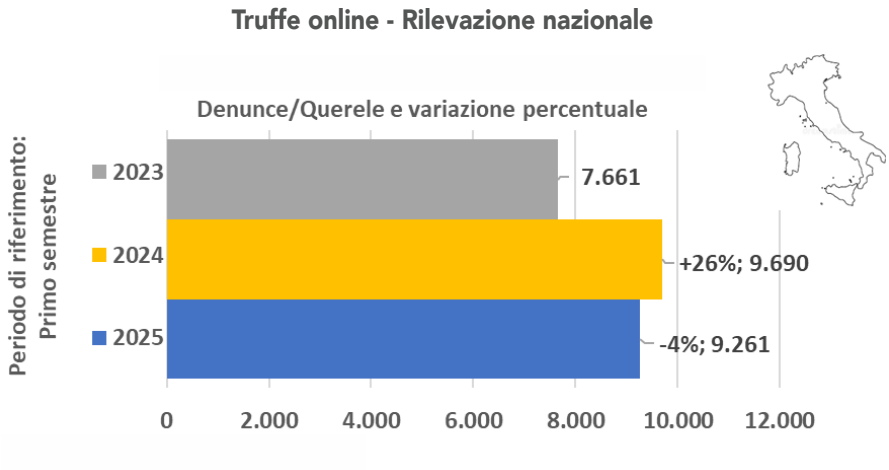
Truffe online - Casi trattati
primo semestre 2025



Truffe online - Somme sottratte
primo semestre 2025



Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025



Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

È stata registrata anche una significativa evoluzione di alcune di tali condotte criminose, caratterizzate sempre più dall'utilizzo di nuove tecnologie che ne agevolano la realizzazione massiva: attraverso l'utilizzo di *software* di "intelligenza artificiale" (IA) i criminali riescono a "costruire" immagini e audio di noti personaggi pubblici, rendendo sempre più credibili informazioni artefatte e inducendo in errore un numero sempre più ampio di utenti del *web*.

Molteplici e in continua evoluzione risultano le tecniche utilizzate dalle organizzazioni criminali, attivate in danno di cittadini, piccole e medie imprese (che costituiscono il tessuto economico portante del Paese), nonché, sovente, in danno delle più grandi e importanti aziende.

Persistono i più tradizionali *modi operandi*, tipici del crimine finanziario di interesse della Polizia Postale e per la Sicurezza Cibernetica. In primo luogo il c.d. *"phishing"*[1], che consente il furto dei dati sensibili per l'accesso ai sistemi di home banking, funzionale a illecite operazioni bancarie: lo scopo di tali tecniche di attacco è quello di entrare in possesso delle credenziali finanziarie delle vittime, per poter poi operare dai conti correnti online con le carte di credito/debito, attraverso prelievi, con bonifici o con l'acquisto di beni online.

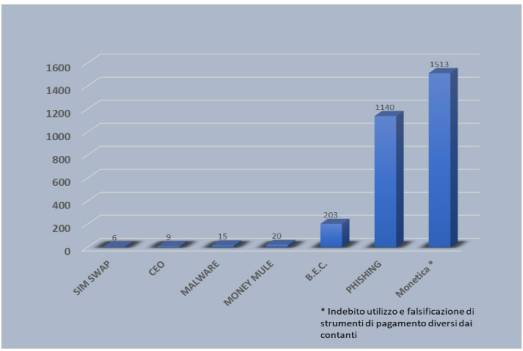
[1] Realizzabile anche nelle varianti del c.d. *"smishing"* (allorché non si utilizzi la classica email, ma il "veicolo" utilizzato per ingannare la vittima sia un messaggio telefonico) e del c.d. *"vishing"* (qualora si ricorra a un contatto diretto a voce).

Per quanto riguarda le fattispecie di truffe più comuni perpetrate online (come a esempio le vendite piramidali, le offerte di lavoro fasulle, i falsi prestiti di denaro, le finte locazioni immobiliari, le false vincite alle lotterie e le polizze assicurative fraudolente), rispetto al medesimo periodo dell'anno 2024, si registra una moderata flessione dei casi trattati con un aumento di circa l'11% di persone indagate.

Inoltre, nel periodo in esame, si è registrato un significativo aumento dei casi di *spoofing*, fenomeno che sta diventando sempre più preoccupante sia per le aziende che per gli utenti privati. Con l'evoluzione delle tecnologie digitali e l'adozione massiccia di strumenti di comunicazione online, i criminali informatici hanno affinato le loro tecniche di inganno, utilizzando lo *spoofing* per travisare la propria identità e ottenere accesso a informazioni sensibili. Tuttavia, recentemente l'Autorità per le Garanzie nelle Comunicazioni (Agcom) ha emanato una specifica delibera, recependo molte proposte tecnico giuridiche di questa Specialità, grazie alla quale potranno essere bloccate le numerazioni sospette, con la previsione di contenere sensibilmente il fenomeno citato.

Indicatore	Primo semestre 2023	Primo semestre 2024	Primo semestre 2025	Δ 23→24	Δ 24→25	Δ Biennio
Frodi informatiche e monetica (ril. nazionale)	5.354	4.557	4.116	↓**-15%**	↓**-10%**	↓**-23%**
Persone indagate	388	532	379	↑**+37%**	↓**-29%**	↓**-2%**
Somme sottratte	€ 21.536.551	€ 22.382.693	€ 28.466.633	↑**+4%**	↑**+27%**	↑**+32%**

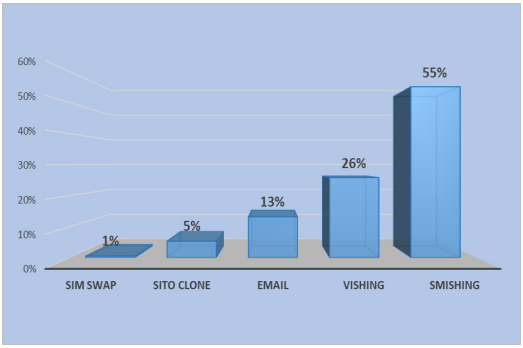
Crimini economico - finanziari online – Primo semestre



Prevalgono i casi di phishing (1.140) e di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti ex art. 493-ter c.p. (1.513), seguiti a distanza da B.E.C., money mule, malware, CEO fraud e SIM swap. I dati confermano la centralità delle frodi digitali legate ai sistemi di pagamento e alle tecniche di ingegneria sociale.

Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Furto identità – Primo semestre 2025



Distribuzione percentuale delle principali modalità di furto d'identità rilevate nel primo semestre 2025: prevale lo *smishing* (55%), seguito dal *vishing* (26%) e dall'uso fraudolento delle *email* (13%). Residuali i casi di *sito clone* (5%) e Sim Swap (1%)

Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025

Per quanto attiene ai fenomeni criminosi riconducibili al c.d. *financial cybercrime*, il periodo in esame è stato caratterizzato dalle consuete dinamiche delinquenziali prevalentemente riconducibili al c.d. *"man in the middle"*, nelle varianti del c.d. *BEC (Business e-mail compromised)*, e del c.d. *Chef Executive Officer fraud* (CEO *Fraud*).

Questo Servizio ha altresì registrato l'evoluzione di fenomeni criminali già collaudati e conosciuti come il *trading online*, che grazie alle nuove tecnologie a disposizione di cyber criminali, come la c.d. intelligenza artificiale (IA), riesce a modificare in maniera verosimile immagini e audio di noti personaggi pubblici, rendono credibili informazioni artefatte, inducendo in errore e creando grave nocumento a una vasta pletora di utenti del web.

Le recenti evidenze investigative hanno consentito di definire le nuove metodologie criminali utilizzate per commettere o monetizzare le attività fraudolente, in particolare il *Deep Fake* e le *criptovalute*.

Deep Fake

Nato con l'odierno sviluppo dell'intelligenza artificiale, si concentra sulla realizzazione di contenuti ingannevoli da veicolare sui principali social con lo scopo di lucrare su tale inganno.

In particolare si parla di *Deep fake*, ossia di contenuti più difficili da individuare come falsi perché "messi in bocca" (letteralmente) a personaggi noti, come fonte più credibile di un qualunque contenuto diffuso. Tra le modalità riscontrate, si individua tra i principali, lo sfruttamento dell'immagine di soggetti istituzionali, dell'imprenditoria e del mondo politico, mediante i quali vengono realizzati video di sponsorizzazioni (sulle principali piattaforme social) di investimenti

finanziari. Tra i vari social spicca come canale di divulgazione il social Facebook. Non ultimo, lo sfruttamento della IA sta portando all'evoluzione del sopra citato *CEO Fraud*, in cui i cybercriminali, con l'acquisizione di fonti aperte relative al soggetto bersaglio, possono ricrearne la voce o le movenze permettendo al falso amministratore di impartire disposizioni su uno o più bonifici correlati a una inesistente operazione finanziaria riservata e urgente.

Criptovalute

Con la diffusione e l'evoluzione delle nuove tecnologie, nel corso dell'ultimo decennio, si è sviluppato in ambito finanziario un fenomeno che ha generato un cambiamento radicale nell'economia globale: le criptovalute.

Le prime a essere state create sono i noti Bitcoin lanciati nel 2009, da allora la diffusione di tali strumenti è aumentata esponenzialmente.

Tali rappresentazioni digitali di valore hanno come obiettivo quello di introdurre dei sistemi di pagamento svincolati dai sistemi bancari tradizionali, non aventi corso legale in alcuna giurisdizione, non emessi o garantiti da alcuna giurisdizione. Tali sistemi di pagamento riescono a svolgere le predette funzioni solo mediante l'accordo che intercorre tra la comunità degli utilizzatori della valuta virtuale, attraverso un sistema di funzionamento basato sull'utilizzo della tecnologia *blockchain*.

Quest'ultima può essere definita come una sorta di "registro digitale", che rientra nella più ampia categoria della c.d. "tecnologia del registro pubblico distribuito" (DLT Distributed Ledger Technology).

Si tratta di un meccanismo di registrazione e condivisione di dati attraverso vari "blocchi", ciascuno contenente la registrazione dei medesimi dati e gestito da una rete di server (i c.d. nodes).

Il meccanismo è basato sulla crittografia, e dunque su specifici algoritmi matematici usati per creare una struttura di raccolta dati in continua crescita, nella quale tali dati possono unicamente essere aggiunti ma non rimossi, anonimi e immodificabili.

Le criptovalute, pertanto, mirano a sfruttare al tempo stesso le caratteristiche della moneta "fisica" e di quella "elettronica", creando dunque un sistema di pagamento che consente sia di effettuare pagamenti a distanza (come avviene con la moneta elettronica), sia di garantire una certa forma di anonimato, e più precisamente di "pseudonimato": il *wallet* che ha disposto o ricevuto l'operazione rimane infatti noto, senza che però ne sia automaticamente svelato il possessore, come avviene per il contante o moneta "fisica".

La caratterizzazione bifronte della valuta virtuale, pertanto, oscillante tra "moneta" e "rappresentazione di valore", genera di fatto problematiche operative

nella fase delle indagini di polizia, soprattutto nella configurazione di reati, come il riciclaggio, storicamente collegati al trasferimento fraudolento di beni e fondi monetari in moneta di conto, laddove le transazioni registrate sulla *blockchain*, benché pubbliche, garantiscono l'anonimato degli attori coinvolti nella transazione e l'oggettiva difficoltà della tracciabilità delle stesse.
Seguire le *cryptocurrencies* rappresenta l'attuale sfida della moderna polizia giudiziaria e dell'Autorità giudiziaria per contrastare le attività criminali, con strumenti tecnologici e collaborazioni internazionali.

I fenomeni criminali sopradescritti sono perpetrati principalmente da sodalizi criminosi transnazionali che, tramite articolate tecniche di riciclaggio, reimpiegano gli ingenti proventi in ulteriori attività criminose di elevato allarme sociale e in attività lecite, idonee a occultare la provenienza criminosa dei valori.

Si riportano di seguito le attività più rilevanti realizzate nel periodo dal 1 gennaio al 30 giugno 2025:

- Il Centro Operativo per la Sicurezza Cibernetica Reggio Calabria e la Guardia di Finanza, a conclusione di una complessa indagine coordinata dalla Procura della Repubblica di Cosenza, hanno individuato un'organizzazione criminale di 51 persone, coinvolte nell'associazione a vario titolo, residenti a Cosenza e nell'hinterland che, attraverso l'istruzione di pratiche false, monetizzavano crediti di imposta relativi a interventi edilizi mai effettuati e successivamente riciclavano il denaro ottenuto tramite acquisti di lingotti e/o di monete d'oro.
  90 militari della Guardia di Finanza di Cosenza con l'ausilio delle unità cinofile "cash dog" e di un elicottero, 60 operatori della Polizia di Stato, tra cui gli specialisti cyber del Servizio Polizia Postale e per la Sicurezza Cibernetica e con il supporto del Reparto Prevenzione Crimine "Calabria Settentrionale" di Rende, hanno eseguito 3 ordinanze di custodia cautelare nei confronti delle persone ritenute a capo dell'organizzazione, 30 perquisizioni e il sequestro per un equivalente di 15 milioni di euro.

- Gli investigatori dei Centri Operativi per la Sicurezza Cibernetica di Ancona, Napoli, Pescara e Roma hanno dato esecuzione a un decreto di perquisizione personale e locale, emesso dalla Procura della Repubblica presso il Tribunale di Ancona, nei confronti di 5 persone indagate per aver concorso nel reato di frode informatica e sostituzione di persona, in quanto resisi responsabili a vario titolo di accessi abusivi aggravati a sistemi informatici preordinati all'utilizzo fraudolento del "bonus cultura".

- I Centri Operativi per la Sicurezza Cibernetica di Firenze, Napoli e Roma, unitamente a personale di questo Servizio, hanno dato esecuzione a un decreto di perquisizione personale, locale e informatica emesso dalla Procura della Repubblica presso il Tribunale di Potenza, nei confronti di 6 persone indagate per concorso in truffa aggravata. L'attività trae origine dalla denuncia di un cittadino che contattato attraverso la tecnica dello *"Spoofing telefonico"* forniva le proprie credenziali dell'*home banking* subendo un danno economico di circa € 119.540.
- Il Centro Operativo per la Sicurezza Cibernetica di Napoli ha eseguito un'ordinanza di applicazione della misura cautelare degli arresti domiciliari emessa dal Giudice per le Indagini Preliminari presso il Tribunale di Genova nei confronti di una persona indagata per truffa aggravata. Il provvedimento è stato emanato all'esito di un'attività di indagine condotta dal Centro Operativo per la Sicurezza Cibernetica di Genova e scaturita dalla denuncia di un cittadino che, a seguito di chiamate apparentemente provenienti da Poste Italiane e dal Centro operativo per la Sicurezza Cibernetica di Genova, veniva convinto a effettuare presso un ufficio postale di Genova due bonifici dell'importo di circa € 29.000 e € 22.800 a favore di un conto riconducibile in realtà agli indagati.
- *ACTION DAY.* Personale di questo Servizio Polizia Postale per la Sicurezza Cibernetica, unitamente a quello dei Centri Operativi per la Sicurezza Cibernetica di Ancona, Bari, Bologna, Firenze, Milano, Napoli, Perugia, Pescara, Reggio Calabria, Roma, Torino, ha eseguito perquisizioni nei confronti di 28 persone dedite alla consumazione di reati specifici quali *phishing*, *smishing*, *spoofing* e accesso abusivo a sistema informatico. L'attività di polizia giudiziaria, ha coinvolto 81 operatori dei Centri Operativi per la Sicurezza Cibernetica dislocati sul territorio nazionale.
- Il Centro Operativo per la Sicurezza Cibernetica Veneto nell'ambito di una complessa operazione di polizia giudiziaria coordinata dalla Procura della Repubblica di Roma, ha individuato nove persone, tutte residenti in provincia di Roma e Frosinone, facenti parte di un sodalizio criminale responsabile di una truffa organizzata ai danni di una nota concessionaria di autovetture della Provincia di Venezia, per un importo complessivo di 300.000 euro.
  La concessionaria veneziana, che nel frattempo aveva versato l'ingente somma a titolo di anticipo sulla fornitura delle automobili, si è insospettita da alcuni particolari emersi nel corso della compravendita e si è rivolta al C.O.S.C. di Venezia che ha immediatamente attivato le indagini.
  Il tempestivo sequestro posto in essere dagli uomini della Polizia Postale ha permesso di bloccare buona parte del denaro, che nel frattempo era stato trasferito

su molteplici conti correnti intestati a società fittizie e radicati presso banche ubicate in provincia di Roma e Frosinone, nonché verso un conto corrente attivato presso un istituto bancario di S. Marino.
L'attività di polizia giudiziaria, che ha visto la collaborazione tramite rogatoria internazionale della Gendarmeria Sanmarinese, si è concretizzata con l'arresto di un uomo residente in provincia di Roma trovato in possesso di falsi documenti d'identità utilizzati per la truffa e l'esecuzione di nove perquisizioni domiciliari a carico di altrettante persone, accusate a vario titolo, di far parte dell'organizzazione criminale.

- "*OPERAZIONE MORGANA*". Il Centro Operativo per la Sicurezza Cibernetica di Milano, con l'ausilio di personale del Reparto Prevenzione Crimine e di un'unità cinofila, ha dato esecuzione a un'ordinanza di custodia cautelare in carcere emessa dal GIP del Tribunale di Milano nei confronti di 3 indagati e a un decreto di perquisizione locale e personale emesso dalla Procura della Repubblica presso il Tribunale di Milano nei confronti di 7 persone indagate per reati di truffa aggravata in concorso. Le indagini sono partite a seguito della segnalazione del personale di un ufficio postale, insospettito dal comportamento anomalo di un'anziana correntista che aveva effettuato cospicui prelievi di denaro in un arco temporale molto breve per un totale di oltre 160.000 €. Le attività del C.O.S.C. Lombardia hanno consentito di disarticolare il sodalizio criminoso facente capo a una sedicente cartomante, la quale, con una serie di scuse ingannevoli, ha ingenerato nella vittima il timore di un pericolo immaginario, convincendola a consegnarle nel tempo ingenti somme di denaro.
- *OPERAZIONE "FAKE LOAN"*. Personale del Centro Operativo per la Sicurezza Cibernetica di Palermo, ha eseguito un'ordinanza del Giudice per le Indagini Preliminari del Tribunale di Termini Imerese (PA) di applicazione di misure cautelare personali nei confronti di cinque persone, ritenute responsabili del reato di associazione a delinquere finalizzata alla commissione di truffe in danno di banche e società finanziarie. L'attività trae origine dalla denuncia presentata dal settore Fraud Management Sicilia di Poste Italiane S.p.A. L'articolata attività di indagine ha disvelato l'esistenza di una consolidata struttura criminale che forniva un illecito servizio di intermediazione per l'ottenimento di finanziamenti e che offriva anche la possibilità di aggirare il blocco dei clienti in "*black list*" dovuta all'iscrizione presso la Centrale Rischi di Intermediazione Finanziaria. Le attività investigative venivano avviate a seguito di un esposto presentato dai responsabili dell'Ufficio siciliano *Fraud Management* di Poste Italiane S.p.a., con il quale vi è una sinergica e costante collaborazione.

- Personale dei Centri Operativi per la Sicurezza Cibernetica di Bologna e di Napoli, in collaborazione con la Guardia di Finanza di Bologna, hanno eseguito sul territorio campano e bolognese un'ordinanza di misure cautelari e interdittive, emessa dalla DDA di Bologna nei confronti di 29 persone, oltre a 37 perquisizioni a 29 soggetti e 8 società, con il contestuale sequestro preventivo di circa 3 milioni di euro. L'attività di indagine ha permesso di individuare un'associazione criminale operante in Emilia Romagna e in Campania, avente quale programma criminoso quello di commettere numerosissimi delitti quali l'emissione di fatture per operazioni inesistenti, omesse dichiarazioni fiscali, presentazione di dichiarazioni fraudolente mediante l'uso di fatture per operazioni inesistenti, indebita compensazione e auto riciclaggio.
- A seguito di indagini coordinate dalla Procura della Repubblica di Roma, Centro Operativo per la Sicurezza Cibernetica di Roma ha eseguito un'ordinanza di custodia Cautelare agli arresti domiciliari, emessa dal Giudice delle indagini preliminari presso il Tribunale di Roma, nei confronti di un sessantatreenne di nazionalità argentina, gravemente indiziato dei reati di esercizio abusivo della professione medica su territorio italiano (attesa l'inesistente iscrizione presso l'apposito Albo Nazionale e l'assenza del provvedimento della Regione Lazio per l'esercizio dell'attività di medico straniero in Italia) e di truffa aggravata ai danni di persone offese, approfittando della loro vulnerabilità psicologica, perché in forte apprensione per le sorti del figlio minore affetto da grave forma di autismo. Le indagini hanno avuto origine dalla denuncia sporta dai genitori di un quindicenne con disturbi neurologici, i quali si erano rivolti al professionista argentino in quanto sedicente "luminare" per quel tipo di patologia, sulla base di informazioni acquisite online, da cui risultava un curriculum ben strutturato sulla pratica di terapie altamente innovative. Lo stesso infatti millantava di essere stato il costante riferimento sanitario di Sua Santità Papa Giovanni Paolo II, nonché quello di 54 Cardinali in carica, circostanze poi smentite in sede di accurati accertamenti investigativi. Il percorso terapeutico, durato 2 anni, per il quale sono stati versati dalla famiglia circa 30 mila euro in contanti, conseguiti dal sedicente medico con "abilità collaudata e glaciale scaltrezza", ha comportato continue somministrazioni di sostanze vietate (prodotti olezzanti, con data di scadenza superata e certamente guasti). Durante le indagini la Polizia Postale, su delega della Procura della Repubblica di Roma, ha eseguito un'accurata perquisizione presso l'abitazione del sedicente professionista, ove venivano rinvenute circa 400 schede personali di pazienti, ancora da identificare compiutamente, di cui alcuni affetti da gravi forme di autismo, nonché numerose provette di laboratorio contenenti esami di urina, sangue e numerose confezioni sigillate

di medicinali scaduti da anni. Oltre all'applicazione della misura personale, il Giudice per le indagini preliminari di Roma, su richiesta dell'ufficio della Procura della Repubblica, ha disposto il sequestro preventivo dei siti internet, utilizzati dall'indagato per vendere integratori e pubblicizzare la propria attività, mediante oscuramento delle pagine web e la conseguente disabilitazione dei relativi domini da notificare a tutti gli ISP presenti sul territorio.

La Quinta Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

All'interno del Servizio Polizia Postale è incardinata la quinta divisione, una struttura con competenze specifiche nel campo dell'Information Technology, nata per offrire supporto e strumenti avanzati alle attività legate al dominio cibernetico e alle indagini di *digital forensics*. Questa divisione ha un compito centrale: da un lato contribuisce a rafforzare la sicurezza informatica, tutelando sistemi e dati; dall'altro favorisce la collaborazione con istituzioni pubbliche e realtà private, creando le condizioni per sviluppare nuove soluzioni e stimolare il progresso scientifico e tecnologico.
Alcune delle principali attività che questa divisione si occupa di svolgere:

- Assicurare un sostegno concreto, sia tecnico che operativo, a tutte le attività che riguardano la sicurezza cibernetica e le indagini digitali (*digital forensics*) in merito alle attività d'istituto della Specialità;
- Mantenere e sviluppare relazioni con enti e istituzioni, sia pubbliche sia private, che operano nel campo della ricerca e dell'innovazione scientifica, così da favorire un aggiornamento continuo di metodologie e soluzioni tecnologiche. Allo stesso tempo, la divisione partecipa alla definizione dei programmi di formazione specialistica, contribuendo a far crescere le competenze necessarie in un settore in costante evoluzione;
- Occuparsi della pianificazione delle acquisizioni in ambito IT e della programmazione triennale dei fabbisogni, coordinando di conseguenza anche la gestione dei contratti di fornitura e l'intero processo legato alle procedure di acquisto;
- Coordinare, nei settori tecnici di rispettiva competenza, le articolazioni territoriali della Specialità anche in relazione all'analisi delle esigenze e alla realizzazione di nuovi sistemi IT a supporto delle attività info-investigative;
- Gestire e implementare l'infrastruttura tecnologica del Servizio attuando gli indirizzi e le politiche di sicurezza IT delineate dai competenti uffici della Polizia di Stato, secondo gli standard e le normative di settore;

- Gestire tutti gli *asset* tecnologici della Specialità a livello nazionale e svolgere le funzioni di *focal point* per gli accessi alle banche dati istituzionali e investigative in uso al Servizio.

In tema di Innovazione e Ricerca Tecnologica, presso la predetta divisione, è stato istituito l'**Ai Lab4Cyber**, ovvero un laboratorio volto alla ricerca e innovazione nel settore dell'intelligenza artificiale a supporto delle investigazioni nel settore Cyber. Detto laboratorio oltre a analizzare gli impatti del Regolamento Europeo e della legislazione nazionale in tema di utilizzo dell'Intelligenza Artificiale a supporto delle investigazioni cyber, provvede altresì alla sperimentazione di modelli e sistemi di IA idonei a supportare le investigazioni nel settore cibernetico e dell'analisi delle immagini per il contrasto alla pedopornografia. In particolare, nell'anno in corso, vista la crescente complessità e velocità degli attacchi informatici, unita all'enorme quantità di dati da monitorare, sono stati istituiti, presso ogni Nucleo Operativo di Sicurezza Cibernetica, laboratori di ricerca locali da dedicare allo studio, allo sviluppo e alla sperimentazione di soluzioni basate su tecniche di intelligenza artificiale, coordinati da questa Divisione. In particolare, nell'anno in corso è stato possibile acquisire, sia presso il Servizio Centrale che presso i 18 Centri Operativi, innovative tecnologie server dotate delle più moderne schede GPU volte all'impiego sperimentale e operativo di tecnologie di intelligenza artificiale a supporto delle investigazioni cyber.

Presso la predetta Divisione vengono, altresì, svolte attività di ricerca di mercato per comprendere le nuove tecnologie disponibili e in via di sviluppo. In merito, sono state consolidate collaborazioni con il mondo accademico attraverso la condivisione di progetti innovativi che vedono l'impiego dell'Intelligenza Artificiale sia nel settore delle investigazioni di pertinenza della Specialità che nella protezione delle infrastrutture critiche.

Per quanto attiene le dotazioni tecnologiche a supporto delle investigazioni, nel corso del 2025 si è provveduto a dare particolare impulso all'avvio di un rilevante programma di potenziamento, atteso il recente incremento dell'organico della Specialità. In particolare, sono state acquisite:

- tecnologie a supporto delle attività di *digital forensics* mediante la fornitura di nuove apparecchiature hardware a elevate prestazioni, nonché tecnologie software per l'acquisizione e l'analisi forense di dispositivi digitali fissi e mobili;
- strumentazioni di ultima generazione volte all'analisi degli incidenti informatici e sistemi di protezione dalle intrusioni, sicurezza per reti aziendali e strumenti di protezione da malware e ransomware;
- piattaforme di servizi info-investigativi volte a supportare le attività d'indagine;
- postazioni di lavoro fisse e mobili con relativi accessori di supporto per le esigenze degli uffici territoriali e centrali;
- tecnologie di connettività di ultima generazione per rispondere alle esigenze operative connesse allo svolgimento delle attività investigative delegate a questa Specialità;
- tecnologie di virtualizzazione per l'implementazione di una infrastruttura maggiormente resiliente alle attività di backup dei dati e dei sistemi;
- tecnologie per la realizzazione e l'integrazione di modelli di intelligenza artificiale a sostegno delle attività di indagine.

Oltre alle predette attività di ampliamento sopra descritte, si è provveduto, altresì, a finalizzare numerose procedure amministrative volte al rinnovo dei contratti già in essere e concernenti le dotazioni strumentali in uso alla Specialità e necessarie a garantire le attività d'Istituto.
Rilevante è stato, inoltre, l'impegno profuso in contesti internazionali che ha visto la Quinta Divisione impegnata su diversi tavoli di lavoro.

Di particolare rilievo è stato il ruolo svolto, sotto la Presidenza Italiana, nell'ambito del gruppo G7 Roma-Lione, sottogruppo *High Tech Crime*, e in ambito EUROPOL, dove sono stati ricoperti vari ruoli sia nel Consiglio di amministrazione dell'EuCB (*European Clear Board*), un organismo volto a individuare le tecnologie più innovative a supporto delle investigazioni, che presso i vari gruppi di lavoro costituiti presso detto organismo, tra cui quelli volti all'analisi del Regolamento Europeo sull'Intelligenza Artificiale, recentemente pubblicato nella Gazzetta Ufficiale Europea, la cui effettiva entrata in vigore avverrà nel 2025.

Preme sottolineare, inoltre, che, sempre in tema di Intelligenza Artificiale, la Quinta Divisione del Servizio Polizia Postale ha fornito un rilevante contributo all'interno dell'*Europol Innovation Lab* al fine di affrontare e anticipare le complesse sfide poste dall'evoluzione delle metodologie criminali.

In particolare, le attività svolte nell'ambito dell'*Innovation Lab* hanno evidenziato la rilevanza delle attività di innovazione e della ricerca tecnologica a supporto delle investigazioni. Infatti, come noto, i rapidi progressi tecnologici hanno avuto profondo impatto su come la criminalità utilizzi dette nuove tecnologie per implementare tattiche operative di attacco sempre più complesse, che possono essere contrastate mediante l'utilizzo di tecnologie che sfruttano l'impiego dell'IA e una stretta collaborazione tra le forze dell'ordine supportate anche da EUROPOL.

Inoltre, la Divisione ha dedicato particolare impegno anche all'ambito formativo, sviluppando percorsi dedicati alla sicurezza informatica e all'*intelligence*. In questo contesto sono stati realizzati moduli mirati a accrescere la consapevolezza (*awareness*) degli utenti e a promuovere un utilizzo corretto e responsabile delle tecnologie di intelligenza artificiale, mettendo in luce sia i benefici che i potenziali rischi connessi al loro impiego. Sempre in merito alla somministrazione di moduli formativi che hanno coinvolto la Quinta Divisione, sono stati erogati corsi di formazione dedicati alle tecniche e agli strumenti impiegati nelle attività di *digital forensics*, con particolare attenzione alle metodologie di acquisizione, conservazione e analisi delle evidenze digitali. I percorsi includono inoltre approfondimenti sull'analisi e sul funzionamento della tecnologia *blockchain*, esaminata sia dal punto di vista tecnico sia in relazione alle sue applicazioni e implicazioni in ambito di sicurezza informatica e investigazioni digitali.

Detti moduli formativi sono stati resi disponibili sia al personale della Polizia di Stato (in vari ruoli direttivi e non direttivi) che a determinate categorie di utenza, inclusi i partecipanti al corso di Cyber Academy realizzato con gli Istituti ITS. Nel nuovo anno è, altresì, prevista l'attivazione di un modulo di IA di livello universitario.

Analisi dei principali attacchi noti del primo semestre 2025 verso il settore Manufacturing a livello globale e in Italia

Presentiamo in questa sezione alcune informazioni di approfondimento a complemento dei dati del rapporto Clusit 2025 con particolare riferimento agli attacchi andati a buon fine e di pubblico dominio verso il settore Manufacturing nel primo semestre dell'anno in corso e il confronto con gli anni precedenti (2018-24).

Nel rapporto sono presentati i dati globali, distinguendo tra attacchi globali e attacchi diretti verso il nostro paese.

Nelle tabelle, la prima relativa al contesto globale e la seconda all'Italia, sono riportati sia il totale di attacchi verso il settore MFG che gli attacchi totali dell'anno/periodo in corso e, successivamente, la percentuale di attacchi verso il settore rispetto al totale.

A livello Global

ATTACCANTI	2018	2019	2020	2021	2022	2023	2024	H1 2025	Totale
Cybercrime	21	24	58	68	116	149	212	200	848
Hacktivism	0	0	0	0	4	7	20	7	38
Espionage/ Sabotage	10	12	6	4	9	6	4	1	52
Information Warfare	3	0	1	0	0	0	0	5	9
Totale anno	34	36	65	72	129	162	236	213	947
Totale attacchi anno	1554	1667	1874	2049	2489	2779	3771	2755	18938
% attacchi su totale anno	2,2	2,2	3,5	3,5	5,2	5,8	6,3	7,7	5,0
% crescita anno su anno	0,0	0,0	0,0	10,8	79,2	25,6	45,7	-9,7	

A livello Italia

ATTACCANTI	2018	2019	2020	2021	2022	2023	2024	H1 2025	Totale
Cybercrime	0	0	8	12	35	41	54	35	185
Hacktivism	0	0	0	0	0	0	4	1	5
Espionage/ Sabotage	2	2	1	0	0	0	0	0	5
Information Warfare	0	0	0	0	0	0	0	0	0
Totale anno	2	2	9	12	35	41	58	36	195
Totale attacchi anno	30	37	48	70	188	310	373	280	1336
% attacchi su totale anno	6,7	5,4	18,8	17,1	18,6	13,2	15,5	12,9	14,6
% crescita anno su anno	0,0	0,0	0,0	33,3	191,7	17,1	41,5	-37,9	

Infine, è stata calcolata la percentuale di crescita anno su anno, portando a 0% il 2018: i numeri (visibili anche nel secondo grafico) indicano di quanto sono cresciuti gli attacchi rispetto all'anno precedente.

Nei grafici, invece, oltre all'andamento totale degli attacchi verso il settore e la crescita anno su anno, sono indicati per ogni categoria (attaccante, tecnica, geografia delle vittime e severity degli attacchi) un confronto tra la situazione del 2024, quella del primo semestre 2025 ed i trend 2018-1H25.

Il primo semestre del 2025 ha confermato una tendenza ormai costante: il settore manifatturiero continua a essere uno dei bersagli preferiti della criminalità informatica a livello globale. Dalle linee di produzione automatizzate alle catene di fornitura interconnesse, il manufacturing è oggi un ecosistema ibrido in cui la convergenza tra Information Technology e Operational Technology moltiplica la superficie d'attacco, generando nuove vulnerabilità e amplificando l'impatto degli incidenti cyber.

Nel primo semestre 2025, infatti, gli attacchi verso il settore manufacturing hanno quasi eguagliato il totale registrato nell'intero 2024 (213 contro 236), confermando un incremento percentuale significativo e un'evidente accelerazione rispetto al trend medio 2018–2024. Dopo il raddoppio registrato tra il 2019 e il 2021 e il picco del 2022 (+79% sul 2021), il 2025 sembra destinato a stabilire un nuovo massimo storico.

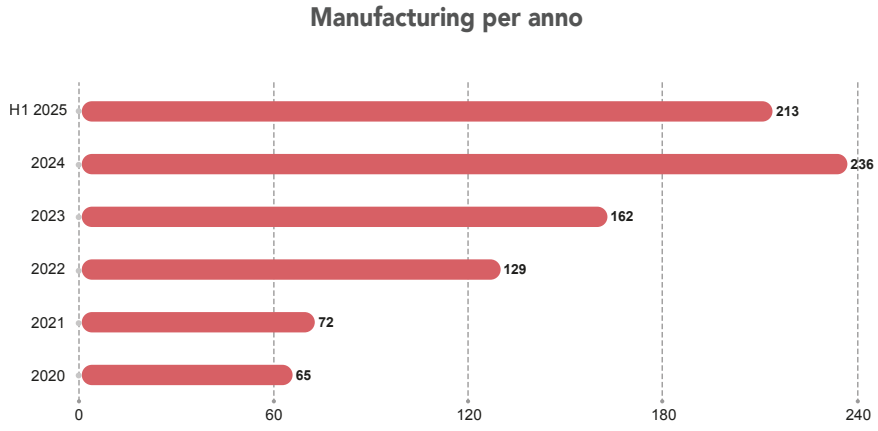


Grafico 1

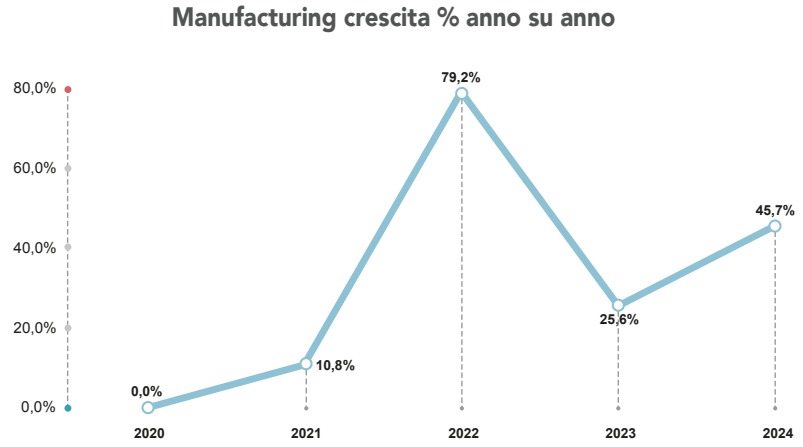


Grafico 2

Il Cybercrime si conferma la minaccia principale per questo settore con oltre il 94% dei casi, con minime percentuali di Hacktivism, attività di intelligence ed information warfare (sempre parecchio problematiche da attribuire). Le finalità economiche restano il motore dominante, con gruppi criminali sempre più strutturati che operano secondo logiche quasi industriali: specializzazione dei ruoli, outsourcing dei servizi di intrusione, marketplace di exploit e ransomware-as-a-service.

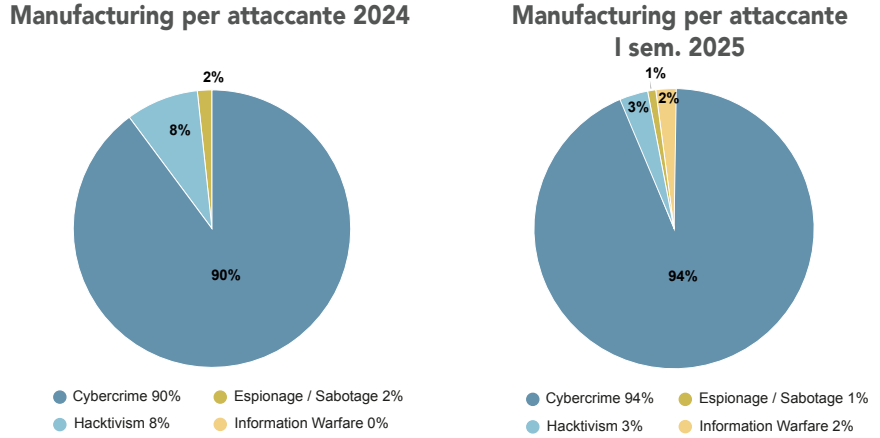


Grafico 3

Il Malware (nello specifico ransomware) è sensibilmente sceso nel 2024, in primis per colpa degli 0-Day. Inquietante il numero di attacchi a vulnerabilità note e non patchate (20%) quasi triplicato. Comunque la "pesca a strascico" del malware è meno onerosa e rende sempre (**Grafico 4**).

Sul piano geografico, l'Europa consolida il proprio ruolo di bersaglio primario, con il 48% degli attacchi globali al settore manufacturing nel 2024, il doppio rispetto all'America, ed un trend che si mantiene stabile nel 2025, seppur con una lieve attenuazione. L'Asia segue con valori comparabili, mentre Oceania e Africa rimangono aree marginali ma in crescita, segnale di un'espansione del fenomeno. Da valutare meglio la consistenza dei numeri relativi ad attacchi nel "Rest Of the World", ovvero Oceania ed Africa che risultano poco rappresentativi (**Grafico 5**).

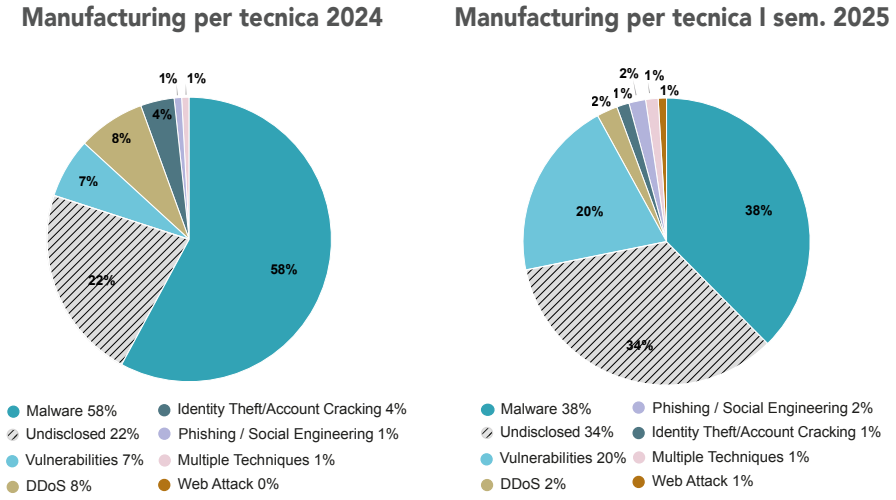


Grafico 4

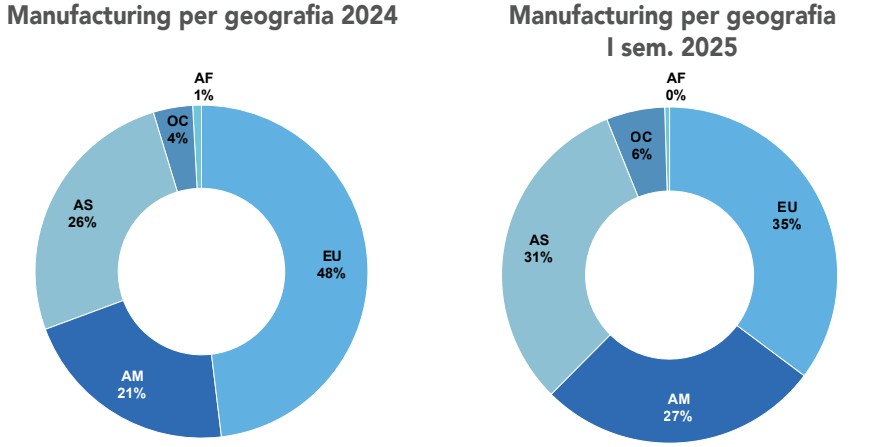


Grafico 5

Gli attacchi con impatti critici erano poco oltre i venti punti nel 2024 (22%) e sono purtroppo risaliti al 33% nel primo semestre del 2025 a scapito di quelli meno gravi (vedremo poi cosa succede alla fine dell'anno) segno che la gravità media degli incidenti sta crescendo. Un dato che deve far riflettere, soprattutto considerando che oltre l'80% degli eventi classificati come high severity compromette in modo significativo la produzione o la supply chain.

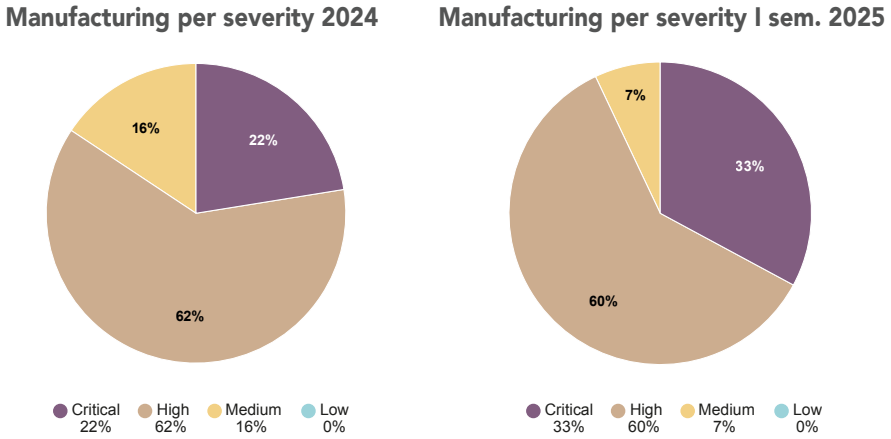
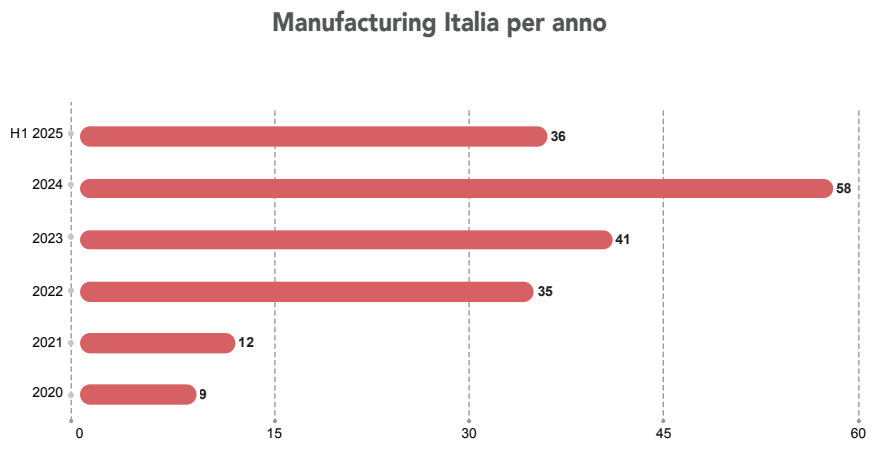


Grafico 6

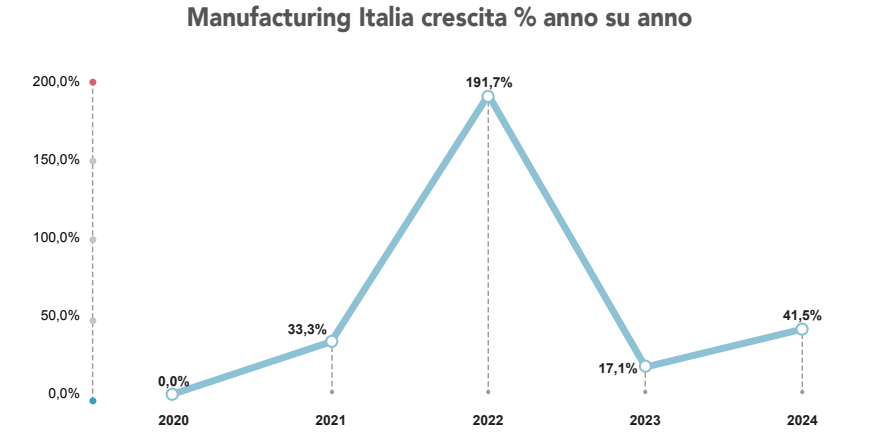
La situazione italiana

In Italia, il settore mostra un andamento solo lievemente più favorevole rispetto al dato globale: il 41% degli attacchi nel 2024 e il 36% nel primo semestre 2025, contro il 45% della media mondiale. Il numero complessivo di incidenti, 36 nei primi sei mesi dell'anno contro i 58 del 2024, resta comunque elevato e conferma la rilevanza strategica del manifatturiero nazionale come nodo critico della filiera europea.



© Clusit - Rapporto 2025 sulla Cybersecurity

Grafico 7



© Clusit - Rapporto 2025 sulla Cybersecurity

Grafico 8

Il Cybercrime si conferma la minaccia principale per questo settore anche in Italia con oltre il 93% dei casi e la tendenza rimane anche per il 2025.

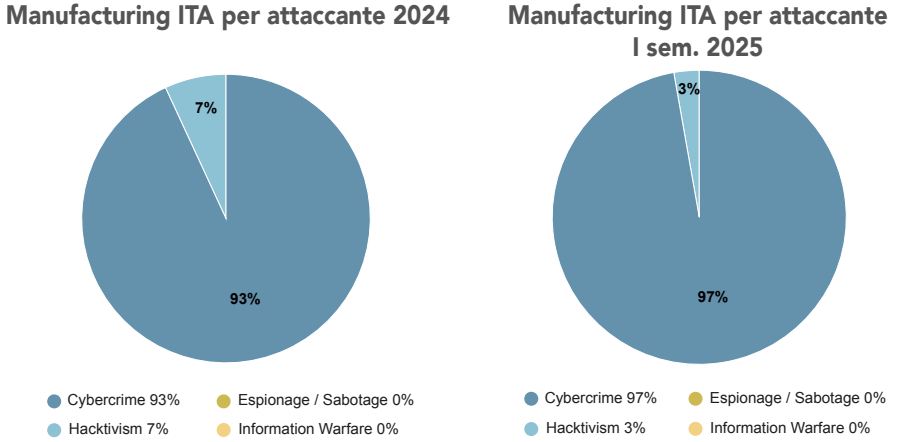
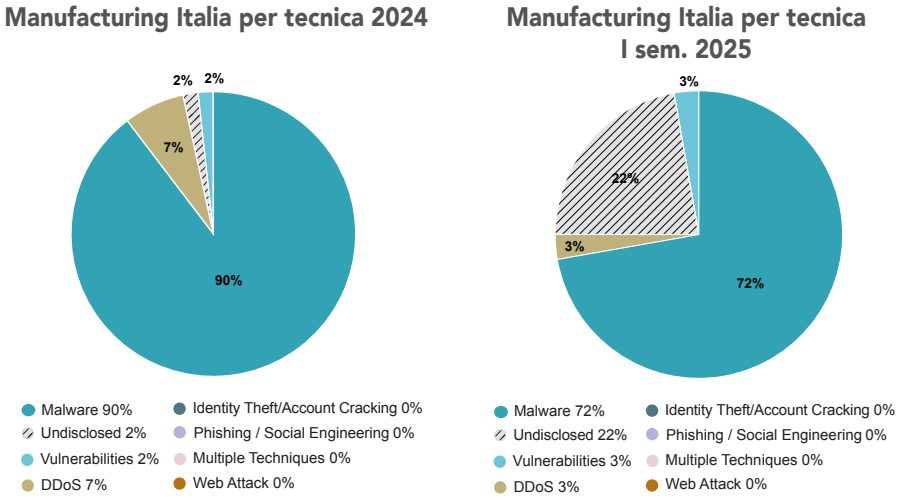


Grafico 9

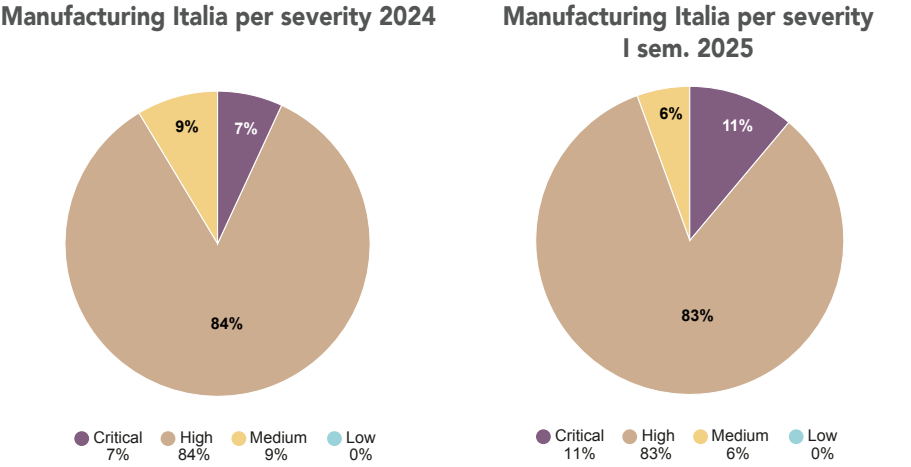
Il Malware (nello specifico ransomware) si è attestato all' 89% nel 2024. Si noti che nel 2024 si sono riscontrati meno incidenti rispetto alle vulnerabilità non patchate e agli 0-Day (Unknown), ma di contro sono aumentati i DDoS. Nel 2025 gli 0-Day son riapparsi in maniera sensibile riducendo le altre problematiche in proporzione (Grafico 10).

Per i danni creati dagli attacchi, il 2025 risale all'11% di Critical severity, ma non ai livelli del 2023. Comunque un 83-84% di High è decisamente oltre soglia di attenzione (Grafico 11).



© Clusit - Rapporto 2025 sulla Cybersecurity

Grafico 10



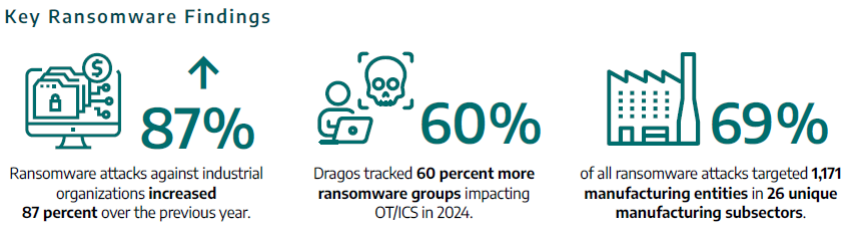
© Clusit - Rapporto 2025 sulla Cybersecurity

Grafico 11

Alcuni dati dal Report Dragos ICS/OT CyberSecurity Year in Review 2025

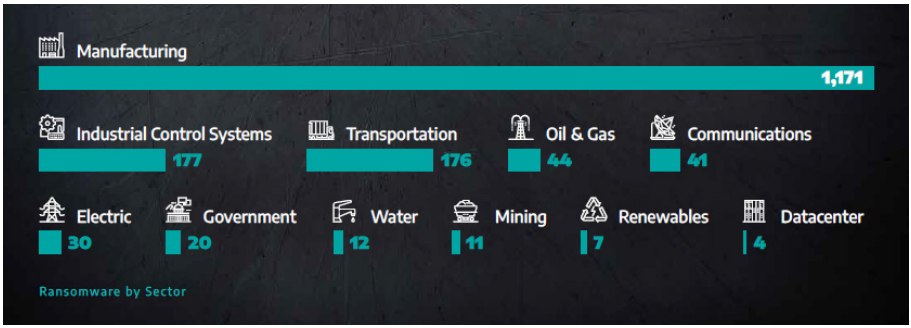
Volendo confrontare i dati del rapporto CLUSIT con altre fonti a livello internazionale, possiamo approfondire l'aspetto del Malware/Ransomware con alcune informazioni contenute nel Report Dragos ICS/OT CyberSecurity Year in Review 2025.

Il confronto con i dati del Dragos ICS/OT Cybersecurity Year in Review 2025 conferma l'escalation di ransomware diretti a impianti e sistemi industriali. Rispetto all'anno precedente, gli attacchi verso ambienti ICS/OT sono aumentati dell'87%, e il numero di gruppi criminali coinvolti è cresciuto del 60%.



A livello geografico, quasi il 60% degli attacchi ransomware si concentra in America, seguita dall'Europa (25%), di cui circa un 5–6% stimato per l'Italia, e dal restante 14% distribuito tra Medio Oriente, Asia e Oceania.

Si noti che subito dopo il manufatturiero generalista i target più frequenti sono gli sviluppatori (e utilizzatori) di software SCADA e, in crescita i data center industriali, segno di un progressivo spostamento verso la compromissione dei nodi infrastrutturali che abilitano la produzione intelligente.



Quasi tutti le problematiche di protezione più complesse sono rese possibili da una scarsa segmentazione delle reti, da una difesa perimetrale obsoleta e da carenze nei controlli di base sulla sicurezza. La citazione più significativa del report evidenzia la radice del problema: "*These findings strongly indicate that numerous ransomware groups are leveraging low-barrier-of-entry intrusion tactics against industrial organizations and capitalizing on a lack of basic network and security hygiene practices. Until these elements are properly addressed and secured, ransomware groups will continue exploiting them.*"

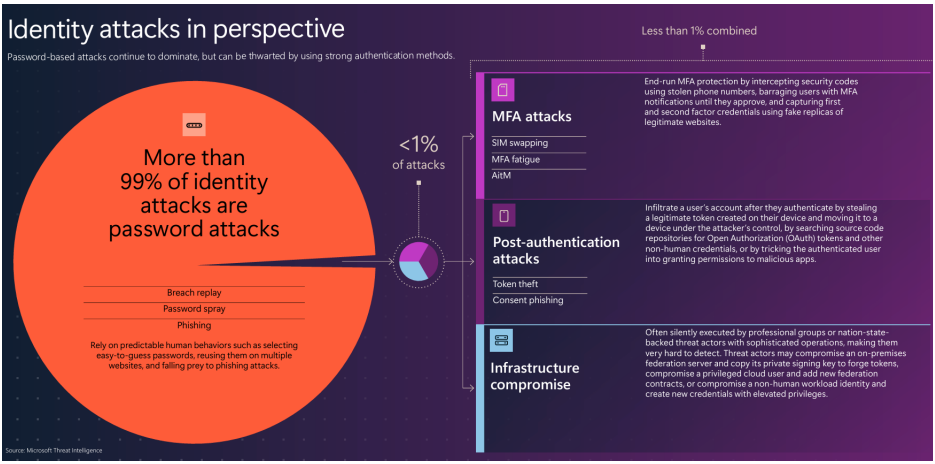
Alcuni dati dai Microsoft Digital Defense Report (2023/24/25)

Valutando il livello di esposizione a Vulnerabilità, censite come CVE (Common Vulnerability Exposure) riguardo a sistemi OT/IoT/IIoT, abbiamo alcuni dati che qui riportiamo:

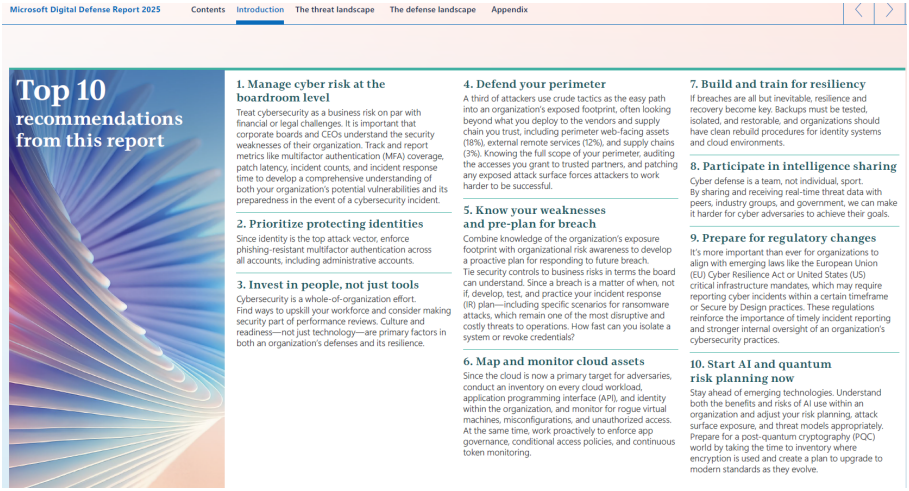
- del 78% dei device IoT con Vulnerabilità conosciute, abbiamo il 46%, quasi la metà, senza possibilità di patch (ovvero il 36% in assoluto);
- 25% dei dispositivi OT usa software non supportato (senza possibilità di patch);
- 96% delle applicazioni usa componenti software Open Source;
- registrato un +742% dal 2010 degli attacchi su software Open Source;
- 57% dei firmware device OT risulta esposto a più di 10 CVE conosciute.

Volendo approfondire alcuni dati riferiti a Device ICS/OT vulnerabili e non vulnerabili (PLC ecc.), possiamo notare che: del 78% IoT con Vulnerabilità conosciute, abbiamo visto che il 46%, quasi la metà, è senza possibilità di patch (ovvero il 36%) ed il 32% potrebbe ricevere patch (il 25%)
Inoltre, fortunatamente, secondo questo studio il 22% risulta non vulnerabile: 15% senza CVE conosciute e il 7% con patch applicate.

Nel rapporto 2024 invece si pone l'accento sul furto di password e l'autenticazione in generale, sempre più critiche in caso di attacchi mirati (e conseguentemente complessi e su commissione):



Nel report 2025 Microsoft sottolinea inoltre tre pilastri fondamentali per l'adeguamento alla Direttiva NIS2: la consapevolezza dei board aziendali, la protezione delle identità digitali (autenticazione multifattore ormai imprescindibile) e il ruolo centrale delle persone. In un contesto dominato dall'intelligenza artificiale, la supervisione umana rimane la prima linea di difesa.



Conclusioni

Il quadro complessivo del 2025, pur mostrando un leggero miglioramento rispetto al 2024, conferma che il settore manifatturiero resta un fronte critico per la sicurezza cibernetica. In Italia, la crescente attenzione delle istituzioni e l'estensione degli obblighi NIS2 rappresentano un'opportunità di maturazione: dalla semplice compliance alla costruzione di un modello di resilienza industriale.

Resta urgente agire su tre direttrici fondamentali: prevenzione del malware distribuito via email, segmentazione efficace delle reti interne e aggiornamento tempestivo dei sistemi. A ciò si aggiunge l'esigenza di una governance unificata tra IT e OT, capace di affrontare in modo sistemico l'espansione della superficie d'attacco dovuta all'Internet of Things e alle tecnologie di Industria 4.0.

Solo una visione integrata, che unisca competenze tecniche, formazione e responsabilità strategica, potrà ridurre il divario tra innovazione digitale e sicurezza industriale - e permettere al manufacturing di rimanere il motore tecnologico ed economico del Paese senza diventarne il punto più vulnerabile.

Conformità alla NIS2 e CyberSecurity OT

Le specifiche di Base nella determina ACN 164179 dell'Aprile 2025 e impatto sulla CyberSecurity OT

(A cura di Enzo Maria Tieghi e Mario Testino, ServiTecno)

A seguito del decreto legislativo 138, del 4 settembre 2024 di recepimento della direttiva NIS 2 (UE 2022/2555), il Direttore Generale dell'Agenzia di Cybersecurity Nazionale nell'Aprile del 2025 ha determinato le modalità e le specifiche di base per l'adempimento dei principali obblighi previsti dallo stesso decreto.

In seguito al decreto legislativo, ACN ha pubblicato alcuni documenti operativi che permettono di meglio comprendere e conseguentemente implementare quelle che sono le misure di sicurezza di base e necessità di notifica richieste dal decreto nonché il Framework di riferimento adottato (FNCDP -Framework Nazionale per la Cybersecurity e la Data Protection Edizione 2025 v2.1).

Si possono quindi identificare 10 ambiti di applicazione delle misure di sicurezza (vedi figura qui sotto), che si traducono complessivamente in 116 requisiti operativi (specificati nel Framework adottato), per i Soggetti Essenziali, e 87 per i Soggetti Importanti.

I dieci ambiti di applicazione delle misure di sicurezza

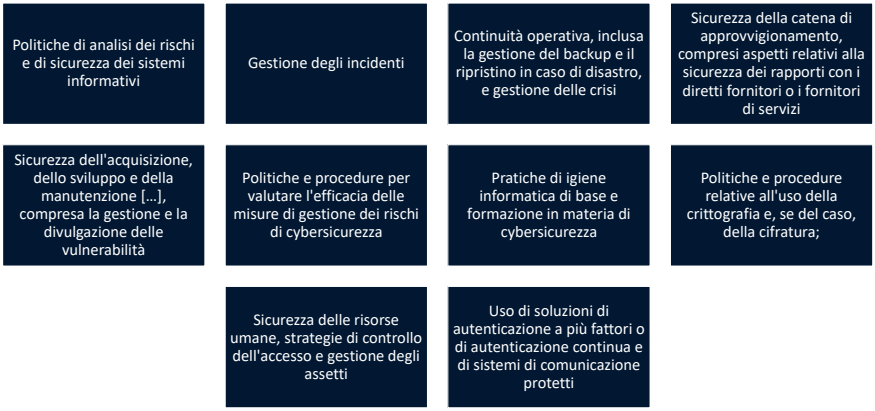


Immagine tratta da: *Gli obblighi di base in capo ai soggetti NIS*
Claudio Ciccotelli - Capo Divisione PSNC, Servizio Regolazione Agenzia per la Cybersicurezza Nazionale *(ACN)*

Con questo approccio, ACN si vuole concentrare, in questa prima fase, sugli aspetti organizzativi e procedurali per istituire all'interno dei soggetti nel perimetro NIS2 un sistema per la gestione della Cybersecurity, ovvero una struttura organizzativa di base (una vera e propria spina dorsale) su cui poi sviluppare ulteriori misure future in proporzione alle criticità delle Aziende ed Organizzazioni.

Oltre a questo, è necessario considerare anche l'altro onere previsto dal DL 138 e dalla Direttiva Europea, ovvero l'obbligo di notifica al CSIRT Nazionale degli "incidenti informatici rilevanti" per i soggetti NIS.
Un obbligo che potrà anche risultare molto gravoso per alcune tipologie di soggetti nella tassonomia dei settori di attività, soprattutto in relazione alle tempistiche di massima dell'informazione di notifica.

NIS2 e impatti sull'organizzazione

È evidente che in questa fase gran parte del lavoro deve essere realizzato dal reparto informatico delle organizzazioni che certamente rappresenta il lato più esposto alle attuali e nuove minacce esterne, nonché la prima area di compliance alla nuova direttiva.

Ciononostante, la nuova regolamentazione europea non intende limitare il campo di applicazione al mero trattamento dei dati o delle informazioni ma il vero obiettivo è quello di rendere il "sistema azienda" maggiormente resiliente in relazione alla continuità del business, nel senso che sia in grado di garantire o riprendere rapidamente la produzione di un bene o l'erogazione un servizio in caso di incidente informatico, ma non solo.

Peraltro, per rafforzare questo principio, la normativa propone un approccio di proporzionalità agli obblighi identificando i reparti produttivi come "attività o servizi" altamente critici, destinatari quindi del maggiore numero di requisiti di sicurezza.

Evidentemente, se analizziamo gli ambiti di applicazione della direttiva da questo punto di vista, lo scenario varia notevolmente e ci costringe ad analizzare gli aspetti organizzativi e tecnologici utilizzando una logica di insieme, permettendo di superare, forse per la prima volta, la oramai vetusta logica IT-OT, spesso visti e intesi come "domini separati", ma sempre più convergenti.

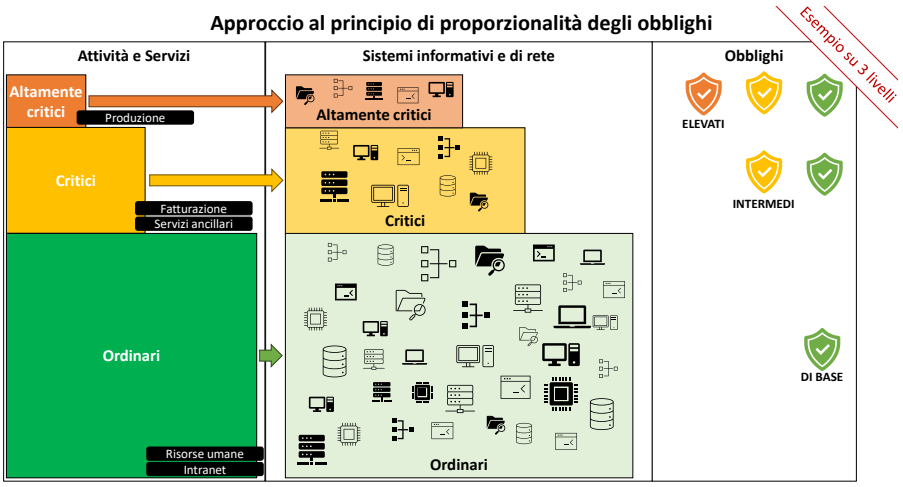


Immagine tratta da: *Gli obblighi di base in capo ai soggetti NIS*
Claudio Ciccotelli - Capo Divisione PSNC, Servizio Regolazione Agenzia per la Cybersicurezza Nazionale *(ACN)*

NIS2 e gestione del rischio "operativo"

Chi progetta con una logica di insieme, deve necessariamente considerare tutti gli aspetti di protezione dell'informazione e conseguentemente dei dati ma anche aspetti relativi al processo produttivo o di erogazione di un servizio essenziale, ovvero come si realizzano le cose con continuità, in sicurezza e qualità, garantendo la redditività.

A titolo di esempio vediamo quindi come affrontare l'ambito della Gestione del Rischio con la suddetta logica di insieme: il rischio informatico può essere considerato il rischio di perdita, furto, corruzione, manipolazione o inaccessibilità dei dati ma evidentemente anche l'impossibilità di effettuare la gestione, il controllo o la movimentazione adeguata di un dispositivo o di un macchinario (o dispositivo) che può impattare sulla produzione di un bene o erogazione di un servizio.

Dal punto di vista tecnologico bisogna quindi inserire nell'insieme dei sistemi informatici tutti i dispositivi industriali (o correlati) dotati di "intelligenza" ovvero con microprocessore (hardware) e di un programma (software) che permette elaborazioni di varia tipologia per la gestione ed il controllo di macchinari ed impianti (PLC, DCS, Sistemi IoT, RTU, ecc.). Tali dispositivi lavorano spesso "al di sotto del radar" dei reparti di Information Technology, appartenendo all'infrastruttura della Operational Technology.

NIS2, Security e Safety

A tutto questo dobbiamo poi aggiungere altri aspetti, per nulla da sottovalutare, ovvero la sicurezza (intesa come safety), la salute umana ed il benessere dei cittadini, che, anche se non rappresentano il target primario della direttiva (ne stanno arrivando altre maggiormente focalizzate, come ad esempio Il Regolamento Macchine, che entrerà a regime nel 2026), impongono un'analisi particolare perché possono portare blocchi alla produzione o interruzioni del servizio, oltre al fatto che sicurezza-safety e salute ed incolumità umana e salvaguardia dell'ambiente devono essere sempre al primo posto delle priorità organizzative.

L'impatto sull'ambiente e sulla salute, oltre agli impatti sulla gestione del rischio, deve anche essere affrontato sia in relazione alla movimentazione automatica di organi meccanici sia relativamente alle possibili contaminazioni di generi alimentari, farmaci o altri generi che possono avere implicazioni dannose sulla fisiologia umana e sull'ambiente.

NIS2 e sistemi di gestione della security

Tutto questo premesso, sembra quindi delinearsi che la definizione di un nuovo sistema di gestione della sicurezza informatica deve al pari essere accompagnata da un cambio di mentalità del management, verrebbe quasi da dire un cambio culturale, che possa riflettersi sull'organizzazione nel suo insieme.

I modelli aziendali, così come le professionalità, tradizionali hanno certamente bisogno di una revisione: IT, Ingegneria, Responsabili di Impianto, Gestori della Produzione o del Servizio, Automazione, Manutenzione, Produzione, ma anche le figure del CIO, CISO, CTO e CSO richiedono una revisione delle responsabilità e delle mansioni seguendo una logica di integrazione e di collaborazione.

Per capire meglio basta immaginare le figure attuali del CIO e CISO (relativamente responsabili informatici e della sicurezza IT delle organizzazioni), ovvero gli attori principali delle organizzazioni che approccio terrebbero nelle more dell'implementazione degli adempimenti normativa.

Con le responsabilità, le mansioni e gli skill attuali CIO e CISO limiterebbero la loro azione alla sola "rete office" o al più ai cluster informatici che gestiscono solo alcuni sistemi industriali "più visibili", rendendo sostanzialmente inefficaci i provvedimenti ai fini della direttiva.
CIO e CISO devono essere in grado invece di gestire le reti e i sistemi di tutto il perimetro aziendale, ovvero sia quelli appartenenti al "dominio IT" che quelli del

"dominio OT", potendo contare su competenze e skill individuali e su personale con esperienza e conoscenze adeguate anche per i sistemi produttivi che sono presenti nella rete amministrata nonché nel cuore operativo dell'azienda.

Le parole d'ordine sembrano quindi essere: formazione, organizzazione, integrazione, comunicazione e, non da ultimo tecnologia e digitalizzazione, con la funzione di driver per lo sviluppo.

Da NIS A NIS2: i nuovi verticals…

È cambiato l'elenco dei settori critici e ad alta criticità: come? Ecco alcune delle new entry:

- fabbricazione, produzione e distribuzione di sostanze chimiche e food & beverage;
- settore sanitario (laboratori, ricerca, produzione e distribuzione farmaci e dispositivi medici);
- fabbricazione di computer, macchinari e apparecchiature NCA;
- fabbricazione di autoveicoli;
- ecc.

L'Impatto della Direttiva NIS 2 sulla cybersecurity OT

Nel 2024 in Italia **il settore Manifatturiero** è stato il secondo settore più colpito dagli attacchi informatici: **secondo i dati di Clusit**, Il 15,7% degli attacchi totali che hanno colpito il nostro Paese, infatti, è stato a danno di aziende appartenenti a questo settore.

Fortunatamente la Direttiva (UE) 2022/2555 (NIS 2) rappresenta una svolta per la cyber-resilienza in Italia ed in Europa. Sostituendo la Direttiva NIS del 2016, la NIS2 risponde alla necessità di aumentare la resilienza della Società presa di mira dalla crescente sofisticazione delle minacce cyber e alla digitalizzazione sempre più pervasiva delle infrastrutture critiche. L'area più toccata da questa trasformazione è quella della Operational Technology (OT), l'insieme di sistemi e reti che monitorano e controllano i processi fisici nell'industria come nelle utility (ad esempio, SCADA, DCS, PLC, sensori intelligenti, microprocessori ed IoT), essenziali per settori vitali come energia, trasporti, sanità e manifatturiero. La NIS 2 non si limita a innalzare i requisiti di sicurezza per la tradizionale Information Technology (IT), ma estende in modo inequivocabile tali obblighi ai sistemi OT, imponendo una vera e propria evoluzione culturale e tecnica.

La convergenza IT-OT come fatto acquisito

La NIS 2 sancisce a livello normativo la realtà della convergenza IT-OT. Se fino a qualche tempo fa, le reti operative erano spesso segregate e isolate, oggi la spinta verso l'Industria 4.0, Transizione 5.0 e la necessità di analisi dei dati in tempo reale hanno portato a una sempre maggiore interconnessione. Questa convergenza espone a vulnerabilità di tipo IT anche l'OT, tradizionalmente progettata per l'affidabilità (ovvero l'alta disponibilità), la continuità operativa e spesso non per la cybersecurity,

La Direttiva NIS2, nel richiedere l'adozione di un approccio alla gestione del rischio a livello aziendale, costringe le organizzazioni a smantellare i silos operativi e a trattare la sicurezza delle reti e dei sistemi informativi (IT) e quella dei sistemi di controllo industriale (OT) come un unico dominio di rischio. Gli attacchi a sistemi OT, come quelli che hanno colpito fornitori di energia o acquedotti a livello globale, hanno dimostrato che l'impatto di un cyber-incident su queste reti si traduce in conseguenze fisiche dirette, con potenziali danni ambientali, pericoli per l'incolumità degli operatori ed utenti, interruzione dei servizi essenziali e minacce alla sicurezza pubblica.

I requisiti minimi obbligatori e il modello di rischio OT

L'**Articolo 21** della NIS 2 è il cuore pulsante degli obblighi per la sicurezza OT. A differenza della precedente NIS1, la NIS 2 è più prescrittiva e specifica dodici misure minime di gestione del rischio che devono essere implementate. Per l'OT, questi requisiti si traducono in azioni concrete e sfidanti.

1. Gestione del rischio e Asset Management

L'obbligo di condurre **analisi dei rischi** e implementare politiche di sicurezza dei sistemi informativi si estende esplicitamente ai sistemi di controllo industriale. Per l'OT, questo implica:

Inventario degli asset (Asset Management): è fondamentale mappare con precisione tutti i dispositivi connessi (PLC, RTU, sensori, sistemi HMI, SCADA, IoT, ecc.), identificando la loro funzione critica, il sistema operativo (spesso obsoleto) e le vulnerabilità note. Molte aziende non hanno una conoscenza completa e aggiornata della propria rete OT, e devono quindi attrezzarsi per poter ottemperare con tool specifici di asset inventory e personale e consulenti competenti.

Modellazione delle minacce (Threat Modeling): il rischio OT deve essere valutato non solo in termini di perdita di dati (come nell'IT) ma di impatto sulla sicurezza fisica (*safety*) e sulla disponibilità del processo. L'adozione di standard industriali come la serie **IEC 62443** (che fornisce un framework di sicurezza per i sistemi di automazione e controllo) diventa una prassi operativa essenziale per dimostrare l'adeguatezza delle misure.

Patch management e gestione delle versioni e configurazioni: nelle reti OT, l'applicazione di patch è spesso difficoltoso per motivi di garanzia, di stabilità del sistema o per la scarsità e l'assenza di finestre di fermo impianti per la manutenzione. La NIS 2 spinge le aziende a trovare soluzioni alternative, come l'implementazione di controlli compensativi. Pensiamo all'uso di diodi dati, ad una micro-segmentazione rigorosa, a sistemi per il versioning e per change-control.

2. Gestione degli incidenti e continuità operativa

Gli obblighi di segnalazione degli incidenti sono rigorosi e mettono sotto pressione i processi OT.

Tempestività nella segnalazione: la Direttiva impone un'**allerta rapida** entro **24 ore** dalla consapevolezza dell'incidente e una notifica completa entro **72 ore**. In un ambiente OT, dove il tempo di risposta a un'anomalia può essere questione di minuti per prevenire una interruzione del servizio, possibili danni agli impianti, alle persone, all'ambiente, questo richiede l'adozione di soluzioni di **Security Monitoring** (ad esempio, sistemi di rilevamento delle anomalie di rete OT) capaci di operare senza influire sulla performance del sistema e di alimentare rapidamente il team di risposta (CSIRT aziendale).

Business Continuity e Disaster Recovery: le aziende devono disporre di solidi piani di **continuità operativa** e di **ripristino dei disastri (DR)**. Per l'OT, ciò significa avere appositi tool che permettano che i backup delle configurazioni dei PLC e di dispositivi OT/IoT siano isolati, integri e testati regolarmente per un rapido ripristino delle operazioni fisiche dopo un attacco di ransomware o di malware distruttivo.

3. Sicurezza della catena di approvvigionamento (Supply Chain)

La NIS 2 pone un'attenzione critica sui rischi derivanti da terze parti e fornitori, una problematica particolarmente sentita nell'OT. Molti attacchi di successo passano attraverso i sistemi dei fornitori che hanno accesso remoto alle reti industriali per la manutenzione.

Controllo degli accessi remoti: la Direttiva richiede l'implementazione di politiche di **controllo degli accessi**, compreso l'uso obbligatorio dell'**autenticazione a più fattori (MFA)** o di soluzioni di autenticazione continua. Estendere segmentazione di rete ed autenticazione a tutti gli operatori e ai tecnici esterni che accedono all'ambiente OT è un passo fondamentale e spesso tecnologicamente complesso.

Audit/Due Diligence sui fornitori: le Organizzazioni/Aziende devono valutare le pratiche di sicurezza dei loro fornitori critici, assicurandosi che anch'essi siano conformi a standard di sicurezza equivalenti per l'accesso e la gestione dei sistemi.

Sfide operative, culturali ed economiche: uniformare sistemi disomogenei

L'implementazione e la compliance ai fini della NIS 2 nell'OT non consistono solo in un investimento ed uno sforzo iniziale, ma una trasformazione anche di cultura aziendale che comporta sfide multilivello, quali?

Gestire sistemi Legacy e Protocolli: i sistemi OT operano spesso con hardware e software legacy, installati tempo fa ed ancora oggi perfettamente funzionanti, con un ciclo di vita di molti anni (a volte anche 15-20 anni), spesso non progettati per le minacce cyber di oggi. Questi sistemi, inoltre, a volte utilizzano protocolli industriali proprietari, anche non basati su IP, che non sono gestibili dagli strumenti di sicurezza IT tradizionali.

Monitoraggio non intrusivo: le soluzioni di sicurezza in OT è meglio che siano passive e non intrusive per non compromettere la stabilità e la sicurezza fisica dei processi. Questo si implementa con l'adozione di tecnologie basate sull'Anomaly Detection e sull'analisi passiva del traffico di rete.

Segmentazione (e micro-segmentazione) e segregazione di asset critici: si può anche pensare all'implementazione del concetto di Zero Trust negli ambienti OT, basato sul principio del "minimo privilegio" (least privilege), ma questo richiede un profondo ridisegno dell'architettura delle reti industriali per garantire che solo le comunicazioni strettamente necessarie siano consentite, isolando i dispositivi critici. Ma questo spesso non è possibile, proprio per i vincoli di componenti legacy, difficilmente sostituibili in tempi brevi

Sfide culturali e organizzative: il gap IT-OT

Forse la sfida più grande è superare il gap culturale tra i team IT e OT. I team operativi (OT) danno priorità alla continuità e alla sicurezza-safety e spesso vedono le misure di sicurezza IT come una minaccia alla stabilità del processo. Come abbiamo visto, la NIS 2 impone una governance integrata e richiede il management e gli organi di gestione ricevano formazione in materia di cybersecurity, specificamente cybersecurity OT. Questo passaggio è cruciale per garantire che le decisioni di sicurezza siano comprese e sostenute a tutti i livelli, dai manager fino al personale di impianto.

Sfide economiche e sanzioni

L'adeguamento comporta investimenti consistenti in tecnologia, processi e personale specializzato. Tuttavia, la NIS 2 bilancia questi costi con la minaccia di sanzioni significative per la non conformità: fino a 10 milioni di euro o al 2% del fatturato annuo globale per le Entità Essenziali (e sanzioni minori per le Importanti). Queste sanzioni,

simili a quelle del GDPR, sono un forte incentivo per il Board ed il Management a trattare la compliance come una priorità strategica.

Conclusioni e next steps

Nonostante le sfide, la NIS 2 rappresenta una grande opportunità di migliorare radicalmente la propria continuità e resilienza operativa e acquisire un vantaggio competitivo. per le aziende industriali ed erogatori di servizi, che utilizzano estensivamente dispositivi OT.

In definitiva, la Direttiva NIS 2 costringe i settori vitali italiani ed europei a un salto di qualità nella "Maturità cyber", trasformando la sicurezza OT da un onere tecnico a un elemento strategico di sopravvivenza aziendale e di stabilità continentale. La Compliance alla NIS2 è solo il punto di partenza per un impegno continuo verso la "Resilienza Cyber" per garantire la Continuità Operativa ad Industrie di produzione di beni "critici" ed erogatori di servizi essenziali per la Società ed il benessere dei cittadini.

Riferimenti

Gli obblighi di base in capo ai soggetti NIS, Claudio Ciccotelli
https://www.acn.gov.it/portale/documents/20119/37358/Webinar+NCC+NIS2_Ciccotelli.pdf/710825ec-433e-9d22-1351-c3d8de674fd1?t=1743513514522

Intelligenza Artificiale (IA) agentica: quali evoluzioni ci attendono nella cybersecurity

(A cura di Federica Maria Rita Livelli)

Nell'era dell'intelligenza artificiale, la sopravvivenza delle organizzazioni non dipenderà più dalla semplice conformità normativa, ma dalla capacità di trasformarla in un sistema integrato: risk intelligence potenziata dall'AI, controlli agili e una vigilanza informatica capace di anticipare le minacce generate dalle macchine.

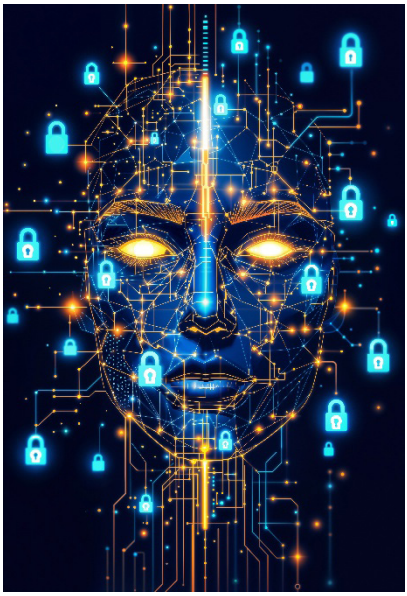


Immagine creata con l'AI

Introduzione

A differenza dell'intelligenza artificiale (IA) tradizionale, che in genere segue regole predefinite e flussi di lavoro statici, i sistemi agentici sono progettati per prendere decisioni autonome, operare senza supervisione e adattarsi dinamicamente nel tempo. Se da un lato questa flessibilità sblocca nuove potenti funzionalità, dall'altro

introduce superfici di attacco uniche e sfide in termini di cybersecurity che richiedono un'attenzione urgente.

Inoltre, l'evoluzione verso l'IA agentica, in ambito cybersecurity, richiede un approccio equilibrato. È doveroso evidenziare che organizzazioni devono considerare sia le opportunità sia i potenziali rischi, investendo in competenze specifiche e in framework di governance adeguati a mantenere il bilanciamento tra automazione e controllo umano, assicurando che l'IA agentica supporti le funzioni difensive senza introdurre nuove vulnerabilità.

Che cos'è l'AI agentica e come funziona

L'IA agentica (Agentic AI) costituisce una tipologia di sistemi basata su autonomia operativa, contestualizzazione avanzata e capacità decisionali sviluppate su più livelli.

I sistemi di IA agentica - a differenza dell'IA tradizionale - che si basa su regole predefinite o prompt manuali - possono: gestire in modo indipendente obiettivi a lungo termine; orchestrare dinamicamente strumenti e sub-agenti; prendere decisioni sensibili al contesto, utilizzando memoria persistente e telemetria in tempo reale. Inoltre, tali sistemi sono progettati per comprendere gli obiettivi aziendali, per scomporre le attività in componenti gestibili, oltre ad essere in grado di imparare dai risultati passati e di correggere continuamente la propria "rotta", senza la costante supervisione umana.

L''IA agentica, sembrerebbe destinata a migliorare il rilevamento delle minacce e la risposta automatizzata, garantendo una protezione più rapida ed efficace contro le minacce in continua evoluzione. Tuttavia, un recente studio dell'Università di Trento "dal titolo "Large language models are unreliable for cyber threat intelligence" mette in dubbio le capacità degli LLM in attività di Threat Intelligence Pertanto si consiglia di verificare le reali capacità raggiunte dall'IA agentica in modo da quantificare la loro coerenza e il loro livello di affidabilità, i.e.: "*Several recent works have argued that Large Language Models (LLMs) can be used to tame the data deluge in the cybersecurity field, by improving the automation of Cyber Threat Intelligence (CTI) tasks. This work presents an evaluation methodology that other than allowing to test LLMs on CTI tasks when using zero-shot learning, few-shot learning, and fine-tuning, also allows to quantify their consistency and their confidence level. [...] We show how LLMs cannot guarantee sufficient performance on real-size reports while also being inconsistent and overconfident. [...]*"

L'IA agentica si distingue per le seguenti principali caratteristiche:

- **Autonomia -** È in grado di eseguire le operazioni in più fasi, allineate agli obiettivi di sicurezza, senza alcun intervento umano.
- **Adattabilità -** Impara dai cicli di feedback e cambia tattica in base all'evoluzione della minaccia o dello stato del sistema.
- **Consapevolezza del contesto -** Integra il contesto tecnico e aziendale nelle decisioni in modo tempestivo.
- **Orchestrazione -** Si integra con strumenti di rilevamento, risposta e gestione: richiama API, esegue playbook, avvia azioni.
- **Memoria persistente -** Grazie a una memoria interna strutturata, l'IA agentica conserva dati, decisioni e stati delle operazioni nel tempo, permettendole di apprendere dai propri processi e di migliorare progressivamente le strategie applicate.

Di fatto, l'IA agentica opera secondo quattro fasi chiave, quali:

Percezione – Raccolta dati dal mondo che la circonda.
Motivazione – Elaborazione dei dati per capire cosa sta succedendo.
Azione – Decisione attuative, in base alla comprensione.
Apprendimento – Miglioramento e adattamento nel tempo, imparando dal feedback e dall'esperienza.

Fonte: immagine creata da FMRLivelli, utilizzando immagine AI – common criteria disponibile online

Differenze tra IA generativa, agenti IA e IA agentica

L'evoluzione dell'IA mostra una chiara progressione in termini di architettura e di autonomia, passando da semplici modelli a sistemi completamente autonomi capaci di gestire flussi di lavoro complessi. Di seguito sono riportate le principali caratteristiche e le differenze tra IA generativa, agenti IA e IA agentica.

- **IA generativa** - I sistemi di IA generativa, quali gli LLM (Large Language Models) generano testo o codice in risposta a richieste. Essi sono privi di memoria e l'output è interamente guidato dall'input, senza persistenza dell'obiettivo o della pianificazione delle attività.
- **Agenti IA –** Gli agenti IA sono sistemi orientati alle attività che usano strumenti come API o ricerca web per raggiungere obiettivi specifici. Essi sono autonomi ma operano in ambiti ristretti e dipendono dai prompt. Di solito funzionano su un singolo ciclo, senza memoria persistente né pianificazione dinamica.
- **IA agentica -** I sistemi di IA agentica sono progettati per operazioni autonome e articolate in più fasi. Essi scompongono gli obiettivi in sotto-attività, coordinano i sotto agenti, utilizzano strumenti esterni e interni e sfruttano la memoria a breve e lungo termine. Tali sistemi dimostrano capacità di pianificazione, adattabilità e iniziativa, consentendo l'esecuzione di attività a lungo termine, con un intervento umano minimo.

Si può affermare che l'IA agentica funziona come un analista junior autonomo, combinando ragionamento, memoria e azione per perseguire obiettivi, ma senza supervisione continua. Può usare un LLM come "cervello", mantenere lo stato delle interazioni passate e interagire in modo dinamico con l'ambiente o altri strumenti.

I rischi per la cybersecurity del processo agentico

È doveroso evidenziare che, a fronte di ogni progresso, corrispondono anche punti di cedimento e l'IA agentica non fa eccezione. Di fatto, consentire agli agenti software la libertà di prendere decisioni e di agire significa anche essere coscienti che essi possono anche sbagliare o essere "*manipolati*" dai cyber criminali. La comunità della sicurezza ha già iniziato a catalogare le minacce uniche che derivano dagli agenti autonomi. In particolare, l'Open Worldwide Application Security Project (OWASP) Foundation, ha pubblicato recentemente l'"*Agentic Threat and mitigation*" sulle minacce e sulle mitigazioni dell'IA agentica poste dagli agenti IA e, al contempo, per proporre strategie di mitigazione.

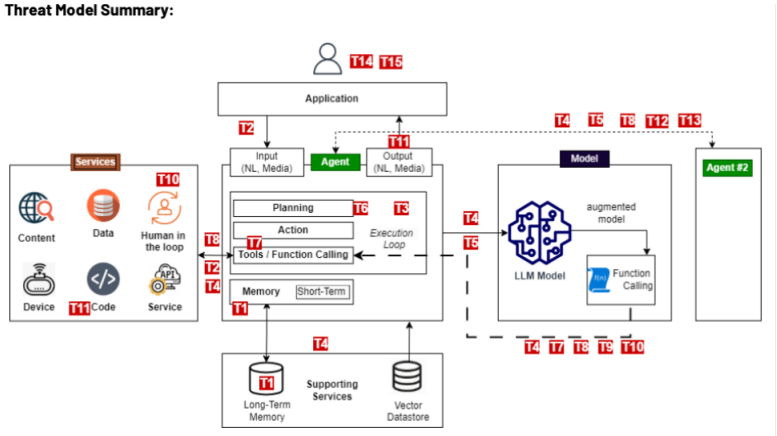
Dal report si evince che OWASP ha identificato una gamma completa di **15 potenziali minacce** di cui le organizzazioni dovrebbero essere a conoscenza, oltre a fornire azioni di mitigazione. Di seguito la traduzione dei contenuti principali della tabella riportata nel report di OSWAP.

ID	Tipologia Minaccia	Definizione della minaccia	Azione di mitigazione
T1	**Avvelenamento della memoria (Memory poisoning)**	Esso consiste nello sfruttare i sistemi di memoria di un'AI, sia a breve che a lungo termine, per introdurre dati falsi o malevoli e compromettere il contesto dell'agente. Ciò può portare a decisioni alterate ed esecuzioni non autorizzate.	Si consiglia di implementare: la validazione dei contenuti della memoria; l'isolamento delle sessioni; meccanismi di autenticazione robusti per l'accesso alla memoria; sistemi di rilevamento delle anomalie; routine regolari di sanitizzazione della memoria. Inoltre, in caso vengano rilevate anomalie, è necessario richiedere snapshot di memoria generati dall'IA per l'analisi forense e il ripristino.
T2	**Uso Improprio degli Strumenti (Tool misuse)**	L'uso improprio degli strumenti si verifica quando un attaccante manipola agenti AI inducendoli ad abusare degli strumenti integrati tramite prompt o comandi ingannevoli, operando comunque entro le autorizzazioni disponibili. Ciò include il fenomeno dell'Agent Hijacking, in cui un agente AI elabora dati manipolati da un avversario ed esegue azioni indesiderate, attivando potenzialmente interazioni malevole con strumenti.	Si consiglia di applicare verifiche rigorose di accesso agli strumenti, monitorare i pattern di utilizzo, validare le istruzioni fornite all'agente e definire confini operativi chiari per rilevare e prevenire abusi. Inoltre, si dovrebbero implementare i log di esecuzione che traccino le chiamate agli strumenti AI, utili per rilevamento di anomalie e per le analisi post-incidente
T3	**Compromissione dei privilegi (Privilege compromise)**	Si verifica quando un attaccante sfrutta debolezze nella gestione delle autorizzazioni per eseguire azioni non consentite, spesso, tramite ereditarietà dinamica dei ruoli o configurazioni errate. |	Si consiglia di implementare: controlli granulari su privilegi; validazioni dinamiche degli accessi; monitoraggio robusto dei cambi di ruolo; audit approfonditi delle operazioni con privilegi elevati. Inoltre, si consiglia di prevenire la delega dei privilegi tra agenti, salvo esplicita autorizzazione, tramite workflow predefiniti.

ID	Tipologia Minaccia	Definizione della minaccia	Azione di mitigazione
T4	**Sovraccarico della risorsa (Resource overload)**	Ciò impatta su: capacità computazionali, memoria e servizio dei sistemi AI, degradandone le prestazioni o causandone il malfunzionamento, sfruttandone la natura intensiva in termini di risorse.	Si consiglia di introdurre: controlli di gestione delle risorse; meccanismi di scaling adattivo; definizione di quote e monitoraggio in tempo reale del carico di sistema. Inoltre, si tratta di implementare policy di rate limiting per contenere le richieste ad alta frequenza per sessione di agente.
T5	**Attacchi dovuti ad allucinazioni a cascata (Cascading hallucination attacks)**	Questi fenomeni sfruttano la propensione delle IA a generare informazioni false che possono influire negativamente sulle decisioni e causare ragionamenti errati o rischiosi, oltre a richiamare involontariamente gli strumenti.	Si consiglia di: definire meccanismi robusti di validazione degli output; applicare vincoli comportamentali; utilizzare la validazione multi-sorgente, oltre a garantire correzioni continue attraverso il feedback loop. Si tratta altresì di richiedere la validazione secondaria delle conoscenze generate dall'IA prima che siano utilizzate in decisioni critiche.
T6	**Manipolazione di intenti ed obiettivi (Intent breaking & goal manipulation)**	Si tratta di una minaccia che sfrutta le vulnerabilità nei processi di pianificazione e di definizione degli obiettivi di un agente IA, consentendo agli attaccanti di manipolare o di reindirizzare le finalità dell'agente. Una tecnica comune è l'Agent Hijacking citato nell'uso improprio degli strumenti.	Si consiglia di implementare: un framework di validazione della pianificazione; gestione dei confini nei processi riflessivi; meccanismi di protezione dinamica per l'allineamento degli obiettivi. È opportuno, altresì, condurre audit comportamentali tramite modelli secondari che monitorino deviazioni significative negli obiettivi.
T7	**Comportamenti disallineati e ingannevoli (Misaligned & deceptive behaviors)**	Si tratta di agenti IA che eseguono azioni dannose o vietate, sfruttando risposte ingannevoli per raggiungere i propri obiettivi.	Si consiglia di: addestrare i modelli a riconoscere e a rifiutare compiti pericolosi; applicare restrizioni di policy; richiedere conferme "umane" per azioni ad alto rischio; implementare logging e monitoraggio. Inoltre, si consiglia di introdurre strategie di rilevamento dell'inganno, quali: analisi della coerenza comportamentale; modelli di verifica della veridicità; attività di red teaming avversario.

ID	Tipologia Minaccia	Definizione della minaccia	Azione di mitigazione
T8	**Ripudio & non tracciabilità (Repudiation & untraceability)**	Si verifica quando le azioni compiute da agenti IA non possono essere attribuite o ricostruite a causa di logging insufficiente o scarsa trasparenza nei processi decisionali.	Si consiglia, per garantire accountability e tracciabilità, di implementare: logging completo; verifiche crittografiche; metadati arricchiti; monitoraggio in tempo reale. Inoltre, è opportuno garantire che i log generati dall'IA siano firmati crittograficamente e immutabili per la conformità normativa.
T9	**Spoofing e impersonificazione dell'identità (Identity spoofing & impersonation)**	Gli attaccanti sfruttano le vulnerabilità nei meccanismi di autenticazione per impersonare agenti AI o utenti umani, eseguendo- sotto false identità - azioni non autorizzate.	Si consiglia, per rilevare tentativi di impersonificazione, di: sviluppare framework completi di validazione delle identità; imporre confini di fiducia; introdurre monitoraggio continuo. Utilizzare il profiling comportamentale, con il supporto di un modello secondario, per identificare deviazioni sospette nelle attività degli agenti IA.
T10	**Sovraccarico -Human in the loop (Overwhelming human in the loop)**	Si tratta di una minaccia che prende di mira i sistemi con supervisione umana e validazione decisionale, mirando a sfruttare i limiti cognitivi o a compromettere i framework di interazione.	Si consiglia di: sviluppare framework avanzati di interazione uomo-IA e meccanismi di fiducia adattivi; applicare modelli dinamici di governance IA che regolino i livelli di intervento umano e automazione in base a rischio, confidenza e contesto; introdurre collaborazioni gerarchiche IA-umano in cui decisioni a basso rischio vengano automatizzate e l'intervento umano sia riservato alle anomalie critiche.
T11	**RCE (Remote Code Execution) inatteso e attacchi al Codice (Unexpected RCE and code attacks)**	Gli attaccanti sfruttano ambienti di esecuzione generati dall'IA per: iniettare codice malevolo; provocare comportamenti imprevisti; eseguire script non autorizzati.	Si consiglia di: limitare i permessi di generazione codice da parte dell'IA; utilizzare sandbox di esecuzione; monitorare gli script generati; applicare policy di controllo che richiedano revisione manuale per codice AI con privilegi elevati.

ID	Tipologia Minaccia	Definizione della minaccia	Azione di mitigazione
T12	**Avvelenamento della comunicazione tra agenti (Agent communication poisoning)**	Gli attaccanti manipolano i canali di comunicazione tra agenti IA per: diffondere informazioni false; interrompere i flussi di lavoro; influenzare i processi decisionali.	Si consiglia, per individuare anomalie, di: applicare l'autenticazione crittografica dei messaggi; imporre policy di validazione delle comunicazioni; monitorare le interazioni tra agenti. Inoltre, è necessario introdurre il consenso multi-agente per decisioni mission-critical.
T13	**Agenti non autorizzati in sistemi multi-agente (Rogue agents in multi-agent systems)**	Si tratta di Agenti IA malevoli o compromessi che operano al di fuori dei normali confini di monitoraggio, eseguendo azioni non autorizzate o esfiltrando dati.	Si consiglia di limitare l'autonomia degli agenti IA tramite vincoli di policy e monitoraggio comportamentale continuo. Sebbene i meccanismi di attestazione crittografica per LLM non esistano ancora, l'integrità degli agenti può essere garantita tramite: ambienti di hosting controllati; attività regolari di red teaming; monitoraggio input/output per rilevare deviazioni.
T14	**Attacchi umani ai sistemi multi-agente (Human attacks on multi-agent systems)**	Si tratta di avversari che sfruttano la delega tra agenti, le relazioni di fiducia e le dipendenze nei workflow per ottenere l'escalation di privilegi o per manipolare le operazioni guidate dall'IA.	Si consiglia, per rilevare tentativi di manipolazione, di: limitare i meccanismi di delega tra agenti; imporre autenticazione inter-agente; implementare monitoraggio comportamentale. Inoltre, è opportuno applicare la segmentazione dei compiti multi-agente per impedire agli attaccanti di ottenere escalation di privilegi attraverso agenti interconnessi.
T15	**Manipolazione umana (Human manipulation)**	Nei contesti in cui agenti IA interagiscono direttamente con utenti umani, la relazione di fiducia riduce lo scetticismo dell'utente e aumenta la dipendenza dalle risposte e dall'autonomia dell'agente. Tale rapporto fiduciario e l'interazione diretta uomo/agente generano rischi: gli attaccanti possono indurre gli agenti a manipolare gli utenti, diffondere disinformazione o eseguire azioni occulte.	Si consiglia di: monitorare il comportamento dell'agente per verificarne la coerenza con il ruolo definito e le azioni attese; limitare l'accesso agli strumenti per ridurre la superficie d'attacco; restringere la capacità dell'agente di generare link; implementare meccanismi di validazione per rilevare e filtrare risposte manipolate, utilizzando guardrail, API di moderazione o un modello secondario.



Un riepilogo del modello di minaccia agentica OWASP, che mappa le minacce contro l'intelligenza artificiale agentica. **Fonte:** OWASP

Il ruolo dell'IA agentica nella cybersecurity: vantaggi, rischi, sfide e implicazioni normative ed etiche

L'IA agentica rappresenta un paradigma rivoluzionario nella cybersecurity, caratterizzato dalla capacità di sistemi autonomi di prendere decisioni indipendenti, apprendere dall'esperienza e adattarsi dinamicamente alle minacce emergenti. I vantaggi sono significativi, considerando che questi sistemi possono:

- operare 24/7 senza affaticamento umano;
- analizzare volumi massivi di dati in tempo reale per identificare pattern anomali;
- rispondere istantaneamente agli attacchi con velocità superiore a qualsiasi team di sicurezza umano.

È doveroso evidenziare che l'IA agentica eccelle ne:

- l'automazione della threat hunting;
- la correlazione di eventi complessi attraverso multiple superfici d'attacco;
- la previsione proattiva di vulnerabilità basata sull'IA.

Tuttavia, i rischi sono altrettanto considerevoli in termini di:

- possibilità di falsi positivi su larga scala che paralizzano le operations;
- adversarial learning dove gli attaccanti manipolano i modelli AI;
- creazione di nuove superfici d'attacco attraverso la compromissione degli stessi sistemi AI.

Inoltre, le sfide tecniche includono la necessità di: explainability per decisioni critiche; integrazione con legacy systems; gestione della complessità emergente di sistemi autonomi che interagiscono tra loro.

Ancora, sul piano normativo ed etico, l'IA agentica in cybersecurity solleva dubbi su responsabilità e accountability, soprattutto in caso di errori che compromettono sicurezza o privacy.
L'AI Act europeo classifica molte applicazioni di cybersecurity come "high-risk", imponendo severi requisiti di governance e audit. È inoltre essenziale garantire trasparenza algoritmica e la tutela dei diritti fondamentali, evitando bias e la sorveglianza eccessiva nei sistemi che monitorano comportamenti umani.

Inoltre, la presenza umana nelle decisioni diventa fondamentale quando sono in gioco diritti o attività critiche. Pertanto, sono necessari standard internazionali per certificare l'IA in ambito cybersecurity, protocolli di risposta agli incident specifici per failure dell'IA, oltre a framework che chiariscano i livelli di autonomia nei vari contesti operativi.

Lo stato attuale dell'IA agentica nella cybersecurity: casi d'uso e implementazioni

L'adozione dell'AI agentica in cybersecurity si trova attualmente in una fase di transizione dalla sperimentazione pilota all'implementazione enterprise, con una maturità tecnologica eterogenea in diversi casi d'uso.
In termini di threat detection & response, soluzioni come Darktrace e CrowdStrike utilizzano IA agents per l'autonomous threat hunting, capaci di identificare e contenere minacce senza intervento umano in scenari a basso rischio.

Microsoft Copilot for Security rappresenta un esempio di IA agentica applicata al Security Operations Center (SOC), automatizzando l'analisi di alert, la correlazione di eventi e la generazione di suggerimenti per la correzione.
Per quanto riguarda la gestione delle vulnerabilità, piattaforme come Tenable e Qualys integrano agents IA che, non solo scansionano e identificano vulnerabilità, ma prioritizzano automaticamente le patch basandosi su threat intelligence in tempo reale e sul business context.

Inoltre, in termini di IAM (Identity & Access Management) l'IA agentica è impiegata in soluzioni come Okta e CyberArk, dove algoritmi autonomi gestiscono provisioning/deprovisioning, rivelano anomalie comportamentali e adattano dinamicamente le policies di accesso.

Conclusione

Ci troviamo di fronte a una nuova classe di avversari e a una nuova classe di alleati allo stesso tempo. Da un lato, gli aggressori utilizzeranno, senza dubbio, l'IA agentica per creare bot più intelligenti e malware in grado di adattarsi ed eludere le difese. D'altra parte, grazie all'IA agentica, le organizzazioni potranno disporre di nuove capacità difensive. Stiamo, di fatto, giocando una nuova partita a scacchi in cui sono stati aggiunti nuovi pezzi per entrambe le parti.

Pertanto, per sfruttare *in toto* l'IA agentica, dobbiamo conoscerne i rischi e preparaci ad affrontarli consapevolmente. Ovvero, la chiave sarà bilanciare l'innovazione con la governance, senza dimenticare che l'IA agentica continuerà a fare affidamento su di noi per porre le domande giuste, impostare le giuste barriere e creare fiducia. Solo bilanciando progresso tecnologico e resilienza sarà possibile valorizzare appieno il potenziale dell'intelligenza artificiale agentica, garantendo al tempo stesso la sicurezza dei sistemi digitali del futuro.

Inoltre, il vero valore dell'IA agentica non sta nel sostituire le persone, ma nel permettere loro di potenziare le proprie competenze ed eccellere. Le organizzazioni dovrebbero puntare sull'amplificazione del talento umano, non sulla sua eliminazione, assicurandosi che i sistemi di IA mantengano sempre l'uomo al centro, offrano piena verificabilità e si integrino in modo naturale con i flussi di lavoro esistenti.

L'IA agentica, se adottata in questa direzione, consente ai team di sicurezza di muoversi più rapidamente, rafforzare le proprie capacità e respingere le minacce in modo proattivo, anziché limitarsi a intervenire dopo un attacco, garantendo, così, la cyber resilience dei nostri ecosistemi. È un futuro non solo possibile, ma quello a cui dovremmo ambire.

Bibliografia

- TrendMicro (articolo) - The road to agentic AI: defining a new paradigm for technology and cybersecurity
- TechTarget (articolo) - TechTarget - Definition/agentic-AI
- Medium magazine (articolo) - Medium - Ai Agents vs agentic AI: what is e difference and why does it matter?
- Human Security Blog (articolo) - Human Security blog - On Agentic AI and Evolution in Cybersecurity;
- Human Security Blog (articolo) - Navigating Agentic AI Security: Understanding OWASP Threats and Enabling Authentic & Trusted Interactions
- Risk Management Magazine (Articolo) - Risk Management Magazine - Securely-deploying-agentic-ai
- Studio Università di Trento - Large language models are unreliable for cyber threat intelligence a firma dei proff. Emanuele Mezzi, Fabio Massacci, Katja Tuma

L'uso dei sistemi di AI generativa gratuiti nella gestione del ciclo di vita dei requisiti normativi

(A cura di Giancarlo Butti)

Negli ultimi anni sono state emanate numerose normative, in particolare in ambito UE, che impattano in modo significativo sul livello di sicurezza delle organizzazioni e, più in generale, sul loro sistema informativo (GDPR, NIS2, DORA, Data ACT, Data governance ACT, AI ACT…).

Spesso tali normative impongono requisiti tecnici ed organizzativi che sono fra loro sovrapponibili e non è facile, da un lato avere un quadro costante ed aggiornato dei vincoli normativi ai quali una organizzazione deve adeguarsi e dall'altro, implementare concretamente tali requisiti e gestirli nel tempo.

La disponibilità di soluzioni di AI facilmente accessibili e spesso gratuite, può agevolare notevolmente questo processo in ogni sua fase.

In questo articolo verranno presentati sia i possibili usi di tali strumenti nel contesto sopra citato, sia i relativi limiti.[1]

La disponibilità di soluzioni di AI generativa, disponibili on line anche in versione gratuita, è in continua crescita.
Ogni giorno compaiono nuovi strumenti e quelli esistenti fanno a gara per migliorare il proprio modello e per aggiungere nuove funzionalità che, nel giro di poco tempo, sono adottate anche dagli altri strumenti.
Questo fa sì che, al di là di alcune particolarità, questi strumenti si somigliano l'un l'altro, rendendo molto facile per l'utente apprendere l'uso delle loro funzionalità di base-

Questo è un bene, ma costituisce anche un difetto, in quanto si corre il rischio di utilizzarli tutti nello stesso modo, senza sfruttare adeguatamente le funzioni e le particolarità tipiche di ognuno di essi.

---

[1] Il presente articolo costituisce una rappresentazione estremamente sintetica delle seguenti pubblicazioni:
G.Butti – IA e audit, ITER 2024 https://iterdigital.it/it_it/ia-e-audit/
G.Butti – Compliance 4.0, ITER 2025 https://iterdigital.it/it_it/compliance-4-0/
G.Butti - Supply chain: gestire i rischi con strumenti di IA gratuita, ITER 2025 https://iterdigital.it/it_it/gestione-rischi-supply-chain/

In linea di massima, strumenti come ChatGPT, Gemini, Claude, tanto per citarne qualcuno, offrono all'utente una interfaccia che presenta come funzionalità principale una chat, con la quale l'utente interagisce con il sistema ponendo le proprie domande (in gergo prompt).
Gli strumenti consentono in genere di allegare file da analizzare, di effettuare ricerche on line, di esportare i risultati della interrogazione in vari formati, di interagire mediante voce (sia durante l'interrogazione, sia durante la loro risposta), di salvare le interrogazioni effettuate…

Inoltre tali strumenti sono in grado di generare immagini e altri contributi multimediali, slide, codice eseguibile in vari linguaggi di programmazione, disegni progettuali…, ma il presente articolo è incentrato unicamente sulla generazione di elaborati sotto forma di testo.
Alcuni strumenti hanno un approccio peculiare, come NoteBook LM, che privilegia l'analisi dei documenti forniti dall'utente rispetto ad una ricerca on line (che può comunque avvenire su richiesta).
Perplexity per contro è un motore di ricerca avanzato, in grado di analizzare decine di fonti diverse on line e di elaborare una risposta originale basata sulle fonti analizzate. È comunque possibile, anche in questo caso, allegare documenti come fonte dati.

Tabella 1 - Esempi di strumenti di AI per i quali è disponibile una versione gratuita

Perplexity	https://www.perplexity.ai/
NoteBook LM	https://notebooklm.google/
Genspark	https://www.genspark.ai/
ChatGPT	https://chatgpt.com/
Mistral	https://mistral.ai/
DeepSeek	https://www.deepseek.com/
Vitruvian 1	https://vitruvian.asc27.com/
Claude	https://claude.ai/
Gemini	https://gemini.google.com/
Copilot	https://copilot.microsoft.com/
X	https://x.ai/
Kuse	https://www.kuse.ai
Grok	https://grok.com/

Quindi, alla fine, più o meno hanno tutti le stesse funzionalità, anche se con prestazioni e capacità molto diverse, ed è quindi importante conoscere potenzialità e limiti dei vari strumenti per sapere quale utilizzare nella specifica situazione o, come consiglio sempre, di utilizzarne più di uno contemporaneamente.

Il fatto che tali strumenti dispongono di una versione gratuita che consente di svolgere già una attività consistente, aiuta questo tipo di approccio.

A cosa possono servire in ambito professionale

Ho dedicato i miei ultimi 3 libri specificatamente a questo argomento.
Il primo testo è stato dedicato all'uso degli strumenti di AI generativa nelle attività di audit, il secondo alla analisi delle normative ed alla loro implementazione, il terzo alla gestione dei rischi della supply chain.

Nelle tabelle 2, 3, 4, riporto una sintesi delle possibili applicazioni che ho individuato in questi 3 ambiti, e che ho sviluppato nei miei libri.
Accanto a questi usi "specialistici", si affiancano quelli di carattere generale, che vanno dalla traduzione di testi al riassunto degli stessi o all'ausilio all'impaginazione o alla ottimizzazione del contenuto di un documento…

Io stesso, a volte, per scrivere un articolo mi limito a dettare al pc qualche appunto, chiedendo poi ad uno di questi strumenti di trasformare un testo sgrammaticato ed approssimativo in un testo corretto e chiaro.
In questo modo, ho ridotto drasticamente i tempi di lavorazione, in particolare di alcuni articoli dove i concetti esposti sono molto complessi e l'attenzione riguarda maggiormente la loro rappresentazione logica rispetto alla forma.
Gli ambiti d'uso condizionano anche gli strumenti utilizzati; se il libro sull'audit è basato prevalentemente su ChatGPT, quello sulla analisi e implementazione delle normative utilizza principalmente NoteBook LM.

Solo la fantasia può limitare l'uso di tali sistemi e il grosso vantaggio di questi strumenti, che è assolutamente innovativo rispetto a qualunque applicazione disponibile in precedenza, è che non è necessario un manuale o studiare per imparare a utilizzarli, in quanto è possibile chiedere allo strumento stesso quali siano le sue funzionalità, come fare per utilizzarlo al meglio, quale aiuto ci possono dare in uno specifico ambito…

Tabella 2 - Uso degli strumenti di AI generativa nelle attività di audit

Fase di preparazione dell'audit	• Descrivi come deve svolgersi una attività di audit interno nell'ambito della business continuity • Come può essere eseguito un audit sulla continuità operativa • Descrivi un processo ideale per la gestione della business continuity • Quali sono le fonti che hai utilizzato per descrivere il processo • Come eseguire al meglio una business impact analysis • Quali sono i controlli che devo effettuare su una BIA per verificare se è conforme ai requisiti previsti dalla normativa di Banca d'Italia • Quali sono i controlli che devo mettere in atto per verificare se un piano di continuità operativa sia conforme alle normative EBA e quali sono le normative EBA da prendere in considerazione • Crea una checklist per svolgere una verifica in ambito business continuity • Puoi ampliare la checklist ad almeno 100 quesiti • Crea una checklist di almeno 100 quesiti per un audit sulla business continuity dove nella prima colonna metti il numero della domanda, nella seconda la domanda, oltre ad altre 5 colonne vuote • Per ogni domanda della checklist precedente predispone 5 risposte che indicano diversi livelli di maturità e compila le colonne della tabella che prima erano vuote • Genera il codice CSV della precedente tabella • Crea una checklist per un audit report sulla business continuity basato sulla ISO 22301 per un'azienda manifatturiera di medie dimensioni.
Fase di esecuzione di un audit	• Dopo aver individuato i ruoli che in un'azienda sono coinvolti nel processo di gestione della business continuity, genera una serie di domane finalizzate ad intervistare ognuno di loro • Puoi fare la stessa cosa considerando figure più operative rispetto a quelle elencate in precedenza • Comportati come un auditor e fammi delle domande considerando che sono il business continuity manager • Puoi dare un peso alle varie domande e giustificare la tua scelta • Come deve essere effettuata una verifica sulla conformità di una informativa privacy • Verifica se la seguente informativa privacy è conforme
Fase di reportistica	• Imposta lo schema di un audit report • Genera lo schema di un audit report relativo alla business continuity

Nei miei libri ho dedicato uno specifico capitolo ad una sommaria descrizione dei principali strumenti di AI generativa.
L'ho fatto con l'avvertenza che fra il tempo di analisi dei vari strumenti ed il tempo della stampa dei libri, gli strumenti sarebbero evoluti così rapidamente da rendere approssimativa la loro descrizione e che, con molta probabilità, la descrizione del singolo strumento sarebbe stata superata nel momento in cui un lettore avesse letto il testo.
Per questo motivo il testo del capitolo è stato scritto direttamente dagli stessi strumenti.

Ogni strumento ha descritto sé stesso o meglio, ha riportato le informazioni che ha trovato in merito alla sua descrizione. In questo modo il lettore, invece che leggere un testo obsoleto, può riformulare lo stesso quesito da me posto agli strumenti, per ottenere da ognuno di essi una auto presentazione aggiornata.

Un approccio particolare dunque, che rende un contenuto che potrebbe diventare subito obsoleto, continuamente aggiornato dal lettore stesso.

Tabella 3 - Uso degli strumenti di AI generativa nelle attività di adeguamento ad una normativa

Normative esistenti	• Verifica delle normative applicabili in un determinato ambito • Verifica delle sanzioni in caso di violazione di una normativa • Scadenze normative
Confronto fra normative	• Requisiti sovrapponibili fra 2 o più normative • Gap fra normative
Sintesi di documenti normativi	• Sintesi complessiva • Sintesi del singolo articolo • Lemmi
Requisiti previsti da una normativa	• Requisiti tecnici • Requisiti organizzativi • Requisiti di sicurezza • Requisiti legali • Requisiti contrattuali • Ruoli coinvolti
Contratti	• Creazione dei documenti contrattuali • Definizione degli allegati ad un contratto • Definizione di SLA

Policy e procedure	• Creazione di policy • Creazione di procedure • Creazione di modulistica • Verifica della conformità di policies - procedure rispetto ad una normativa
Creazione di applicazioni software di supporto	• crea una applicazione interattiva che consenta ad un titolare di trattamento di decidere se un potenziale fornitore debba essere designato quale responsabile del trattamento dei dati • crea una applicazione che operi in locale in html per porre tutte le domande per raccogliere le informazioni necessarie per creare una informativa privacy. dopo aver raccolto le informazioni l'applicazione deve scrivere una corretta informativa privacy.

Tabella 4 - Uso degli strumenti di AI generativa nelle attività di gestione del rischio della supply chain

Gestione dei rischi di fornitura
Comparazione fornitori
Due diligence
Monitoraggio della catena di fornitura
Chiusura del rapporto di fornitura
Exit plan

In effetti questi miei libri sono una raccolta di prompt e delle relative risposte, risposte che cambiano nel tempo.
Una applicazione di AI generativa non risponde infatti mai nello stesso modo, anche se si lancia lo stesso prompt a distanzia di pochi minuti, e questo è un altro modo per ottenere più informazioni in merito allo stesso quesito.
Saper scrivere un prompt, sapere interrogare questi strumenti, è diventata una nuova arte o meglio, una nuova professione per la quale esistono figure specializzate.
In realtà, anche in questo caso, sono gli strumenti stessi che possono rendere questi professionisti in gran parte superflui.

La creazione dei prompt

Come per la propria auto descrizione, è possibile chiedere agli strumenti stessi come realizzare un prompt efficace, ovvero procedere alla creazione del prompt ideale per la propria interrogazione.

In altre parole è lo strumento stesso che può creare il prompt più efficace per raggiungere il miglior risultato possibile.

Al riguardo è sufficiente che l'utente inserisca un proprio prompt base nel quale riporti le informazioni che desidera ottenere.

Tabella 5 - I contenuti di un prompt ideale secondo ChatGPT

Componente	Indicazione
Oggetto	Specifico e delimitato
Contesto	Obiettivo d'uso, target, ruolo del richiedente
Approfondimento	Superficiale / tecnico / comparato / operativo
Stile	Formale, divulgativo, accademico
Struttura	Richiesta di sezioni definite
Fonti	Normative, tecniche, linee guida
Formattazione	Tabelle, elenchi, paragrafi brevi
Materiale di partenza	Se disponibile, includerlo

Non mancano anche gli strumenti specificatamente dedicati a questo compito, come quello reso disponibile da Antrophic (produttore di Claude) all'indirizzo https://console.anthropic.com.
Questo generatore di prompt non si limita ad ottimizzare un prompt grezzo, ma ne sviluppa il contenuto contestualmente alla richiesta stessa.

Se il vostro prompt di base è realizzato per richiedere la creazione di una procedura per la gestione degli asset ICT, il generatore di prompt di Anthropic ne crea uno che contiene già la struttura della procedura.
Considerando che la qualità delle risposte fornite dagli strumenti sono condizionate dalla qualità dei prompt, disporre di uno strumento di questo tipo aumenta considerevolmente la qualità dei risultati.

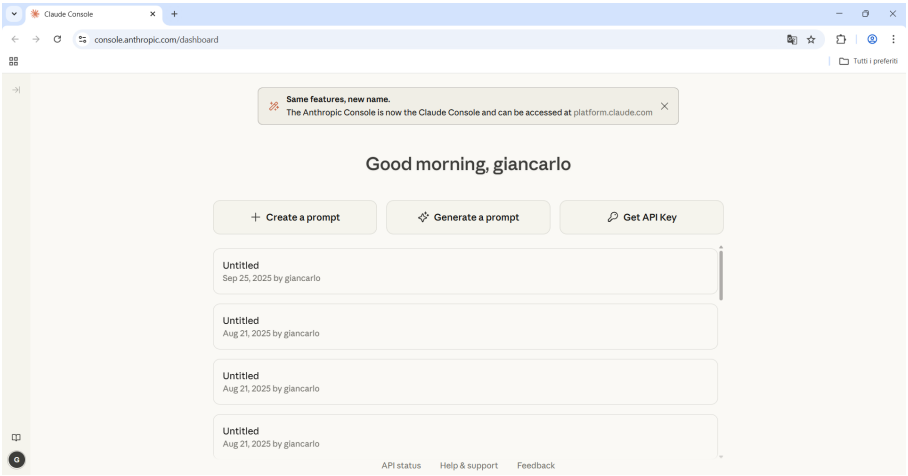


Fig. 1 - Claude Console

I limiti nell'uso degli strumenti

Sebbene l'uso di questi strumenti comporti notevoli vantaggi, non mancano gli aspetti negativi che è necessario considerare e che si possono riassumere principalmente nei seguenti punti:

- problemi legati alla riservatezza delle informazioni fornite agli strumenti
- errori nelle risposte
- qualità delle fonti utilizzate dagli strumenti per formulare le risposte
- limiti d'uso delle versioni gratuite.

Per quanto attiene la riservatezza, il rischio legato all'uso di questi strumenti (indipendentemente dall'uso di una versione gratuita o di un abbonamento) riguarda la possibilità che le informazioni fornite, ad esempio in un prompt o allegando un documento, siano utilizzate per addestrare il modello stesso e quindi perdano le loro caratteristiche di riservatezza.

In realtà diversi strumenti consentono, in teoria, di impostarne l'uso affinché questa eventualità sia espressamente esclusa, ma anche in questo caso sta alla fiducia dell'utente fidarsi o meno nelle dichiarazioni del produttore.

Alternativamente, se si desira una garanzia assoluta di riservatezza, è possibile installare dei modelli di IA in locale, sul proprio pc. Ne esistono molteplici, adatti a diverse potenze di calcolo e dimensione della memoria. Tutti questi modelli sono rigorosa-

mente gratuiti e adatti ad usi di carattere generale o come base da addestrare con le proprie basi di conoscenza.

Inoltre, molti degli strumenti qui citati dispongono di versioni dedicate alle aziende, che prevedono la predisposizione di ambienti personalizzati per la singola azienda cliente, garantendo così la riservatezza delle informazioni utilizzate.

Errori nelle risposte

Questi sistemi sono addestrati per fornire una risposta in ogni caso, anche se non hanno reali informazioni con le quali poterle elaborare e, pertanto, a volte forniscono risposte prive di fondamento.

Le così dette allucinazioni non sono però l'unico motivo per cui le risposte fornite da un sistema di AI devono essere verificate prima di prenderle in considerazione.

Fig. 2 - Gemini segnala ogni volta che il risultato di una interrogazione può contenere degli errori

Anche quando hanno a disposizione le informazioni necessarie per formulare una risposta, la qualità di quest'ultima è legata alla qualità delle fonti dati.

Queste ultime sono raggruppabili, semplificando, in 3 diverse aree:

- informazioni già disponibili nel modello
- documenti allegati allo strumento
- fonti reperite dallo strumento on line.

In linea di massima tutti gli strumenti sono in grado di utilizzare contemporaneamente queste 3 fonti di informazione e, ovviamente, le fonti più critiche sono quelle disponibili on line.

La qualità delle informazioni reperite on line non è infatti garantita; spesso tali informazioni sono incomplete se non del tutto errate o fuorvianti, motivo per cui la qualità delle risposte fornite da strumenti che si basano soprattutto su tali fonti, deve essere attentamente valutata.

Viceversa, strumenti con NoteBook LM, che si basano essenzialmente su fonti dati fornite direttamente dall'utente, forniscono risposte la cui qualità può essere considerata intrinsecamente molto elevata, in quanto si presume che i documenti forniti per la valutazione, siano stati selezionati in modo tale da essere attendibili.

Perplexity, che basa le proprie risposte per lo più su documenti on line, permette comunque di selezionare, fra le fonti dati, generiche pagine web ovvero articoli accademici e quindi, si ritiene, più attendibili.

Solitamente gli strumenti enumerano quelle che sono le fonti dati on line che hanno utilizzato e tale indicazione può essere generica (semplicemente elencandoli), puntuale (indicando quale parte della risposta è stata generata facendo riferimento ad una specifica fonte) o estremamente puntuale, come nel caso di NoteBook LM, che indica precisamente quale parte del testo di un determinato documento ha prodotto una singola parte della risposta.

Va da sé che è possibile chiedere allo strumento stesso su quali fonti si è basato per produrre una certa risposta, in particolare se si è chiesto allo strumento di non effettuare ricerche on line, opzione questa disponibile in alcuni degli strumenti citati.

Una delle particolarità di tali strumenti consiste infatti nel superare il limite di quelle che sono le funzionalità base di cui dispongono, in quanto è l'utente stesso che, con un adeguato prompt, può chiedere di integrarle.

La possibilità che le risposte fornite da questi strumenti siano errate può essere mitigata quindi, adottando fonti attendibili, ma soprattutto utilizzandoli solo per effettuare interrogazioni su materie di cui si è già esperti, al fine di poter valutare criticamente quanto hanno generato.

È anche possibile porre la stessa domanda a strumenti diversi e confrontare le relative risposte per verificare la loro corrispondenza.

Il confronto può essere effettuato con l'uso degli stessi strumenti, e non necessariamente manualmente.

Risposte simili, fornite da strumenti diversi, possono aumentare il livello di confidenza sulla correttezza della risposta che tuttavia non è certa. Infatti, se le fonti sono le medesime (in particolare fonti on line) e queste contengono informazioni errate, si avranno delle risposte fornite dai vari sistemi errate, ma fra loro coerenti.

Limiti d'uso delle versioni gratuite

Le versioni gratuite dei vari strumenti hanno ovviamente delle limitazioni.

I produttori hanno tutto l'interesse di permetterne di saggiarne le funzionalità, limitandole, al fine di indurre gli utenti a passare ad un abbonamento a pagamento (allineato fra i vari strumenti a circa 20 euro mensili).

Fa eccezione NoteBook LM che, sebbene limitato rispetto alla versione a pagamento, ha dei limiti talmente elevati da non richiedere un upgrade salvo situazioni molto particolari.

I limiti imposti dai produttori possono, a dire il vero, essere superati in vario modo.

Il più banale è quello di disporre di più di un account, ma anche in questo caso è l'uso contemporaneo di più strumenti che permette ad un utente di poter disporre di un numero di interrogazioni giornaliere in grado di soddisfare le esigenze più comuni.

Nella tabella 1 sono elencati solo 9 strumenti, ma nella realtà nuovi modelli vengono rilasciati con una frequenza molto elevata arricchendo il numero di strumenti di cui un utente può disporre.

A tal proposito è pertanto utile effettuare periodicamente una ricerca on line per individuare nuovi modelli.

Perché usare più strumenti

Nei paragrafi precedenti è apparso evidente come la possibilità di utilizzare contemporaneamente più strumenti, comporti dei vantaggi sia in termini di confidenzialità nella risposta fornita, sia per il superamento dei limiti d'uso delle versioni gratuite.

Ma un altro motivo delle necessità di usare più modelli è legato alla specificità di ognuno di essi.

Ad esempio, l'analisi di documenti di grandi dimensioni è una caratteristica di NoteBook LM che trova poco riscontro negli altri strumenti.

Non va infatti confusa la teoria con la pratica che deriva dall'esperienza.

Questo considerando sempre la particolarità di questi strumenti, e cioè la loro costante e velocissima evoluzione, che rende la propria esperienza con ognuno di essi, obsoleta nel giro di poche settimane.

Ad esempio, nella mia esperienza (con tutti i limiti appena evidenziati), strumenti diversi da NoteBook LM sono in grado di prendere in carico documenti molto corposi,

ma ne analizzano dettagliatamente solo le prime pagine. Solo NoteBook LM, nel corso delle mie prove, ha mantenuto una costante capacità di analisi.

Al di là di questo esempio specifico, un confronto con i risultati di un'analisi effettuata con strumenti diversi permette di valutare quale strumento sia il più adatto ad uno specifico scopo.

Anche in questo caso tuttavia, il risultato non necessariamente è legato effettivamente allo strumento in uso, ma può derivare da un prompt non appropriato.

Se ad esempio chiedete ai vari strumenti di generare una check list per effettuare un audit in ambito business continuity, otterrete risposte molto diversificate in quanto numerosità e rappresentazione delle domande che la compongono.

Ma se chiedete di generare una check list specificando che deve contenere 100 domande, il risultato ottenuto con i vari strumenti sarà in realtà molto simile.

Il rispetto delle normative

Il fatto che tali strumenti siano così facili da utilizzare e per lo più gratuiti non deve far dimenticare che il loro uso è soggetto ad alcune normative, in particolare al GDPR e all'AI ACT.

Se si trattano dati personali devono essere rispettate tutte le prescrizioni del GDPR e, nella maggior parte dei casi, se si usano dati personali con questi strumenti, lo si fa per profilare un soggetto, un trattamento questo, specificatamente normato dal GDPR e sottoposto a pesanti limitazioni.

Attenzione quindi a effettuare attività di questo tipo.

Quanto all'AI ACT, alcuni usi potrebbero configurarsi, in determinate circostanze, anche come una attività ad alto rischio, e quindi soggetta a tutte le limitazioni del caso.

Conclusione

Per chiudere, l'uso degli strumenti di AI generativa, anche nelle loro versioni gratuite, aumenta considerevolmente la produttività individuale anche nell'ambito della individuazione e della implementazione dei requisiti di una qualunque normativa. Quello che è indispensabile è conoscerne a fondo limiti e funzionalità, avendo presente che la loro evoluzione è costante e quindi è necessario rivedere continuamente le proprie aspettative e le proprie certezze.

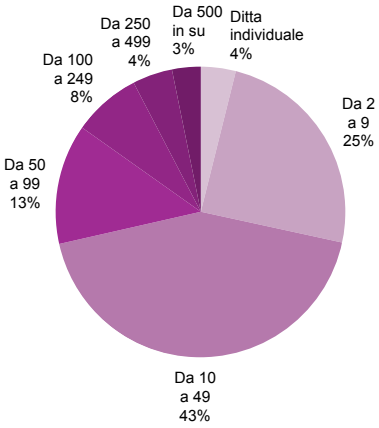
Analisi della survey sulla cybersecurity delle imprese promossa dalla Camera di Commercio di Modena nel 2025

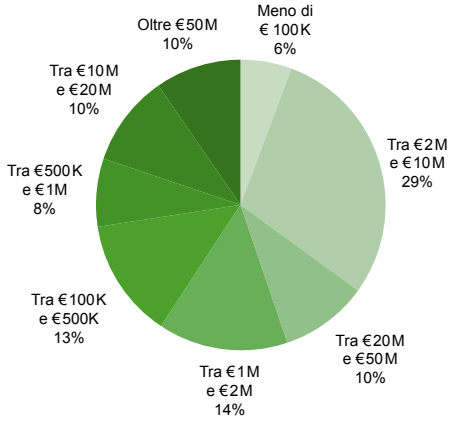
[A cura di Antonio Apruzzese, Mauro Andreolini, Luca Chiantore, Mauro Cicognini, Mauro Leoncini, Mirco Marchetti e Giuseppe Molinari]

Come nel 2024, la Camera di Commercio di Modena ha promosso nei confronti delle imprese del proprio territorio una survey che è stata predisposta in collaborazione con Clusit e l'Università di Modena e Reggio.

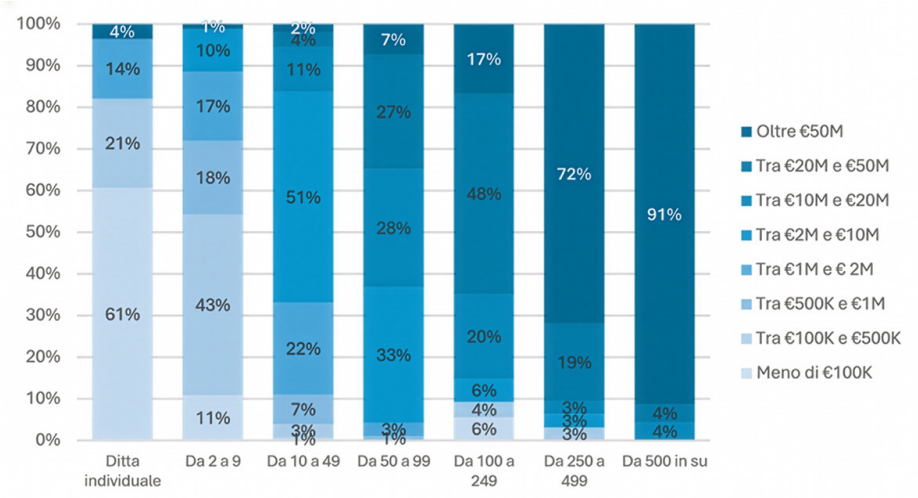
Quest'anno le risposte al questionario sono giunte da 715 aziende (501 nel 2024), caratterizzate dalla seguente distribuzione per numero di addetti e fatturato. Rispetto ai dati del 2024, l'incremento nelle aziende che hanno risposto è avvenuto principalmente nella fascia tra 10 e 49 addetti, più che raddoppiate da 147 a 308.

Questo rispecchia la realtà più diffusa delle aziende italiane, e consente di trarre delle conclusioni sicuramente interessanti e forse valide anche a livello nazionale.





La distribuzione in termini di fatturato in base al numero di addetti è evidenziata nel grafico che segue, il quale rispecchia quanto ci si aspetterebbe, con il fatturato sostanzialmente commisurato al numero di addetti.



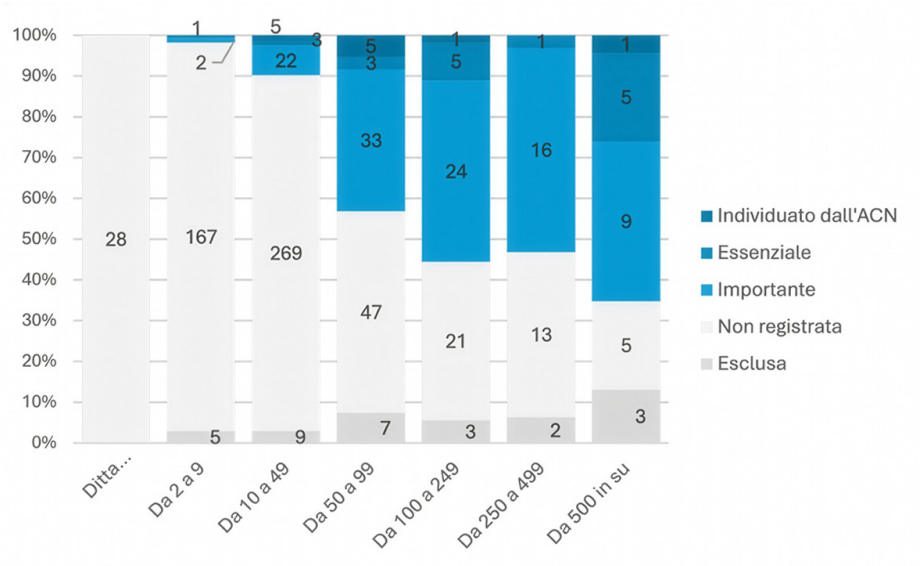
Normativa NIS2

Rispetto alla survey dell'anno scorso, una differenza assai importante è stata l'entrata in vigore, il 16 Ottobre 2024, del cosiddetto "Decreto NIS2" (D. Lgs. 138/2024), che recepisce Direttiva (UE) 2022/2555.

Tra le 715 aziende della survey, 136 hanno dichiarato di essere soggetti NIS2, avendo anche ricevuto conferma dall'ACN, che è Autorità NIS per l'Italia. Dei soggetti regolati, 13 sono state individuati direttamente dall'ACN stessa (verosimilmente perché sono enti molto importanti e/o che già ricadevano sotto la versione precedente della direttiva NIS); 17 sono soggetti "essenziali", ovvero le aziende più grandi e ad alta criticità; i restanti 106 sono soggetti "importanti".

Delle 579 aziende che non sono soggetti NIS, 550 hanno direttamente ritenuto di non essere soggetti NIS, mentre 29 si sono registrate ma sono poi state esplicitamente escluse dall'ACN.

La distribuzione dei soggetti NIS rispetto al totale è mostrata nel grafico seguente.



La Direttiva NIS2 esclude, salvo eccezioni, le imprese piccole e le microimprese, e pertanto non sorprende che il grosso dei soggetti sia nelle fasce con 50 addetti o più.

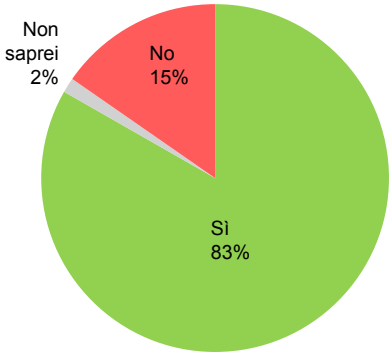
È interessante notare, tuttavia, come le eccezioni in effetti esistano, anche in un ambito locale come la provincia di Modena, dove addirittura ci sono 3 soggetti NIS (di cui uno individuato dall'ACN) nella fascia con meno di 10 addetti, e 30 soggetti NIS (di cui 3 essenziali ed uno individuato dall'ACN) con meno di 50 addetti.

La NIS2 si conferma, come già altri hanno notato, come una regolamentazione pervasiva nel tessuto produttivo, e che non potrà mancare di portare effetti importanti sulle aziende, in primis sui soggetti regolati e nei settori dove è direttamente applicabile, ma immediatamente a seguire, tramite il meccanismo del controllo sulla *supply chain* anche su buona parte delle realtà che non sono immediatamente soggette.

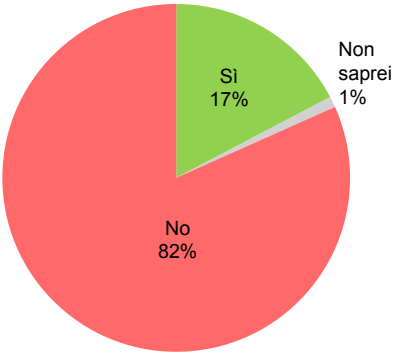
Infrastrutture Web e rete

La percentuale di aziende dotate di un sito Web è sostanzialmente invariata rispetto al 2024, nonostante l'incremento delle risposte, il che ci conferma che l'esposizione su Internet è ormai un fatto consolidato, e ha un buon livello di maturità.

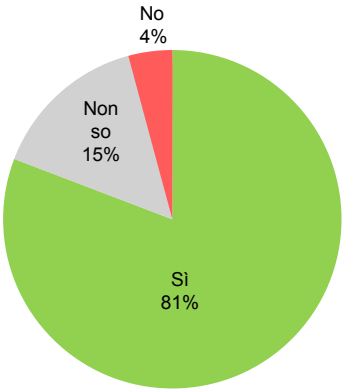
Presenza sito Web



Presenza e-commerce



Presenza in Rete



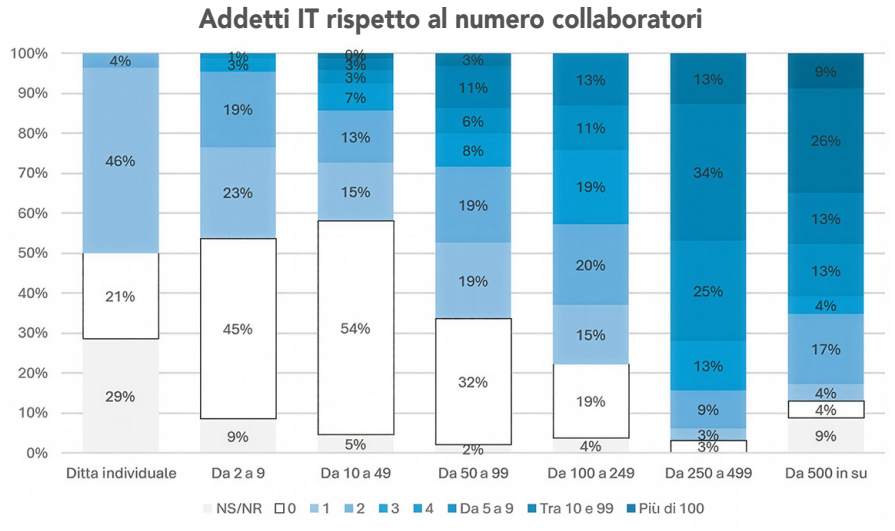
Anche la percentuale di aziende dotate di un sito di e-commerce è del tutto invariata; ciò suggerisce che l'appetito delle aziende della zona per l'uso di questi strumenti ha forse raggiunto un plateau da cui non è semplice muoversi.

È interessante anche notare che le protezioni di base dell'infrastruttura di rete sono ormai parte del patrimonio comune.

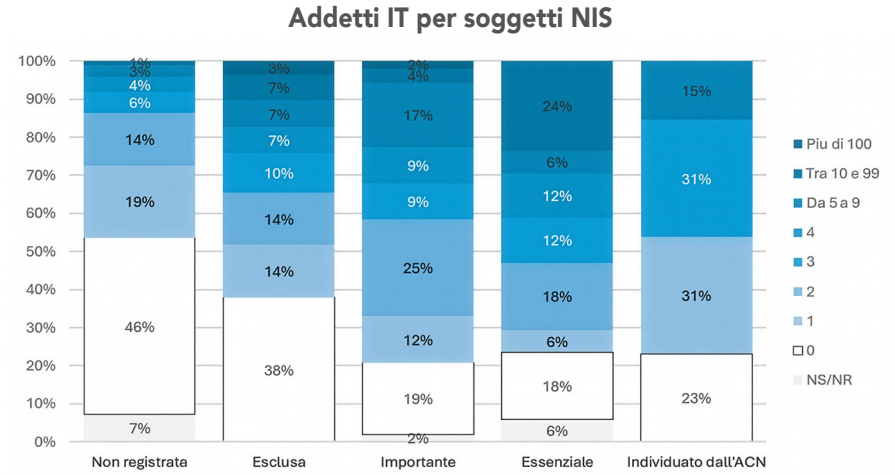
Organizzazione IT e cybersecurity

Nel 2025 si conferma come l'equipe IT "tipica", ovvero quella più presente nelle aziende più numerose del campione (le aziende tra 10 e 49 collaboratori) sia fatta di una, due, o meno spesso di tre persone. La terza persona diventa più frequente solo in realtà che superano i 100 addetti.

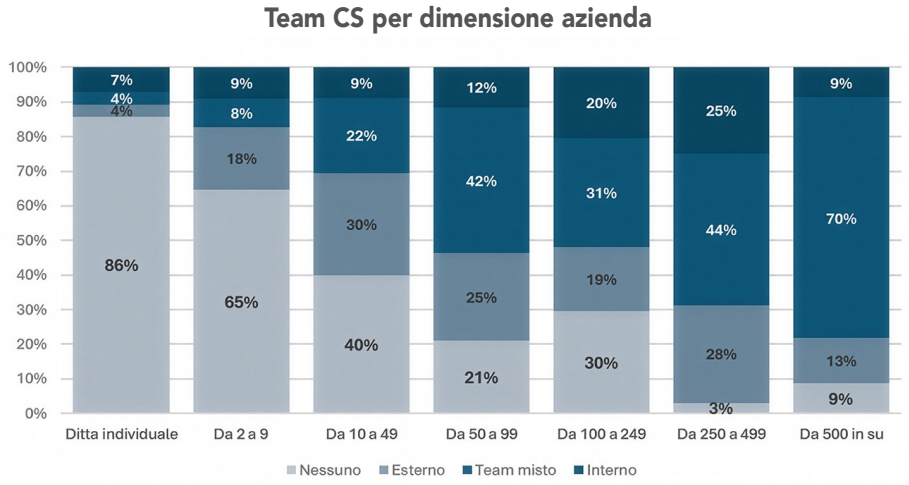
In più di metà delle aziende fino a 50 dipendenti nessuno si occupa di IT, nemmeno a tempo parziale.



Suddividendo le aziende in base all'essere soggetti NIS, vediamo che l'attenzione per l'IT cresce, ed in circa i tre quarti del totale vi è almeno una persona in organico con funzioni dedicate all'IT. Rimane vero, purtroppo, che anche nei soggetti NIS i team dedicati all'informatica sono poco numerosi: ad esempio, il 47% dei soggetti essenziali ed il 58% dei soggetti importanti conta meno di 3 persone nel reparto IT.

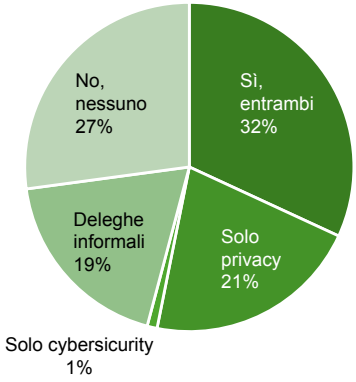


Per quanto riguarda i team di cybersecurity, i dati del 2025 confermano in buona parte quelli del 2024. Risulta positivamente un visibile incremento del personale interno nelle aziende tra 250 e 500 collaboratori, che è detto presente nel 25% dei casi mentre nel 2024 era riportato solo dal 13%. Nelle aziende più grandi c'è un parziale riequilibrio tra team solo interni e team misti, ma il totale delle aziende con almeno parte del personale interno risulta cresciuta dal 63% al 79%.



Purtroppo, si deve riscontrare invece che la presenza di responsabilità formali per cybersecurity e privacy diminuisce dal 61% al 54%, forse per la maggiore numerosità del campione sulle fasce relativamente meno organizzate del mercato. Inoltre, diminuisce la consapevolezza delle certificazioni, con la percentuale di rispondenti che non ne sanno nulla che cresce dal 36% al 42%, e le percentuali di persone certificate che diminuiscono leggermente.

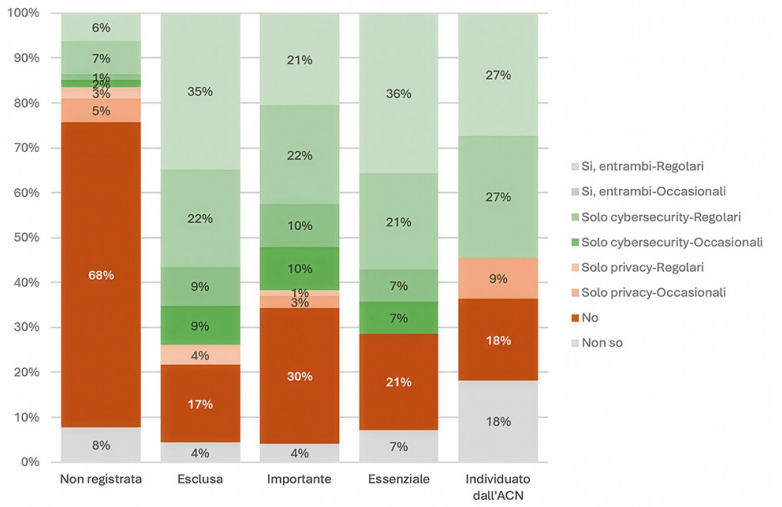
Responsabili Privacy e Security



Presenza Certificazioni

La formazione si conferma essere un ambito in cui le aziende dovranno investire di più, anche alla luce degli obblighi specifici derivanti dalla normativa NIS. Nei soggetti importanti ed essenziali la formazione di cybersecurity è presente solo in circa due terzi del totale (con un dato leggermente più favorevole nel caso dei soggetti essenziali), ma comunque in un'impresa essenziale su cinque non viene fatta alcuna formazione, ed in molte l'offerta di formazione è solo occasionale.

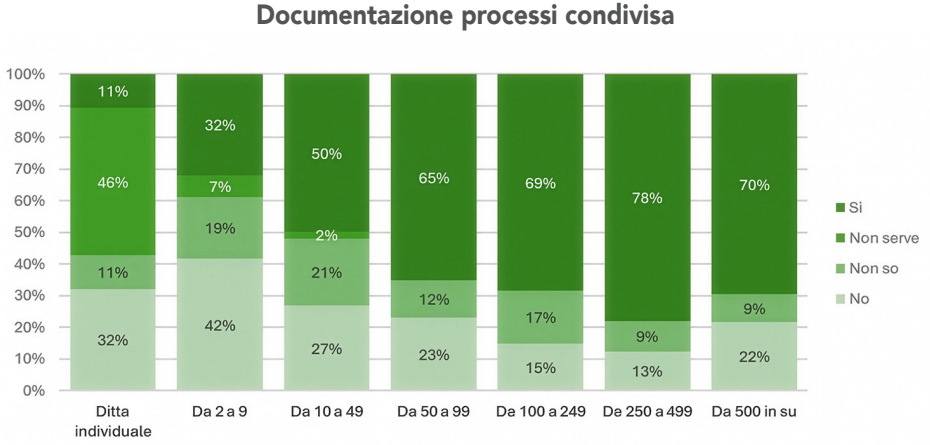
Offerta di formazione Cyber/Privacy



Le aziende che si sono registrate ma sono state escluse dimostrano comunque un tasso di consapevolezza del tema significativo, al punto di disporre di formazione in ambito cybersecurity più spesso delle realtà che sono state individuate dall'ACN (le quali, ricordiamo, sono in genere realtà molto importanti, e spesso anche assai grandi).

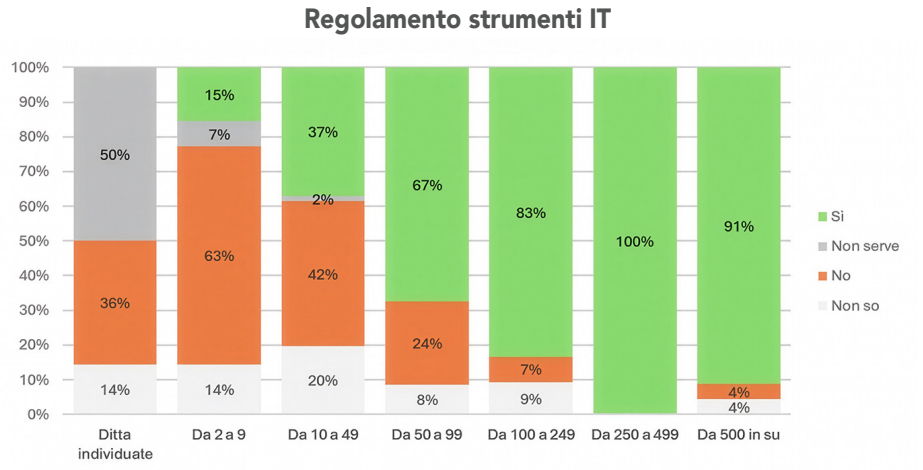
Politiche e procedure

L'adozione di politiche formalizzate, e la loro conoscenza da parte dei collaboratori, sono altresì un punto ancora problematico. Tranne il caso delle ditte individuali, che naturalmente non hanno collaboratori ai quali divulgare le procedure, il dato di conoscenza delle procedure aziendali rimane basso, e fa sospettare che in realtà nasconda l'assenza di queste procedure.



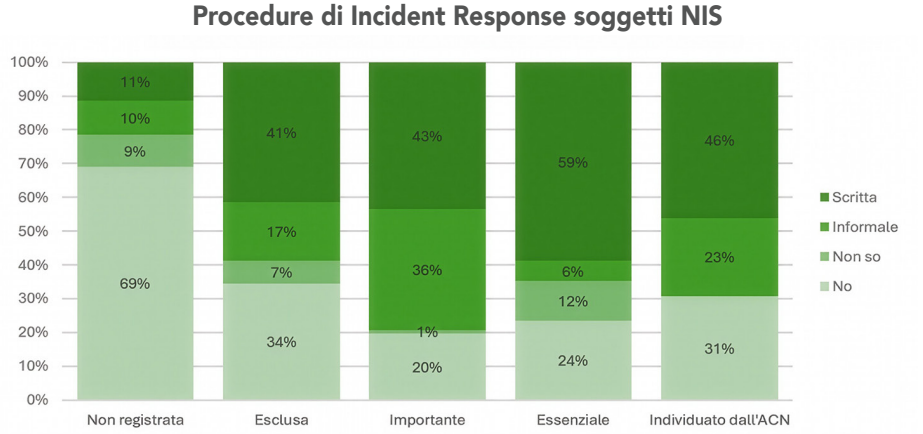
La perdurante scarsa presenza del regolamento d'uso degli strumenti IT aziendali, che è fondamentale per la conformità sia a NIS2 ma anche al GDPR (che impatta su tutti) corrobora la deduzione precedente, ovvero che le procedure aziendali siano assai poco formalizzate, soprattutto nelle aziende sotto i 50 dipendenti, e che lo siano quasi per nulla in quelle sotto i 10.

Ricordando che le aziende sotto i 50 collaboratori costituiscono quasi il 75% del campione, si può dedurre che questo regolamento interno, obbligatorio da anni, viene detto assente (o inutile) in circa metà delle realtà che hanno risposto alla survey.

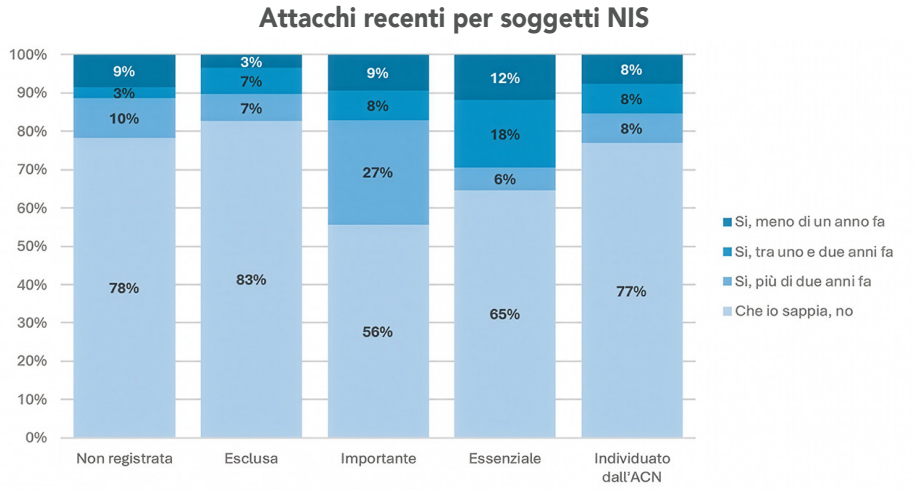


Attacchi e risposta agli incidenti

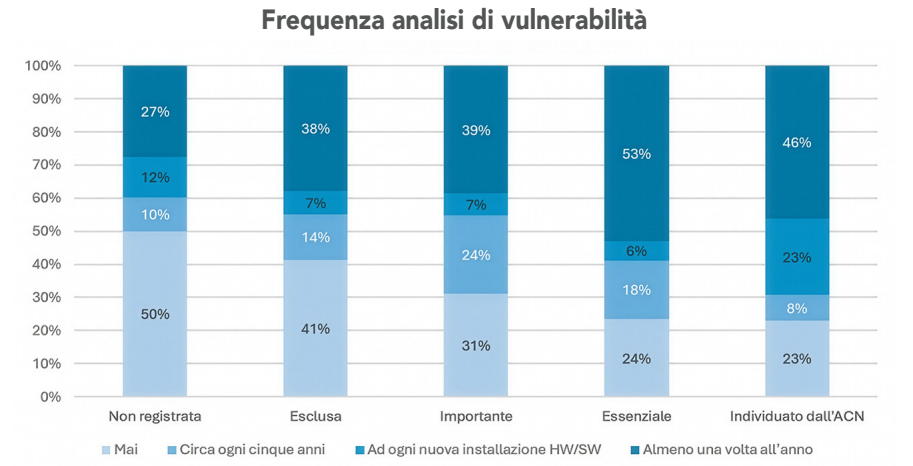
Tra gli obblighi derivanti dalla normativa NIS2 vi è quello di una pronta reazione agli incidenti cyber, che sono un'eventualità ormai del tutto comune e contro la quale il legislatore correttamente prescrive di essere preparati. Risulta quindi confortante constatare che una procedura formale di Incident Response viene detta già presente in circa metà dei soggetti NIS; auspichiamo, negli aggiornamenti futuri di questa survey, di poter vedere il 100% dei soggetti dotati di questo importante strumento.



Gli attacchi cyber, infatti, si confermano una realtà per una percentuale assai significativa dei rispondenti, come si può vedere nel grafico sottostante. Assai interessante che i soggetti NIS importanti riportino più attacchi dei soggetti essenziali, i quali, tuttavia, risultano essere stati attaccati più di recente.



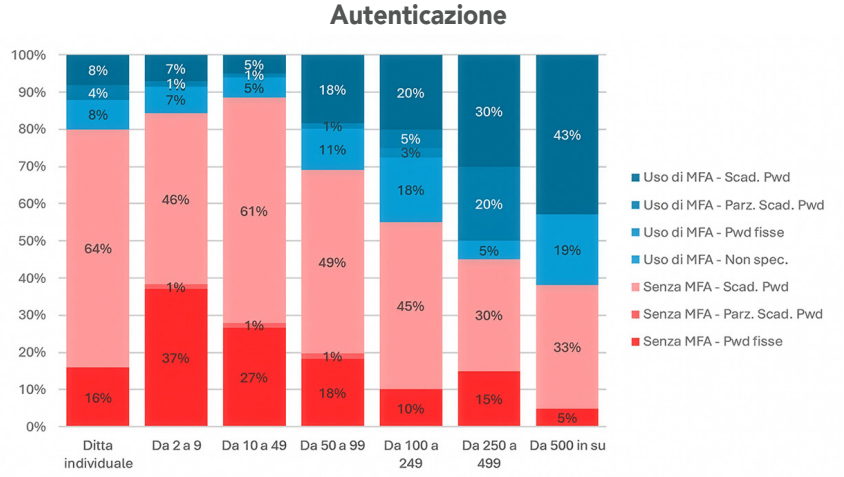
Interessante anche constatare come l'analisi di vulnerabilità non sia ancora particolarmente diffusa; anche tra i soggetti NIS quasi un terzo non ha un programma regolare di VA, e circa un quarto non lo ha affatto.



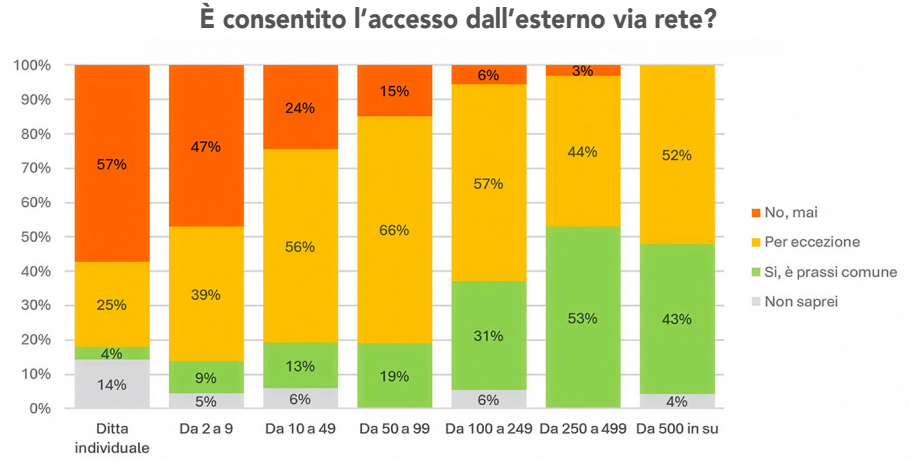
Gestione dispositivi e accesso

Il controllo degli accessi rimane in larga misura affidato alla tradizionale combinazione username/password, mitigata almeno in parte da misure di scadenza periodica delle password. Cogliamo l'occasione per rimarcare come, tuttavia, la scadenza automatica delle password non sia più parte delle best practice da parecchio tempo, essendo stata rimpiazzata dalla raccomandazione di implementare MFA dovunque possibile, richiedere password di elevata lunghezza ma senza imporre particolari sintassi, e prescrivere di cambiarle solo in caso vi sia il sospetto che possano essere state compromesse.

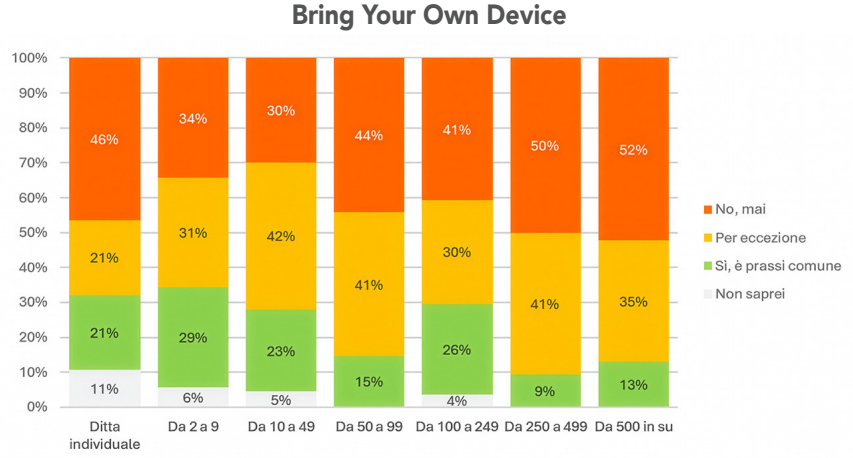
Rispetto al 2024, si può apprezzare una evidente crescita della percentuale di aziende che fanno uso di MFA, indice della crescente consapevolezza dei numerosi attacchi che hanno sfruttato la presenza di password compromesse e non modificate tempestivamente.



Le aziende, a quanto si può supporre, amano pensarsi molto protette nelle loro infrastrutture informatiche, e generalmente dicono di consentire accessi "dall'esterno" con grande cautela. Nelle aziende più piccole prevale una quasi totale chiusura, almeno a priori; al crescere della dimensione, verosimilmente è sempre più frequente accorgersi di dover fare almeno qualche eccezione. Nelle grandi aziende, si può notare che rispetto al 2024 è sparita la fetta di "No, mai", e forse un po' di pragmatismo si è fatto strada.



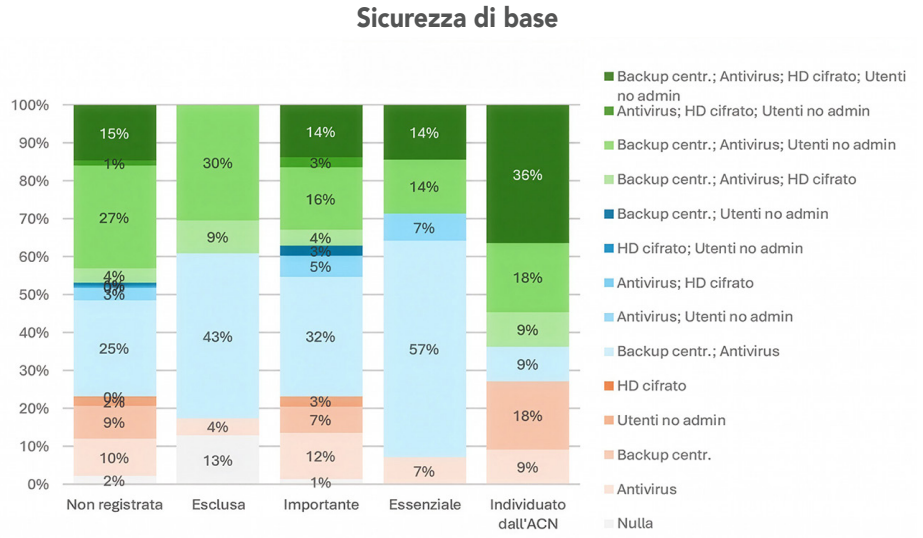
Nella realtà dei fatti, più o meno qualsiasi azienda consente in larga misura l'utilizzo di dispositivi personali per collegarsi alla rete aziendale, cosa che introduce variabili non controllate direttamente all'interno dell'infrastruttura IT, contraddicendo direttamente quanto affermato nella policy di cui sopra. Si auspica che in futuro si possa normare questi accessi senza chiusure preconcette, tenendo conto delle normali necessità lavorative.



Tecnologie di sicurezza di base

Si riscontra una insufficiente diffusione di tecnologie di sicurezza di base, anche negli ambienti NIS, benché le tecnologie delle quali si è investigata la diffusione siano ormai ampiamente consolidate, affidabili, e diffuse su tutte le piattaforme. Anche il loro costo risulta assai contenuto, o anche nullo, come nel caso della pratica di non dare agli utenti credenziali amministrative sui computer a loro in uso.

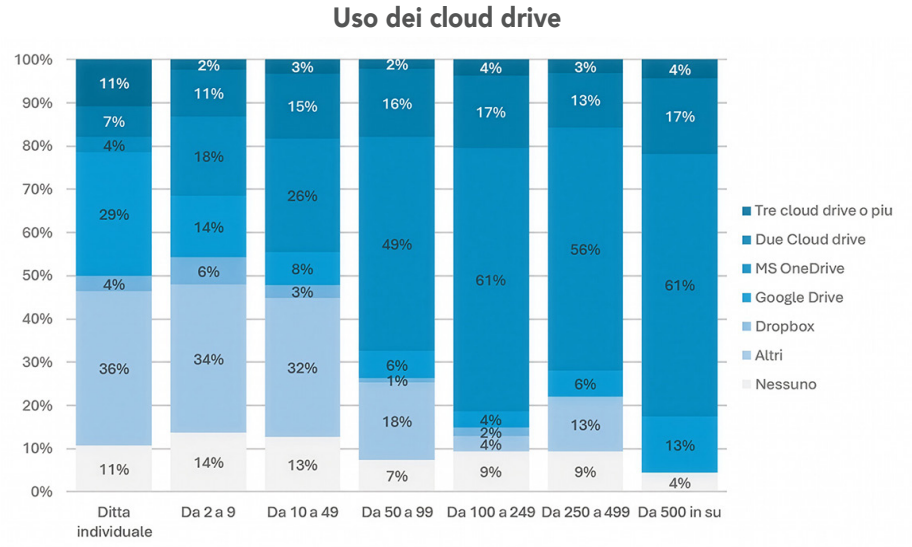
In particolare, meno di un terzo dei soggetti NIS adotta tutte e quattro le misure di sicurezza di base proposte, e particolarmente preoccupante risulta la presenza, in quasi due terzi dei soggetti essenziali, di utenti dotati di credenziali amministrative per il loro dispositivo.



Più confortante è, dal punto di vista dell'affidabilità della memorizzazione dei dati, la presenza ormai pervasiva dei sistemi di "cloud drive", come Microsoft Onedrive, Google Drive, ed altri, con quasi tutte le aziende che hanno a disposizione almeno una tecnologia, ed in una percentuale significativa anche due o tre.

Queste tecnologie rappresentano senz'altro un notevole complemento di cautela, rispetto all'utilizzo dei soli meccanismi di backup tradizionali. Non si sostituiscono ad esse, naturalmente, ma si affiancano in una strategia complessiva di affidabilità del dato, ed aggiungono una notevolissima facilità d'uso che è senz'altro positiva.

Naturalmente, il rovescio della medaglia consiste nella necessità di farne un uso consapevole, che per chi fa sicurezza consiste nell'evitare che la condivisione molto semplice consentita dai cloud drive porti a diffusioni incontrollate di dati ed informazioni, soprattutto qualora il dato condiviso sia anche un dato personale. Con le opportune cautele, tuttavia, l'uso dei cloud drive rappresenta un significativo passo avanti, soprattutto per le realtà che difficilmente si sarebbero potute permettere un'infrastruttura così evoluta in locale.



Conclusioni

La survey del 2025 ci mostra una certa tendenza alla crescita della maturità di cybersecurity delle imprese modenesi, ma evidenza anche, in modo a volte impietoso, un divario tra uno stato adeguato alla situazione attuale delle minacce e le misure di sicurezza esistenti. A maggior ragione la presenza di requisiti cogenti, che derivano dalla normativa NIS2 e non solo, fa risaltare la lunghezza del cammino che a volte è ancora necessario percorrere.

Inoltre, è evidente una bassa tendenza ad integrare il rischio cyber nelle valutazioni aziendali per quello che è, ovvero un rischio di business, e non un rischio IT. Si percepisce dai dati la voglia di potersi semplicemente dimenticare del problema,

ignorandolo nella speranza forse che se ne vada da solo, o delegandolo ad una persona: spesso, come si notava, letteralmente una sola persona.

Infatti, se da un lato la presenza di team IT e l'offerta di formazione sono aumentate in alcune segmentazioni di mercato, dall'altro solo metà delle aziende soggette a NIS2 dispone di una procedura formale di Incident Response – cosa che, a due mesi dall'entrata in vigore degli obblighi di segnalazione NIS, appare quantomeno imprudente. La diffusione di pratiche di sicurezza di base rimane insufficiente, soprattutto nelle piccole realtà; il persistente uso di credenziali amministrative, la dipendenza da username/password e l'assenza di regolamenti IT costituiscono vulnerabilità evidenti, mentre la gestione dei dispositivi personali e l'uso dei cloud drive, se non controllati, possono generare fughe di dati.

Per raggiungere la piena conformità e mitigare i rischi, è fondamentale intensificare la formazione specifica, rafforzare i processi, formalizzare le necessarie procedure, e implementare tecnologie di sicurezza di base (MFA tra tutti). Le autorità di controllo e governo e gli stakeholder dovrebbero promuovere programmi di supporto, incentivi e audit mirati per le imprese con meno di 50 dipendenti, in modo da ridurre l'ineguaglianza digitale e garantire che la NIS2 non sia solo una norma di riferimento ma un reale strumento di resilienza aziendale.

Cybersecurity nei sistemi portuali: dall'esigenza di adeguamento alla resilienza sistemica

Analisi, governance e piano di miglioramento per la protezione di un'infrastruttura critica complessa

(A cura di: Georgia Cesarone e Paola Girdinio [Centro di Competenza START 4.0]; Antonella Granero e Marco Molinari [Autorità di Sistema Portuale del Mar Ligure Occidentale])

La digitalizzazione dei porti rappresenta una delle frontiere più delicate e strategiche della trasformazione digitale del Paese. I porti italiani e in particolare quelli del sistema ligure, sono infrastrutture vitali per l'economia nazionale e per la catena logistica europea. Gestiscono ogni anno non solo milioni di tonnellate di merci, ma anche flussi di dati e servizi interconnessi che coinvolgono una molteplicità di attori: autorità e istituzioni pubbliche, imprese, operatori marittimi, fornitori di servizi digitali, enti di sicurezza.

In questo ecosistema complesso, la **cybersecurity** deve smettere di subire l'errata percezione di elemento tecnico di contorno e deve diventare condizione essenziale e imprescindibile di operatività, affidabilità e competitività.

È su questa consapevolezza che si fonda il progetto "**Interventi a supporto della consapevolezza e della postura nel rischio cyber per la resilienza di un sistema portuale complesso**", promosso dall'**Autorità di Sistema Portuale del Mar Ligure Occidentale** con il supporto del **Centro di Competenza START 4.0** e finanziato dall'Agenzia per la cybersecurity nazionale grazie al **PNRR Missione 1 – Componente 1 – Investimento 1.5 'Cybersecurity'**.

L'iniziativa nasce dall'esigenza di rafforzare la **resilienza cybe**r di un'infrastruttura, come il sistema dei porti di Genova, Pra', Savona e Vado Ligure, che non è solo un nodo logistico ma un **sistema socio-tecnico** ad alta interdipendenza tra mondo fisico e digitale.Un attacco informatico in questo contesto non comporta solo la perdita di dati o l'interruzione di servizi digitali: può bloccare navi, interrompere catene di fornitura, compromettere la sicurezza fisica delle persone e degli impianti.

Governance e consapevolezza: la base della resilienza

La prima area di intervento del progetto riguarda la **governance e la programmazione cyber**, un punto critico per molte organizzazioni pubbliche e private. Nel caso dell'Autorità di sistema portuale, la complessità deriva dal duplice ruolo dell'ente: da un lato soggetto di governance, dall'altro parte attiva della supply chain portuale. Questa posizione intermedia rende indispensabile un **modello di gestione integrato** che includa ruoli, responsabilità e processi trasversali, capace di armonizzare le esigenze di sicurezza interna con quelle del cluster marittimo nel suo insieme.

L'approccio proposto da START 4.0 si basa su una **logica data-driven real-time**, che consente di monitorare costantemente vulnerabilità, rischi e azioni di mitigazione. La cybersecurity, dunque, non è intesa come un insieme statico di misure, ma come un **processo dinamico e misurabile**, in cui il dato diventa lo strumento per la decisione e la pianificazione strategica.

In questa direzione, il progetto prevede una serie di fasi fondamentali:

1. **Rilevamento del perimetro cyber-fisico**, comprendendo sia i sistemi IT che quelli OT e IoT;

2. **Individuazione dei processi di governance** che garantiscano sicurezza tecnologica, organizzativa e umana;
3. **Contestualizzazione del Cybersecurity Framework nazionale** e delle normative europee, dalla Direttiva NIS2 al Cyber Resilience Act;
4. **Deployment di una piattaforma GDPR e privacy compliance** integrata nella strategia di rischio;
5. **Definizione di una roadmap di miglioramento** che renda la postura cyber dell'ente continuamente aggiornabile.

Analisi e gestione del rischio: dal perimetro alla catena del valore

Un secondo asse strategico riguarda la **gestione del rischio cyber** e la **continuità operativa**. L'analisi del rischio, spesso percepita come un mero esercizio burocratico, diventa qui uno **strumento di prevenzione attiva**, capace di orientare politiche, investimenti e priorità di intervento.
La valutazione si estende oltre i confini dell'Autorità portuale per includere i partner e i fornitori, con un'attenzione particolare alla **supply chain digitale**: un ecosistema che, se non governato, può amplificare le vulnerabilità dell'intero sistema.

Oltre all'analisi dei rischi, il progetto prevede lo sviluppo di **piani di business continuity** e **disaster recovery** che tengano conto non solo degli aspetti tecnologici, ma anche di quelli organizzativi e comunicativi.

Il principio guida è quello della **resilienza multilivello**: la capacità non solo di reagire ad un attacco, ma di mantenere operativi i servizi critici e ripristinare rapidamente la normalità grazie a procedure consolidate, competenze aggiornate e una governance coordinata.

Incident management e risposta coordinata: la centralità dei fattori, competenze e procedure per ridurre i tempi

La gestione e risposta agli incidenti di sicurezza è il banco di prova della maturità cyber di un'organizzazione. Nel contesto portuale, in cui l'interruzione di un servizio può avere impatti immediati su scala nazionale, il tempo di reazione è una variabile determinante.

Il progetto di AdSP introduce un approccio strutturato di **Incident Response Management**, fondato su processi documentati, strumenti di **monitoraggio in tempo reale**, e capacità di **analisi forense** per comprendere la natura e la portata dell'attacco. A questo si aggiunge l'integrazione di **piani di comunicazione interna ed esterna**,

indispensabili per gestire in modo coordinato la notifica alle autorità competenti — come l'Agenzia per la Cybersicurezza Nazionale — e l'informazione al pubblico.
La logica è quella del **miglioramento continuo**: ogni incidente diventa occasione per rivedere policy, procedure e competenze, riducendo progressivamente il tempo di rilevamento e risposta.

Identità digitali e sicurezza perimetrale: la nuova frontiera dell'accesso

Un'infrastruttura distribuita come quella portuale richiede un approccio avanzato alla **gestione delle identità e degli accessi logici**.
Il progetto prevede l'estensione generalizzata **dell'autenticazione** a più fattori a tutto il personale interno e agli stakeholder esterni, tramite l'implementazione di un **sistema di Identity & Access Management** capace di profilare utenti e dispositivi. In un contesto in cui il lavoro remoto e la connessione di dispositivi personali sono ormai prassi, l'autenticazione forte e la segregazione degli accessi diventano elementi di sicurezza imprescindibili.

Parallelamente, l'AdSP sta completando l'ammodernamento dell'infrastruttura di rete, con l'introduzione di apparecchiature di nuova generazione. La protezione perimetrale, tuttavia, è vista come parte di un **sistema difensivo integrato**, che combina aggiornamento tecnologico, formazione specialistica e politiche di sicurezza condivise.

La cultura della sicurezza: le persone al centro.

La tecnologia è solo una parte dell'equazione.
Il vero fattore abilitante della resilienza cyber è la **cultura della sicurezza**, costruita attraverso formazione, consapevolezza e collaborazione. Per questo, il progetto prevede **programmi di cybersecurity awareness** rivolti non solo al personale dell'Autorità ma anche agli operatori del cluster marittimo, alle società concessionarie, ai fornitori di servizi tecnici e alle imprese portuali.
Questa visione si inserisce perfettamente nel principio cardine della **Direttiva NIS2**, che riconosce la sicurezza come responsabilità condivisa lungo l'intera filiera produttiva.

Il porto diventa così un **ecosistema consapevole**, in cui ogni attore — dal dirigente al tecnico di banchina — comprende il proprio ruolo nella difesa digitale collettiva. La formazione è concepita non come un evento episodico, ma come un processo continuo di aggiornamento, adattivo alle nuove minacce e coerente con le evoluzioni normative.

Un approccio sistemico: dalla compliance alla resilienza

Uno degli aspetti più innovativi del progetto è la capacità di **trascendere la logica della compliance** per abbracciare una **visione olistica della resilienza**.

Le normative (dalla NIS2 al Cyber Resilience Act, dal GDPR al nuovo Regolamento Macchine) non sono trattate come vincoli burocratici, ma come strumenti per orientare la strategia di sicurezza nel lungo periodo.

L'obiettivo è quello di costruire un **modello di gestione ripetibile**, in grado di adattarsi alle trasformazioni tecnologiche e organizzative senza ricominciare ogni volta da zero.

Il riferimento è il **Cybersecurity Framework nazionale** che struttura la sicurezza in sei funzioni chiave: Identify, Protect, Detect, Respond, Recover e Govern. Attraverso l'analisi di gap tra profilo corrente e profilo target, l'Autorità di sistema portuale può pianificare interventi mirati e misurare nel tempo il progresso verso una maturità cyber evoluta.

Un laboratorio per la sicurezza delle infrastrutture critiche

Il valore del progetto dell'Autorità di sistema portuale del Mar Ligure Occidentale non risiede solo nelle soluzioni implementate, ma nel metodo che propone. Si tratta di un **laboratorio di cybersecurity applicata alle infrastrutture critiche**, un modello esportabile ad altri porti e ad altri settori — dall'energia ai trasporti, fino ai servizi idrici e digitali — che condividono la medesima esigenza di protezione integrata.

La collaborazione con il **Centro Operativo Sicurezza Cibernetica della Polizia Postale** e con la **Capitaneria di Porto** sancisce l'integrazione tra sicurezza fisica e digitale, superando definitivamente la separazione tra *safety e security.* È un passo fondamentale per passare dalla gestione dell'emergenza *alla* **prevenzione sistemica**, in cui la cyber difesa diventa parte del tessuto operativo quotidiano.

Verso un porto intelligente, sicuro e sostenibile

Il futuro della portualità passa per la **connessione intelligente** tra infrastrutture fisiche e digitali, tra macchine, dati e persone. Ma la trasformazione digitale non può essere sostenibile se non è anche sicura.

Il progetto dell'Autorità di Sistema Portuale del Mar Ligure Occidentale rappresenta, da questo punto di vista, un caso emblematico di **integrazione tra innovazione tecnologica, governance e cultura della sicurezza**. Analizzare per prevenire, adeguare per proteggere, collaborare per crescere: sono queste le parole-chiave di una transizione portuale che guarda al futuro con consapevolezza.

La cybersecurity non è più un costo o un vincolo, ma un **abilitatore strategico di efficienza, affidabilità e competitività**. E, come dimostra questa esperienza, può diventare anche un'occasione per ripensare il modo stesso di fare sistema, mettendo la **resilienza collettiva** al centro della sicurezza nazionale.

Sicurezza delle applicazioni cloud: visibilità e controllo continuo dell'ecosistema SaaS

(A cura di Luca Nilo Livrieri e Alberto Greco, CrowdStrike)

Introduzione: il panorama delle minacce e la trasformazione digitale

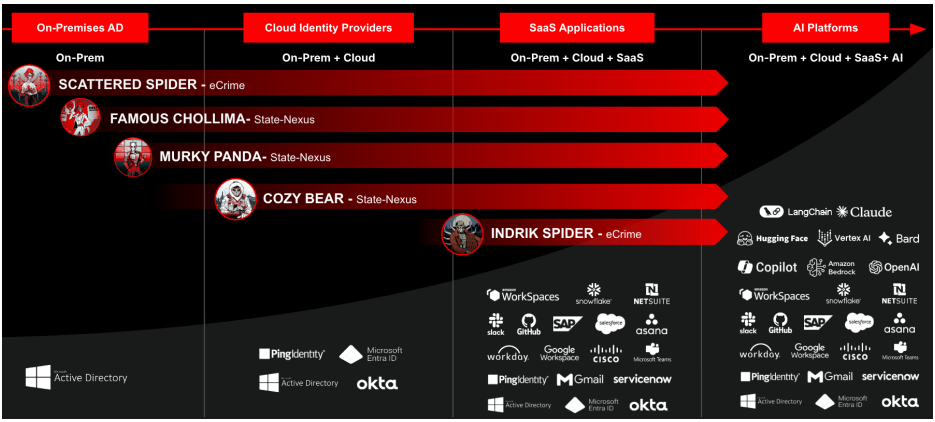
L'adozione massiva delle applicazioni Software as a Service (SaaS) ha rivoluzionato il panorama tecnologico aziendale, offrendo flessibilità operativa, scalabilità dinamica e significative riduzioni dei costi. Tuttavia, questa trasformazione digitale ha introdotto complessità di sicurezza senza precedenti che richiedono approcci innovativi e metodologie avanzate per garantire la protezione dei dati sensibili e la conformità normativa.

Nel contesto aziendale contemporaneo, le organizzazioni utilizzano in media oltre cento applicazioni SaaS diverse, creando un ecosistema tecnologico estremamente articolato che richiede visibilità costante e controllo continuo. La sicurezza tradizionale, basata su perimetri chiaramente definiti e controllabili, risulta inadeguata in un ambiente dove i dati critici risiedono nel cloud pubblico e gli utenti accedono alle applicazioni da qualsiasi posizione geografica attraverso una varietà di dispositivi personali e aziendali.

Perché le applicazioni SaaS sono obiettivi primari per gli attaccanti

Le applicazioni SaaS contengono una ricchezza di dati sensibili, inclusi dati personali di clienti e dipendenti, segreti aziendali e pianificazione strategica. Le comunicazioni aziendali transitano attraverso applicazioni SaaS e molte di queste applicazioni svolgono un ruolo critico nelle operazioni quotidiane. Gruppi di attaccanti sofisticati come COZY BEAR, SCATTERED SPIDER e altri gruppi nation-state ed eCrime ora prendono regolarmente di mira le applicazioni SaaS per rubare dati sensibili.

L'ambiente SaaS presenta una superficie di attacco unica e gli avversari stanno sfruttando lacune che gli strumenti di sicurezza tradizionali non riescono a rilevare. Gli attaccanti fanno leva sulle caratteristiche di accesso distribuito delle applicazioni SaaS, sulla mancanza di supervisione centralizzata della sicurezza e sull'implementazione incompleta dei controlli di accesso per infiltrarsi e persistere negli ecosistemi SaaS.



Le minacce più comuni includono credenziali compromesse attraverso efficaci attacchi di phishing che forniscono agli avversari accesso diretto all'applicazione. Metodologie come hijacking di token OAuth e bypass dell'autenticazione multi-fattore (MFA) permettono agli attaccanti di mantenere accesso persistente anche dopo che le credenziali sono state cambiate.

L'evoluzione da CASB a SSPM: superare i limiti strutturali

I limiti dei Cloud Access Security Broker (CASB)

I Cloud Access Security Broker (CASB) sono stati tra i primi strumenti sviluppati specificamente per affrontare le emergenti sfide di sicurezza del cloud computing. Tuttavia, con l'evoluzione rapida del panorama cloud e l'aumento della sofisticazione delle minacce, sono emersi significativi limiti strutturali che rendono i CASB inadeguati per le esigenze di sicurezza moderne.

Uno dei principali problemi è rappresentato dall'incapacità dei CASB di monitorare efficacemente le configurazioni delle applicazioni senza richiedere personalizzazioni estensive e costose. Ogni applicazione SaaS presenta configurazioni uniche che i CASB non riescono a gestire in modo nativo, richiedendo sviluppi personalizzati per ogni singola integrazione.

Un problema particolarmente critico è quello della "cecità sulla sicurezza". I CASB operano concentrandosi principalmente sui percorsi di accesso e osservando le applicazioni "dall'esterno", attraverso il traffico di rete e le API pubbliche. Questo approccio impedisce di cogliere le sfumature del comportamento degli utenti all'in-

terno delle applicazioni, perdendo informazioni cruciali sui pattern di utilizzo e sui rischi interni. Questa limitazione è particolarmente problematica considerando che le soluzioni di sicurezza tradizionali per endpoint e rete non forniscono visibilità sugli attacchi nativi SaaS, permettendo agli attaccanti di sfruttare questi punti ciechi per muoversi lateralmente tra applicazioni SaaS senza essere rilevati.

L'ascesa del SaaS Security Posture Management (SSPM)

Le soluzioni SaaS Security Posture Management (SSPM) rappresentano l'evoluzione naturale della sicurezza cloud, progettate specificamente per superare le limitazioni dei CASB e per affrontare le minacce avanzate che prendono di mira gli ambienti SaaS. Queste soluzioni lavorano in partnership diretta con gli amministratori delle applicazioni, operando dall'interno dell'ecosistema SaaS piuttosto che dall'esterno.

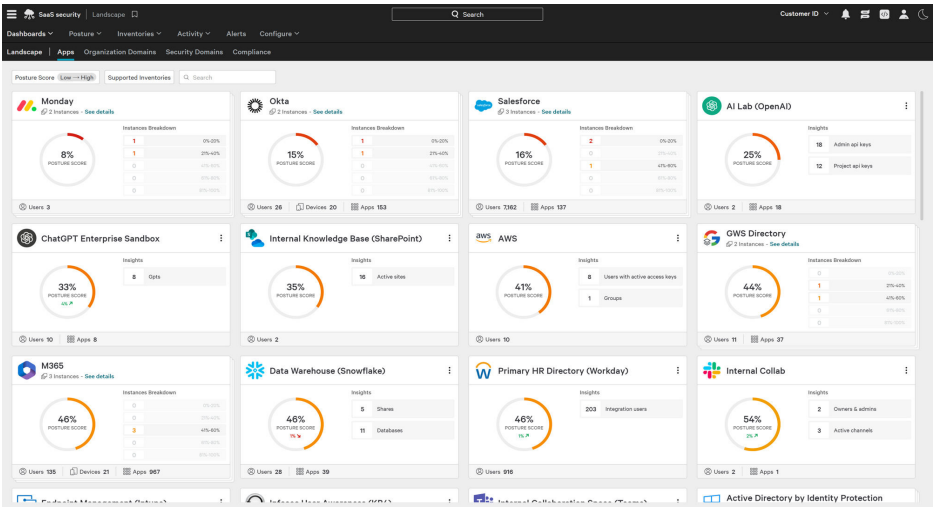
La soluzione SSPM offre una visibilità superiore su configurazioni, utenti e applicazioni di terze parti, resa possibile dall'accesso diretto alle configurazioni e ai dati alla fonte. Una delle caratteristiche distintive è la capacità di fornire non solo visibilità, ma anche strumenti concreti per la remediation, permettendo alle organizzazioni di rispondere efficacemente alle minacce e alle derive delle configurazioni in tempo reale.

Capacità avanzate della gestione della postura di sicurezza SaaS

Gestione completa delle configurazioni errate

La gestione delle configurazioni errate rappresenta il primo pilastro fondamentale della sicurezza SaaS e si tratta di un ambito particolarmente critico considerando che le configurazioni errate SaaS espongono dati sensibili attraverso condivisioni di file accessibili pubblicamente, permessi utente eccessivi e API non protette. Secondo la Cloud Security Alliance, la mancanza di visibilità sull'intero stack SaaS e l'accesso eccessivo alle impostazioni di sicurezza da parte di troppi team rappresentano le cause principali delle vulnerabilità di sicurezza.

La soluzione SSPM fornisce visibilità continua e approfondita su tutte le configurazioni errate presenti nell'ecosistema SaaS aziendale. Ogni configurazione viene tracciata in modo centralizzato, permettendo sia agli utenti business che amministrano quelle applicazioni che ai team di sicurezza di visualizzare i controlli di sicurezza falliti, di categorizzarli automaticamente per gravità, per assegnare in modo dinamico ed adattativo punteggi di rischio alle differenti applicazioni, identificare gli utenti interessati e valutare potenziali impatti sulle conformità.

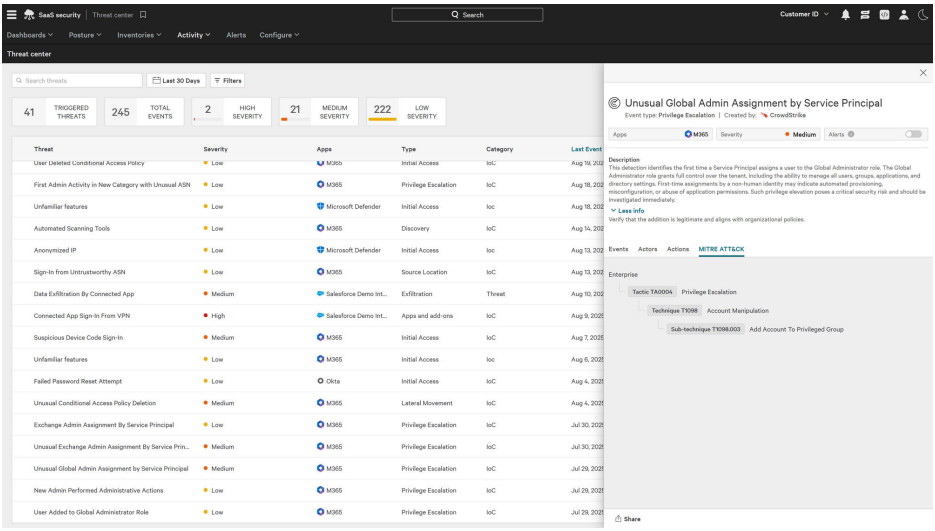


Le funzionalità chiave includono controlli automatizzati delle impostazioni di sicurezza critiche, così da eliminare la necessità di verifiche manuali su migliaia di configurazioni. Il monitoraggio continuo permette di ricevere segnalazioni non appena le configurazioni si discostano dalle impostazioni ottimali, permettendo la creazione automatica di ticket nei sistemi di gestione in uso.

Identity Security Posture Management: controllo completo delle identità

Ogni identità umana e non umana rappresenta un potenziale punto di ingresso nell'ecosistema SaaS e questa vulnerabilità è amplificata dal fatto che gli account dormienti diventano punti di ingresso per gli attaccanti, permettendo loro di evadere rilevamenti tradizionali. La soluzione SSPM rafforza l'ecosistema delle identità delle aziende, prevenendo l'accesso non autorizzato alle applicazioni SaaS aziendali e identificando potenziali minacce interne.

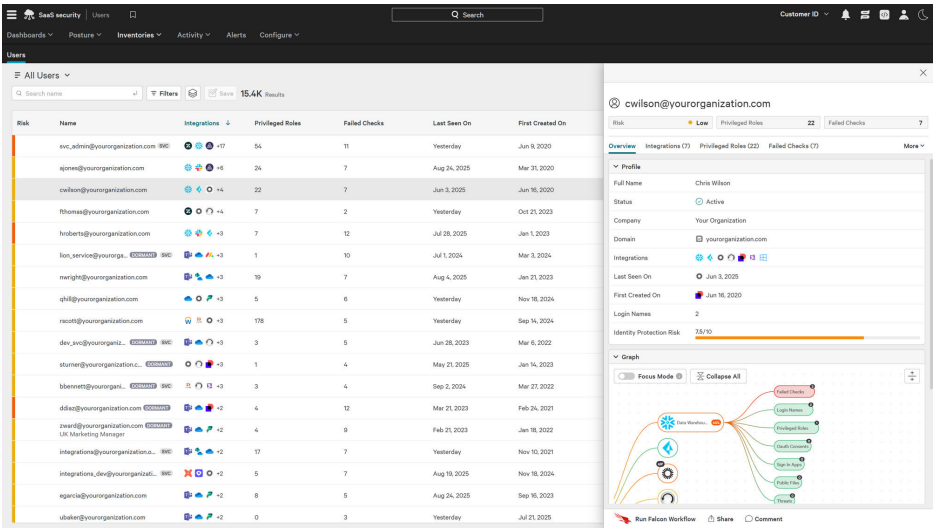
Il monitoraggio degli utenti esterni rappresenta una capacità critica, permettendo di identificare e monitorare tutti gli utenti esterni che hanno accesso alle applicazioni SaaS aziendali. L'identificazione degli utenti dormienti utilizza algoritmi avanzati per il rilevamento automatico di account inattivi che potrebbero essere sfruttati da attaccanti per ottenere accesso non autorizzato.



La gestione degli utenti non più in uso identifica automaticamente utenti che dovrebbero essere stati rimossi dal sistema ma che, per differenti ragioni, mantengono ancora accessi attivi.

Controllo degli accessi SaaS-to-SaaS: gestione delle app non autorizzate

L'ecosistema SaaS moderno è caratterizzato da interconnessioni complesse tra le diverse applicazioni e le app SaaS non autorizzate, spesso configurate senza la supervisione dei team IT o cyber, non onorano le policy di sicurezza e creano vettori di attacco non monitorati. La soluzione SSPM fornisce visibilità completa sulle applicazioni di terze parti connesse, permettendo di identificare potenziali minacce provenienti da app malevole e di controllare l'espansione non autorizzata dell'ecosistema applicativo.



Attraverso questa funzionalità è possibile visualizzare quante applicazioni di terze parti sono connesse alle app SaaS aziendali, quali sono, quale livello di rischio hanno in base ai permessi che sono stati loro concessi. I team di sicurezza possono identificare quali utenti hanno autorizzato l'applicazione, visualizzare i dettagli dell'applicazione e di chi la crea e mantiene, monitorare le configurazioni e le integrazioni per prendere decisioni informate sulla disabilitazione di applicazioni potenzialmente rischiose.

Protezione contro il Hijacking di Token OAuth e Bypass MFA

Una delle minacce più sofisticate che la soluzione SSPM è progettata per affrontare è il hijacking di token OAuth e il bypass dell'autenticazione multi-fattore. Le concessioni di consenso OAuth e altre integrazioni permettono agli attaccanti di mantenere accesso persistente anche dopo che le credenziali sono state cambiate, mentre tecniche come hijacking di sessioni e il furto di cookie possono eludere del tutto l'MFA.

La soluzione monitora continuamente i token OAuth attivi, identificando caratteristiche anomale come token con durata di vita eccessiva o token utilizzati da posizioni geografiche inusuali. Questa capacità è essenziale per rilevare tentativi di persistenza avanzata che potrebbero altrimenti passare inosservati per lunghi periodi.

Rilevamento avanzato delle minacce SaaS: visibilità oltre i punti ciechi tradizionali

Il rilevamento delle minacce SaaS utilizza dati e comportamenti dall'intero stack SaaS per rilevare attività sospette, affrontando specificamente il problema che le soluzioni di sicurezza tradizionali per endpoint e rete non forniscono visibilità sugli attacchi nativi SaaS. Attraverso la sua ampia copertura di integrazioni, le diverse fonti di dati forniscono contesto a ogni avviso, limitando significativamente i falsi positivi.

Rilevamento di credenziali compromesse e attacchi sofisticati

Le capacità di rilevamento includono l'identificazione di attacchi di phishing riusciti che forniscono agli avversari accesso diretto alle applicazioni. La soluzione rileva pattern di accesso anomali che potrebbero indicare account compromessi, inclusi accessi da posizioni geografiche inusuali, utilizzo di dispositivi non riconosciuti o pattern di attività che deviano significativamente dal comportamento normale dell'utente.

Il rilevamento di attacchi di password spraying identifica differenti tentativi di accesso da singoli indirizzi IP che portano ad accessi riusciti, mentre il monitoraggio delle credenziali compromesse rileva accessi con password che sono state violate e appaiono in marketplace di terze parti.

Analisi comportamentale avanzata per minacce interne

La soluzione implementa algoritmi avanzati di analisi comportamentale per identificare potenziali minacce interne e attività sospette che potrebbero indicare account compromessi. Questa capacità include il monitoraggio di attività di download anomale, accessi a dati sensibili al di fuori dei pattern normali di lavoro e tentativi di accesso a risorse per le quali l'utente non ha una necessità operativa legittima.

L'analisi comportamentale si estende anche al rilevamento di movimenti laterali tra applicazioni SaaS, identificando pattern di accesso che potrebbero indicare che un attaccante sta esplorando l'ambiente per identificare dati di valore o stabilire persistenza aggiuntiva.

Strategie di implementazione e best practice

Valutazione dell'ecosistema e identificazione dei rischi

Prima di implementare qualsiasi soluzione SSPM è essenziale condurre un audit completo dell'ecosistema SaaS esistente che tenga conto del panorama delle minacce specifiche per SaaS. Questa valutazione deve includere un'analisi approfondita delle

configurazioni di sicurezza attuali, dei flussi di dati tra applicazioni, degli utenti e dei loro livelli di accesso e una valutazione specifica dei rischi associati alle minacce avanzate come hijacking di token OAuth e le minacce interne.

L'audit dovrebbe anche includere una mappatura completa di tutte le applicazioni di terze parti connesse, identificando potenziali vettori di attacco non autorizzati e valutando il rischio associato a ogni integrazione. Questa analisi fornirà la base per sviluppare una strategia di implementazione che tenga conto delle specificità dell'organizzazione e del suo profilo di rischio specifico.

Implementazione di controlli Zero Trust per SaaS

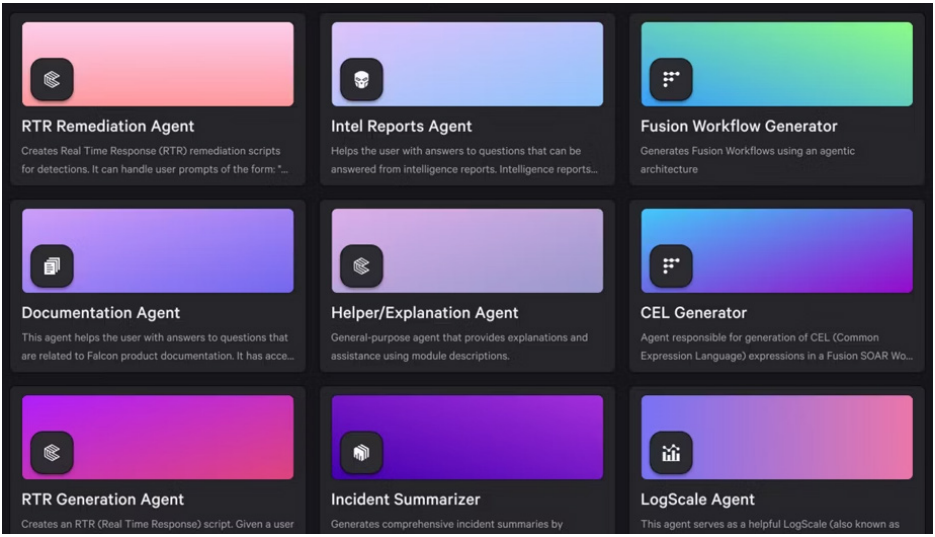
L'adozione crescente di architetture Zero Trust richiede soluzioni SSPM sempre più sofisticate per supportare la verifica continua delle identità, il controllo granulare degli accessi e il monitoraggio in tempo reale delle attività. L'implementazione di principi Zero Trust nell'ambiente SaaS richiede un approccio che vada oltre la semplice autenticazione iniziale per includere la valutazione continua del rischio e l'adattamento dinamico dei controlli di accesso.

La soluzione SSPM deve essere configurata per implementare controlli di accesso condizionale basati su fattori di rischio multipli, inclusi il comportamento dell'utente, la posizione geografica, il tipo di dispositivo utilizzato e il livello di sensibilità dei dati a cui si sta tentando di accedere.

Il futuro della sicurezza SaaS: innovazioni e tendenze

Intelligenza Artificiale per la prevenzione proattiva

L'integrazione di tecnologie di Intelligenza Artificiale e Machine Learning nelle soluzioni SSPM rappresenta una delle metodologie più efficaci per contrastare le minacce avanzate. Queste tecnologie permettono il rilevamento proattivo di pattern di attacco sofisticati, inclusi tentativi di hijacking di token OAuth, movimenti laterali tra applicazioni e comportamenti anomali che potrebbero indicare minacce interne.



L'analisi comportamentale avanzata utilizza tecniche di deep learning per comprendere i pattern complessi di utilizzo normale delle applicazioni e identificare deviazioni sottili che potrebbero indicare attività malevole. Questa capacità è particolarmente importante per identificare attacchi avanzati persistenti che utilizzano tecniche di evasione sofisticate.

Automazione della risposta alle minacce

Il futuro delle soluzioni SSPM include capacità sempre più avanzate di risposta automatizzata alle minacce, permettendo di bloccare automaticamente account compromessi, revocare token OAuth sospetti e implementare controlli di accesso aggiuntivi quando vengono rilevate attività anomale.

Questa automazione sarà particolarmente critica per contrastare attacchi che si muovono rapidamente attraverso l'ecosistema SaaS, dove la velocità di risposta può fare la differenza tra un incidente contenuto e una violazione di dati su larga scala.

Conclusioni: verso un ecosistema SaaS sicuro e resiliente

La sicurezza delle applicazioni cloud rappresenta una delle sfide più complesse che le organizzazioni moderne devono affrontare, particolarmente considerando l'evoluzione del panorama delle minacce e la sofisticazione crescente degli attaccanti che prendono di mira specificamente gli ambienti SaaS. Le soluzioni SSPM rappresentano non solo il futuro della sicurezza SaaS, ma una necessità immediata per mantenere una postura di sicurezza robusta ed efficace contro minacce avanzate.

L'adozione di una strategia SSPM efficace richiede un cambiamento culturale profondo che deve coinvolgere tutti i livelli dell'organizzazione, dalla leadership esecutiva che deve comprendere i rischi specifici del SaaS, ai team operativi che devono implementare e mantenere i controlli di sicurezza appropriati.

Le organizzazioni che investiranno proattivamente in soluzioni SSPM avanzate saranno significativamente meglio posizionate per affrontare le sfide di sicurezza del futuro digitale, inclusa la capacità di rilevare e rispondere a minacce sofisticate come il hijacking di token OAuth, le minacce interne e i movimenti laterali tra applicazioni SaaS.

La chiave del successo risiede nell'implementazione di una strategia olistica che combini tecnologie avanzate, processi ottimizzati e personale adeguatamente formato per riconoscere e rispondere alle minacce specifiche del SaaS. Solo attraverso questo approccio integrato le organizzazioni potranno garantire la sicurezza del loro ecosistema SaaS in continua evoluzione, proteggendo efficacemente i loro asset più preziosi contro avversari sempre più sofisticati.

L'investimento nella sicurezza SaaS dovrebbe essere visto come un investimento strategico che abilita la trasformazione digitale sicura e sostenibile, permettendo alle organizzazioni di sfruttare appieno i benefici del cloud computing mantenendo i più alti standard di sicurezza e conformità, anche di fronte alle minacce più avanzate del panorama attuale.

Analisi degli incidenti Cyber nel settore culturale italiano tra il 2020 e il 2024

(A cura di Joram Marino e Federica Vennitti)

Scenario di riferimento

Il concetto di patrimonio culturale ha subito una significativa evoluzione nel tempo, passando da una visione circoscritta ai "beni fisici" a una più estesa e inclusiva. Con l'emanazione del Codice dei Beni Culturali e del Paesaggio (D.Lgs. 42/2004), il concetto si è ampliato, includendo beni paesaggistici e riconoscendo l'interesse artistico, storico, archeologico, antropologico, archivistico e bibliografico.

La Convenzione di Faro (2005) ha ulteriormente allargato questa prospettiva, definendo il patrimonio culturale come un insieme di risorse ereditate dal passato che alcune persone identificano come riflesso ed espressione dei valori, delle credenze, delle conoscenze e delle tradizioni, trasformandosi in una costruzione culturale dinamica e relazionale.

Il patrimonio culturale italiano così definito affronta una crisi cyber sistemica. L'analisi 2020-2024 documenta l'evoluzione delle minacce digitali in un settore che coinvolge un ecosistema complesso di oltre 13.000 istituzioni: 101 Archivi di Stato con 143.680 utenti annui, 8.131 biblioteche pubbliche che servono 5,7 milioni di residenti, oltre 4.500 musei e istituzioni similari con 40,7 milioni di visitatori negli istituti statali autonomi, e una rete universitaria con 359.000 studenti nei corsi di area culturale. A questi si aggiungono il Ministero della Cultura con le sue Direzioni Generali e Istituti Centrali (ICCD, ICPAL, ICR), le Biblioteche nazionali che conservano per deposito legale l'intera produzione editoriale italiana, le fondazioni culturali private e tutti i fornitori di servizi che operano in sinergia con queste e altre realtà culturali.

La digitalizzazione massiva del patrimonio, accelerata dalla pandemia 2020-2021, ha aumentato l'esposizione agli attacchi informatici perché il trasferimento dall'analogico al digitale ha moltiplicato le vulnerabilità in modo significativo: i sistemi obsoleti aumentano l'esposizione agli attacchi, soprattutto ransomware; il patrimonio *born digital*, privo di backup analogico, è esposto a perdite irreversibili; l'infrastruttura digitale frammentata delle biblioteche accademiche facilita il data scraping massivo da parte di sistemi di Intelligenza Artificiale, con impatti diretti sulle prestazioni e sul monitoraggio.

Questa fragilità organizzativa si riflette nei dati: nel 2024 l'Italia ha subito 357 incidenti cyber gravi e, pur rappresentando lo 0,7% della popolazione mondiale, ha registrato il 10,1% degli attacchi globali. Al di là delle singole percentuali, che vedono il ransomware come una delle minacce predominanti, è l'impatto qualitativo di questi attacchi a definire la gravità dello scenario.
Un esempio emblematico è rappresentato dall'attacco ransomware che ha colpito i sistemi della Regione Lazio nell'agosto del 2021. Questo incidente non è stato un semplice data breach, ma ha paralizzato un'infrastruttura pubblica critica nel pieno di un'emergenza sanitaria, bloccando servizi essenziali per i cittadini come la prenotazione dei vaccini. L'evento ha messo a nudo la vulnerabilità sistemica delle nostre istituzioni e ha dimostrato come un attacco cyber possa minacciare direttamente la continuità dei servizi pubblici e la sicurezza dei dati sensibili di milioni di persone.

L'implementazione della Direttiva NIS2 (D.Lgs. 138/2024), che coinvolgerà circa 1.200-1.500 istituzioni culturali[1], rappresentanti il 70% del patrimonio digitalizzato nazionale, potrebbe offrire un'opportunità irripetibile per elevare la maturità cyber del settore attraverso requisiti stringenti di governance, risk management e resilienza operativa.

La digitalizzazione del patrimonio culturale: accelerazioni e limiti

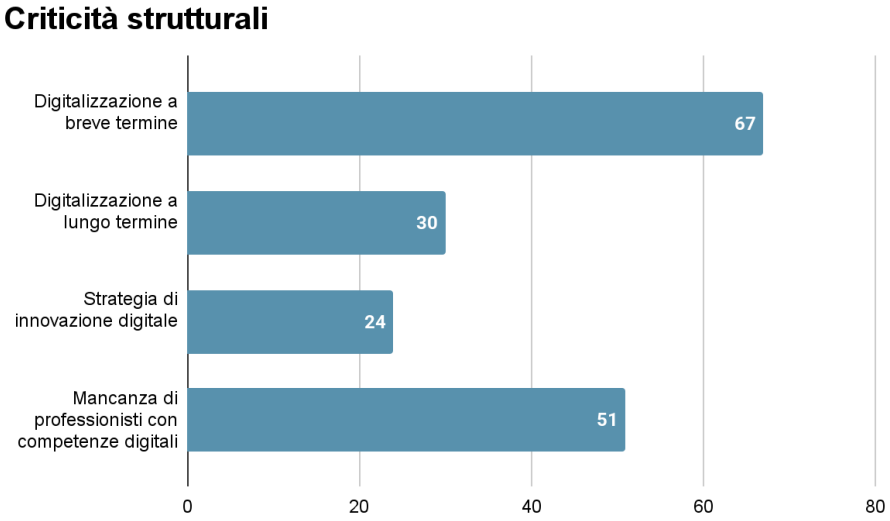
La pandemia ha accelerato i processi di digitalizzazione del patrimonio culturale italiano, evidenziando limiti e potenzialità del rapporto, ad esempio, tra musei e digitale. Dal 57,4% di istituti che dichiaravano di utilizzare il digitale nel 2019 (secondo l'indagine Istat), il settore ha ricevuto una grande spinta verso la comunicazione e la fruizione digitale. Tuttavia, questa produzione digitale spesso non è stata accompagnata da una strategia apposita o da adeguati investimenti a medio e lungo termine, con una conseguente gestione talvolta approssimativa delle tecnologie digitali che mette in luce diverse criticità strutturali[2]:

- il 67% dei musei pianifica attività di digitalizzazione a breve termine;
- il 30% ha una visione a lungo termine;

[1] La stima numerica delle istituzioni coinvolte (1.200-1.500 soggetti / 70% del patrimonio digitalizzato) è basata sul Piano Nazionale di Digitalizzazione del Ministero della Cultura che trova riscontro sulle rilevazioni empiriche non ufficiali in quanto l'elenco stilato dall'ACN con i nomi delle singole organizzazioni (circa 20.000 soggetti totali, di cui abbiamo stimato un 6-8% di istituzioni culturali) è riservato e l'inserimento viene notificato solo individualmente all'organizzazione.

[2] Senza considerare che l'82% delle strutture dipende da fornitori esterni per la digitalizzazione, con tutte le conseguenze che analizzeremo in seguito nel paragrafo relativo agli attacchi alla Catena di approvvigionamento.

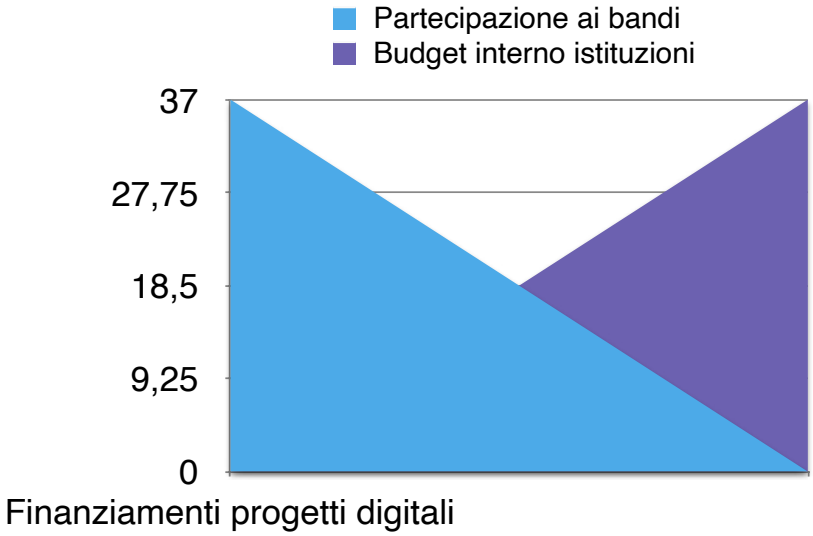
- il 24% dei musei possiede una strategia di innovazione digitale;
- Il 51% non si avvale di professionisti con competenze digitali.



L'analisi dell'indagine pilota sui musei italiani (2020-2021) conferma criticità sistemiche.

Indicatore	%	Implicazioni
Pianificazione digitalizzazione breve termine	67%	Approccio emergenziale, mancanza visione strategica
Visione a lungo termine	30%	Limitata capacità di pianificazione strutturale
Strategia innovazione digitale	24%	Assenza di governance digitale nella maggioranza dei musei
Mancanza professionisti digitali	51%	Deficit competenze critiche per la trasformazione digitale
Ricorso a soggetti esterni per digitalizzazione	82%	Dipendenza sistemica da fornitori terzi

Sono infine rilevate alcune criticità finanziarie in quanto i progetti di digitalizzazione risultano, secondo le rilevazioni disponibili[3], finanziati per il 37% dal budget interno all'istituzione e per un altro 37% dalla partecipazione a bandi, confermando la difficoltà a reperire finanziamenti costanti e aumentando la dipendenza da risorse esterne che potrebbero ostacolare la sostenibilità a lungo termine degli investimenti in sicurezza[4].



Minacce e vulnerabilità del patrimonio culturale digitale

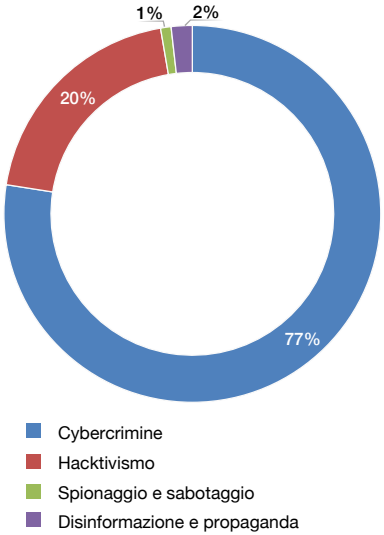
Prendendo a modello l'evoluzione generale degli incidenti cyber nel quinquennio in esame, possiamo delineare, con buona approssimazione, la situazione del settore culturale, in attesa di poter analizzare i dati che sta raccogliendo l'ACN in merito all'anno in corso.

[3] Affidabilità stimata con il 10% di scarto, secondo una valutazione per verosimiglianza con paesi come il Giappone e Israele che rilasciano alcune indicazioni sulla materia.

[4] Visto il breve lasso di tempo preso in esame, le previsioni sul medio periodo vanno considerate speculative, sebbene fondate sull'esperienza pregressa.

Distribuzione degli attaccanti

Come indicato nel grafico seguente, il cybercrimine rappresenta la motivazione principale degli attaccanti, soprattutto a causa del basso costo di entrata e di un altissimo danno potenziale.



- Cybercrimine: 86% a livello globale, circa 77% in Italia.
- Hacktivismo: 22% in Italia - Eventi prevalentemente di matrice geopolitica correlati ai conflitti in essere.
- Spionaggio e Sabotaggio: <1% - Presenza marginale ma potenzialmente sottostimata.
- Information Warfare: 2% globale - Operazioni in crescita, quasi raddoppiate rispetto al 2023.

Vulnerabilità del patrimonio culturale digitale

Partendo dalle informazioni disponibili, si è cercato di costruire un quadro della distribuzione degli Attacchi per Tipologia e Settore nel 2024.

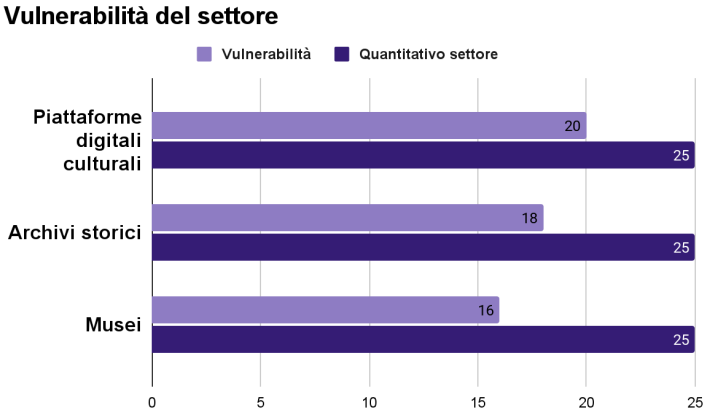
I settori risultati più **vulnerabili** sono stati (Ranking 2024):

1. Piattaforme Digitali Culturali (20/25) - Massima superficie di attacco
2. Archivi Storici (18/25) - Dati irreplicabili, bassa resilienza
3. Musei (16/25) - Sistemi ibridi legacy/moderni

Legenda:

●●●●● = Critico ●●●●○ = Alto ●●●○○ = Medio ●●○○○ = Basso ●○○○○ = Minimo

Settore	Ransomware	Data Scraping	DDoS	Phishing	Data Breach	Defacement
Musei	●●●○○	●●○○○	●●●●○	●●●○○	●●○○○	●●●●●
Biblioteche	●●○○○	●●●●●	●●○○○	●●○○○	●●●○○	●●○○○
Archivi Storici	●●●●●	●●●○○	●●○○○	●●●○○	●●●●○	●○○○○
Siti Archeologici	●●○○○	●○○○○	●●●●●	●●○○○	●○○○○	●●●●●
Piattaforme Digitali	●●●○○	●●●●●	●●●●●	●●●●●	●●●●○	●●●○○



Infrastrutture digitali e vulnerabilità sistemiche: l'esempio delle biblioteche

Nelle biblioteche accademiche italiane, l'infrastruttura digitale è spesso frammentata. Il personale IT è sottodimensionato o, in molti casi, esternalizzato tramite convenzioni. A ciò si aggiunge una scarsa consapevolezza della necessità di proteggere a dovere i sistemi digitali.

Questa fragilità espone i cataloghi OPAC (On-line public access catalog) a data scraping massivo. I dati (metadati bibliografici) vengono estratti dalle aziende di Intelligenza Artificiale per addestrare modelli linguistici sempre più vasti.
Questo fenomeno è descritto come una forma di "colonialismo digitale", ovvero l'estrazione di valore dai cataloghi senza alcun ritorno per le istituzioni proprietarie che li hanno costruiti. L'estrazione non autorizzata di dati risulta particolarmente impattante sulla qualità del servizio erogato.

Vulnerabilità apprese studiando il patrimonio *born* digital

Il patrimonio culturale nativo digitale (*born digital*), privo quindi di equivalente analogico, rappresenta lo scenario più esposto. Studiarne le criticità peculiari fornisce una chiave di lettura per identificare con maggiore accuratezza i rischi dell'intero patrimonio culturale digitalizzato:

- assenza dell'originale analogico (backup fisico): la perdita può essere inestimabile poiché il contenuto digitale potrebbe essere l'unica traccia disponibile. Le operazioni di digitalizzazione sono spesso non ripetibili e, se l'oggetto analogico non esiste più, la perdita è definitiva. Anche la preservazione di oggetti complessi come gli archivi email è problematica;
- obsolescenza tecnologica: gli oggetti digitali soffrono dell'obsolescenza dei formati, del software che deve leggerli e dell'hardware. Il rischio di obsolescenza è uno dei maggiori pericoli identificati per la conservazione. La difficoltà di mantenere i sistemi legacy o i sistemi operativi non aggiornati rende l'intera rete vulnerabile;
- fragilità estrema: un attacco ransomware può criptare le informazioni rendendole irrecuperabili. I guasti richiedono sistemi di business continuity e disaster recovery. La possibilità che l'organizzazione culturale vada fuori business per mancanza di risorse finanziarie è un rischio grave;
- complessità relazionale e metadati: l'autenticità e la preservazione del patrimonio digitale richiedono di tracciare la provenienza e di salvare il contesto. È cruciale preservare la parte fisica, logica e concettuale dell'oggetto digitale e documentare tutti i processi (come lo strumento, il sensore e il software utilizzati per la digitalizzazione);
- frammentazione archiviale: se un archivio è disperso su sistemi frammentati (come i silos amministrativi), si presta maggiormente alla manipolazione. Ad esempio, l'infrastruttura digitale frammentata nelle biblioteche accademiche italiane, dove l'integrazione di pezzi vecchi e nuovi non sempre funziona, ne aumenta la vulnerabilità;

- autenticità difficile da verificare: la migrazione da un formato all'altro crea un file diverso e colpisce l'autenticità. Quando il documento nasce digitale, la verifica dell'originalità e dell'autenticità possono essere difficoltose;
- manipolazione invisibile: modifiche minime ai documenti digitali possono risultare impercettibili ai sistemi di verifica tradizionali, compromettendo l'integrità del patrimonio senza essere rilevate. Questo rischio include sia alterazioni sottili dei contenuti esistenti sia l'inserimento di dati falsi (fake data o data poisoning) che possono minare l'affidabilità dell'intera collezione.

Minacce emergenti specifiche del settore

Intelligenza Artificiale e manipolazione del patrimonio

L'impiego dell'IA generativa nel cybercrimine rende necessarie nuove competenze difensive.

Deep Fake su immagini e video patrimonio storico

- Creazione di contenuti totalmente artificiali indistinguibili dagli originali
- Simulazione di persone defunte o recupero di voci storiche
- Rilevamento delle contraffazioni (debunking) estremamente complesso
- Necessità di strumenti avanzati per verificare l'autenticità

Ricostruzione 3D e alterazione

- Tecnologie di ricostruzione 3D da immagini ad alta risoluzione
- Possibilità di alterazione minima e invisibile
- Rischio per l'autenticità della documentazione storica

Data Scraping avanzato e colonialismo digitale Tecniche avanzate

- Scraping per alimentazione modelli IA/LLM
- Algoritmi di machine learning per profilazione completa
- Elusione anti-bot adattiva
- Aggregazione multi-fonte per attacchi mirati

Caratteristiche dell'attacco

- Bot simulano un utilizzo standard per eludere il rilevamento
- Richieste con pattern di complessità non compatibili con l'utilizzo umano standard
- Attacco dissimulato come traffico legittimo
- Estrazione sistematica con aggravio sulle strutture dell'istituzione e senza ritorno economico o copertura delle spese vive.

Attacchi steganografici al patrimonio digitalizzato con tecniche di persistenza

- Steganografia per nascondere payload malevoli
- Minacce persistenti avanzate (APT) con durata di mesi/anni
- Manipolazione per minare la fiducia nel repository
- Alterazione minima non rilevata dai sistemi di verifica

Vulnerabilità dei controlli

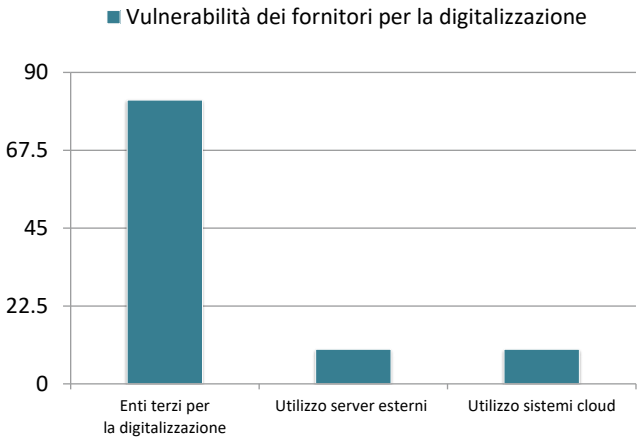
- Funzioni hash tradizionali (MD5) superate
- Possibilità di generare file con lo stesso hash ma con contenuto differente
- Inefficacia dei controlli di integrità su volumi massivi
- Necessità di sistemi basati su IA per il rilevamento

Attacchi alla catena di approvvigionamento nel settore culturale

Gli attacchi alla catena di approvvigionamento rappresentano una minaccia crescente, tanto che Gartner prevede che il 45% delle organizzazioni subirà attacchi sfruttando le vulnerabilità dei propri fornitori.

Criticità identificate per il settore

- 82% delle istituzioni ricorre a terzi per la digitalizzazione
- 10% dei musei usa server esterni, 10% sistemi cloud
- Dipendenza da Managed Service Provider (MSP)
- Piattaforme basate su standard proprietari obsoleti



Scenario "Attacco a Cascata": il caso Collins Aerospace (settembre 2025) offre spunti interessanti. La compromissione del software MUSE ha paralizzato tre dei principali aeroporti europei in meno di 24 ore:

- 29 voli cancellati
- Migliaia di passeggeri bloccati
- Interruzione completa dei sistemi elettronici
- Effetti a cascata sulle connessioni internazionali e sulla gestione del personale

Rischi comparabili nel patrimonio culturale: una rapida analisi di mercato rivela che, con buona approssimazione, tre vendor controllano l'80% dei sistemi di gestione delle collezioni italiane. Una compromissione in questo ambito potrebbe:

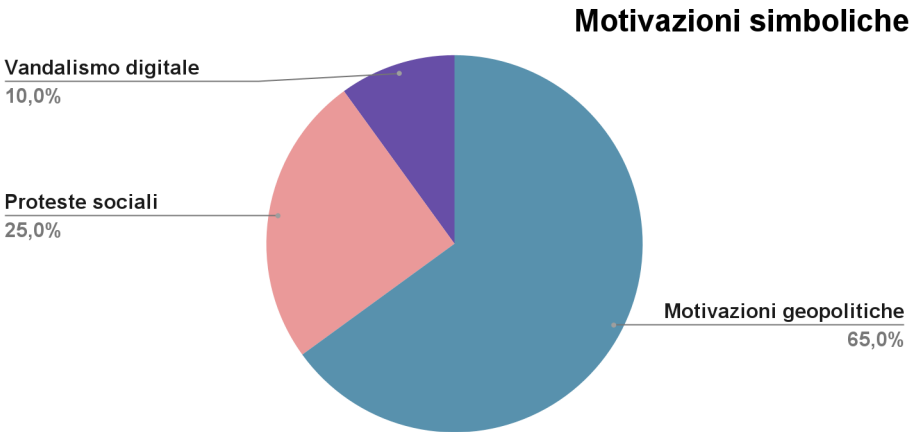
- Impattare simultaneamente centinaia di istituzioni
- Compromettere l'accesso ai cataloghi online
- Bloccare i sistemi di biglietteria
- Paralizzare le piattaforme di conservazione digitale
- Generare impatti superiori ai 5 milioni di euro nei primi tre giorni
- Mettere offline oltre 500 istituzioni

Hacktivismo culturalmente motivato

Il settore culturale, custode dell'identità nazionale, è sempre più coinvolto in dinamiche di conflitto digitale:

Distribuzione delle motivazioni

- Motivazioni geopolitiche: 65%
- Proteste sociali: 25%
- Vandalismo digitale: 10%



Caratteristiche operative

- L'hacktivismo è la seconda motivazione di attacco in Italia (22% nel 2024)
- Gli eventi sono prevalentemente di matrice geopolitica
- Colpiscono istituzioni di primo livello per avere visibilità
- Di recente si sono registrati defacement per manifestazioni filorusse o filopalestinesi
- Obiettivo: manipolazione o distruzione dell'eredità culturale

Analisi degli attacchi: casi di studio e insegnamenti

Di seguito vengono riportati alcuni attacchi informatici che hanno avuto impatto sul patrimonio culturale o su enti pubblici. La validità degli esempi ai fini dell'analisi successiva rimane invariata anche se la mancanza di dati sistematici impedisce una classificazione *severity* standardizzata[5].

Eventi emblematici nel settore culturale e pubblico

British Library - Ottobre 2023: attacco ransomware ad alto impatto

La British Library ha subito un significativo attacco cyber di tipo ransomware nell'ottobre 2023[6], rivendicato dal gruppo Rhysida. L'incidente, definito dalle autorità britanniche come di gravità critica[7], rappresenta un caso paradigmatico per comprendere le vulnerabilità del settore.

Impatto tecnico

- Compromissione della maggior parte dei sistemi online
- 600GB di file copiati ed esfiltrati illegalmente, inclusi dati personali di utenti e staff
- Blocco dei servizi e del catalogo per oltre 11 settimane (circa 4 mesi di interruzione operativa)
- Servizi colpiti: catalogo online, sistemi di catalogazione, accesso alle collezioni, prestito interbibliotecario

---

[5] La classificazione degli incidenti per severity seguirà gli standard del Rapporto una volta disponibili i dati sistematici delle notifiche obbligatorie previste dalla Direttiva NIS2. L'attuale analisi si basa su informazioni parziali da fonti pubbliche.

[6] Il rapporto ufficiale si trova in https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

[7] In questa dichiarazione dell'aprile 2025, l'ICO, autorità britannica per la protezione dei dati, elogia la trasparenza della British Library e sottolinea la causa scatenante dell'incidente: la mancanza di autenticazione a più fattori (MFA) su un account amministrativo.
Pur decidendo di non avviare un'indagine formale, l'ICO fornisce indicazioni chiare sulla necessità di adottare misure di sicurezza adeguate al link: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/04/statement-on-british-library-s-2023-ransomware-attack/

Dinamiche dell'attacco

- Gli aggressori hanno prima esfiltrato i dati
- Quando è stato chiaro che non sarebbe stato pagato alcun riscatto, i dati sono stati messi all'asta e successivamente pubblicati sul dark web
- Il danno più significativo è stato causato dalla distruzione dei server operata dagli attaccanti per inibire il recupero dei sistemi

Fattori aggravanti

- Infrastruttura legacy con numerosi sistemi obsoleti
- Rete complessa e datata che ha contribuito alla gravità dell'impatto
- Necessità di eliminare fisicamente le macchine non bonificabili perché troppo datate
- Ricostruzione dell'intera infrastruttura tecnologica quasi da zero

Lezione appresa

L'investimento nella prevenzione, pur significativo, è giustificato dalle conseguenze devastanti derivanti dall'assenza di un'adeguata protezione: perdita irreversibile di patrimonio digitale, interruzioni operative prolungate e costi di ripristino enormemente superiori agli investimenti preventivi. L'obiettivo di fondo per le istituzioni è di garantire che il patrimonio, gran parte del quale è solo digitale, sia protetto da attacchi sempre più sofisticati e distruttivi.

Regione Lazio - Agosto 2021: attacco Ransomware[8]

Si tratta di uno degli incidenti più significativi avvenuti in Italia nel 2021 e di un esempio emblematico di attacco a un'infrastruttura critica della Pubblica Amministrazione. L'attacco è stato perpetrato sfruttando le credenziali di un dipendente che lavorava in smart working in un momento storico in cui non si erano ancora affermate delle pratiche di sicurezza adeguate, evidenziando per la prima volta, in Italia, il rischio associato al "fattore umano" e alla sicurezza degli accessi remoti.

L'attacco ha avuto un fortissimo impatto locale, paralizzando il Centro Elaborazione Dati (CED) della Regione, mandando offline il portale regionale e, soprattutto, il sistema di prenotazione dei vaccini anti-COVID-19, in un momento critico della campagna vaccinale.

[8] La fonte primaria è la comunicazione ufficiale della Regione Lazio, ai sensi del GDPR, raggiungibile al link: https://www.regione.lazio.it/notizie/attacco-hacker

Non è mancata l'esfiltrazione dei dati sensibili, inclusi quelli sanitari dei cittadini e, per settimane, molti servizi sono rimasti bloccati o hanno funzionato a regime ridotto, con un impatto significativo sull'amministrazione e sui cittadini[9].
Questo attacco è rilevante perché ha dimostrato la vulnerabilità degli enti pubblici che gestiscono dati sensibili e servizi essenziali, interrompendo un servizio sanitario fondamentale come le prenotazioni vaccinali e mostrando quanto un attacco cyber possa avere conseguenze dirette sulla vita dei cittadini.

L'incidente sottolinea l'importanza critica della formazione del personale: la consapevolezza sulla sicurezza informatica deve diventare parte integrante dei percorsi di formazione continua e di sviluppo professionale per ogni dipendente.

Miles33 - Agosto 2024: attacco alla Supply Chain del settore editoriale

Questo è un esempio estremamente pertinente[10] per illustrare come si possano bloccare centinaia di siti web, applicazioni, applicazioni e servizi online attraverso un singolo attacco a un fornitore di servizi. Nel caso in oggetto si tratta di Miles33, un'azienda che fornisce un CMS in cloud e altri servizi digitali a centinaia di testate giornalistiche.

L'attacco è stato rivendicato dal gruppo "Alpha Team", che ha dichiarato di aver sottratto dati da 77 aziende (62 vittime note in Italia di cui 59 nel settore News/Multimedia) e di aver rubato 5 milioni di righe contenenti i dati personali (email, password, date di nascita).

L'incidente evidenzia come, colpendo un singolo fornitore, sia possibile danneggiare un intero ecosistema di aziende clienti. Dimostra inoltre la fragilità del settore dell'informazione, dove molti operatori si affidano agli stessi fornitori tecnologici: l'incidenza delle vittime italiane sul totale globale del settore è del 38%.

---

[9] Le ricostruzioni tecniche sono disponibili nei provvedimenti contro la Regione Lazio emessi dal garante per la protezione dei dati personali ed in particolare:

a. Ordinanza ingiunzione nei confronti di Regione Lazio - 28 marzo 2024
Ricostruisce l'incidente, evidenzia le numerose violazioni della normativa privacy (GDPR) e le inadeguate misure di sicurezza https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9999027

b. Provvedimento contro LAZIOcrea S.p.A. (la società IT della Regione)
Specifica le responsabilità del fornitore di servizi IT della Regione, LAZIOcrea, sanzionandola per le carenze tecniche che hanno contribuito al successo dell'attacco. Questo documento è utile per approfondire gli aspetti legati alla responsabilità della catena di fornitura (supply chain) nel settore pubblico https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9998991

[10] Vale la pena approfondire l'evento su https://s-mart.biz/attacco-informatico-nei-confronti-di-miles33

Lezioni strategiche

L'attacco dimostra come una tecnologia informatica utilizzata in modo prevalente in un settore specifico possa diventare un *single point of failure*.
Quando una tecnologia è nota per essere ampiamente adottata e presenta criticità di sicurezza, diventa un target ad alto valore strategico: i criminali informatici possono generare, con una sola campagna, un numero ingente di danni, fino a mettere in crisi un intero settore.

Internet Archive - 2024: attacchi multipli e sistematici

L'Internet Archive, una delle principali piattaforme per la conservazione digitale, è stato colpito ripetutamente nel corso del 2024[11], dal mese di maggio sino ad ottobre[12], quando si è consumato l'attacco di massimo impatto secondo la classificazione interna.

Il fondatore ha dichiarato che questo trend indica un cambio di paradigma nelle minacce cyber e i fatti confermano l'affermazione: poiché gli attacchi sono stati sostenuti e mirati, è stato necessario chiudere temporaneamente l'accesso per lavorare al ripristino del registro.

Gli eventi hanno evidenziato diverse vulnerabilità delle grandi piattaforme di conservazione digitale[13]: nonostante l'uso di tecnologie come Filecoin (basato su IPFS), che dimostra ampia consapevolezza dei rischi e grande impegno nel trovare soluzioni innovative per proteggere i dati a lungo termine, l'Internet Archive è stato comunque colpito.

Parliamo di tecnologie per l'archiviazione decentralizzata o distribuita: a differenza di un server tradizionale (dove i dati sono in un unico luogo), un sistema distribuito salva frammenti di dati su molti computer diversi in una rete. Questo approccio è stato progettato proprio per aumentare la resilienza: se un computer (o "nodo") va offline, i dati rimangono accessibili tramite gli altri.

---

[11] La ricostruzione si basa sulla fonte più diretta e autorevole: la pubblicazione, da parte del fondatore Brewster Kahle, e dello staff, di aggiornamenti costanti durante la crisi, spiegando la natura degli attacchi (DDoS, defacement, data breach) e le azioni intraprese per il ripristino.

[12] The Verge fornisce un'ottima sintesi dell'intera vicenda, dall'inizio della crisi fino agli aggiornamenti sul ripristino, rendendo la cronologia degli eventi chiara e accessibile. L'articolo *The Internet Archive is still down but will return in 'days, not weeks'* è raggiungibile al link: https://www.theverge.com/2024/10/11/24269558/internet-archive-down-outage-cyberattack-data-breach-update

[13] È possibile leggere un approfondimento da una testata specializzata, corredata da interazioni con informatori che hanno ottenuto il database e un'analisi tecnica precisa collegandosi al link: https://www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/

Un'architettura decentralizzata, che in teoria dovrebbe essere più robusta, non ha impedito agli attaccanti di raggiungere l'obiettivo: ciò suggerisce che le vulnerabilità non risiedevano solo nel modo in cui i dati erano archiviati, ma anche in altri punti dell'architettura complessiva (ad esempio, negli applicativi, nei sistemi di accesso, nella gestione delle credenziali o in altri componenti centralizzati necessari per far funzionare il servizio).
L'incidente evidenzia come, anche adottando tecnologie all'avanguardia pensate per la sicurezza, come i sistemi distribuiti, le organizzazioni culturali rimangano esposte a vulnerabilità sistemiche che possono essere sfruttate da attacchi sofisticati, mirati e persistenti.

My Jewish Italy - Novembre 2020: "Zoombombing" culturale

Il 18 novembre 2020[14], durante la presentazione online della nuova app "My Jewish Italy", si è verificato un grave attacco di tipo "zoombombing" che rappresenta il primo caso documentato in Italia di hacktivismo motivato dall'odio verso una cultura specifica. L'app, ideata dall'Unione delle Comunità Ebraiche Italiane (UCEI) per promuovere la conoscenza del patrimonio culturale ebraico in Italia, era al centro di una conferenza pubblica sulla piattaforma Zoom.

Dinamica dell'attacco

Un gruppo di aggressori si è introdotto nella videoconferenza pubblica, interrompendo bruscamente i relatori. Hanno proiettato sugli schermi dei partecipanti immagini offensive, tra cui svastiche e inneggiamenti ad Adolf Hitler e ad Al Qaeda[15]. L'attacco è stato accompagnato da scritte minacciose, con cui gli aggressori si vantavano di aver violato i sistemi e di essere entrati in possesso dei dati personali dei partecipanti, incluse le loro carte di credito. Sebbene queste minacce fossero probabilmente false, l'obiettivo era chiaramente quello di generare panico tra i presenti.

L'incidente è classificabile come un attacco cyber di matrice antisemita. Non si è trattato di un semplice disturbo, ma di un'azione coordinata e premeditata con il chiaro intento di intimidire, offendere e diffondere odio. La duplice simbologia utilizzata

[14] Mosaico (Bollettino della Comunità Ebraica di Milano), "My Jewish Italy: la presentazione sotto attacco hacker", https://www.mosaico-cem.it/attualita-e-news/italia/my-jewish-italy-la-presentazione-sotto-attacco-hacker/

[15] Shalom (Mensile della Comunità Ebraica di Roma), "Incursione antisemita alla presentazione della app My Jewish Italy", https://www.shalom.it/blog/news-in-italia-e-nel-mondo/incursione-antisemita-alla-presentazione-della-app-my-jewish-italy-b1064899

(nazista e jihadista) evidenzia la convergenza di diverse matrici estremiste nell'odio antisemita[16].

Effetti e ripercussioni

Impatto Culturale e Sociale: L'attacco non ha causato un danno tecnico permanente ma un gravissimo danno simbolico e morale. Ha violato uno spazio virtuale dedicato alla promozione culturale, trasformandolo in un veicolo di odio e di paura.

Vulnerabilità delle Piattaforme Digitali: L'accaduto ha messo in luce la vulnerabilità delle piattaforme di comunicazione digitale, diventate onnipresenti durante la pandemia. Ha dimostrato come iniziative pubbliche online, al pari delle loro controparti in presenza, se non adeguatamente protette, possano essere facilmente prese di mira da gruppi organizzati per compiere raid d'odio.

Sottovalutazione del Rischio: L'incidente ha evidenziato come le istituzioni culturali, anche nel passaggio al digitale, debbano considerare non solo i rischi di data breach, ma anche quelli legati a manifestazioni di odio e a interruzioni violente delle proprie attività online. Ha sottolineato la necessità di protocolli specifici per gli eventi online del settore culturale, inclusa l'implementazione di sale d'attesa virtuali, di sistemi di autenticazione dei partecipanti e di moderazione attiva.

Museo di Storia Naturale di Berlino - Ottobre 2023

Per completezza bisogna ricordare anche l'attacco al Museo di Storia Naturale di Berlino (Museum für Naturkunde Berlin) che ha gestito la comunicazione dell'incidente in modo trasparente e diretto attraverso il proprio sito ufficiale[17].

Distribuzione ed evoluzione 2020-2024

La distribuzione delle tecniche di attacco nel settore culturale mostra pattern evolutivi significativi.

Ransomware e Malware (38% degli incidenti nel 2024)

- Sono tornati ad essere la tecnica predominante in Italia
- Crescita del 30% tra il 2023 e il 2024 in Italia
- Basso costo di entrata: codici ransomware acquistabili per pochi soldi nel mercato nero

[16] Patria Indipendente (Rivista dell'ANPI), "Se sul web il raid nazifascista diviene seriale", https://www.patriaindipendente.it/persone-e-luoghi/inchieste/se-sul-web-il-raid-nazifascista-diviene-seriale/

[17] https://www.museumfuernaturkunde.berlin/en/current-information-cyber-attack-museum-fur-naturkunde-berlin

- Alto rischio e altissimo danno potenziale con capacità di criptare anche i backup, se non opportunamente isolati e se l'attacco viene rilevato tardivamente

DDoS - Distributed Denial of Service (21% in Italia, 8% globale)

- Crescita globale del +36% nel 2024
- In Italia c'è una diminuzione del 36% (da 111 a 76 incidenti)
- Tecnica tipicamente utilizzata dall'hacktivismo
- Pattern stagionale con picchi significativi nei mesi estivi (giugno-luglio)
- Attacchi principalmente dimostrativi con finalità di visibilità mediatica

Vulnerabilità e Zero-Day (19% in Italia, 15% globale)

- Crescita del 90% in Italia (da 7 a 67 incidenti)
- Incremento giustificato dall'attacco al settore News/Multimedia
- Sistemi legacy comuni contribuiscono alla gravità dell'impatto
- Sfruttamento sistematico di vulnerabilità note e sconosciute

Data Scraping avanzato e sottrazione sistematica di dati

- Estrazione automatizzata di metadati bibliografici
- Bot dell'IA progettati per estrarre quantità massicce di dati
- Estrazione non autorizzata con impatto significativo sulla qualità del servizio
- I dati vengono utilizzati per addestrare modelli linguistici (LLM)

Phishing e Social Engineering (11% in Italia, 8% globale)

- Crescita del 35% in Italia nel 2024
- Il fattore umano resta la principale fonte di rischio (80-90% degli attacchi)
- Tecniche sempre più sofisticate grazie all'uso dell'IA generativa

Crimine d'odio e hacktivismo culturale

- Crescita a livello globale di oltre il 50% nel settore Government
- Manovre di defacement prevalentemente filorusse o filopalestinesi
- Finalità dimostrative per ottenere clamore mediatico
- La Polizia Postale contrasta anche i fenomeni di hate speech e furto d'identità

L'impatto della Direttiva NIS2

Il nuovo quadro normativo

La Direttiva NIS2, recepita nell'ordinamento italiano con il Decreto Legislativo 138 del 2024, rappresenta un progresso significativo nella strategia di cybersicurezza europea. L'ampliamento del campo di applicazione coinvolge ora anche le strutture di medie dimensioni e riflette la consapevolezza che le minacce cyber non fanno distinzioni in base alle dimensioni del bersaglio.

Perimetro di applicazione per il patrimonio culturale

Il settore del patrimonio culturale è al centro della strategia di digitalizzazione del Ministero della Cultura che ha identificato i soggetti coinvolti nel PND - Piano Nazionale di Digitalizzazione.

- 1.200-1.500 istituzioni culturali identificate
- 70% del patrimonio digitalizzato nazionale interessato
- 44 musei statali autonomi con gestione bilanci propri
- 101 Archivi di Stato
- 8.131 biblioteche pubbliche e private (79% di natura pubblica)
- Fondazioni culturali (33% del campione museale)
- Parchi archeologici autonomi

Obblighi operativi specifici

La NIS2 introduce requisiti stringenti con implicazioni dirette per il settore culturale.

Governance e Responsabilità

- Responsabilizzazione della direzione e del top management sui temi cyber
- Obbligo di approvazione e supervisione delle misure di sicurezza
- Responsabilità personale dei dirigenti per le violazioni
- Formazione obbligatoria per il management sulla sicurezza informatica

Misure tecniche di sicurezza

- Backup e ripristino: continuity plan obbligatorio con sistemi di disaster recovery e business continuity
- Controllo degli accessi: implementazione di autenticazione multi-fattore (MFA) per account critici
- Segmentazione della rete: prassi obbligatoria per diminuire il «blast radius»[18] in caso di attacco

[18] Metafora mutuata dall'edilizia che indica l'estensione massima del danno che un singolo incidente di sicurezza può causare all'interno di un'organizzazione.

- Monitoraggio Continuo: sistemi di rilevamento di anomalie e minacce in tempo reale
- Gestione Vulnerabilità: aggiornamento sistematico e gestione delle patch

Notifica degli incidenti

- Obbligo di segnalazione al CSIRT Italia (ente operativo dell'ACN)
- Tempistiche definite per la notifica
- Piano di risposta agli incidenti (Incident Response Plan) obbligatorio
- Gestione della comunicazione istituzionale durante una crisi

Sanzioni e responsabilità

- Sanzioni economiche19 fino a 10 milioni di euro o al 2% del fatturato globale annuo
- Responsabilità patrimoniale del dirigente in caso di inosservanza

Rischi reputazionali

- Perdita di credibilità istituzionale
- Distruzione della fiducia (trust) con utenti e stakeholder
- I danni alla reputazione sono considerati tra gli impatti più gravi

Impatti operativi

- Sospensione del servizio in caso di incidente grave
- Costi di conformità e legali in aumento
- Spese impreviste per colmare le lacune di sicurezza

Mappa delle vulnerabilità per tipologia di istituzione

Sulla base dell'esperienza e dello storico degli interventi di consulenza abbiamo stilato un elenco delle vulnerabilità che più frequentemente rileviamo nelle istituzioni culturali. Non abbiamo alcuna pretesa di completezza ma riteniamo l'elenco utile per una valutazione iniziale del rischio.

[19] La stima relativa all'ammontare delle sanzioni è basata sull'esperienza, sulle regolamentazioni pubblicate e sulle indicazioni non ufficiali che si riscontrano ma non sono direttamente supportate dalle statistiche ufficiali in quanto non risultano ancora comminate sanzioni ad alcun soggetto.

Piattaforme digitali culturali (Biblioteche/Archivi online)

Criticità principali

- Infrastrutture digitali frammentate
- Personale IT limitato o esternalizzato
- Scarsa consapevolezza delle problematiche di sicurezza
- Cataloghi OPAC esposti a data scraping massivo

Rischi prioritari

- DDoS in crescita globale (+36%)
- Data scraping «invisibile» da bot IA
- Saturazione della memoria di sistema
- Data Integrity Attack per minare l'affidabilità

Azioni critiche da intraprendere tempestivamente, se non già in essere

- Web Application Firewall (WAF) essenziale
- Protezione DDoS avanzata
- Monitoraggio delle anomalie del traffico dati
- Politiche strutturate di accesso ai dati

Archivi Storici (Collezioni centralizzate)

Criticità principali

- Obsolescenza tecnologica sistemica
- Infrastruttura legacy con criticità operative severe
- Dipendenza da sistemi proprietari datati
- Server con obsolescenza hardware che compromette la stabilità operativa

Rischi prioritari

- Ransomware (38% incidenti 2024)
- Perdita dati per obsolescenza
- Cifratura di backup non isolati
- Impossibilità di recupero per i sistemi datati

Azioni critiche da intraprendere tempestivamente, se non già in essere

- Backup air-gapped obbligatori
- Strategie di conservazione a lungo termine
- Piani di disaster recovery testati
- Migrazione progressiva dai sistemi legacy

Musei

Criticità principali

- Sistemi complessi legacy/moderni
- Catalogazione realizzata con strumenti generici (Word/Excel)
- Archiviazione rischiosa (26% usa hard disk esterni)
- Mancata verifica per dati omogenei e relativa normalizzazione

Rischi prioritari

- Defacement reputazionale
- Hacktivismo per visibilità mediatica
- Compromissione dei sistemi IoT
- Lateral movement tra reti non segmentate

Azioni critiche da intraprendere tempestivamente, se non già in essere

- Segmentazione rete IT/IoT fondamentale
- Incident Response Plan specifico
- Monitoraggio continuo delle anomalie
- Formazione del personale sui rischi specifici

Priorità di investimento e strategia di mitigazione

Sempre basandoci sull'esperienza, abbiamo suddiviso gli investimenti necessari per ottenere il massimo risultato con le risorse disponibili al momento dell'avvio dell'*audit* di sicurezza.

Livello 1 - Budget limitato: resilienza di base (investimento <50k€/anno)

Backup offline isolato (air-gapped)

- Protezione essenziale contro ransomware
- Test periodici di ripristino dei backup
- Rotazione periodica dei supporti
- Documentazione delle procedure di ripristino

Segmentazione base della rete

- Separazione ambienti pubblici/amministrativi
- Isolamento sistemi IoT/OT
- Strategia «Blast Radius»[20]
- VLAN dedicate per i servizi critici

[20] Si intende qui l'insieme delle pratiche di contenimento degli attacchi già indicate in precedenza

SOC condiviso per piccole istituzioni

- Monitoraggio 24/7 condiviso tra enti
- Riduzione dei costi attraverso economie di scala
- Risposta coordinata agli incidenti
- Intelligence condivisa sulle minacce

Livello 2 - Budget medio: intelligence e supervisione della catena di approvvigionamento (50-150k€/anno)

Rilevazione deepfake e manipolazioni

- Strumenti IA per la verifica dell'autenticità
- Sistemi di watermarking digitale
- Blockchain per la certificazione dei contenuti
- Audit trail immutabili

Audit fornitori critici

- Valutazione dei rischi della catena di approvvigionamento
- Certificazioni di sicurezza minime
- Clausole contrattuali specifiche per la cybersicurezza
- Monitoraggio continuo della conformità (compliance)

Sistemi di steganalisi

- Rilevamento payload nascosti
- Analisi dell'integrità dei contenuti multimediali
- Protezione contro il data poisoning
- Monitoraggio delle alterazioni invisibili

Livello 3 - Investimenti strategici: ricerca e sviluppo e rafforzamento delle competenze (>150k€/anno)

Intelligence sulle minacce settoriali

- CTI[21] specifica per il patrimonio culturale
- Feed intelligence real-time
- Analisi predittiva delle minacce
- Collaborazione ISAC culturale

[21] La Cyber Threat Intelligence (CTI) specifica per il patrimonio culturale è il processo di raccolta, analisi e contestualizzazione di informazioni sulle minacce informatiche che prendono di mira specificamente musei, archivi, biblioteche, siti archeologici e altre istituzioni culturali. Non si tratta di una CTI generica, ma di un'intelligence mirata a comprendere chi sta attaccando il settore culturale, perché lo sta facendo e come, al fine di organizzare difese proattive ed efficaci.

Team cybersicurezza interno specializzato[22]
- CSO-Heritage dedicato (70-90k€ stipendio)
- Analisti SOC specializzati (25-35k€)
- Incident responder certificati

Formazione continua del personale

Ricerca e sviluppo in Cyber Humanities
- Sviluppo di metodologie specifiche per il settore
- Progetti di ricerca applicata
- Pubblicazioni scientifiche
- Partnership con le università
  - Roma Tre: Digital humanities
  - Bologna: Conservazione beni culturali
  - Firenze: Informatica umanistica
  - Politecnico Milano: Cybersicurezza

Raccomandazioni operative immediate

Azioni preliminari di cybersicurezza (azioni immediate - 30 giorni)

Inventario degli asset critici
- Definizione del perimetro da difendere
- Identificazione degli asset digitali critici
- Mappatura delle dipendenze tecnologiche
- Valutazione dell'impatto potenziale della perdita di dati

Test dei backup esistenti
- Verifica dell'effettiva capacità di ripristino
- Test del restore completo dell'ambiente
- Documentazione dei tempi di recovery
- Identificazione di eventuali gap procedurali

Audit delle password amministrative
- Eliminazione delle password di default
- Implementazione di policy per password complesse
- Rotazione delle credenziali privilegiate
- Implementazione MFA sugli account critici

Formazione di tutto lo staff sul phishing del settore culturale
- Simulazioni email fake eventi/mostre
- Riconoscimento delle tecniche di social engineering

[22] Valutazioni economiche basate sulle offerte di lavoro del settore privato ad agosto 2025

- Procedure di segnalazione degli incidenti
- Mitigazione dei rischi relativi al fattore umano (80-90% attacchi)

Strategia a breve termine (3-6 mesi)

Analisi dei requisiti mancanti per l'adeguamento alla NIS2

- Valutazione dello stato attuale e requisiti di adeguamento
- Stima dei costi di adeguamento
- Piano di implementazione delle misure più idonee
- Timeline di adeguamento

Implementazione delle governance di cybersicurezza

- Nomina dei responsabili della sicurezza
- Definizione di ruoli e responsabilità
- Procedure di gestione degli incidenti

Reporting al management

Sviluppo di partnership strategiche

- Accordi con altre istituzioni culturali
- Convenzioni con le università
- Collaborazione con ACN/CSIRT
- Network sharing intelligence

Sviluppo delle competenze e profili professionali

Figure professionali emergenti[23]

Il settore richiede lo sviluppo di figure ibride che combinino competenze tecniche e conoscenza del patrimonio.

Chief Security Officer for Heritage (CSO-H)

- Competenze di tecniche certificate (CISSP, CISM)
- Conoscenza di standard catalografici (ICCD, ICPAL)
- Esperienza di conservazione digitale
- Comprensione delle normative del patrimonio culturale
- Inquadramento: ruolo dirigenziale e uno stipendio di 70-90k€ per grandi istituzioni

[23] Le percentuali e gli importi indicati sono stimati sulla base delle informazioni rilevate dalla lettura degli articoli di riviste del settore e devono essere considerati in questa ottica e non come dati certificabili o ricerche di mercato.

Digital Preservation Security Specialist

- Expertise in conservazione a lungo termine
- Competenze in forensics digitali
- Conoscenza di formati e metadati
- Certificazioni specifiche (DPOE)
- Inquadramento: ruolo di coordinamento e uno stipendio di 45-60k€

Consulente NIS2 per il patrimonio culturale

- Conoscenza approfondita della normativa
- Esperienza in audit e compliance
- Capacità di gap analysis
- Project management certificato
- Tariffa: 500-800€/giorno

Security Awareness Trainer Culturale

- Competenze pedagogiche
- Conoscenza delle minacce specifiche del settore
- Capacità di sviluppo dei materiali formativi
- Certificazioni training (SANS)
- Inquadramento: ruolo di supervisione e uno stipendio di 35-45k€

Partnership formative strategiche con istituzioni pubbliche e organizzazioni professionali

- MiC: Coordinamento nazionale
- ACN: Supporto tecnico-operativo
- AGID: Standard e linee guida
- ICOM Italia: Network museale
- AIB: Associazione bibliotecari
- ANAI: Archivisti

Il Paradigma delle Cyber Humanities for Heritage Security

Definizione e ambito

Le *Cyber Humanities* rappresentano l'integrazione necessaria tra competenze umanistiche e tecniche per la protezione del patrimonio culturale digitale. La disciplina amplia i costrutti della sicurezza fisica e informatica, permettendo di tutelare il patrimonio sia materiale che immateriale.

Elementi costitutivi

Convergenza disciplinare

- Cybersicurezza applicata
- Digital Humanities
- Conservazione digitale
- Normativa relativa al patrimonio culturale
- Etica digitale

Obiettivi formativi

- Dominio tecnologico (non solo recepimento)
- Capacità di guidare progetti complessi
- Visione strategica integrata
- Competenze di risk management
- Capacità di leadership e trasformazione digitale

Percorsi di sviluppo

La creazione di questa disciplina richiede:

- Sviluppo di curricula universitari specifici
- Certificazioni professionali dedicate
- Ricerca applicata settoriale
- Pubblicazioni e conferenze specializzate
- Community of practice
- Redazione di best practice

Nota terminologica sulla Cybersicurezza

Per indicare il mondo immateriale frutto del progresso tecnologico, esistono diversi termini che provengono da altre discipline e si sono estesi per adattarsi al nuovo contesto:

Digitale (dall'informatica): indica apparecchi e dispositivi che trattano grandezze sotto forma numerica, convertendo i valori in numeri del sistema binario. L'accezione è in contrapposizione ad analogico.

Virtuale (dalla Filosofia, attraverso Meccanica e STEM): indica ciò che esiste "in potenza" e, per estensione, le simulazioni di situazioni reali o realistiche con cui il soggetto può interagire. In contrapposizione a reale, effettivo.

Artificiale (dal mondo produttivo): indica prodotti simili o identici per aspetto, com-

posizione, funzione ai prodotti naturali, ma ottenuti dall'uomo con mezzi tecnici. In contrapposizione a naturale.

Cyber (dalla Medicina): Abbreviazione di cybernetics, dal greco[24], formalizza l'analogia funzionale dei meccanismi di comunicazione e autoregolazione (mediante feedback) negli esseri viventi e nelle macchine. La cibernetica integra nozioni neurofisiologiche e biologico-molecolari con la teoria matematica dell'informazione, la teoria dei sistemi e la ricerca operativa.

Sebbene esista il termine italiano cibernetica, e il prefisso ciber sarebbe più che adatto, ci siamo arresi *obtorto collo* al fascino irresistibile che l'idioma d'oltremanica esercita sui reparti marketing, e non solo. Abbiamo pertanto usato il termine Cybersicurezza per riferirci alla disciplina che, ampliando i costrutti della sicurezza fisica, di quella informatica e delle telecomunicazioni e i metodi della continuità operativa, permette di tutelare il patrimonio, sia esso materiale, immateriale o una combinazione di entrambi.

Conclusioni e prospettive

L'analisi degli incidenti cyber nel settore del patrimonio culturale italiano 2020-2024 evidenzia una crisi sistemica che richiede interventi urgenti e strutturali. Il settore, caratterizzato da un deficit cronico di competenze digitali (51% senza professionisti specializzati) e da una pianificazione prevalentemente emergenziale (67% a breve termine), si trova esposto a minacce in costante evoluzione.

Abbiamo visto come l'Italia subisca una quota sproporzionata di attacchi cyber a livello globale: questa elevata esposizione al rischio assume i contorni di una minaccia sistemica quando colpisce settori nevralgici per la vita culturale e sociale del Paese.

Più che le singole statistiche, sono gli incidenti reali a descrivere la gravità del contesto. L'attacco di tipo *supply chain* che ha colpito il fornitore Miles33 nell'agosto 2024 è emblematico: compromettendo un singolo anello della catena di fornitura digitale, gli aggressori hanno oscurato centinaia di testate giornalistiche contemporaneamente, dimostrando l'estrema fragilità dell'ecosistema mediatico e informativo nazionale.

Allo stesso modo, l'attacco *ransomware* che ha paralizzato i sistemi della Regione Lazio nell'agosto 2021 non è stato un semplice *data breach*, ha rappresentato un attacco diretto a un'infrastruttura pubblica critica, interrompendo servizi essenziali per la comunità – come le prenotazioni sanitarie in piena pandemia – e colpendo il

[24] Il termine greco **κυβερνητική (τέχνη)**, che significa «arte del timoniere», è stato adottato dal matematico americano Norbert Wiener (1894-1964) per fondare la cibernetica. Il termine è stato poi ripreso in medicina e nella letteratura fantascientifica.

patto di fiducia tra cittadini e istituzioni che è il fondamento del patrimonio sociale e culturale collettivo.

L'implementazione della Direttiva NIS2 rappresenta un'opportunità irripetibile per elevare la propria maturità cyber. Con 1.500 istituzioni culturali attenzionate, che rappresentano il 70% del patrimonio digitalizzato nazionale, l'adeguamento normativo può catalizzare un cambio di paradigma necessario, agendo in via preventiva anziché attendere il prossimo incidente critico, come accaduto per lo zoombombing nel caso "My Jewish Italy".

Le priorità immediate sono chiare:

- sviluppo urgente di competenze specialistiche attraverso le Cyber Humanities;
- implementazione delle misure di base (backup, segmentazione, monitoraggio);
- creazione di partnership strategiche per condividere costi e competenze;
- investimento in tecnologie di protezione specifiche per il *born digital.*

Il rischio di perdita irreversibile del patrimonio digitale è concreto. Come dimostrano i casi della British Library e dell'Internet Archive, il costo della non-prevenzione supera di diversi ordini di grandezza gli investimenti necessari in sicurezza. La cybersicurezza non è più un costo differibile ma un prerequisito essenziale per la conservazione della memoria culturale nell'era digitale.

Il percorso verso la resilienza digitale del patrimonio culturale richiederà anni di investimenti, lo sviluppo di competenze specialistiche e un cambio culturale profondo. Tuttavia, l'alternativa - la perdita progressiva e irreversibile della memoria digitale collettiva - non è accettabile per una nazione che fonda sulla cultura una parte significativa della propria identità e del proprio sviluppo economico.

Metodologia di raccolta e analisi dati

L'analisi si basa su incidenti documentati da fonti pubbliche nel periodo 2020-2024. Il campione include eventi con impatto significativo sulle istituzioni culturali italiane.

Come già sottolineato, la classificazione per *severity* non può seguire completamente gli standard del Rapporto a causa della limitata disponibilità di dati sugli impatti economici e operativi reali. Come dichiarato nell'Appendice Metodologica: "Gli incidenti analizzati rappresentano certamente un campione significativo di quelli resi pubblici dalle fonti principali". Tuttavia, le percentuali e gli importi economici presentati sono stime derivate dall'esperienza e da fonti giornalistiche e vanno intesi come valori indicativi, non come dati certificati.

Per il patrimonio culturale, questa limitazione è amplificata dalla natura tradizionalmente riservata del settore e dalla mancanza di obblighi di disclosure pre-NIS2. Le organizzazioni culturali tendono a non rendere pubblici gli incidenti per timore di danni reputazionali, rendendo il fenomeno probabilmente sottostimato.

I dati presentati in questo studio rappresentano la migliore analisi possibile con le fonti attualmente disponibili. Una valutazione completa del rischio cyber nel patrimonio culturale sarà possibile solo a partire dal 2026, con l'entrata a regime degli obblighi di notifica NIS2 e la prevista disponibilità di dataset sistematici dall'Agenzia per la Cybersicurezza Nazionale.

Noi e i nostri dati in Rete: un universo da scoprire

(A cura di Andrea Rui)

I recenti casi emersi su fughe di notizie di sicurezza nazionale in America e sulla possibilità di reperire pubblicamente account e password di figure apicali governative italiane (ri)porta prepotentemente all'attenzione il serissimo problema della protezione delle informazioni.
In tempi in cui la sicurezza nazionale, la protezione delle infrastrutture critiche e la sopravvivenza delle aziende sono costantemente messe a rischio, occorre focalizzarsi sulle cause dei problemi.

Come dimostrato dai recenti eventi (SignalGate e violazione di TeleMessage), i soldi non fanno la sicurezza: gli USA sono probabilmente il paese che investe di più al mondo in sicurezza, e nonostante ciò sono accaduti fatti che sono riusciti a stupire anche l'ultimo degli utenti della Rete.

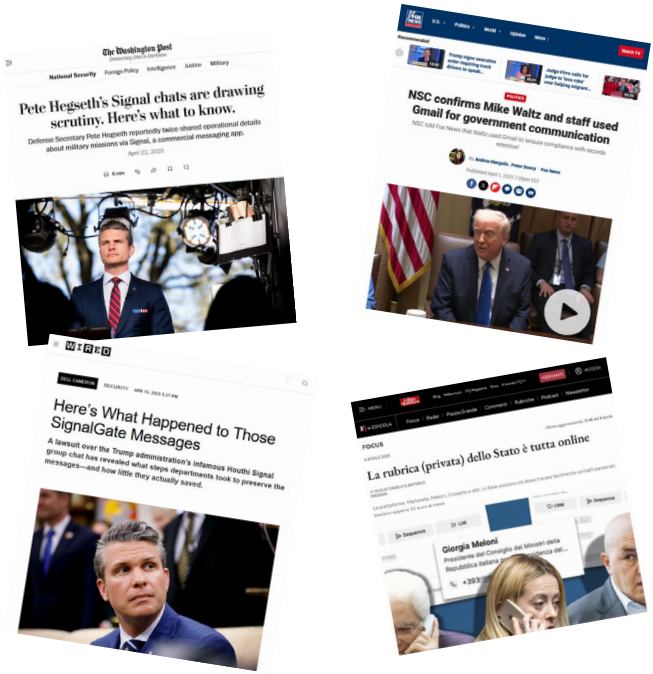


Figura 1 - USA & SignalGate, TeleMessage, etc.

Recenti eventi, per quanto molto diversi, come quello della *kiss cam* al concerto dei Coldplay, la pubblicazione di immagini e commenti sul gruppo 'mia moglie' di Facebook e il data breach di 2.5 miliardi di account di GMail evidenziano la grave mancanza di percezione di quali siano i rischi e le implicazioni della pervasiva mancanza di una educazione alla cybersecurity e alla Privacy.

Il futuro degli Stati, delle Istituzioni, delle infrastrutture critiche, delle aziende, dei segreti industriali e del destino politico e professionale delle persone è legato indissolubilmente a come i giovanissimi di oggi gestiranno le informazioni nel prossimo futuro.

Ed è pertanto fondamentale che gli adulti di oggi siano in grado di trasmettere ai giovani un messaggio educativo e culturale per costruire un futuro più sicuro per tutti.

Quanto valgo io in rete (= quanto valgono i miei dati?)

Viviamo in un'epoca in cui si dà sempre più per scontato che tutto sia gratis.

Riusciamo ancora ad accettare che un prodotto tangibile possa avere un costo, perché possiamo toccarlo.

Tutto ciò che invece si trova dall'altra parte dello schermo del PC o dello smartphone invece è intangibile, e non abbiamo percezione di quanto possa costare e valere (né ci siamo mai posti il problema di provare a quantificarlo).

Tuttavia le chat, le e-mail, i video, gli spazi di archiviazione dei nostri documenti '*nel Cloud*', le nostre videoconferenze, l'AI che ormai quotidianamente utilizziamo esistono grazie a investimenti colossali.

Ogni bit che entra ed esce dal nostro smartphone viaggia attraverso costosissime reti dati, fibre ottiche transoceaniche, reti cellulari e satellitari, e viene elaborato in immensi datacenter che contengono centinaia di migliaia di server.

E di datacenter ce ne sono a migliaia sul pianeta, e ciascuno può consumare dalle decine alle centinaia di MWh all'anno.

Investimenti in datacenter

Solo nel 2025 Microsoft intende investire altri 80 miliardi di dollari in nuovi datacenter.
Altri 300 miliardi (di Euro, questa volta) sono già stati stanziati in Europa.
Il 21 Gennaio 2025 alla Casa Bianca è stato dato l'annuncio del Progetto Stargate: una nuova azienda che vuole investire 500 miliardi (100 già stanziati) nei prossimi quattro anni per costruire una nuova infrastruttura per l'AI negli USA.

Se poi si va a vedere come stanno le aziende che sostengono questi costi incredibili, vedremo che valgono migliaia di miliardi di dollari, e fanno miliardi di dollari di utili tutti gli anni.
A fine Luglio 2025, e con delle semplici divisioni tra capitalizzazione e numero di utenti attivi, vedremo che per il mercato ogni utente di Microsoft valeva circa 2.500$, uno di Meta 620$, uno di Apple 450$ e uno di Google 750$.
Come semplice esercizio, ciascuno può estendere questa valutazione a tutte le app e tutti i servizi che utilizza, per poi sommarne tutti i risultati.
Già alcuni anni fa era stata fatta una stima del valore di circa 35.000$ di ogni utente attivo in Rete.

Chi paga tutto questo, visto che gli utenti non pagano (o al limite pagano prezzi irrisori)?

L'interessante caso del Fisco italiano

Un altro fatto assolutamente rilevante è il fatto che il Fisco italiano abbia ufficializzato il fatto che il rapporto tra utente e fornitore di servizi concretizza una transazione tassabile (scambio sinallagmatico, ovvero l'accesso ad un servizio in cambio dei dati).
Ai dati è stato quindi riconosciuto un valore commerciale, e possono essere scambiati per ottenere servizi che a loro volta producono valore.

It's Free, Baby!

In occasione degli incontri nelle scuole, arriva sempre il momento in cui si chiede a tutti se per caso utilizzino Google, WhatsApp, Facebook, Instagram, TikTok, ChatGPT e così via …

Tutte le mani vengono alzate (avevate dei dubbi?).
Si chiede quindi a tutti quanto abbiano pagato per utilizzare tutti questi servizi, e altrettanto ovviamente si viene guardati con occhi stupiti come se fossimo degli alieni.
Si passa quindi a raccontare cosa c'è dietro alle loro app, le chat, i video, i commenti: investimenti colossali in datacenter, ricerca, sviluppo, energia, connettività, satelliti, fibre ottiche sottomarine, incredibili consumi di acqua per il raffreddamento e, soprattutto, guadagni colossali.

A questo punto i ragazzi (ma anche i docenti e i genitori) iniziano a percepire che qualcosa non torna: costi esorbitanti e tutto gratis …
Iniziano a supporre che i guadagni arrivino dalle pubblicità, ma si rendono conto che non è una spiegazione sufficiente.
Arriva quindi il momento in cui si lancia lo slogan di rito: ***"se non paghi, è perché il prodotto sei tu!"***.
E a questo punto si passa a spiegare quante informazioni loro diffondano inconsapevolmente in Rete, quante altre ne vengano raccolte a loro insaputa, e come vengano utilizzate.

Siamo pesci rossi in un acquario

Vivresti in una casa di vetro con pareti a specchio verso l'interno, dove tutti possono vederti, ma tu non puoi sapere chi ti sta guardando, e perché?

Il tuo smartphone ti apre infinite finestre sul mondo, ma non tutte sono trasparenti.
Molte ti fanno vedere solo ciò che vuoi vedere.
Altre ti fanno vedere solo ciò che vogliono farti vedere, e altre soltanto ciò che vogliono farti comperare.
Inoltre da alcune finestre tutti dall'esterno possono vedere l'interno (cioè ciò che tu racconti) e pochi, da altre finestre, possono invece vedere tutto di te, e in base a ciò che vedono, decidono cosa tu potrai o dovrai vedere in futuro.
Pensi che sia uno scenario distopico? È la realtà delle cose: ci hanno fornito un acquario molto accogliente, e noi ci nuotiamo pensando di essere liberi di andare dove vogliamo, ma non vedendo cosa c'è fuori, non sappiamo se ci sia un mare in cui invece poter nuotare liberi.

Accetteresti di essere pedinato e spiato 365h24?

"… impossibile! Me ne sarei certamente accorto!"
Eppure c'è qualcuno che, giorno e notte, sa dove ti trovi e con chi sei.
Sa dove vuoi andare, e che strada farai; anche quali mezzi pubblici stai utilizzando.
Sa anche cosa stai guardando, cosa ti piacerebbe comperare, quali sono i tuoi desideri e quanto puoi spendere.
Sa anche quali sono i tuoi amici, se sei di buon carattere, quando invii i cuoricini alla tua compagna, …
Ovviamente sa dove e a che piano abiti e dove e per chi lavori.
Sa anche quando sei a casa e quando no (e molto probabilmente ne ha anche fatto la mappatura).
Quasi sicuramente conosce la tua voce, e ascolta tutto ciò che dici.

"Non ci credo: com'è possibile?"
Iniziamo dalle cose semplici: i social network a cui ti sei registrato conoscono tutta la tua rete di contatti (professionali e non), e se utilizzi WhatsApp (cosa assai probabile!) anche tutta la rete dei tuoi contatti telefonici.
Probabilmente hai anche un account Google (ma se non lo hai, fa poca differenza): praticamente ogni sito web contiene riferimenti a Google, Facebook e X (ex Twitter), e grazie a questi possono sapere quale pagina di quale sito stai consultando, quanto ti soffermi su ogni contenuto, e su quali pubblicità fai click (o tap).
Se hai uno smartphone con Android, le stesse cose accadono con tutte le app che hai installato, e altrettanto accade con i dispositivi della Apple.

Vi sono poi gli assistenti vocali (Siri, Alexa, ...), le webcam di computer, smartphone e anche quelle indossabili e quelle che forse hai installato in casa.
Esistono aziende che raccolgono e analizzano audio raccolti dai microfoni degli smartphone e delle Smart-TV entro un raggio concordato con il cliente interessato ai dati (Active Listening).

È possibile utilizzare gli accelerometri degli smartphone per 'ascoltare' le conversazioni, senza bisogno di accedere al microfono e agli altoparlanti: in sostanza, la vostra app di contapassi, quella della bussola e quella di sky-view possono di fatto ascoltare le vostre conversazioni.
Naturalmente poi c'è tutto ciò che noi e gli altri raccontiamo in Rete su di noi ...

Pigrizia

In occasione degli interventi nelle scuole sull'importanza di proteggere le informazioni (proprie e degli altri), alla richiesta agli studenti di cosa facciano per proteggere i propri dati, ci si trova davanti il vuoto pneumatico.

Nessun antivirus sui loro smartphone, nessuna modifica alle impostazioni per la privacy delle app, nessuna protezione antitracking …

Chiedendo quindi se non siano preoccupati del fatto che tutti i loro dati personali vengono raccolti e utilizzati da sconosciuti e per scopi a loro ignoti, le risposte sono sempre le stesse:

1. ***"non ho nulla da nascondere", e***
2. ***"cosa vuoi che se ne facciano dei miei dati?".***

La cosa più preoccupante è che le medesime risposte le danno generalmente anche i loro insegnanti e i loro genitori.

Come la fretta, anche la pigrizia è una cattiva consigliera.

Ci porta ad installare applicazioni di cui sappiamo poco o niente, soltanto perché l'hanno installata amici o colleghi, o perché hanno una bella icona, o perché sembra identica a quella dell'applicazione ufficiale.

Inoltre, tutte le volte che installiamo un'applicazione, o visitiamo un sito web, click'iamo (o 'facciamo tap') sul bottone 'Accetta', accettando ciecamente qualsiasi cosa, e altrettanto vale per l'accettazione dei cookie sui siti web, senza neppure chiederci cosa stiamo accettando.

Probabilmente non abbiamo mai letto le licenze d'uso delle app che abbiamo installato, né abbiamo mai letto le informative sulla privacy che ci raccontano a cosa servono i cookie che accettiamo.

E non sapendo cosa accettiamo, non ci siamo neppure mai chiesti se per fare ciò che desideriamo esistano anche applicazioni alternative e servizi differenti (anche se possono avere un'icona diversa o meno bella di quella a cui siamo abituati).

Privacy o Information Security?

È opportuno dedicare qualche riga per chiarire un concetto semplice ma diffusamente poco compreso.
Troppo spesso le persone si appellano al *concetto di Privacy* quando in realtà ci si riferiscono alla sicurezza nella gestione delle informazioni, e viceversa.
Il furto di un numero di carta di credito ha a che fare con la protezione delle informazioni.
Al contrario, telefonare a un amico per cercare di vendergli un depuratore d'acqua ha a che fare con la Privacy: ho titolo per avere il suo numero di telefono (è un amico), ma non per utilizzarlo per scopi commerciali.
La protezione delle informazioni deve garantire che queste debbano essere certamente disponibili soltanto agli autorizzati e solo quando ne hanno necessità.
La Privacy invece deve garantire che le informazioni personali non vengano utilizzate per invadere la sfera personale e intima delle persone.

Per fare un esempio semplice e molto pratico, il browser Chrome è oggettivamente molto sicuro: è sviluppato con cura e aggiornato frequentemente, in modo che i vostri dati non cadano nelle mani sbagliate (e cioè dei 'cattivi', e soprattutto della concorrenza): devono rimanere al sicuro nell'ecosistema di Google, e altrettanto vale per Edge di Microsoft e Safari di Apple.
E ciò rappresenta il concetto di 'sicurezza (o protezione) delle informazioni'.
Se invece ci riferiamo al concetto di Privacy, siamo sul pianeta sbagliato: la quantità di informazioni che questi browser raccolgono e inviano a Google, Apple e Microsoft è impressionante, se confrontata con altri browser nati per essere rispettosi della Privacy.
E per fare un altro esempio pratico, è stupefacente vedere quante persone chiedano ai motori di ricerca anche il proprio indirizzo di casa: inserire il percorso di un sito (URL) che si desidera visitare nella barra dei link è completamente diverso che inserirlo nel campo di ricerca presente nella pagina.

Quanto vale Chrome?

La possibilità che il DOJ americano imponga a Google di vendere Chrome ha portato a farne una valutazione: le stime variano tra i 20 ed i 50 miliardi di dollari, ed ha già ricevuto un'offerta reale da 34.5B$.
Eppure di browser ce ne sono tanti, e di ottima qualità: cosa avrà Chrome che gli altri non hanno …?

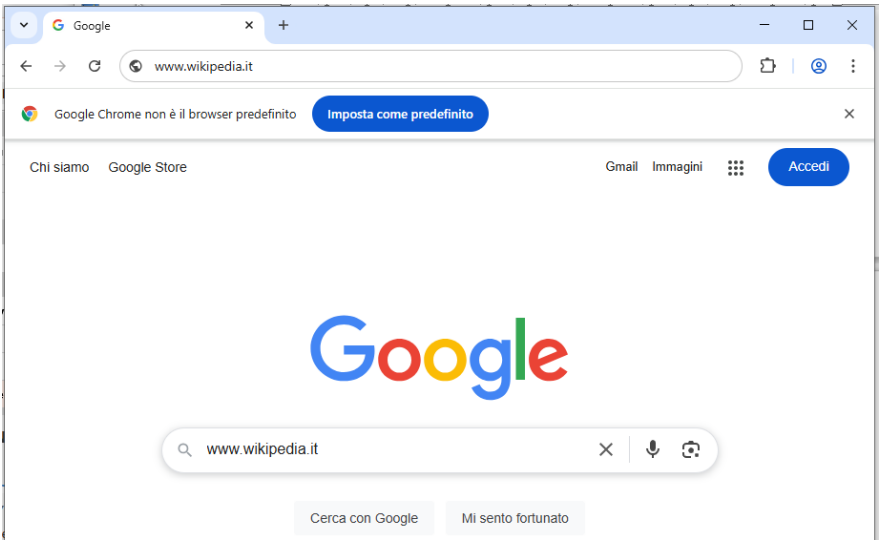


Figura 2 - Perché chiedere al motore di ricerca ciò che già so?

La differenza è la stessa che corre tra l'andare dove si desidera, e chiamare l'Ufficio Informazioni per chiedere dove vogliamo andare (cosa che, ovviamente, già sappiamo, ma ora lo sa anche l'"Ufficio Informazioni").

Il modello di business

Dedichiamo un paragrafo specifico al modello di business di Google (e degli altri principali attori sul mercato), non perché sia l'unica azienda a raccogliere e profilare i dati delle persone, ma per la pervasività con cui è riuscita a farlo.

Apple ha fatto altrettanto creando un ecosistema chiuso in un recinto di hardware e software di prim'ordine, e Microsoft ha fatto, con molto ritardo, centralizzando nel cloud tutto ciò che prima era memorizzato localmente sui PC.
Quanto esposto può (e deve) essere trasposto anche in molte altre realtà, aziende e multinazionali.
La rivoluzione nella raccolta dei dati in Rete è arrivata con Google, che ha ribaltato il precedente modello di raccolta e indicizzazione dei dati.

Il precedente modello si basava sull'idea di cataloghi, creati per lo più manualmente, dei siti che venivano trovati in Rete, come delle specie di 'Pagine Gialle' di Internet.

Il colpo di genio è stato quello di fare in modo che fossero i siti stessi e gli utenti del Web a segnalare e far indicizzare automaticamente i propri contenuti e i propri comportamenti in Rete.

L'approccio è stato semplice e geniale al tempo stesso: Google ha messo a disposizione pochi servizi di larghissimo e semplice utilizzo, con un'infrastruttura e una semplicità e qualità tali da garantire una fruibilità molto migliore di quella della concorrenza, oltre che a un sistema di remunerazione legato alla quantità di contenuti pubblicati e al numero di interazioni.

Hai bisogno di cercare qualcosa? Chiedilo a Google (tanto è gratis!)
Hai bisogno di una casella di posta elettronica, e gli altri provider ti chiedono qualche dollaro all'anno? Creala su Google (tanto è gratis!)
Il tuo sito include nelle proprie pagine script e font? Non pagare per aumentare la tua banda: falli ospitare da Google (tanto è gratis!)

E così via con la web analytics, lo streaming di video, indagini di mercato, captcha, e potremmo proseguire con Maps, StreetView, Google Drive, i DNS e così via ...

Se andate oggi a verificare il contenuto di qualsiasi pagina web, troverete che quasi certamente questa scarica contenuti da servizi di Google (script, font, ID pubblicitari, tagging dei contenuti, web analytics, …).
E per ridurre il rischio che altri veicolassero i vostri dati, Google ha anche sviluppato un sistema operativo (Android) e un browser (Chrome), ovviamente gratuiti affinché produttori di smartphone e tablet li adottassero a tappeto, risparmiando moltissimo tempo e denaro: in questo modo i dati rimangono chiusi in un ecosistema completamente Google.
Per impedire ad altri di poter diventare potenziali concorrenti, Google ha anche siglato accordi miliardari con i più importanti produttori di dispositivi (smartphone, tablet, etc.) per l'installazione esclusiva del proprio ecosistema di applicazioni, e con altri concorrenti (Apple e sviluppatori di browser) per impostare come motore di ricerca predefinito il proprio.

Accordi miliardari

Nel 2021, per avere l'esclusività del motore di ricerca, Google ha pagato ad Apple 18B$.
Nel 2022: l'importo versato ad Apple sale a 20B$ all'anno!
Nel 2025 Google si impegna a versare 8B$ a Samsung per installare Gemini AI come motore di AI predefinito.

Azioni similari sono state naturalmente adottate da Apple per mantenere i propri utenti nel proprio giardino dorato, e Microsoft per mantenere i propri utenti all'interno dell'ecosistema di Windows e Office.

Ciò significa che ogni volta che voi accedete ad un qualsiasi sito (probabilmente anche a quello della vostra banca!) Google sa che voi, in quel momento e da dove vi trovate, siete interessati e state consultando esattamente quel contenuto.

Significa anche che ogni volta che inviate una mail dalla vostra casella di Microsoft, Apple o Gmail, o comunque scrivete a qualcuno che utilizza una di queste caselle, queste aziende sanno esattamente chi conoscete e con chi state comunicando, e cosa vi state raccontando (includendo anche gli allegati, anche se si tratta di immagini, scansioni e anche file *zippati!).*

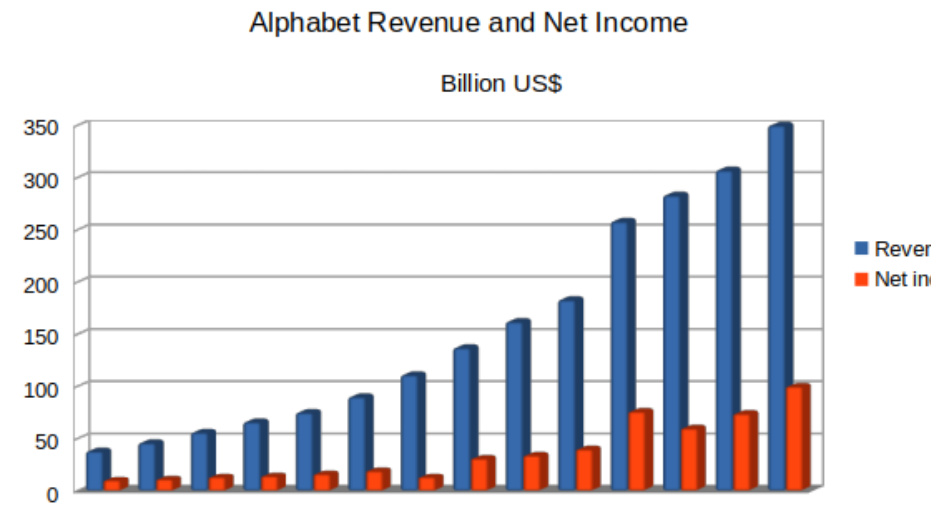


Figura 3 - Fatturato e utili di Alphabet negli ultimi 15 anni

Il controllo di tutte queste informazioni consente quindi a queste aziende di fare una eccezionale profilazione dei propri utenti, che viene rivenduta per un precisissimo targeting pubblicitario.

Mi costringono a scaricare contenuti indesiderati?

Introduciamo ora l'argomento di come vengano raccolti i dati personali (e quanti) attraverso la navigazione nel Web (escludendo ovviamente quelli che forniamo direttamente con le informazioni che pubblichiamo).

Limitiamoci a mostrare quanti diversi contenuti vengono scaricati, e da quanti diversi siti, quando consultate una singola pagina.

Prendiamo come esempio il sito di un importante quotidiano italiano, utilizzando l'estensione NoScript per il browser.

La semplice consultazione della home page del sito mostra che questa scarica a sua volta contenuti da più di una ventina di altri siti, oltre a quelli istituzionali.

La maggior parte di questi sono siti di advertising e di profilazione del traffico e del comportamento dell'utente sulla pagina, e in ogni caso troverete praticamente sempre un riferimento ad almeno un servizio di Google (in questo caso, ben 4).
Ciò significa che quando accedete e navigate nel sito di quella testata, a vostra insaputa una ventina di altre aziende vengono informate delle pagine che state visitando e dei contenuti che state consultando.

Figura 4 - Contenuti scaricati a nostra insaputa dalle pagine web

Connessioni indesiderate

Proseguiamo con un approfondimento su come veniamo costantemente tracciati.
Un aspetto che è normalmente invisibile all'utente è quanto ogni app installata acceda a siti e servizi non necessari. Installando un semplice personal firewall (non vi spaventate: è una app come un'altra!) è possibile vedere quante e quali connessioni vengano aperte, e con quale frequenza.

Se l'aspetto inerente la quantità di connessioni con contenuti indesiderati è già stato visto nel paragrafo precedente, vediamo ora l'aspetto della frequenza delle connessioni. Scoprirete che le app fanno traffico verso questi servizi anche quando non vengono utilizzate e non interagite con loro.

A parte l'ovvia considerazione sull'inutile consumo di energia (per farlo la batteria si scarica prima!), l'aspetto più interessante risiede in una semplice domanda: cosa viene scambiato in questo continuo traffico di dati ...?

Web o App? Questo è il problema!

Perché ci spingono continuamente ad installare app invece che consultare gli equivalenti servizi web?
La parola chiave, come sempre, è "gratuito": in ogni messaggio pubblicitario vi diranno "… scarica gratuitamente la nostra app!".
Anche l'accesso al corrispondente sito web lo è: e allora, perché questa insistenza?

Vediamo innanzitutto cosa è una 'app': fondamentalmente, si tratta di una versione memorizzata localmente sul dispositivo delle pagine web relative ad un servizio; tecnicamente sono chiamate 'PWA' (Progressive Web App).

I vantaggi delle PWA sono principalmente tre:

- evitano di scaricare ripetutamente il corpo delle pagine del sito,
- funzionano anche in assenza di connessione, sincronizzando i dati modificati quando questa torna disponibile,
- si riduce il traffico tra il dispositivo e il web server, offrendo prestazioni migliori.

Tuttavia la ragione principale per cui veniamo spinti a preferire le 'app' è che l'accesso ai servizi mediante un normale browser offre all'utente molte opportunità di filtrare il traffico (Ad Blocker, blocco dei tracker, script blocking, selezione del DNS, user fingerprinting, blocco di protocolli non sicuri e connessioni indesiderate, e così via).
Le app non offrono invece all'utente queste opportunità, impedendogli quindi di esercitare un controllo sui propri dati e sulla propria Privacy.

Per riuscire a limitare la raccolta di dati personali ci si trova quindi costretti a installare un personal firewall, da utilizzare per bloccare tutte le connessioni non inerenti al servizio desiderato.

A titolo di esempio, gli screenshot riportati in Figura 5 sono relativi alle connessioni che vengono aperte dall'app di un importante social network professionale e da una di un importante istituto bancario.
Quelle oscurate sono le uniche riferibili ai siti desiderati; come potrete osservare, sono molte le connessioni non pertinenti aperte dalle app, e troverete praticamente sempre connessioni verso qualche servizio di Google.

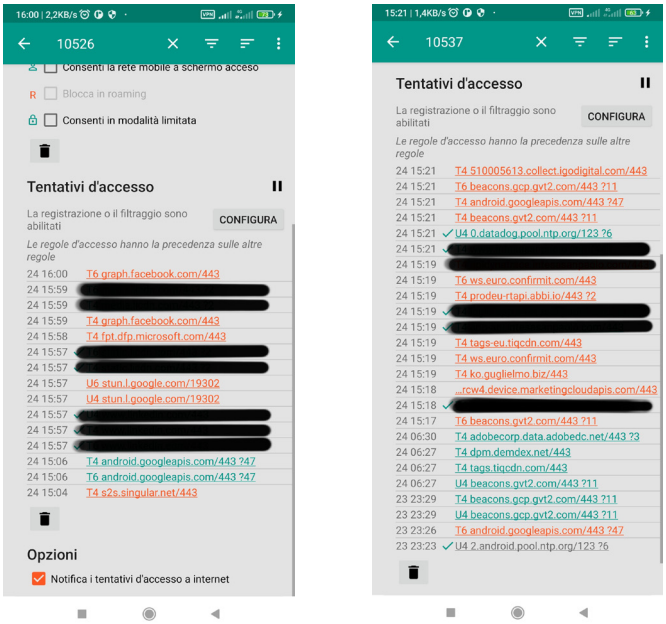


Figura 5 - Contenuti scaricati a nostra insaputa dalle app

Come raccolgono i miei dati?

La raccolta dei dati viene fatta in molti modi, tra cui:

- ciò che raccontiamo e pubblichiamo (su di noi e sugli altri);
- ciò che le app e le pagine web raccolgono da nostri dispositivi (contatti, telefoni, caratteristiche dell'HW e SW dei nostri dispositivi, geolocalizzazione, etc.);
- dati inviati da dispositivi IoT o indossabili, webcam, microfoni, smartwatch, etc.;
- ciò che viene raccolto con artifici per il fingerprinting dei dispositivi e degli utenti;
- inferenza per deduzione e induzione (immagini, etc.) = conoscenze, gruppi, preferenze, abitudini, …;
- utilizzo dei social;
- assistenti personali (Siri, Alexa, …), inclusa la voce;
- contenuti e metadati forniti da browser e app;
- domotica, aspirapolvere, frigorifero, lampadine, citofono, telecamere, …;
- interessi, siti visitati, utilizzo delle app, contenuti su cui ci si sofferma, acquisti,
- … e molto, molto altro ancora!

Quali e quanti dati vengono raccolti?

Riprendendo quanto già intravisto nei paragrafi precedenti, possiamo formulare un primo elenco, senza alcun ordine e lontano dall'essere esaustivo, di dati che direttamente o indirettamente esponiamo in Rete:

- account e nomi utente (ne utilizziamo più di uno);
- indirizzi e-mail (probabilmente ne utilizziamo più di una);
- numeri di telefono (personali, aziendali);
- dati personali come nome e cognome, codice fiscale, data e luogo di nascita, etc.;
- indirizzi (casa, ufficio, casa di vacanza, recapiti per le consegne, …);
- quali social network utilizziamo, e come e quanto li utilizziamo;
- la nostra voce (Alexa, Siri, Smart-TV, assistenti personali, …);
- la nostra immagine, attraverso mille fotografie e selfie;
- interessi (acquisti, commenti sui social, siti visitati, pubblicità visualizzate, ...);
- ubicazione, piano e struttura delle abitazioni dove utilizziamo un aspirapolvere 'smart';
- dove siamo, i nostri tragitti e le nostre mete (navigatori, geolocalizzazione degli smartphone e dei nostri veicoli);
- chi conosciamo: tutti i nostri contatti sui social (i loro username ed e-mail), i loro numeri di telefono (WhatsApp, …), etc.;
- orari e le nostre abitudini (geolocalizzazione, domotica, ...);
- per chi lavoriamo (attraverso gli indirizzi IP delle connessioni di rete aziendali);
- cosa non sappiamo (tutte le ricerche fatte attraverso i motori di ricerca e le varie AI);
- la nostra cultura e il nostro profilo psicologico (attraverso le nostre comunicazioni e tutte le chat e i post e i relativi commenti lasciati sui social);
- il nostro grado di accettazione del rischio, attraverso i commenti che facciamo sugli incidenti in cui eventualmente incorriamo;
- lo stato di salute nostro e di parenti e conoscenti, attraverso le notizie che pubblichiamo e le ricerche che facciamo su problemi di salute, cure e medicinali;
- i metodi di pagamento preferiti e le disponibilità finanziarie, in relazione a quanto spendiamo;
- i nostri gusti, in relazione agli alimenti e ai prodotti per la casa che comperiamo;
- il nostro percorso di studi e interessi professionali, attraverso il curriculum vitae che diffondiamo per le ricerche di lavoro, e i corsi e convegni a cui ci iscriviamo, anche on-line;

- i prodotti che possediamo (auto, smartphone, tablet, computer, dispositivi indossabili, etc.);
- i viaggi che facciamo, attraverso i biglietti che acquistiamo, oltre che, naturalmente, alla nostra geolocalizzazione continua;
- i nostri gusti, attraverso i biglietti per cinema, spettacoli e concerti che acquistiamo;
- i locali dove andiamo: ristoranti, discoteche, parrucchieri, etc., attraverso i nostri pagamenti elettronici (e, naturalmente, la geolocalizzazione);
- le reti Wi-Fi e i dispositivi Bluetooth a cui ci connettiamo (o che comunque i nostri smartphone rilevano, anche senza che avvenga una connessione);
- le persone che conosciamo e con cui ci troviamo, attraverso la correlazione tra orari e geolocalizzazione, oltre che la presenza con altri nelle medesime fotografie che pubblichiamo in Rete;
- cronologie di navigazione, includendo sistemi di navigazione e servizi online di intrattenimento, e relativi gusti e preferenze;
- pubblicità più o meno viste (attraverso cookie e tracker, e web analytics);
- immagini e video condivisi e relativi tagging;
- orientamento politico e sociale, in relazione ai quotidiani e ai siti di informazione che visitiamo;
- la nostra padronanza di lingue straniere;
- ciò che diciamo e facciamo, anche a casa nostra, grazie agli assistenti vocali e alle Smart-TV, senza contare le telecamere che eventualmente installiamo in casa e fuori;
- i contenuti dei documenti che facciamo analizzare e riassumere all'AI;
- i documenti di identità nostri e di qualche parente, con foto, date di nascita e altro ancora (chi non ne ha mai inviato una copia per qualche ragione?).

E questa è soltanto una parte delle informazioni che forniamo, più o meno direttamente, attraverso il nostro essere in Rete.

Da queste e altre informazioni che forniamo è possibile derivare profili analitici che consentono di classificare la nostra persona secondo una pletora di categorie (potere di spesa, profilo culturale, ambiti di conoscenza, interessi, abitudini, attitudini, profilo psicologico, etc.), grazie alle quali è possibile progettare e presentare messaggi commerciali e politici mirati alla singola persona (oltre che creare fake news e messaggi di phishing per truffarci).

In questo modo è inoltre possibile orientare anche gli acquisti e il voto politico dell'utente.

Esistono poi aziende ultra-specializzate nella raccolta di dati sulle persone: i cosiddetti "data broker", di cui Acxiom, Equifax, LexisNexis ed Experian sono i nomi più rilevanti.
A titolo di esempio, Acxiom pubblicizza il fatto di disporre il profilo di 2.5 miliardi di utenti in 62 paesi, con oltre 3000 attributi per profilo, e copre il 95% degli utenti americani; altre aziende dichiarano di avere addirittura 7000 attributi per profilo.

Chi raccoglie e utilizza i miei dati?

Qualsiasi servizio digitale con cui interagiamo raccoglie più o meno dati e per svariate ragioni.

Esistono servizi rispettosissimi della privacy, che non raccolgono né conservano dati personali, utilizzando ciò che ricevono al minimo indispensabile e soltanto per valutare le prestazioni e la qualità dei propri servizi.
Vi sono poi lo Stato e gli enti e aziende che per poter fornire i propri servizi devono necessariamente raccogliere dei dati e gestirli a norma di legge (come l'Anagrafe, l'Erario, i servizi di paghe e stipendi, di fatturazione e acquisti online, e così via).
Inoltre più o meno tutti gli Stati, in base alle proprie disponibilità e capacità, raccolgono e analizzano i dati di chiunque (non solo dei propri cittadini: anche di quelli degli altri Stati), in generale per scopi di sicurezza e prevenzione, con 'eccellenze' come il Project 415 (ECHELON) gestito dai 'Five Eyes', i programmi segreti Fairview e STORMBREW della NSA americana e il Sistema di Credito Sociale (SCS) cinese.
Esistono poi persone che pubblicano illegalmente informazioni personali e intime di altre persone per varie ragioni, e aziende (data broker) che raccolgono e analizzano molte più informazioni di quanto ci si possa immaginare, e addirittura costruiscono il proprio business proprio sul livello di dettaglio con cui riescono a profilare centinaia di milioni, o addirittura miliardi, di persone.
Infine vi è il Cybercrime, un insieme di persone e di aziende (e a volte di Stati) che raccolgono informazioni per utilizzarle contro gli avversari, per estorsioni, ricatti e per acquisire vantaggi industriali e politici.

Cosa possono fare con i miei dati?

Anche in questo caso, ci limitiamo a una breve serie di esempi di come possono essere utilizzati i dati che diffondiamo inconsapevolmente:

- aumentarmi il premio dell'assicurazione dell'auto;
- aumentarmi il premio dell'assicurazione medica;
- decidere quanto potrò spendere per il biglietto aereo che sto comperando;
- orientare il mio voto politico (vi ricordate del caso di Cambridge Analytica?);
- farmi comperare i prodotti non migliori per me, ma quelli su cui il venditore ha un margine economico maggiore;
- farmi spendere il massimo possibile per le mie tasche per un prodotto per cui potrei spendere meno;
- concedermi o negarmi un mutuo o un finanziamento in relazione allo stato finanziario della mia azienda, o per il fatto che è in corso un'acquisizione societaria e un possibile licenziamento di lavoratori (loro lo sanno già, ma io probabilmente no);
- in base alle mie attitudini, indirizzarmi a siti di fake news per massimizzare il numero di click;
- trattenermi il più possibile all'interno di un social network per massimizzare la quantità di impressioni pubblicitarie, e impedirmi di spendere del tempo su altri social (TikTok è un'eccellenza in questo);
- in base a ciò che viene ascoltato attraverso i personal assistant, possono propormi pubblicità di prodotti che possono interessarmi senza che debba neppure cercarli in rete, anticipando i miei desideri;
- creare nostri profili fake e utilizzarli in telefonate e video-chiamate, grazie alle immagini e alle registrazioni della nostra voce che disseminiamo in Rete;
- sapere in anticipo di cosa mi ammalerò, e quanto potrò spendere per curarmi.

La truffa milionaria mediante deep-fake ad Hong Kong

A inizio 2024 è stata riportata una truffa da 25 milioni di dollari perpetrata mediante l'uso di deepfake per simulare una conference call con l'amministratore delegato e il direttore finanziario di una multinazionale con sede a Hong Kong.
Un dipendente dell'azienda è stato ingannato durante una videoconferenza in cui tutti i partecipanti, eccetto lui, erano avatar generati mediante intelligenza artificiale.
Durante la riunione, gli è stato ordinato di trasferire circa 25 milioni di dollari su diversi conti bancari. Il dipendente ha eseguito 15 bonifici prima di insospettirsi e portarlo a contattare (troppo tardi) la sede centrale dell'azienda per verificare.

Daresti a uno sconosciuto i numeri di telefono di tutti i tuoi contatti?

Ce l'hanno insegnato fin da bambini (oltre che il non accettare caramelle dagli sconosciuti): non si danno ad altri i numeri di telefono dei propri conoscenti senza averne prima chiesto il permesso.
Eppure trasferiamo a Meta tutta la rubrica telefonica presente nel nostro smartphone, senza chiedere il permesso a nessuno.
Meta afferma di non trasferire i numeri di telefono ma soltanto i loro hash; tuttavia Meta conosce i numeri di telefono di tutti coloro che hanno installato WhatsApp (oltre a quelli utilizzati come 2FA – autenticazione a due fattori – per gli altri propri servizi, e può ricalcolare gli hash, di fatto risalendo a tutti i numeri.
Naturalmente utilizziamo WhatsApp indistintamente per contatti e comunicazioni personali e professionali, anche se con numeri di telefono diversi, e molto probabilmente sullo stesso smartphone.
Forse non saremmo tanto contenti, se sapessimo che un nostro fornitore avesse accesso completo alla rubrica di tutti i nostri contatti ...

Hai l'autorizzazione degli utenti del tuo sito a farsi profilare?

Praticamente ogni pagina web include link verso gstatic.com, fonts.google.com, googletagmanager.com, googleapis.com, analytics.google.com, etc.
Molte app utilizzano anche i DNS di Google per risolvere i nomi dei siti che vogliamo visitare.
In misura minore, il discorso può essere esteso ad Apple, Meta, X (ex Twitter) e a molte altre aziende.
Sono tutti servizi che avrebbero un costo per chi realizza i siti: spazio disco, backup, maggior necessità di banda per i server, corrente elettrica, sistemisti per installare, aggiornare e manutenere il software di web analytics, e così via.
Tutti costi che si azzerano, se trasferiamo i costi al provider: così a noi non costa niente.
Ma al provider tutti questi servizi costano (e tanto, anche!), e con le nostre scelte progettuali decidiamo a priori che questi costi li pagheranno i visitatori del nostro sito, a loro insaputa.
Certamente avremo pubblicato una bellissima informativa sulla Privacy, ma (sarà una svista?) ci dimentichiamo di dire ai visitatori che stiamo pagando la nostra bolletta della corrente e quella di Internet vendendo i loro dati ...

Per favore, svaligiami la casa!

Nel 2010 si è verificata una impressionante quanto inspiegabile ondata di furti nelle ville dei VIP a Hollywood.
In seguito alle indagini si è scoperto che una banda di ragazzi sfruttava il mondo dei social e dei siti di gossip per verificare quali gioielli le star sfoggiassero in pubblico e dove fossero le loro abitazioni.
Sempre grazie ai social si tenevano aggiornati su dove si trovassero in ogni momento le star, per svaligiare le loro ville quando queste risultavano fuori casa.

Dopo l'accaduto è stato creato il sito ***PleaseRobMe.com***, con lo scopo di dimostrare quanto sia semplice invitare qualcuno a derubarci, sulla base della quantità di informazioni e tracce che seminiamo costantemente in Rete.
Il sito non è più disponibile, ma potete trovarne traccia su Internet Archive e in interessanti articoli pubblicati dalla stampa a inizio 2010.
Analogamente a quanto sopra, è possibile utilizzare le informazioni condivise in rete per geolocalizzare e rapire le persone.

Figura 6 - Home page del sito PleaseRobMe.com

So cosa stai facendo!

Analogamente, nel 2012 uno studente di 18 anni ha realizzato un sito che classificava gli utenti di Facebook in base a cosa stavano raccontando di fare, denominato "We know what you're doing".

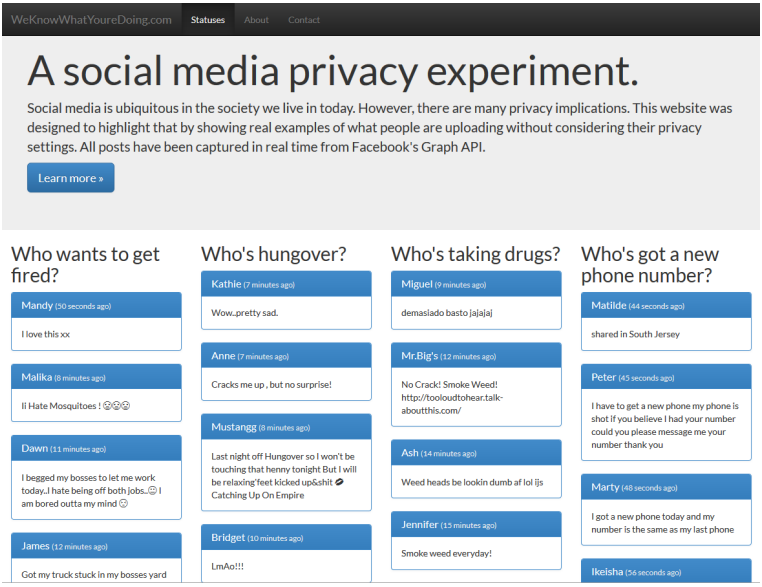


Figura 7 - Home page del sito 'We know what you're doing'

Come fanno a sapere che ti conosco?

Vi è mai capitato di ricevere un suggerimento di amicizia con una persona che non è tra i vostri contatti diretti o indiretti, ma che effettivamente conoscete?
Come è possibile? Vi racconto alcuni metodi, applicati già da anni.
Visto che viene fatto il riconoscimento dei volti (almeno fino al 2021, e vietato o non vietato che sia, è possibile che continuino comunque a farlo), se voi e un'altra persona comparite in una fotografia, è molto probabile che vi conosciate; se entrambi avete un profilo sullo stesso social network, vi verrà probabilmente proposto di chiedere l'amicizia all'altra persona.
In ogni caso c'è sempre qualcuno che vi '*tagga*' in una foto, e il gioco è fatto ...

Inoltre, visto che gli smartphone sono costantemente geolocalizzati, altrettanto accade se frequentate lo stesso luogo negli stessi orari (caffè? a pranzo? in palestra …?):

se ricorrentemente vi trovate negli stessi luoghi e negli stessi orari, è molto probabile che vi conosciate.
È anche possibile che vi conosciate in quanto avete un collegamento attraverso un altro servizio.

Vi siete mai chiesti come mai nel 2014 Mark Zuckerberg (Facebook) abbia speso 19 miliardi di dollari per comperare WhatsApp?
Facebook aveva l'intera rete di contatti attraverso le e-mail con cui gli utenti si registravano, mentre WhatsApp aveva l'intera rete di contatti telefonici delle persone che avevano installato l'app sul proprio smartphone.
Grazie alla correlazione dei dati di questi servizi, Meta può mettere in relazione utenti di Facebook e di WhatsApp, per non parlare di Instagram (comperata nel 2012 per 1 miliardo di dollari).

Facebook ha la sfera di cristallo o qualcuno ci spia?

Non vi è mai capitato di rimanere stupiti per il fatto di veder comparire annunci pubblicitari strettamente attinenti ad argomenti di cui avete parlato con qualcuno poco prima?
Possiamo intuire che se si fanno delle ricerche in Rete o si visitano siti specifici, i sistemi con cui ci interfacciamo possano in qualche modo presumere che ci siano dei prodotti inerenti che possano interessarci.
Ma se lo smartphone non lo abbiamo utilizzato?
Riportiamo un paio di casi reali, anche banali nella loro semplicità, in modo da aiutarvi a fare mente locale su altri casi che vi saranno sicuramente capitati.

Devo riparare lo scaldabagno ...
Due persone sono a pranzo, e una racconta all'altra di un problema sullo scambiatore di calore della propria caldaia, indicandone anche la marca.
Dopo pranzo torna al proprio PC, e inizia a ricevere da Facebook pubblicità di scambiatori di calore per quel modello di caldaia.

Che sia stata magia?

O forse è stato l'assistente personale, sempre attivo nel telefono di ciascuno, che ha reso disponibile quest'informazione a Facebook, anche se non esplicitamente interrogato?
Così discreti, così comodi … chissà quante altre cose avranno ascoltato questi 'assistenti personali', nei giorni, mesi o anni di utilizzo ...

Perché devo andare in vacanza dove vai tu?
Due amici sono in giardino, e iuno racconta all'altro di avere intenzione di andare in vacanza in Islanda.
I due sono amici su Facebook, e dopo poco il secondo inizia a ricevere pubblicità di vacanze in Islanda …
Nota bene: Facebook non ha presentato queste pubblicità a tutti gli amici del primo, ma soltanto a quello che era presente mentre il primo raccontava delle sue intenzioni.
O Facebook ha una sfera di cristallo, oppure in qualche modo sapeva che queste due persone erano insieme mentre parlavano dell'argomento.
Non viene da porsi qualche domanda …?

Siri ci ascolta? Apple nega

Tuttavia nel 2025 Apple paga 95 milioni di dollari per chiudere una class action per l'utilizzo scorretto dell'assistente vocale Siri.
E nel 2023, Amazon ha pagato più di 30 milioni di dollari alla Federal Trade Commission degli Stati Uniti per aver violato la privacy con le sue telecamere Ring Doorbell e l'assistente digitale Alexa.

Gli agenti AI ci semplificano la vita?

I servizi di AI di oggi sono '*solo*' dei motori di ricerca molto evoluti; il problema è che vengono alimentati non soltanto con tutto ciò che riescono a rastrellare in Rete (legalmente o meno), ma anche con tutto ciò che gli chiediamo e raccontiamo.
L'incredibile semplicità con sui si può interagire con i modelli di AI e la qualità delle risposte che forniscono ci porta a trasferire in Rete una quantità sempre maggiore di informazioni e sempre più personali o riservate.
Ogni volta che chiediamo la revisione di una lettera, di un curriculum, o che chiediamo la stesura di un pezzo di codice di un programma, rischiamo di raccontare anche fatti personali nostri e dei nostri clienti, oltre che anticipare indiscrezioni su programmi e prodotti che stiamo realizzando.
Può capitare di includere password, chiavi di identificazione, dati personali, immagini nostre o di altri, e anche materiale riservato o coperto da copyright.
Recentemente è stata resa disponibile anche la possibilità di effettuare acquisti e prenotazioni di viaggi, e per farlo occorre memorizzare carte di credito e dati anagrafici.
Senza contare i milioni di persone che chiedono all'IA un supporto religioso, medico e psicologico, la previsione del futuro, o addirittura di poter parlare con i propri cari defunti.

Il problema è che tutto ciò che inseriamo (e anche le risposte che riceviamo) viene riutilizzato per riaddestrare l'AI. Tutto. E potrà essere riutilizzato per elaborare risposte per altri.
E la tendenza è quella di inserire l'AI in tutti i PC, browser, app, smartphone, dispositivi indossabili e apparecchi domòtici con il buon proposito di semplificarci la vita. Con la contropartita di raccontare e 'far digerire' tutta la nostra vita ai loro produttori.

Sanzioni (visto che non ci proteggiamo da soli!)

È impensabile elencare qui le sanzioni comminate negli ultimi anni dalle varie autorità garanti per la Privacy, soprattutto a livello europeo, ma anche nel resto del mondo.
Tuttavia è utile evidenziare che svariate sanzioni superano il miliardo di Euro, e molte ammontano a centinaia di milioni (senza contare le innumerevoli di importo inferiore).
Nonostante ciò, finché queste sanzioni saranno inferiori agli utili generati con lo sfruttamento dei dati degli utenti, converrà sempre pagare e proseguire, aggirando le regole.

Il principio di Pareto, ovvero: spendete bene i vostri soldi!

E per concludere, dedichiamo un paragrafo essenzialmente alle aziende, che sono ormai costrette a fare i conti con la Cybersecurity per motivi di conformità normativa e per la propria sopravvivenza.
Nel 1897 Vilfredo Pareto, uno dei maggiori economisti italiani, osservò che la maggior parte degli effetti è dovuta a un numero ristretto di cause, da cui derivò empiricamente la cosiddetta "legge 80/20".

Dal punto di vista aziendale, questo principio porta a due considerazioni:

- pochi incidenti informatici possono causare grandi danni;
- con poca spesa ci si può proteggere da molti attacchi.

Andando ad analizzare le cause di moltissimi attacchi andati a segno e che hanno avuto serie conseguenze per le aziende, sia in Italia che all'estero, si osserva che il principale vettore di attacco è l'utente.

Una buona formazione e una buona gestione dei sistemi già utilizzati in azienda potrebbero quindi spostare l'asticella molto più in alto per gli attaccanti.

La parola chiave è '*consapevolezza*': ogni persona, dall'ultimo dei dipendenti e consulenti fino all'amministratore delegato, deve comprendere che un suo errore può costare molto caro all'azienda.
I prodotti pensati per proteggere la vostra azienda dagli errori del personale e da voi stessi hanno costi elevati, soprattutto in termini di complessità, configurazione, gestione e monitoraggio.
È quindi molto più efficace spendere 4 Euro in organizzazione, formazione e informazione per ogni Euro che spendete di tecnologia (legge 80/20).
E per finire, qualche compito da svolgere a casa …!

Probabilmente si continuerà a utilizzare gli stessi programmi e le app, forse con qualche dubbio latente, ma niente che spinga veramente a vedere se esistano alternative ai programmi a cui ci siamo ormai abituati.
La fretta di installare la nuova app di grido probabilmente non ci darà il tempo di ascoltare il grillo parlante che abbiamo risvegliato.

Una piccola sfida per chiunque (inclusi genitori, docenti e responsabili per la protezione delle informazioni in azienda) può essere quella di leggersi:

- la 'cookie policy' del sito web del quotidiano online più letto;
- la politica per la privacy del motore di ricerca più utilizzato;
- la politica per la privacy dell'app più utilizzata.

Un bel 10 a tutti coloro che riusciranno a portare a termine il compito assegnato, e tutti coloro che ne avranno anche compreso le implicazioni per la propria vita personale e per il business della propria azienda riceveranno anche lode ed encomio!

Crediti fotografici

p. 202 - pixabay.com, credits: Peggy Marco
p. 204 - flickr.com, credits: xploitme, CC-BY-SA 2.0
p. 206 - flickr.com, credits: Magnus Johansonn, CC-BY-SA 2.0
p. 216 - commons.wikimedia.org, German Federal Archives, CC-BY-SA 3.0
p. 223 - pixabay.com, credits: geralt
p. 223 - flickr.com, CC-BY 2.0
p. 224 - pixabay.com, credits: Peggy Marco

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phishing***.
Account take-over	Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).
ACDC (Advanced Cyber Defence Center)	Progetto europeo la cui finalità è offrire soluzioni e creare conoscenza per aiutare le organizzazioni in tutta Europa a combattere le botnet. (www.acdc-project.eu/).
AI agentica	Tipologia di sistemi basata su autonomia operativa, contestualizzazione avanzata e capacità decisionali sviluppate su più livelli.
AISP (Account Information Service Provider)	Prestatori di servizi di informazione sui conti di pagamento che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti.
Agentive AI	AI in grado di prendere decisioni e agire in modo autonomo perseguendo uno specifico obiettivo.
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.
APA (Attack Path Analysis)	Tecnica utilizzata nel campo della sicurezza informatica per identificare e valutare i percorsi potenziali attraverso i quali un attaccante potrebbe violare un sistema o una rete.
Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e malware sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.

Arbitrary File Read	Vulnerabilità che consente ad un attaccante di accedere a file tramite richieste Web remote.
Assume breach	Approccio secondo cui gli operatori di sicurezza partono dal presupposto che, prima o poi, un attacco andrà a buon fine, e dunque strutturano processi, strumenti e competenze per rilevare, investigare e contenere rapidamente qualsiasi compromissione.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
BEC fraud (Business e-mail compromise)	Tipi di attacco phishing mirati verso figure aziendali al fine di convincere le vittime a trasferire somme di denaro o rilevare dati personali. (Vedi anche ***CEO fraud***)
BITS Jobs (Background Intelligent Transfer Service)	Tecnica che consente ai cybercriminali di programmare ed eseguire download malevoli in background senza destare sospetti.
Blocj	Tecnica utilizzata nell'ambito dell'***e-voting***. Con la firma elettronica cieca (blind signature) la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna.
Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi ***DDOS.***
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo ***DDOS***.

Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
CAL (Cybersecurity Assurance Level)	Indicatore dinamico dello sforzo necessario per garanzia la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale.
Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CDR (Cloud Detection and Response)	Approccio alla sicurezza che nasce per fornire ai team di SecOps, in particolare SOC (Security Operations Center) e IR (Incident Response), le capacità di cui hanno bisogno per monitorare, individuare e bloccare attacchi specifici per il Cloud.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.
CERT (Computer Emergency Response Team)	Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT (vedi CERT Nazionale): • fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; • incrementare la consapevolezza e la cultura della sicurezza; • cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione; • facilitare la risposta ad incidenti informatici su larga scala; • fornire supporto nel processo di soluzione di crisi cibernetica.

CFC (Cyber Fusion Center)	Approccio olistico e multidisciplinare alla gestione della sicurezza che mira a superare la tradizionale suddivisione fra compiti (intelligence, analisi, risposta…) e team.
CLOSINT (Close Source Intelligence)	Processo di raccolta di informazioni attraverso la consultazione di fonti chiuse, cioè non accessibili pubblicamente: intelligence feed, fonti governative, informazioni classificate, etc.
Cloud weaponization	Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
CNAPP (Cloud-Native Application Protection Platform)	Categoria di soluzioni che riunisce diverse funzionalità di sicurezza in un'unica piattaforma, per proteggere le applicazioni in cloud.
CNOs (Computer Network Operations)	Tipologia di ***Information warfare*** finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.
CNP (Card-Not-Present)	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.
CoA (Courses of Action)	Nella dottrina militare identifica un piano che descrive le strategie e le azioni operative scelte per portare a termine una determinata missione. Nell'ambito della ***Cyber Intelligence*** rappresenta le attività poste in essere rispettivamente dagli attaccanti o dai difensori per la conduzione o il contrasto delle azioni funzionali ad un attacco cyber.
Constituency	Nell'ambito di un ***CERT*** indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).

Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione, ma con dei limiti, oppure richiedere verifiche aggiuntive.
C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la ***botnet***, al fine di rendere più difficile la localizzazione di questi ultimi.
Counterintelligence	Identificazione, valutazione, neutralizzazione e sfruttamento delle attività di intelligence svolte da entità avversarie.
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: due azioni passive: Discover e Detect cinque attive - Deny, Disrupt, Degrade, Deceive, Destroy).
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.
Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.

CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito ***IRU*** a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.
CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. (https://www.first.org/cvss/specification-document)
CTI (Cyber Threat Intelligence)	Disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri asset e sviluppare azioni di contrasto efficaci. In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.

Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.
Cyber-reasoning systems	Sistemi sviluppati per individuare automaticamente le vulnerabilità delle reti più complesse implementando algoritmi cognitivi.
Cyber-weapon	***Malware*** (o anche hardware) progettato o utilizzato per causare danni attraverso il dominio cyber. (NATO Cooperative Cyber Defence Centre of Excellence).
CYBINT (Cyber Intelligence)	Disciplina che trae origine dalla declinazione classica delle attività di intelligence con riferimento alle peculiarità del dominio di ricerca informativa in ambito cyber. L'attività CYBINT si evolve includendo attività di analisi strategica e analisi di contesto su trend di eventi, scenari geopolitici e previsionali.
Data Leakage	Trasferimento non autorizzato di informazioni riservate.
DDoS (Distributed Denial of Service)	Attacchi ***DOS*** distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
Debunking	Insieme di attività volte a verificare se il contenuto, ad esempio di un file multimediale, sia falso.
Deep Fake	Algoritmi di deep learning in grado di creare foto o video falsi.
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni ***malware*** per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server ***C&C***.
Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. (Adversary, Infrastructure, Victim, Capability).

Digital Scarcity	In una ***blockchain*** la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
DMARC (Domain-based Message Authentication, Reporting and Conformance	Standard di autenticazione delle e-mail che aiuta a prevenire la falsificazione del mittente (spoofing) e il phishing.
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il ***protocollo***, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo ***DDOS*** amplificati.
DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai ***DNS.***
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di ***C&C*** si parla di ***DDOS*** (Destribuited Denial of Service).

Double extortion	Attacchi ransomware che, oltre a cifrare i file, ne fanno anche una copia di "sicurezza" con il loro trasferimento sui computer dei cyber criminali minacciando di procedere alla loro diffusione pubblica e/o metterli all'asta nel dark web per la vendita al miglior offerente.
Downloader	Software deputati a scaricare ulteriori componenti malevoli dopo l'infezione iniziale.
Drive-by exploit kit	Il fenomeno dei drive-by ***exploit kit*** è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli ***exploit kit***, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.
DRdos (Destribuited Reflection Denial of Service)	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di ***DDOS*** permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del ***protocollo NTP***.
Dropper	Codice che installa il ***malware*** sul computer della vittima.
Eavesdropping	Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni
eBPF (Extended Berkeley Packet Filter)	Tecnologia integrata nel kernel di Linux, che consente di monitorare e filtrare il traffico di rete in tempo reale senza impattare negativamente sulle prestazioni, offrendo un livello di protezione granulare e adattivo, capace di rispondere automaticamente ai cambiamenti dell'infrastruttura.
EDR (Endpoint Detection and Response)	Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.

Enterprise Architecture	Sistema informativo che, raccogliendo dati da tutte le funzioni dell'organizzazione, li collega in un unico modello informativo consentendo di visualizzare complessivamente lo stato dell'organizzazione e contemporaneamente di immaginarne la possibile evoluzione futura, rinforzandone la capacità di reagire ad eventi esterni.
Evasion	Nell'ambito delle applicazioni di IA attacco che consiste nel confondere la classificazione del dato in ingresso, da parte di un algoritmo precedentemente addestrato, manipolandone il contenuto.
Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le ***vulnerabilità*** note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Facing applications	Applicazioni rivolte al pubblico, quali ad esempio siti web.
Fast flux	Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.
Ghost broking	Pratica secondo la quale il frodatore, spacciandosi per agente di un'impresa assicurativa, a seguito del pagamento di un "premio" rilascia al cliente una polizza assicurativa, ovviamente falsa.
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.

Hate speech	Il Comitato dei ministri del Consiglio d'Europa definisce gli hate speech come le forme di espressioni che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o più in generale l'intolleranza, ma anche i nazionalismi e gli etnocentrismi, gli abusi e le molestie, gli epiteti, i pregiudizi, gli stereotipi e le ingiurie che stigmatizzano e insultano. RECOMMENDATION No. R (97) 20 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON "HATE SPEECH" - Adopted by the Committee of Ministers on 30 October 1997
Harvest now, decrypt later	Tecnica che consiste nel raccogliere i dati crittografati per una successiva decrittazione, quando la potenza di calcolo quantistico diventerà più accessibile.
Hit & Run (o Pulse wave)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).
Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.
HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.

HUMINT (HUMan INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Kill Switch	Termine generico per indicare un dispositivo che serve a bloccare in modo forzato un'attività.
IBAN Swapping	Sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
ICS (Industrial Control System)	Sistemi di controllo industriale.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IGA (Identity Governance & Administration)	Strumento di governance ed amministrazione delle identità che aiuta a garantire un provisioning, un re-provisioning ed un deprovisioning accurato dell'accesso degli utenti.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile
IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
IoB (Internet of Bodies)	IoT applicato ai sistemi biologici. Dispositivi che raccolgono dati biometrici, fisiologici e comportamentali.
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.

Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Infostealer	***Malware*** finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Instant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.
Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
Intrusion software	***Spyware*** (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti ***dual use***). Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.
IoA (Indicatori di attacco)	Informazioni funzionali all'individuazione di un potenziale attacco anche prima che ci sia contatto diretto tra attaccante e attaccato.
IoC (Indicatori di compromissione)	Qualsiasi informazione che possa essere utilizzata per cercare o identificare sistemi potenzialmente compromessi (indirizzo IP/nome dominio, URL, file hash, indirizzo email, X-Mailer…) (Common Framework for Artifact Analysis Activities – ENISA)
IP Fragmentation	Tipo di attacco ***DDOS*** (Destribuited Denial of Service) che sfrutta il principio di frammentazione del protocollo IP.

IPMI (Intelligent Platform Management Interface)	Specifica di una interfaccia di basso livello utilizzata da diversi costruttori che consente ad un amministratore di sistema di gestire server a livello hardware. Attraverso la BMC (Baseboard Management Controller) consente, tra le altre cose, l'accesso al BIOS, ai dischi ed ai dispositivi hardware in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
ITDR (Identity Threat Detection and Response)	Insieme di strategie, processi, tecnologie utilizzati per rilevare, analizzare e rispondere alle minacce che prendono di mira le identità digitali.
Jamming	Interferenza intenzionale o volontaria di un segnale elettromagnetico al fine di disturbare, bloccare o impedire la ricezione corretta del segnale da parte dei dispositivi destinatari.
LOTL (Living Off The Land)	Tipo di attacco basato su strumenti nativi preinstallati nel sistema operativo.
LOTS (Living Off Trusted Sites)	Tecnica di attacco che permette agli attori di sfruttare strumenti presenti nei sistemi attaccati per eseguire attività malevole senza essere scoperti.
MAAS (Malware as a Service)	Modello di erogazione del codice malevole dove un team di esperti "produce" malware, sviluppa exploits e si occupa della loro ricerca e sviluppo, mentre una catena di distributori si occupa di procacciare i clienti.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Meaconing	Interferenza con i segnali di navigazione, come quelli provenienti dai sistemi GPS, al fine di alterare le informazioni di posizione e indirizzare in modo errato i dispositivi di navigazione o di localizzazione.

Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.
MFA (Multi-Factor Authentication)	Autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
MFU (Malicious File Upload)	Attacco ad un web server basato sul caricamento remoto di ***malware*** o più semplicemente di file di grandi dimensioni.
Mining	Creazione di nuova criptovaluta attraverso la potenza di calcolo degli elaboratori di una ***blockchain***.
MitC (Man in the Cloud) *Definizione coniata dall'azienda Imperva*	Tipo di attacco nel quale la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.
Mules	Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.
NTP (Network Time Protocol)	***Protocollo*** che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.
OF2CEN (On line Fraud Cyber Centre and Expert Network)	Piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è il progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. (https://www.poliziadistato.it)

OPSEC (Operation Security)	Processo mediante il quale, durante un'operazione di intelligence, si previene l'esposizione involontaria di informazioni sensibili/riservate/classificate riguardanti le proprie attività, intenzioni o capacità.
Oracoli	Fonti esterne (API di un sito, output di un oggetto IoT…) alla ***blockchain*** per alimentare uno smart contract e scatenarne o influenzarne l'esecuzione.
OSINT (Open Source INTelligence)	Attività di intelligence tramite la consultazione di fonti aperte di pubblico accesso.
OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio e alla gestione di asset fisici in ambito industriale, trasporti…
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una ***botnet***, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.

Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PIR (Priority Intelligence Requirements)	Requisiti informativi che orientano le priorità nella pianificazione delle attività di intelligence.
Plausible Deniability	Capacità di un soggetto, in genere in posizione gerarchica elevata, di negare di essere a conoscenza di azioni dannose commesse da soggetti di livello più basso, in assenza di prove che possano dimostrare il contrario.
Poisoning	Nell'ambito delle applicazioni di IA attacco che consiste nel contaminare i dati di addestramento per impedire al sistema di funzionare correttamente.
Port Sweeping	Scansione di vari sistemi alla ricerca di una specifica porta in ascolto.
Pretexting	Tecnica di ingegneria sociale nella quale l'attaccante usa una storia inventata, ad esempio una carta di credito bloccata, per carpire la fiducia della vittima e manipolarla fino a farle condividere informazioni sensibili, scaricare malware, inviare denaro a criminali o arrecare danni alla propria organizzazione.
PSYOPs (Psychological Operations)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Pulse Wave (o Hit & Run)	***Hit & Run (o Pulse wave)***
QKD (Quatum Key Distribution)	Tecnologia che utilizza i principi della meccanica quantistica per creare canali di comunicazione sicuri; permettendo di condividere chiavi crittografiche con totale sicurezza, poiché qualsiasi tentativo di intercettazione verrebbe immediatamente rilevato.
QTSP (Qualified Trust Service Provider)	Un ***prestatore di servizi fiduciari*** che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.

Quishing/QRishing	Tecnica di attacco che utilizza QR code malevoli per indurre le vittime a visitare siti web fraudolenti o scaricare malware.
Ransomware	***Malware*** che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l'accesso al dispositivo (locker-ransomware).
RDP (Remote Desktop Protocol)	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server).
Resilienza	"La capacità di un'organizzazione di assorbire gli shock e di adattarsi ad un contesto in continua evoluzione". Definizione da ISO 22316:2017
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.
Retrieving data	Fase di ricerca e raccolta dei dati relativi all'obiettivo individuato durante un'attività ***OSINT***. In questa fase gli analisti sfruttano i motori di ricerca, scandagliano i siti web alla ricerca di documenti di interesse avendo cura di conservare ogni traccia raccolta come ad esempio testi, URL, video, immagini, documenti, etc.
Rootkit	***Malware*** che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
SASE (Secure Access Service Edge)	Approccio alla sicurezza attraverso il modello Zero-Trust, dove ogni accesso è rigorosamente controllato per garantire che solo utenti e dispositivi autorizzati possano accedere alle risorse aziendali.
SAST (Static Application Security Testing)	Analisi statica del codice finalizzata alla individuazione di vulnerabilità.
SBOM (Software Bill of Materials)	Inventario "nested" di tutti i prodotti software e relativi componenti e fornitori presenti all'interno dell'azienda.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.

Security Architecture (NIST)	Insieme di rappresentazioni logiche e fisiche di un'architettura di sistema rilevanti dal punto di vista della sicurezza, che raccoglie le informazioni su come il complessivo sistema sia organizzato in domini di sicurezza, e ne fa uso per rinforzare le policy che prescrivono come dati ed informazioni debbano essere protetti all'interno di un dominio di sicurezza e nelle relazioni tra i domini.
Self-sovereign Identity	Modello di identità digitale dove la gestione dei dati non è affidata a provider esterni o Identity Provider, ma lascia agli utenti il pieno controllo sui propri dati.
Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.
SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
SIGINT (SIGnals INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la COMINT e la ELINT. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.
SMB (Server Message Block)	Protocollo per la condivisione di file e stampanti nelle reti locali. Se esposto su internet può essere utilizzato per accedere a documenti e file condivisi.
Smoking Guns	Termine che indica una prova (quasi) certa dell'aver commesso un crimine.

SOAR (Security Orchestration Automation and Response)	Approccio che consente di orchestrare le tecnologie di sicurezza al fine di avere una gestione il più possibile automatizzata della raccolta, analisi e risposta agli eventi di sicurezza.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
SOCMINT (Social Media Intelligence)	Ramo dell'Open Source Intelligence specificatamente dedicato alla raccolta di informazione attraverso i social network.
SOP (Standard Operating Procedure)	Procedure operative standard che indicano i passi da seguire durante la conduzione di indagini ***OSINT***, consentendo di rendere efficiente l'esecuzione di operazioni ripetitive e di ottenere uniformità nelle prestazioni, nella qualità degli output ed evitando il mancato rispetto di standard e normative di settore, eventualmente imposte dalla propria organizzazione.
Spear phishing	***Phishing*** mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	***Malware*** che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SL-A (Security Level - Achieved)	Livello di sicurezza effettivamente raggiunto.
SL-T (Security Level-Target)	Livello di sicurezza richiesto.

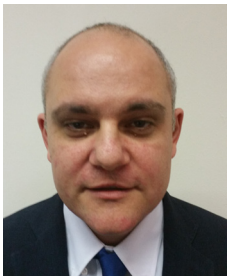
SSDLC (Secure Software Development Life Cycle)	Programma che indirizza la sicurezza sin dalle prime fasi di progettazione di un'applicazione software e non si conclude con la fase di delivery, ma segue tutto il ciclo di vita dell'applicazione.
SSDP (Simple Service Discovery Protocol)	***Protocollo*** che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	***Protocollo*** cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
SSPM (Security Posture Management)	Soluzioni di sicurezza per ambienti SaaS che garantiscono un monitoraggio costante delle impostazioni di sicurezza, delle autorizzazioni degli utenti, delle connessioni esterne…, permettendo alle organizzazioni di individuare e intervenire rapidamente su possibili rischi.
Steganografia	Tecnica che consiste nel nascondere una informazione all'interno di un media (immagine, video, file audio…). Un attacco basato su tale tecnica può nascondere, ad esempio, un malware all'interno di file multimediali.
STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo ***TAXII.***
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
TARA (Threat Analysis Risk Assessment)	Metodologia utile per dettagliare tutti i possibili threat a cui un prodotto può essere soggetto e assegnare un rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.
TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante ***STIX***.

TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del ***protocollo NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
TLP (Traffic Light Protocol)	Protocollo per facilitare la condivisione delle informazioni "sensibili" che definisce il grado di possibile diffusione (red, amber, green, white) stabilito dalla controparte inviante.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
Tradecraft	Combinazione di metodi, capacità e risorse che un attaccante sfrutta nel compimento delle proprie azioni.
TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come ***prestatore di servizi fiduciari qualificato*** o come prestatore di servizi fiduciari non qualificato.

UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sistema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
UDP Flood	Il ***protocollo*** UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	***Protocollo*** di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.
Vetting	Il processo di identificazione dei partecipanti ad una ***blockchain***.
VHUMINT (Virtual Human Intelligence)	Estensione al mondo virtuale del concetto di Human Intelligence, cioè di una metodologia investigativa imperniata sulla raccolta di informazioni per mezzo di contatti interpersonali. Attraverso la VHUMINT vi è dunque l'interazione proattiva con gli attori della minaccia al fine di raccogliere informazioni di contesto necessarie a mitigare efficacemente la minaccia.
Vishing	Variante "vocale" del ***phishing***.
Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Weaponization	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.

Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.
WEF Quantum Readiness Toolkit	Kit che fornisce cinque principi per aiutare le organizzazioni a prepararsi per l'economia quantistica sicura, valutando la loro prontezza quantistica e identificando le azioni prioritarie.
Whaling	Letteralmente "caccia alla balena"; è un'ulteriore specializzazione dello ***spearphishing*** che consiste nel contattare una persona interna all'azienda spacciandosi per un dirigente della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è l'amministrazione con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
Wiper	Tipologia di virus che hanno come unico scopo quello di distruggere il sistema target (IT e OT).
XDR (Extended Detection and Response)	Dispositivi che integrano tutte le componenti della soluzione di sicurezza in un'unica piattaforma di individuazione (detection) e risposta agli incidenti (Incident Response) portando l'intelligenza di protezione fino al terminale del dipendente, sia esso un computer o uno smartphone.
XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.
Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.
Zoom bombing	Irruzione virtuale in una videoconferenza finalizzata a creare disturbo.

Gli autori del Rapporto Clusit 2025 - Edizione di ottobre



Mauro Andreolini è ricercatore universitario presso l›Università di Modena e Reggio Emilia. Svolge ricerca negli ambiti della Sicurezza Informatica (con particolare riferimento all›automazione delle operazioni offensive e difensive) e dei Sistemi Operativi, con oltre 50 pubblicazioni internazionali. È docente titolare degli insegnamenti «Sistemi Operativi» (LT) e «Sviluppo di Software Sicuro» (LM). È responsabile di Ateneo per l›iniziativa CyberChallenge.it.

Antonio Apruzzese, Prefetto, con laurea in Giurisprudenza, è stato Direttore della Polizia Postale e delle Comunicazioni dal 2009 al 2015. Impegnato nel contrasto dei crimini informatici, ha sperimentato innovativi modelli di investigazione portando a definizione un complesso progetto europeo denominato OF2CEN (On-line Fraud Cyber Centre and Expert Network) per la tutela transnazionale di servizi bancari on line impostata su una innovativa partnership pubblico/privato tra primari gruppi bancari e Forze di Polizia specializzate europee. Ha inoltre ricoperto ruoli di rilievo istituzionale nel settore, tra cui quello di rappresentante del Ministero dell'Interno nel Tavolo Tecnico di supporto del CISR (Comitato Interministeriale per la Sicurezza della Repubblica) per la definizione della nuova architettura nazionale in tema di cyber sicurezza. Attualmente svolge attività di consulenza per primarie realtà pubbliche e private tra cui l'Automobile Club d'Italia per la gestione e la sicurezza di interconnessioni tra banche dati istituzionali. È altresì Docente di Criminalità Informatica presso l'Università di Modena e Reggio Emilia, e relatore in numerosi convegni sulle problematiche della sicurezza informatica e dei processi di digitalizzazione, con attività di pubblicazione scientifica. È membro del Collegio dei Probiviri e del Comitato Scientifico del Clusit.

Luca Bechelli, Information & Cyber Security Advisor, è Partner in P4I - Digital360, dove ha contribuito a fondare e gestisce l'area di IT & Cybersecurity Governance. Svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Security Governance, Risk Management, Data Protection, Privilege Management, Cryptography, Incident Handling, Crisis Management, OT Security, IT Compliance e Application Security. Ha operato, tra gli altri, nei settori delle telecomunicazioni, bancario, assicurativo, difesa, aerospaziale, retail e grande distribuzione, manifacturing, trasporti, navale, sanità, pubblica amministrazione centrale e locale, andando di volta in volta a calare gli standard e le best practice della cybersecurity nell'ambito delle regolamentazioni e delle esigenze operative degli specifici mercati, prima come libero professionista e in collaborazione con grandi firme della consulenza, fino al 2017 con l'attuale impegno in P4I. Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha partecipato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore, ed ha contribuito alla stesura di standard, normative e linee guida tecniche in materia di sicurezza delle informazioni. Dal 2007 è membro del Consiglio Direttivo e del Comitato Scientifico del Clusit. Dal 2017 è Senior Advisor presso l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, supportando il coordinamento e la redazione di linee guida e pubblicazioni nell'ambito di gruppi di lavoro. Dal 2023 coordina il team per l'elaborazione e la stesura dei dati del Rapporto Clusit.

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Referente Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT.

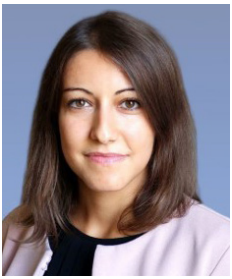
Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 170 corsi e seminari tenuti presso ISACA/ AIEA, ORACLE/CLUSIT, ITER, Informa Banca, CONVENIA, CETIF, IKN, Università di Milano, CEFRIEL, Ca Foscari, Università degli Studi Suor Orsola Benincasa, ABI…; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei. Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate. Ha pubblicato 30 fra libri e white paper alcuni dei quali utilizzati come

testi universitari; ha partecipato alla redazione di 31 opere collettive nell'ambito di ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT. Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di ACFE, di DFA e del BCI e partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni (LA BS 7799), (LA ISO IEC 27001:2005/2013/2022), (LA ISO 20000-1), (LA ISO 22301), (LA ISO IEC 42001), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI.

Georgia Cesarone è Responsabile Innovazione e Formazione del Centro di Competenza START 4.0. È Consigliere Segretario dell'Ordine degli ingegneri di Genova, Presidente del Club per Tecnologie dell'Informazione CTI Liguria e Vicepresidente FIDA Inform (Federazione Nazionale delle Associazioni Professionali di Information Management). Membro del CdA e Vicepresidente di IIC (Istituto Internazionale delle Comunicazioni). Ingegnere elettronico con un master di secondo livello in Trasferimento tecnologico, imprenditorialità e innovazione nei settori dell'alta tecnologia. È innovation manager riconosciuto dal Ministero dello Sviluppo Economico e Project Manager certificato. Fondatrice di due start-up innovative, con un forte background nell'elettronica hardware e nella gestione di progetti di R&I, negli ultimi anni si è concentrata sull'introduzione delle tecnologie e lo sviluppo delle competenze che abilitano la trasformazione digitale nelle aziende.

Luca Chiantore è Direttore Generale dell'Università di Modena e Reggio Emilia, Ingegnere Informatico, esperto di informatica forense, smart city e tecnologie biomediche. Ha ricoperto incarichi di dirigente dei sistemi informativi presso aziende sanitarie pubbliche, è stato dirigente del settore "Smart city, servizi demografici e partecipazione" del Comune di Modena e Responsabile della Transizione Digitale dell'Ente. Si occupa di trasformazione digitale e pianificazione delle politiche di cyber security nelle aziende pubbliche. Collabora ad importanti progetti in ambito automotive.

Mauro Cicognini, parte del team che ha fondato Rexilience nel 2021, si occupa di ICT dal 1989 e di cybersecurity dal 1996. Ha lavorato in aziende dei servizi e dell'alta tecnologia (software, systems integration, telecomunicazioni, automazione industriale), progettando e gestendo software, servizi e reti ICT in realtà che spaziano dalla multinazionale alla PMI. Le sue aree di responsabilità hanno toccato Europa, Africa, Sud America e Medio Oriente; parla inglese, italiano, spagnolo e francese. Interviene sui media nazionali e di settore, ed ha tenuto sessioni su IoT, sul GDPR, sulla Business Continuity, sulla sicurezza fisica, e così via. La sua attività convegnistica è rivolta sia agli specialisti di settore sia, a livello divulgativo, alle scuole ed alle iniziative civiche. Dal 2019 è docente presso il Cefriel – Politecnico di Milano nell'ambito del Corso di Alta Formazione per DPO. Ha fatto parte del Comitato Direttivo e poi del Comitato Scientifico di Clusit ininterrottamente dal 2006. Si è laureato nel 1995 al Politecnico di Milano in ingegneria elettronica (indirizzo bioingegneria), ed ha conseguito nel 2009 un "Executive Certificate in Management and Leadership" presso il Massachussetts Institute of Technology.



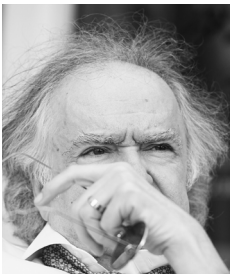
Giorgia Dragoni, Ricercatrice Senior dell'Osservatorio Cybersecurity & Data Protection e Direttrice dell'Osservatorio Digital Identity del Politecnico di Milano, si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e cybersecurity. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection e dei Big Data Analytics e dal 2020 è Direttrice dell'Osservatorio Digital Identity. Nel 2022 ha conseguito l'Executive Master in Management presso la Polimi Graduate School of Management. È membro del Comitato Scientifico del Clusit e delle Women for Security.

Cinzia Ercolano, Fondatrice e amministratore delegato di Astrea, agenzia nata e cresciuta nel mondo della tecnologia e, in particolare, della Sicurezza Informatica, si occupa del format del Clusit "Security Summit", uno degli eventi di Sicurezza Informatica di riferimento in Italia da oltre 15 anni. Dal 2015 si occupa attivamente della comunicazione del CLUSIT, coordinando le attività di ufficio stampa, social media e relazioni con le aziende. Nel 2020 ha ideato e creato, insieme ad un gruppo di specialiste della cybersecurity, Women For Security, community tutta al femminile, che si pone l'obiettivo di mettere a fattor comune le competenze delle donne in ambito information security. Partecipa a diversi eventi di divulgazione del digitale in generale e della cybersecurity in particolare verso le nuove generazioni, inoltre contribuisce con la community a sostenere le campagne di diffusione delle discipline STEM e delle professioni cyber verso il mondo femminile in particolare e adolescenziale in generale.

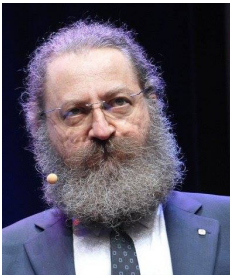
Gabriele Faggioli, legale, è amministratore delegato di Partners4Innovation- società del gruppo Digital360, Presidente Onorario del Clusit e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Gabriele inoltre è Adjunct Professor della Graduate School of Management – Politecnico di Milano ed è stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea.

Ivano Gabrielli, laureato in Giurisprudenza e Scienze Politiche con il massimo dei voti, master in Scienze della Sicurezza e master in Homeland Security, è nella Polizia Postale dal 2006. Ha diretto prima il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) e successivamente la III Divisione del Servizio Polizia Postale (CNAIPIC e Cyber-terrorismo). Nel gennaio 2022 è stato nominato Direttore del Servizio Polizia Postale e delle Comunicazioni. Dal luglio 2024, nominato Dirigente Superiore della Polizia di Stato, ha assunto l'incarico di Direttore del Servizio Polizia Postale e per la sicurezza cibernetica, incardinato nella neoistituita Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, che ha ereditato anche le storiche competenze del Servizio Polizia Postale e delle Comunicazioni.

Paola Girdinio è professore ordinario di elettrotecnica presso l'Università degli Studi di Genova, è stata preside della facoltà di ingegneria e membro del consiglio di amministrazione di Ateneo. È stata consigliere di amministrazione di Enel, di Ansaldo STS, , del Distretto ligure delle tecnologie marine, di Banca Carige, della società D'Appolonia, di Fondazione Carige, di Banca Popolare di Bari, ricopre attualmente analogo incarico in Ansaldo Energia, Ansaldo Nucleare, in Wsense, in Fondazione Costa Crociere e in Fondazione Amga. È presidente del Centro di Competenza sulla sicurezza e ottimizzazione delle infrastrutture strategiche 4.0 e presidente dell'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici. L'attività di ricerca di Paola Girdinio riguarda i settori della superconduttività applicata, dei materiali dielettrici a basse temperature, del calcolo di campi elettrici e magnetici con metodi numerici e della progettazione assistita da calcolatore di dispositivi elettrici e magnetici, compatibilità elettromagnetica industriale, cybersecurity per le infrastrutture.



Paolo Giudice è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto a interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.



Corrado Giustozzi, membro del Comitato Scientifico di Clusit, è fondatore e senior partner di Rexilience. Già esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale/ CERT-AGID (2015-2020) con la responsabilità dello sviluppo del CERT della Pubblica Amministrazione, già membro (mandati 2010-12, 2012-15, 2015-17 e 2017-20) dell'Advisory Board dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). In oltre trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti

di audit ed assessment, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni. Ha collaborato per oltre venti anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del cybercrime e del cyberterrorismo. Ha partecipato a progetti internazionali di contrasto alla cybercriminalità e al cyberterrorismo con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) e l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). È docente in numerosi Master Universitari. Giornalista pubblicista e membro dell›Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un›intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri. L'Università di Roma Tor Vergata gli ha conferito la laurea magistrale honoris causa in Ingegneria di Internet e delle Tecnologie per l'Informazione e la Comunicazione.

Antonella Granero, dopo una Laurea in Lettere Classiche e una carriera da giornalista, approda alla gestione delle risorse umane prima quale Dirigente nell'Autorità Portuale di Savona e quindi quale Direttore del Personale dell'Autorità di Sistema Portuale del Mar Ligure Occidentale. Arricchisce il suo percorso professionale e culturale con una seconda Laurea in Scienze delle Pubbliche Amministrazioni e due master universitari in Diritto del Lavoro pubblico e in Organizzazione e Innovazione nelle PA. Presso l'Autorità di Sistema Portuale del Mar Ligure Occidentale ricopre, dal 2024, anche l'incarico di Responsabile della Transizione al Digitale, oltre al coordinamento dello Staff Porto Digitale, Business Intelligence e Transizione al Digitale, che comprende, tra gli altri, il gruppo di lavoro che si occupa, nell'Ente, di cybersecurity.

Alberto Greco è SE di CrowdStrike per l'Italia. L'inizio in CrowdStrike avviene nel gennaio 2022 con lo scopo di seguire il team dedicato al mercato enterprise e mid-market; il suo ruolo è agire da punto di congiunzione tra le esigenze di business dei clienti e le soluzioni tecnologiche di CrowdStrike: dall'endpoint al cloud, dal mondo identity alla threat intelligence, dall'XDR all'IT Operations. In passato è stato SE Enterprise per l'intero portfolio Palo Alto Networks, SE in Forcepoint con focus sulla network security, technical trainer Fortinet in Exclusive Networks e, prima ancora, network security specialist in Thales

Alenia Space. Convinto sostenitore della frase "Se non lo sai spiegare in modo semplice, non l'hai capito abbastanza bene", Alberto è convinto che una diffusione della cultura CyberSec ad ogni livello sia fondamentale per una piena consapevolezza delle problematiche e, ancor più, delle opportunità che ne derivano.

Lorenzo Ivaldi, ingegnere elettronico e funzionario tecnico dell'Università di Genova è consulente in materia di sicurezza industriale. Oltre a svolgere attività di sistemista, esperto di sicurezza informatica ed informatico forense, è relatore in convegni e docente in master universitari negli stessi ambiti. È membro del comitato direttivo del Clusit, con delega per la formazione e sensibilizzazione in ambito industriale.

Mauro Leoncini è professore ordinario di Informatica presso il Dipartimento di Scienze Fisiche, Informatiche e Matematiche dell'Università di Modena e Reggio Emilia, dove è titolare dell'insegnamento di "Compilatori" per la laurea triennale e di "Algoritmi di crittografia" per la laurea magistrale. I suoi interessi di ricerca vertono nel più ampio settore degli algoritmi per diversi modelli di calcolo e della complessità computazionale. Su questi temi ha pubblicato una quarantina di lavori su rivista internazionale.

Federica Maria Rita Livelli, Certificata in Risk Management (FERMA/RIMAP certificazioni Iso 3100:2018) & Business Continuity (AMBCI Certification – BCI UK; CBCP Certification – DRI Usa), svolge consulenze in Risk Management & Business Continuity, oltre a effettuare un'attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni e università italiane e straniere. È membro del Comitato Direttivo di CLUSIT, del BCI Cyber Resilience Group e del FERMA Digital Committee, del Comitato Scientifico di ENIA e di diversi comitati tecnici UNI. Speaker e moderatore a convegni nazionali e internazionali, è altresì autrice di numerosi articoli inerenti alle tematiche di Risk Management & Business Continuity, Cybersecurity e Resilience pubblicati da diverse riviste italiane e straniere. Co-autrice dei Rapporti Clusit 2020-2021-2022-2023-2024-2025 e di "Lo stato in Crisi" ed. Franco Angeli.

Luca Nilo Livrieri è il Direttore della struttura di Sales Engineering di CrowdStrike per il Sud Europa. L'ingresso in CrowdStrike avviene nel maggio 2021, con la responsabilità di seguire lo sviluppo e la crescita della struttura di prevendita nel Sud Europa e Israele. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, AI, sicurezza, cloud e digital transformation fra cui Clusit Security Summit, di cu è anche autore del rapporto, ISMS forum, IDC, Cybersecurity Italy, Tisec e Cybertech. Prima di Crowdstrike, Livrieri è stato manager per l'Italia, la Spagna e il Portogallo della struttura prevendita di Forcepoint. Ha maturato esperienze come membro dell'"Office of the CSO" e Senior SE per il mercato enterprise, e la formazione e affiancamento del canale di rivendita in Websense e Surfcontrol. Prima di svolgere il ruolo di SE ha lavorato come consulente Gfi-Ois per la programmazione web presso alcune importanti aziende italiane. Precedentemente ha conseguito la Laurea magistrale in Comunicazione nella Società dell'Informazione, con tesi specialistica presso il dipartimento di informatica dell'Università Degli Studi Di Torino.

Mirco Marchetti è Professore Associato presso il Dipartimento di Ingegneria "Enzo Ferrari" dell'Università di Modena e Reggio Emilia, dove insegna "Sicurezza Informatica" e "Automotive Cyber Security". Ha conseguito il Dottorato di Ricerca in Information and Communication Technologies nel 2009 presso la stessa università. I suoi interessi di ricerca includono la Sicurezza informatica per i sistemi cyber-fisici e le interazioni tra Sicurezza informatica e intelligenza artificiale.

Joram Marino è ICT Manager con una consolidata esperienza nella progettazione, realizzazione e gestione di architetture telematiche. La sua leadership si distingue per la capacità di definire strategie efficaci, coordinare team multidisciplinari e risolvere criticità, perseguendo l'equilibrio ottimale tra innovazione tecnologica e stabilità operativa e promuovendo un ambiente di lavoro collaborativo. Nel 2019 intraprende un percorso di formazione umanistica con la laurea triennale in Lettere, seguita dalla magistrale in Scienze Cognitive, per integrare competenze tecniche e approccio umanistico. Questa duplice prospettiva gli

consente di affrontare le sfide della cybersecurity e della trasformazione digitale con una visione più ampia e inclusiva.

Giuseppe Molinari (Modena 1962) ha conseguito la laurea in Ingegneria Meccanica a Bologna nel 1987 e dopo aver lavorato per 5 anni in Ferrari Auto Spa, oggi ricopre la carica di Amministratore Delegato nell'azienda Caffè Molinari spa di cui è socio. Ha assunto nel tempo alcuni incarichi di natura istituzionale: tra il 2009 e il 2018 è stato Consigliere in Confindustria Modena e Confindustria Emilia Romagna, Presidente di Confindustria Servizi Modena. Dal 2018 è Presidente della Camera di Commercio di Modena, dal 2021 Consigliere della Fondazione Casa Natale Enzo Ferrari e dal 2022 è Presidente del Centro Sudi Guglielmo Tagliacarne di Unioncamere.

Marco Molinari, appassionato da sempre di tecnologia e informatica, dopo la laurea in Ingegneria Elettronica ha intrapreso il proprio percorso professionale nel settore ICT, inizialmente in ambito privato e successivamente nella pubblica amministrazione. Ha conseguito un Master in Innovazione e trasformazione digitale nella pubblica amministrazione e frequentato corsi di perfezionamento in ambito cybersecurity. Attualmente ricopre il ruolo di Responsabile dell'Ufficio Evoluzione Digitale e Tecnologie Informatiche dell'Autorità di Sistema Portuale del Mar Ligure Occidentale. Nel corso della sua carriera ha partecipato a numerosi progetti di digitalizzazione, evoluzione tecnologica e sicurezza informatica, integrando competenze tecniche maturate in oltre 20 anni di esperienza con un approccio analitico e multidisciplinare. È responsabile del gruppo di lavoro Cybersecurity dell'Ente ed è referente NIS2.

Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed interna-

zionali. All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate. Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching. Alessio è inoltre membro del Comitato Scientifico di Clusit, membro del Comitato Direttivo di AIP -Associazione Informatici Professionisti, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.

Pier Luigi Rotondo è Advanced Technical Leader per i prodotti e le soluzioni IBM. Ha contribuito a molti progetti, nazionali e internazionali, su soluzioni per il Threat Management, Threat Intelligence, Attack Surface Management, Identity e Access Governance, e Single Sign-on. Con una laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di sicurezza delle informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Scrive articoli divulgativi, e contribuisce dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia su temi di cybercrime nel settore finanziario, presentando le tendenze del mercato della cyber security. È stato membro del Comitato Scientifico del CLUSIT dal 2021, ora è membro del Comitato Direttivo.

Andrea Rui ha sviluppato una forte passione per l'Informatica sin dal 1982, spaziando nel corso degli anni attraverso molteplici ambiti dell'Information Technology. Si è occupato anche di programmazione in molti linguaggi, di computer graphics e di OCR della scrittura manuale mediante algoritmi autoadattivi. Nel corso della sua carriera ha ideato, progettato e realizzato sistemi per il trattamento automatico della messaggistica nel settore del trasporto aereo e sistemi per la valutazione del rischio per la protezione delle informazioni sensibili. Si è laureato in Informatica ed ha conseguito certificazioni in ambiti attinenti, come l'auditing di sistemi informativi, la business continuity e la sicurezza del

cloud. Oltre a essere membro attivo di Clusit, partecipa ad altre associazioni del settore, contribuendo con la sua esperienza e passione. È un convinto sostenitore della condivisione della conoscenza e si considera un "evangelist" del software libero e delle licenze copyleft, promuovendo costantemente la cultura open source. Da oltre vent'anni, Andrea è impegnato nel campo della Cybersecurity, un ambito che non solo approfondisce professionalmente, ma cerca di diffondere anche nella vita quotidiana. Attraverso interventi nelle scuole, si dedica a sensibilizzare giovani e meno giovani sull'importanza della sicurezza digitale. È membro del GdL che coordina il progetto "SicuraMente Clusit", il cui obiettivo è promuovere la cultura della sicurezza informatica nelle scuole.

Leonardo Sartore, diplomato in "Industrial Cyber Security" presso l'ITS Academy Meccatronico Veneto, ricopre il ruolo di Information & Cyber Security Advisor in Partners4Innovation. Affianca quotidianamente diverse realtà nazionali su tematiche di Compliance, Security Governance e Data Protection. Le sue principali aree di competenza comprendono la tutela del patrimonio informativo aziendale e la protezione dei dati personali. Collabora con gli Osservatori del Politecnico di Milano come relatore di webinar su tematiche di Information & Cyber Security.

Sofia Scozzari, appassionata di tecnologia da sempre, ha maturato oltre 15 anni di esperienza nella Cyber Security. Ha lavorato come System Administrator, ICT Consultant, Project Manager, Pre-sale, Cyber Security Consultant e Cyber Security Manager per principali società Italiane e multinazionali. Già CEO e COO di iDIALOGHI, società di consulenza e formazione in ambito Cyber Security, è stata anche co-founder di Security Brokers, cooperativa di Global Cyber Defense & Security Services. Da 4 anni risiede negli Emirati Arabi Uniti dove ha fondato e dirige Hackmanac, con cui elabora dati sulle minacce Cyber a supporto di attività di Threat Intelligence e Risk Management. È nel Comitato Direttivo di Women For Security, la Community delle Cyber Ladies italiane con cui partecipa ad iniziative a supporto della Cyber Security Awareness, dai corsi di formazione per scuole ed aziende ad eventi di settore. Membro del Comitato Scientifico CLUSIT, fin dalla prima edizione nel 2011 contribuisce come co-autore al Rapporto Clusit, curando l'analisi di migliaia di attacchi informatici ogni anno e diversi approfondimenti verticali. È inoltre

autrice di diversi articoli e guide in tema di Cyber Security, e co-autrice dei paper «La Sicurezza dei Social Media» (2014, Oracle Community for Security), e «Blockchain & Distributed Ledger: aspetti di governance, security e compliance» (2019, CLUSIT).

Claudio Telmon, è membro del Comitato Direttivo del Clusit e Senior Partner - Information & Cyber Security at P4I - Partners4Innovation. Attivo nel campo della sicurezza da più di venti anni, ha gestito il laboratorio di sicurezza del Dipartimento di Informatica dell›Università di Pisa, ed in seguito ha continuato a collaborare con il Dipartimento per attività di didattica e di ricerca, in particolare nel campo della gestione del rischio. Si è occupato come professionista dei diversi aspetti tecnologici e organizzativi della sicurezza, lavorando per aziende del settore finanziario, delle telecomunicazioni e per pubbliche amministrazioni.

Mario Testino, Ingegnere elettronico, dirigente d'azienda, Managing Director di ServiTecno, è docente universitario a contratto, vanta una consolidata esperienza nella progettazione e la realizzazione di soluzioni per la digitalizzazione industriale e l'Industry 4.0, ed in particolare: Networking e Cyber Security e i relativi standard internazionali. Nella sua carriera professionale ha fatto consolidate esperienze, in multinazionali e PMI, come responsabile di Business Unit e di Divisione in aziende di produzione di componenti elettronici ed informatici e di sistemi elettronici per i settori Energia, Industria e Trasporti. Nell'ambito industriale, in particolare, ha sviluppato una lunga esperienza nelle problematiche legate alla qualifica dei sistemi e delle infrastrutture informatiche e di rete nel settore farmaceutico.

Enzo Maria Tieghi, imprenditore, informatico, milanese, da oltre 40 anni si occupa di software per automazione e controllo di impianti, di security e compliance a standard e normative in diversi settori industriali in cui è attiva ServiTecno, azienda di cui è Presidente. ServiTecno azienda da lui cofondata nel 1979, dal 1986 distribuisce e supporta software e sistemi per applicazioni industriali per controllo di processo, automazione di fabbrica, supervisione impian-

ti e monitoraggio infrastrutture nell'industria e nelle utility. Tieghi è attivo in Associazioni di settore (quali Clusit, AIIC, ISPE, Anipla, ISA, AFI, ecc.), a lungo ha fatto parte del Comitato Scientifico di Clusit, tiene spesso lezioni e partecipa come organizzatore e relatore ad eventi specialistici sia in Italia che all'estero, oltre a contribuire con articoli e memorie a riviste specializzate e conferenze internazionali. Tieghi è stato l'autore del Quaderno Clusit "Introduzione alla protezione di reti e sistemi di controllo ed automazione (DCS, SCADA, PLC, ecc.)" (vedi https://clusit.it/pubblicazioni/) e ha curato l'edizione italiana del Volume TNO report "SCADA Security Good Practices per il settore delle acque potabili" per Franco Angeli Editore.

Anna Vaccarelli è Presidente del Clusit. E' stata Dirigente Tecnologo al Consiglio Nazionale delle Ricerche (CNR) nell' Istituto di Informatica e Telematica di Pisa. Per quasi 15 anni, a partire dal 1998, si è occupata di ricerca nel settore delle cybersecurity e dal 2010 di divulgazione del digitale in generale e della cybersecurity in particolare. Dal 2004 al 2012 è stata docente del corso di sicurezza informatica al Master congiunto Università di Pisa-Cnr in Tecnologie Internet. Nel 2011 ha ideato e poi coordinato fino al 2024, il progetto di formazione Ludoteca del Registro.it, un'azione di diffusione della cultura di internet nelle scuole, focalizzata soprattutto sulla cybersecurity, incontrando oltre 20.000 studenti. Nel dicembre 2021 ha ricevuto dall'Associazione Informatici Professionisti il premio come miglior informatico dell'anno. Negli anni ha coordinato numerosi progetti di ricerca nazionali e internazionali e scritto oltre 100 pubblicazioni scientifiche e tecniche. Dal 2020 è nel comitato direttivo delle Women For Security e dal 2022 nel comitato direttivo di Clusit.

Federica Vennitti è una studentessa impegnata nella valorizzazione del patrimonio artistico e culturale attraverso le nuove tecnologie. Dopo una laurea in Didattica e Comunicazione dell'Arte all'Accademia di Belle Arti di Bologna, ha proseguito la sua formazione con una specializzazione in Informazione, culture e organizzazione dei media all'Università di Bologna, affiancata da un percorso in Giurisprudenza dedicato alla tutela del patrimonio artistico. La sua ricerca si concentra sulla rottura dei tabù sociali e sulla valorizzazione delle tradizioni della sua regione d'origine. Attualmente si sta specializzando in Digital Humanities e

Cybersecurity for Cultural Heritage, sviluppando progetti legati alla protezione digitale del patrimonio culturale.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. È membro del Comitato Scientifico del Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

Il Clusit, **nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano**, è la più numerosa e autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre **700 organizzazioni**, appartenenti a tutti i settori del Sistema-Paese.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar CLUSIT.
- Ricerca e studio: Premio "**Innovare la Sicurezza delle Informazioni**" per la migliore tesi universitaria arrivato alla 21ª edizione.
- Le Conference specialistiche: i Security Summit On Site (a Milano, Roma, Napoli, Cagliari, Firenze, Verona, in Puglia e in Sicilia), gli Atelier della Security Summit Academy, Le Tavole Rotonde Verticali (Energy & Utilities, Health Care, Finance, Manufacturing), gli Atelier della Security Summit Academy, i Security Summit Streaming Edition.
- I Gruppi di Lavoro della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sulla sicurezza ICT in Italia, in produzione dal 2012; Rapporti di approfondimento nei settori P.A., Energy e Utilities, Healthcare e Manufacturing.
- Il progetto "SicuraMente Clusit" con attività di formazione nelle scuole sul territorio.

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Autorità Garante per la tutela dei dati personali, Cyber 4.0 - il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, Start 4.0, Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, 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), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni. Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.
La partecipazione è libera e gratuita, con il solo obbligo dell'iscrizione online.

Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.
Certificata dalla folta schiera di **relatori** (**più di 700** sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre **20.000 partecipanti**, e sono stati rilasciati circa 15.000 attestati validi per l'attribuzione di oltre **48.000 crediti formativi** (CPE).
Nel 2025 i Security Summit sono stati oggetto di oltre **800 articoli e servizi su web, cartaceo, Radio e TV.**

Gli eventi del 2025

Dopo le edizioni in presenza a **Milano** in marzo, a **Roma** in giugno, a **Napoli** in settembre e a **Verona** in ottobre, abbiamo chiuso l'anno con una **Streaming Edition.** Tra gli eventi **Verticali**, se ne sono tenuti 4: **Energy & Utilities** (in maggio), **Health Care** (in giugno), **Manufacturing** e **Finance** (entrambi in novembre).

L'edizione 2026

In presenza, inizieremo con la tappa di **Milano dal 17 al 19 marzo**, cui seguiranno: **Roma**, **Napoli**, **Firenze** e **Verona** e almeno un'altra tappa nel Sud (in **Puglia** e/o in **Sicilia**). Tra gli eventi in streaming, invece: **3/4 Verticali** ed alcuni **Atelier** della **Security Summit Academy**.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882
- Altre informazioni: info@astrea.pro
- Informazioni per la stampa: press@securitysummit.it
- Sito web: www.securitysummit.it/

SECURITY SUMMIT

www.securitysummit.it